Lab Manager User's Guide

vCenter Lab Manager 4.0

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-000173-01

vmware®

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

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book

The *Lab Manager User's Guide* provides information about configuring and working with VMware® vCenter Lab Manager. It also describes how to set up resources such as datastores and networks, configure users and groups, and work with workspaces, configurations, virtual machine and network templates.

Intended Audience

This book is intended for VMware vSphere administrators and current Lab Manager and Stage Manager administrators.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

Getting Started with Lab Manager 1

VMware vCenter Lab Manager is an application that provides a rapid provisioning portal and image library management system to automate the setup and teardown of multimachine software configurations and manage service transition activities. Lab Manager leverages VMware vSphere and VMware vCenter to provide virtual infrastructure resources to multiple teams, projects, and geographies from a central location.

Using Lab Manager, you can create a shared virtual machine library that stores commonly used configurations and provide users with self-service access to these configurations for application development, testing, support, training, software demonstrations, and more. Lab Manager administrators control access rights, storage quotas, and deployment policies.

This chapter includes these topics:

Lab Manager Components

Lab Manager requires VMware vSphere. VMware ESX/ESXi™ hosts provide the memory and CPU resources to run Lab Manager virtual machines. Lab Manager manages the ESX/ESXi hosts through a vCenter Server and the Lab Manager agent installed on the hosts. ESX/ESXi hosts continue to function even if the vCenter Server system becomes unreachable (for example, the network connection is severed).

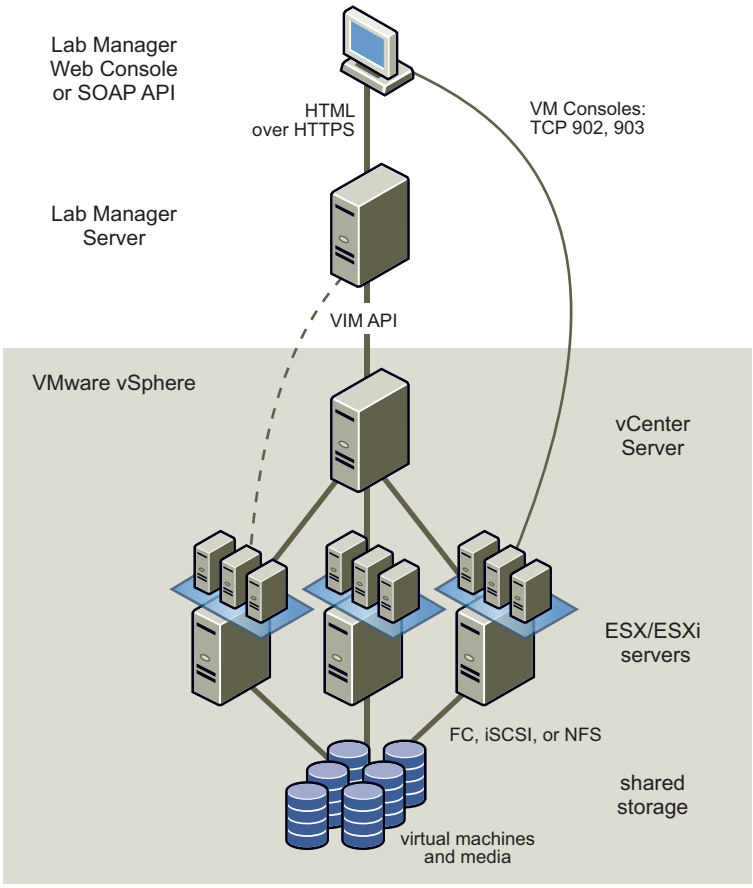
vSphere datastores provide shared storage for Lab Manager virtual machines and media files to install guest operating systems and applications.

Users can access the Lab Manager server through Web and SOAP interfaces:

- Use Microsoft Internet Explorer or Mozilla Firefox to access the Lab Manager Web console to interact with the Lab Manager server.
- Use the Lab Manager SOAP API to access the Lab Manager server programmatically. The SOAP API allows easy integration with build management systems and with automated testing tools. See the *Lab Manager SOAP API Guide* for more information.

Figure 1-1 illustrates the components of Lab Manager and how it works with VMware vSphere.

Figure 1-1. Lab Manager Components



Lab Manager supports VMware vSphere capabilities such as VMware VMotion™, VMware Distributed Resource Scheduler (DRS), and VMware High Availability (HA). These distributed services enable efficient and automated resource management and high virtual machine availability. Lab Manager does not support VMware Fault Tolerance (FT) or vSphere linked clones. FT is disabled for all virtual machines managed by Lab Manager.

Accessing the Lab Manager Web Console

You connect to the Lab Manager Web console using a browser. To access the Lab Manager Web console, a computer must satisfy these requirements:

- Microsoft Internet Explorer or Mozilla Firefox

  For information about which Web browsers are supported on which client operating systems, see Appendix B, "Client and Browser Support," on page 159. If you are using Internet Explorer, see "Set Microsoft Internet Explorer Options" on page 15.

- Routable access to the Lab Manager server and ESX/ESXi hosts
- 1024 x 768 or higher resolution monitor

Set Microsoft Internet Explorer Options

Before you can access the Lab Manager Web console using Microsoft Internet Explorer, you must enable some security and advanced options.

To set Internet Explorer options

1 In Internet Explorer, select **Tools** > **Internet Options**.

2 Click the **Security** tab, select the Web content zone for the Lab Manager server, and click **Custom Level**.

3 Enable the following options and click **OK**.

- **Download signed ActiveX controls**
- **Run ActiveX controls and plug-ins**
- **Allow META REFRESH**
- **Active scripting**
- **Allow paste operations via script**

4 Click **OK** and click the **Advanced** tab.

5 Enable the **Play animations in web pages** option and click **OK**.

6 If you are using Internet Explorer on Windows 2003, open the Control Panel and click **Add or Remove Programs**.

7 Click **Add/Remove Windows Components**.

8 Disable **Internet Explorer Enhanced Security Configuration**.

Log In to the Web Console

Before you can log in to the Web console, you need a user name and password, and you must be a member of at least one organization in Lab Manager.

To log in to the Lab Manager Web console

1 Open a browser and navigate to `https://<Lab_Manager_Server_domain_name_or_IP_address>`.

2 Type your user name and password and click **Login**.

Lab Manager displays the Web console. If Lab Manager displays an error, check with a Lab Manager administrator to make sure you are using the correct user name and password and that you are a member of a Lab Manager organization.

View Performance, Usage, and Support Information

The Overview page is the default landing page in the Web console. It includes performance summary data, information about your quotas, usages, and leases, and links to additional resources to help you learn about Lab Manager.

NOTE A Lab Manager system administrator must enable SupportLink if you want to view all statistics. See "Configuring SupportLink Settings" on page 142.

To view performance, usage, and support information

In the left pane, click **Overview**.

The Performance Summary column includes information about CPU and memory consumption, the number of configurations and virtual machine templates, and storage.

The information in the column is specific to the organization selected in the **Organization** drop-down menu. Select **Global** to view information for the entire Lab Manager installation.

The My vCenter Lab Manager column includes information about the number of virtual machines that you are allowed to deploy and store and the number of deployed and stored virtual machines that you have.

The column also includes information about your storage and deployment leases that will be expiring in the next week.

The Documentation & Support column provides access to documentation, video tutorials to become familiar with the product, and customer support.

Setting User Preferences

Each user can specify how information displays in the Lab Manager Web console and when to be notified about deployment and storage leases that are about to expire. These preferences are used in all the user's organizations. Users who log in with an account created in Lab Manager can change their password.

Set Display and Lease Alert Preferences

You can set default display and lease alert preferences.

To set display and lease alert preferences

1 Click the **Preferences** link.

2 Click the **Defaults** tab.

3 Select the page to display when you log in to the Web console.

The Overview page is the default setting.

4 Deselect the **Show Page Header** check box to not display IP addresses, virtual machine descriptions, and snapshot thumbnails at the top of the each page.

Removing the header gives you more room to view the console.

5 Type the number of rows to display on pages with data in a table.

The maximum number is 500. The default is 20.

6 Select the number of days or hours before a deployment lease expiration that you want Lab Manager to send an email notification.

When a deployment lease expires, Lab Manager undeploys the virtual machine template or configuration.

7 Select the number of days or hours before a storage lease expiration that you want Lab Manager to send an email notification.

When a storage lease expires, Lab Manager deletes the virtual machine template or configuration, or marks it for deletion (depending on how the system administrator has configured Lab Manager).

8 Click **OK**.

Change Your User Password

You can change the password only for a user account created in Lab Manager. You cannot use Lab Manager to change an LDAP account password.

To change your user password

1 Click the **Preferences** link.

2 Click the **Change Password** tab.

3 Type and confirm a new password and click **Change Password.**

The next time you log in to the Web console, use your new password.

Lab Manager Workflow

When you install or upgrade Lab Manager, you connect Lab Manager to a vCenter Server and add resource pools, ESX/ESXi hosts, and a physical network to use with Lab Manager virtual machines.

Your next steps might involve adding more resources to the system, setting up organizations and workspaces, and adding users and groups to those organizations and workspaces.

When Lab Manager has resources and users, you can create or import virtual machine templates to serve as the basis for virtual machines. Use these virtual machine templates to create configurations composed of one or more virtual machines.

You can work with a configuration and its virtual machines in a workspace and save a configuration to the Library to share it with other users.

Adding Resources 2

Lab Manager gets its resources from the vCenter Server system to which it connects. The system administrator assigns some of these resources to Lab Manager during setup, but you can add resources as needed. Only system administrators can add resources to Lab Manager.

NOTE There is a limit of eight managed servers (hosts) per LUN. If you exceed this limit, an error message appears. See http://kb.vmware.com/kb/1003319 for more information.

In Lab Manager, resources can be dedicated to an organization or shared between organizations. Resource pools and hosts provide computing and memory resources for virtual machines. Datastores provide storage for virtual machines. Media stores provide storage for CD/DVD and floppy image files for use with virtual machines. Physical networks provide virtual machines with access to physical networks. Host spanning transport networks enable Host Spanning for configurations that use fenced or virtual networks.

This chapter includes the following topics:

Attach a Resource Pool

If you need additional CPU and memory resources for virtual machines, you can attach a resource pool. By default, only system administrators can attach resource pools.

To attach a resource pool

1 In the left pane, click **Resources**.

2 Click the **Resource Pools** tab.

3 In the **Organization** drop-down menu, select the organization to which you want to add the resource pool.

If you select **Global,** the added resource pool is available to all organizations but assigned to none. You can assign it to an organization later.

4 Click **Attach Resource Pool**.

5 Select the resource pool, cluster, or host from the vCenter inventory.

6 (Optional) Type a name for the resource pool to display in Lab Manager.

7 Click **OK**.

If Lab Manager detects that a host is not prepared (for example, the host does not have an agent that Lab Manager installed on the host), a message appears. See "Prepare a Host" on page 91.

If you added the resource pool to the **Global** organization, you can now assign it to an organization, so the virtual machines in this organization can use its resources. See "Add or Remove the Resource Pools in an Organization" on page 117 for more information.

Add a Media Store

By default, only system administrators can add media stores. A media store is an NFS or VMFS datastore that is enabled for media. You can use different directories on the same datastore for media and virtual machines.

To add a media store

1 In the left pane, click **Resources**.

2 In the **Organization** drop-down menu, select the organization to which you want to add the media store.

If you select **Global**, the added media store is available to all organizations but assigned to none. You can assign it to organizations later.

3 On the **Datastores** tab, move the pointer over the datastore that you want to use as a media store and select **Enable Media**.

4 On the **Media Stores** tab, click **Add Media Store**.

5 Type a name.

6 Select the datastore.

7 Type the directory path to the media.

For NFS datastores, type the path relative to the mount point. For VMFS datastores, type the path relative to the root. A media store and its NFS datastore cannot have the same NFS path root.

8 Click **OK**.

9 On the **Media Stores** tab, move the pointer on the media store name and select **Synchronize**.

NOTE VMware supports one directory without subdirectories.

Add a Physical Network

By default, only system administrators can add a physical network.

To add a physical network

1 In the left pane, click **Resources**.

2 In the **Organization** drop-down menu, select the organization to which you want to add the physical network.

If you select **Global**, the added physical network is available to all organizations but assigned to none. You can assign it to an organization later.

3 On the **Physical Networks** tab, click **New Physical Network**.

4 Type a name.

5 (Optional) Type a description and a VLAN Identifier.

6 Select the IP addressing modes for the network.

If you selected **Static - IP Pool** or **Static - Manual**, type the static mode settings and add an IP pool.

7 Select the fencing policy.

If you selected **Fenced Only**, select a **Connectivity** option:

- **Allow In and Out** – Virtual machines can communicate with machines outside the fence and machines outside the fence can communicate with virtual machines inside the fenced configuration.
- **Allow Out** – Virtual machines in a fenced configuration can initiate communication to machines outside the fence, and can receive messages back on the same connection. Machines outside the fence cannot initiate communication to virtual machines inside the fenced configuration.
- **Block In and Out** – Network traffic does not travel across the fence. Virtual machines in a fenced configuration cannot communicate with machines outside of the fence, and machines outside the fence cannot communicate with virtual machines in the fenced configuration.

8 Select the physical network bindings.

- **Bind to a Virtual Switch (per host)**

  If you select this option, you must select a virtual switch from the drop-down menu for each host.

- **Bind to a vNetwork Distributed Switch**

  If you select this option, you must select the switch that spans multiple hosts from the drop-down menu.

9 Click **OK**.

Add a Host Spanning Transport Network

Before you can add a host spanning transport network, you must create a vNetwork Distributed Switch in vSphere. See the vSphere documentation for more information on creating a vNetwork Distributed Switch.

By default, only system administrators can add host spanning transport networks.

To add a host spanning transport network

1 In the left pane, click **Resources**.

2 In the **Organization** drop-down menu, select the organization to which you want to add the host spanning transport network.

If you select **Global**, the added host spanning transport network is available to all organizations but assigned to none. You can assign it to an organization later.

3 On the **Host Spanning Transport Networks** tab, click **Add Transport Network**.

4 Select a vNetwork Distributed Switch.

5 Type a VLAN Identifier.

6 Select **Enabled** if you want to enable the network for use in virtual/fence network Host Spanning.

7 Select the **Customize Name** check box to modify the display name.

8 Click **OK**.

Adding Users and Groups 3

VMware recommends that you connect Lab Manager to an LDAP server to add and authenticate users. This method allows you to use the LDAP server's existing user and group information, without recreating this information in Lab Manager. You can also create local users from the Web console.

A system administrator or an administrator with rights at the organization level can add users or groups to an organization and assign each user or group a role in the organization. The organization determines which resources a user has access to, and the role determines how a user can interact with these resources. Users cannot log in to Lab Manager or access any resources until they are added to an organization.

This chapter includes the following topics:

Import a User

By default, only system administrators and administrators with rights at the organization level can import users. You can import users that exist on an LDAP server or users that you created from the Web console. See "Configuring LDAP Settings" on page 138 and "Create a User" on page 24 for more information.

To import a user

1 In the left pane, click **Users and Groups**.

2 In the **Organization** drop-down menu, select the organization to which you want to add the user.

If you select **Global**, this user is available to all organizations.

3 On the **Users** tab, click **Import Users**.

4 Deselect the **Show Existing Users/Groups** check box.

Deselecting this option allows you to search for users who are not members of the selected organization.

5 Type the name (complete or partial) of the user that you want to add and click **Search**.

Lab Manager searches for LDAP and non-LDAP users and displays the first 200 results that match the search terms.

6 Select the check box for each user that you want to import.

7 Click **Add**.

8 Assign a role to the added users.

If you are importing users to the **Global** organization, you can only select **No Role** or **Administrator**. If you add a user who is a system administrator in **Global**, Lab Manager assigns that user the same role in all other organizations.

9 Click **OK**.

Repeat these steps to add more users with different roles.

Create a User

To provide Lab Manager access to a user who does not exist on your LDAP server, or if you do not plan to use an LDAP server, you can create users in Lab Manager.

To create a user

1 In the left pane, click **Users and Groups**.

2 In the **Organization** drop-down menu, select the organization to which you want to add the user.

If you select **Global**, this user is available to all organizations but assigned to none. You can assign the user to an organization later.

3 On the **Users** tab, click **New User**.

4 Type a user name.

5 Type and confirm a password.

6 Type a full name.

This name is displayed for all objects owned by this user.

7 Type an email address.

8 (Optional) Type IM and phone information.

9 Select a role for the user in the selected organization.

If you are adding a user to the **Global** organization, you can only select **No Role** or **System Administrator**. If you select **No Role**, this user cannot log in to Lab Manager or access resources until the user is added to another organization.

10 Deselect the **Is Enabled** check box to prevent the user from accessing the Web console.

11 Type a stored virtual machine template and library configuration quota.

12 Type a deployed virtual machine template quota.

If you are in the **Global** organization, the quota text boxes do not appear.

13 Click **OK**.

Import an LDAP Group

By default, only system administrators and administrators with rights at the organization level can import LDAP groups. Lab Manager does not support non-LDAP groups.

To add an LDAP group

1 In the left pane, click **Users and Groups**.

2 In the **Organization** drop-down menu, select the organization to which you want to add the group.

If you select **Global,** the added group is available to all organizations.

3 On the **Groups** tab, click **Import Groups**.

4 Deselect the **Show Existing Users/Groups** check box.

Deselecting this option allows you to search for users and groups that are not in the selected organization.

5 Type the name (complete or partial) of the group that you want to import and click **Search**.

Lab Manager displays the first 200 results that match the search terms.

6 Select the check box for each group that you want to add.

7 Click **Add**.

8 Assign a role to the added groups.

All members of the group are assigned the selected role. If you are adding groups to the **Global** organization, you can only select **No Role** or **System Administrator**. You can change the roles of individual group members later. See "Modify User Properties" on page 110 for more information.

9 Click **OK**.

Repeat these steps to import groups with different roles.

Setting Up Organizations and Workspaces

4

Lab Manager organizations and workspaces include resources and users. You can use these organizations and workspaces to control which users have access to which resources. Lab Manager has access to the resources of the vCenter Server system to which it is connected.

A system administrator can assign some or all of these resources to an organization. Users in that organization only have access to their assigned resources. An organization can have dedicated resources or share resources with other organizations. In an organization, an administrator can create workspaces and assign some or all of the organization resources to each workspace. A workspace can have dedicated resources or share resources with other workspaces. These levels of granularity provide the system administrator with control over system resources.

This chapter includes the following topics:

Create an Organization

Lab Manager includes an organization named **Default**. A system administrator can create additional organizations. For example, you can create an organization for IT, one for human resources, one for engineering, and so on.

When you add a resource pool to a new organization, Lab Manager also adds all its hosts, datastores, and media stores to the organization.

To add an organization

1 In the left pane, click **Organizations**.

2 Select **Global** from the **Organization** drop-down menu.

3 Click **New Organization**.

4 Type a name.

5 (Optional) Type a description.

6 Select one or more resource pools from **Available** and move them to **Selected**.

7 Select one or more host spanning transport networks from **Available** and move them to **Selected**.

8 Select one or more physical networks from **Available** and move them to **Selected**.

9 Click **Import Members**.

10 Select your search option from the **Look for** drop-down menu.

11 Type your search terms and click **Search**.

Lab Manager displays the first 200 results that match the search terms.

12 Select the check boxes next to the users or groups that you want to add.

13 Click **Add** and **OK**.

14 Select a role for each added user or group.

15 Click **OK**.

Lab Manager creates the organization and creates the **Main** workspace.

Create a Workspace

Every organization includes a **Main** workspace. System administrators and administrators with rights at the organization level can create additional workspaces. For example, you can create integration, testing, staging, and production workspaces to manage service transition activities. When you create a workspace, you can choose whether you want to share its configurations or keep them private. In a shared workspace, by default, all the users in that workspace can access the configurations. In a private workspace, by default, users can only access their own configurations.

To create a workspace

1 In the **Organization** drop-down menu, select the organization in which you want to create a workspace.

2 In the left pane, click **Workspace(s)**.

3 Click **New Workspace**.

4 Type a name.

5 (Optional) Type a description.

6 Click **Add Users and Groups**.

7 Select your search option from the **Look for** drop-down menu.

8 Type your search terms and click **Search**.

9 Select the check box next to the users or groups you want to add.

10 Click **Add** and **OK**.

11 Select a role for each added user and group.

12 Decide whether you want the workspace to be shared or private.

13 Select one or more resource pools from **Available** and move them to **Resource Pools used by this Workspace**.

14 Click **OK**.

Setting Up Network Templates

5

A network template is a specification for a virtual network. You can associate a virtual machine NIC with a network template. When you deploy the virtual machine, Lab Manager creates a virtual network based on the network template and connects the NIC to that network.

Network templates allow system administrators, administrators with rights at the organization level, and template creators to predefine virtual networks for other users. A network template provides a level of control and consistency across the Lab Manager installation. These templates are created and owned by a user, but they can be shared with other users in an organization or across the entire installation.

This chapter includes the following topics:

Create a Network Template

By default, only system administrators, administrators with rights at the organization level, and template creators can create network templates.

To create a new network template

1 In the left pane, click **Network Templates**.

2 Click **New Network Template**.

3 Type a name.

4 (Optional) Type a description.

5 Select the IP addressing modes.

6 If you selected **Static - IP Pool** or **Static - Manual**, type the static mode settings and add an IP pool.

7 Click **OK**.

Lab Manager creates the network template in the user's organization.

Copy a Network Template

By default, only system administrators, administrators with rights at the organization level, and template creators can copy network templates. You can copy an existing network template to use it as the basis for a new network template. The user who creates or copies it becomes its owner. Lab Manager creates the copy in the currently selected organization.

To copy an existing network template

1 In the left pane, select **Network Templates**.

2 Move the pointer over a network template name and select **Copy**.

3 Type a name for the copied network template.

4 Modify the network template settings and click **Copy**.

Share a Network Template

If you are the owner of a network template, or if your user role includes the Administrator View and Control right, you can share a network template with other users. Sharing a network template grants access to other users.

Depending on your rights, you can share a network template within or between workspaces, within or between organizations, or across the entire Lab Manager installation.

When you share a network template, you can specify access rights for the users with whom you are sharing the configuration. Access rights combine with the rights provided by a user's role to determine how that user can interact with the shared network template. Access rights cannot provide users with rights that they do not already have based on their role.

To share a network template with other users

1 In the left pane, select **Network Templates**.

2 Move the pointer over a network template name and select **Sharing**.

The Sharing Network Template dialog box displays the users and organizations that currently have access to the network template and their level of access control.

3 Click **Add Users**.

4 Select the organization containing the users with whom you want to share the network template or select **Global** to view users from all organizations.

5 Select with whom you want to share the network template.

- **Everyone in Organization** shares the network template with all users in the selected organization.
- **Everyone in Workspace** shares the network template with all users in the selected workspace.
- **Selected Users** shares the network template with specific users in the selected organization.

  Select the check box next to each user with whom you want to share the network template.

6 Specify the access rights for the users and click **OK**.

If you share a network template with users outside of the organization in which the template was created, you can only specify Read access. In addition, network templates created in Global can only be shared with Read access.

7 Click **OK** and **Done**.

Setting Up Virtual Machine Templates 6

A virtual machine template is a virtual machine image loaded with an operating system, applications, and data. After you define and publish a virtual machine template, you can create additional virtual machines based on this template, without reinstalling software or redoing setup tasks on each virtual machine. Using virtual machine templates ensures that virtual machines are consistently configured across an entire organization.

By default, system administrators and administrators with rights at the organization and workspace levels, and template creators can create a new virtual machine template, import a virtual machine template, save an existing virtual machine as a template, and clone an existing virtual machine template.

Lab Manager adds the **ttylinux-4-ESX3** virtual machine template to the VM Templates page during installation. You can use this sample virtual machine template to learn more about virtual machine templates. Log in to the guest operating system of the sample virtual machine template by typing **`root`** as the user name and **`password`** as the password.

This chapter includes these topics:

Create a Virtual Machine Template

The properties that you specify when you create a virtual machine template are the default properties for all virtual machines based on the template.

After creating a virtual machine template, you can deploy the virtual machine template and install a guest OS, VMware Tools, and applications. After the virtual machine template meets the requirements for guest customization, and you complete the steps for Windows NT and Solaris templates, you can share this template with other Lab Manager users and publish it. This makes it available for building configurations.

To create a virtual machine template

1 In the left pane, click **VM Templates**.

2 Click **New VM Template**.

3 Type a name.

4 (Optional) Type a description.

5 Select a datastore.

6 Select a virtual machine version.

The version determines on which ESX/ESXi host that the virtual machine runs. The default is virtual machine version 7, which runs on ESX/ESXi 4.0 or later.

7 Select a guest operating system (OS).

If you select a 64-bit guest OS, the datastore must be connected to an ESX/ESXi host that provides the required 64-bit processor for that guest OS. You can create a template without a host, but you cannot deploy the virtual machine template until you attach a host with the correct processor. If you have some (but not all) 64-bit hosts, Lab Manager limits the number of hosts on which the virtual machine template can be deployed. For information on enabling an ESX/ESXi host to provide 64-bit support, see the VMware Infrastructure documentation.

8 Select the number of virtual CPUs.

The datastore for this virtual machine template must be connected to a host that provides the required SMP technology for the guest OS. If you choose a CPU number not currently compatible with the CPU of the host, you cannot deploy the virtual machine template until you attach a host with the appropriate SMP support. If you have some but not all hosts that provide the required SMP technology, Lab Manager limits the number of hosts on which the virtual machine template can be deployed.

9 Type the memory.

10 In the **Hard Disk** panel, type the size and select the bus type.

11 In the **Network Interface** panel, select a network, and if applicable, select an IP address mode.

12 Select a storage lease.

13 Click **OK**.

Lab Manager creates the virtual machine template in the current organization, and it appears on the VM Templates page as **Undeployed** and **Unpublished**.

Importing Virtual Machine Templates

Importing a virtual machine template involves copying an external virtual machine into the Lab Manager template library. You can import a virtual machine that is new to, or was previously exported by, Lab Manager. Lab Manager changes the MAC address of all imported virtual machines.

Lab Manager supports these virtual machines types for import operations:

- VMware Workstation
- VMware Server
- VMware ESX/ESXi
- BEA LiquidVM

  Only LiquidVMs that use static IP mode and DHCP mode are supported. If importing takes longer than two hours, Lab Manager times out. To modify the timeout for vCenter and SMB imports, see "Configuring General Preferences" on page 135.

You cannot import a virtual machine that uses raw device mappings (RDMs).

Import a Virtual Machine Template from vCenter

By default, only a system administrator can import virtual machine templates from vCenter.

If you have a virtual machine in a resource pool managed by vCenter, you can import this machine as a virtual machine template to Lab Manager. If a virtual machine has vCenter snapshot files, Lab Manager imports the original virtual machine as a template and discards the snapshot files.

The virtual machine must be powered off and in the same datacenter as the one being managed by Lab Manager.

NOTE Before you import virtual machines from vCenter, they cannot be in a folder named **VM**.

To import a virtual machine template from vCenter

1 In the left pane, select **VM Templates**.

2 Click **Import VM Template**.

3 Type a name.

4 (Optional) Type a description.

5 Select **vCenter** and select a virtual machine that is not managed by Lab Manager.

6 Click **Next**.

7 (Optional) Deselect the **Perform customization** check box if you do not want Lab Manager to customize the network settings for the virtual machine template or virtual machines based on the virtual machine template.

8 Specify the networking information for each NIC in the imported virtual machine template:

   a Select the **Connected** check box.

   b Choose a default virtual or physical network.

   c Choose a default IP addressing mode.

9 Select a storage lease.

10 Select a deployment lease.

11 Select the datastore to which you want to import the virtual machine template.

12 Select whether to copy or move the source virtual machine template.

   If you copy the virtual machine template, it continues to exist in the original location, but if you move the virtual machine template, it will not exist in this location.

13 Click **Import**.

Lab Manager imports the virtual machine template into the current organization and displays it on the VM Templates page.

Import a Virtual Machine Template from SMB Storage

An SMB port needs to be open on the ESX host. Although Lab Manager opens the port during installation, you need to make sure that the port remains open after installation. To check the port status, run **`esxcfg-firewall -q smbClient`** on each host.

By default, only a system administrator, an administrator with rights at the organization, and a template creator can import virtual machines as templates from an SMB share.

IMPORTANT Do not import virtual machine templates manually with ESX commands.

To import a virtual machine template from SMB storage

1 In the left pane, click **VM Templates**.

2 Click **Import VM Template**.

3 Type a name.

4 (Optional) Type a description.

5 Select **SMB File Server**.

6 Type the UNC path to the appropriate SMB share (relative to the Lab Manager server).

For example, **`\\10.10.10.10\importdir`**.

Use English characters for the UNC path. Lab Manager does not support SMB shares that include the `$` symbol in the UNC path.

7 If the UNC folder requires authentication, type the user name and password.

8 Click **Next**.

9 (Optional) Deselect the **Perform customization** check box if you do not want Lab Manager to customize the network settings for the virtual machine template or virtual machines based on the virtual machine template.

If you are importing a virtual machine template that was previously exported from Lab Manager, skip this step, because Lab Manager can detect whether the template was set up for customization.

10 Specify the networking information for each NIC in the imported virtual machine template.

a Select the **Connected** check box.

b Choose a default virtual or physical network.

c Choose a default IP addressing mode.

