Installing and Configuring VMware Workspace Portal

Workspace Portal 2.0

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

EN-001428-00
You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/
The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com
Contents

1 About Installing and Configuring VMware Workspace Portal  5

2 Installing VMware Workspace Portal  7
   Workspace User Authentication  8
   System and Network Configuration Requirements  8
   Preparing to Deploy Workspace  12
      Download Workspace  13
      Creating DNS Records and IP Addresses with Reverse Lookup  13
      Deployment Checklists  14
   Deploying Workspace  16
      Install the OVA File in the vSphere Client  16
      Configure Basic Workspace Settings  17
      Set Up Workspace  18
      Update Workspace Settings with Connector  29
      Add Desktop Client Installer Files to service-va Virtual Machines  30

3 Configuration for Workspace Virtual Machines  31
   Configuring Workspace in an Active Directory Forest  32
      Configuring Workspace in a Multi-forest Active Directory Environment  32
      Configuring a Multidomain Active Directory Single Forest  34
   Customizing the Demo User Store  35
      Add a User to the Demo User Store  36
      Add Groups and Assign Users to Groups in the Demo User Store  38
   Integrating VMware ThinApp Packages  39
      Workspace Requirements for ThinApp Packages and the Network Share Repository  39
      Create a Network Share for ThinApp Packages That Workspace Manages  43
      Configuring Workspace Access to ThinApp Packages  44
      Change the ThinApp Packages Share Folder  47
   Integrating Workspace with Citrix-based Applications  47
      Enabling Citrix PowerShell Remoting on Citrix Server Farm  50
      Preparing and Installing Integration Broker  52
      Deploying Integration Broker  53
      Synchronizing Workspace Connector with Integration Broker  56
   Integrating View  58
      Join an Active Directory Domain  58
      Sync View Pools  59
      Configure SAML Authentication  60
      Set Proxy Server Settings for Manager  63
4 Advanced Configuration for VMware Workspace Portal Virtual Machines  65
   Enabling External Access to Workspace  66
      Establish SSL Trust between Workspace vApp and Load Balancer  67
      Enable AUDIT Events via Proxy Server  68
   Configuring Redundancy/Failover for Workspace Virtual Machines  69
      Create Multiple gateway-va Virtual Machines  69
      Create Multiple service-va Virtual Machines  70
      Create Multiple connector-va Virtual Machines  72
   Update Workspace Settings with Configurator  76
      Change vCenter Administrator Password  77
      Enable the Syslog Server  77
      Use System Diagnostics Tool  78
   Configuring SecurID for Workspace  78
      Prepare the RSA SecurID Server for the Connector  79
      Configure SecurID with the Connector Web Interface  80
   Configuring Kerberos for Workspace  80
      Configure Internet Explorer to Access the Web Interface  82
      Configure Firefox to Access the Web Interface  83
      Configure the Chrome Browser to Access the Web Interface  84
   Using SSL Certificates in Workspace  84
      Apply an SSL Certificate from a Major or Private Certificate Authority  84
   Adjusting Java Heap Size for Improved Performance  85
      Update Java Heap Size on the connector-va Virtual Machine  85

5 Troubleshooting  87
   Setting for vCenter Server Quiesce Timeout Is Too Low  87
   Delete Unused Extensions from vCenter  87

Index  89
About Installing and Configuring VMware Workspace Portal

The VMware Workspace Portal Installation and Configuration Guide leads you through the installation and configuration process for the Workspace server. When the installation is finished, you can use VMware Workspace™ Portal to entitle users for managed, multi-device access to your organization's data and applications, including Windows applications, software as a service (SaaS) applications, and View desktops. Workspace includes a multiple virtual machine vApp, distributed as an Open Virtualization Archive (OVA) file. You deploy the vApp to vCenter. Workspace includes the following virtual appliances.

Table 1-1. Workspace Server Components

<table>
<thead>
<tr>
<th>Workspace Server Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Workspace Portal Configurator configurator-va</td>
<td>You start configuring Workspace with this virtual appliance, using both its console and the Configurator Web interface. The configurations you make with the configurator-va configurator-va are distributed to the other virtual appliances in the vApp.</td>
</tr>
<tr>
<td>VMware Workspace Portal Manager service-va</td>
<td>This virtual appliance gives you access to the MyApps and the Workspace Admin Console, from which you can manage users, groups, and resources.</td>
</tr>
<tr>
<td>VMware Workspace Portal Connector connector-va</td>
<td>The connector-va provides the following services: user authentication (identity provider), directory synchronization, and View pool synchronization.</td>
</tr>
<tr>
<td>VMware Workspace Portal Gateway gateway-va</td>
<td>The Workspace Gateway is the single endpoint for all end user communication. User requests come to the gateway-va virtual machine, which then routes the request to the appropriate virtual appliance.</td>
</tr>
</tbody>
</table>

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

End users can access their Workspace App Portal from the following browsers.

- Mozilla Firefox (latest)
- Google Chrome (latest)
- Safari (latest)
- Internet Explorer 8 or later
- Native browser and Google Chrome on Android devices
- Safari on iOS devices

Viewing Workspace pages with Internet Explorer 8 might not display all elements on the page correctly. For best viewing users should upgrade to a newer version.

**Intended Audience**

This information is intended for system and functional administrators of VMware® Workspace™. 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 appliances in the vApp. Knowledge of other technologies, such as VMware® ThinApp®, RSA SecurID, and Active Directory is helpful if you plan to implement those features.
Installing VMware Workspace Portal

Each deployment of Workspace has different requirements. You can select the appropriate installation tasks for your deployment.

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

Note: Load-balanced connectors use corporate network load balancers.
Workspace User Authentication on page 8
Workspace user authentication requires the use of one or more identity provider instances, which can be Connector instances, third-party identity provider instances, or a combination of both. The identity provider instances authenticate users with Active Directory within the enterprise network.

System and Network Configuration Requirements on page 8
When you install and configure Workspace in its basic configuration, you install the VMware Workspace Portal Configurator (configurator-va), VMware Workspace Portal Manager (service-va), VMware Workspace Portal Connector (connector-va), and VMware Workspace Portal Gateway (gateway-va) virtual appliances and use the interface of the configurator-va virtual appliance and the Web interface for configuration purposes.

Preparing to Deploy Workspace on page 12
Before you deploy Workspace, you must prepare your environment. This preparation includes downloading Workspace and creating DNS records and IP addresses with reverse lookup.

Deploying Workspace on page 16
To install Workspace, you must install the OVA file and run the Configurator's virtual appliance interface on vCenter Server. Otherwise, the installation fails. After Workspace is installed, you might need to configure additional parameters on the virtual machines in your environment.

Workspace User Authentication
Workspace user authentication requires the use of one or more identity provider instances, which can be Connector instances, third-party identity provider instances, or a combination of both. The identity provider instances authenticate users with Active Directory within the enterprise network.

Workspace authenticates users based on how you configure authentication methods, default access policy set, network ranges, and identity provider instances.

The identity provider instances that you use with Workspace create an in-network federation authority that communicates with Workspace using SAML 2.0 assertions. The identity provider instances authenticate the user with Active Directory within the enterprise network (using existing network security).

By default, Workspace supports the following authentication methods with the Connector:
- Active Directory password
- Kerberos
- RSA SecurID

System and Network Configuration Requirements
When you install and configure Workspace in its basic configuration, you install the VMware Workspace Portal Configurator (configurator-va), VMware Workspace Portal Manager (service-va), VMware Workspace Portal Connector (connector-va), and VMware Workspace Portal Gateway (gateway-va) virtual appliances and use the interface of the configurator-va virtual appliance and the Web interface for configuration purposes.

Prerequisites
- VMware™ vCenter and one or more ESX servers to deploy Workspace vApp.

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.

- The VMware™ vSphere client provides access to the virtual appliance interface. The vSphere client is required to deploy the Open Virtual Appliance (OVA) file to vSphere and to access the deployed virtual appliance remotely to configure networking.
The appropriate VMware licenses.

- The vApp virtual machines, Active Directory, and vCenter server must be in the same vLAN network. If they are not in the same vLAN network, they must be accessible to each other.

Consider your entire Workspace deployment, including how you integrate Workspace when you make decisions about hardware, resources, and network requirements. For example, you need more hardware for larger deployments. Review Chapter 4, “Advanced Configuration for VMware Workspace Portal Virtual Machines,” on page 65.

**Virtual Appliance Requirements**

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

**Table 2-1. VMware Workspace Portal Gateway Virtual Appliance (gateway-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>2GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>9GB</td>
</tr>
</tbody>
</table>

**Table 2-2. VMware Workspace Portal Manager Virtual Appliance (service-va) Requirements**

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2</td>
</tr>
<tr>
<td>Random-access memory</td>
<td>4GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>36GB</td>
</tr>
</tbody>
</table>

**Additional notes**

- A PostgreSQL database is included in the virtual appliance to make testing easier. For production, you must use an external database server (vPostgreSQL or Oracle). For information about specific database versions and service pack configurations supported with Workspace, see the VMware Product Interoperability Matrices at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

**Table 2-3. VMware Workspace Portal Configurator Virtual Appliance (configurator-va) Requirements**

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

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

**Note** You can convert (and scale) an internal PostgreSQL database to an external database at a later time.

- External database sizing information: 64GB for first 100,000 users. Add 20GB for each additional 10,000 users.
- Storage: 32GB

Ensure that the resources allocated to the virtual appliances meet the minimum requirements.
Table 2-4. VMware Workspace Portal Connector Virtual Appliance (connector-va) Requirements

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

**Note:** The service-va virtual machine automatically adjusts the Java heap size when you add memory. You must adjust the Java heap size manually for the connector-va and configurator-va virtual machines.

Table 2-5. Recommended Virtual Machine Requirements

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

**Network Configuration Requirements**

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

The connector-va virtual machine might need to join the Windows domain if Kerberos, View, or ThinApp functions are enabled. In that case, the connector-va virtual machine’s hostname must be in the same domain as the Active Directory.

Table 2-6. Network Configuration Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
</table>
| IP pool               | ■ Must be configured in vCenter and contain an appropriate subnet and gateway for the number of free static IP addresses used in the Workspace vApp, database, and any other load balancers.  
                        | ■ Must have a DNS server specified, even though the interface allows you to specify multiple DNS servers, only one must be defined.  
                        | ■ Must specify the DNS domain.  
                        | ■ IP pool network configuration is required. Workspace does not support transient addresses. |
| DNS records and IP addresses | Add DNS records and IP addresses with reverse lookup for each virtual appliance. |
| Firewall port         | Ensure that the inbound firewall port 443 is open for users outside the enterprise network to Workspace. |

**Port Requirements**

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

- To sync users and groups, the responsible connector-va virtual machine must connect to Active Directory.
- To sync with ThinApp, the responsible connector-va virtual machine must join the Active Directory domain and connect to the ThinApp Repository share.
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 machines.
Table 2-7. 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>

Preparing to Deploy Workspace

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

Prerequisites

- Before you proceed with your deployment, review Chapter 4, “Advanced Configuration for VMware Workspace Portal Virtual Machines,” on page 65. If you configure any of these options, the way you deploy might change.
- SMTP server is required.
- Download Workspace on page 13
  Download the Workspace OVA package file from the VMware Web site.
- Creating DNS Records and IP Addresses with Reverse Lookup on page 13
  A DNS entry and a static IP address that uses reverse lookup must be available for each virtual appliance in the vApp. Because each company administers their IP addresses and DNS records differently, before you begin your installation, consult your network administrator and request four DNS records and four IP addresses that use reverse lookup. You must have one IP address for each virtual appliance: VMware Workspace Portal Configurator (configurator-va), VMware Workspace Portal Manager (service-va), VMware Workspace Portal Connector (connector-va), and VMware Workspace Portal Gateway (gateway-va).
- Deployment Checklists on page 14
  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 machines when you create the static IP addresses in the DNS before the installation and during a Workspace installation.
Download Workspace

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

Creating DNS Records and IP Addresses with Reverse Lookup

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

Reverse Lookup and IP Addresses

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

You can use the following sample list of DNS records when you talk to your network administrator. Replace the sample information with information from your environment. This example shows forward DNS records and IP addresses.

Table 2.8. Examples of Forward DNS Records and IP Addresses

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

This example shows reverse DNS records and IP addresses.

Table 2.9. Examples of Reverse DNS Records and IP Addresses

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

Note After you complete the DNS configuration, verify that the reverse DNS lookup is properly configured. For example, the virtual appliance command `host IP_address` must resolve to 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.
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 machines when you create the static IP addresses in the DNS before the installation and during a Workspace installation.

Information for Configurator Fully Qualified Domain Name

Table 2-10. 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 Configurator (configurator-va)

Table 2-11. Configurator Network Information Checklist

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

Network Information for Manager (service-va)

Table 2-12. Manager Network Information Checklist

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

Network Information for VMware Workspace Portal Connector (connector-va)

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

Table 2-13. Connector Network Information Checklist

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

Network Information for Gateway (gateway-va)

Table 2-14. Gateway Network Information Checklist

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

**Table 2-15. IP Pools Network Information Checklist**

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

# Active Directory Domain Controller

**Table 2-16. 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>

# SMTP Server

**Table 2-17. SMTP Server Information Checklist**

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

# vCenter Credentials

**Table 2-18. vCenter Credentials Information Checklist**

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

# SSL Certificate (Optional)

**Table 2-19. 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.
Deploying Workspace

To install Workspace, you must install the OVA file and run the Configurator's virtual appliance interface on vCenter Server. Otherwise, the installation fails. After Workspace is installed, you might need to configure additional parameters on the virtual machines in your environment.

You can use the information in the deployment checklists that you completed to complete the installation. See “Deployment Checklists,” on page 14.

Install the OVA File in the vSphere Client

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

Prerequisites

- Log in to the vSphere Client.
- If the ESX host is part of a cluster, enable DRS in the cluster. If an ESX host belongs to a non-DRS cluster, all resource pool functionality is disabled. Deploying a vApp composed of multiple virtual machines automatically creates a resource pool. Because no reservation settings are added to the resource pool, it does not affect the other hosts and virtual machines in the cluster.
- Use Firefox or Chrome instead of Internet Explorer, or deploy the OVF file by using the VMware vSphere Client.

**IMPORTANT** Do not use the vSphere Web Client (also known as the vSphere Next Generation Client) with Internet Explorer to deploy the Workspace OVF file. If you use the vSphere Web Client with Internet Explorer to deploy the OVF file, the wizard displays junk characters.

Procedure

1. Select **File > Deploy OVF Template**.

   Respond to the prompts with information specific to your deployment.
### Table 2-22. Deploy OVF Template Information

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Type a URL or navigate to the OVA package location.</td>
</tr>
<tr>
<td>OVF template details</td>
<td>Verify that you point to the correct OVA template for this installation.</td>
</tr>
<tr>
<td>End user license agreement</td>
<td>Accept the end user license agreement.</td>
</tr>
<tr>
<td>Name and location</td>
<td>Name the vApp.</td>
</tr>
<tr>
<td>Storage</td>
<td>Select the location to store the virtual machine files.</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Select the provisioning type.</td>
</tr>
<tr>
<td>Network mapping</td>
<td>Select the network for each virtual machine to use. Ensure you select the virtual machine network associated with the IP pool you created.</td>
</tr>
<tr>
<td>IP address allocation</td>
<td>Select <strong>Fixed</strong> and type a static IP address.</td>
</tr>
<tr>
<td><strong>Note</strong> DHCP and transient IP addresses are not supported in Workspace. Only static IP addresses with reverse lookup are enabled.</td>
<td></td>
</tr>
<tr>
<td>Properties</td>
<td>1 Select the correct time zone.</td>
</tr>
<tr>
<td></td>
<td>2 Type the static IP address for each virtual appliance. The configurator-va, service-va, connector-va, and gateway-va virtual machines each use a static IP address.</td>
</tr>
</tbody>
</table>

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

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

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

### What to do next

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

### Configure Basic Workspace Settings

Before you deploy Workspace, you configure the network, SSL, and vCenter extension.