11 Select a storage lease option.

12 Select a deployment lease option.

13 Select the datastore to which you want to import the virtual machine template.

14 Click **Import**.

Lab Manager imports the virtual machine template into the current organization and displays it on the VM Templates page.

Save a Virtual Machine as a Virtual Machine Template

You can create a virtual machine template from any virtual machine in Lab Manager. This new template is a linked clone of the original virtual machine.

To create a virtual machine template from an active virtual machine

1 In the left pane, click **All Configurations**.

2 Move the pointer over a configuration name and select **Open**.

3 Move the pointer over the virtual machine name and select **Add To VM Templates**.

4 Type a name.

5 (Optional) Type a description.

6 Select a deployment lease.

7 Select a storage lease.

8 Click **OK**.

9 In the left pane, click **VM Templates**.

Clone a Virtual Machine Template

You can create a linked or a full clone of a virtual machine template to use the software installed on that virtual machine template.

A linked clone operation creates a delta disk instead of copying the entire virtual hard disk. This operation uses referential provisioning, which involves storing new changes but refers back to a chain of delta disks. For each change, Lab Manager freezes the original delta disk and creates a new one.

A full-clone operation copies all the delta disks and the base disk and consolidates them into a new base disk. The original base disk remains unchanged. Lab Manager creates the cloned virtual machine template in the current organization. The user performing the clone operation becomes the owner of the cloned virtual machine template.

NOTE You can create a full clone only on undeployed virtual machine templates.

Create full clones when you want to dismantle the storage and move the virtual machine template to a different server or maximize performance for virtual machines (for example, for certain production-level virtual machines).

To clone a virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over the virtual machine template name and select **Clone**.

3 Type a name.

4 (Optional) Type a description.

5 Select a storage lease.

6 Select a deployment lease.

7 Select the type of clone that you want to create.

If you select **Full Clone of Virtual Machine Template**, select a datastore.

8 Click **OK**.

Deploying Virtual Machine Templates

Deploying a virtual machine template registers it with a resource pool and provides access to Lab Manager operations at the virtual machine console level. By default, system administrators, administrators, template creators, and application owners can deploy and undeploy virtual machine templates. You can only deploy unpublished templates.

Deploy a Virtual Machine Template with Default Settings

When you deploy a virtual machine template with default settings, Lab Manager uses:

- **Any Available** resource pool option is used.
- The **Power On After Deployment** check box is selected.
- The deployment lease comes from the template properties.

To deploy a virtual machine template with default settings

Move the pointer over the virtual machine template name and select **Deploy with defaults**.

Deploy a Virtual Machine Template with Custom Settings

You can deploy a virtual machine template to a resource pool using custom settings.

To deploy a virtual machine template with custom settings

1 On the **VM Templates** page, move the pointer over the virtual machine template name and select **Deploy**.

2 Select a resource pool or select **Any Available**.

3 Deselect the **Power On Machines After Deployment** check box to prevent Lab Manager from turning on the virtual machine immediately after deployment.

Deselect this option when you want to manually bring up a virtual machine template.

4 Select a deployment lease and click **OK**.

Lab Manager deploys the virtual machine template.

Install a Guest Operating System

A virtual machine template must be deployed to install an operating system on it. To install a guest OS, you must ensure that the appropriate ISO image file for the OS is available in the Lab Manager media library. See "Managing the Media Library" on page 105 for more information.

Installing a guest OS on a virtual machine template is similar to installing an OS on a physical machine and takes a similar amount of time.

To install a guest operating system on a virtual machine template

1 In the left frame, click **VM Templates**.

2 Click a console thumbnail of a deployed template.

3 Move the pointer over the tab with the virtual machine template name and select **Insert CD**.

4 Select an ISO file and click **OK**.

5 On the tab, move the pointer over the virtual machine template name and select **Ctrl-Alt-Del** to boot from the ISO image and launch the operating system installer.

6 In the virtual machine console of the virtual machine template, enter the required information for the installation process.

Installing VMware Tools

Lab Manager depends on VMware Tools to customize the guest operating system in a virtual machine. VMware Tools also allows you to move the pointer in and out of the virtual machine console window.

A virtual machine template must be deployed to install VMware Tools. This process takes several minutes and requires you to restart the virtual machine.

Install VMware Tools in a Windows Guest

By default, system administrators, administrators with rights at the organization level, and template creators can install VMware Tools. After you install VMware Tools, Windows 2000 and Windows XP guest operating systems must be rebooted to use the new driver. For more information about the installation, see VMware vSphere documentation.

To install VMware Tools on a Windows Guest

1 On the VM Templates page, move the pointer over the virtual machine template name and select **View Console**.

2 Log in to the guest operating system inside the virtual machine console.

3 Click **Install VMware Tools**.

Depending on whether autorun is enabled, one of the following occurs inside the guest operating system:

- If autorun is enabled in the guest operating system, a dialog box appears after a few seconds. It asks whether you want to install VMware Tools.
- If autorun is not enabled, the dialog box does not appear automatically. Click **Start > Run** and enter **`D:\setup\setup.exe`** where `D:` is your first virtual CD-ROM drive.

4 Click **Yes** to launch the InstallShield wizard.

5 Follow the on-screen instructions.

On some Windows operating systems, after the SVGA driver is installed, you are prompted to reboot to use this new driver.

6 Reboot the virtual machine if necessary.

Install VMware Tools on a Linux Guest Within X with the RPM Installer

By default, only system administrators, administrators with rights at the organization level, and template creators can install VMware Tools. For more information about the installation, see VMware vSphere documentation.

To install VMware Tools on a Linux guest within X with the RPM installer

1 On the VM Templates page, move the pointer over the virtual machine template name and select **View Console**.

2 Log in to the guest operating system.

3 Click **Install VMware Tools**.

The remaining steps are completed in the guest operating system.

4 Complete one of the tasks.

- If you see a VMware Tools CD icon on the desktop, double-click it, and double-click the RPM installer in the root of the CD-ROM.
- If you see a file manager window, double-click the RPM installer file.

In some Linux distributions, if the VMware Tools CD icon fails to appear, install VMware Tools from the command line.

5 When prompted, type the root password and click **OK**.

The installer prepares the packages.

6 Click **Continue** when the package is ready.

A dialog box appears with a progress bar. When VMware Tools is installed, there is no confirmation or **Finish** button.

7 In an X terminal, as root (`su –`), run **`vmware-config-tools.pl`** to configure VMware Tools.

8 Press **Enter** to accept the default value.

9 After the upgrade is complete, restart the network by running **`/etc/init.d/network restart`**.

10 When you are finished, type **`exit`**.

11 To start the VMware Tools control panel, run **`vmware-toolbox &`**.

Install VMware Tools on a Linux Guest with the Tar Installer or RPM Installer

By default, only system administrators, administrators with rights at the organization level, and template creators can install VMware Tools. For more information about the installation, see VMware vSphere documentation.

To install VMware Tools on a Linux guest with the tar installer or RPM installer

1 On the VM Templates page, move the pointer over the virtual machine template name and select **View Console**.

2 Log in to the guest operating system in the virtual machine console.

3 Click **Install VMware Tools**.

The remaining steps take place in the guest operating system.

4 As root (`su –`), mount the VMware Tools virtual CD-ROM image and change to a working directory (for example, `/tmp`).

Some Linux distributions automatically mount CD-ROMs. If your distribution uses automounting, do not use the `mount` and `umount` commands described in this procedure. You still must untar the VMware Tools installer to `/tmp`.

Some Linux distributions use different device names or organize the `/dev` directory differently. If your CD-ROM drive is not `/dev/cdrom`, or if the mount point for a CD-ROM is not `/mnt/cdrom`, modify the following commands to reflect the conventions used by your distribution.

```
mount /dev/cdrom /mnt/cdrom
```

```
cd /tmp
```

If you have an existing installation, delete the `vmware-tools-distrib` directory before you install. The location of this directory depends on where you placed it when you did the previous installation, for example, `/tmp/vmware-tools-distrib`.

5 Uncompress the installer and unmount the CD-ROM image.

- For the tar installer, at the command prompt, type:

  ```
  tar zxpf /mnt/cdrom/VMwareTools-3.5.0-<xxxx>.tar.gz
  ```

  ```
  umount /dev/cdrom
  ```

  <xxxx> is the build/revision number of the release.

  This tar installer string applies to an ESX 3.5 host. If you are using an ESX 4.0 host, type **`tar zxpf /mnt/cdrom/VMwareTools-4.0.0-<xxxx>.tar.gz`**

- For the RPM installer, at the command prompt, type:

  ```
  rpm -Uhv /mnt/cdrom/VMwareTools-3.5.0-<xxxx>.i386.rpm
  ```

  ```
  umount /dev/cdrom
  ```

  <xxxx> is the build/revision number of the release.

  This rpm installer string applies to an ESX 3.5 host. If you are using an ESX 4.0 host, type **`tar zxpf /mnt/cdrom/VMwareTools-4.0.0-<xxxx>.i386.gz`**

If you attempt to install an `rpm` installation over a `tar` installation, or the reverse, the installer detects the previous installation and must convert the installer database format before continuing.

6 Run the installer.

- For the tar installer, type:

  cd vmware-tools-distrib

  ./vmware-install.pl

  Press **Enter** to accept the default value.

- For the RPM installer, configure VMware Tools:

  vmware-config-tools.pl

  Press **Enter** to accept the default value.

7 After the upgrade is complete, restart the network by running **/etc/init.d/network restart**.

8 Type **exit**.

9 Start your graphical environment.

10 In an X terminal, run **vmware-toolbox &**.

Install VMware Tools on a Solaris Guest

By default, only system administrators, administrators with rights at the organization level, and template creators can install VMware Tools. For more information about the installation, see VMware vSphere documentation.

To install VMware Tools on a Solaris guest

1 On the VM Templates page, move the pointer over the virtual machine template name and select **View Console**.

2 Log in to the guest operating system in the virtual machine console.

3 Click **Install VMware Tools**.

The remaining steps take place in the virtual machine.

4 Log in as root (`su –`) and, if necessary, mount the VMware Tools virtual CD-ROM image.

The Solaris volume manager `vold` mounts the CD-ROM under `/cdrom/vmwaretools`. If the CD-ROM is not mounted, restart the volume manager by running the following commands:

/etc/init.d/volmgt stop

/etc/init.d/volmgt start

5 After the CD-ROM is mounted, change to a working directory (for example, `/tmp`) and extract VMware Tools.

cd /tmp

gunzip –c /cdrom/vmwaretools/vmware-solaris-tools.tar.gz | tar xf –

6 Run the VMware Tools tar installer:

cd vmware-tools-distrib

./vmware-install.pl

7 Press **Enter** to accept the default value.

8 Type **exit.**

9 Start your graphical environment.

10 In an X terminal, run **vmware-toolbox &**.

Customizing the Guest Operating System

Lab Manager can customize the network settings of a guest operating system that was created from a virtual machine template. These settings include the machine name, IP settings, and security identifier (SID) for Windows guest operating systems. The customization allows you to create and deploy multiple, unique virtual machines based on the same virtual machine template without a machine name or network conflicts.

When you configure a virtual machine template with the prerequisites for guest customization and create a virtual machine that uses this virtual machine template, Lab Manager creates a package with guest customization tools. When you deploy and power on the virtual machine the first time, Lab Manager copies the package, runs the tools, and deletes the package from the virtual machine.

You can enable or disable customization for a virtual machine template or a virtual machine. To avoid conflicts when you are not using guest customization, access the virtual machine console through Lab Manager and manually set its network parameters to unique values. By default, Lab Manager enables guest customization when you create a new template.

Access the machine.id from an ESX Host

The configuration file for a virtual machine, the `.vmx` file, contains a `machine.id` line. The Lab Manager server system sets the values for this line while deploying virtual machines.

Enabling guest customization on a virtual machine template configures a script to run every time the system starts up. This script reads the `machine.id` information and determines which action to take.

The Lab Manager server system does not set any actions in the `machine.id` line while deploying virtual machine templates. As a result, the guest customization script does not perform any customization for the virtual machine template when it starts up.

The Lab Manager server system does set customization actions in the `machine.id` line while deploying virtual machines or changing virtual machine network settings. When these virtual machines first start up, the guest customization script performs the relevant actions.

To access the machine.id line from the ESX/ESXi host

1 From the ESX/ESXi host system, open the `.vmx` file.

2 Find the `machine.id` line.

Access the machine.id from a Guest Operating System

If you install VMware Tools, you can access the `machine.id` from the guest operating system of a deployed virtual machine.

To access the machine.id line from the guest operating system

1 In the left pane, click **Workspace**s.

2 Move the pointer over the configuration name and select **Open**.

3 Move the pointer over the deployed virtual machine name and select **Show Console**.

4 Search for `machine.id` from inside the guest operating system.

- From a Linux guest OS, type:

  ```
  # vmware-guestd --cmd machine.id.get
  ```

- From a Windows guest OS, navigate to the directory where VMware Tools is installed (usually `C:\Program Files\VMware\VMware Tools`) and type:

  ```
  >VMwareService.exe -cmd machine.id.get
  ```

The following is an example of a `machine.id` line:

```
numnics=2&macaddr_0=00:50:56:3f:00:1c&bootproto_0=static&ip_0=10.115.127.10&netmask_0=255.255.248
.0&gateway_0=10.115.127.253&dns1_0=10.20.20.1&dns2_0=10.20.20.2&suffix_0=eng.vmware.com&macaddr_1
=00:50:56:3f:00:1d&bootproto_1=static&ip_1=1.1.1.100&netmask_1=255.255.0.0&gateway_1=1.1.1.1&dns1
_1=2.2.2.2&dns2_1=&suffix_1=BLUE.ORG&primaryNic=0&computerName=Config10VM1&UseSysPrep=No&bitMask=
11&markerid=504810238&reconfigToken=411678171
```

Prerequisites for Guest Customization

Before you configure the template, complete or check these issues:

- Specify the correct guest operating system on the Virtual Machine Template Properties page. Lab Manager uses this information to determine how to customize the operating system.
- Install the version of VMware Tools packaged with ESX 3.5 or later. The Lab Manager Web console also provides the correct version for installation.

  If you import a virtual machine as a virtual machine template, you must deploy the virtual machine template. The deploy operation allows Lab Manager to detect the version of VMware Tools installed on the virtual machine template. If the virtual machine template has an outdated version or never had VMware Tools installed on it, you must install it.

  If you import a virtual machine template that was originally used in VMware Lab Manager version 2.x, see "Importing Virtual Machine Templates from Lab Manager 2.x with VMware Tools and LM Tools" on page 45.
- Ensure that the virtual machine template is not part of a domain.
- Do not configure the virtual machine template as a Microsoft Cluster Service server, a Microsoft Certificate Services server, or a domain controller.
- As the administrator, set up a Microsoft Sysprep package for the following Windows guest operating systems:
  - Microsoft Windows XP 64 bit
  - Microsoft Windows 2003 64 bit
  - Microsoft Windows 2008
  - Microsoft Vista

  See "Build a Microsoft Sysprep Package" on page 41 for more information.
- See "Complete Guest Customization for Windows NT and Solaris Virtual Machine Templates" on page 42 for additional steps for Microsoft Windows NT Server 4 and Solaris virtual machine templates.

Build a Microsoft Sysprep Package

By default, Lab Manager uses SIDgen, a tool packaged with the installation, to perform guest customization for Windows 2000, Windows 2003 (32 bit), and Windows XP (32 bit) guest operating systems. You can also use Microsoft Sysprep instead of SIDgen to perform guest customization in these guest operating systems. For Windows 2003 (64 bit) and Windows XP (64 bit), Microsoft Windows 2008, Microsoft Vista guest operating systems, you must use Microsoft Sysprep to perform guest customization.

Before you can use Microsoft Sysprep, you must build a package that includes the Microsoft Sysprep files for the following guest OS:

- Windows 2000
- Windows 2003 (32 bit)
- Windows 2003 (64 bit)
- Windows XP (32 bit)
- Windows XP (64 bit)

Microsoft Sysprep is included on the installation CDs for Windows 2000, Windows 2003, and Windows XP.

CAUTION Lab Manager provides a customized `sysprep.inf` file. When the Microsoft Sysprep package is being built, do not overwrite this file with the `sysprep.inf` file from the Windows CD.

To build a Microsoft Sysprep package for guest customization

1 Insert the Windows OS CD in the Lab Manager server.

If you have an ISO, mount the ISO using a third-party tool.

2 Find the `DEPLOY.CAB` file in `\Support\Tools`.

3 Expand the `DEPLOY.CAB` file with a tool that can read Microsoft CAB files.

You can also use Windows Explorer in Windows XP or Windows 2003.

4 Copy the files to the appropriate Lab Manager directory for Microsoft Sysprep support.

For example, if you installed Lab Manager in `C:\Program Files\VMware\VMware Lab Manager`, copy the files to one of the following directories.

- `C:\Program Files\VMware\VMware Lab Manager\Tools\CustomizeGuest\Windows\Sysprep\win2k3`
- `C:\Program Files\VMware\VMware Lab Manager\Tools\CustomizeGuest\Windows\Sysprep\win2k3_64`

  This location is for 64-bit Windows 2003.
- `C:\Program Files\VMware\VMware Lab Manager\Tools\CustomizeGuest\Windows\Sysprep\win2000`
- `C:\Program Files\VMware\VMware Lab Manager\Tools\CustomizeGuest\Windows\Sysprep\winxp`

  This location is for 64-bit Windows XP:
- `C:\Program Files\VMware\VMware Lab Manager\Tools\CustomizeGuest\Windows\Sysprep\winxp_64`

5 In the Web console, click **Settings** in the left pane.

6 In the **Guest Customization** tab, click **Build Package**.

A green check confirms that the package has been built.

Complete Guest Customization for Windows NT and Solaris Virtual Machine Templates

Windows NT virtual machine templates require extra steps for guest customization.

To complete guest customization for Windows NT virtual machine templates

1 In the left pane, click **VM Templates**.

2 Move the pointer over the deployed virtual machine template name and select **View Console**.

3 Log in to the Windows NT guest operating system.

4 Move the pointer over the virtual machine template name and select **Insert Customization CD**.

This option starts a script that copies files to the guest and prepares the virtual machine template for customization.

Complete Guest Customization for Solaris Virtual Machine Templates

Solaris virtual machine templates require extra steps for guest customization.

To complete guest customization for Solaris virtual machine templates

1 In the left pane, click **VM Templates**.

2 Move the pointer over the deployed virtual machine template name and select **View Console**.

3 Move the pointer over the virtual machine template name and select **Insert Customization CD**.

4 Log in to the Solaris guest operating system.

5 In the terminal, run these case-sensitive commands:

```
/etc/init.d/volmgt stop

/etc/init.d/volmgt start

sh /cdrom/cdrom/customize-guest.sh install

eject cdrom
```

6 Run **`shutdown -y -g0 -i5`** to shut down the virtual machine from inside the guest operating system.

Working with the Guest Customization SID Generation Tool

For guest operating systems that support multiple SID generation tools, you can set a global preference to use Microsoft Sysprep instead of SIDgen, which is packaged with Lab Manager. You can also select SIDgen or Microsoft Sysprep as the SID generation tool for a virtual machine or virtual machine template.

For Windows 2003 (64 bit) and Windows XP (64 bit) guest operating systems, you must use Microsoft Sysprep. Windows Vista and Windows 2008 guest operating systems always use Microsoft Sysprep instead of SIDgen, because Microsoft Sysprep is already built into these operating systems.

See Appendix C, "Guest Operating System Support," on page 161 for more information on guest operating support for SIDgen and Microsoft Sysprep.

Select the SID Generation Tool for Lab Manager

You need to set the default SID generation tool to use with the new virtual machine templates that require Microsoft Sysprep and templates that support SIDgen or Microsoft Sysprep.

To select the tool for Lab Manager

1 In the left pane, click **Settings**.

2 On the **Guest Customization** tab, select a default SID generation mechanism.

This selection determines the default mechanism of new virtual machine templates. If you are not ready to use Sysprep, select **Use Pre-Installed SID Generation Tool (SIDgen)**.

To change the SID mechanism for a virtual machine or virtual machine template, edit the properties of that virtual machine or virtual machine template.

3 Click **OK**.

Lab Manager sets the default SID generation mechanism.

Change the SID Generation Tool for a Virtual Machine Template

You can override the default SID generation tool specified on the Guest Customization tab for individual virtual machine templates. You can only use Microsoft Sysprep if you have already built a Microsoft Sysprep package. See "Build a Microsoft Sysprep Package" on page 41.

To change the SID generation tool for a virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over a virtual machine template name and select **Properties**.

3 Select the SID mechanism.

4 Click **Update**.

Lab Manager changes the SID generation tool for a virtual machine template.

Select the SID Generation Tool for a Virtual Machine

You can override the default SID generation tool specified on the **Guest Customization** tab for individual Windows-based virtual machines. To display Microsoft Sysprep as an option, you must first build a Microsoft Sysprep package. See "Build a Microsoft Sysprep Package" on page 41.

To select the SID generation tool for a virtual machine

1 In the left pane, move the pointer over a configuration name and select **Open**.

2 Move the pointer over a virtual machine name and select **Properties**.

3 Select the SID mechanism.

4 Click **Update**.

Disabling Guest Customization

Lab Manager activates guest customization when you create or import a virtual machine template. When you add a virtual machine to a configuration, it inherits the guest customization settings of the virtual machine template on which it is based.

Disable guest customization in the following situations:

- The software in the virtual machine or virtual machine template is configured to use specific network settings.
- You have virtual machines that must remain untouched for specific security or integrity requirements.
- You are not using one of the supported guest operating systems listed in Appendix C, "Guest Operating System Support," on page 161.

Disable Guest Customization for a Virtual Machine Template

You can disable guest customization in the properties of virtual machine templates. The setting is stored when you export the virtual machine template to SMB storage and import it back to Lab Manager. If you create a virtual machine template based on an active virtual machine in a configuration, the virtual machine template inherits the customization setting of the active virtual machine.

To disable guest customization for a virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over an unpublished virtual machine template name and select **Properties**.

3 Deselect the **Perform customization** check box.

4 Click **Update**.

Disable Guest Customization for a Virtual Machine

Virtual machines inherit their guest customization settings from the virtual machine templates on which they are based. You can override these settings in the properties of a virtual machine.

To disable guest customization for a virtual machine

1 In the left pane, click **Workspace**.

2 Move the pointer over a configuration name and select **Open**.

3 On the **Virtual Machines** tab, move the pointer over a virtual machine name and select **Properties**.

4 Deselect the **Perform customization** check box.

5 Click **Update**.

Customize Guest Customization

Lab Manager allows you to add a customization script to a virtual machine template. The script runs before and after the guest customization when you deploy a virtual machine based on the virtual machine template. For example, the script could check for viruses or start and stop processes.

The script is called with the `precustomization` command line parameter before the guest customization process starts and is called with the `postcustomization` command line after the guest customization process has finished.

To add a customization script to a template

1 In the left pane of the console, click **VM Templates**.

2 Move the pointer over the virtual machine template name and select **Customization Script**.

3 Click **Browse** to locate an existing script or type the script.

Specify a batch script for Windows guests and a shell script for UNIX guests. The script can include text and cannot include binary data.

4 Click **OK**.

Importing Virtual Machine Templates from Lab Manager 2.x with VMware Tools and LM Tools

If you import virtual machine templates from Lab Manager 2.x, the templates probably have an older version of VMware Tools, and the enforcement check prevents you from publishing the virtual machine templates.

If you cannot publish the templates, do one of the following:

- Upgrade VMware Tools to the current Lab Manager version. Upgrading allows guest customization and publishing to occur.
- If the virtual machine template has LM Tools, disable the VMware Tools enforcement check, which allows Lab Manager to customize guests based on the method used in the previous version. See "Disable VMware Tools Check Before Publishing Virtual Machine Templates" on page 47. VMware does not recommend this approach.
- If the virtual machine template does not have LM Tools and you do not upgrade VMware Tools, deselect the **Perform Customization** check box in the virtual machine template properties. See "Disabling Guest Customization" on page 44.

Undeploy a Virtual Machine Template

You must undeploy a virtual machine template before publishing, exporting, consolidating, or deleting it. Undeploying a virtual machine template unregisters it from vCenter.

When you undeploy, you can save or discard the state of the virtual machine template. You cannot save or discard state for a template that is powered off, because the virtual machine does not have a state. Saving memory state helps you to debug memory-specific issues.

To undeploy a virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over the deployed virtual machine template name and select **Undeploy - Save State** or **Undeploy - Discard State**.

If an ESX/ESXi host goes offline or someone manually removes a virtual machine template from the vCenter inventory, the standard undeploy operation does not work. In this case, move the pointer over the virtual machine template name and select **Force Undeploy**.

Share a Virtual Machine Template

If you are the owner of a virtual machine template, or if your user role includes the Administrator View and Control right, you can share a virtual machine template with other users. Sharing a virtual machine template grants access to other users.

Depending on your rights, you can share a virtual machine template within or between workspaces, within or between organizations, or across the entire Lab Manager installation.

When you share a virtual machine template, you can specify access rights for the users with whom you are sharing the template. Access rights combine with the rights provided by a user's role to determine how that user can interact with the shared virtual machine template. Access rights cannot provide users with rights that they do not already have based on their role.

To share a virtual machine template

1 On the VM Templates page, move the pointer over the virtual machine template name and select **Sharing**.

The Sharing Template dialog box displays the users and organizations that currently have access to the template and their level of access control.

2 Click **Add Users**.

3 Select the organization containing the users with whom you want to share the virtual machine template or select **Global** to view users from all organizations.

4 Select with whom you want to share the virtual machine template.

- **Everyone in Organization** shares the virtual machine template with all users in the selected organization.
- **Everyone in Workspace** shares the virtual machine template with all users in the selected workspace.
- **Selected Users** shares the virtual machine template with specific users in the selected organization.

  Select the check box next to each user with whom you want to share the virtual machine template.

5 Specify the access rights for the users and click **OK**.

If you share a virtual machine template with users outside of the organization in which the template was created, you can only specify Read access. In addition, virtual machine templates created in Global can only be shared with Read access.

6 Click **OK** and **Done**.

Publishing Virtual Machine Templates

Publishing a virtual machine template allows you to build configurations without reinstalling software or redoing setup tasks. Templates ensure that virtual machines are consistently configured with the correct operating systems, versions, system packs, and so on.

Check VMware Tools Status Before Publishing Virtual Machine Templates

Lab Manager depends on VMware Tools for guest customization. Before you publish a virtual machine template, check the status of VMware Tools on the virtual machine template and address any issues. To publish a virtual machine template without VMware Tools, see "Disabling Guest Customization" on page 44 for more information.

To check VMware Tools status

1 In the left pane, click **VM Templates**.

2 Check the **VMware Tools** column on the VM Templates page.

If the status is Installed (Requires Update) or Not Installed, you must deploy the virtual machine template and follow the prompts to update or install VMware Tools. See "Installing VMware Tools" on page 36.

If the status is Unknown, you must deploy the virtual machine template and allow Lab Manager to check for VMware Tools and update the information.

Disable VMware Tools Check Before Publishing Virtual Machine Templates

You can publish a template that does not have the current version of VMware Tools in these circumstances:

- You cannot install the current version of VMware Tools because you need special scripts in the virtual machine template for customization.
- You import virtual machine templates with an old version of LM Tools and you cannot upgrade VMware Tools on these templates.

  Lab Manager recognizes LM Tools and can customize the guest operating system according to the needs of that utility. VMware does not recommend this approach.
- You are not using one of the supported guest operating systems listed in Appendix C, "Guest Operating System Support," on page 161.

To disable the check of VMware Tools

1 In the left pane, click **Settings**.

2 On the **Guest Customization** tab, deselect the **Only Allow Publishing of Templates With a Version of VMware Tools That Supports Guest Customization** check box.

3 Click **OK**.

Publish a Virtual Machine Template

You can only publish undeployed virtual machine templates.

To publish a virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over the virtual machine template name and select **Publish**.

Working with Configurations 7

Configurations are the core of Lab Manager. A configuration consists of one or more virtual machines that are based on a virtual machine template or imported from vCenter. You can create, deploy, share, and monitor multimachine configurations.

In Lab Manager, configurations can exist in workspaces and in the configuration library. You can deploy a configuration and work with its virtual machines in a workspace. The configuration library is a repository of commonly used configurations and archived configurations. You cannot deploy a library configuration, but you can create a copy of any library configuration that you can access and work with that copy in a workspace.

Your actions at the configuration level affect all the virtual machines in the configuration. For information about working with the individual virtual machines within a configuration, see Chapter 8, "Working with Virtual Machines," on page 73.

Lab Manager adds the **Sample Configuration** to the Main workspace in the Default organization during installation. The sample configuration includes two virtual machines based on the **ttylinux-4-ESX3** sample virtual machine template. Use this sample configuration to learn more about configurations. You can log in to the guest operating system of the virtual machines as **`root`** and use **`password`** as the password.

This chapter includes these topics:

Adding Configurations to a Workspace

Before you can deploy a configuration and begin working with its virtual machines, you must add the configuration to a workspace. You can create a configuration that includes virtual machines based on virtual machine templates and virtual machines imported from vCenter. You can import entire configurations that you previously exported from VMware vCenter Lab Manager, vCenter Stage Manager, or vCenter Lab Manager. You can also copy a library configuration to a workspace. If you already have a workspace configuration that you want to use as the basis for a new configuration, you can clone it.