The Configurator virtual appliance interface guides you through the basic configuration. After the basic configuration is finished, you must perform more advanced configurations. You can return to the Configurator’s virtual appliance interface at any time to update these settings or to perform other configurations. For information about setting the advanced configurations, see Chapter 4, “Advanced Configuration for VMware Workspace Portal Virtual Machines,” on page 65.

**IMPORTANT** During deployment, leave the virtual appliances powered off. After deployment, the deployment process powers on the virtual appliances. If the virtual appliances are already on, an error occurs.

### Prerequisites

- Log in to vSphere Client.
- Verify that the vCenter administrator has privileges to the Workspace vApp or the resource pool that contains the Workspace vApp. See the vCenter Server 5.1 Documentation Center.
- Verify that you know the SMTP server name.
- Verify that the keyboard used to enter the root password is a standard en_US keyboard.

### Procedure

1 Select the vApp you deployed and expand it.
2 Select the configurator-va virtual machine and click the Console tab.

3 Press Enter to start the configuration.

If an error occurs, you might have a problem with your IP Pools.

4 If an error occurs, when prompted, select no.

This option shuts down the virtual machine. After you resolve the IP pool errors, you can return to the Configurator's virtual appliance interface. When you select yes on the Summary page, the configuration resumes from the point where you stopped.

5 Respond to the prompts with information specific to your deployment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global root password</td>
<td>Type and confirm the global root password to use for all five virtual appliances in Workspace.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: You must use a keyboard that is configured in the en_US layout to enter the root password. If you use a keyboard that is not the en_US layout, when you enter the root password later, you might receive a message that your password is incorrect. This can happen because the character keys on keyboards in other languages do not always correspond to the character keys on en_US keyboards.</td>
</tr>
<tr>
<td>SMTP server name</td>
<td>Type the SMTP server name.</td>
</tr>
<tr>
<td>SMTP port number</td>
<td>Type the SMTP port number.</td>
</tr>
<tr>
<td>vCenter IP address</td>
<td>Type the vCenter IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The Configurator virtual appliance registers a vCenter extension and queries the vCenter server periodically to check the status of the other virtual machines in the vApp.</td>
</tr>
<tr>
<td>vCenter port number</td>
<td>Type the vCenter port number.</td>
</tr>
<tr>
<td>vCenter admin username</td>
<td>Type the vCenter administrator's username. The vCenter administrator needs privileges only to the Workspace vApp or the resource pool that contains the Workspace vApp.</td>
</tr>
<tr>
<td>vCenter admin password</td>
<td>Type and confirm the vCenter administrator's password.</td>
</tr>
<tr>
<td>Is this correct?</td>
<td>Type y if all of the information is correct.</td>
</tr>
</tbody>
</table>

The Configurator virtual appliance processes your information. Depending on your network speed, this process can take 30 minutes or more.

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 configurator-va virtual machine. Then, you can continue with the deployment process. The new network settings are not available to the Configurator until after you reboot the configurator-va virtual machine.

**What to do next**

Configure the Workspace setup.

**Set Up Workspace**

You start installing Workspace by configuring certain basic settings.

**Prerequisites**

- Deploy the OVA File.
- Configure the basic Workspace settings. See “Configure Basic Workspace Settings,” on page 17.

Additional information is available about connecting to Active Directory, filtering users, and Workspace modules.
Procedure

1. Go to https://ConfiguratorHostname/cfg to start the Workspace Setup wizard. You must set a security exception when you see the message, This Connection is untrusted. See the instructions for your browser on setting security exceptions.

2. Type the license key that VMware provides and create an administrator password.
   This administrator account is a special account outside of your enterprise directory. If your connection to Active Directory is unavailable, you can use this account. You also use this username and password to access the Workspace Administrator, Configurator, and Connector Web interfaces directly.

3. Select an internal or external database.
   You can use the internal database for the proof-of-concept phase. Do not use the internal database server in production. For production, install and configure an external database server.
   **Note** You can change your selection later. See “Configuring an External Database,” on page 20.

4. Select the directory type and enter the directory information used in your environment.

5. Map the user attributes for Workspace to push from your directory to Workspace.
   **Important** If you plan to integrate with View, select the Required check box for UPN.

6. Start with the Base DNs to filter the users to synchronize with Workspace.
   You can also include or exclude users to narrow the results.

7. Add group information from your directory type to import to Workspace during the synchronization.
   You can assign a new name to your Directory group in Workspace. When you select a group, all members of the group are synced to Workspace. You can sync users from multiple DNs. Only users identified in the Base DN can be authenticated.

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

9. Verify the number of directory users and groups to add to Workspace.

10. Click Enable this module to enable the modules you select. You can enable additional modules later.

11. If you have your own certificate, paste an SSL certificate and a private key to the Workspace FQDN and SSL Certificate page. Otherwise, accept the default self-signed certificate.
   You must use the complete certificate chain and private key to gain external access service.

12. (Optional) Add the IP addresses for any load balancers or gateways between the Workspace gateway and the end user.
   These are the IP addresses that the gateway uses for client identification on the X-Forwarded-For page. The Workspace gateway uses the X-Forwarded-For header to identify source IP addresses from the browser client and determines which Connector to log in to based on this IP address. The IP addresses you add here are populated to all of the gateways in your environment.

13. When the setup is finished, click the Go to Workspace button and log in to the Workspace Web interface.
   The log in requires the Bind DN username and password that you entered when you set up a connection between Active Directory and Workspace. If you can log in to the Workspace Admin Console, your Workspace deployment was successful.
What to do next
Continue configuring Workspace including connecting to Active Directory, filters, Workspace modules, FQDN, and SSL certificates.

Configuring an External Database
The service-va virtual machine provides an internal PostgreSQL database for trial purposes only. It is recommended that you use an external database for production. If your production environment requires more than one service-va virtual machine for high availability and load balancing, you must use an external database.

You can configure an external database connection when you run the Workspace Setup wizard, or after you run the wizard, you can go to the Database Connections page in the Configurator.

Your database administrator must prepare an empty, external, Oracle, or PostgreSQL database and schema before connecting to the database in Configurator.

**Note** If you were using the internal trial database, Configurator automatically disables the internal database server when you connect to your external database server.

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.
   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 service-va virtual machine requires a minimum of 300 process connections to function with Workspace. For example, if your environment has two service-va virtual machines, run the `alter` command as sys or system user.
   a. Increase the process connections using the `alter` command.

```sql
alter system set processes=600 scope=spfile
```
   b. Restart the database.
Create a database trigger that all vApp users can use.

Table 2-23. Create Database Trigger SQL

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.

Table 2-24. Create a New Oracle 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 service-va virtual machine instance to the database.

**Note** The service-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.auto file.
   
   For example, the VMware vFabric PostgreSQL database location is `/var/vmware/vpostgres/current/pgdata/`.
3. Increase the `max_connections` parameter. Each additional service-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 service-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 2-25. Create a New Database Schema SQL**

Sample SQL to Create a New Database Schema

```sql
CREATE ROLE horizon LOGIN
PASSWORD yourpassword
NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION;
ALTER ROLE horizon
SET search_path = saas;
CREATE DATABASE saas
WITH OWNER = postgres
ENCODING = 'UTF8'
TABLESPACE = pg_default
CONNECTION LIMIT = -1;
GRANT CONNECT, TEMPORARY ON DATABASE saas TO public;
GRANT ALL ON DATABASE saas TO postgres;
GRANT ALL ON DATABASE saas TO horizon;
\connect saas;
CREATE SCHEMA saas AUTHORIZATION horizon;
CREATE EXTENSION citext SCHEMA saas;
```

**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 21.
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.

Use the Configurator to Configure Workspace to Use an External Database

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 Enterprise Edition as the external database server. For information on configuring a PostgreSQL database for Workspace, see “Configure a PostgreSQL Database,” on page 21. 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.
- Run the Configurator’s virtual appliance interface to start the initial Workspace configuration.

Procedure

1. Log in to Configurator.
2. Select External Database as the Database Type.
3. Enter information about the database connection.
   a. Type the JDBC URL of the database server.
      - PostgreSQL: `jdbc:postgresql://IP_address/soas?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: “soas”
   c. Type the password for the user you created when you configured your Oracle or PostgreSQL database.
4. Click Test Connection to verify and save the information.
What to do next

Finish changing the configuration settings in Workspace.

Establishing a Connection to Active Directory

Workspace includes the directory types, Active Directory and Demo User Store (for evaluation only). This configuration information establishes a connection between Workspace and Active Directory.

Directory Information

During the initial setup of Workspace 2.0, you establish a connection between Workspace and an Active Directory instance that is a single or multiple domain environment in a single forest. If your environment uses multiple forests and you plan to connect to Active Directory in a multi-forest environment, you must create a new connector-va virtual machine to connect with each forest. You configure your multi-forest environment after the initial setup, or later, after testing is complete. See the list below for more information:

- To establish a connection between a multi-forest Active Directory and Workspace, see “Configuring Workspace in a Multi-forest Active Directory Environment,” on page 32.
- For information about the global catalog and multiple domains in a single Active Directory forest, see “Configuring a Multidomain Active Directory Single Forest,” on page 34.
- To create multiple connector-va virtual machines, of the same type, in your single or multiple domain environment in a single forest for load balancing or failover, see “Create Multiple connector-va Virtual Machines,” on page 72.

Workspace uses this information to verify your end user’s credentials when they log in. See the table for details about the directory information you need to provide for your deployment.

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

Bind password  The text box for the Active Directory password for the Bind DN account.

Filter Types
You create queries to select the users to synchronize with Workspace. Depending on the type of query, you filter users by attribute and either include or exclude their attributes from the query to limit the users in the results. Processing time varies based on the type of query you run.

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

You can synchronize users from multiple DNs. However, you can authenticate only users under the Base DN that you defined in your directory.

Using an exclude filter is best when you want to exclude a small number of users. This method extracts all the users defined by DN first, and based on the filters you create, excludes the users you do not want to synchronize with Workspace. If you want to exclude hundreds of users, it is best to add additional user attributes to your query to include them rather than trying to exclude large numbers individually.

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

Create Queries to Filter Users
You create queries to filter users from a large group. The results of the query make it easier to select only the users to synchronize to Workspace.

Procedure
1. Create an exclude filter with the base DN.
   a. Type the DN where the users are located. For example, to include all the users in the base DN for Company A’s Active Directory, use the following query.
      ou=Users,DC=testDC,DC=acme,DC=com
   b. Create filters to exclude users you do not want to sync to Workspace using this syntax.
      name contains John Smith
2 Create an include filter with base DN user attributes.
   a Enter the DN that contains the users and append a semicolon (;) after the user base DN.
   b After the semicolon, add attribute information to narrow your query and include only the users to
      sync with Workspace. For example, to include only the sales team in Company A, use the
      following query.

      ou=Users,DC=testDC,DC=acme,DC=com;(&(objectClass=user)(objectCategory=person)(department=Sales))

      If you do not want to include additional user attributes in your query, do not use the default filter,
      (&(objectClass=user)(objectCategory=person)).

What to do next

After you create and run your query, you synchronize the users you selected with Workspace.

Workspace Modules

You use different modules to perform different types of tasks in Workspace, such as entitlement, adding, or
importing SAML-based Web applications. You enable the modules during set up or afterward in the
Configurator.

Table 2-26. Workspace Modules

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Applications</td>
<td>When this module is enabled, the administrator can add or import SAML-based Web applications for installation from a published global catalog hosted by VMware. After adding the Web applications to the Catalog, the administrator can grant users and groups access to these applications. Users can use single sign-on to access the SAML-based Web applications.</td>
</tr>
<tr>
<td>ThinApp Packages</td>
<td>When this module is enabled, access to ThinApp packages from a Windows network share is enabled. You must log in to the Connector and load the ThinApp packages. The administrator can entitle ThinApp packages to users and groups from the Manager Administrator Web interface, and end users can start these applications using the Workspace Client for Windows.</td>
</tr>
<tr>
<td>View</td>
<td>When this module is enabled, the administrator can sync information about the available View pools and entitlements from the View Connection Server. After it is enabled, end users can launch the View desktops they have access to from the Workspace Web interface. To enable the View module, you must join the Active Directory domain, sync the View Connection Server with it, and enable SAML authentication. See “Integrating View,” on page 58.</td>
</tr>
</tbody>
</table>

Workspace FQDN and SSL Certificates

Workspace includes a self-signed certificate. You can upload a trusted certificate later.

The SSL certificate works with Workspace only if you include the entire certificate chain when you
configure the SSL certificate setting. You must copy the certificate chain order exactly.

You use the option to generate certificates only when you install Workspace for evaluation. You must use
the appropriate third-party signed certificates in your production environment. The architecture used in a
production environment often includes a load balancer in front of Workspace.

Certificate Chain Example

```
-----BEGIN CERTIFICATE-----
SSL Cert - Workspace SSL Cert
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
Intermediate/Issuing CA Cert
-----END CERTIFICATE-----
```
Certificate Chain Example
-----BEGIN CERTIFICATE-----
Root CA Cert
-----END CERTIFICATE-----

Log File Information

During testing or troubleshooting, you will need feedback about the activity and performance of the virtual appliances as well as information about any problems that occur. Workspace includes these log files.

Table 2.27. Log File Information

<table>
<thead>
<tr>
<th>Component</th>
<th>Log File Name</th>
<th>Location of Log File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>horizon.log</td>
<td>/opt/vmware/horizon/horizoninstance/logs/horizon.log</td>
<td>Information about activity on the Workspace manager appliance, such as entitlements, users, groups, and so on.</td>
</tr>
<tr>
<td>Configurator</td>
<td>configurator-console.log</td>
<td>/opt/vmware/var/log/configurator-console.log</td>
<td>Configuration details from the vApp deployment and installation.</td>
</tr>
<tr>
<td></td>
<td>configurator.log</td>
<td>/opt/vmware/horizon/configuratorinstance/logs/configurator.log</td>
<td>Requests that the Configurator receives from the REST client and the Web interface.</td>
</tr>
<tr>
<td></td>
<td>catalina.log</td>
<td>/opt/vmware/horizon/configuratorinstance/logs/catalina.out</td>
<td>Apache Tomcat records messages that are not recorded by the configurator.log files.</td>
</tr>
<tr>
<td>Upgrade</td>
<td>update.log</td>
<td>/opt/vmware/var/log/update.log</td>
<td>A record of output messages related to update requests during an upgrade from Workspace 1.5 to Workspace 1.8 to Workspace 2.0. 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></td>
<td></td>
<td>/opt/vmware/var/log/vami</td>
<td></td>
</tr>
<tr>
<td>Connector</td>
<td>connector.log</td>
<td>/opt/vmware/horizon/workspace/logs/connector.log</td>
<td>A record of each request received from the Web client. Each log entry also includes the request URL, timestamp, and exceptions. No sync actions are recorded.</td>
</tr>
<tr>
<td>Gateway</td>
<td>access.log</td>
<td>/opt/vmware/nginx/logs/access.log</td>
<td>URLs that were requested and the status of each request.</td>
</tr>
<tr>
<td></td>
<td>error.log</td>
<td>/opt/vmware/nginx/logs/error.log</td>
<td>Errors reported from the Web server running on the gateway.</td>
</tr>
</tbody>
</table>

Caution Upgrading from Workspace 1.0 to Workspace 1.8 is not supported. You must upgrade from Workspace 1.0 to Workspace 1.5 to Workspace 1.8.

Workspace URLs

You use different URLs to access different Workspace Web interfaces.

Each interface gives you access to different functions. Each Web interface URL listed uses a placeholder, such as WorkspaceFQDN, ConnectorHostname, and ConfiguratorHostname for the hostname. Replace the placeholder names with the actual values.
**Table 2.28. Workspace URLs**

<table>
<thead>
<tr>
<th>URL</th>
<th>User Interface</th>
<th>What you can do here</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://WorkspaceFQDN/admin">https://WorkspaceFQDN/admin</a></td>
<td>Workspace Admin Console (Active Directory user)</td>
<td>Manage your catalog, users and groups, entitlements, reports, etc. (Log in as the Active Directory user with administrator role.)</td>
</tr>
<tr>
<td><a href="https://WorkspaceFQDN/SAAS/login/0">https://WorkspaceFQDN/SAAS/login/0</a></td>
<td>Workspace Admin Console (non-Active Directory user)</td>
<td>Use this URL if you cannot login as the Active Directory user with the administrator role. (Log in as an administrator using the username admin and the password you set during configuration.)</td>
</tr>
<tr>
<td><a href="https://WorkspaceFQDN/web">https://WorkspaceFQDN/web</a></td>
<td>App Portal</td>
<td>This URL brings you to the Active Directory user login page. From the Active Directory user login page, users can log in to Workspace to manage the resources available to them, such as Web applications and View pools.</td>
</tr>
<tr>
<td><a href="https://ConnectorHostname/hc/admin/">https://ConnectorHostname/hc/admin/</a></td>
<td>Connector Web interface</td>
<td>Configure additional ThinApp settings, View pool settings, Citrix published application settings, check directory sync status, or alerts. (Log in as an administrator using the password you set during configuration.)</td>
</tr>
<tr>
<td><a href="https://ConfiguratorHostname/cfg">https://ConfiguratorHostname/cfg</a></td>
<td>Configurator Web interface</td>
<td>See system information, check modules, set license key, or set admin password. (Log in as an administrator using the password you set during configuration.)</td>
</tr>
</tbody>
</table>

**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

End users can access their Workspace App Portal from the following browsers.

- Mozilla Firefox (latest)
- Google Chrome (latest)
- Safari (latest)
- Internet Explorer 8 or later
- Native browser and Google Chrome on Android devices
- Safari on iOS devices

Viewing Workspace pages with Internet Explorer 8 might not display all elements on the page correctly. For best viewing users should upgrade to a newer version.
Update Workspace Settings with Connector

After you configure Workspace, you can use the Connector to perform specialized Connector configurations, such as directory, user attributes, Windows auth, SecurID, Packaged Apps - ThinApp, Published Apps - Citrix, and so on.

Information is available for each of the pages that you use to change the Connector’s settings.

Table 2-29. Connector Settings

<table>
<thead>
<tr>
<th>Page Name</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>You can reset the Connector configuration, import the Connector configuration from a file, or export the Connector configuration to a file from the Configuration page.</td>
</tr>
<tr>
<td>Directory</td>
<td>“Establishing a Connection to Active Directory,” on page 24</td>
</tr>
<tr>
<td>User Attributes</td>
<td>“Workspace General Configuration and Individual Connector Configuration,” on page 35</td>
</tr>
<tr>
<td>Join Domain</td>
<td>“Configuring Workspace Access to ThinApp Packages,” on page 44</td>
</tr>
<tr>
<td>Windows Auth</td>
<td>“Workspace Authentication,” on page 73</td>
</tr>
<tr>
<td>SecurID</td>
<td>“Configure SecurID with the Connector Web Interface,” on page 80</td>
</tr>
<tr>
<td>Identity Provider</td>
<td>“Create Multiple connector-va Virtual Machines,” on page 72</td>
</tr>
<tr>
<td>SSL Certificate</td>
<td>“Using SSL Certificates in Workspace,” on page 84</td>
</tr>
<tr>
<td>Directory Sync</td>
<td>“Update Workspace Settings with Connector,” on page 29</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.</td>
</tr>
<tr>
<td>Packaged Apps - ThinApp</td>
<td>“Configuring Workspace Access to ThinApp Packages,” on page 44</td>
</tr>
<tr>
<td>View Pools</td>
<td>“Configure View Client to Use a Custom Port Number,” on page 62</td>
</tr>
<tr>
<td>Published App - Citrix</td>
<td>“Synchronizing Workspace Connector with Integration Broker,” on page 56</td>
</tr>
</tbody>
</table>

Procedure

1. Go to https://ConnectorHostname/hc/admin/.
2. Log in to the Connector with the administrator password.
3. Use the left navigation pane to select the page to view.

What to do next

Verify that the settings or updates you made have taken effect.
Add Desktop Client Installer Files to service-va Virtual Machines

When new versions of the Desktop clients are released, you copy and install a zip file that includes the Desktop client file for Windows computers from the VMware Downloads page to each service-va virtual machine that is configured. You run the `check-client-updates` command on each service-va virtual machine to deploy the installer files and restart the Tomcat service on each service-va virtual machine.

**Prerequisites**

- Users must have administrator privileges on their computers to install and automatically update the Desktop client. If users do not have administrator privileges, you can use software distribution tools to distribute and update the Workspace desktop applications to your users.
- Schedule adding these installer files to the service-va servers to run during a maintenance window since the service-va virtual machine is restarted and this might interrupt user access.

**Procedure**

1. Download the Workspace Desktop client zip file from the VMware Web site, https://my.vmware.com/web/vmware/downloads, to a computer that can access the service-va virtual machines.

2. Copy the zip file to a temporary location on the service-va virtual machine.

   ```
   scp clients-n.n.n-nnnnnnn.zip root@service-va.com:/tmp/
   ```

3. Log in to the service-va machine as the root user.

4. Unzip and install the new clients to the Downloads directory.

   ```
   /usr/local/horizon/scripts/check-client-updates.pl --install --clientfile /tmp/clients.n.n.n-nnnnnn.zip
   ```
   
   This script automatically unzips the file and copies the Desktop clients' installer file for the Windows computers to the /opt/vmware/horizon/horizoninstance/webapps/ROOT/client directory. It automatically updates to the /opt/vmware/horizon/horizoninstance/webapps/ROOT/client/cds directory, and updates the URL parameter value for the downloads link.

5. Restart the Tomcat service on the service-va virtual machine.

6. Repeat these steps on each service-va virtual machine in your environment.

   Users can download the Desktop clients from their Workspace accounts or via the download link, https://WorkspaceFQDN/download. Each user's Desktop clients are automatically updated.
Configuration for Workspace Virtual Machines

After you finish setting up Workspace, you might need to configure View and ThinApp integration, or clone virtual machines. You use the Configurator to perform these tasks.

- **Configuring Workspace in an Active Directory Forest** on page 32
  You can connect to Workspace from an Active Directory that uses single or multiple domains in a single or multiple forest environment. For each environment, you perform different configuration tasks when you establish a connection to Active Directory.

- **Customizing the Demo User Store** on page 35
  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.

- **Integrating VMware ThinApp Packages** on page 39
  To use Workspace to distribute and manage applications packaged with VMware® ThinApp®, you must have a ThinApp repository that contains the ThinApp packages, point your Workspace system to that repository, and sync the packages. After the sync process is finished, the ThinApp packages are available in your Workspace catalog and you can entitle them to your Workspace users and groups.

- **Integrating Workspace with Citrix-based Applications** on page 47
  Workspace supports Citrix-based applications. You can use Workspace to seamlessly integrate with existing Citrix deployments. Workspace also supports applications, such as View, ThinApp, SAAS, and so on.

- **Integrating View** on page 58
  To use View with Workspace, you must join the Active Directory domain and sync with the View Connection Server.

- **(Optional) Set Proxy Server Settings for Manager** on page 63
  Workspace Manager virtual machines access the global 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 Manager (service-va) virtual machine.
Configuring Workspace in an Active Directory Forest

You can connect to Workspace from an Active Directory that uses single or multiple domains in a single or multiple forest environment. For each environment, you perform different configuration tasks when you establish a connection to Active Directory.

During the initial set up of Workspace 2.0, you establish a connection between Workspace and an Active Directory instance that is a single or multiple domain environment in a single forest. If your environment uses multiple forests and you plan to connect to Active Directory in a multi-forest environment, you must create a new connector-va virtual machine to connect with each forest. You configure your multi-forest environment after the initial set up, or later, after testing is complete. See the list below for more information:

- To establish a connection between a multi-forest Active Directory and Workspace, see “Configuring Workspace in a Multi-forest Active Directory Environment,” on page 32.
- For information about the global catalog and multiple domains in a single Active Directory forest, see “Configuring a Multidomain Active Directory Single Forest,” on page 34.
- To create multiple connector-va virtual machines, of the same type, in your single or multiple domain environment in a single forest for load balancing or failover, see “Create Multiple connector-va Virtual Machines,” on page 72.

Configuring Workspace in a Multi-forest Active Directory Environment

To configure Workspace in a multi-forest Active Directory environment, you make configurations for the first forest and each additional forest as necessary, either as a single-domain forest or as a multidomain forest.

ATTENTION In a multi-forest Active Directory environment, Workspace does not support VMware View resources or Citrix-based applications. To enable Workspace users to access these resource types, you must integrate Workspace with a single Active Directory domain environment or a multidomain, single forest Active Directory environment.

The following steps describe the planning and tasks you need to perform to configure Workspace in a multi-forest Active Directory deployment.

Procedure

1. Plan how to integrate Workspace with your multi-forest Active Directory environment.
   - Decide, according to your organization’s needs, the number of user stores required and the best way to associate user stores to your Active Directory deployment per forest.
   - Determine the authentication types required to meet the needs of your organization. For example, you can configure Workspace to use Kerberos authentication for users internal to your organization and RSA SecurID authentication for users external to your organization.
   - Determine the mixture of Connector instances and third-party identity provider instances required in your deployment.
   - Determine how to configure high availability for the identity provider instances.

2. Install and configure Workspace to integrate with one of your Active Directory forests.
   - For a forest that consists of a single domain, see “Establishing a Connection to Active Directory,” on page 24 and follow the instructions for a single-domain Active Directory forest.
   - For a forest that consists of multiple domains, see “Configuring a Multidomain Active Directory Single Forest,” on page 34.
3 Add identity provider instances as required for each new forest you plan to integrate with Workspace, each additional authentication method you plan to add, and high availability purposes.

You can associate an identity provider with a forest. Decide which option best suits your deployment.

- For third-party identity providers, verify that Workspace can reach each identity provider instance.
- For the Connector, use the `hznAdminTool addvm` command with the `--activateOnly=y` option to add Connector instances to a multi-forest Active Directory environment. See “Manually Create a New connector-va Virtual Machine for Each Forest,” on page 33.
- Use the Connector Web interface to manually configure the Connector instances. A result of using the setting `--activateOnly=y` is that Workspace does not automatically configure the Connector instances, which requires you to manually configure them. See “Configure the New connector-va Virtual Machine,” on page 33.

4 For each identity provider instance, either the Connector or a third-party identity provider, use the Administrator Web interface to complete the configuration of user stores, network ranges, and authentication methods. For information about adding and configuring identity provider instances, see the Workspace Administrator’s Guide.

### Manually Create a New connector-va Virtual Machine for Each Forest

You must integrate your multi-forest Active Directory environment with Workspace 2.0 after installation. Each forest must connect with a dedicated connector-va virtual machine. To set up a path between the new connector-va virtual machine and each forest in your environment, you create an unconfigured connector-va virtual machine.

#### Prerequisites

- Deploy Workspace with one Active Directory.
- Create a connector-va virtual machine to point to a single forest by running the `addvm` command.

#### Procedure

1 Log in to the configurator-va virtual machine as the administrator.

2 From the command line, run the `addvm` command using the following parameters and values.

   ```bash
   hznAdminTool addvm --type=CONNECTOR --ip=xx.xxx.xxx.xxx --useGatewayAsIDP=n --ActivateOnly=y
   ```

   Set the `activateOnly` parameter to `y` to create a connector-va virtual machine. If the `activateOnly` parameter is set to `n`, the `addvm` command copies an old or existing Active Directory instead of creating a new connector-va virtual machine.

#### What to do next

After the `addvm` command runs, configure the connector-va virtual machine Web user interface.

### Configure the New connector-va Virtual Machine

After you create a connector-va virtual machine for each forest in your environment, you must configure the connector-va virtual machine in the Connector Web interface to establish a connection between the forest and Workspace.

If you want the new connector-va virtual machine to synchronize users and groups, define the new connector-va virtual machine as the sync client in the Web interface. If the sync client is not defined, when you attempt to sync users and groups with Workspace, Active Directory rejects the request and synchronization fails.

For more information about filtering Active Directory users and groups, see “Filter Types,” on page 25.
Prerequisites

Log in to each Connector Web interface as the administrator.

Procedure

1. Configure the connector-va virtual machine by entering the information for your environment on the Directory, Join Domain, Windows Authentication, Kerberos, SecurID pages, and so on.

2. Select the Enable Directory Sync check box.
   - You can configure backup synchronization clients by selecting the manual schedule option and setting the connector-va virtual machine as the default synchronization client.


4. Type the DN to include the users to synchronize.

5. (Optional) Add filters to restrict users from the synchronization.

6. Select the groups to include in the synchronization and click Next.
   - The synchronization starts.

After the synchronization finishes, a message displays that reports the number of users and groups added to Workspace.

What to do next

The connection between your multi-forest Active Directory environment is established. You can synchronize Active Directory with Workspace.

Configuring a Multidomain Active Directory Single Forest

If your deployment uses a multidomain Active Directory single forest, you must base the Workspace general configuration and individual Connector configuration on the Active Directory global catalog instead of LDAP.

Active Directory Global Catalog

The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory forest. The global catalog is stored on domain controllers that are designated as global catalog servers. The global catalog is distributed through multi-master replication.

Searches that are directed to the global catalog are faster because they do not involve referrals to different domain controllers. A global catalog server is a domain controller that stores a full, writable domain directory partition replica and a partial, read-only replica of all other domain directory partitions in the forest. The additional domain directory partitions are partial because only a limited set of attributes is included for each object. By including only the attributes that are most used for searching, every object in every domain in even the largest forest can be represented in the database of a single global catalog server.

The Active Directory replication system builds and updates the global catalog. The attributes that are replicated to the global catalog are identified in the schema as the partial attribute set (PAS) and are predefined by Microsoft. To optimize or extend searching, you can edit the schema by adding or removing attributes that are stored in the global catalog.

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

Active Directory uses ports 389 and 636 for standard LDAP queries, instead of ports 3268 and 3269 for global catalog queries. This configuration separates forest-wide queries that require a global catalog server from local, domain-wide queries that the domain controller in the user’s domain can service.
Users must log in to Workspace with a user principal name (UPN). When a user account is created, the UPN suffix is generated by default as userName@DnsDomainName, but an administrator can change this default setting.

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

**Workspace General Configuration and Individual Connector Configuration**

The installation and configuration of Workspace and the Connector for an Active Directory forest scenario is similar to that for a single domain scenario. You must configure a few of the Active Directory pages differently when your deployment uses an Active Directory forest.