Create a Workspace Configuration

Creating a configuration involves defining configuration properties and adding virtual machines to the configuration. Lab Manager creates the configuration in the current organization and workspace.

To create a configuration

1 In the **Organization** drop-down menu, select the organization in which you want to create the configuration.

2 Click **Workspaces** and click the name of the workspace in which you want to create the configuration.

If you only have access to one workspace, click **Workspace**.

3 Click **New Configuration**.

4 Type a name.

5 (Optional) Type a description.

6 Specify the amount of time to allow the configuration to be deployed before Lab Manager undeploys the configuration.

7 Specify the amount of time to store the configuration before Lab Manager deletes the configuration or marks the configuration for deletion.

8 Specify the fencing policy.

9 Add virtual machines.

You can add virtual machines based on a Lab Manager virtual machine template or import virtual machines from vCenter. See "Add a Virtual Machine Based on a Virtual Machine Template" on page 50 and "Add a Virtual Machine from vCenter" on page 51.

10 Click **OK**.

Add a Virtual Machine Based on a Virtual Machine Template

Virtual machine templates provide the specifications for creating virtual machines, such as the guest operating system, number of virtual CPUs, and network interfaces. You can only add virtual machines based on published virtual machine templates.

To add a virtual machine based on a template

1 In the **Source** drop-down menu, select a virtual machine template.

You can select a virtual machine template that you created or a virtual machine template that is shared with you.

2 Type a name.

3 Specify the network information for the virtual machine.

Your options are based on how the virtual machine template was defined.

a Select a primary NIC for virtual machines with multiple NICs.

The primary NIC setting determines the default and only gateway for the virtual machine. The virtual machine can use any NIC to connect to other machines that are directly connected to the same network as the NIC, but it can only use the primary NIC to connect to machines on networks that require a gateway connection.

Consider this behavior when selecting a primary NIC, especially if you plan to deploy configurations that use fencing or connect virtual networks to physical networks.

b Select a network.

c Select an IP addressing mode. The available options are based on the IP addressing modes available to the selected network.

- **Static - IP Pool** pulls static IP addresses from the IP address pool.
- **DHCP** pulls IP addresses from a DHCP server.

  This option avoids the preparation and specification of an IP address or IP range. However, you cannot use Lab Manager fencing or connect virtual networks to physical networks with DHCP.
- **Static - Manual** allows you to specify an IP address.

d If you selected **Static - Manual** as the IP addressing mode, type an IP address in the **IP Address** field.

4 Select the **Full Clone** check box to consolidate the virtual machine.

By default, when you add a virtual machine to a configuration, the virtual machine is a linked clone that refers to the base disk of the virtual machine template and uses delta disks to describe the difference between the virtual machine template and the virtual machine.

NOTE Choosing this option requires additional disk space and increases the amount of time required to add the virtual machine to the configuration.

---

5 To add another virtual machine to this configuration, click **Add VM** and specify the required information.

Add a Virtual Machine from vCenter

You can add a virtual machine created in vCenter to a configuration. The virtual machine must be powered off and not already under Lab Manager control. Add a vCenter virtual machine if you know its vCenter network settings and want to maintain those settings in Lab Manager. If you do not care about the network settings, import the virtual machine from vCenter as a virtual machine template instead. See "Import a Virtual Machine Template from vCenter" on page 33.

To add a virtual machine from vCenter

1 Click **Import VM from vCenter**.

2 Select a virtual machine and click **OK**.

3 Type a name.

4 Specify the network information for the virtual machine.

a Specify a primary NIC for virtual machines with multiple NICs.

The primary NIC setting determines the default and only gateway for the virtual machine. The virtual machine can use any NIC to connect to other machines that are directly connected to the same network as the NIC, but it can only use the primary NIC to connect to machines on networks that require a gateway connection.

Consider this behavior when selecting a primary NIC, especially if you plan to deploy configurations that use fencing or connect virtual networks to physical networks.

b Select a network.

If the virtual machine is connected to a network that is available to both vCenter and Lab Manager, you cannot change the network during import. If the virtual machine is connected to a network that is only available to vCenter, you must choose a new network.

c Select an IP addressing mode.

5 Select a datastore.

6 To add another virtual machine to this configuration, click **Import VM from vCenter** and specify the required information.

Import a Configuration to a Workspace

You can import an existing configuration and all its virtual machines from an SMB share. Lab Manager supports importing configurations that were exported from vCenter Lab Manager or vCenter Stage Manager.

Import operations require access to a datastore connected to an ESX host with an open SMB port. Although Lab Manager opens the port during installation, make sure that the port was not closed after the install. To check the port status, run `esxcfg-firewall -q smbClient` on each host. If you only have access to datastores connected to ESXi hosts, you cannot import configurations.

When you import a configuration that you previously exported, Lab Manager sets the fencing policy for the imported configuration to Fenced Only. See "Modify Configuration Properties" on page 68 for information about how to modify the fencing policy.

When you import a configuration that was exported from Stage Manager or a version of Lab Manager prior to version 3.0.x, Lab Manager creates a virtual network (DefaultNetwork) and assigns all the configuration NICs to this network. You can add a different network to the configuration and reassign the NICs to that network. See "Add a Network to a Workspace Configuration" on page 67 and "Edit Network Interface Settings" on page 83.

To import a configuration

1. In the **Organization** drop-down menu, select the organization to which you want to import the configuration.
2. Click **Workspaces** and click the name of the workspace to which you want to import the configuration.

   If you only have access to one workspace, click **Workspace**.
3. Click **Import Configuration**.
4. Type the UNC path of the directory (relative to the Lab Manager server system) where the configuration file is stored.

   Use English characters for the UNC path. A sample path is `\\10.6.1.246\VMwareLM\ExportedConfigs`.
5. Type the user name and password for the import directory, if necessary.
6. Click **Next**.
7. Provide configuration details.
8. Click **Import**.

Copy a Workspace Configuration

You can copy a workspace configuration by cloning some or all of its virtual machines to a new configuration. If you have access to more than one workspace, you can clone configurations from one workspace to another. You cannot clone configurations from one organization to another.

When you create a clone, Lab Manager assigns the same network parameters to the cloned virtual machines. If you deploy the original and cloned configurations at the same time, duplicate IP address errors occur unless you deploy one of the configurations in fenced mode.

Full Clones and Linked Clones

When you clone configurations, you can consolidate the source configuration's virtual machines during the cloning process to create full clones of the virtual machines. Typically, you do not need to create full clones unless you plan to dismantle the storage and move the configuration to a different server, or if you need to maximize the performance of specific virtual machines (for example, for certain production-level virtual machines).

A full-clone operation copies all of a virtual machine's delta disks and its base disk and consolidates them into a new base disk. The original base disk remains unchanged. A full-clone operation takes longer than a linked-clone operation. You cannot make a full clone of a deployed configuration.

A linked-clone operation creates a delta disk instead of copying an entire virtual hard disk. This operation addresses virtual machine proliferation by using referential provisioning, a process that involves storing new changes but refers back to a chain of delta disks. For each clone, Lab Manager freezes the original delta disk and creates a new one.

To copy a workspace configuration

1 Move the pointer over the configuration name and select **Clone**.

2 Specify the destination workspace, if applicable.

3 Select **New Configuration** and type a name, description, and storage lease for the new configuration.

4 (Optional) Type change summary text that will appear on the new configuration's History tab.

5 Specify the type of clone.

6 Specify the virtual machines to clone.

   If you are creating a full clone and choose **Selected Virtual Machines**, you can specify a datastore.

7 Click **OK**.

Clone a Library Configuration to a Workspace

The configuration library is the central location for storing commonly used or base configurations. Users with the necessary rights can clone a library configuration to a workspace and then modify and deploy it. The original configuration remains in the library where it can be cloned again.

When you clone a captured library configuration to a workspace, Lab Manager creates a linked clone. Linked clones conserve storage space. Instead of copying the entire virtual disk for each virtual machine in the configuration, Lab Manager uses delta disks to track the differences between the original virtual machines and the cloned virtual machines.

When you clone an archived library configuration to a workspace, you can create a linked clone or a full clone.

You can clone all virtual machines in a configuration or selected machines. You can also combine configurations by cloning a library configuration to an existing workspace configuration.

To clone a configuration to the workspace

1 On the Library page, move the pointer over a configuration name and select **Clone to Workspace**.

2 Specify the destination workspace, if applicable.

3 Specify the destination.

   For a new configuration, type a name and description and specify a storage lease. For an existing configuration, select the configuration.

4 (Optional) Type change summary text that will appear on the configuration's History tab.

5 Specify the type of clone.

   This option is only available for archived library configurations. When you clone a captured library configuration to a workspace, Lab Manager always creates a linked clone.

6 Specify the virtual machines to clone.

   If you are creating a full clone and choose **Selected Virtual Machines**, you can specify a datastore.

7 Click **OK**.

After a brief time, an undeployed copy of the library configuration appears in the destination workspace.

Adding Configurations to the Library

You can add a workspace configuration to the Library by capturing it or archiving it. Capturing a workspace configuration makes it available as a base configuration that other users can copy and customize. Archiving a configuration preserves it for future reference. For example, an audit might require that you show the exact state of your software from years ago.

Capture a Workspace Configuration to the Library

You can save a workspace configuration to the Library to make a copy available to other users. You should save common base configurations to the library so that other Lab Manager users can work with or modify copies of those configurations.

When you capture a configuration to the Library, it becomes private, regardless of the sharing properties it had in the workspace. You can modify a library configuration at any time to share it with members of other organizations and workspaces.

To capture a configuration to the Library

1 Move the pointer over the configuration name and select **Capture to Library**.

2 Type a name.

Use a unique naming convention to simplify identification.

3 (Optional) Type a description.

4 (Optional) Select the **Gold Master** check box to indicate an important or administrator-approved configuration.

5 (Optional) Type change summary text that will appear on the captured configuration's History tab.

6 Specify a time to delete the configuration from storage or mark the configuration for deletion.

7 Click **Capture**.

Archive a Workspace Configuration to the Library

You can preserve the exact state of a configuration in the configuration library. Archived configurations are read-only, but you can clone, export, and delete them.

When you archive a configuration to the Library, it retains the sharing properties it had in the workspace. For example, if you archive a private workspace configuration, the library configuration is also private. You can modify a library configuration at any time to share it with members of other organizations and workspaces.

To archive a configuration to the Library

1 Move the pointer over the configuration name and select **Archive to Library**.

2 Type a name for the configuration.

Use a unique naming convention to simplify identification.

3 (Optional) Type a description.

4 (Optional) Type change summary text that will appear on the archived configuration's History tab.

5 Specify a time to delete the configuration from storage or mark the configuration for deletion.

6 Select the clone type.

If you select **Full Clone**, specify the destination datastore.

7 Click **OK**.

Lab Manager creates an archived configuration in the library.

Clone a Library Configuration

Lab Manager allows you to create full clones of Library configurations. A full-clone operation creates a new configuration that includes some or all of the virtual machines in the original configuration. As part of the process, Lab Manager consolidates the virtual hard disks of the virtual machines in the cloned configuration.

When you create a clone, Lab Manager assigns the same network parameters to the cloned virtual machines. If you move the original and cloned configurations to a workspace and deploy them at the same time, duplicate IP address errors occur unless you deploy one of the configurations in fenced mode.

Lab Manager creates cloned configurations in the organization currently selected in the Organization drop-down menu. The user performing the clone operation becomes the owner of the cloned configuration.

To clone a Library configuration

1 On the Library page, move the pointer over the configuration name and select **Clone to Library** from the menu.

2 Type a name.

3 (Optional) Type a description.

4 Specify a time to delete the configuration or mark the configuration for deletion.

5 (Optional) Type change summary text that will appear on the configuration's History tab.

6 Specify the virtual machines to clone and select a datastore.

7 Click **OK**.

Share a Configuration

If you are the owner of a configuration, or if your user role includes the Administrator View and Control right, you can share a workspace or library configuration with other users. Sharing a workspace configuration grants access to other users. Sharing a library configuration allows other users to clone their own copy of the configuration to a workspace.

Depending on your rights, you can share a configuration within or between workspaces, within or between organizations, or across the entire Lab Manager installation.

When you share a configuration, you can specify access rights for the users with whom you are sharing the configuration. Access rights combine with the rights provided by a user's role to determine how that user can interact with the shared configuration. Access rights cannot provide users with rights that they do not already have based on their role.

To share a configuration

1 Move the pointer over a workspace or library configuration name and select **Sharing**.

The Sharing Configuration dialog box displays the users and organizations that currently have access to the configuration and their level of access control.

2 Click **Add Users**.

3 Select the organization containing the users with whom you want to share the configuration or select **Global** to view users from all organizations.

4 Select with whom you want to share the configuration.

- **Everyone in Organization** shares the configuration with all users in the selected organization.
- **Everyone in Workspace** shares the configuration with all users in the selected workspace.
- **Selected Users** shares the configuration with specific users in the selected organization.

  Select the check box next to each user with whom you want to share the configuration.

5 Specify the access rights for the users and click **OK**.

If you share a configuration with users outside of the workspace in which the configuration was created, you can only specify Read access. In addition, configurations created in Global can only be shared with Read access.

6 Click **OK** and **Done**.

Configuration Networking

Before you deploy a configuration, it is helpful to understand how configuration networking works in Lab Manager.

Physical Networks

In Lab Manager, physical networks represent physical networks connected to the vSphere datacenter. These networks exist outside configurations and span configurations. Virtual machines that connect to the same physical network can communicate with each other, even if the virtual machines belong to different configurations.

The physical networks available to a configuration are based on the physical networks assigned to the configuration's organization.

Physical networks are bound to virtual switches (vSwitches) on one or more ESX/ESXi hosts in Lab Manager. You can bind a physical network to a single vSwitch per host, and you can only bind physical networks to vSwitches with physical adapters. The adapter-vSwitch association is made in vCenter, and the user must make the correct association. You can also bind a physical network to a vNetwork Distributed Switch. A vNetwork Distributed Switch functions like a single virtual switch across all associated hosts. This allows virtual machines to maintain consistent network configuration as they migrate across multiple hosts.

When you bind, Lab Manager creates a portgroup on the vSwitch, or a dvPort group on the vNetwork Distributed Switch, names it based on the Lab Manager physical network name, and reports that as the Name in vCenter on the Network Properties page. If the Lab Manager physical network specifies a VLAN ID, Lab Manager sets this on the portgroup or dvPort group. Lab Manager does not use or affect existing portgroups on the vSwitch or vNetwork Distributed Switch.

Fencing Virtual Machines

When you deploy a configuration that includes a physical network, you can choose to isolate the configuration virtual machines from other machines on the network. This prevents IP and MAC address conflicts that could exist if multiple copies of the same machine are deployed at the same time.

Fencing a configuration isolates the virtual machines that are defined to be connected to the physical network from the datacenter network using a virtual router (VR) and bidirectional network address translation (NAT).

Typically, you want to enable network fencing under these circumstances:

- You have a configuration with one or more servers, and you anticipate cloning the configuration numerous times.
- You have a configuration involving a difficult and complex setup, and cloning the configuration is an easier route than repeating the setup.

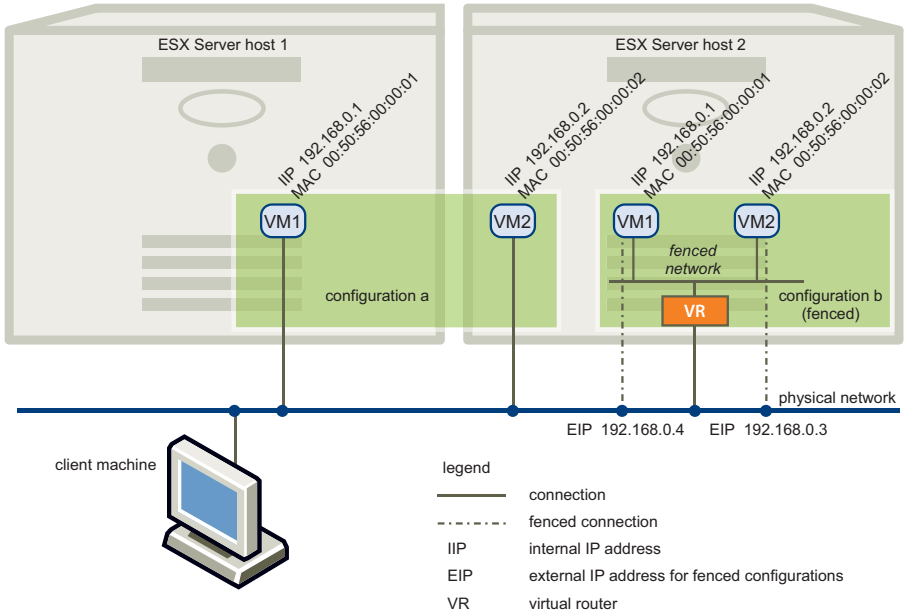
From a performance perspective, network fencing impacts the traffic flow between modules. Fencing requires a slightly higher number of resources on the host, such as memory, CPU, and networking. If you enable fencing but never use it, these resources are not consumed.

Virtual machines in a configuration have preconfigured (internal) IP addresses. When you deploy virtual machines in fenced mode, Lab Manager assigns a unique external IP address to each of these machines. Through these external addresses, virtual machines both inside and outside the fence can communicate with each other. Lab Manager uses a virtual machine called a virtual router (VR) to route packets between these virtual machines. Lab Manager configures the virtual router when you deploy a fenced configuration and deletes it when you undeploy the configuration.

NOTE When you deploy a configuration in fenced mode with the **Block In and Out** option, Lab Manager does not create a virtual router or assign external IP addresses. See "Fencing Connectivity" on page 57.

Figure 7-1 illustrates configurations without fencing and with fencing.

Figure 7-1. Configuration A (Without Fencing) and Configuration B (With Fencing)



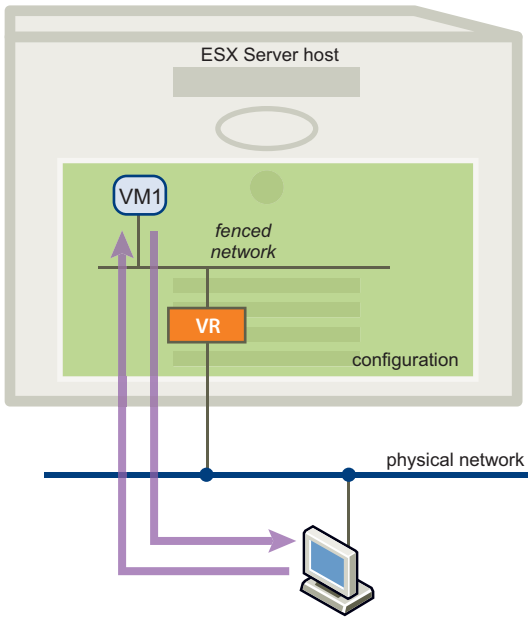
Fencing a configuration does not require any changes to its virtual machines. Within a fenced configuration, virtual machines continue to use preassigned IP addresses to communicate with each other.

Fencing Connectivity

Three connectivity modes are available when you fence a configuration:

- **Allow In and Out** – Virtual machines can communicate with machines outside the fence, and machines outside the fence can communicate with virtual machines inside the fenced configuration.

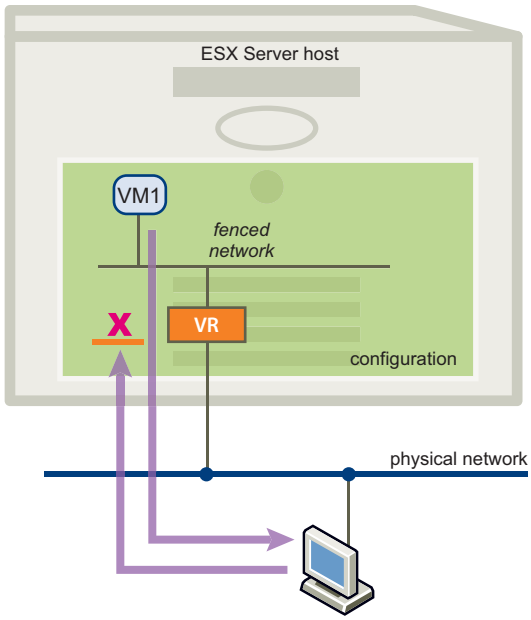
Figure 7-2. Allow In and Out Fencing Mode



- **Allow Out** – Virtual machines in a fenced configuration can initiate communication with machines outside the fence and can receive messages back on the same connection. Machines outside the fence cannot initiate communication to virtual machines inside the fenced configuration.

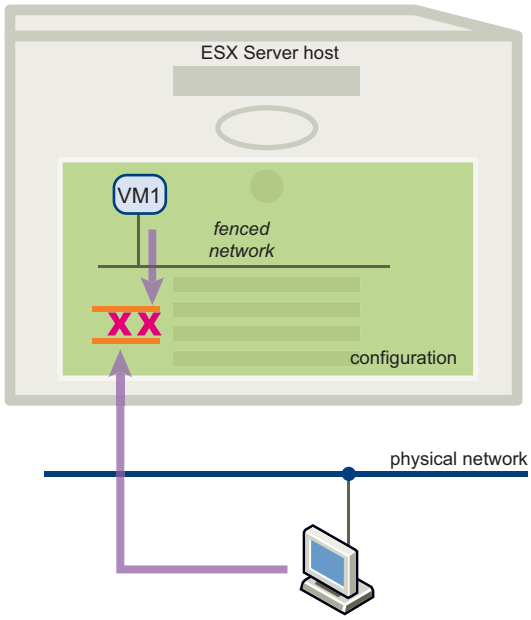
  This option is useful when virtual machines need to obtain data or execute code outside the fence (such as with Web services or databases) but do not want to receive messages that might disrupt testing.

Figure 7-3. Allow Out Fencing Mode



- **Block In and Out** – Network traffic does not travel across the fence. Virtual machines in a fenced configuration cannot communicate with machines outside of the fence, and machines outside the fence cannot communicate with virtual machines in the fenced configuration. When you deploy a fenced configuration with this option, Lab Manager does not create a virtual router or assign external IP addresses.

Figure 7-4. Block In and Out Fencing Mode



The Block In and Out option is useful in these circumstances:

- You are testing software viruses that need to remain isolated from the physical network.
- You are testing a client-server application in isolation.

Virtual Networks

Virtual networks are based on the specifications defined in a network template and get created by Lab Manager when you deploy a configuration. See "Setting Up Network Templates" on page 29 and "Managing Network Templates" on page 123 for more information about network templates.

Virtual networks are configuration local networks. They exist inside configurations and do not span configurations. Virtual machines connected to a virtual network cannot communicate with virtual machines connected to a different virtual network. Each virtual network that Lab Manager creates is unique and isolated from other virtual networks, even if the networks are based on the same network template.

vSwitches and port groups created by Lab Manager for virtual networks are named with the network name concatenated with IDs associated with the network, installation, and host.

Connecting Virtual Networks to Physical Networks

Virtual networks can be connected to physical networks at deploy time. Connecting virtual networks to physical networks provides the virtual machines using those virtual networks access to physical networks.

Lab Manager uses a virtual router to connect the virtual and physical networks.

Virtual to Physical Network Connectivity

Two connectivity modes are available when you connect a virtual network to a physical network:

- **Allow In and Out** – Virtual machines can communicate with machines on the selected physical network, and machines on the selected physical network can communicate with virtual machines inside the configuration.
- **Allow Out** – Virtual machines in the configuration can initiate communication with machines on the selected physical network and can receive messages back on the same connection. Machines on the selected physical network cannot initiate communication with virtual machines inside the configuration.

Host Spanning

Host Spanning is a feature that enables the virtual machines in a configuration that uses fencing or virtual networks to be deployed on different ESX/ESXi hosts. When you deploy a configuration that uses Host Spanning, some of the virtual machines can get deployed to one ESX/ESXi host and some of the virtual machines can get deployed to a different host.

For a configuration that is unfenced and does not include any virtual networks, Lab Manager can always deploy its virtual machines across multiple hosts. For a configuration that is fenced or includes a virtual network, you can enable Host Spanning, provided that the configuration has access to an enabled host spanning transport network.

If you do not enable Host Spanning for a configuration that uses fencing or a virtual network, all of its virtual machines must deploy to the same host. In some cases, this restriction may prevent you from deploying a configuration. For example, for a large configuration, there might not be any single host available that has enough resources to deploy the configuration. In addition, Host Spanning is required in order to support VMware DRS and HA for configurations that use fencing or a virtual network.

Host Spanning Networks

Host spanning networks are logical overlay networks that use the resources of an underlying host spanning transport network to enable Host Spanning. Lab Manager creates a host spanning network when you deploy a configuration with Host Spanning enabled. Host spanning networks are not visible within Lab Manager.

Host Spanning Transport Networks

Host spanning transport networks are Lab Manager resources that enable Host Spanning and consist of a vNetwork Distributed Switch and a LAN or VLAN. Host spanning transport networks require a VMware vSphere Enterprise Plus license and ESX/ESXi 4.0 hosts. If your environment meets these requirements, you can create a vNetwork Distributed Switch, which is a type of vSphere virtual switch that spans multiple ESX/ESXi hosts. Lab Manager creates and uses a virtual machine (VMwareLM-ServiceVM) on each of these hosts to send packets between the hosts using the vNetwork Distributed Switch.

Setting Up a Host Spanning

A configuration that uses fencing or virtual networks must meet the following requirements before you can deploy it across multiple hosts.

- A host spanning transport network exists and is enabled. See "Add a Host Spanning Transport Network" on page 21 and "Enable or Disable a Host Spanning Transport Network" on page 104.
- Host Spanning is enabled for the organization containing the configuration. See "Disable or Enable Host Spanning" on page 103.
- Host Spanning is enabled for at least two ESX/ESXi hosts that are available to the configuration. See "Disable and Enable Host Spanning for a Host" on page 92.

Deploying and Undeploying Configurations

Deploying a configuration registers its virtual machines on ESX/ESXi hosts and provides access to its virtual machine consoles and guest operating systems. You can deploy an entire configuration or individual virtual machines in the configuration. See "Deploy a Virtual Machine" on page 73 for information about deploying an individual virtual machine in a configuration.

You can only deploy workspace configurations. If you want to deploy a library configuration, clone it to a workspace first and then deploy it.

The first time you deploy a configuration, all of its virtual machines with guest customization enabled go through a customization process, which might involve multiple reboots. Do not shut down the virtual machines until the customization is complete.

When you deploy a configuration, you can either provide custom settings or use the default settings.

Deploy a Configuration with Custom Settings

When you deploy a configuration with custom settings, you can specify various deployment options that determine the configuration's network connectivity, deployment lease, resource pool, and so on.

To deploy a configuration with custom settings

1 Move the pointer over the configuration name and select **Deploy**.

If you have already partially deployed the configuration, you can only modify certain settings.

2 Select the **Fence Virtual Machines** check box to deploy the configuration in fenced mode.

This option is only available if the configuration allows fencing and includes a physical network that also allows fencing.

Use the **Connectivity** drop-down menu to select a connectivity mode for each physical network. See "Fencing Connectivity" on page 57 for more information.

3 Select the **Connect Virtual Networks to Physical Networks** check box to connect virtual networks to physical networks.

This option is only available if the configuration includes a virtual network.

Select a physical network to connect to and use the **Connectivity** drop-down menu to select a connectivity mode. See "Virtual to Physical Network Connectivity" on page 59 for more information.

4 Specify the Host Spanning setting.

This option is only available if the configuration's organization includes an enabled host spanning transport network and the configuration uses fencing or a virtual network. For a configuration that is unfenced and does not include any virtual networks, Lab Manager can always deploy its virtual machines across multiple hosts

For network intensive operations, enabling Host Spanning may result in a slight decrease in throughput and a slight increase in latency.

5 Select the **Use Server Boot Sequence** check box to boot the virtual machines in the order specified in the configuration properties.

If you do not select this option, Lab Manager boots the virtual machines all at once.

6 Deselect the **Power On Machines After Deployment** check box to prevent Lab Manager from powering on virtual machines immediately after deployment.

Use this option when you need to manually power on virtual machines. For example, you might need to ensure a database, application, and Web server are working individually rather than all at once.

7 Specify a resource pool on which to deploy the configuration or select **Any Available**.

8 Specify a time to undeploy the configuration.

9 (Optional) Type change summary text that will appear on the configuration's History tab.

10 Click **OK**.

Deploy a Configuration with Default Settings

If you do not need to specify any custom deployment settings, you can deploy a configuration using its default settings. For more information about how the default settings are determined, see "Understanding Default Deployment Settings" on page 61.

To deploy a configuration with default settings

Move the pointer over the configuration name and select **Deploy with defaults**.

If the configuration is already partially deployed, Lab Manager only deploys the configuration's undeployed virtual machines.

Understanding Default Deployment Settings

Table 7-1 provides information about how Lab Manager determines default deployment settings.

Table 7-1. Default Deployment Settings

Setting Name	Setting Value
Fence Virtual Machines	If the configuration or any of its physical networks has a Fenced Only fencing policy, then all physical networks in the configuration are fenced and network connectivity is set to Allow In and Out, unless one of the physical networks requires a different connectivity setting. If the configuration and physical network policies conflict (one is set to Fenced Only and the other is set to Unfenced Only), Lab Manager displays an error and prevents deployment. If both the configuration and physical network properties are set to Allow Fenced or Unfenced, the default is determined by the deployment setting specified in the organization properties.
Connect Virtual Networks to Physical Networks	Not selected.