**Table 3-1. Connector Web Interface Configurations Specific to an Active Directory Forest**

<table>
<thead>
<tr>
<th>Connector Web Interface Page</th>
<th>Location of Connector Web Interface Page</th>
<th>Configurations Specific to an Active Directory Forest</th>
</tr>
</thead>
</table>
| Directory                   | 1 Go to the Connector Web interface.  
2 Click the Advanced tab.  
3 Click Directory in the left navigation. | ■ Server Port: You enter the global catalog port number. The default ports for the global catalog are 3268 without SSL and 3269 with SSL.  
■ Search Attribute: Select userPrincipalName from the drop-down menu.  
■ Base DN: You leave the Base DN text box empty. |
| User Attributes             | 1 Go to the Connector Web interface.  
2 Click the Advanced tab.  
3 Click User Attributes in the left navigation. | ■ On the Map User Attributes page, map the Workspace userName attribute to the Directory userPrincipalName attribute. This mapping occurs because the userPrincipalName value is carried forward from the Directory page. Do not change this value from userPrincipalName.  
■ On the Map User Attributes page, add only attributes that are stored in the global catalog. To synchronize a special user attribute, such as employeeID, with Workspace, first add the attribute to the global catalog. |
| Select Users                | 1 Go to the Connector Web interface.  
2 Click the Advanced tab.  
3 Click Directory Sync in the left navigation.  
4 Click the Edit Directory Sync Rules button. | On the Select Users page, you can add users from multiple domains of the same Active Directory forest by clicking Add another in the DN section and providing another DN.  
On the Selected Groups page, multiple group DNs can exist. They are prepopulated with values from the Select Users page. You can use only universal groups. To synchronize special local or global group membership information with Workspace, you must change the scope of the group to universal. |

**Customizing the Demo User Store**

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 connector-va virtual machine. You can use standard LDAP commands to perform operations in the embedded OpenLDAP server. The required binaries (ldapadd, ldapsearch, ldopdelete, and ldopmodify) are installed on the virtual appliance.
You must use certain parameters when you configure OpenLDAP in the Configurator and Connector Web interfaces.

### Table 3-2. 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. Workspace stores the sample information on the connector-va virtual machine.

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 36 and “Add Groups and Assign Users to Groups in the Demo User Store,” on page 38.

### Table 3-3. 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>
<tr>
<td>Password for all</td>
<td>password</td>
</tr>
<tr>
<td>Sample group</td>
<td>testgroup1</td>
</tr>
<tr>
<td>The sample group,</td>
<td>contains ten sample users.</td>
</tr>
</tbody>
</table>

- **Add a User to the Demo User Store** on page 36
  
  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 38
  
  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 Connector 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 Connector 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 3-4. Sample ldapusers.ldif File

<table>
<thead>
<tr>
<th>Sample ldapusers.ldif</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a unique value for each parameter.</td>
</tr>
<tr>
<td>dn: cn=value,ou=users,dc=test,dc=example,dc=com</td>
</tr>
<tr>
<td>objectClass: user</td>
</tr>
<tr>
<td>objectCategory: person</td>
</tr>
<tr>
<td>cn: value</td>
</tr>
<tr>
<td>sn: value</td>
</tr>
<tr>
<td>sAMAccountName: value</td>
</tr>
<tr>
<td>canonicalName: value</td>
</tr>
<tr>
<td>mail: value</td>
</tr>
<tr>
<td>givenName: value</td>
</tr>
<tr>
<td>distinguishedName: cn=value,ou=users,dc=test,dc=example,dc=com</td>
</tr>
<tr>
<td>objectGUID: value (For example, cd0ff02b-f9d6-4fac-a5bc-6380d1867999.)</td>
</tr>
<tr>
<td>userPassword: value (For example, {SSHA}WbipwJh13Jdy2tHppdkFMzzNVSfksZ.)</td>
</tr>
</tbody>
</table>

What to do next
Generate an encrypted password for use by your Demo User Store users. See “Generate an SSHA Encrypted Password,” on page 37.

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
“Add a User to the Demo User Store,” on page 36.

Procedure
1. Open the Connector virtual machine.
2. Run the slappasswd command.
3 Type and verify a new password.
   The SSHA encrypted value appears.

4 Add this value to the ldif file to set the user password.

What to do next
Add groups and assign users to the Demo User Store.

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 Connector virtual machine.

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

2 Copy the ldif file to the Connector virtual machine.

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

   /usr/bin/ldapadd -h 127.0.0.1 -D cn=Manager,dc=test,dc=example,dc=com -w Horizon! -x -f ldif file path
   You can add multiple groups by using different values in a single ldif file.

4 Restart the LDAP service.

   /sbin/service ldap restart

Table 3-5. Example of the ldapgroups.ldif File

<table>
<thead>
<tr>
<th>Sample Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>dn: cn=value,ou=users,dc=test,dc=com</td>
</tr>
<tr>
<td>objectClass: group</td>
</tr>
<tr>
<td>objectCategory: group</td>
</tr>
<tr>
<td>sAMAccountName: value</td>
</tr>
<tr>
<td>canonicalName: value</td>
</tr>
<tr>
<td>mail: value</td>
</tr>
<tr>
<td>distinguishedName: cn=value,ou=users,dc=test,dc=example,dc=com</td>
</tr>
<tr>
<td>objectGUID: value (e.g. cd0f02b-f9d6-4fac-a5bc-6380d1867899)</td>
</tr>
<tr>
<td>member: User DN1 (e.g. cn=user1,ou=users,dc=test,dc=example,dc=com)</td>
</tr>
<tr>
<td>member: User DN2</td>
</tr>
<tr>
<td>member: User DN3</td>
</tr>
<tr>
<td>member: User DN4</td>
</tr>
</tbody>
</table>

What to do next

Use the Demo User Store for testing until you are ready to move Workspace in production.
Integrating VMware ThinApp Packages

To use Workspace to distribute and manage applications packaged with VMware ThinApp, you must have a ThinApp repository that contains the ThinApp packages, point your Workspace system to that repository, and sync the packages. After the sync process is finished, the ThinApp packages are available in your Workspace catalog and you can entitle them to your Workspace users and groups.

ThinApp provides application virtualization by decoupling an application from the underlying operating system and its libraries and framework and bundling the application into a single executable file called an application package. To be managed by Workspace, these packages must be enabled with the appropriate options. For example, in the ThinApp Setup Capture wizard, you select the Manage with Workspace check box. For more information about ThinApp features and how to enable your applications for management by Workspace, see the VMware ThinApp documentation.

Typically, you perform the steps to connect your Workspace system to the repository and sync the packages as part of the overall setup and configuration of your Workspace environment. The ThinApp repository must be a network share that is accessible to your Workspace Connector using a Uniform Naming Convention (UNC) path. The Connector synchronizes with this network share regularly to obtain the ThinApp package metadata that the Workspace system needs to be able to distribute and manage the packages. See “Workspace Requirements for ThinApp Packages and the Network Share Repository,” on page 39.

The network share can be a Common Internet File System (CIFS) or a Distributed File System (DFS) share. The DFS share can be a single Server Message Block (SMB) file share or multiple SMB file shares organized as a distributed file system. CIFS and DFS shares running on NetApp storage systems are supported.

- **Workspace Requirements for ThinApp Packages and the Network Share Repository** on page 39
  When you capture and store ThinApp applications to distribute from Workspace, you must meet certain requirements.

- **Create a Network Share for ThinApp Packages That Workspace Manages** on page 43
  If you want to enable the VMware ThinApp management capabilities of Workspace and allow users to access ThinApp packages from the user application catalog, you must create a network share and store the ThinApp packages in that network share folder.

- **Configuring Workspace Access to ThinApp Packages** on page 44
  To configure Workspace to provide users access to ThinApp packages, you must enable your Workspace system to locate the stored ThinApp packages and sync the packages with your system.

- **Change the ThinApp Packages Share Folder** on page 47
  After you configure Workspace access to your ThinApp packages, your IT environment might change such that your ThinApp packages are in a new location. When this situation occurs, use the ThinApp Packages page in the Connector Web interface to update the path to the new location.

**Workspace Requirements for ThinApp Packages and the Network Share Repository**

When you capture and store ThinApp applications to distribute from Workspace, you must meet certain requirements.

**Requirements on the ThinApp Packages**

To create or repackage ThinApp packages that Workspace can manage, you must use a version of ThinApp that Workspace supports. For information about specific ThinApp versions that are supported by Workspace, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
You must have ThinApp packages that Workspace can manage. In the ThinApp capture-and-build process, you can create packages that Workspace can manage or ones that it cannot manage. For example, when you use the ThinApp Setup Capture wizard to capture an application, you can make a package that Workspace can manage by selecting the Manage with Workspace check box. See the VMware ThinApp documentation for detailed information on ThinApp features and the appropriate parameters to use to create a package compatible with Workspace.

For existing ThinApp packages, you can use the relink -h command to enable the packages for Workspace. For information about how to convert existing ThinApp packages to packages that Workspace can manage, see the VMware Workspace Portal Administrator’s Guide.

You must store the ThinApp packages on a network share that meets the requirements for the combination of network share type, repository access, and desired ThinApp package deployment mode for your organization’s needs.

**Requirements on the Network Share Repository**

The ThinApp packages must reside on a network share, also known as the ThinApp package repository. The network share must be accessible using a Uniform Naming Convention (UNC) path from each system running the Workspace client used to access the ThinApp packages. For example, a network share named appshare on a host named server is accessible using the UNC path \server\appshare. The fully qualified hostname of the network share folder must be resolvable from your Workspace Connector.

The network share can be a Common Internet File System (CIFS) or a Distributed File System (DFS) share. The DFS share can be a single Server Message Block (SMB) file share or multiple SMB file shares organized as a distributed file system. CIFS and DFS shares running on NetApp storage systems are supported.

The network share must meet the criteria appropriate for the type of access you configure your Workspace Connector to use for accessing the ThinApp package repository: domain-based access or account-based access. The type of access determines the allowable combinations for the following items:

- Whether you use a CIFS network share or a DFS network share for the ThinApp package repository.
- Whether you must join your system’s Connector and the network share’s host to the same Active Directory domain.
- Whether the user’s Windows system must join the Active Directory domain to use the ThinApp packages.
- The ThinApp package installation mode that the installed Windows client program is set to use for obtaining and running the virtualized applications on the Windows system on which the client is installed. The package installation mode that is used on the user’s Windows system is set during the installation process when the Windows client is installed on that Windows system. This package installation mode determines the mode of ThinApp deployment used by that Windows system, download mode or streaming mode.
<table>
<thead>
<tr>
<th>Access Type</th>
<th>Network Share Type</th>
<th>Requirements on the Workspace Connector</th>
<th>Requirements for the User's Windows System</th>
</tr>
</thead>
</table>
| Domain-based access | You can use a CIFS share for your ThinApp package repository when you use domain-based access. You cannot use a DFS share for domain-based access. If you have a DFS share, you must use account-based access. | You must join your Workspace Connector to the Active Directory domain so that your Connector instance can join the Windows network share and access the packages. For more information about how to configure your Workspace Connector to join the domain, see “Configuring Kerberos for Workspace,” on page 80. **NOTE** Windows authentication is not required. The network share must support authentication and file permissions that are based on computer accounts. The Workspace Connector accesses the network share with the Connector’s computer account in the domain. The network share’s folder and file permissions must be configured such that the combination of permissions allows read access for the Connector’s computer account in the domain. | The user’s Windows system must join the Active Directory domain before that user can use their entitled ThinApp packages. The following systems must all be joined to the same domain:  
- The user’s Windows system  
- Your Workspace system’s Connector  
- The host of the network share drive with the ThinApp packages  
When you use domain-based access, the following installation modes for the ThinApp packages are allowed.  
- COPY_TO_LOCAL. With this installation mode, packages are downloaded to the client Windows system. This installation mode corresponds to using the ThinApp download mode for the virtualized application. The account that is used to log in to the client Windows system is the user account that is used to copy the packages from the network share to the client Windows system, and that account must have permissions to read the packages and copy the files from that network share. After the package is downloaded to the client Windows system and the user launches the package, the virtualized application runs locally on the client Windows system.  
- RUN_FROM_SHARE. With this installation mode, packages are not downloaded to the client Windows system. A user launches the packages using shortcuts on the local desktop and the virtualized applications run from the network share using ThinApp streaming mode. The account that is used to log in to the client Windows system is the user account that is used to run the packages from the network share, and that account must have permissions to read and execute files from that network share. **NOTE** RUN_FROM_SHARE is best suited for Windows systems that will always have connectivity to the ThinApp packages’ network share. Windows systems that best fit that description are Workspace desktops, because they are always connected to their domain. Floating, or stateless, Workspace desktops best use RUN_FROM_SHARE to avoid the resource usage inherent in downloading the packages to the Windows system.  
By default, the COPY_TO_LOCAL installation mode is set as the default installation mode when you install the Workspace for Windows client application on a Windows system by running the graphical version of the client’s installer program. To set a different installation mode as the default installation mode for the packages, you must run the command-line version of the client’s installer program. See the VMware Workspace Portal Administrator’s Guide. |
| Account-based access | You can use either a CIFS share or a DFS share for your ThinApp packages. | You must configure your Workspace system to use a share user account and password to access the ThinApp packages. | The user’s Windows system does not have to join the Active Directory domain before that user can use their entitled ThinApp packages. Windows authentication is not required. |
### Access Type

| ThinApp package repository when you use account-based access. |

#### Network Share Type

| Requirements on the Workspace Connector |

- network share and the packages. The share user account and password is any combination that has read access to the UNC path to the network share folder.
- You do not have to join your Workspace Connector to the Active Directory domain to access the network share.

#### Requirements for the User’s Windows System

- The user’s Windows system, your Workspace system’s Connector, and the host of the network share with the ThinApp packages do not have to be joined to the same Active Directory domain.
- When your Workspace system is configured to use account-based access, the following installation modes for the ThinApp packages are allowed:
  - If the user’s Windows system is not joined to the domain, the client must use the HTTPDOWNLOAD installation mode to obtain the virtualized application. This installation mode corresponds to using the ThinApp download mode for the virtualized application. The Connector uses the share user account to retrieve the packages from the repository.
  - If the user joins the Windows system to the domain, the client can use either the COPY_TO_LOCAL installation mode or the RUN_FROM_SHARE installation mode to run the user’s entitled ThinApp packages. The account that is used to log in to the client Windows system is the user account that is used to obtain the packages from the network share, and that account must have the appropriate permissions on the network share.
  - If the user’s Windows system might be joined to the domain at some times and not joined to the domain at other times, you can install the client with the COPY_TO_LOCAL mode and the AUTO_TRY_HTTP option enabled, as long as the Connector is configured for account-based access. With this configuration, the client first tries to use the COPY_TO_LOCAL mode to download the packages. If the Windows system is not joined to the domain at that time, that attempt to copy the packages fails. However, with the AUTO_TRY_HTTP option enabled, the client immediately makes an attempt to use HTTP to download the packages. This combination of COPY_TO_LOCAL and AUTO_TRY_HTTP is the default when you install the Workspace for Windows client application on a Windows system by running the graphical version of the client’s installer program. The Connector must be configured for account-based access for the attempt to download the packages using HTTP to succeed.

In addition, the ThinApp packages repository must meet the following criteria according to the described situation:

- When your settings involve systems joining the Active Directory domain, make sure that a disjoint namespace does not prevent domain member computers from accessing the network share that hosts the ThinApp packages. A disjoint namespace occurs when an Active Directory domain name is different from the DNS namespace that machines in that domain use.
- The network share’s file and sharing permissions must be configured to provide read access and the ability to run applications to those users that you want to run the ThinApp applications using the COPY_TO_LOCAL or RUN_FROM_SHARE option.

For example, for the Active Directory user accounts of those users that you want to run the ThinApp applications in streaming mode, setting the Shared Folder permission to Read and the NTFS permission to Read & Execute provides read access and the ability to run the applications to those users.
The NTFS permission setting of **Read & Execute** is required to run a ThinApp application using the ThinApp streaming mode, which corresponds to the Workspace for Windows client's RUN_FROM_SHARE installation mode. If your organization requires the NTFS permission set to **Read**, your users can use the ThinApp download mode for the virtualized application. ThinApp download mode corresponds to installing the Windows client with either the COPY_TO_LOCAL installation mode or HTTP_DOWNLOAD installation mode. With either of those installation modes, the applications are downloaded to the Windows systems and launched locally.

Both CIFS and DFS network shares must have the ThinApp packages organized in individual subdirectories in a directory under the namespace, not subdirectories in the namespace itself, such as `\\server\appshare\thinapp1`, `\\server\appshare\thinapp2`, and so on. See “Create a Network Share for ThinApp Packages That Workspace Manages,” on page 43.

### Create a Network Share for ThinApp Packages That Workspace Manages

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

Your Workspace Connector obtains the metadata it needs about the ThinApp packages from the network file share.

**Prerequisites**

- Verify that the ThinApp packages meet Workspace requirements.
- Verify that you have the appropriate access and permissions to create a network file share in your IT environment that meets Workspace requirements for ThinApp packages.

**Procedure**

1. Create a network share that meets the Workspace requirements for ThinApp packages.

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

   Typically, you name the subfolder to match the name of the ThinApp application, or indicate what application is in the folder. For example, if the network share is named `appshare` on a host named `server`, and the application is called `abceditor`, the subfolder for the ThinApp package is `\\server\appshare\abceditor`.

   **NOTE** Do not use non-ASCII characters when you create your network share subfolder names for ThinApp packages to distribute by using Workspace. Non-ASCII characters are not supported.

3. For each ThinApp package, copy its files, such as its EXE and DAT files, to the subfolder that is named for that package's virtualized application.

   After copying the files, you have a set of subfolders and files that are similar to these files:

   - `\\server\appshare\abceditor\abceditor.exe`
   - `\\server\appshare\abceditor\abceditor.dat`

**What to do next**

Configure your Workspace system’s access to the ThinApp packages.
Configuring Workspace Access to ThinApp Packages

To configure Workspace to provide users access to ThinApp packages, you must enable your Workspace system to locate the stored ThinApp packages and sync the packages with your system.

Prerequisites

- Create a network share with the appropriate configuration and store the ThinApp packages in the appropriate location in that network share. See “Create a Network Share for ThinApp Packages That Workspace Manages,” on page 43.

- Verify that you have the UNC path to the network share folder where the ThinApp packages are located.

- Verify that you have an Active Directory domain name and the username and password of an account in that Active Directory that has the rights to join the domain. Even if you are using account-based access, the Connector Web interface requires the completion of the Join Domain page before you can use the ThinApp Packages page in the Connector Web interface.

To enable domain-based access, you must also join the Connector to the same Active Directory domain to which the ThinApp package repository is joined. Verify that you have the Active Directory domain name for the domain that the network share uses and the username and password of an account in that Active Directory that has the rights to join the domain. The Active Directory account is used to join your Workspace Connector to the domain. See “Workspace URLs,” on page 27.

- When enabling account-based access, verify that you have a username and password that has permission to read the network share. See “Workspace Requirements for ThinApp Packages and the Network Share Repository,” on page 39.

**Note**  Unless you want to restrict use of the ThinApp packages to domain-joined Windows systems for all runtime situations, you should enable account-based access in addition to domain-based access. This combination provides the most flexibility for supporting runtime situations where users need to use their entitled ThinApp packages without joining their Windows systems to the domain.
Procedure

1. Join your Workspace Connector instance to an Active Directory domain.
   
   a. Log in to the Connector Web interface.
   
   b. Select the **Join Domain** tab.
   
   c. On the Join Domain page, type the information for the Active Directory domain and click **Join Domain**.

**IMPORTANT** Do not use non-ASCII characters when you enter the Active Directory (AD) domain name, AD username, or AD password. Non-ASCII characters are not supported in these entry fields in the Connector Web interface.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Directory</strong></td>
<td>Type the fully qualified domain name of the Active Directory. An example is <strong>HS.TRDOT.COM</strong>.</td>
</tr>
<tr>
<td><strong>AD Username</strong></td>
<td>Type the username of an account in the Active Directory that has permissions to join systems to that Active Directory domain.</td>
</tr>
<tr>
<td><strong>AD Password</strong></td>
<td>Type the password associated with the <strong>AD Username</strong>. This password is not stored by Workspace.</td>
</tr>
</tbody>
</table>

**IMPORTANT** Each time you import the Connector’s configuration you must rejoin the Connector to the domain.

The Join Domain page refreshes and displays a message that you are currently joined to the domain.
2  Enable your Workspace system to access the stored ThinApp packages.
   a  Select the Packaged Apps - ThinApp tab.
   b  Select the Enable packaged applications check box.
   c  Complete the information and click Save.

**IMPORTANT** Do not use non-ASCII characters for entries in the fields on this page. Non-ASCII characters are not supported in these entry fields in the Connector Web interface.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>Type the path to the shared folder where the ThinApp packages' folders are located, in the UNC path format <code>\server\share\subfolder</code>. For example: <code>\DirectoryHost\ThinAppFileShare</code>. For <code>DirectoryHost</code>, provide the hostname, not the IP address. For both CIFS and DFS network shares, this path must be a directory under the namespace, and not the namespace itself.</td>
</tr>
<tr>
<td>Choose Frequency</td>
<td>Select the interval at which you want the Connector to synchronize the information about the ThinApp packages located at the network share location with Workspace. For a weekly interval, set the day and time of day at which the syncing occurs. For a daily interval, set the time.</td>
</tr>
<tr>
<td>Enable account based access</td>
<td>Select this option if you want to use account-based access. <strong>Note:</strong> If your ThinApp package repository is a DFS network share, you must select this option. If you want the ability for users to use their entitled ThinApp packages on non-domain-joined Windows systems, you must enable account-based access.</td>
</tr>
<tr>
<td>Share User</td>
<td>Type the username for a user account that has read access to the network share. This information is used when Enable account based access is selected.</td>
</tr>
<tr>
<td>Share Password</td>
<td>Type the password associated with the Share User user account.</td>
</tr>
</tbody>
</table>

A message appears stating that the values are saved, and a summary of the last sync status is displayed.

3  Sync the ThinApp packages with your Workspace system by clicking Sync Now.

The time it takes to complete the sync process depends on the number of ThinApp packages.

When the sync process is done, a list of the ThinApp packages that were synced appears.

Your Workspace system is configured so that you can entitle groups and users to ThinApp packages, and those users can run their entitled ThinApp packages using the Workspace client installed on their Windows systems.

You can use the Dashboard page in the Workspace Admin Console to verify that the ThinApp Packages module is enabled and displays the number of ThinApp packages in your catalog.

**What to do next**

Entitle groups and users to ThinApp packages. See the *VMware Workspace Portal Administrator’s Guide*. 

---

46  VMware, Inc.
Change the ThinApp Packages Share Folder

After you configure Workspace access to your ThinApp packages, your IT environment might change such that your ThinApp packages are in a new location. When this situation occurs, use the ThinApp Packages page in the Connector Web interface to update the path to the new location.

Prerequisites

Verify that the new network share location adheres to the network share requirements as described in “Workspace Requirements for ThinApp Packages and the Network Share Repository,” on page 39.

Procedure

1. Log in to the Connector Web interface.
2. Select the Packaged Apps - ThinApp tab.
3. Change the value in the Path text box to the new shared folder where the ThinApp packages are located, in the UNC path format.
4. (Optional) If the previous network share was a CIFS share and the new share is a DFS share, select the Enable account based access check box and enter the name and password of a user who has read access to that network share.
5. Click Save.

Integrating Workspace with Citrix-based Applications

Workspace supports Citrix-based applications. You can use Workspace to seamlessly integrate with existing Citrix deployments. Workspace also supports applications, such as View, ThinApp, SAAS, and so on.

You can see more details about Workspace and Citrix farm synchronization in the Workspace and Citrix Farm Synchronization diagram. Workspace does not overwrite the settings in Citrix-based applications. Instead, it copies the information from the Citrix farm and reuses it in Workspace.
Workspace provides support for the following functions:

- Synchronize applications from a Citrix farm to Workspace.
- Synchronize entitlements from a Citrix farm to Workspace entitlement store.
- Launch Citrix-based applications using SSO.

Workspace uses the Integration Broker to deliver Citrix-based applications to the end user, including the following functions:

- Connector pushes Citrix farm information and publishes application information from the Citrix farm to the catalog based on configured synchronization.
- A Workspace tenant administrator can set the generic user settings template and the ICA launch template for all the resources in an organization. This template is saved as an organization artifact in the Workspace data store.
- Workspace tenant administrator can set the ICA launch template by resource in the Workspace catalog. This template is saved as part of the resource definition in the Workspace catalog.

The Connector synchronizes the Citrix-based applications and entitlements from the Citrix farm to the Workspace entitlement store. Synchronization occurs based on the frequency set in the schedule. The Citrix farm is the single source of truth for all supported operations in Workspace.

Workspace uses the Citrix Receiver to launch Citrix-based applications. The end user must install the Citrix Receiver on their device. The Citrix Receiver delivers the Citrix-based applications to the end user.
Workspace also provides multi-device support. End users can launch a Citrix-based application, such as Textpad, from Workspace on any device, such as a laptop, mobile device, domain-joined desktop, or non-domain-joined desktop.

The following table describes the administrator’s task on the Citrix farm and the corresponding operation that results after a synchronization with Workspace.

**Table 3-6. Workspace and Citrix Farm Synchronization**

<table>
<thead>
<tr>
<th>Action in the Citrix farm</th>
<th>Result after sync with Workspace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish a new application to the Citrix farm.</td>
<td>Connector creates the Citrix-based application in the Workspace catalog.</td>
</tr>
<tr>
<td>Edit an application in the Citrix farm.</td>
<td>Connector updates the Citrix-based application in the Workspace catalog.</td>
</tr>
<tr>
<td>Delete an application in the Citrix farm.</td>
<td>Connector deletes the entitlements associated with the Citrix-based application, and then Connector deletes the Citrix-based application from the catalog.</td>
</tr>
<tr>
<td>Add an end user entitlement for an application in the Citrix farm.</td>
<td>Connector creates an entitlement in the Workspace entitlement store to associate with the Citrix-based application and domain identities.</td>
</tr>
<tr>
<td>Remove an end user entitlement for an application in the Citrix farm.</td>
<td>Connector creates an entitlement in the Workspace entitlement store to associate with the Citrix-based application and domain identities.</td>
</tr>
</tbody>
</table>

Workspace does not require additional setup after an Workspace upgrade or a Citrix product upgrade to maintain the integration between Workspace and Citrix-based application support. To reinstall Citrix Receiver, see the Citrix documentation.

Workspace uses its own Integration Broker component and a Citrix SDK to handle SSO from Workspace to Citrix-based applications.
Enabling Citrix PowerShell Remoting on Citrix Server Farm

You must enable remote invocations between the Integration Broker and the Citrix farm. Citrix PowerShell Remoting requires a secure HTTPS channel to make remote calls. To enable this function, you must install a valid certificate from a certification authority.

**Prerequisites**

Verify that the instructions you use to set up Citrix PowerShell Remoting match the version of the Citrix server farm you use.

**Set Up Citrix PowerShell Remoting on Citrix Server Farm 6.5**

You must enable Citrix PowerShell remoting on every machine where you want to receive connections. Citrix PowerShell remoting enables connections between Integration Broker and the Citrix server farm.

**Procedure**

1. Install an SSL server certificate on each Citrix server farm host.
   
   For information about how to install an SSL server certificate, see the Microsoft documentation.

2. Click **Properties** and verify that Server Authentication is enabled for the certificate.

3. Enable Citrix PowerShell Remoting.
   a. Open **Citrix PowerShell Module > Program Files**.
   b. Type the `set-executionpolicy remotesigned` command.
c Type the `Import-Module` command.

```powershell
Import-Module C:\Program Files\Citrix\PowerShell\Modules\Citrix.XenApp.Commands.Remoting\Enable-XAPSRemoting.ps1
```

If the Citrix PowerShell modules are not installed in the default location, replace the default path with the path that is used in your environment.

d Type the `Enable-XAPSRemoting` command.

**Set Up Citrix PowerShell Remoting on Citrix Server Farm 5.0 or 6.0**

You must enable Citrix PowerShell remoting on every machine where you want to receive connections. Citrix PowerShell remoting enables connections between Integration Broker and the Citrix server farm.

**Prerequisites**

- If you do not have Winrm installed, download and install Winrm from the Microsoft Web site.

**Procedure**

1. Install an SSL server certificate on each Citrix server farm host.
2. Click **Properties** and verify that Server Authentication is enabled for the certificate.
3. Open the PowerShell console in the administrator mode.
4. Enable Citrix PowerShell Remoting.
   a. Type the `Get-Service winrm` command to verify that Winrm is installed on the server.
   b. Type the `Enable-PSRemoting` command.
      This command enables PowerShell Remoting on the server.
   c. Install the Citrix PowerShell SDK 5.0 or 6.0 depending on the Citrix server version.
   d. Enable winrm HTTPS listener from the command prompt.
      1. Create a certificate on the server.
      2. Record the certificate's thumb print.
      3. Verify that the certificate's thumb print is configured.
         ```powershell
         winrm quickconfig -transport:https
         ```
   e. Create the listener.
      ```powershell
      winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{"Hostname"="host FQDN";"CertificateThumbprint"="certificate thumbprint"}"
      ```
Preparing and Installing Integration Broker

Before you install Integration Broker, you must prepare your Workspace environment. You must verify that your software is installed and configured correctly.

**IMPORTANT** Workspace 2.0 does not install or require installation of any VMware software on Citrix servers.

Prepare Integration Broker Server for Windows Server 2008 or Windows Server 2012

Before you install Integration Broker, you must prepare your Workspace environment and verify that your software is installed and configured correctly.

**Prerequisites**

- Verify that Windows Server 2008 R2 or Windows Server 2012 are installed with the latest updates. To check for updates, select **Control Panel > Windows Update**.
- Install .NET Framework 3.5. When you install .NET, it installs version 3.5 as a feature. Verify that you include WCF activation.
- From the Add Role Service pane, install IIS 7 with 6.0 Management Compatibility Mode. You must also install the Management Tools if this is your only IIS 7 instance.
- Configure an application pool. You can use the default application pool or create an application pool that is dedicated to Integration Broker.

**NOTE** See the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php to verify version information.

**Procedure**

1. Configure the Integration Broker using the default application pool.
   a. Click the default application pool.
   b. Verify these requirements.
      - .NET framework version 2.0
      - Set 32-bit applications to true.
2 Configure Identity to use the same account as the Citrix published applications administrator.
   Integration Broker uses this account to authenticate.
   a Right-click the application pool.
   b Click Identity in the Advanced Settings dialog.
   c Click Custom Account and click Set.
   d Type the credentials for the Citrix published applications administrator username and password,
     Domain Name username and Domain Name password.