Table 7-1. Default Deployment Settings (Continued)

Setting Name	Setting Value
Host Spanning	If the configuration does not use fencing or include a virtual network, Lab Manager can always deploy virtual machines across multiple hosts. If the configuration uses fencing or includes a virtual network, the Host Spanning setting comes from the organization properties. An organization must have an enabled host spanning transport network to enable Host Spanning.
User Server Boot Sequence	If the configuration properties specify a boot sequence, this option is selected. Otherwise, it is not selected.
Power on machines after deployment	Selected.
Resource Pool	Set to **Any Available**.
Deployment Lease	Uses the deployment lease set in configuration properties.

Undeploy a Configuration

Undeploying a configuration unregisters its virtual machines from vCenter. When you undeploy a configuration, you can save or discard its state. Saving the memory state helps when debugging memory-specific issues and makes virtual machines in the configuration ready for deployment and use almost instantly.

If all the virtual machines in the configuration are powered off, you cannot save or discard state, because there is no state information to save or discard.

To undeploy a configuration

Move the pointer over the configuration name and select **Undeploy - Save State** or **Undeploy - Discard State**.

Stopping and Starting Configuration Virtual Machines

You can stop workspace configurations from running using the suspend and power off operations. Undeploying a configuration also stops it from running. See "Undeploy a Configuration" on page 62 for more information.

Suspend a Configuration

Suspending a deployed configuration freezes the CPU of the virtual machines, but the virtual machines remain registered with vCenter.

To suspend a configuration

Move the pointer over the deployed configuration name and select **Suspend**.

Resume Operation of a Suspended Configuration

You can reverse a suspended state.

To resume operation of a suspended configuration

Move the pointer over the deployed configuration name and select **Resume**.

Power Off a Configuration

Powering off a deployed configuration turns the virtual machines off. It is the virtual equivalent of powering off physical machines. The virtual machines remain registered with vCenter.

To power off a configuration

Move the pointer over the deployed configuration name and select **Power Off**.

Power On a Configuration

Powering on a deployed configuration powers on the virtual machines in the configuration that are not already powered on. It is the virtual equivalent of powering on physical machines.

To power on a configuration

Move the pointer over the deployed configuration name and select **Power On**.

Reset a Configuration

Resetting a configuration restarts the virtual machines in a configuration and clears the machine states. This operation does not shut down the guest operating systems.

To reset a configuration

Move the pointer over the deployed configuration name and select **Reset**.

Working with Configuration Snapshots

A snapshot, also known as a revert point, captures the state of the virtual machines in a configuration at a specific point in time. You can revert the virtual machines in the configuration to that snapshot at a later time. Lab Manager stores the snapshot persistently with the configuration. If you undeploy a configuration and deploy it, the snapshot remains.

You can only take a snapshot of a configuration if at least one of its virtual machines is deployed. Only one snapshot of each virtual machine in a configuration can exist at a time. Taking a new snapshot replaces the previous one.

See "Working with Virtual Machine Snapshots" on page 77 for information about working with snapshots for a specific virtual machine in a configuration.

Take a Configuration Snapshot

When you take a configuration snapshot, Lab Manager captures the state of the configuration's virtual machines. You can revert the configuration to that snapshot at a later time.

To take a configuration snapshot

Move the pointer over the configuration name and select **Snapshot**.

Lab Manager changes the status of the configuration to Setting the Revert Point while it takes a snapshot of each virtual machine.

Revert to a Configuration Snapshot

When you revert a configuration to a snapshot, all virtual machines in the configuration lose their current state. If you revert to a configuration snapshot, Lab Manager retains the snapshot so that you can revert to it again later.

To revert to a configuration snapshot

Move the pointer over the configuration name and select **Revert**.

Lab Manager changes the status of the configuration to Reverting while it reverts each virtual machine to its snapshot.

Delete a Configuration Snapshot

Configuration snapshots take up space on datastores. You can free up space by deleting snapshots.

To delete snapshots for all virtual machines in a configuration

Move the pointer over the configuration name and select **Delete Revert Point**.

For each virtual machine in the configuration that has a revert point, Lab Manager deletes the snapshot.

Viewing Configuration Virtual Machines, Networks, and History

You can view information about the virtual machines and networks in a library or workspace configuration and view a diagram of how they interact. You can also review a list of the changes that have been made to a configuration.

View Virtual Machines in a Configuration

You can view basic information about each virtual machine in a configuration. You can also add or import virtual machines to the configuration.

To view details about the virtual machines in a configuration

1 Move the pointer over the configuration name and select **Open**.

2 Click the **Virtual Machines** tab.

For each virtual machine in the configuration, Lab Manager displays the following information:

- **Console** – Displays a thumbnail icon of the virtual machine console.
- **VM Name** – Displays the virtual machine name.
- **Status** – Lists the status (deployed or undeployed) of the virtual machine.
- **NIC** – Lists a number for each NIC in the virtual machine. An asterisk (*) indicates a virtual machine's primary NIC.
- **Network** – Lists the network to which each NIC connects.
- **IP Address** – Provides the IP address of each NIC in the virtual machine.
- **External IP** – Provides the external IP address for the virtual machine if it requires one.
- **Template** – Indicates the virtual machine template that the virtual machine is based on.
- **Host** – Indicates the ESX/ESXi host for a deployed virtual machine.

  This column only appears for workspace configurations.
- **Connectivity** – Indicates whether a deployed virtual machine uses fencing or has a virtual network connected to physical network.
- **Messages** – Messages or alerts about vCenter activity that could raise errors in Lab Manager.

View Configuration Networks

You can view basic information about each network in the configuration. You can interact with the networks and add networks to the configuration.

To view details about the networks in a configuration

1 Move the pointer over the configuration name and select **Open**.

2 Click the **Networks** tab.

For each network in the configuration, Lab Manager displays the following information:

- **Configuration Network Name** – Displays the network name.
- **Network Type** – Indicates whether the network is a physical network or a virtual network.
- **Connectivity** – Indicates whether a physical network uses fencing or a virtual network is connected to physical network.
- **VLAN ID** – Displays the network's VLAN ID (if applicable).
- **Gateway** – Displays the IP address for the network gateway.
- **Subnet Mask** – Displays the subnet mask for the network.
- **Primary DNS** – Displays the primary DNS for the network.
- **IP Addressing Mode** – Displays the IP addressing modes available to the network.
- **IP Pool (Free/Total)** – Displays the number of IP addresses currently available and the total number of IP addresses in the network's IP pool.

View a Configuration Diagram

You can view a configuration displays a visual representation of the virtual machines and networks in the configuration. You can see which NICs are connected to which networks and initiate various virtual machine and network operations.

To view a configuration diagram

1 Move the pointer over the configuration name and select **Open**.

2 Click the **Configuration Diagram** tab.

View Configuration History

You can view change summaries for a configuration. Lab Manager records certain configuration operations, such as adding or removing a network and deploying or undeploying the configuration, as change summaries. Other operations, such as cloning, moving, and archiving, allow you to input change summary text. Change summaries can be helpful for tracking and auditing purposes.

To view configuration history

Move the pointer over the configuration name and select **History**.

Add a Note to Configuration History

You can add a note to a configuration to provide users with additional information or to expand upon the change summaries.

To add a note to configuration history

1 Move the pointer over the configuration name and select **Open**.

2 Click the **History** tab.

3 Click **Add Note**.

4 Type the note text and click **OK**.

Lab Manager displays the note text in the Change Summary column.

Modifying Configurations

You can change the virtual machines and networks in a configuration, modify the properties, or change the configuration owner. You can also upgrade the virtual machine version of the virtual machines, discard saved state information, or delete an entire configuration. For library configurations, you can modify properties, change the owner, discard state, and delete.

Adding a Virtual Machine to a Workspace Configuration

You can add more virtual machines to a workspace configuration at any time. You can add a virtual machine based on a template or import a virtual machine from vCenter.

For more information, see:

- "Add a Virtual Machine Based on a Virtual Machine Template" on page 50
- "Add a Virtual Machine from vCenter" on page 51

When you add a virtual machine to an existing configuration, you can provide change summary text that will appear on the configuration's History tab.

Remove a Virtual Machine from a Workspace Configuration

You can only remove undeployed virtual machines.

To remove a virtual machine from a workspace configuration

1 Move the pointer over the configuration name and select **Open**.

2 In the **Virtual Machines** tab, move the pointer over the virtual machine name and select **Delete** from the menu.

3 Click **OK** to confirm the deletion.

Lab Manager records the removal on the configuration's History tab.

Move Virtual Machines Between Workspace Configurations

You can move virtual machines from one configuration to another. A move operation removes the selected virtual machines from the source configuration and adds them to the destination configuration. If you have access to more than one workspace, you can move virtual machines from a configuration in one workspace to a configuration in another workspace.

To move virtual machines to another configuration

1 Move the pointer over the configuration name and select **Move**.

2 Specify the destination workspace, if applicable.

3 Specify the destination.

For a new configuration, type a name and description and specify a storage lease. For an existing configuration, select the configuration.

4 (Optional) Type change summary text that will appear on the configuration's History tab.

5 Specify the virtual machines to move.

If you move all the virtual machines in a configuration, Lab Manager deletes the original configuration by default. Deselect the **Delete Empty Configuration** check box to save the empty configuration.

6 Click **OK**.

Combine Workspace Configurations

You can combine workspace configurations by cloning some or all of a configuration's virtual machines to another configuration. If you have access to more than one workspace, you can combine configurations from different workspaces. You cannot combine configurations from different organizations.

Full Clones and Linked Clones

When you combine configurations, you can consolidate the source configuration's virtual machines during the cloning process to create full clones of the virtual machines. Typically, you should not create full clones, unless you plan to dismantle the storage and move the configuration to a different server, or you need to maximize the performance of specific virtual machines (for example, for certain production-level virtual machines).

A full-clone operation copies all of a virtual machine's delta disks and its base disk and consolidates them into a new base disk. The original base disk remains unchanged. A full-clone operation takes longer than a linked-clone operation. You cannot make a full clone of a deployed configuration.

A linked-clone operation creates a delta disk instead of copying an entire virtual hard disk. This operation addresses virtual machine proliferation by using referential provisioning, a process that involves storing new changes but refers back to a chain of delta disks. For each clone, Lab Manager freezes the original delta disk and creates a new one.

When you create a clone, Lab Manager assigns the same network parameters to the cloned virtual machines. If you deploy the original and cloned configurations at the same time, duplicate IP address errors occur unless you deploy one of the configurations in fenced mode.

To combine workspace configurations

1 Move the pointer over the configuration name and select **Clone**.

2 Specify the destination workspace, if applicable.

3 Select **Existing Configuration** and select a destination configuration.

4 (Optional) Type change summary text that will appear on the History tab of the source and destination configurations.

5 Specify the type of clone.

   If the configuration is deployed, you can only create linked clones.

6 Specify the virtual machines to clone.

   If you are creating full clones, select a datastore.

7 Click **OK**.

Add a Network to a Workspace Configuration

Virtual machines in a configuration can connect to any network in the configuration. If you want to connect a virtual machine NIC to a different network, you must first add the network to the configuration.

A configuration can include a network to which no virtual machines connect.

To add a network to a configuration

1 Move the pointer over the configuration name and select **Open**.

2 Click the **Networks** tab.

   The page displays the networks currently available to virtual machines in the configuration.

3 Click **Add Network**.

4 Select a network.

   The list of networks includes the available physical networks and virtual networks.

5 (Optional) Type change summary text that will appear on the configuration's History tab.

6 Click **OK**.

You can edit the properties of a virtual machine in the configuration to use the new network. See "Modifying Virtual Machine Network Interfaces" on page 83 for more information.

Remove a Network from a Workspace Configuration

You can remove a network from an undeployed configuration to prevent virtual machines in the configuration from using the network. You can only remove a network that is not used by any of the virtual machines in the configuration.

To remove a network from a configuration

1 Move the pointer over the configuration name and select **Open**.

2 Click the **Networks** tab.

The page displays the networks currently available to virtual machines in the configuration.

3 Move the pointer over a configuration network name and select **Remove**.

4 Click **OK** to confirm.

If none of the virtual machines in the configuration connect to the network, the network is removed from the configuration. If the network is being used by any virtual machines, Lab Manager displays an error message stating that the network is in use. You can reassign the NICs of virtual machines to use a different network and try again, or use the **Force Remove** command to remove the network and disconnect the virtual machine NICs that used the network.

Replace a Workspace Configuration Network

You can change the network to which a configuration's virtual machines are connected. For example, if you move or clone a configuration from a development workspace to a production workspace, you could replace a virtual network (used by the virtual machines in the development workspace) with the physical production network.

To replace a configuration network

1 Move the pointer over the configuration name and select **Open**.

2 Click the **Networks** tab.

3 Move the pointer over a configuration network name and select **Replace**.

4 Select a compatible replacement network or create a new virtual network based on the current network.

If you have the necessary rights, you can also create a network template using the specifications of the new virtual network.

5 (Optional) Type change summary text that will appear on the configuration's History tab.

6 Click **OK**.

Modify Configuration Properties

You can modify configuration properties in the workspace or library.

You can also change a configuration's owner. See "Change Ownership of a Configuration" on page 69 for more information.

To edit configuration properties

1 Move the pointer over the configuration name and select **Properties**.

2 Edit any of the following properties:

- Name of the configuration.
- Description of the configuration.
- Whether a captured library configuration is labeled as a Gold Master.
- Deployment lease for workspace configurations.
- Storage lease.
- Fencing policy.
- Description, boot sequence, and boot delay for individual virtual machines in the configuration. For workspace configurations, you can also change the names of individual virtual machines.

3 Click **OK**.

Change Ownership of a Configuration

The owner of a configuration is the user who created, captured, or archived it. If you have sufficient rights, you can change the owner.

To change ownership of a configuration

1 Move the pointer over the configuration name and select **Properties**.

2 Click **Change Owner**.

3 Select an organization and user and click **OK**.

If you assign an owner in an organization other than the one in which the configuration was created, make sure that the new organization has the resources required to deploy the configuration.

4 Click **OK**.

Lab Manager reassigns the configuration to the new owner in the primary workspace of the selected organization.

Upgrade Virtual Hardware in a Configuration

Lab Manager configurations can include version 4 and version 7 virtual machines. If a configuration includes version 4 virtual machines, you can upgrade these virtual machines to version 7. Version 4 virtual machines can run on hosts with ESX 3.5 and above, while version 7 virtual machines require hosts with ESX 4.0 and above.

Before you can upgrade a virtual machine to version 7, you must install the latest version of VMware Tools. See "Install VMware Tools" on page 78 for more information.

When you upgrade virtual hardware, Lab Manager discards state information and deletes any snapshots associated with the virtual machines.

To upgrade configuration virtual hardware, you must first undeploy the configuration.

To upgrade configuration virtual hardware

1 Move the pointer over the configuration name and select **Upgrade Virtual Hardware**.

2 Click **OK**.

Lab Manager deploys the configuration, upgrades the virtual hardware, and undeploys the configuration.

Discard State for a Configuration

When you save the state of a configuration by either using the Undeploy - Save State option or suspending the virtual machines in the configuration, Lab Manager saves information about the processor type of the host on which the virtual machines were deployed. When you redeploy a configuration with saved state, Lab Manager requires an available host with a compatible processor type. If processor incompatibility issues prevent you from deploying a configuration, you can discard the saved state.

This requirement especially affects configurations that use fencing or a virtual network without Host Spanning, since these require that all the virtual machines in the configuration get deployed to the same host. You can enable Host Spanning for these configurations to allow the virtual machines to deploy to different hosts.

You can also discard state to free up storage space.

You can only discard state for undeployed configurations that include at least one virtual machine with saved state. If you add a workspace configuration with saved state to the Library, the library configuration includes the saved state.

To discard state for a configuration

1 Move the pointer over the undeployed configuration name and select **Discard State**.

2 Click **OK**.

Delete a Configuration

You can delete a workspace or library configuration if you no longer need it or to free up disk space on a datastore.

You must undeploy a configuration before you can delete it.

To delete a configuration

1 Move the pointer over the configuration name and select **Delete**.

2 Click **OK** to confirm the deletion.

Using LiveLink

A LiveLink is the HTTPS URL of a library configuration. You can create a LiveLink and email its URL to another Lab Manager user, who can click it to deploy a copy of the configuration exactly as it was when it was saved to the library.

For example, if you are testing software in a workspace configuration and encounter a bug, you can capture the configuration to the library and then create a LiveLink to that configuration.

Create a LiveLink

You can only create LiveLinks for shared library configurations. See "Share a Configuration" on page 55 for more information.

NOTE You cannot create a LiveLink of a configuration that includes any virtual machines using DHCP.

To create a LiveLink to a configuration

1 On the Library page, move the pointer over a configuration name and select **LiveLink**.

Lab Manager displays the LiveLink URL for the library configuration.

2 Click **Copy URL** to copy the URL to your Windows clipboard.

If you are using the Mozilla Firefox browser, the **Copy URL** button might not appear. In this case, copy the URL manually.

3 (Optional) Type a note to the user deploying the configuration in the **Attach a comment** field.

4 Click **OK**.

You can now email the LiveLink URL.

Deploy a LiveLink

If you receive a LiveLink URL, you can deploy a copy of the original configuration to view it.

To deploy a LiveLink

1 Open a LiveLink URL in a browser.

If you are not logged in to the Lab Manager Web console, the login page appears. Type your user name and password.

2 In the Restore vCenter Lab Manager LiveLink page, select a workspace.

3 Click **Deploy** to deploy the configuration in the workspace.

The configuration uses its library configuration name with "LiveLink" prefixed to it. For example, "Oracle Linux Bob" becomes "LiveLink – Oracle Linux Bob (n)," where "n" indicates the number of times the LiveLink has been deployed.

Exporting Configurations

You can export an undeployed workspace or library configuration and all its virtual machine files to vCenter or to an SMB share. When you export a configuration, Lab Manager copies all of its virtual machines to the destination as full clones. The original configuration and all of its virtual machines remain available in Lab Manager.

Exported configurations might require a significant amount of disk space on the destination depending on the size of their consolidated virtual disks.

Export a Configuration to vCenter

You can export a configuration to vCenter if you want to access copies of its virtual machines that are not under Lab Manager control. You cannot import configurations from vCenter, although you can import virtual machines.

To export a configuration to vCenter

1 Move the pointer over the configuration name and select **Export**.

2 Select **vCenter**.

3 Type an export name.

During the export operation, vCenter copies the configuration virtual machines to a folder with the name you specify here.

4 Select a datastore.

5 Click **OK**.

Lab Manager creates consolidated copies of the configuration virtual machines and registers them in vCenter.

Export a Configuration to an SMB Share

You can export a configuration to an SMB share if you want to be able to import a configuration back into Lab Manager at a later time, or if you want to import it into a separate Lab Manager installation.

This operation requires that you have a shared folder with full control permissions at the share and file system level. In addition, this operation requires that the datastore on which the configuration virtual machines reside be connected to an ESX host with an open SMB port. Although Lab Manager opens the port during installation, make sure that the port was not closed after the install. To check the port status, run `esxcfg-firewall -q smbClient` on each host. If the datastore on which the configuration resides is only connected to ESXi hosts, you cannot export to an SMB share.

To export a configuration to an SMB share

1. Move the pointer over the configuration name and select **Export**.
2. Select **SMB File Server**.
3. Type the UNC path of the directory (relative to the Lab Manager server system) where you want your configuration files stored.

   Use English characters for the UNC path. A sample path is `\\10.6.1.246\VMwareLM\ExportConfigs`.
4. Type the user name and password for the export directory, if necessary.
5. Click **OK**.

Lab Manager creates consolidated copies of the configuration virtual machines on the destination.

Working with Virtual Machines

8

Lab Manager configurations consist of virtual machines. A host server can run multiple virtual machines concurrently and isolate each virtual machine in a self-contained environment.

Virtual machines have a guest operating system on which you can install and run any software supported by that operating system.

This chapter discusses how to access and interact with individual virtual machines and virtual machine consoles.

This chapter includes the following topics:

Deploying and Undeploying Virtual Machines

Deploying a virtual machine registers it with vCenter and provides access to Lab Manager operations at the virtual machine console level. Undeploying a virtual machine unregisters it from vCenter.

Deploy a Virtual Machine

When you deploy a virtual machine from a configuration, Lab Manager deploys all physical and virtual networks associated with the configuration using the network connectivity options that you select, regardless of whether the deployed virtual machine is connected to them. These connectivity settings remain in effect when you deploy other virtual machines in the configuration. To modify the settings, you must undeploy and redeploy the virtual machines.

When you a deploy a virtual machine from a configuration that uses fencing or that has a virtual network connected to a physical network, the Lab Manager server requires IP connectivity to the physical network on which the virtual machine is stored.

To deploy a virtual machine

1 Move the pointer over a configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over a virtual machine name and select **Deploy**.

3 Select the **Fence Virtual Machines** check box to deploy the virtual machine in fenced mode and select a connectivity mode:

- **Allow In and Out** – Virtual machines can communicate with machines outside the fence, and machines outside the fence can communicate with virtual machines inside the fenced configuration.
- **Allow Out** – Virtual machines in a fenced configuration can initiate communication with machines outside the fence and can receive messages back on the same connection. Machines outside the fence cannot initiate communication with virtual machines inside the fenced configuration.
- **Block In and Out** – Network traffic does not travel across the fence. Virtual machines in a fenced configuration cannot communicate with machines outside the fence, and machines outside the fence cannot communicate with virtual machines in the fenced configuration.

The check box is only available if the virtual machine has a NIC connected to a physical network that allows fencing.

Fencing isolates the virtual machine from other machines on the network and prevents IP and MAC address conflicts that could exist if multiple copies of the same machine are deployed at the same time.

4 Select the **Connect Virtual Networks to Physical Networks** check box to connect virtual networks to physical networks.

This option is only available if the virtual machine has a NIC connected to a virtual network.

a Select a physical network.

b Select a connectivity mode.

- **Allow In and Out** – Virtual machines can communicate with machines on the selected physical network, and machines on the selected physical network can communicate with virtual machines inside the configuration.
- **Allow Out** – Virtual machines in the configuration can initiate communication with machines on the selected physical network and can receive messages back on the same connection. Machines on the selected physical network cannot initiate communication with virtual machines inside the configuration.

5 Specify the Host Spanning setting.

This option is only available if Host Spanning is enabled and the configuration uses fencing or a virtual network.

6 To boot the virtual machine in the sequence specified during the configuration creation, select the **Use Server Boot Sequence** check box.

7 To prevent Lab Manager from powering on a virtual machine immediately after deployment, deselect the **Power On Machines After Deployment** check box.

Use this option when you need to manually bring up a virtual machine. For example, you might need to ensure a database, application, and Web server are working individually rather than all at once.

8 To recustomize the virtual machine, select the **Force Re-customization** check box.

If customization failed in a previous deploy operation, or if you changed the network settings for a virtual machine in the guest operating system, you might have to force recustomization. See "Customizing the Guest Operating System" on page 40.

9 Specify a resource pool on which to deploy the configuration or select **Any Available**.

10 Specify a time to undeploy the configuration.

11 (Optional) Type change summary text that will appear on the configuration's **History** tab.

12 Click **OK**.

Undeploy a Virtual Machine

When you undeploy a virtual machine, you can save or discard its state. Saving the memory state of virtual machines helps you to debug memory-specific issues and makes virtual machines ready for deployment and use almost instantly.

To undeploy a virtual machine

1 Move the pointer over a configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over the machine name and select **Undeploy - Save State** or **Undeploy - Discard State**.

If the virtual machine is powered off, you can only select **Undeploy** because no state information is available to save or discard.

If an ESX/ESXi host goes offline or someone manually removes a virtual machine from the vCenter inventory, the standard undeploy operation does not work. Move the pointer over the virtual machine name and select **Force Undeploy**.

Accessing Virtual Machine Consoles

From the virtual machine console page, you can view information about a virtual machine, work with the guest operating system, and perform operations that affect the guest operating system. For a configuration that includes multiple virtual machines, you can view a virtual machine's console page or view a page that displays the consoles of all the virtual machines.

View a Virtual Machine Console

You can view the virtual machine console for a deployed virtual machine or virtual machine template from a workspace or from the VM Templates pages. The virtual machine console provides access to the guest operating system that is running on a virtual machine and to operations that affect the guest operating system.

To view a virtual machine console, you must install either the ActiveX control (for Internet Explorer) or the VMware Remote MKS Plugin (for Firefox). If the Active X control or VMware Remote MKS Plugin is not installed, you are prompted to install it the first time that you try to view a virtual machine console.

To view a virtual machine console in a configuration

1 Move the pointer over the configuration name and select **Open**.

2 Move the pointer over the virtual machine name and select **View Console** or **Pop Out Console**.

The virtual machine console page displays the internal and external (if applicable) IP addresses of a virtual machine. If the virtual machine has a revert point, Lab Manager displays a thumbnail icon of the snapshot.

For a configuration that includes multiple virtual machines, the **Configuration** drop-down menu provides access to other virtual machines in the same configuration.

To view the virtual machine console of a virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over the name of a deployed virtual machine template and select **View Console** or **Pop Out Console**.

View All Virtual Machine Consoles

You can view the virtual machine consoles for all virtual machines in a configuration. The consoles page provides access to the guest operating systems that are running on the virtual machines and to operations that affect the guest operating systems.

To view virtual machine consoles, you must install either the ActiveX control (for Internet Explorer) or the VMware Remote MKS Plugin (for Firefox). If the Active X control or VMware Remote MKS Plugin is not installed, you are prompted to install it the first time that you try to view all virtual machine consoles.

To view all virtual machine consoles in a configuration

Move the pointer over the configuration name and select **Show Consoles**.

Lab Manager displays the consoles for all the virtual machines in the configuration.

Stopping and Starting Virtual Machines

You can stop a virtual machine from running by using the suspend, power off, or shut down operations. Undeploying a virtual machine also stops it from running.

Suspend a Virtual Machine

Suspending a deployed virtual machine freezes its CPU. Suspend a machine when you need to step away from a virtual machine but you do not want to lose its current state.

The virtual machine remains registered with vCenter.

To suspend a virtual machine

From the virtual machine console page, move the pointer over the virtual machine name and select **Suspend**.

Resume a Virtual Machine

Use the **Resume** operation to reverse a suspended state.

To resume operation of a suspended virtual machine

From the virtual machine console page, move the pointer over the virtual machine name and select **Resume**.

Power Off a Virtual Machine

Powering off a virtual machine is the equivalent of powering off a physical machine.

To power off a virtual machine

From the virtual machine console page, move the pointer over the virtual machine name and select **Power Off**.

Power On a Virtual Machine

Powering on a virtual machine is the equivalent of powering on a physical machine.

To power on a virtual machine

From the virtual machine console page, move the pointer over the virtual machine name and select **Power On**.

Reset a Virtual Machine

Resetting a virtual machine restarts it and clears the machine state. This operation does not shut down the guest operating system.

If a boot image is not available in peripheral storage, the virtual machine boots off the virtual hard disk.

To reset a virtual machine

1 From the virtual machine console page, move the pointer over the virtual machine name and select **Reset**.

2 Confirm the reset operation.

Shut Down a Virtual Machine

Use the virtual machine console to shut down the guest operating system. This produces the same results as shutting down the operating system from within the guest.

This operation is only available if VMware Tools is installed and the virtual machine is booted. If you cannot see this operation after meeting these conditions, refresh the page.

If the shut down operation is still not available, install the latest version of VMware Tools. See "Install VMware Tools" on page 78 for more information.

To shut down a virtual machine

From the virtual machine console page, move the pointer over the virtual machine name and select **Shut Down**.

Working with Virtual Machine Snapshots

A snapshot, also known as a revert point, captures the state of a virtual machine at a specific point in time. You can revert the virtual machine to that snapshot at a later time. Lab Manager stores the snapshot persistently with the virtual machine. If you undeploy a virtual machine and deploy it, the snapshot remains.

Take a Snapshot of a Virtual Machine

When you take a virtual machine snapshot, Lab Manager captures the state of the virtual machine. You can revert the virtual machine to that snapshot at a later time. You can only take a snapshot of a deployed virtual machine.

Only one snapshot of a virtual machine can exist at a time. Taking a new snapshot replaces the previous one.

To take a virtual machine snapshot

From the virtual machine console page, move the pointer over the virtual machine name and select **Snapshot**.

Lab Manager powers off the virtual machine for a short time and then displays the console. A thumbnail icon of the snapshot appears on the console page.

Revert to a Virtual Machine Snapshot

When you revert a virtual machine to a snapshot, the virtual machine loses its current state. If you revert to a virtual machine snapshot, Lab Manager retains the snapshot so that you can revert to it again later.

To revert to a snapshot

1 From the virtual machine console page, move the pointer over the virtual machine name and select **Revert**.

2 Click **OK** to revert to the last snapshot of the machine and lose the current state of the machine.

Lab Manager turns off the virtual machine for a short time and then displays the console.

Delete a Virtual Machine Snapshot

Virtual machine snapshots take up space on datastores. You can free up space by deleting snapshots.

To delete a snapshot

1 From the virtual machine console window, move the pointer over the virtual machine name and select **Delete Revert Point**.

2 Click **OK** to confirm.

Lab Manager deletes the snapshot and removes its thumbnail icon from the console page.

Managing Virtual Machines

Managing virtual machines involves a number of tasks, including installing VMware Tools, accessing media files, modifying virtual machine properties, and consolidating virtual machines.

Install VMware Tools

Lab Manager uses VMware Tools to customize the guest operating system. VMware Tools also allows you to move the pointer into and out of the virtual machine console window. Without VMware Tools, you can lose the pointer when navigating in and out of the console window.

Installing VMware Tools takes several minutes and requires you to restart the virtual machine.

For more information about the installation, see vSphere documentation.

To install VMware Tools

1 From the virtual machine console page, click in the console to work with the guest operating system.

2 Log in to the guest operating system inside the virtual machine console.

3 Click **Install VMware Tools**.

The rest of the procedure depends on the guest operating system. For more information, see:

- "Install VMware Tools in a Windows Guest" on page 36
- "Install VMware Tools on a Linux Guest Within X with the RPM Installer" on page 37
- "Install VMware Tools on a Linux Guest with the Tar Installer or RPM Installer" on page 37
- "Install VMware Tools on a Solaris Guest" on page 39

Insert and Swap a CD

From the virtual machine console page, you can access CD images from the Lab Manager media library to use in a virtual machine guest operating system. Insert a CD to install operating systems, applications, drivers, and so on in virtual machine guest operating systems.

To insert a CD into a virtual machine

1 From the virtual machine console page, move the pointer over the virtual machine name and select **Insert CD**.

2 Select an ISO file from the Lab Manager media library and click **OK**.

After inserting a CD to a virtual machine, you can eject the CD and insert another with the **Swap CD** command.

To swap CDs in a virtual machine

1 From the virtual machine console page, move the pointer over the virtual machine name and select **Swap CD**.

2 Select an ISO file from the Lab Manager media library and click **OK**.

Eject a CD

After inserting a CD to a virtual machine, you can eject the CD.

To eject a CD from a virtual machine

From the virtual machine console page, move the pointer over the virtual machine name and select **Eject CD**.

Insert and Swap a Floppy Disk

From the virtual machine console page, you can access floppy disk images from the Lab Manager media library to use in a virtual machine guest operating system.Insert a floppy disk to install operating systems, applications, drivers, and so on in a virtual machine guest operating system.

To insert a floppy disk into a virtual machine

1 From the virtual machine console page, move the pointer over the virtual machine name and select **Insert Floppy**.

2 Select a floppy file from the media library and click **OK**.

After inserting a floppy disk to a virtual machine, you can eject the floppy disk and insert another with the **Swap Floppy** command.

To swap floppy disks in a virtual machine

1 From the virtual machine console page, move the pointer over the virtual machine name and select **Swap Floppy**.

2 Select a floppy file from the media library and click **OK**.

Eject a Floppy Disk

After you finish using a floppy disk you can eject it.

To eject a floppy disk from a virtual machine

From the virtual machine console page, move the pointer over the virtual machine name and select **Eject Floppy**.

Create a Remote Desktop Connection File

You can create a Remote Desktop Connection file to connect to a virtual machine from your desktop. The virtual machine must be running a Windows guest operating system and have customization enabled.

Before you create a Remote Desktop Connection file, enable Remote Desktop in the virtual machine guest operating system.

To create a Remote Desktop Connection file

On the virtual machine console page, click **Remote Desktop** and save the Remote Desktop Connection file.

Connect Remotely to a Virtual Machine

After you create a Remote Desktop Connection file for a virtual machine, you can use it to access the virtual machine from outside Lab Manager. The virtual machine must be deployed and powered on and you must have network access and access permission to the virtual machine.

To access a virtual machine using Remote Desktop

1 Double-click the Remote Desktop connection file.

2 Type the user name and password for the guest operating system and click **OK**.

Modify Virtual Machine Properties

For virtual machines in workspace configurations, you can modify many of the virtual machine properties. However, if the virtual machine is deployed, the number of properties you can modify is limited. For virtual machines in library configurations, you can only modify the storage lease. Virtual machine properties originate from the virtual machine template on which the machine is based.

To modify other properties, see "Modifying Virtual Machine Hard Disks" on page 82, "Modifying Virtual Machine Network Interfaces" on page 83, "Enable Memory Hot Add" on page 85, and "Enable Virtual CPU Hot Add" on page 86.

To modify virtual machine properties

1 Move the pointer over the configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over the virtual machine name and select **Properties**.

3 Change any of the following properties.

- **Name** – Can only contain alphanumeric characters (a–z, A–Z, 0–9), hyphens, underscores, or periods. Maximum length is 20 characters.
- **Description** – (Optional) Maximum number of characters is 128.
- **Guest OS** – If you select a 64-bit guest operating system, the datastore must be connected to an ESX/ESXi host that provides the required 64-bit processor for that guest OS. You can proceed without fulfilling this requirement, but you cannot deploy the virtual machine until you attach a host with the correct processor. If you have some but not all 64-bit hosts, Lab Manager limits the number of hosts on which the virtual machine can be deployed.

  For information on enabling a host to provide 64-bit support, see the vSphere documentation.
- **32-bit Virtual CPU** – By default, the virtual CPU type assumes the physical host CPU type.

  Select this check box to override the default behavior and ensure that the virtual CPU type is 32-bit. For example, you might have 64-bit ESX/ESXi hosts that do not have the required software (kernel or drivers) for a Solaris guest operating system. Another example involves a mixed (32-bit and 64-bit) ESX/ESXi host environment where you need to complete a testing process specifically on a 32-bit guest operating system, and the operating system accommodates both 32-bit and 64-bit CPU architecture.

- CPU information:
  - **Number of Virtual CPUs** – Maximum number of processors is four for version 4 virtual machines and eight for version 7 virtual machines. If virtual CPU hot add is supported and enabled, you can add virtual CPUs to a deployed and powered on virtual machine.

    The datastore for a virtual machine must be connected to a host that provides the required SMP technology for the guest operating system. If you select a CPU number not currently compatible with the CPU of the host, you cannot deploy the virtual machine until you attach a host with the appropriate SMP support. If you have some but not all hosts that provide the required SMP technology, Lab Manager limits the number of hosts on which the virtual machine can be deployed.
  - **CPU Reservation (Mhz)** – Minimum amount of CPU set aside for the virtual machine.
  - **CPU Priority** – Priority for shares of CPU.
  - **CPU Shares** – Relative amount of CPU for a virtual machine compared to other virtual machines in the same configuration.
  - **CPU Limit (Mhz)** – Maximum amount of CPU available for the virtual machine.

  See the vSphere documentation for details on CPU priorities, shares, reservations, and limits.
- Memory information:
  - **Memory (MB)** – Amount of RAM allocated for running the virtual machine. If memory hot add is supported and enabled, you can add memory to a deployed and powered on virtual machine.
  - **Memory Reservation (MB)** – Minimum amount of memory set aside for the virtual machine.
  - **Memory Priority** – Priority for shares of memory.
  - **Memory Shares** – Relative amount of memory for a virtual machine compared to other virtual machines in the same configuration.
  - **Memory Limit (MB)** – Maximum amount of memory available for the virtual machine.

  See the vSphere documentation for details on memory priorities, shares, reservations, and limits.
- **Use Time Synchronization** – Enables time synchronization between the guest (virtual machine) and ESX/ESXi host operating systems. You must install VMware Tools to use this option.
- **Perform Customization** – Specifies whether guest customization is enabled.
- **Boot Sequence** – Integer (**0**-**n**) indicating the boot sequence for the virtual machine. You do not need to use sequential numbers. Lab Manager can determine the relative order.
- **Boot Delay** – Delay in seconds between the bootup process of this machine and the next machine.
- **SID mechanism** – Specifies the mechanism Lab Manager uses to change the SID. You can switch the default tool Lab Manager uses to change the SID, or select **None**.

  To use Microsoft Sysprep, you must first create a Microsoft Sysprep package for guest customization. See "Build a Microsoft Sysprep Package" on page 41.
- **Deployment Lease** or **Storage Lease** – Depending on whether the virtual machine is deployed or not, this option allows you to update a time to undeploy the virtual machine or delete the virtual machine (or mark it for deletion).
- **System Messages** – Messages or alerts about vCenter activity that could raise errors in Lab Manager. Click **Clear All** to remove system messages.

4 Click **Update**.

Modifying Virtual Machine Hard Disks

For virtual machines in workspace configurations, you can add hard disks, edit hard disks, and delete hard disks. The type of disks supported depends on the virtual machine version.

Table 8-1. Virtual Machine Versions and Supported Disk Types

Virtual Machine Version	BusLogic Parallel (SCSI)	LSI Logic Parallel (SCSI)	IDE	LSI Logic SAS (SCSI)	Paravirtual (SCSI)
Version 4	X	X			
Version 7	X	X	X	X	X

Add a Virtual Machine Hard Disk

You can add one or more virtual hard disks (`.vhd` files) to an undeployed virtual machine.

To add a virtual hard disk

1 Move the pointer over the configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over the virtual machine name and select **Properties**.

3 In the Hard Disks section, click **Add Hard Disk**.

4 Type the disk size (GB).

5 Select the disk bus type.

6 Select a bus number.

7 Select a bus ID and click **OK**.

8 Click **Update**.

You can now deploy the virtual machine and use the guest operating system tools to partition and format the new disk. If you add a SCSI hard disk to a virtual machine, the guest operating system might generate an error message about missing drivers the next time that you power on the virtual machine. If this error occurs, download and install the appropriate driver, and contact VMware for further support.

Edit a Virtual Machine Hard Disk

You can update the bus number and bus ID of a virtual machine hard disk.

To edit a virtual machine hard disk

1 Move the pointer over the configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over the virtual machine name and select **Properties**.

3 In the Hard Disks section, click **Edit**.

4 Modify the bus number and bus ID and click **OK**.

5 Click **Update**.

Delete a Virtual Machine Hard Disk

You can delete a virtual machine hard disk.

To delete a virtual machine hard disk

1 Move the pointer over the configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over the virtual machine name and select **Properties**.

3 In the Hard Disks section, click **Delete**.

4 Click **OK** and **OK**.

5 Click **Update**.

Modifying Virtual Machine Network Interfaces

For virtual machines in workspace configurations, you can modify network settings, reset a MAC address, add a network interface, and delete a network interface. Virtual machine version 4 supports up to four NICs, and virtual machine version 7 supports up to ten NICs.

Edit Network Interface Settings

You can disconnect a virtual machine NIC, change the network to which a NIC connects, specify a primary NIC, and change the IP addressing mode for a NIC.

To edit network interface settings

1 Move the pointer over the configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over the virtual machine name and select **Properties**.

3 In the Network Interfaces section, change any of the following settings:

- Deselect the **Connected** check box to disconnect a virtual NIC.
- Select a network from the **Network** drop-down menu.

  The available options are based on the networks in the virtual machine template. If you have access to other networks in Lab Manager, you can add them to the configuration and they will appear here. See "Add a Network to a Workspace Configuration" on page 67.
- Specify a primary NIC.

  The primary NIC setting determines the default and only gateway for the virtual machine. The virtual machine can use any NIC to connect to other machines that are directly connected to the same network as the NIC, but it can only use the primary NIC to connect to machines on networks that require a gateway connection.

  Consider this behavior when selecting a primary NIC, especially if you plan to deploy configurations that use fencing or connect virtual networks to physical networks.
- Select an IP addressing mode for the network.

  The available options are based on the IP addressing modes available to the selected network.

  - **Static - IP Pool** pulls static IP addresses from the IP address pool.
  - **DHCP** pulls IP addresses from a DHCP server.

    This option avoids the preparation and specification of an IP address or IP range. However, you cannot use Lab Manager fencing or connect virtual networks to physical networks with DHCP.
  - **Static - Manual** allows you to specify an IP address.
- If you selected **Static - Manual**, type an IP address in the **IP Address** text box.

4 Click **Update**.

Reset a Network Interface MAC Address

You can reset a network interface MAC address for an undeployed virtual machine. You might reset a MAC address if you have a MAC address conflict or if you need to discard saved state quickly and easily.

To reset the MAC address for a network interface

1 Move the pointer over the configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over the virtual machine name and select **Properties**.

3 In the Network Interfaces section, select **Reset** from the **MAC Address** drop-down menu for the network interface that you want to update.

4 Click **Update**.

Add a Network Interface

You can add one or more virtual NICs to an undeployed virtual machine. A virtual machine can have up to four NICs (virtual machine version 4) or ten NICs (for virtual machine version 7).

To add a network interface

1 Move the pointer over the configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over the virtual machine name and select **Properties**.

3 In the Network Interfaces section, click **Add Interface**.

Lab Manager adds and connects a new virtual NIC.

4 (Optional) Edit the virtual NIC settings.

a Deselect the **Connected** check box to disconnect the virtual NIC.

b Select a network from the **Network** drop-down menu.

The available options are based on the networks in the virtual machine template. If you have access to other networks in Lab Manager, you can add them to the configuration and they will appear here. See "Add a Network to a Workspace Configuration" on page 67.

c Specify a primary NIC.

The primary NIC setting determines the default and only gateway for the virtual machine. The virtual machine can use any NIC to connect to other machines that are directly connected to the same network as the NIC, but it can only use the primary NIC to connect to machines on networks that require a gateway connection.

Consider this behavior when selecting a primary NIC, especially if you plan to deploy configurations that use fencing or connect virtual networks to physical networks.

d Select an IP addressing mode for the network.

The available options are based on the IP addressing modes available to the selected network.

- **Static - IP Pool** pulls static IP addresses from the IP address pool.
- **DHCP** pulls IP addresses from a DHCP server.

  This option avoids the preparation and specification of an IP address or IP range. However, you cannot use Lab Manager fencing or connect virtual networks to physical networks with DHCP.
- **Static - Manual** allows you to specify an IP address.

e If you selected **Static - Manual**, type an IP address in the **IP Address** text box.

5 Click **Update**.

Delete a Network Interface

You can delete virtual NICs from an undeployed virtual machine.

To delete a network interface

1 Move the pointer over the configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over the virtual machine name and select **Properties**.

3 In the Network Interfaces section, click **Delete**.

4 Click **Update**.

Upgrade Virtual Machine Version

Lab Manager supports version 4 and version 7 virtual machines. You can upgrade version 4 virtual machines to version 7. Version 4 virtual machines can run on hosts with ESX 3.5 and later, while version 7 virtual machines require hosts with ESX 4.0 and later.

When you upgrade virtual hardware, Lab Manager discards state information and deletes any snapshots associated with the virtual machine.

Before you can upgrade a virtual machine to version 7, you must install the latest version of VMware Tools. To upgrade virtual machine virtual hardware, you must first undeploy the virtual machine.

To upgrade virtual machine virtual hardware

1 Move the pointer over the configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over the virtual machine name and select **Upgrade Virtual Hardware**.

3 Click **OK**.

Lab Manager deploys the virtual machine, upgrades the virtual hardware, and undeploys the virtual machine.

Enable Memory Hot Add

For a version 7 virtual machine running a guest OS that supports it, you can enable memory hot add. This feature allows you to add memory to a deployed and powered on virtual machine.

See "Guest Operating System Support" on page 161 for information about which guest operating systems support memory hot add.

To enable memory hot add

1 Move the pointer over the configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over an undeployed virtual machine name and select **Properties**.

3 Select **Memory Hot Add**.

4 Click **Update**.

Enable Virtual CPU Hot Add

For a version 7 virtual machine running a Guest OS that supports it, you can enable virtual CPU hot add. This allows you to add virtual CPUs to a deployed and powered on virtual machine.

See "Guest Operating System Support" on page 161 for information about which guest OSes support virtual CPU hot add.

To enable virtual CPU hot add

1 Move the pointer over the configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over an undeployed virtual machine name and select **Properties**.

3 Select **Virtual CPU Hot Add**.

4 Click **Update**.

Lab Manager updates the virtual machine properties.

Discard State for a Virtual Machine

When you save the state of a virtual machine, by either using the **Undeploy - Save State** option or suspending the virtual machine, Lab Manager saves information about the processor type of the host on which the virtual machine was deployed. Lab Manager requires an available host with a compatible processor type to redeploy the virtual machine. If processor incompatibility issues prevent you from deploying a virtual machine, you can discard state information for the virtual machine. You can also discard state to free up storage space.

You can only discard state for undeployed virtual machines with saved state.

To discard state for a virtual machine

1 Move the pointer over the configuration name and select **Open**.

2 On the **Virtual Machines** tab, move the pointer over the undeployed machine name and select **Discard State**.

3 Click **OK** to confirm.

Consolidate a Virtual Machine

Each time you create a linked clone of a virtual machine, Lab Manager freezes the virtual hard disk associated with the original virtual machine and creates delta disks to store future changes to the clone and its source. Over time, the increasing number of delta disks stored across the directories of a datastore can affect performance. You do not need to consolidate virtual machines until Lab Manager generates an error requesting this operation.

NOTE You can also use this operation to move a virtual machine to a different datastore.

Consolidating a virtual machine can take an extended period of time, depending on the disk size and storage performance. Consolidation reduces the free space on datastores because the virtual machine no longer benefits from delta disks.

You can consolidate virtual machines in both workspace and library configurations.

To consolidate a virtual machine

1 Move the pointer over the configuration name and select **Open**.

2 If the virtual machine is deployed, undeploy it.

3 On the **Virtual Machines** tab, move the pointer over the virtual machine name and select **Consolidate**.

4 Select a datastore for the consolidated virtual machine and click **OK**.

Working with BEA LiquidVMs

Lab Manager supports importing BEA LiquidVMs as virtual machine templates from vCenter or an SMB file server. See "Importing Virtual Machine Templates" on page 32.

Before you can work with a LiquidVM, you must do the following:

- Make sure that the media library includes all the versions of the WLS-VE ISO that you need. Different versions are available for different versions of LiquidVM. See "Managing Media Stores" on page 100.
- Deploy the LiquidVM, view the console, and use the **Insert CD** command to insert the WLS-VE ISO.

Although you can add multiple NICs to a LiquidVM, Lab Manager only uses the primary NIC.

Managing Resources 9

In vCenter Lab Manager, resources, such as resource pools, hosts, datastores, and media stores, can be dedicated to one organization or shared between organizations.

By default, only system administrators can add, edit, and remove resources. If you are an administrator with rights at the organization level, you can also edit the resources in your organization. If you are an administrator with rights at the workspace level, you can edit the resources in your workspace.

See the VMware vSphere documentation for more information on resource pools, clusters, hosts, and datastores.

This chapter includes the following topics:

Managing Resource Pools

Lab Manager provides access to VMware vCenter resource pools. Resource pools provide the CPU and memory resources for Lab Manager virtual machines.

Enable or Disable a Resource Pool

By default, only system administrators can enable and disable resource pools.

To enable or disable a resource pool

1 In the left pane, click **Resources**.

2 Move the pointer over the resource pool and select **Enable** or **Disable**.

3 Click **OK**.

Lab Manager enables or disables the resource pool.

Modify Resource Pool Properties

By default, only system administrators can modify resource pool properties.

To modify resource pool properties

1 In the left pane, click **Resources**.

2 Move the pointer over the resource pool and select **Properties**.

3 Modify the properties and click **OK**.

Lab Manager modifies the resource pool properties.

Undeploy All Virtual Machines in a Resource Pool

System administrators can undeploy all virtual machines associated with a resource pool to, for example, perform maintenance. Undeploying affects anyone using the virtual machines and can result in partially deployed configurations. You must manually redeploy the undeployed virtual machines. When you select **Undeploy all VMs**, the virtual machines are suspended but their state is saved.

This operation undeploys the virtual machines on all hosts in the resource pool. To undeploy all virtual machines on a specific host, see "Undeploy All Virtual Machines on a Host" on page 93.

To undeploy all virtual machines in a resource pool

1 In the left pane, click **Resources**.

2 Move the pointer over the resource pool and select **Disable**.

3 Click **OK**.

4 Move the pointer over the resource pool and select **Undeploy All VMs**.

For the Global organization, Lab Manager undeploys all the virtual machines deployed on hosts in the resource pool. For other organizations, Lab Manager undeploys only the virtual machines from configurations deployed by users in the selected organization.

5 Click **OK**.

Lab Manager undeploys the virtual machines in the resource pool.

Detach a Resource Pool

Before you can detach a resource pool, you must disable it and undeploy all virtual machines associated with it. See "Enable or Disable a Resource Pool" on page 89 and "Undeploy All Virtual Machines on a Host" on page 93 for more information. By default, only system administrators can detach resource pools.

To detach a resource pool

1 In the left pane, click **Resources**.

2 Click the **Resource Pools** tab.

3 Move the pointer over the resource pool and select **Disable**.

4 Click **OK**.

5 Move the pointer over the resource pool and select **Detach**.

6 Click **OK**.

Lab Manager detaches the resource pool.

Managing Hosts

A host is an ESX/ESXi server that provides CPU and memory resources for Lab Manager virtual machines. You can add vCenter hosts to Lab Manager on the **Resource Pools** tab. See "Attach a Resource Pool" on page 19. You can undeploy, redeploy, and force undeploy all virtual machines on a host. Other operations include disabling and unpreparing hosts, and accessing a host's deployed virtual machines and properties.

Prepare a Host

After attaching unprepared hosts to a resource pool, administrators are prompted to start the Prepare Hosts wizard. You can also start the wizard from the Hosts tab. Unprepared hosts include new hosts that are added to a cluster in vCenter or hosts that are not prepared immediately after you attach a resource pool. This preparation involves such tasks as installing Lab Manager agent on the hosts.

If you are using a DRS cluster, VMware recommends that you prepare all the hosts in the cluster. Otherwise, virtual machines with no NICs, or with NICs connected to the None network, might get migrated to a disabled host.

To prepare a host

1 In the left pane, click **Resources**.

2 On the **Hosts** tab, move the pointer over the host name and select **Prepare**.

3 Select or deselect the check box that specifies whether to use the same user name and password for all hosts.

4 If you selected the check box, type the user name and password.

5 Select the check boxes next to the hosts that you want to prepare.

6 Type user names and passwords, if necessary.

7 Click **Next**.

8 Select the datastores that you want to enable for virtual machine use.

9 Click **Finish**.

Enable and Disable Hosts

When you disable a host, Lab Manager prevents the deployment of new virtual machines on the host. Virtual machines that are already deployed on the host are unaffected. To perform maintenance on a host, you need to undeploy the virtual machines. See "Undeploy All Virtual Machines on a Host" on page 93. To unprepare a host, you must first disable it.

By default, only system administrators can enable and disable hosts.

To enable or disable a host

1 In the left pane, click **Resources**.

2 On the **Hosts** tab, move the pointer over the host and select **Enable** or **Disable**.

3 Click **OK**.

Lab Manager enables or disables the host.

Disable and Enable Host Spanning for a Host

When you add an ESX/ESXi 4.0 host with a vSphere Enterprise Plus license, Lab Manager enables Host Spanning for the host. If you want to use VMware Distributed Power Management, you must disable Host Spanning. By default, only system administrators can disable and enable Host Spanning.

To disable or enable Host Spanning

1 In the left pane, click **Resources**.

2 On the **Hosts** tab, move the pointer over the host name and select **Properties**.

3 Deselect or select the **Enable host for Host Spanning** check box.

See "Managing Host Spanning Transport Networks" on page 103 for more information on removing, disabling, or enabling transport networks.

Unprepare a Host

Unpreparing a host allows you to remove it from the Lab Manager environment. By default, only system administrators can unprepare hosts.

To unprepare a host

1 In the left pane, click **Resources**.

2 In the **Hosts** tab, move the pointer over the host name and select **Unprepare**.

3 Click **Unprepare**.

During this process, Lab Manager tries to uninstall the agent. If this attempt fails, Lab Manager continues to unprepare the host and an error message appears.

Modify Host Properties

By default, only system administrators can modify host properties.

To modify host properties

1 In the left pane, click **Resources**.

2 On the **Hosts** tab, move the pointer over the host and select **Properties**.

3 After you have modified the properties, click **OK**.

Lab Manager updates the host's properties.

NOTE The Maximum Number of VMs field is only available for a cluster without DRS and applies to the machines deployed in this installation. If this option is managed by DRS, you cannot modify it.

The maximum quota for deployed virtual machines on a host can increase in these circumstances:

- A VMotion or VMware HA failover.
- Switching a DRS cluster to a cluster without DRS, where the default quotas associated with the non-DRS cluster can negate the Lab Manager quota.

View Deployed Virtual Machines on a Host

You can view the deployed virtual machines on a specific ESX/ESXi host. To view the deployed virtual machines across all hosts, see "View Deployed Virtual Machines" on page 147.

To view the deployed virtual machines on a host

1 In the left pane, click **Resources**.

2 In the **Hosts** tab, move the pointer over the host and select **Deployed VMs**.

The Deployed Virtual Machines page displays information about the virtual machines from the currently selected organization that are deployed on the selected host. If you select **Global** and **All Deployed Machines**, the page lists all the virtual machines deployed on the host.

Knowing the virtual machine template that serves as the basis of the virtual machine is useful when you plan to retire a virtual machine template and need to evaluate its usage. The **Template** column lists the virtual machine templates used in undeployed virtual machines.

3 In the top left corner, select a view:

- **My Deployed Machines in This Organization**– View your private and shared virtual machines in the selected organization.
- **All Deployed Machines in This Organization**– View your private, shared, and all virtual machines shared by others that are available to you in the selected organization.

  System administrators can select this option in the **Global** organization to view all the virtual machines deployed on the host across the entire Lab Manager installation.
- **Deployed Machines in Other Organizations** – View all your deployed machines in organizations other than the selected organization. This option is not available from the **Global** organization or for users who are members of one organization.

Undeploy All Virtual Machines on a Host

System administrators can undeploy all the virtual machines associated with a host, which is useful when you want to complete maintenance on a host. Undeploying these virtual machines can result in partially deployed configurations, and the undeployed virtual machines must be manually redeployed.

NOTE When you select Undeploy all VMs, the virtual machines are suspended, but their state is saved.

To undeploy all virtual machines on a host

1 In the left pane, click **Resources**.

2 In the **Hosts** tab, move the pointer over the host name and select **Undeploy All VMs**.

In the **Global** organization, Lab Manager undeploys all the virtual machines deployed on the host. For the other organizations, only the virtual machines deployed by users in the selected organization are undeployed.

3 Click **OK**.

Lab Manager undeploys the virtual machines. If the undeploy operation does not work, move the pointer over the host name and select **Force Undeploy**.

Redeploy All Virtual Machines on a Different Host

When you redeploy, you are undeploying the virtual machines from the current host and redeploying them to other available hosts. Before you can redeploy its virtual machines, you need to disable a host.
The organization from which the redeployment is initiated must have access to another host that is CPU compatible with the current host and has the capacity to deploy the virtual machines.

To redeploy all virtual machines on a host

1 In the left pane, click **Resources**.

2 In the **Hosts** tab, move the pointer over the host name and select **Disable**.

3 Click **OK**.

4 Move the pointer over the host name and select **Redeploy All VMs**.

In the **Global** organization, Lab Manager undeploys all the virtual machines deployed on the host. For the other organizations, only virtual machines deployed by users in the selected organization are undeployed.

5 Click **OK**.

Lab Manager redeploys the virtual machines.

NOTE When you select **Redeploy all VMs**, the virtual machines are suspended, but their state is saved.

Repair a Host

If the agent cannot be contacted, if the service VM is powered off, or if a host cannot be enabled or disabled for Host Spanning, you can repair the host.

To repair the host

1 In the left pane, click **Resources**.

2 In the **Hosts** tab, move the pointer over the host name and select **Repair**.

Lab Manager completes the repair and enables Host Spanning. See "Host Spanning" on page 59 for information.

Managing Datastores

Lab Manager supports VMFS and NFS datastores, which it accesses through vCenter. You can add datastores by attaching them to ESX/ESXi hosts in vCenter. VMware recommends shared storage (NFS, iSCSI, or Fiber Channel). If you store virtual machine files on local (not shared) storage, you can only deploy the virtual machines on the local ESX/ESXi host.

Datastores can also be enabled as media stores. See "Managing Media Stores" on page 100.

NOTE There is a limit of eight managed servers (hosts) per LUN. If you exceed this limit, an error message appears. See http://kb.vmware.com/kb/1003319 for more information.

Delete a Datastore

Deleting a datastore removes the datastore from all organizations and deletes all Lab Manager data on that datastore. Only system administrators can delete datastores.

NOTE The operation does not delete files in the actual datastore.

Before you delete a datastore, complete these activities:

- Disconnect the datastore in vCenter.

  For example, if the datastore is connected to three hosts managed by Lab Manager, disconnect the datastore from all three hosts through vCenter.

- Disable the datastore. See "Enable and Disable Datastores" on page 95.

- Make sure that the media files associated with a datastore are not in use.

  If you remove a datastore with media stores and add it back to Lab Manager later, you need to recreate the media stores because the original ones are no longer available.

To delete a datastore

1 In the **Organization** drop-down menu, select **Global**.

2 In the left pane, click **Resources**.

3 On the **Datastores** tab, move the pointer over the datastore and select **Delete**.

4 Click **OK**.

Lab Manager deletes the datastore.

Remove a Datastore

You can only remove a datastore from an organization other than Global. Removing a datastore deletes the datastore as a resource from just that organization. The datastore is available to the other organizations in Lab Manager.