   Note Depending on your operating system, you might need to download either the 32-bit or 64-bit
   version of Microsoft Visual J#.

4 Depending on your version of Citrix Server Farm, download and install version 6.0 or 6.5 of Citrix
   PowerShell SDK from the Citrix Web site.
   a Set the execution policy for Citrix PowerShell Remoting.
   b If the Citrix XenApp Farm’s execution policy is configured to use remote sign on, you must add
     your root certificate to the Trusted Root Certification Authorities store. See the Microsoft Web site
     about adding root certificates to the store.
   c If the Citrix XenApp Farm’s execution policy is configured to unrestricted, you do not need to add
     root CAs to the Trusted Root Certification Authorities store.

5 Before you run this command, verify that PowerShell SDK is successfully installed.
   a Launch PowerShell SDK as administrator.
   b Verify PowerShell remoting.
     This sample command string applies to Citrix Server Farm 6.5.
     Get-XAApplication –ComputerName CITRIX SERVER NAME
     This sample command string applies to Citrix Server Farm 6.0.
     Invoke-Command –ComputerName XENAPP_HOST_NAME -ScriptBlock { Add-PSSnapin Citrix* ;Get-
       XAApplication } -Credential DOMAIN\USERNAME
   c Verify that the list includes all the applications hosted by Citrix.

What to do next
Deploy and configure Integration Broker.

Deploying Integration Broker
To deploy Integration Broker, you must run the Integration Broker installation and set up a secure channel
between Integration Broker and the Citrix server farm.

Attention It is recommended that you install only one instance of Integration Broker per Windows Server
instance.
Install Integration Broker

Workspace uses the Workspace Integration Broker component and the Citrix SDK to handle single sign-on between Workspace, Citrix server farms, and Citrix-based applications.

Prerequisites

Install Citrix PowerShell remoting. See the Citrix documentation for more information.

Procedure

1. Log in as a Windows administrator.
2. Open the IB.msi file to run the Integration Broker installation.
3. Type the Web location where you want to install the Integration Broker.
4. (Optional) If you created a separate pool for the Integration Broker, select your application pool.

⚠️ **CAUTION**  Do not change the Virtual Directory name.

5. Click Next to finish installing Integration Broker.

Set Up Integration Broker for HTTP and HTTPS Bindings

Citrix PowerShell Remoting requires a secure HTTPS channel to make remote calls. Without a secure HTTPS channel, you cannot enable remote invocations between Integration Broker and Citrix server farm.

A certificate is required to use the IIS Server. You can purchase or generate a certificate from a third-party root CA.

OpenSSL is installed by default. OpenSSL is an open source implementation of the SSL and TLS protocols.

Prerequisites

Mark the certificate key exportable. See the Microsoft documentation for more information on certificate keys.

Procedure

1. Add HTTPS binding to the Integration Broker Web site.
   a. Click Start > Run.
   b. Open inetmgr and right-click on the default Web site.
   c. Click Edit Bindings.
   d. Add the HTTPS binding using the newly created certificate in the drop-down menu.
2. Download the Citrix Web Interface SDK 5.4 (WISDK zip file) from the Citrix Web site.
3. After the installation is finished, unzip the wisdk.zip file.
4. Copy the contents from the WinSDK_SDK/zipfiles/sdkdemo/wisdk directory to the default bin directory at c:\inetpub\wwwroot\IB\bin.
5. Restart IIS.
6. Type http://hostname/IB/API/RestServiceImpl.svc/ibhealthcheck to verify that the Integration Broker Web application is running.

   The expected output displays.

   All ok
Type https://hostname/IB/API/RestServiceImpl.svc/ibhealthcheck to verify that the Integration Broker Web application is running.

The expected output displays.

All ok

Create a Self-signed Certificate Example

These instructions provide a sample for how to set a self-signed certificate using OpenSSL for Integration Broker.

Procedure

1 Create a self-signed certificate for the IIS server.

2 Create the ibcerts folder to use as the working directory.

3 Create a configuration file using the vi openssl_ext.conf command.
   a Copy and paste the following OpenSSL commands into the configuration file.

```
# openssl x509 extfile params
extensions = extend
[req] # openssl req params
prompt = no
distinguished_name = dn-param
[dn-param] # DN fields
  C = US
  ST = CA
  O = VMware (Dummy Cert)
  OU = Horizon Workspace (Dummy Cert)
  CN = hostname (Virtual machine hostname where the Integration Broker is installed.)
  emailAddress = EMAIL PROTECTED
[extend] # openssl extensions
  subjectKeyIdentifier = hash
  authorityKeyIdentifier = keyid:always
  keyUsage = digitalSignature,keyEncipherment
  extendedKeyUsage=serverAuth,clientAuth
[policy] # certificate policy extension data
```

NOTE Type the CN value before you save the file.
   b Run this command to generate a private key.

```
openssl genrsa -des3 -out server.key 1024
```
   c Type the passphrase for server.key, for example, vmware.
   d Rename the server.key file to server.key.orig.

```
mv server.key server.key.orig
```
   e Remove the password associated with the key.

```
openssl rsa -in server.key.orig -out server.key
```

4 Create a CSR (certificate signing request) with the generate key. The server.csr is stored in your working directory.

```
openssl req -new -key server.key -out server.csr -config ./openssl_ext.conf
```
5 Sign the CSR.

openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt -extfile openssl_ext.conf

The expected output displays.

Signature ok subject=/C=US/ST=CA/O=VMware (Dummy Cert)/OU=Horizon Workspace (Dummy Cert)/CN=w2-hwdog-xa.vmware.com/emailAddress=EMAIL PROTECTED

Getting Private key

6 Create P12 format.

openssl pkcs12 -export -in server.crt -inkey server.key -out server.p12

a Press Enter at the prompt for an export password.

IMPORTANT Do not enter a password.

The expected output is server.p12 file.

b Move the server.p12 file to the Windows machine where Integration Broker is installed.

c From the Command Prompt, type mmc.

d Click File > Add or Remove Snap-ins.

e In the Snap-in window, click Certificates and click Add.

f Select the Computer account radio button.

7 Import the certificate into the root and personal store certificates.

a Choose All Files in the dialog.

b Select the server.p12 file.

c Click the Exportable check box.

d Leave the password blank.

e Accept the defaults for the subsequent steps.

8 Copy the certificate into the Trusted Root CAs in the same mmc console.

9 Verify that the content of the certificate includes these elements.

- Private key
- CN in the subject attribute that matches the Integration Broker Host Name
- Extended key usage attribute with both client and server authentication enabled

**Synchronizing Workspace Connector with Integration Broker**

When you enable Citrix-based application support, you establish communication and schedule the synchronization frequency between Workspace and the Citrix server farm.

**Prerequisites**

- Configure the network, SSL, and vCenter extension. See “Configure Basic Workspace Settings,” on page 17.
- Review Citrix documentation for Citrix server 5.0, 6.0, and 6.5 at the Citrix Web site.
- Set up dedicated Sync and SSO Integration Brokers to distribute the load in a large-scale enterprise deployment.
Procedure

1. Log in to the Connector Web Interface at https://connectorhost/hc/admin/.
2. Click Published Apps - Citrix in the left navigation pane.
3. Select the Enable Citrix-based Applications check box.
4. Type the Sync Integration Broker host name and port number.
5. Click Use same as Sync Integration Broker button if you do not need to distribute heavy traffic.
6. Select the Use SSL check box.

**Note** Do not select Use SSL for both the Sync Integration Broker and the SSO Integration Broker.

7. (Optional) Set up the SSO Integration Broker.
   a. Type the SSO Integration Broker host name and port number.
   b. Select the Use SSL check box.
   c. Do not select Use SSL for both the Sync Integration Broker and the SSO Integration Broker.
   d. Add a server farm.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>5.0, 6.0, or 6.5</td>
</tr>
<tr>
<td>Server name</td>
<td>Server name assigned in your environment.</td>
</tr>
<tr>
<td>Servers (failover order)</td>
<td>Organize the servers in failover order. Workspace respects this order during SSO and under failover conditions.</td>
</tr>
<tr>
<td>Transport type</td>
<td>HTTP, HTTPS, and SSL RELAY</td>
</tr>
<tr>
<td>Port numbers</td>
<td>HTTP Port, SSL Relay Port</td>
</tr>
<tr>
<td>Choose frequency</td>
<td>Manually, Once per week, Once per day, or Every hour</td>
</tr>
</tbody>
</table>

8. Click Sync now.

At times, when you synchronize Integration Broker with SSL, the synchronization can be slow depending on factors in your environment, such as network speed and traffic.

**Note** The anonymous user group feature in the Citrix product is not supported with Workspace.

The **Sync now** operation forces a synchronization between Workspace and Citrix-based applications.

After the synchronization is complete, Citrix-based applications and corresponding entitlements are synchronized with Workspace. You can enable the Citrix-based application module during the basic configuration or on the Module Configuration page in the Configurator user interface.

**What to do next**

End users can now add Citrix-based applications to the Workspace launcher and launch Citrix-based applications.
Integrating View

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

Prerequisites

- Verify that View is installed. For information about specific View versions that are supported by Workspace, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- Deploy and configure View to use the default port, 443. You can also use custom port numbers.
- Deploy and configure View pools and desktops with entitlements set for Active Directory users and groups.
- Ensure that you create the View pools as a user with administrator permissions on the root folder in View. If you give the user administrator permissions on a folder other than the root folder, Workspace will not recognize the SAML you configure in View or be able to query the View pools and entitlements. You cannot configure the pool in Workspace.
- Deploy and configure Workspace.
- Enable the UPN attribute on Workspace on the User Attributes page.
- Configure SAML authenticator on the View Connection Server. You must always use the Workspace FQDN on the Authenticator configuration page.
- Verify that you have a DNS entry and an IP address that uses reverse lookup for each View Connection Server in your View setup. Workspace requires reverse lookup for View Connection Servers, View Security server, and load balancer. If reverse lookup is not properly configured, the Workspace integration with View fails.
- Sync Active Directory users and groups with View Pool entitlements to Workspace. You can use the Workspace setup wizard to sync users and groups, or go to the Directory tab in the configurator-va virtual machine.

**NOTE** If you are using a third-party IdP and a Smart card or non-Workspace authentication module, you must disable Enable SSO on the View Pools tab to enable authentication.

- **Join an Active Directory Domain** on page 58
  To use View with Workspace, you must join the same Active Directory domain where the View Connection Server is joined.
- **Sync View Pools** on page 59
  Each time you change information in View, such as add an entitlement, add a user, and so on, you must force a sync to propagate the changes to Workspace.
- **Configure SAML Authentication** on page 60
  Ensure that you select the Enable SSO function on Workspace Connector Administrator Web interface.

Join an Active Directory Domain

To use View with Workspace, you must join the same Active Directory domain where the View Connection Server is joined.

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

- Verify that UPN is enabled on the User Attribute Mapping tab.
- Verify that users and groups with View Pool entitlements assigned are synced using Directory sync.

Procedure

1. In the Select Modules pane of the Workspace Setup wizard, click **Enable this Module** for View.

2. Type the domain information for Workspace and click **Join Domain**. Do not use non-ASCII characters when you enter your domain name.

   **Table 3-7. Active Directory Domain Information**
   
<table>
<thead>
<tr>
<th>Join Domain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD FQDN</td>
<td>Type the fully qualified domain name of the Active Directory to join.</td>
</tr>
<tr>
<td></td>
<td><strong>IMPORTANT</strong> The Active Directory FQDN must be in the same domain as the View Connection Server. Otherwise, your deployment will fail.</td>
</tr>
<tr>
<td>AD User</td>
<td>Type the username of the user in Active Directory that has the right to join the computer to the domain.</td>
</tr>
<tr>
<td>AD Password</td>
<td>Type the password associated with the username. This password is not stored by Workspace.</td>
</tr>
<tr>
<td></td>
<td><strong>IMPORTANT</strong> Each time you import the Connector’s configuration you must rejoin the domain.</td>
</tr>
</tbody>
</table>

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

   **Table 3-8. View Information**
   
<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Connection Server</td>
<td>Type the fully qualified domain name of the View Connection Server instance you want to sync with.</td>
</tr>
<tr>
<td>Username</td>
<td>Choose an account that has the Administrators or Administrators (Read only) role in View Administrator.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password associated with the Active Directory username.</td>
</tr>
</tbody>
</table>

Follow these steps to set up View integration in a multidomain environment.

- a Verify that Workspace and the View servers are joined to the same domain.
- b Verify that the Directory Server Host and the View servers are joined to the same domain. The Directory Server Host (defined on the Workspace Directory configuration page) must be an Active Directory host. Do not specify parent or sibling domain controller information.
- c On the Workspace Directory configuration page, you must provide global catalog information to allow users in sub-domains and sibling domains to access Workspace and View desktops.

What to do next

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

**Sync View Pools**

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

After you enable View in the Configurator, you must sync the View pools on the Connector.
Procedure

1. Go to https://ConnectorHostname/he/admin/ to open the Connector.
2. Enter the administrator password.
3. Click View Pools and click Sync Now.
4. Verify that you can synchronize View Pools and their entitlements from View Connection Server to Workspace.
   a. Log in to Workspace Admin Console.
      https://WorkspaceFQDN/SAAS/login
   b. Click the Catalog tab.
   c. Select a View pool and check the Details and Entitlements tabs.

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

What to do next

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

Configure SAML Authentication

Ensure that you select the Enable SSO function on Workspace Connector Administrator Web interface.

- Establish or Update SSL Trust between the Connector and the View Connection Server on page 61
  Initially, you must accept an SSL certificate on the View Connection server to establish trust between the Connector and the View Connection server. If you change an SSL certificate on the View Connection server after the integration, you must return to the Connector and reestablish that trust.

- Enable Multiple View Client URLs Access to Custom Network Ranges on page 61
  If your company uses multiple client access URLs for different network ranges, the administrator must edit the default network range so the end user connects to the correct View Client Access URL and port number. If these settings are not updated, the View client will not launch.

- Launch a View Pool on page 62
  Users can launch a View pool from Workspace.

- Configure View Client to Use a Custom Port Number on page 62
  On the Connector View Pools page, enter the port number of the View Connection server in the text boxes provided for the View Connection server in the broker list.

- Modify the View Integration Configuration on page 62
  You can modify the View integration configuration in the Connector virtual machine.

Procedure

1. Log in to the View Administrator Web interface as a user with the Administrator role assigned.
2. Configure SAML authentication for each replicated server in your View infrastructure.

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

What to do next

You must establish and maintain SSL Trust between the Connector and the View Connection Server.
Establish or Update SSL Trust between the Connector and the View Connection Server

Initially, you must accept an SSL certificate on the View Connection server to establish trust between the Connector and the View Connection server. If you change an SSL certificate on the View Connection server after the integration, you must return to the Connector and reestablish that trust.

Prerequisites

- Verify that View has an SSL certificate installed. By default, View has a self-signed certificate.
- In View, change the certificate of the View Connection Server to a root-signed certificate. See the VMware View documentation for information about configuring a View Connection server instance or Security Server to use a new certificate.
- Configure SAML authentication on the View Connection server. You must always use the Workspace FQDN on the authenticator configuration page.

**NOTE** If you use a third-party identity provider to access View desktops from Workspace, SAML authentication, on the View Connection server, must be set to **allowed**.