To remove a datastore

1 In the **Organization** drop-down menu, select an organization other than **Global**.

2 In the left pane, click **Resources**.

3 On the **Datastores** tab, move the pointer over the datastore and select **Remove**.

4 Click **OK**.

Enable and Disable Datastores

As the system administrator, you can enable and disable datastores. When you disable a datastore, you cannot deploy the configurations associated with the datastore, create virtual machines on the datastore, or create a media store on the datastore.

To enable or disable a datastore

1 In the left pane, click **Resources**.

2 In the **Datastores** tab, move the pointer over the datastore and select **Enable** or **Disable**.

3 Click **OK**.

Lab Manager enables or disables the datastore.

Disable Virtual Machine Creation in a Datastore

If you do not want to completely disable a datastore, you can disable it for virtual machine creation only. You can still deploy configurations associated with the datastore. When you disable virtual machine creation, you cannot use the datastore to complete these operations:

- Make linked or full clones
- Take snapshots
- Revert snapshots
- Create virtual machine templates or virtual machines
- Add new virtual machines to existing configurations
- Import virtual machines

To disable virtual machine creation in a datastore

1 In the left pane, click **Resources**.

2 In the **Datastores** tab, move the pointer over the resource and select **Disable VM Creation**.

3 Click **OK**.

Lab Manager disables virtual machine creation on the datastore.

Disable Media Store Creation in a Datastore

If you do not want to completely disable a datastore, you can disable it for media store creation only.

To disable media store creation in a datastore

1 In the left pane, click **Resources**.

2 In the **Datastores** tab, move the pointer over the resource and select **Disable Media**.

3 Click **OK**.

Lab Manager disables media store creation in a datastore.

Modify Datastore Properties

By default, only system administrators can modify datastore properties.

To modify datastore properties

1 In the left pane, click **Resources**.

2 On the **Datastores** tab, move the pointer over the datastore and select **Properties**.

3 Change the display name and disk space thresholds.

4 If necessary, clear messages about vCenter activity.

5 Click **OK**.

Datastore properties have been modified.

View Virtual Machine Datastore Usage

By default, system administrators and administrators with rights at the organizational level can monitor disk space usage for all virtual machines and perform maintenance tasks.

NOTE Your configuration files will only be accessible from the same host or datastore as the base template. For example, if you have VM1 on DataStoreX, all the configurations you create from VM1 will be created on DataStoreX. You can copy this virtual machine as the base template to other datastores. See "Add a Virtual Machine Based on a Virtual Machine Template" on page 50 if you want to consolidate the configuration virtual machines on different datastores.

To view virtual machine datastore usage

1 In the left pane, click **Resources**.

2 On the **Datastores** tab, click **View Datastore Usage**.

You can display usage for one datastore by clicking the **Datastores** tab, moving the pointer over the datastore name, and selecting **Open**.

3 Select the organization for which you want to view datastore usage.

Selecting **Global** displays datastore usage for all organizations.

Consider this information when reviewing your datastore usage:

- **Disk Space Freed Upon Deletion (MB)** – Displays the space freed after a virtual machine is deleted. Includes the space occupied by the virtual machine directory and parent directories up to an ancestor that has children or other dependent directories. For more information on virtual machine directories and disk space assessment, see "Understanding Virtual Machine Datastore Directories" on page 98.
- **Chain Length** – Indicates how scattered the virtual machine image is across the datastore directories. Lab Manager displays a message when you need to consolidate a chain.
- **Cleanup Date** – Displays the date that the virtual machine's storage lease expires. Depending on the resource cleanup settings specified by the system administrator, Lab Manager deletes the virtual machine or marks it for deletion. See "Configuring Resource Cleanup Settings" on page 143.

Using the pop-up menu, you can view the high-level topography of the virtual machine directories, consolidate and delete virtual machines, and access virtual machine properties.

View Virtual Machine Datastore Directories

In the Context view, the chain of virtual machine and internal node directories are to the right of the ancestor directories. The boxes with thick borders represent virtual machines that you can see in the Web console. The boxes with lighter borders represent the hidden internal directories associated with the virtual machines. Deletion of internal nodes only occurs as a side effect of deleting the virtual machines associated with those nodes.

To view virtual machine datastore directories

1 In the left pane, click **Resources**.

2 On the **Datastores** tab, click **View Datastore Usage**.

To view the usage on a single datastore, move the pointer over the datastore name and select **Open**.

3 Click **Refresh Disk Space** to ensure that the data is current.

4 Move the pointer over the virtual machine name and select **Context**.

To move data from one datastore to another, you can use SSMove, which is a utility installed on the Lab Manager server. The `SSMove` utility is found in: `C:\Program Files\VMware\VMware Lab Manager Server\Tools\SSMove`. See Appendix D, "Using SSMove," on page 163 for more information.

Understanding Virtual Machine Datastore Directories

When you move the pointer over a datastore name and select **Context**, Lab Manager displays a high-level, tree diagram of the virtual machine's relationship to virtual machines on which it depends (ancestor nodes) and that depend on it (child nodes). Each node in the tree represents a directory location on the datastore. Your configuration files must live on the same datastore as the base. For example, if you have VM1 on DataStoreX, all the configurations you create from VM1 must live on DataStoreX. You can copy this virtual machine as the base template to other datastores.

NOTE If you are using Microsoft Internet Explorer 8, you can only view context diagrams using the Compatibility View. To access this view, in Internet Explorer, select **Tools** > **Compatibility View**.

Lab Manager creates nodes for operations such as linked cloning. When you create a linked clone of a virtual machine, Lab Manager creates a delta disk, rather than copying the entire virtual hard disk. With each linked clone operation, Lab Manager freezes the original delta disk and creates a new one. The virtual machine disk consists of its own delta disk and the delta disks of ancestor disks. This series of disks represents the chain length of a virtual machine.

Deleting a virtual machine deletes the storage occupied by the virtual machine node and ancestor nodes that can be safely deleted.

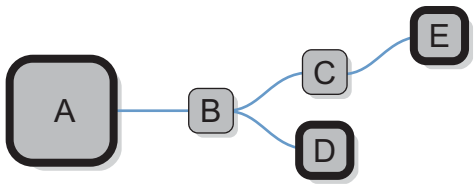
Lab Manager does not delete an ancestor node in the following situations:

- The ancestor directory has other child directories that depend on it.
- A virtual machine (for example, a virtual machine template or virtual machine in the configuration library) is associated with the ancestor node.
- Another node is using the ancestor node as a revert point.

  For example, a full clone operation might consolidate and create a new disk but refer to the revert point of the original chain.

Figure 9-1 shows a basic example of a tree of related virtual machines and the internal nodes affected by a delete operation.

Figure 9-1. Example of Nodes Affected by a Delete Operation



If you delete node D, node B stays intact because node C and E depend on it. If you delete node E, the space for node E and node C becomes available because the deletion affects all nodes up to a directory with child dependencies (node B).

If you move the pointer over a box, details, such as the owner's name, the configuration in which this virtual machine is located, chain length, and the amount of space the virtual machine or internal node consumes, are displayed. Previously deployed and currently deployed virtual machines display information about when they were previously deployed. Internal nodes do not display this information.

A turquoise box indicates a revert reference, which means that another directory (created by a full clone operation on a different datastore) exists outside the displayed directory tree but uses a directory linked to this revert reference as a revert point. To delete a directory linked to a revert reference, you need to delete the virtual machine associated with the revert reference and the descendants of the directory.

Delete Expired Virtual Machines

When the storage lease for a virtual machine expires, Lab Manager deletes the virtual machine or marks it for deletion, depending on the resource cleanup settings. See "Configuring Resource Cleanup Settings" on page 143. You can delete virtual machines that are marked for deletion in the Virtual Machine Datastore Usage page.

By default only a system administrator and an administrator with rights at the organization level can delete expired virtual machines.

To delete expired virtual machines

1 In the left pane, click **Resources**.

2 On the **Datastores** tab, click **View Datastore Usage**.

To view the usage on one datastore, move the pointer over the datastore name and select **Open**.

3 Click **Refresh Disk Space** to ensure that the data is current.

4 Click **Delete Expired VMs**.

Lab Manager deletes all the undeployed virtual machines with an expired storage lease. In the **Global** organization, Lab Manager deletes all the expired virtual machines. For the other organizations, Lab Manager only deletes the expired virtual machines owned by users in the selected organization.

Renew the Storage Lease for an Expired Virtual Machine

When the storage lease for a virtual machine expires, Lab Manager deletes the virtual machine or marks it for deletion, depending on the resource cleanup settings. See "Configuring Resource Cleanup Settings" on page 143.

You can renew the storage lease for virtual machines that are marked for deletion in the Virtual Machine Datastore Usage page. By default, only a system administrator and an administrator with rights at the organization level can review storage leases.

To renew the storage lease for an expired virtual machine

1 In the left pane, click **Resources**.

2 On the **Datastores** tab, click **View Datastore Usage**.

To view the usage on one datastore, move the pointer over the datastore name and select **Open**.

3 Click **Refresh Disk Space** to ensure the data is current.

4 Move the pointer over the expired virtual machine name and select **Renew Storage Lease**.

5 Click **OK**.

Lab Manager renews the storage lease for the selected virtual machine and all other virtual machines in its configuration (if applicable) and updates the **Cleanup Date** column to reflect the new lease expiration date. Expired leases are renewed for the same period as the original lease (for example, 30 days).

Delete Revert Points

Revert points take up space on datastores so deleting them frees up space.

To delete a revert point

1 In the left pane, click **Resources**.

2 On the **Datastores** tab, click **View Datastore Usage**.

To view the usage on one datastore, move the pointer over the datastore name and select **Open**.

The **Revert Point Datastore** lists the datastore on which the revert point is stored.

3 Click **Refresh Disk Space** to ensure that the data is current.

4 Move the pointer over a virtual machine name and select **Delete Revert Point**.

Consolidate a Virtual Machine Based on Datastore Usage

You can consolidate undeployed virtual machines. For information on consolidation, see "Consolidate a Virtual Machine" on page 86.

To consolidate a virtual machine based on datastore usage

1 In the left pane, click **Resources**.

2 On the **Datastores** tab, click **View Datastore Usage**.

To view the usage on one datastore, move the pointer over the datastore name and select **Open**.

3 Move the pointer over the virtual machine name and select **Consolidate**.

4 Select a datastore and click **OK**.

You can keep the consolidated virtual machine in the current datastore or move it to a different datastore.

Delete a Virtual Machine or Configuration Based on Datastore Usage

You can delete an undeployed virtual machine or configuration that contains the virtual machine.

To delete a virtual machine or configuration based on datastore usage

1 In the left pane, click **Resources**.

2 On the **Datastores** tab, click **View Datastore Usage**.

To view the usage on one datastore, move the pointer over the datastore name and select **Open**.

3 Move the pointer over an undeployed virtual machine name and select **Delete** (virtual machine) or **Delete Configuration** (configuration with the virtual machine).

4 Click **OK**.

Lab Manager deletes the machine or configuration.

Managing Media Stores

A media store is an NFS or VMFS datastore that contains a directory for media. Use media stores to store CD, DVD, and floppy images of operating systems and applications that you need to install on Lab Manager virtual machines. You must add media files to media stores outside of the Lab Manager environment and then synchronize the Lab Manager media library with the media stores.

Add Media Stores

To add a media store, you must enable an NFS or VMFS datastore for media. You can use different directories on the same datastore for media and virtual machines. For information on NFS and VMFS datastore requirements, see the *Lab Manager Installation and Upgrade Guide*.

By default, only system administrators can add media stores.

To add a media store

1 Click Resources in the left pane.

2 Select the organization to which you want to add the media store from the **Organization** drop-down menu.

Select **Global** to add the media store as a resource available to all organizations, but assigned to none. You can assign it to organizations later.

3 On the **Datastores** tab, move the pointer over the datastore you want to use as a media store and select **Enable Media**.

4 On the **Media Stores** tab, click **Add Media Store**.

5 Type a name for the media store.

The name can only contain alphanumeric characters (a–z, A–Z, 0–9), hyphens, underscores, or periods.

6 Select the datastore.

7 Type the path to the media.

For NFS datastores, type the path relative to the mount point. For VMFS datastores, type the path relative to the root.

A media store and its NFS datastore cannot have the same NFS path root.

8 Click OK.

9 Move the pointer over the media store name and choose Synchronize from the menu.

Synchronize a Media Store

When you synchronize the contents of a media store with the Lab Manager media library, files are added to or deleted from the library based on the files on the selected media store. To synchronize the Lab Manager media library with all media stores, see "Synchronize the Media Library with Media Store Files" on page 105.

To synchronize media with a media store

1 In the left pane, click **Resources**.

2 On the **Media Stores** tab, move the pointer over the media store name and select **Synchronize**.

Lab Manager synchronizes the media stores.

Enable and Disable a Media Store

By default, system administrators can enable and disable media stores. When you disable a media store, you cannot access the media files stored on the media store. Use the disable operation to block the use of a media store.

To enable or disable a media store

1 In the left pane, click **Resources**.

2 On the **Media Stores** tab, move the pointer over the media store and select **Enable Media Store** or **Disable Media Store**.

3 Click **OK**.

Lab Manager enables or disables the media store.

Change the Name of a Media Store

By default, only system administrators can change the name of a media store.

To change the name of a media store

1 In the left pane, click **Resources**.

2 On the **Media Stores** tab, move the pointer over the media store and select **Properties**.

3 Change the name of the media store and click **OK**.

Managing Physical Networks

To provide virtual machines with access to a physical network, you must first add the network as a resource in Lab Manager, and then assign the resource to one or more organizations.

Monitor IP Pool Usage for a Physical Network

Every virtual machine using a static IP addressing mode for a NIC connected to a physical network requires an IP address from the IP pool of the physical network. This IP address stays with the virtual machine through the various operations in Lab Manager. When you delete all instances of the virtual machine with this IP address, Lab Manager releases the IP address to the IP pool. You can control the length of time Lab Manager reserves released IP addresses before returning them to the IP pool. See "Configuring General Preferences" on page 135.

If a network is running out of IP addresses, you can add more. See "Add or Remove IP Addresses to the IP Pool of a Physical Network" on page 102 for information about adding IP addresses.

When you deploy a configuration in fenced mode (unless you use the **Block In and Out** option), Lab Manager assigns external IP addresses from the physical network IP pool to virtual machines in the configuration. You can, for example, use the external IP address to access a virtual machine from outside a fenced configuration. When you undeploy this configuration, Lab Manager releases the external IP addresses.

For fenced configurations (except those using the **Block In and Out** option), Lab Manager creates a virtual router that requires two IP addresses. The addresses for a virtual router return to the IP pool when you undeploy the configuration.

To monitor an IP Pool

1 In the left pane, click **Resources**.

2 On the **Physical Networks** tab, move the pointer over a physical network name and select **IP Pool**.

The IP Pool page displays the network name, the IP pool, and the number of used and total IP addresses.

The table includes information about IP addresses from the pool that are in use. The **Deallocate In** column indicates the amount of time remaining before an unused external IP address becomes available.

Add or Remove IP Addresses to the IP Pool of a Physical Network

Only system administrators can add IP addresses to a physical network.

To add or remove IP addresses to the IP pool of a physical network

1 In the left pane, click **Resources**.

2 On the **Physical Networks** tab, move the pointer over a physical network name and select **Properties**.

3 Click the **General** tab.

4 Type an IP address or IP address range in the **Static IP Address Pool** text box and click **Add** or select an IP address or IP address range and click **Remove**.

5 Click **Update**.

Modify Physical Network Properties

By default, only system administrators can modify a physical network.

To modify a physical network

1 In the left pane, click **Resources**.

2 On the **Physical Networks** tab, move the pointer over a physical network name and select **Properties**.

3 Click the **General** tab.

4 Edit the network properties and click **Update**.

For information about the properties of a physical network, see "Add a Physical Network" on page 20

Delete a Physical Network

By default, only system administrators can delete a physical network.

To delete a physical network

1 In the left pane, click **Resources**.

2 In the **Physical Networks** tab, move the pointer over a physical network name and select **Delete**.

3 Click **OK**.

Lab Manager deletes the physical network.

Managing Host Spanning Transport Networks

Host spanning transport networks are Lab Manager resources that enable Host Spanning and consist of a vNetwork Distributed Switch and a LAN or VLAN. Host spanning transport networks require a VMware vSphere Enterprise Plus license and ESX/ESXi 4.0 hosts. If your environment meets these requirements, you can create a vNetwork Distributed Switch, which is a type of vSphere virtual switch that spans multiple ESX/ESXi hosts. For more information, see "Host Spanning" on page 59.

View Host Spanning Transport Networks

In the Organization drop-down menu, select an organization to see the transport networks available to that organization. Selecting Global displays all the available host spanning transport networks in Lab Manager.

To view host spanning transport networks

1 In the left pane, click **Resources**.

2 Click the **Host Spanning Transport Network** tab.

Lab Manager displays the available host spanning transport networks in the selected organization. In **Global**, in the **In Use By** column, the number of networks that are using a host spanning transport network is displayed.

Disable or Enable Host Spanning

By default, only system administrators can disable and enable Host Spanning. You can disable and enable Host Spanning for an organization or for the entire installation.

To disable or enable Host Spanning

1 In the left pane, click **Resources**.

2 On the **Host Spanning Transport Networks** tab, deselect or select the **Enable Host Spanning** check box.

3 Click **OK**.

Lab Manager disables or enables Host Spanning for the selected organization. When you disable Host Spanning, currently deployed configurations are unaffected and continue to use Host Spanning until you undeploy or redeploy them.

Enable or Disable a Host Spanning Transport Network

Only system administrators can disable or enable host spanning transport networks. When you disable or enable a transport network, the change affects all organizations that use the network.

To enable or disable a host spanning transport network

1 In the left pane, click **Resources**.

2 On the **Host Spanning Transport Networks** tab, move the pointer over the network name and select **Enable** or **Disable**.

3 Click **OK**.

Lab Manager enables or disables the host spanning transport network.

Remove a Host Spanning Transport Network

Only system administrators can remove a host spanning transport network. You can remove a host spanning transport network from an organization or from the entire installation. You cannot remove a transport network from Global if the network is enabled or in use by any deployed configurations.

To remove a host spanning transport network

1 In the left pane, click **Resources**.

2 On the **Host Spanning Transport Networks** tab, move the pointer over the network name and select **Remove**.

3 Click **OK**.

Modify Host Spanning Transport Network Properties

Only a system administrator can modify transport network properties.

To modify transport network properties

1 In the left pane, click **Resources**.

2 On the **Host Spanning Transport Networks** tab, move the pointer over the transport network name and select **Properties**.

3 Modify the properties.

- Select a vNetwork Distributed Switch.
- Type a VLAN identifier.
- Select the check box to enable the network for Host Spanning.
- Update the maximum transmission unit (MTU).

  MTU is the maximum amount of data (packet size) that can be transmitted in one packet before it has to be split into smaller packets.
- Select the check box to and type a display name for the transport network in Lab Manager.

4 Click **OK**.

Lab Manager modifies the transport network's properties.

10 Managing the Media Library

The media library enables you to store media image files. You can upload data, such as the drivers, to a virtual machine template or virtual machine from the media library.

During the CD and floppy operations available from the individual console of a virtual machine template or virtual machine, you can access the image files in the media library.

This chapter includes these topics:

Synchronize the Media Library with Media Store Files

You can synchronize the contents of the Lab Manager media library with the contents of the media store directories on all your datastores. Synchronizing adds files to or deletes files from the library. When you synchronize the media library, you become the owner of the added media. See "Synchronize a Media Store" on page 101 to synchronize the contents of a media store with the Lab Manager media library.

Media files have the following requirements:

- CD and DVD files must end with `.iso`.
- Floppy disk files must end with `.img`, `.vfd`, or `.flp`.

To synchronize the media library with media store content

1 Select the organization that contains the media stores you want to synchronize.

   Select **Global** to synchronize all media stores.

2 Click **Synchronize Media** and click **OK**.

Lab Manager synchronizes the media library with media store content.

Change Ownership of Media Files

The original owner of a media file is the user who added it to the media library. If you have sufficient rights, you can change the owner.

To change ownership of a media file

1 In the left pane, click **Media**.

2 Move the pointer over the media file name and select **Properties**.

3 Click **Change Owner**.

4 Select an organization and user and click **OK**.

5 Click **OK**.

Lab Manager reassigns the media file to the new owner.

Restrict Access to Media Files

When you add media files to the Lab Manager media library, the files are shared with all Lab Manager users in all organizations. If you are the owner of a media file, or if your user role includes the Administrator View and Control right, you can limit access to a media file by modifying its sharing properties.

Depending on your rights, you can restrict access to users in a specific workspace or organization.

When you share a media file, you can specify access rights for the users with whom you are sharing the media. Access rights combine with the rights provided by a user's role to determine how that user can interact with the shared media file. Access rights cannot provide users with rights that they do not already have based on their role.

NOTE Users can only access media that resides on media stores that are available to their organization and workspace.

To modify media sharing properties

1 In the left pane, click **Media**.

2 Move the pointer over the media name and select **Sharing**.

The Sharing Media dialog box displays the users and organizations that currently have access to the media and their level of access control.

3 Click **Remove** to stop sharing the media with a user or group.

4 Click **Add Users** to share the media with a user or group.

5 Select the organization containing the users with whom you want to share the media or select **Global** to view users from all organizations.

6 Select with whom you want to share the media.

- **Everyone in Organization** shares the media with all users in the selected organization.
- **Everyone in Workspace** shares the media with all users in the selected workspace.
- **Selected Users** shares the media with specific users in the selected organization.

  Select the check box next to each user with whom you want to share the media.

7 Specify the access rights for the users and click **OK**.

8 Click **OK** and **Done**.

Modify Media Properties

You can change the display name and add comments for media files in the properties information. You can also change the media file owner. See "Change Ownership of Media Files" on page 106.

To modify media properties

1 In the left pane, click **Media**.

2 Move the pointer over a media filename and select **Properties**.

3 Change the display name for the media file.

4 Type your comments about the media file.

5 Click **OK**.

Lab Manager modifies the properties of the media file.

Managing Users, Groups, and Roles 11

By default, a system administrator or an administrator with rights at the organization level can add users or groups to an organization and assign each user or group a role in the organization. The organization determines which resources (resource pools, hosts, datastores, media stores, host spanning transport networks, and physical networks) a user can access, and the role determines how a user can interact with those resources.

Users cannot log in to the Lab Manager system or access any resources until they are added to an organization.

This chapter includes the following topics:

Managing Users

By default, only a system administrator or an administrator with rights at the organization level can manage users.

Disable or Enable Users

By default, only the system administrator can disable and enable users in the **Global** organization. When you disable users, they are logged out of the Web console and cannot log in until they are enabled.

To disable or enable a user

1 In the left pane, select **Users and Groups**.

2 In the **Organization** drop-down menu, select **Global**.

3 Click the **Users** tab.

4 Move the pointer over the user name and select **Disable** or **Enable**.

5 Click **OK**.

Lab Manager disables or enables the user.

Remove a User from an Organization

By default, a system administrators and administrators with rights at the organization level can remove a user from an organization. When you remove a user from an organization, they become stranded. See "Managing Stranded Users" on page 111.

To remove a user from an organization

1 In the left pane, select **Users and Groups**.

2 Select the organization from which you want to delete the user.

3 Click the **Users** tab.

4 Move the pointer over the user name and select **Remove**.

5 Click OK.

Lab Manager removes the user from the organization.

Delete a User from Lab Manager

When system administrators delete a user from the entire installation, Lab Manager removes the user from all organizations, deletes all the private objects (for example, media, undeployed configurations, and virtual machine templates) of the user, and reassigns the shared objects to the system administrator who is currently logged in.

To delete a user from Lab Manager

1 In the left pane, select **Users and Groups**.

2 Select **Global**.

3 Click the **Users** tab.

4 Move the pointer over the user name and select **Disable**.

5 Click **OK**.

6 Move the pointer over the user name and select **Delete**.

7 Click **OK**.

Lab Manager deletes the user from the entire installation.

Modify User Properties

By default, only system administrators and administrators with rights at the organization level can modify user properties. For LDAP users, you can only modify the user's role, stored virtual machine template and library configuration quota, and deployed virtual machine template quota. Because these properties are specific to an organization, a user who is a member of two organizations can have a different role or quota in each organization.

To modify user properties

1 In the left pane, select **Users and Groups**.

2 Select the organization for which you want to modify the user properties.

Select **Global** to modify the user properties for all organizations.

3 Click the **Users** tab.

4 Move the pointer over the user name and select **Properties**.

5 Modify the user properties.

All members of an LDAP group inherit the role assigned to the group. You can deselect the **Use Group roles instead of user role** check box and select a role from the drop-down menu to override this rule.

6 Click **OK**.

Lab Manager changes the user's properties.

View User Roles and Organizations

You can display a list of the organizations to which a user belongs and the user's role in each organization. A user who is a member of multiple organizations can have different roles in each organization.

To display the roles and organizations

1 In the left pane, select **Users and Groups**.

2 Click the **Users** tab.

3 Move the pointer over the user name and select **Properties**.

Send User Notifications

You can send an email notification to all the users in a workspace, organization, or the entire installation. You can also send an email to users with deployed virtual machines in a specific resource pool or with virtual machines stored on a specific datastore.

Before you can send an email notification, you need to verify your SMTP settings in the Web console. See "Set Email Preferences" on page 137.

To send an email notification

1 In the left pane, select **Users and Groups**.

2 Click the **Users** tab.

3 In the **Organization** drop-down menu, select an organization.

Select **Global** if you want to send an email to users with deployed virtual machines in a specific resource pool or with virtual machines stored on a specific datastore.

4 Click **Send Notification**.

5 Select the recipients.

6 Type the subject and message and click **Send**.

Lab Manager sends an email notification.

Managing Stranded Users

When a user who owns objects (such as virtual machine templates, configurations, or media) is removed from an organization, the user is stranded. When you disable an organization, all its users are stranded. All the Lab Manager objects (media, virtual machine templates, and so on) owned by a stranded user are saved. A system administrator or administrator with rights at the organization level can assign these objects a new owner. You must reassign ownership of a stranded user's objects before you can delete the user.

Reassign Ownership of All Stranded Users' Objects

You can reassign the objects for all stranded users in an organization.

To reassign the objects of all stranded users

1 In the left pane, select **Users and Groups**.

2 Select the **Stranded Users** tab.

3 Click **Assign All To Me.**

4 Click **Delete All Empty Users** to delete users with no objects.

Reassign Ownership of a Stranded User's Objects

When you disable an organization, all its users are stranded. You can reassign the objects for a stranded user in an organization.

To reassign the objects of a specific stranded user

1 In the left pane, select **Users and Groups**.

2 Select the **Stranded Users** tab.

3 Move the pointer over the user name and select **Assign Resources To Me**.

4 Move the pointer over the user name and select **Delete**.

Managing Groups

Groups and their users are defined in the LDAP. Lab Manager synchronizes with the specified LDAP server to make sure it is up to date on the current users and groups. Lab Manager does not support non-LDAP groups.

Remove a Group from an Organization

When you remove a group from an organization, other than Global, the group is still available to the other organizations. Removing groups can result in stranded users. See "Managing Stranded Users" on page 111.

To remove a group

1 In the left pane, select **Users and Groups**.

2 Select the **Groups** tab.

3 In the **Organization** drop-down menu, select the organization from which you want to remove the group.

4 Move the pointer over the group name and select **Remove**.

5 Click **OK**.

Lab Manager removes the group from the organization.

Delete a Group from Lab Manager

By default, only a system administrator can delete a group from Lab Manager. When you delete a group from Global, the group is no longer available in Lab Manager.

To delete a group from Lab Manager

1 In the left pane, select **Users and Groups**.

2 Select the **Groups** tab.

3 In the **Organization** drop-down menu, select **Global**.

4 Move the pointer over the group name and select **Delete**.

5 Click **OK**.

Lab Manager deletes the group from the entire installation.

Modify Group Properties

By default, only system administrators and administrators with rights at the organization level can modify group properties.

To modify group properties

1 In the left pane, select **Users and Groups**.

2 Select the **Groups** tab.

3 Select the organization for which you want to edit the group properties.

4 Move the pointer over the group name and select **Properties**.

5 Change the group description and role.

If you are editing a group in the **Global** organization, you can only select **No Role** or **Administrator**.

6 Click **OK**.

Lab Manager changes the group properties.

Managing Roles and Rights

When a user or group is assigned to an organization, each is assigned a role in that organization. A user can have different roles in different organizations.

Lab Manager includes the following predefined roles:

- **System Administrator** – Includes all rights across Lab Manager. System administrators can access all organizations and perform all operations. They are the only users who can access the **Global** organization. This is the only role that cannot be modified.
- **Administrator** – Can do almost anything in an organization or a workspace, except add or delete organization resources (datastores, media stores, resource pools, or physical networks). A user can be an administrator at the organization or workspace level.
- **Template Creator** – Can create virtual machine templates, network templates, and configurations in an organization.
- **Application Owner** – Can create configurations in an organization.
- **User** – Can deploy and edit configurations in an organization and check out and view LiveLink Library configurations.
- **View Only** – Can only display workspace configurations.

See Appendix A, "Roles and Rights," on page 149 for more information about the rights assigned to predefined roles. System administrators can create new roles or modify existing roles.

Add a Role

By default, only system administrators can add new roles. You can also create a new role by copying an existing one. See "Copy a Role" on page 114.

To add a role

1 In the left pane, select **Roles and Rights**.

2 Click **New Role**.

3 Type a name.

4 (Optional) Type a description.