Procedure

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

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

Enable Multiple View Client URLs Access to Custom Network Ranges

If your company uses multiple client access URLs for different network ranges, the administrator must edit the default network range so the end user connects to the correct View Client Access URL and port number. If these settings are not updated, the View client will not launch.

Prerequisites

Install Workspace 2.0.

Procedure

1. Log in to the Administrator Web interface.
2. Click the **Settings** tab.
3. Click **Network Ranges** in the left navigation.
4. Click the **Edit** link by each network range.
5. Type in the View Client Access URL using your company’s configuration.
6. Verify that each network range in your environment contains a View Client Access URL.

**IMPORTANT** If you miss a network range, end users who launch through that network range might have problems.
What to do next
If necessary, you can modify the View integration configuration.

Launch a View Pool
Users can launch a View pool from Workspace.
You can switch the display protocol between Open with View Client or Open with Browser by clicking Preferences from the drop-down.

Prerequisites
Install View Client. You must install View Client on the machine that launches Workspace.

NOTE For information about specific View Client versions, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Procedure
1 Log in to your Workspace instance.
2 Click the View Desktops icon.
3 Select your View pool.
4 Right-click the selected View pool and choose a protocol to launch the View desktop.

What to do next
If necessary, you can configure View on a custom port number.

Configure View Client to Use a Custom Port Number
On the Connector View Pools page, enter the port number of the View Connection server in the text boxes provided for the View Connection server in the broker list.

Prerequisites
Install Workspace 2.0.

Procedure
1 Log in to the Workspace Admin Console.
2 Click the View Pools tab
3 Update the port number for each network range in Connection Server.
4 Click Save.

What to do next
If necessary, modify the View integration configuration.

Modify the View Integration Configuration
You can modify the View integration configuration in the Connector virtual machine.
The following View integration configuration settings can be changed on the Connector virtual machine.

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

You use the View Connection Server to entitle Workspace users to View Pools.

**Procedure**

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

**Optional** Set Proxy Server Settings for Manager

Workspace Manager virtual machines access the global 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 Manager (service-va) virtual machine.

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. Log in as the root user to the Manager (service-va) virtual machine. See “Configure Basic Workspace Settings,” on page 17 for more information about the global root password.
2. Run the YaST utility from the service-va virtual machine's command line.
3. Select the **Network Services** tab 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 tcservice on the service-va virtual machine to use the new proxy settings.
   ```
   /etc/init.d/horizon-frontend restart
   ```

**IMPORTANT** Repeat these steps on each service-va virtual machine in your vApp to configure the proxy.

The global catalog and other Web services are now available to Workspace.
Advanced Configuration for VMware Workspace Portal Virtual Machines

After you complete the basic Workspace installation, you might need to complete other configuration tasks in the Configurator, such as configuring View, integrating ThinApp, or cloning virtual machines.

Each component has multiple instances and custom functionality. Additionally, each virtual machine offers different features. The Workspace architecture diagram demonstrates what you can build using the various Workspace components. See Chapter 2, “Installing VMware Workspace Portal,” on page 7 for a typical deployment.

- **Enabling External Access to Workspace** on page 66
  During deployment, the Workspace setup wizard installs the Workspace vApp 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.

- **Configuring Redundancy/Failover for Workspace Virtual Machines** on page 69
  Workspace lets enterprises achieve failover and redundancy by adding multiple virtual machines of the same type in the Workspace vApp. For instance, you can add a second gateway-va virtual machine and enable the load balancer to redirect requests to both gateways. If one of the gateway-va virtual machines shuts down for any reason, Workspace will still be available.

- **Update Workspace Settings with Configurator** on page 76
  After you configure Workspace, you can use the Configurator to update the current configuration and monitor system information for each virtual appliance. For some settings, you must use the Connector to perform specialized Connector configurations.

- **Configuring SecurID for Workspace** on page 78
  When you configure RSA SecurID server, you must prepare the RSA SecurID server for the Workspace and configure SecurID with the Workspace Web interface.

- **Configuring Kerberos for Workspace** on page 80
  When you configure Kerberos for Workspace, you must consider many different components. Configuring Kerberos for the Connector involves installation, and possibly configuration tasks.

- **Using SSL Certificates in Workspace** on page 84
  SSL protects communications to Workspace and within it. During the Workspace Web interface initialization, the Configurator randomly generates a self-signed Workspace root CA certificate.

- **Adjusting Java Heap Size for Improved Performance** on page 85
  The Java heap size settings must be changed manually on the connector-va virtual machine if you add or remove memory. The service-va virtual machine automatically adjusts the settings.
Enabling External Access to Workspace

During deployment, the Workspace setup wizard installs the Workspace vApp 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 gateway-va virtual machines in the future. You might need to add more gateway-va virtual machines to provide redundancy and load balancing. Typically, if you have more than 2,000 users, you may need to add an additional gateway-va virtual machine. Additionally, if your deployment exceeds 2,000 users, you must also deploy the public service hostname and IP address with a load balancer. The following diagram shows the basic deployment architecture you can use to enable external access.

**Figure 4-1. External Gateway Proxy with Virtual Machine**

Specify Workspace FQDN during Deployment

During deployment for the configurator-va 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 gateway-va virtual machine in the Workspace vApp always runs on port 443. You can use a different port number for the load balancer. If you use a different port number, you must specify it during deployment time.
All the virtual machines in the Workspace vApp must be able to ping the Workspace FQDN. If one of the virtual machines cannot ping Workspace FQDN, the deployment process fails. Additionally, if the Workspace FQDN does not resolve to the gateway-va virtual machine, the configuration process in the Web interface fails.

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

- `curl -kv https://WorkspaceFQDN/SAAS`
- `curl -kv https://WorkspaceFQDN/web`

**Using Configurator Web Interface to Complete Deployment**

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

**X-Forwarded-For Headers**

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

**Load Balancer Timeout**

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

**Enabling Sticky Session on the Load Balancer to the Gateway**

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

- **Establish SSL Trust between Workspace vApp and Load Balancer** on page 67
  By default, the Workspace Setup wizard configures the Workspace vApp with a self-signed certificate. The Workspace Setup wizard enables HTTPS communication between the virtual machines and the vApp.

- **Enable AUDIT Events via Proxy Server** on page 68
  Workspace audits various user events, such as login, logout, entitlement, and provisioning. The service-va virtual machine uses a Web application to audit the events. The Web application runs on /AUDIT endpoint. Workspace does not authenticate the /AUDIT endpoint application to maintain performance. For security purposes, the gateway-va virtual machine only permits virtual machines in the Workspace vApp to use the /AUDIT endpoint.

**Establish SSL Trust between Workspace vApp and Load Balancer**

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

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

**Procedure**

2 Paste the root certificate to the correct location on your load balancer.
   See the documentation provided by your load balancer vendor.

3 Run the following commands to check your installation.
   - curl -v https://Workspace FQDN:Workspace port/SAAS
   - curl -v https://Workspace FQDN:Workspace port/web

What to do next
Now, you can proceed to the Configurator to continue configuring your deployment

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

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

Procedure
1 Verify that you can access the /AUDIT endpoint from the service-va virtual machine.
   b Click Reports and click Audit Events.
      If no Audit Events appear in the table or you see an error, Audit Events are not working.
2 Modify the gateway-va virtual machine to update the Real_IP to resolve the issue.
   a Edit /opt/vmware/nginx/conf/nginx.conf.
   b Add the set_real_ip_from IP of Load Balancer; line after the include gen/real_ip.conf; statement.
      The new line is the last in the sample.
      real_ip_header X-Forwarded-For;
      real_ip_recursive off;
      include gen/real_ip.conf;
      set_real_ip_from IP of Load Balancer;
   c Type /etc/rc.d/nginx restart to restart nginx.
3 (Optional) If the audits still do not work, you can turn off the IP-based checks.
   a Edit /opt/vmware/nginx/conf/location-443.conf.
   b Search for /AUDIT.
   c Comment out # allow 127.0.0.1; # include gen/all.allow; and # deny all;
   d Type /etc/rc.d/nginx restart to restart nginx.

With the Audit function configured, you can use the audit information for tracking or troubleshooting.
Configuring Redundancy/Failover for Workspace Virtual Machines

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

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

**IMPORTANT** The `hznAdminTool addvm --type=` command must be executed only after both the command-line and Web interface configuration of Workspace vApp is completed successfully.

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

This command creates the new virtual machine by cloning a base snapshot of the original virtual machine of the same type. The base snapshot is captured for all virtual machines during the initial deployment. The command fails if the base snapshot does not exist.

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

- **Create Multiple gateway-va Virtual Machines** on page 69
  Your enterprise can create multiple gateways of the same type to distribute traffic and eliminate potential downtime.

- **Create Multiple service-va Virtual Machines** on page 70
  Your enterprise can create multiple service-va virtual machines of the same type to distribute traffic and eliminate potential downtime.

- **Create Multiple connector-va Virtual Machines** on page 72
  Your enterprise can create multiple connector-va virtual machines of the same type to reduce traffic and eliminate potential downtime.

Create Multiple gateway-va Virtual Machines

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

Adding multiple gateway virtual machines helps your enterprise:

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

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

**Procedure**

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

2. Go to the configurator-va virtual machine and run the `hznAdminTool addvm --type=GATEWAY --ip=New VM IP address` command.
3 Add the new gateway to your load balancer so the requests are sent to both gateway virtual machines.

**What to do next**

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

### Add or Resize a Disk for Buffering Files

The gateway-va virtual machine buffers client requests. Large files that are waiting to upload are temporarily stored on this disk. Depending on the upload size limit set for your environment, the space on the buffer disk can easily exceed the maximum limit.

During the Workspace 2.0 installation, an additional disk is created and configured for the gateway-va virtual machine to use to buffer files waiting to upload.

The Workspace 2.0 upgrade creates the configuration that points to an additional buffer disk on the gateway-va virtual machine. However, you can create the buffer disk only after the upgrade is complete.

**Procedure**

1. Stop the gateway-va virtual machine.
   
   `/etc/rc.d/nginx stop`

2. (Optional) To increase or decrease the disk size allotted to the buffer, delete the disk.

3. Create a new disk.

4. Remove the existing sub-directories: `proxy_temp` and `client_body_temp`.

5. Mount the disk at `/opt/vmware/nginx/buffer`.

6. Start the gateway-va virtual machine.
   
   `/etc/rc.d/nginx start`

**What to do next**

When the gateway-va virtual machine buffers large files, the end user's performance is not usually affected. If large files do affect performance, increase the disk space allotted to the buffer.

### Create Multiple service-va Virtual Machines

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

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

**Prerequisites**

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

**Procedure**

1. Log in to configurator-va virtual machine as the root user.

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

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

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

5 Go to the configurator-va virtual machine to configure the IP table rules for multiple service-va virtual machines to enable clustered audit event reports.

a Edit the iptables configuration file.

```
vi /usr/local/horizon/conf/iptables.cfg
```

b Change the following configuration parameters.

<table>
<thead>
<tr>
<th>Table 4-1. Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Original Parameter</strong></td>
</tr>
<tr>
<td>APPLICATION_MANAGER_tcp_vapp=&quot;443 8443 5443 9300&quot;</td>
</tr>
<tr>
<td>APPLICATION_MANAGER_udp_vapp=&quot;&quot;</td>
</tr>
</tbody>
</table>

6 Run the following commands on the new service-va virtual machine, as well as, the existing service-va virtual machines to establish communication and record audit events.

<table>
<thead>
<tr>
<th>Table 4-2. Multiple service-va Virtual Machines Communication Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>Run these commands on all existing service-va virtual machines.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Run these commands on newly added service-va virtual machines.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Restart the elastic server on all existing service-va virtual machines.</td>
</tr>
</tbody>
</table>

Verify the status by running the following command on the service-va virtual machine.

```
curl -XGET 'http://localhost:9200/_cluster/health?pretty=true'
```

Find the output.

"number_of_nodes" : 2,

The number of nodes and the number of service-va virtual machines must match. If the number of nodes equals 1, verify that the parameter value in the /etc/sysconfig/elasticsearch configuration file equals true.
Go to the Configurator Web interface at http://ConfiguratorHostname/cfg and click Exit Maintenance Mode.

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

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

What to do next

You can add additional Connector virtual machines.

Create Multiple connector-va Virtual Machines

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

Using multiple connector-va virtual machines helps your enterprise:

- Improve load balancing, failover, and availability to the Workspace authentication functionality.
- You can authenticate end users to Workspace using multiple methods of authentication, such as Active Directory username and password, username and RSA SecurID passcode, or Kerberos-based Windows authentication. To enable multiple forms of authentication, you must set up multiple connector-va virtual machines.

During the initial set up of Workspace 2.0, you establish a connection between Workspace and an Active Directory instance that is a single or multiple domain environment in a single forest. If your environment uses multiple forests and you plan to connect to Active Directory in a multi-forest environment, you must create a new connector-va virtual machine to connect with each forest. You configure your multi-forest environment after the initial set up, or later, after testing is complete. See the list below for more information:

- To establish a connection between a multi-forest Active Directory and Workspace, see “Configuring Workspace in a Multi-forest Active Directory Environment,” on page 32.
- For information about the global catalog and multiple domains in a single Active Directory forest, see “Configuring a Multidomain Active Directory Single Forest,” on page 34.
Figure 4-2. Multiple Connector Deployment with Various Authentication Types

External proxy server load balances the gateway servers
Hostname: workspace.company.com

DMZ Firewall

Gateway servers:
- gateway-va
- gateway-va-2
- gateway-va-3

Connector servers:
- connector-va
- connector-va-2
- connector-va-3
- connector-va-4
- connector-va-5

Internal proxy server load balances connector-va-3
Hostname: workspace-conn-vip.company.com

Virtual Appliance

Workspace Authentication

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

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

- Connector hostname

- Load balancer server that load balances the requests among multiple connectors. When you use a load balancer server this way, the connectors it load balances must use the same type of authentication.

- Load balancing with Kerberos requires special URL rewriting configuration at the load balancer.

- Workspace FQDN redirects to the gateway and can also load balance the requests among multiple Connectors. The Connectors that are load balanced using this option must use the same type of authentication.
Enable SecurID Authentication

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

You can enable RSA SecurID authentication with Workspace.

**NOTE** If you use the Workspace FQDN as the IDP URL, you must set the `useGatewayAsIDP` flag to `y`. As a result, maintenance mode is turned on for the new connector-va virtual machine. When a virtual machine is in maintenance mode, the gateway-va virtual machine will not be aware of the virtual machine or route requests to it.

**Procedure**

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

2. Go to the configurator-va virtual machine and run the `hnzAdminTool addvm` command.
   ```bash
   hnzAdminTool addvm --type=CONNECTOR --ip=New VM IP address --useGatewayAsIDP=y --directoryPassword='AD BindDN password'
   ```
   The new connector-va virtual machine is automatically activated and connected to Active Directory.
   Provide the password for the BindDN user that you used during initial configuration.

   a. Click **System Information**.
   b. Find the new virtual machine you added.
   c. Click **Exit Maintenance Mode**.

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

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

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

What to do next
To configure SecurID for end users who connect to the network from external networks, see “Configuring SecurID for Workspace,” on page 78.

Enable a New Username and Password
Enterprises can enable new usernames and passwords for their end users who connect from internal Windows machines.

Procedure
2. Run the hznAdminTool addvm --type=CONNECTOR --ip=New VM ip address --useGatewayAsIDP=y or n --directoryPassword='AD BindDN password' command.
   - You must set the useGatewayAsIDP flag to y or n.
   - If you use the Workspace FQDN as the IDP URL, set the useGatewayAsIDP flag to y. This flag turns on maintenance mode for the new connector-va virtual machine. When a virtual machine is in maintenance mode, the gateway-va virtual machine will not be aware of the virtual machine or route requests to it.
   - If you set the useGatewayAsIDP flag to no, the new connector-va virtual machine starts in normal mode.

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

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.

You can enable Kerberos authentication with Workspace.

Procedure
1. Obtain an IP address that is resolvable using reverse DNS and select the IDP URL. This IP must be set up using the same netmask, network gateway, and DNS server name used in the original IP pool to deploy the vApp.
Go to the configurator-va virtual machine at https://configurator-va hostname.

a. Run the `hznAdminTool addvm` command.

```
hznAdminTool addvm --type=CONNECTOR --ip=New VM ip address --useGatewayAsIDP=n --
directoryPassword='AD BindDN password'
```

b. Set the flag `useGatewayAsIDP` to `n`.

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

Go to Connector Web interface at https://new connector-va hostname/hc/admin and log in with the administrator password.

a. Join the new connector-va virtual machine to the domain.

b. Click **Windows Auth**.

c. Enable Windows Authentication.

Go to Service Web interface at https://Workspace FQDN/admin.

a. Click **Settings** tab.

b. Click **Identity Providers**.

c. Edit the new Identity Provider.

d. Edit the IP address list.

If you have View integrated with a multi-connector Workspace deployment, ensure that you enable and configure View Pools on every connector that supports View desktops. You cannot connect to your desktop from a connector without View Pools enabled. When you schedule a **View Pool Sync** operation from one of the connectors, this operation syncs the connectors with the View configuration.

**What to do next**

To enable Kerberos authentication for end users who connect to the network using internal Windows machines, see “Configuring Kerberos for Workspace,” on page 80.

**Update Workspace Settings with Configurator**

After you configure Workspace, you can use the Configurator to update the current configuration and monitor system information for each virtual appliance. For some settings, you must use the Connector to perform specialized Connector configurations.

You can switch the service-va and connector-va virtual machines to maintenance mode to monitor information about each virtual machine, and view the IP address, status, or relative drift of a virtual appliance. You can also update or change settings for your database, modules, FQDN and SSL certificates, and more on the following pages.

- System Information
- System Diagnostics
- Database Connection Setup
- Module Configuration
- Workspace FQDN and SSL Certificates
- X-Forwarded-For Header
- License Key
- Password
Log File Locations

Additional information is available about connecting to Active Directory, filtering users, and Workspace modules.

Procedure
2. Log in to the Configurator with the administrator password.
3. Use the left navigation pane to select the page to view.

What to do next
Verify that the settings or updates you made are in effect.

Change vCenter Administrator Password

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

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

Procedure
1. Log in to the configurator-va virtual machine.
2. Run the hznAdminTool command.
   
   hznAdminTool editproperty --set=vim_password:yournewpassword

3. Run the configurator-tc restart command to restart the configurator-va virtual machine.

What to do next
Log in to the Workspace Configurator Web interface and verify that you can access all the pages.

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 Configurator Web interface.

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. Log in to the configurator-va virtual machine.
2. Click Syslog in the left navigation.
   
   This opens the Syslog Configuration page.

3. Click the Enable radio button.
4 Type in the IP or the FQDN of the server where you want to store the logs.
5 Click Save.

Workspace sends a copy of your logs to the syslog server.

Use System Diagnostics Tool

You can use the System Diagnostics tool to identify application-specific issues and connectivity with integrated components. The information the tool provides includes the results of different diagnoses performed on each virtual machine in your deployment, as well as basic data points that enable you to troubleshoot your Workspace environment.

This tool can be used during initial Workspace configuration. When you run the wizard, if you see an error, you can navigate to the diagnostic page, identify and fix problematic issues, and return to the wizard. The tool is also useful after initial configuration and during regular use of Workspace.

The System Diagnostics page is on-demand. The information it displays represents the status at the time when the page was loaded. The page should be refreshed to view more recent information. Error notifications are not provided.

The diagnostic page provides a drill down approach. The top element shows the overall health of the system. You can drill down further to review specific information about a problematic component.

Review the status information for each virtual machine in the vApp and troubleshoot problems by locating the appliance where the error occurred. The System Diagnostics page displays status icons for critical, informational, and cautionary states for each virtual appliance. You can drill down and read a detailed description of a message by clicking the link of the appliance with a status icon.

You can identify problems in your environment. For example, when a user cannot log in to Workspace, you can drill down to see that the connector-va virtual machine is not connected to the Active Directory server. Or you can review the information and find out why your service-va virtual machine cannot connect to the database.

If you need to forward this report, you can use the Printer Friendly View link to print or save the report to a PDF file.

Procedure

1 Log in to the configurator-va virtual machine.
2 Open the System Diagnostics page.
   - From the Workspace setup wizard, click Workspace.
   - From the Configurator, click Workspace in the left navigation.
3 Use the links to view the status information, message details, or raw output.

What to do next

You can use the System Diagnostics page during the Workspace installation, and afterward, to view status information.

Configuring SecurID for Workspace

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

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, you use the Workspace Web interface to configure the SecurID page.

- **Prepare the RSA SecurID Server for the Connector** on page 79
  If you want to provide RSA SecurID security, prepare the RSA SecurID server for the Connector.

- **Configure SecurID with the Connector Web Interface** on page 80
  After you run the Workspace setup wizard, you can configure the SecurID page.

## Prepare the RSA SecurID Server for the Connector

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

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

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

### Prerequisites

- Verify that one of the following RSA Authentication Manager versions is installed and functioning on the enterprise network to allow communication with the Connector: 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.

- Install and configure the Connector. After you install the Connector and use the Configurator Web interface to run the setup wizard, you have the information necessary to prepare the RSA SecurID server.

### Procedure

1. On a supported version of the RSA SecurID server, add the Connector as an authentication agent.

2. Type in the following Connector-related information when you add the Connector as an agent.

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

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

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

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

### What to do next

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

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

Prerequisites

- Verify that RSA Authentication Manager (the RSA SecurID server) is installed and properly configured.
- Download the compressed file from the RSA SecurID server and extract the server configuration file.

Procedure

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

Information used and files generated on the RSA SecurID server are required when you configure the SecurID page. See “Prepare the RSA SecurID Server for the Connector,” on page 79.

Table 4-3. SecurID Configuration Settings

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

4. Save your SecurID settings.

The connector-va virtual machine is configured to use RSA SecurID to authenticate users with Workspace.

Configuring Kerberos for Workspace

When you configure Kerberos for Workspace, you must consider many different components. Configuring Kerberos for the Connector involves installation, and possibly configuration tasks.

Kerberos authentication provides another layer of security for your Workspace deployment.

Active Directory Configuration

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

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

Configuring Join Domain

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

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

Table 4-4. Active Directory Information

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

Enabling Windows Authentication

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

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

Table 4-5. Windows Authentication Information

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

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 browsers can support Workspace, on Windows only, during Kerberos authentication: Firefox, Internet Explorer, and Chrome. All the browsers require additional configuration.
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 Connector is part of the local intranet zone.
   a. Use Internet Explorer to access the Connector login URL at
      https://ConnectorHostname.DomainName/authenticate/.
   b. Locate the zone in the bottom right corner on the status bar of the browser window.
      If the zone is Local intranet, Internet Explorer configuration is complete.
4. If the zone is not Local intranet, add the Connector to the intranet zone.
   a. Select Tools > Internet Options > Security > Local intranet > Sites.
   b. Select Automatically detect intranet network.
      If this option was not selected, selecting it might be sufficient for adding the Connector to the intranet zone.
   c. (Optional) If you selected Automatically detect intranet network, click OK until all dialog boxes are closed.
   d. In the Local Intranet dialog box, click Advanced.
      A second dialog box named Local intranet appears.
e Type the Connector URL in the Add this Web site to the zone text box.

https://ConnectorHostname.DomainName/authenticate/

f Click Add > Close > OK.

5 Verify that Internet Explorer is allowed to pass the Windows authentication to the trusted site.

a In the Internet Options dialog box, click the Advanced tab.

b Select Enable Integrated Windows Authentication.

   This option takes effect only after you restart Internet Explorer.

c Click OK.

6 Log in to the Connector Web interface at https://ConnectorHostname.DomainName/authenticate/ to check access.

   If Kerberos authentication is successful, the test URL goes to the Web interface.

The Kerberos protocol secures all interactions between this Internet Explorer browser instance and 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!.

3 Double-click network.negotiate-auth.trusted-uris in the Preference Name column.

4 Type your Connector URL in the text box.

   https://ConnectorHostname

5 Click OK.

6 Double-click network.negotiate-auth.delegation-uris in the Preference Name column.

7 Type your Connector URL in the text box.

   https://ConnectorHostname

8 Click OK.

9 Test Kerberos functionality by using the Firefox browser to log in to the Connector at https://ConnectorHostname.

   If the Kerberos authentication is successful, the test URL goes to the Web interface.

   The Kerberos protocol secures all interactions between this Firefox browser instance and 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 Connector at `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.

Using SSL Certificates in Workspace

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

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

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

If you deploy Workspace with our generated SSL certificates, 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 `http://gateway hostname workspace_rootca.pem`.

You can use your own certificates with Workspace, even if you use CAs that were not included initially.

Apply an SSL Certificate from a Major or Private Certificate Authority

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

All communication in the vApp is processed by the Workspace FQDN server. Workspace pre-loads the machines in the vApp to trust the major certificate vendors. As a result, if custom SSL certificates chain to one of the major certificate vendors or if you want to use a new private certificate, you can apply the new certificate by copying it to the load balancers, Gateway, or Connector.
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 gateway-va virtual machine, you must copy the Workspace root CA certificate to the load balancer as a trusted root certificate. When you update your certificate, if you are using View integration, you must follow the steps in “Establish or Update SSL Trust between the Connector and the View Connection Server,” on page 61.

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

Procedure

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

2. Apply the certificate to the gateway-va virtual machine.
   b. Log in and click SSL Certificate.
   c. Copy the complete certificate chain and private key. Ensure that the certificate includes the Workspace FQDN hostname in the CN.
   d. Save the SSL certificate.
      The Configurator copies the certificate to the gateway-va virtual machine.

3. If your deployment uses external Connectors that grant users access to the Connector as an IDP URL either directly or through a load balancer, apply the certificate to the connector-va virtual machine.
   b. Log in and click SSL Certificate.
   c. Copy the complete certificate chain and private key. Ensure that the certificate includes the FQDN hostname for the connector-va virtual machine in the CN.
   d. Save the SSL certificate.
      The Configurator copies the certificate to the connector-va virtual machine.

4. Verify that users can log in successfully.

Workspace will use the newly applied certificate.

(Optional) Adjusting Java Heap Size for Improved Performance

The Java heap size settings must be changed manually on the connector-va virtual machine if you add or remove memory. The service-va virtual machine automatically adjusts the settings.

Update Java Heap Size on the connector-va Virtual Machine

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

Procedure

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

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

You can use these procedures to diagnose and fix problems with Workspace.

This chapter includes the following topics:

- “Setting for vCenter Server Quiesce Timeout Is Too Low,” on page 87
- “Delete Unused Extensions from vCenter,” on page 87

Setting for vCenter Server Quiesce Timeout Is Too Low

In an environment with heavy traffic, a vCenter Server quiesce timeout problem can occur that might cause your deployment to fail.

Problem

When an error message appears, vCenter Server records the error message, *Failed to quiesce the virtual machine*, to the vCenter Server log.

Cause

This problem occurs when the virtual machines stop responding during heavy traffic.

Solution

1. Search for an entry of the following error message in the vCenter Server log to verify the cause of the problem.

   Failed to quiesce virtual machine

2. Increase the timeout values.

   The default values range from 30 to 120 seconds. See the article on increasing vCenter server timeout settings at http://kb.vmware.com.

3. Redeploy Workspace.

Delete Unused Extensions from vCenter

If you deploy Workspace multiple times after failures or upgrades, Workspace creates multiple extensions in vCenter. If you do not remove the unused extensions, errors can occur.

Procedure

1. Log in as a vCenter administrator at https://vcenterFQDN/mob/?moid=ExtensionManager.

2. Use the `UnregisterExtension` command to remove the unused extension.

3. Look at the most recent heartbeat to determine the extension in use.
What to do next

Remove unused extensions to minimize potential errors and improve performance.
Index

A
Active Directory
domain service forest 34
global catalog 34
groups 18, 29
join 58
multi-forest 32
users 18, 24, 29
add desktop client applications to virtual
machines 30
add user, Demo User Store 36
AUDIT events 68
authentication 74, 75
automatic client application update directory 30

C
checklist
Active Directory Domain Controller 14
network information
Configurator 14
Connector 14
Gateway 14
IP Pools 14
Manager 14
Chrome 84
Citrix server 50
Citrix PowerShell Remoting 50, 51
Citrix server farm 51
Citrix-based, applications 47
Citrix-based application support 56
client downloads directory 30
Configurator, settings 76
configurator-va 17
configure
logging 27
SAML authentication 60
View 62
virtual machines 65
Connector 8
connector password 75
connector username 75
connector-va 69, 72

d data, transfer 22
delete extensions 87
demo user store 35
deployment
checklists 14
preparation 12
disk buffer 70
DNS 13
download OVA file 13

E
enable 61
example 55
external database, Configurator 23
external access 66

F
failover 69, 70, 72
filter 25
Firefox 83
forward DNS 13
FQDN 26

G
gateway-va 69
groups
assign groups 38
assign users 38

H
hardware
ESX 8
requirements 8
HTTPS on IIS 54

I
identity provider
Connector 8
third-party 8
IdP URL 73
install 16, 53, 54
Integration Broker 52, 54, 56
Integration Broker Server 53
Internet Explorer 82
J
Java Heap Size, connector-va 85
join, Active Directory Domain 58

K
Kerberos 75, 80, 82–84

L
Linux
  SUSE 5
  system administrator 5
load balancer 67
logging 27

M
Microsoft Windows Preview 14
module 26
multi-forest 33
multiple virtual machines 69, 70, 72

N
network configuration, requirements 8
network share, ThinApp packages 43

O
oracle database 20
OVA file
  deploy 16
  install 16, 53, 54
overview, install 7

P
port, 3268, 3269 34
PostgreSQL database 21
PowerShell Remoting 50
proxy server 68
proxy server settings 63

Q
query 25
quiesce timeout 87

R
redundancy 69, 70, 72
reverse lookup 13
reverse DNS 13
RSA SecurID server 79
run, Configurator Virtual Appliance 17

S
SAML authentication 60, 73
SecurID, configure 80
self-signed certificate 55
server components 5

service-va 69, 70
setup wizard, setup wizard 18, 29
SMTP Server 14
SSHA encrypted password 37
SSL certificate, major certificate authority 84
SSL trust, update on View Connection Server 61
SUSE Linux 5
sync
  View pools 59
  View Connection Server 58
syslog server 77
System Diagnostics 78
system and functional administrator
  Linux 5
  Windows 5

T
ThinApp, packages 39
ThinApp applications 39
ThinApp packages
  change share folder 47
  configuring access to 44
  network share repository 43

U
URLs 27
user authentication 5

V
vApp 67
vCenter
  credentials 14
  extensions 87
  password 77
vCenter Server, timeout 87
View 58
View pools
  configuration 62
  sync 59
View desktop, start 62
virtual appliance, requirements 8

W
Windows, system administrator 5
Workspace
  deploy 16
  install 16
  license key 14
Workspace setup wizard 18, 29