5 Expand the check boxes and select the rights that you want to include.

See Appendix A, "Roles and Rights," on page 149 for more information.

6 Click **OK**.

Lab Manager adds the role to the Roles and Rights page. You can now assign it to users and groups.

Copy a Role

You can copy any existing role, except **System Administrator**, to use as the basis for a new role.

To copy a role

1 In the left pane, select **Roles and Rights**.

2 Move the pointer over a role name and click **Copy**.

3 Type a name.

4 (Optional) Type a description.

5 Expand the check boxes and select and deselect the rights you want to include.

See Appendix A, "Roles and Rights," on page 149 for more information.

6 Click **OK**.

Lab Manager copies the role to the Roles and Rights page. You can now assign it to users and groups.

Delete a Role

By default, only system administrators can delete a role. You cannot delete the system administrator role or a role that is currently being used.

To delete a role

1 In the left pane, select **Roles and Rights**.

2 Move the pointer over the role name and select **Delete**.

3 Click **OK**.

Lab Manager deletes the role.

Modify Role Properties

Only system administrators can change the name, description, or rights of a role. The system administrator cannot be modified.

To modify role properties

1 In the left pane, select **Roles and Rights**.

2 Move the pointer over the role name and select **Properties**.

3 Change the name, description, or rights and click **OK**.

Lab Manager modifies the role properties.

Managing Organizations and Workspaces

12

The majority of Lab Manager operations occur in organizations and workspaces.

Organizations can have workspaces that represent different business units or different functional groups. An administrator with rights at the organization level manages a variety of operations in an organization. See "Roles and Rights" on page 149 for more information on these roles and their rights.

A workspace consists of one or more configurations and users, groups, and resource pools that belong to that workspace. Administrators with rights at the workspace level can create, delete, edit, or add a virtual machine; deploy or undeploy fenced (and unfenced) machines; and add or remove resource pools. See "Setting Up Organizations and Workspaces" on page 27 for more information on creating a workspace.

This chapter includes the following topics:

Modifying Organization Properties

By default, system administrators can modify the properties of all organizations. As an administrator with rights at the organizational level, you can edit properties of the organizations of which you are the administrator.

Modify Default User Preferences

You can set the default use preferences for all users in an organization.

To set default user preferences

1 In the left pane, click **Organizations**.

2 Move the pointer over an organization name and select **Properties**.

3 Type a default quota for the number of stored virtual machine templates and library configurations.

4 Type a default quota for the number of deployed virtual machine templates.

5 Click **OK**.

Modify Default Deployment Settings

You can set the default deployment settings for all the configurations in an organization.

To set default deployment settings

1 In the left pane, click **Organizations**.

2 Move the pointer over an organization name and select **Properties**.

3 Select the default fencing setting.

4 Select the default Host Spanning setting.

5 Click **OK**.

Modify the Users and Groups in an Organization

The Add Members page displays the users and groups that are members of the organization and their roles. You can add and remove members or groups and change their roles.

Add Members or Groups to an Organization

By default, only the system administrator and an administrator with rights at the organizational level can add users or groups.

To add members or groups to an organization

1 In the left pane, click **Organizations**.

2 Move the pointer over an organization and select **Users and Groups**.

3 Click **Import Members**.

4 In the **Look for** drop-down menu, select a search option.

5 Type your search terms and click **Search**.

6 Select the check box for the users or groups that you want to add.

7 Click **Add** and **OK**.

8 Select a role for each user or group and click **OK**.

Lab Manager adds the specified users or groups to an organization.

Remove Members or Groups from an Organization

By default, only a system administrator and an administrator with rights at the organization level can delete users or groups.

To remove members or groups from an organization

1 In the left pane, click **Organizations**.

2 Move the pointer over an organization and select **Users and Groups**.

3 Click **Remove** next to the users or groups that you want to remove from the organization.

4 Click **OK**.

Lab Manager removes the user or group from the organization.

Add or Remove the Resource Pools in an Organization

By default, only a system administrator can add or remove resource pools. For example, if an organization is running out of CPU and memory resources to deploy virtual machines, you can add a resource pool.

To add or remove resource pools in an organization

1 In the left pane, click **Organizations**.

2 Move the pointer over the organization name and select **Properties**.

3 In the **Resources Pools** panel, click **Edit**.

4 Select a resource pool and click the relevant arrow to add it to or remove it from the organization.

5 Click **OK** and **OK**.

Lab Manager modifies the resource pools available to the organization.

Add or Remove the Datastores in an Organization

By default, only a system administrator can add or remove datastores.

To add or remove datastores in an organization

1 In the left pane, click **Organizations**.

2 Move the pointer over an organization and select **Properties**.

3 In the **Datastores** panel, click **Edit**.

4 Select a datastore and click an arrow to add it to or remove it from the organization.

5 Click **OK** and **OK**.

Lab Manager modifies the datastores available to an organization.

Add or Remove the Media Stores in an Organization

By default, only a system administrator can add or remove media stores.

To add or remove media stores in an organization

1 In the left pane, click **Organizations**.

2 Move the pointer over an organization and select **Properties**.

3 In the **Media Stores** panel, click **Edit**.

4 Select a media store and click an arrow to add it to or remove it from the organization.

5 Click **OK** and **OK**.

Lab Manager modifies the media stores available to the organization.

Add or Remove the Physical Networks in an Organization

By default, only a system administrator can add or remove physical networks.

To add or remove a physical network to an organization

1 In the left pane, click **Organizations**.

2 Move the pointer over an organization and select **Properties**.

3 In the **Physical Networks** panel, click **Edit**.

4 Select a physical network and click an arrow to add it to or remove it from the organization.

5 Click **OK** and **OK**.

Lab Manager modifies the physical networks available to the organization.

Add or Remove a Host Spanning Transport Network in an Organization

By default, only system administrators can add or remove the host spanning transport networks to an organization.

To add or remove a host spanning transport network

1 In the left pane, click **Organizations**.

2 Move the pointer over an organization and select **Properties**.

3 In the **Host Spanning Transport Networks** panel, click **Edit**.

4 Select a host spanning transport network and click an arrow to add it to or remove it from the organization.

5 Click **OK** and **OK**.

Lab Manager modifies the host spanning transport networks available to the organization.

Enable or Disable an Organization

By default, only system administrators can enable or disable organizations. When you disable an organization, all of its users become stranded. See "Managing Stranded Users" on page 111.

To enable or disable an organization

1 In the left pane, click **Organizations**.

2 Move the pointer over an organization name and select **Enable** or **Disable**.

3 Click **OK**.

Lab Manager enables or disables the organization.

Delete an Organization

By default, only system administrators can delete an organization. Before you can delete an organization, you must disable it and reassign the objects owned by any stranded users. See "Managing Stranded Users" on page 111.

To delete an organization

1 In the left pane, click **Organizations**.

2 In the **Organization** drop-down menu, select **Global**.

3 Move the pointer over the organization name and select **Disable** and click **OK**.

4 In the left pane, click **Users and Groups**.

5 On the **Stranded Users** tab, reassign the relevant objects.

6 In the left pane, click **Organizations**.

7 Move the pointer over the organization name and select **Delete**.

8 Click **OK**.

Lab Manager deletes the organization.

Using the Primary Workspace

All organizations have a primary workspace. When you add users and groups to the organization, Lab Manager automatically adds the users and groups to the primary workspace. You can manually add them to other workspaces. When you add a resource pool to an organization, Lab Manager automatically adds the resource pool and its associated resources to the primary workspace. You can manually add the resource pool to other workspaces.

Initially, the primary workspace in each organization is **Main**, but you can select a different primary workspace. Each organization can have either one primary workspace or no primary workspace.

Delete the Primary Workspace

You can delete the primary workspace if you do not want Lab Manager to automatically add users, groups, and resource pools to a workspace in the organization.

To delete the primary workspace

1 In the left pane, select an organization.

2 Select **Workspace(s)**.

3 Move the pointer over the primary workspace and select **Delete**.

4 Click **OK**.

Lab Manager deletes the primary workspace and sets the primary workspace for the organization to **None**. You can select an existing workspace to be the new primary workspace; otherwise, the next workspace that you create is set as the new primary workspace.

Set the Primary Workspace for an Organization

In the Organization Properties page, you can select a workspace to be the primary workspace.

To set another workspace as the primary workspace

1 In the left pane, select **Organizations**.

2 Move the pointer over the organization name and select **Properties**.

3 In the **Primary Workspace** drop-down menu, select a workspace.

Lab Manager sets this workspace as the primary workspace. When you add users, groups, and resource pools to this organization, they are added to the primary workspace. If you select **None**, the organization has no primary workspace, so you must add users, groups, and resource pools to each workspace.

Modify Workspace Properties

By default, only system administrators and administrators with rights at the organization level can edit workspaces.

To edit workspace properties

1 In the left pane, click **Workspace(s)**.

2 Move the pointer over the workspace name and select **Properties**.

3 Modify the properties.

4 Click OK.

Modifying Users and Groups in a Workspace

You can modify the users and groups who can access a workspace.

Add Users and Groups to a Workspace

By default, system administrators and administrators with rights at the organization and workspace levels can add users and groups to a workspace.

To add users and groups to a workspace

1 In the left pane, select **Workspace(s).**

2 Move the pointer over a workspace name and select **Properties**.

3 In the **Users and Groups** panel, click **Edit**.

4 Click **Add Users and Groups**.

5 In the **Look** for drop-down menu, select one of the options.

6 Type your search term and click **Search**.

7 Select the check boxes for the users or groups that you want to add and click **Add**.

8 Click **OK**.

9 Select a role for the user.

10 Click **OK** and **OK**.

Lab Manager adds the specified users or groups to the workspace.

Remove Users and Groups from a Workspace

By default, system administrators and administrators with rights at the organization and workspace levels can remove users and groups from a workspace.

To remove users and groups from a workspace

1 In the left pane, select **Workspace(s)**.

2 Move the pointer over a workspace name and select **Properties**.

3 In the **Users and Groups** panel, Click **Edit**.

4 Click **Remove** next to the user or group that you want to delete.

You cannot remove the system administrator role.

5 Click **OK** and **OK**.

Lab Manager removes the selected users or groups.

Add or Remove the Resource Pools Available to a Workspace

By default, only system administrators and adminstrators with rights at the organization level can add or remove resource pools.

To add or remove the resource pools available to a workspace

1 In the left pane, click **Workspace(s)**.

2 Move the pointer over the organization name and select **Properties**.

3 In the **Resource Pools** panel, click **Edit**.

4 Select a resource pool and click an arrow to add or remove it from the workspace.

5 Click **OK** and **OK**.

Lab Manager modifies the resource pools available to the workspace.

Disable a Workspace

By default, only system administrators can enable or disable workspaces. When you disable a workspace, all of its users become stranded. See "Managing Stranded Users" on page 111 for more information.

To disable a workspace

1 In the left pane, click **Workspace(s)**.

2 Move the pointer over the workspace name and select **Disable**.

3 Click **OK**.

Lab Manager disables the workspace from the organization. You can now reassign stranded users and objects and delete a workspace.

Delete a Workspace

By default, only system administrators and administrators with rights at the organization level can delete workspaces. Before you can delete an workspace, you must disable it and reassign the objects owned by any stranded users.

To delete a workspace

1 In the left pane, click **Workspace(s)**.

2 Move the pointer over the workspace name and select **Disable**.

3 Click **Delete** and **OK**.

Lab Manager deletes the workspace from the organization.

Managing Network Templates 13

System administrators, administrators with rights at the organization and workspace levels, and template creators can manage network templates.

This chapter includes the following topics:

Modify Network Template Properties

By default, only system administrators, administrators with rights at the organization level and template creators can edit network template properties. For information on the properties, see "Create a Network Template" on page 29.

To modify network template properties

1 In the left pane, select **Network Templates**.

2 Move the pointer on the network template name and select **Properties**.

3 Modify the properties and click **Update**.

Lab Manager updates the network template properties.

Change Ownership of a Network Template

The owner of a network template is the user who created it. If you have sufficient rights, you can change the owner.

To change ownership of a network template

1 In the left pane, select **Network Templates**.

2 Move the pointer over the network template name and select **Properties**.

3 Click **Change Owner**.

4 Select an organization and user and click **OK**.

5 Click **Update**.

Lab Manager reassigns the network template to the new owner.

Delete Network Templates

By default, only system administrators, administrators with rights at the organization level, and template creators can delete network templates. After you delete a network template, you cannot select it as the network for a virtual machine network interface, or add it to a configuration.

Existing virtual machines and configurations that are use the network template are not affected. You cannot delete a network template that is being used by a virtual machine template.

To delete a network template

1 In the left pane, select **Network Templates**.

2 Move the pointer over the network template name and select **Delete**.

3 Click **OK**.

Lab Manager deletes the network template.

Monitor IP Pool Usage for a Virtual Network

System administrators can monitor the IP pool of a virtual network that is based on a network template. If a virtual network is running out of IP addresses, and you want to add more, see "Add IP Addresses to the IP Pool of a Virtual Network" on page 124.

Every virtual machine that uses a static IP addressing mode for a NIC, and is connected to a virtual network, requires an IP address from the virtual network's IP pool. This IP address stays with the virtual machine through the various operations in Lab Manager. When you delete all instances of the virtual machine with this IP address, Lab Manager releases the IP address back to the IP pool.

To control the length of time Lab Manager reserves released IP addresses before returning them to the IP pool, see "Configuring General Preferences" on page 135.

When you deploy a configuration with a virtual network connected to a physical network, Lab Manager creates a virtual router and assigns it an IP address from the virtual network IP pool. When you undeploy this configuration, Lab Manager releases the IP address immediately.

To monitor a virtual network's IP pool

1 In the left pane, select **All Configuration(s)**.

2 Move the pointer over a configuration name and select **Open**.

3 Click the **Networks** tab.

4 Move the pointer over a virtual network name and select **IP Pool**.

Add IP Addresses to the IP Pool of a Virtual Network

By default, system administrators, administrators with rights at the organization level, and template creators can add IP addresses to a virtual network. Configuration owners and users with the right to edit configurations can also add IP addresses to a virtual network.

To add IP addresses to a virtual network

1 Move pointer over a configuration name and select **Open**.

2 Click **Networks** tab.

3 Move pointer over a virtual network name and select **IP Pool**.

4 Click the **General** tab.

5 Enter an IP address or IP address range in the **Static IP Address Pool** text box and click **Add**.

6 Click **Update**.

Remove IP Addresses from the IP Pool of a Virtual Network

Only system administrators, administrators with rights at the organization level and template creators can remove IP addresses from a virtual network.

To remove IP addresses from a virtual network

1 Move pointer over a configuration name and select **Open**.

2 Click the **Networks** tab.

3 Move the pointer over a virtual network name and select **IP Pool**.

4 Click the **General** tab.

5 Enter an IP address or IP address range in the **Static IP Address Pool** text box, or select an existing IP address or IP address range, and click **Remove**.

6 Click **Update**.

Managing Virtual Machine Templates 14

A virtual machine template is a virtual machine image loaded with an operating system, applications, and data. After you define and publish a template, you can quickly and easily create multiple virtual machines based on the template without having to reinstall software or redo setup tasks on each virtual machine. Using the templates ensures that virtual machines are consistently configured across an entire organization.

By default, only system administrators, administrators with rights at the organization level, and template creators can create templates. These users can create a new template, import a template, save a vCenter Lab Manager virtual machine as a template, and clone an existing template.

This chapter includes these topics:

Unpublish a Virtual Machine Template

Unpublish a virtual machine template to make it unavailable for configuration use.

To unpublish a virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over the published template name and select **Unpublish**.

3 Click **OK**.

Export a Virtual Machine Template to an SMB Share

You can export an undeployed virtual machine template to an SMB share. This operation requires that you have a shared folder with full control permissions at the share and file system level.

Exporting can take an extended period of time, depending on the size of the virtual machine. By default, Lab Manager times out when export operations take longer than two hours. See "Configuring General Preferences" on page 135 to modify the timeout for SMB exports.

Export operations require an open SMB port on the ESX hosts. Although Lab Manager opens the port during installation, you need to make sure that the port was not closed after the install. To check the port status, run **`esxcfg-firewall -q smbClient`** on each host.

Before exporting a virtual machine template, Lab Manager consolidates it. This results in an increase in the disk space required to store the template. The exported template might also require a significant amount of disk space depending on the size of its consolidated virtual disk.

When you export a template to an SMB file server, the datastore on which the template resides must be connected to an ESX host. If the datastore is only connected to an ESXi host, you cannot export the template to an SMB file server. You can still export the template to vCenter.

To export a virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over the template name and select **Export**.

3 Provide the location and user credentials:

- Type the UNC path of the SMB share (relative to the Lab Manager server system) where you want to store the files. Use English characters for the UNC path, for example, A sample path is **`\\10.6.1.246\VMwareLM\ExportTemplates`**.
- If the UNC folder requires authentication, type the user name and password to access the files.

4 Click **OK**.

Export a Virtual Machine Template to vCenter

By default, system administrators, administrators with rights at the organization and workspace levels, and template creators can export virtual machine templates to vCenter.

To export a virtual machine template to vCenter

1 In the left pane, click **VM Templates**.

2 Move the pointer over a template name and select **Export**.

3 Select **vCenter**.

4 Type a display name for the exported template.

5 Select a datastore.

6 Select a network.

7 Click **OK**.

Lab Manager exports the template to vCenter.

Consolidate a Virtual Machine Template

Each time you create a linked clone of a virtual machine template, Lab Manager freezes the virtual hard disk associated with the original template and creates delta disks to store future changes to the clone and its source. Over time, the increasing number of stored delta disks can affect performance. You do not need to consolidate templates until Lab Manager generates an error requesting this operation.

NOTE Even if you do not have to consolidate disks, you can use this operation to move a template to a different datastore.

You can only consolidate templates that are unpublished and undeployed. Consolidation can take an extended period of time, depending on the disk size and storage performance. Consolidation reduces the free space on datastores because the template no longer benefits from delta disks.

To consolidate a virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over the template name and select **Consolidate**.

3 Select a datastore and click **OK**.

Lab Manager consolidates the template.

Discard the State for a Virtual Machine Template

When you save the state of a virtual machine template by using the **Undeploy - Save State** option or by suspending the virtual machine template, Lab Manager saves information about the processor type of the host on which the virtual machine template was deployed. Lab Manager requires an available host with a compatible processor type to redeploy the virtual machine template. If processor incompatibility issues prevent you from deploying a virtual machine template, you can discard the state information. You can also discard state to free up storage space.

You can only discard state for undeployed virtual machine templates with saved state.

To discard state for a virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over the undeployed template name and select **Discard State**.

3 Click **OK**.

Lab Manager discards the template's state.

Modify Virtual Machine Template Properties

By default, only system administrators, administrators with rights at the organization level and template creators can modify the properties of a template. Before you modify the properties of a template, undeploy the template. If it is deployed, the number of properties you can modify is limited.

See "Modifying Virtual Machine Template Hard Disks" on page 131 and "Modifying Virtual Machine Template Network Interfaces" on page 132 for information about modifying virtual machine template hard disks and network interfaces.

See "Change Ownership of a Virtual Machine Template" on page 134 For information about changing the owner of a template.

To modify virtual machine template properties

1 In the left pane, click **VM Templates**.

2 Move the pointer over the template name and select **Properties**.

3 Modify the name.

4 (Optional) Type a description.

5 Select a Guest OS.

If you select a 64-bit guest operating system, the datastore must be connected to an ESX/ESXi host that provides the required 64-bit processor for that guest OS. You can proceed without fulfilling this requirement, but you cannot deploy the virtual machine template until you attach a host with the correct processor. If you have some but not all 64-bit hosts, Lab Manager limits the number of hosts on which the virtual machine template can be deployed.

6 Select or deselect **Virtual CPU Hot Add**.

Selecting this check box enables virtual CPU hot add.

7 Select or deselect **Memory Hot Add**.

Selecting this check box enables memory hot add.

8 Select or deselect **32-bit Virtual CPU**.

By default, the virtual CPU type assumes the physical host CPU type.

Select this check box to override the default behavior and ensure the virtual CPU type is 32 bits. For example, you might have a virtual machine template with a 32-bit guest operating system that does not have the requires software (kernel or drivers) to run on a 64-bit processor. Another example involves a mixed (32-bit and 64-bit) ESX/ESXi host environment where you need to complete a testing process specifically on a 32-bit guest operating system, and the operating system accommodates both 32-bit and 64-bit CPU architecture.

See the VMware Infrastructure documentation for details on priorities, shares, reservations, and limits.

9 Select the number of virtual CPUs.

The maximum number of processors is four.

The datastore must be connected to a host that provides the required SMP technology for the guest operating system. If you choose a CPU number not currently compatible with the CPU of the host, you cannot deploy the virtual machine template until you attach a host with the appropriate SMP support. If you have some but not all hosts that provide the required SMP technology, Lab Manager limits the number of hosts on which the virtual machine template can be deployed.

10 Modify the CPU reservation.

11 Select a CPU priority.

12 Select a CPU limit.

If you select **Maximum**, type a value.

13 Modify the memory value.

14 Modify the memory reservation value.

15 Select a memory priority.

16 Select a memory limit.

If you select **Maximum**, type a value.

17 Select or deselect the **Use Time Synchronization** check box.

Enables time synchronization between the guest (virtual machine template) and ESX/ESXi host operating systems.

18 Check whether the **Perform Customization** is selected.

It specifies whether guest customization is enabled.

19 Select a **SID mechanism**.

The selection specifies the mechanism Lab Manager uses to change the SID. If the virtual machine template is unpublished, you can switch the default tool Lab Manager uses to change the SID, or select **None**.

To use Microsoft Sysprep, you must first create a Microsoft Sysprep package for guest customization. See "Build a Microsoft Sysprep Package" on page 41.

20 Select deployment or storage leases.

These selections determine when undeploy the virtual machine template or delete the virtual machine template (or mark it for deletion), depending on whether the virtual machine template is deployed.

21 Click **Update**.

Modifying Virtual Machine Template Hard Disks

For undeployed and unpublished virtual machine templates, you can add hard disks, edit hard disks, and delete hard disks.

Add a Hard Disk to a Template

You can add one or more virtual hard disks (`.vhd` files) to a virtual machine template.

To add a virtual hard disk to a template

1 In the left pane, click **VM Templates**.

2 Move the pointer over the virtual machine template name and select **Properties**.

3 In the Hard Disks section, click **Add Hard Disk**.

4 Type the disk size (GB).

5 Select the bus type.

6 Select a bus number.

7 Select a bus ID.

8 Click **OK** and **Update**.

You can deploy the virtual machine template and use the guest operating system tools to partition and format the new disk for use. If you add a SCSI hard disk to a virtual machine template, the guest OS might generate an error message about missing drivers the next time you power on the template. If this error occurs, download and install the appropriate driver, and contact VMware for further support.

Edit a Virtual Machine Template Hard Disk

You can update the bus number and bus ID of a virtual machine hard disk.

To edit a virtual machine template hard disk

1 In the left pane, click **VM Templates**.

2 Move the pointer over the virtual machine template name and select **Properties**.

3 In the Hard Disks section, click **Edit** next to one of the listed disks.

4 Modify the bus number and bus ID and click **OK**.

5 Click **Update**.

Delete a Virtual Machine Template Hard Disk

You can delete a virtual machine template hard disk.

To delete a virtual machine template hard disk

1 In the left pane, click **VM Templates**.

2 Move the pointer over the virtual machine template name and select **Properties**.

3 In the Hard Disks section, click **Delete**.

4 Click **OK** and **Update**.

Modifying Virtual Machine Template Network Interfaces

You can modify the network settings, reset a MAC address, add a network interface, and delete a network interface for undeployed templates.

Add a Network Interface to a Virtual Machine Template

You can add one or more virtual NICs to an undeployed virtual machine template. Depending on your virtual machine version, a template can have up to four NICs.

To add a network interface

1 In the left pane, click **VM Templates**.

2 Move the pointer over the template name and select **Properties**.

3 In the Network Interfaces panel, click **Add Interface**.

Lab Manager adds and connects a new virtual NIC.

4 Edit the virtual NIC settings, if necessary.

a Deselect the **Connected** check box to disconnect the virtual NIC.

b Choose a network from the **Network** drop-down menu.

The available options are based on the network templates that you own or share and the physical networks available to your organization.

c Specify a primary NIC.

The primary NIC setting determines the default, and only gateway, for the virtual machines based on the template. These virtual machines can use any NIC to connect to other machines that are directly connected to the same network as the NIC, but it can only use the primary NIC to connect to machines on networks that require a gateway connection.

Consider this behavior when selecting a primary NIC, especially if you plan to deploy configurations that use fencing or connect virtual networks to physical networks.

d Select an IP addressing mode for the network.

The available options are based on the IP addressing modes available to the selected network.

e If you selected **Static - Manual** as the IP addressing mode, type an IP address in the **IP Address** text box.

5 Click **Update**.

Lab Manager generates a MAC address for the network interface.

Edit a Virtual Machine Network Interface

You can disconnect a virtual machine template NIC, change the network to which a NIC connects, specify a primary NIC, and change the IP addressing mode for a NIC.

To edit network interface settings

1 In the left pane, click **VM Templates**.

2 Move the pointer over the template name and select **Properties**.

3 In the Network Interfaces panel, change the settings as necessary:

- Deselect the **Connected** check box to disconnect a virtual NIC.
- Choose a network from the **Network** drop-down menu.

  The available options are based on the network templates you own or share and the physical networks available to your organization.
- Specify a primary NIC.

  The primary NIC setting determines the default and only gateway for virtual machines based on the template. Those virtual machines can use any NIC to connect to other machines that are directly connected to the same network as the NIC, but it can only use the primary NIC to connect to machines on networks that require a gateway connection.

  Consider this behavior when selecting a primary NIC, especially if you plan to deploy configurations that use fencing or connect virtual networks to physical networks.
- Select an IP addressing mode for the network.

  The available options are based on the IP addressing modes available to the selected network. **DHCP** allows Lab Manager avoids the preparation and specification of an IP address or IP range. However, you cannot use Lab Manager fencing or connect virtual networks to physical networks with DHCP.

4 Click **Update**.

Delete a Network Interface from a Virtual Machine Template

You can delete virtual NICs from an undeployed template.

To delete a network interface

1 In the left pane, click **VM Templates**.

2 Move the pointer over the template name and select **Properties**.

3 In the Network Interfaces panel, click **Delete**.

4 Click **Update**.

Lab Manager deletes the network interface.

Reset a Virtual Machine Template Network Interface MAC Address

You can reset a network interface MAC address for an undeployed template. Reasons to reset include having a MAC address conflict or discarding the saved state quickly and easily.

To reset the MAC address for a network interface

1 In the left pane, click **VM Templates**.

2 Move the pointer over the template name and select **Properties**.

3 In the **Network Interfaces** panel, select **Reset** from the **MAC Address** drop-down menu.

4 Click **Update**.

Upgrade Virtual Hardware

Lab Manager supports version 4 and version 7 virtual machine templates. You can upgrade version 4 templates to version 7. Version 4 templates can run on hosts with ESX 3.5 and above, while version 7 templates require hosts with ESX 4.0 and above.

Before you can upgrade a template to version 7, you must install the latest version of VMware Tools. When you upgrade virtual hardware, Lab Manager discards state information and deletes any snapshots associated with the template.

To upgrade virtual hardware, you must first undeploy and unpublish the template.

To upgrade virtual hardware

1 Move the pointer over the template name and select **Upgrade Virtual Hardware**.

2 Click **OK**.

Lab Manager upgrades the virtual hardware.

Change Ownership of a Virtual Machine Template

The owner of a virtual machine template is the user who created it. If you have sufficient rights, you can change the owner.

To change ownership of a virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over the template name and select **Properties**.

3 Click **Change Owner**.

4 Select and organization and user and click **OK**.

5 Click **Update**.

Lab Manager reassigns the virtual machine template to the new owner.

Delete a Virtual Machine Template

To delete a template, it must be undeployed and unpublished. If you are unable to unpublish a template, you can force delete it. See "Delete a Virtual Machine Template with Force" on page 134.

To delete a virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over the virtual machine template name and select **Delete**.

3 Click **OK**.

Delete a Virtual Machine Template with Force

If an ESX/ESXi host failure or some other event prevents you from unpublishing and deleting a template, Lab Manager system administrators can still forcefully delete a published template.

The Force Delete command removes the template from the Lab Manager database but not from the vCenter inventory. You can manually remove the virtual machine from the vCenter inventory.

To delete a published virtual machine template

1 In the left pane, click **VM Templates**.

2 Move the pointer over the published template name and select **Force Delete**.

3 Click **OK**.

Managing Lab Manager Settings 15

The Lab Manager system administrator controls various systemwide settings related to LDAP, licensing, guest customization, storage and deployment leases, and so on. You can generally specify these settings once and change them later, if necessary.

This chapter includes the following topics:

Configuring General Preferences

You can configure preferences for settings related to Lab Manager, email, system alerts, and recording change summaries.

Change vCenter Lab Manager Preferences

The Lab Manager preferences include settings that you entered during installation as well as prepopulated default values. If needed, you can change the settings.

To change Lab Manager preferences

1 In the left pane, click **Settings**.

2 Click the **General** tab.

3 Modify the Lab Manager preferences and click **OK**.

You can modify any of the preferences described in Table 15-1, "vCenter Lab Manager Preferences," on page 136.

Table 15-1. vCenter Lab Manager Preferences

Name	Details
Login Policy	Select **Remember User Name Only** if you want Lab Manager to retain the user name but not the password. Select **Automatically Login** if you want Lab Manager to log users in when they start Lab Manager. Lab Manager uses persistent cookies (physically stored on the computer hard disk) to retain the login information. If you delete the browser cookies, this information is not available until you log in again.
vCenter Lab Manager Installation ID	Lab Manager uses the installation ID to generate MAC addresses for virtual machines. If you have more than one Lab Manager installation on the same network, each installation must have a unique ID to ensure that there are no MAC address conflicts. Lab Manager randomly assigns an ID and allows the administrator to manually edit the value if an ID collision occurs.
vCenter Lab Manager Installation Host IP Address	IP address of the Lab Manager server.
vCenter Lab Manager Host Name	DNS name of the Lab Manager server.
Session Timeout	Time you want the Lab Manager application to remain active without user interaction.
IP Release Timeout	Specifies how long to reserve released IP addresses before returning them to the IP pool. See "Monitor IP Pool Usage for a Physical Network" on page 102.
Host Refresh Frequency	Frequency of checking whether ESX/ESXi hosts are accessible or hung. The default is 60 seconds.
Host Hung Timeout	Time to wait before marking a host as hung.
Host Default Maximum Number of VMs	Maximum number of deployed virtual machines allowed on a host. The default is 64. For information on quotas, see "Modify Host Properties" on page 92.
Host Agent Request Timeout	Time to wait before an operation that uses the Lab Manager agent fails. For example, importing a virtual machine template from an SMB share.
Import from vCenter Timeout	Time to wait before a vCenter import fails. The default is 120 minutes. When Lab Manager imports a virtual machine from vCenter, vCenter clones the virtual machine. The timeout value applies to this cloning task.
Datastore Garbage Collection Frequency	Frequency of garbage collection on datastores. The default is 120 seconds. Garbage collection is the automatic detection and freeing of images that are no longer in use. Lab Manager does not immediately delete files associated with a deleted virtual machine. Lab Manager stores virtual machine files in a tree of related linked clones. Each pass of the garbage collector involves an attempt to delete nodes that no longer have dependencies. Several passes over time might be required to free up the space associated with a deleted virtual machine.
Activity Log History to Keep	Days of log history to keep before deleting it. The default is 90 days. Type `0` to never delete logs.
Activity Log History Shown	Days of log history to display in the Web console. The default is 30 days. Type `0` to show all activity.
Display Background Image on Login Screen	Choose whether to display the background image. If you have a slow or remote connection to Lab Manager, you can turn off the background image to speed up loading time.
Provide Default Configuration and Machine Names	Choose whether you want Lab Manager to generate default names for configurations and virtual machines.

Set Email Preferences

Lab Manager uses an SMTP server to send user notifications and system alert emails.

To set email preferences

1 In the left pane, click **Settings**.

2 Click the **General** tab.

3 Type the DNS host name or IP address of the SMTP mail server.

4 If the SMTP server requires a user name, select the **Requires User Name** check box and type the user name and password for the SMTP server account.

5 Type an email address that appears as the sender for Lab Manager emails.

Lab Manager uses the sender's email address to send system alerts under these conditions:

- Deployment lease expiration alerts are enabled, and a configuration or virtual machine template falls within the specified alert time.
- Storage lease expiration alerts are enabled, and a configuration or virtual machine template falls within the specified alert time.

6 Type text to use as the subject prefix for Lab Manager emails.

7 Type the destination email address to test SMTP settings.

8 Click **Test SMTP Settings** to verify that the server connection works.

9 Click **OK**.

Set System Alert Preferences

Lab Manager can send system alert emails to all Lab Manager system administrators or to a specified list of email addresses.

Lab Manager sends system alert emails to the specified recipients under these conditions:

- Status of a host or datastore changes.
- Disk threshold (yellow or red) of a host or datastore is crossed.
- Lab Manager loses or resumes the connection to the vCenter Server.
- Lab Manager detects that an ESX/ESXi host is not responding or starts responding.

To set system alert, preferences

1 In the left pane, click **Settings**.

2 Click the **General** tab.

3 Select the recipients of system alert emails:

- **All vCenter Lab Manager Administrators** – Select this option to send system alerts to all system administrators.
- **These Email Addresses** – Select this option to send system alerts to a specified list of email addresses.

4 Click **OK**.

Set Configuration Change Summary Preferences

Lab Manager records certain configuration operations, such as adding or removing a network, deploying or undeploying the configuration, and so on, as change summaries. Other operations, such as cloning, moving, and archiving, allow you to input change summary text. Change summaries can be helpful for tracking and auditing purposes.

When you create a new configuration based on an existing one (for example, by cloning a configuration) you can specify how many of the original configuration's change summaries you want the new configuration to inherit.

To set configuration change summary preferences

1 In the left pane, click **Settings**.

2 Click the **General** tab.

3 Select how many change summaries you want to inherit.

4 Click **OK**.

Configuring LDAP Settings

You can configure Lab Manager to create and authenticate user credentials against an LDAP server. Instead of manually creating all the user accounts, you enable an entire company (or subset) of users by pointing the installation to the appropriate Microsoft Active Directory or OpenLDAP server.

Lab Manager does not support hierarchical domains for LDAP authentication.

See "Create a User" on page 24 for information on manually creating Lab Manager user accounts for non-LDAP users.

To provide Lab Manager access to LDAP users, you must specify the LDAP settings and then add LDAP users or groups to a Lab Manager organization (see "Create an Organization" on page 27).

When an LDAP user who has been added to an organization logs into Lab Manager, Lab Manager checks the credentials of the user against the LDAP directory. If the credentials are accepted, Lab Manager creates a new user account and logs the user into the system.

Lab Manager cannot modify the information in your LDAP directory. You can add, delete, or modify LDAP users or groups only in the LDAP directory itself. Lab Manager regularly synchronizes user and group information with the LDAP directory.

Locate an LDAP Server

Before typing a host name and port information for your LDAP server, you can have Lab Manager try to locate an available LDAP server.

To locate an LDAP server

1 In the left pane, click **Settings**.

2 Click the **LDAP** tab.

3 Click **Locate LDAP Server**.

Lab Manager looks for LDAP servers registered with the DNS server for the local computer. If Lab Manager finds an LDAP server, it populates the Server and Port text boxes. If Lab Manager finds multiple LDAP servers, it chooses one based on the DNS LDAP priority and weight.

Set Up an LDAP Connection

You can set up an LDAP connection to provide Lab Manager access to users and groups that already exist on the LDAP server.

To set up an LDAP connection

1 In the left pane, click **Settings**.

2 Click the **LDAP** tab.

3 Type the host name or IP address of the LDAP server.

If you do not specify a server, Lab Manager uses serverless binding (for Active Directory only), which connects to any available domain controller. Serverless binding provides redundancy and load-balancing benefits and requires that the Lab Manager server is in the same domain as the Active Directory domain controller.

4 Type a port number or leave blank to use the default ports.

If the LDAP server is listening on a nondefault port, type the port number. For LDAP, the default port is 389; for LDAPS, the default port is 636.

5 Type the base distinguished name (DN).

The base DN is the location in the LDAP directory where Lab Manager connects.

Lab Manager can detect the base DN if your LDAP server supports this. Leave this text box blank and click **Test LDAP Settings** to determine if your server supports base DN detection.

VMware recommends connecting at the root. You need to type the domain components only, for example, **`DC=vmware,DC=com`**.

To connect to a node in the tree, type the distinguished name for that node, for example, **`OU=LabManager,DC=vmware,DC=com`**. Connecting at a node limits the scope of the directory available to Lab Manager.

CAUTION If you specify an OU, only LDAP users in that OU can log in to Lab Manager. In some cases, this restriction can block access to users that you do not want to block.

For example, consider the following scenario:

- Domain Name: mydomain.com
- Top Level OUs: DublinOffice and HeadOffice
- Groups: LabMan group that includes users from both the DublinOffice and HeadOffice OUs.

If your binding string is **`OU=HeadOffice,DC=mydomain,DC=com`**, and you add the LabMan group to a Lab Manager organization, only members of the LabMan group who are also members of the HeadOffice OU can log in to Lab Manager and access the organization. Members of the LabMan group from the DublinOffice OU are excluded.

6 Select the **Use LDAPS** check box if you have an LDAP server set up to support LDAPS.

LDAPS makes LDAP traffic confidential and secure by using LDAP over Secure Sockets Layer (SSL).

7 Select the **Accept all certificates** check box to allow LDAPS communication between the LDAP server and Lab Manager server without requiring the LDAPS server certificate in the Lab Manager server certificate store.

CAUTION Do not select this option unless you are sure that your network is secure.

If you do not select this option, you must import a server authentication certificate from the LDAPS server into the Lab Manager server's certificate store. See the Windows Server 2003 Product Help for information about importing certificates.

8 Select the authentication method for your LDAP server.

- **Active Directory Negotiate** – Choose this method for Active Directory.
- **Digest-MD5** – Choose this method for OpenLDAP without LDAPS. You must provide MD5 Realm information.
- **Basic** – Choose this method for OpenLDAP only if you are using LDAPS. If you are using LDAP, be aware that the LDAP password is sent over the network in clear text.

9 Type a user name and password to connect to the LDAP server.

If anonymous read support is enabled on your LDAP server, you can leave these text boxes blank. By default, Active Directory does not enable anonymous read, but OpenLDAP does.

10 Specify how often Lab Manager synchronizes with the LDAP server.

Synchronizing updates Lab Manager user and group information based on changes to the LDAP directory. To synchronize immediately, click the **Synchronize LDAP** button.

Specify the LDAP Connector and Schema

Lab Manager supports Microsoft Active Directory and OpenLDAP, as well as the most common schemas associated with each.

To specify the LDAP connector and schema

1 In the left pane, click **Settings**.

2 Click the **LDAP** tab.

3 Select a connector.

Lab Manager supports Active Directory and OpenLDAP. Certain options are enabled or disabled based on your selection. For example, only Active Directory supports serverless binding.

4 Select an LDAP schema.

The LDAP schema defines the required and optional attributes for an LDAP directory entry.

If you select Active Directory as the connector, select **Active Directory**, unless you are using a custom schema.

If you select OpenLDAP as the connector, select **OpenLDAP(1)**, **OpenLDAP(2)**, or **OpenLDAP(3)**, unless you are using a custom schema. OpenLDAP(1), (2), and (3) represent the most common implementations of OpenLDAP. OpenLDAP(1) should work in most environments that are not significantly customized. Check with your OpenLDAP administrator to determine which schema to choose or if you need a custom schema.

The combination of connector and schema populates the text boxes in LDAP User Attributes and LDAP Group Attributes.

Customize LDAP User and Group Attributes

The LDAP user attributes provide Lab Manager with details about how user and group information is defined in the LDAP directory. These settings allow Lab Manager to access the information and map it to its own user and group database.

If your LDAP directory uses different syntax for user and group attributes than what is displayed, modify the information here to match the LDAP directory.

To customize LDAP user and group attributes

1 In the left pane, click **Settings**.

2 Click the **LDAP** tab.

3 Modify the user and group attributes to match the attributes in your LDAP server.

Test LDAP Settings

After you enter your LDAP settings, you can test the settings to make sure that attributes are mapping correctly.

To test LDAP settings

1 In the left pane, click **Settings**.

2 Click the **LDAP** tab.

3 Click **Test LDAP Settings**.

Lab Manager tries to connect to the LDAP server and look up information about the user in the User Name text box. For anonymous read, you must provide a valid user name to test.

4 Review the test results and modify your connection information or attribute values, if necessary.

Detach an LDAP Server

To stop using LDAP to authenticate Lab Manager users, you can detach the LDAP server.

To detach an LDAP server

1 In the left pane, click **Settings**.

2 Click the **LDAP** tab.

3 Click **Detach LDAP Server**.

Lab Manager detaches the LDAP server and LDAP users are prevented from logging in to the Web console.

Synchronize Lab Manager with the LDAP Server

Lab Manager regularly synchronizes its user and group information with the LDAP server. You can manually synchronize with the LDAP server at any time.

To synchronize with an LDAP server

1 In the left pane, click **Settings**.

2 Click the **LDAP** tab.

3 Click **Synchronize LDAP**.

Configuring Lab Manager Licenses

Lab Manager capacity is licensed on a per-processor or per-socket basis for prepared ESX/ESXi hosts. You need at least two processors of available licensed capacity to prepare a dual-processor host.

View Capacity License Information

You can view information about your Lab Manager capacity licenses, such as expiration and number of CPUs.

To view capacity license information

1 In the left pane, click **Settings**.

2 Click the **License** tab.

Lab Manager displays information about your licenses.

Add a Capacity License

If you run out of licensed capacity, you can add capacity licenses to Lab Manager.

To add a capacity license

1 In the left pane, click **Settings**.

2 In the **License** tab, click **Add Capacity License**.

3 Type the serial number and click **OK**.

Configuring Guest Customization Settings

For virtual machines created from templates, Lab Manager can customize the network settings of the guest operating system. Guest customization requires VMware Tools.

- For information about building a Microsoft Sysprep package, see "Build a Microsoft Sysprep Package" on page 41.
- For information about choosing the default SID generation mechanism, see "Select the SID Generation Tool for Lab Manager" on page 43.
- For information about virtual machine template publishing, see "Disable VMware Tools Check Before Publishing Virtual Machine Templates" on page 47.

Configuring SupportLink Settings

Lab Manager SupportLink provides the performance statistics displayed on the Overview page and sends usage data to VMware that helps improve the product. VMware does not share this data with other organizations or trace any data back to individual users. SupportLink also allows you to collect support information to troubleshoot issues with VMware Support.

Enable SupportLink

During the Lab Manager installation and initialization process, you can decide whether to enable SupportLink. If you did not enable SupportLink at that time you can enable it later.

To enable SupportLink

1 In the left pane of the console, click **Settings**.

2 Click the **SupportLink** tab.

3 Select the check box to turn on SupportLink.

4 Type your company name and Lab Manager administrator email address.

   Do not alter the SupportLink server unless instructed to change the name by VMware support.

5 If the Lab Manager server uses a proxy server to connect to the Internet, enter the proxy server information.

6 If VMware support requests a test of SupportLink, click **Test Settings** to verify the connection to the Lab Manager SupportLink Server.

7 Click **OK**.

Collect Support Information

If VMware Support requests that you collect information about your Lab Manager environment for troubleshooting, you can collect support information from the SupportLink tab.

To collect support information

1 On the **SupportLink** tab, click **Collect**.

2 After Lab Manager collects support information, click the link to download a `.zip` file that contains the support logs.

Configuring Resource Cleanup Settings

You define the maximum deployment lease and storage lease times for virtual machine templates and configurations. The values you type are also used as the default settings for new virtual machine templates and configurations. You can override these defaults (up to the maximum) when you create or edit individual virtual machine templates and configurations.

NOTE If a Lab Manager system administrator changes the maximum value after the initial setting, a user can only extend an existing lease to the original value.

Understanding Leases

When a deployment lease expires, Lab Manager undeploys the configuration or virtual machine template. When a storage lease expires, Lab Manager deletes (or flags for deletion) the virtual machine template or configuration. See "Delete Expired Virtual Machines" on page 99 for more information about deleting virtual machines that are flagged for deletion.

Users can request email notification before a lease expires. See "Setting User Preferences" on page 16.

Storage leases do not affect published virtual machine templates or deployed virtual machine templates and virtual machines. After a virtual machine template changes from a published to an unpublished state, or a virtual machine template or virtual machine changes from a deployed to an undeployed state, the storage lease begins.

A storage lease is intended to delete unused or inactive virtual machine templates. The unpublish, clone, export, and consolidate operations renew the lease because Lab Manager identifies the virtual machine template as in use.

Setting or changing the memory or time synchronization properties for virtual machine templates or virtual machines renews the lease because Lab Manager identifies the virtual machine template or virtual machine as in use.

Set Deployment and Storage Lease Maximums

You can set the maximum deployment and storage lease times for configurations and virtual machine templates.

To set the maximum time for deployment and storage leases

1 In the left pane, click **Settings**.

2 Click the **Resource Cleanup** tab.

3 Choose the deployment lease maximums for workspace configurations and virtual machine templates.

4 Choose the storage lease maximums for workspace configurations, virtual machine templates, and library configurations.

5 Choose whether to delete or mark for deletion configurations and templates with expired storage leases.

6 Click **OK**.

Configuring vCenter Settings

The **vCenter** tab displays the settings for the vCenter Server associated with Lab Manager. From the **vCenter** tab, you can reconnect to the vCenter Server and change the vCenter Server log in information.

Reconnect to a vCenter Server

If Lab Manager loses its connection to the vCenter Server, Lab Manager attempts to reconnect periodically. If you want to connect immediately, you can force the connection process.

To reconnect Lab Manager to vCenter Server

1 In the left pane, click **Settings**.

2 Click the **vCenter** tab.

3 Click **OK**.

Lab Manager attempts to re-establish a connection with the vCenter Server.

Change the vCenter Server User Name and Password

If the user name and password for your vCenter Server changes or if the account you are currently using does not have the necessary vCenter privileges, you can change the log in information. For more information about the required vCenter privileges, see the *VMware vCenter Lab Manager Installation and Upgrade Guide*.

To change the vCenter Server log in information

1 In the left pane, click **Settings**.

2 Click the **vCenter** tab.

3 Type a new user name and password for the vCenter Server connection.

4 Click **OK**.

Lab Manager attempts to establish a connection with the vCenter Server using the new credentials.

16 Monitoring Lab Manager

Administrators can monitor completed and in-progress operations, view a list of currently deployed virtual machines, and review resource usage information. Most other Lab Manager users can only view information about their own jobs.

This chapter includes the following topics:

Monitoring Lab Manager Operations

Information about all recent Lab Manager operations appears in the Activity Log. In addition, you can view detailed information about each job in the log.

View the Activity Log

View the Activity Log to monitor operations that are in progress, to find and troubleshoot failed jobs, and to view jobs by owner or organization. Lab Manager system administrators can see all entries. Other users can see entries about their own operations.

To specify how long to retain Activity Log entries and how many days worth of history to display, see "Change vCenter Lab Manager Preferences" on page 135.

To view the Activity Log

In the left pane, click **Activity Log**.

The log lists activities for the currently selected organization. If you select **Global**, the log lists activities for the entire Lab Manager installation.

On this page, a table includes this information:

- The Status column indicates the success, failure, or in progress status of a job.

  A failed job includes a short description in the Details column.

- The Activity column includes a brief description of the operation.

  Click the activity description to view details about the job.

- The Owner and Location columns provide information about who initiated a job and from which organization and workspace they initiated it.

View Activity Details

You can view details about any job on its Activity Details page. The information is especially useful for troubleshooting.

To view the Activity Details page

1 In the left pane, click **Activity Log**.

2 Click the text in the Activity column.

Lab Manager displays detailed information about the job.

Monitoring Resource Usage

In Lab Manager, deployed virtual machines get their CPU and memory resources from resource pools. Administrators can get information about the availability of these resources for each resource pool, organization, and workspace.

View Resource Pool Resource Usage

You can view information about the CPU and memory resources used by each resource pool across the entire installation or within an organization.

To view resource pool usage information

1 In the left pane, click **Resource Usage** and click the **Resource Pools** tab.

2 Select the organization for which you want to view resource pool usage information from the **Organization** drop-down menu.

Select **Global** to view usage information across the entire installation.

Lab Manager displays resource usage information for all the resource pools in the selected organization or across the entire installation. If you select an organization, Lab Manager displays only the resources being used by that organization.

View Workspace Resource Usage

You can view information about the CPU and memory resources used by each workspace across the entire installation or within a specific organization.

To view workspace resource usage information

1 In the left pane, click **Resource Usage** and click the **Organizations and Workspaces** tab.

2 Select the organization for which you want to view workspace resource usage information from the **Organization** drop-down menu.

Select **Global** to view usage information for all workspaces in all organizations.

Lab Manager displays resource usage information for all the workspaces in the selected organization or across the entire installation. If you select an organization, Lab Manager displays only the resources being used by workspaces in that organization.

View Deployed Virtual Machines

You can view all deployed virtual machines in the Lab Manager installation or in an organization. See "View Deployed Virtual Machines on a Host" on page 93 to view the deployed virtual machines on a specific host.

To view deployed virtual machines

In the left pane, click **Deployed Machines**.

The page displays a list of deployed machines for the currently selected organization. If you select Global, the page lists deployed machines for the entire Lab Manager installation.

On this page, a table includes this information:

- **Console** – Provides access to the virtual machine console through the thumbnail icon.
- **Virtual Machine** – Provides a pop-up menu to view the virtual machine console or undeploy the virtual machine.
- **Status** – Indicates that the virtual machine is deployed.

  If there is an error associated with a virtual machine, it appears as a link. Click the link to view job details.
- **Configuration** – Specifies whether the virtual machine is a virtual machine template (indicated by a dash) or part of a configuration.
- **NIC** – Displays a number for each NIC associated with the virtual machine.
- **IP Address** – Displays the IP address of the virtual machine or specifies DHCP.
- **External IP** – Displays the external IP address for the virtual machine if it requires one.
- **Template** – Shows the virtual machine template that serves as the basis of the virtual machine.

  This is useful when you plan on retiring a virtual machine template and need to evaluate its usage. When a virtual machine template is removed from a configuration or is deployed, a dash appears in the **Template** column.
- **Host** – Displays the ESX/ESXi host name.
- **Deployed By** – Indicates the user who deployed the virtual machine.
- **Location** – Shows the organization and workspace from which the virtual machine was deployed.
- **Sharing** – Indicates whether the configuration is accessible for others to use.
- **Date Deployed** – Displays the date and time of deployment.
- **Messages** – Messages about the virtual machine.

Roles and Rights

A

vCenter Lab Manager applies roles and rights to determine which users and groups can perform which operations. See "Managing Users, Groups, and Roles" on page 109 for information on predefined roles, creating roles, and assigning rights to roles. See "Create an Organization" on page 27 for information on assigning roles to users and groups.

In addition, when users share an object that they own (for example, a virtual machine template or configuration), they can specify a level of access rights. Access rights combine with the rights of a user's role to determine how a user can interact with shared objects. Access rights cannot provided users with rights that they do not already have based on their role.

Predefined Roles

This appendix includes information about the rights assigned to Lab Manager's predefined roles and how access rights affect users who work with shared objects.

The Lab Manager predefined roles are:

- System Administrator
- Administrator

  The system administrator can assign the administrator role rights at the organization or workspace level.

- Template Creator
- Application Owner
- User
- View Only

Datastore Rights

By default, only system administrators can create, delete, and edit datastores. The create right is required to add a datastore to an organization. Other users can access datastores that are added to their organization as resources.

Table A-1. Datastore Rights for Predefined Roles

	Delete	Edit Properties
System Administrator	X	X
Administrator		
Template Creator		
Application Owner		
User		
View Only		

General Rights

The Change Ownership right allows system administrators to assign a new owner to Lab Manager objects (network templates, virtual machine templates, configurations, and media files) in any organization. Administrators with rights at the organization level can change the owner of objects in their organization.

The Administrator View and Control right allows system administrators to see and interact with all objects in the Lab Manager installation, even objects that are not shared with them. Only system administrators can modify Lab Manager's global settings.

Table A-2. General Rights for Predefined Roles

	Administrator View and Control	Change Ownership	Global Settings Modify
System Administrator	X	X	X
Administrator	X	X	
Template Creator			
Application Owner			
User			
View Only			

Group Rights

Only system administrators and administrators with rights at the organization level can add, delete, and edit groups. Lab Manager only supports groups created on an LDAP server. You cannot create a group or add users to a group within the Lab Manager environment.

Table A-3. Group Rights for Predefined Roles

	Create	Delete	Edit Properties
System Administrator	X	X	X
Administrator	X	X	X
Template Creator			
Application Owner			
User			
View Only			

High I/O Rights

Lab Manager restricts certain high I/O operations based on user roles.

Table A-4. High I/O Rights for Predefined Roles

	Consolidate	Export	Full Clone	Import from SMB	Import from vCenter
System Administrator	X	X	X	X	X
Administrator	X	X	X	X	
Template Creator	X	X	X	X	
Application Owner	X	X	X	X	
User					
View Only					

When an owner shares an object with another user, the user's ability to perform high I/O operations on that object is based on the intersection of the rights of their role and the access rights assigned by the owner sharing the object.

Table A-5. High I/O Rights for Sharing Roles

Access	Consolidate	Export	Full Clone	Import
Full Control	X	X	X	N/A
Change		X	X	N/A
Read		X	X	N/A

Host Rights

This table lists the rights that the predefined roles have for hosts in Lab Manager.

Table A-6. Host Rights for Predefined Roles

	Edit Properties	Enable/Disable	Undeploy/Redeploy
System Administrator	X	X	X
Administrator			
Template Creator			
Application Owner			
User			
View Only			

Host Spanning Transport Networks

This table lists the rights that the predefined roles have for host spanning transport networks in Lab Manageri.

Table A-7. Host Spanning Transport Network Rights for Predefined Roles

	Add/Remove
System Administrator	X
Administrator	
Template Creator	
Application Owner	
User	
View Only	

Library Configuration Rights

This table lists the rights that the predefined roles have for library configurations in Lab Manager.

Table A-8. Library Configuration Rights for Predefined Roles

	Clone to Workspace	Create	Delete	Discard State	Edit Properties	LiveLink	View
System Administrator	X	X	X	X	X	X	X
Administrator	X	X	X	X	X	X	X
Template Creator	X	X	X	X	X	X	X
Application Owner	X	X	X	X	X	X	X
User						X	X
View Only							

When an owner shares a Library configuration with another user, the user's rights are based on the intersection of the rights of the role and the access rights assigned by the owner sharing the object.

Table A-9. Library Configuration Rights for Sharing Roles

Access	Clone to Workspace	Create	Delete	Edit Properties	LiveLink
Full Control	X	N/A	X	X	X
Change	X	N/A		X	X
Read	X	N/A			X

Machine Rights

This table lists the rights that the predefined roles have for virtual machines in Lab Manager.

Table A-10. Machine Rights for Predefined Roles

	Edit Boot Seq./Delay	Edit CPU	Edit Hard Disk	Edit Memory	Edit Network	Edit Properties
Sys. Admin.	X	X	X	X	X	X
Admin.	X	X	X	X	X	X
Template Creator	X	X	X	X	X	X
App. Owner	X	X	X	X	X	X
User						
View Only						

Machine Rights for Predefined Roles (cont'd)

	Power On/Off	Revert	Snapshot	Suspend/ Resume	Use Console	View
Sys. Admin.	X	X	X	X	X	X
Admin.	X	X	X	X	X	X
Templ. Creator	X	X	X	X	X	X
App. Owner	X	X	X	X	X	X
User	X	X	X	X	X	X
View Only						X

The **Edit Properties** column refers to all virtual machine properties, except those called out in their own column. For example, a user can edit a virtual machine name but not its memory or network information.

When an owner shares a configuration or virtual machine template with another user, the user gets rights to the virtual machine template or configuration's virtual machines. Those rights are determined based on the intersection of the rights of their role and the access rights assigned by the owner sharing the object.

Table A-11. Machine Rights for Sharing Roles

Access	Edit Boot Seq. and Delay	Edit CPU	Edit Hard Disk	Edit Memory	Edit Network	Edit Properties
Full Control	X	X	X	X	X	X
Change	X	X	X	X	X	X
Read						

Media Rights

This table lists the rights that the predefined roles have for media in Lab Manager.

Table A-12. Media Rights for Predefined Roles

	Edit Properties	Synchronize	View
System Administrator	X	X	X
Administrator	X	X	X
Template Creator	X		X
Application Owner	X		X
User	X		X
View Only			

When an owner shares media with another user, the user's rights are based on the intersection of the rights of their role and the access rights assigned by the owner sharing the object.

Table A-13. Media Rights for Sharing Roles

Access	Edit Properties	Synchronize
Full Control	X	
Change	X	
Read		

Media Store Rights

By default, only system administrators can create, delete, and edit media stores. Other users can access media stores that are added to their organization as resources.

Table A-14. Media Store Rights for Predefined Roles

	Create	Delete	Edit Properties
System Administrator	X	X	X
Administrator			
Template Creator			
Application Owner			
User			
View Only			

Network Template Rights

By default, system administrators, administrators with rights at the organization level, and templates creators can create, delete, and edit network templates.

Table A-15. Network Template Rights for Predefined Roles

	Create	Delete	Edit Properties	View
System Administrator	X	X	X	X
Administrator	X	X	X	X
Template Creator	X	X	X	X
Application Owner				X
User				
View Only				

When an owner shares a network template with another user, the user's rights are based on the intersection of the rights of their role and the access rights assigned by the owner sharing the object.

Table A-16. Network Template Rights for Sharing Roles

Access	Create	Delete	Edit Properties
Full Control	N/A	X	X
Change	N/A		X
Read	N/A		

Organization Rights

By default, only system administrators can create and delete organizations.

Table A-17. Organization Rights for Predefined Roles

	Edit Membership	Edit Properties	Edit Resource	View
System Administrator	X	X	X	X
Administrator	X	X		X
Template Creator				
Application Owner				
User				
View Only				

Physical Network Rights

By default, only system administrators can create, delete, and edit physical networks. Other users can access physical networks that are added to their organization as resources.

Table A-18. Physical Network Rights for Predefined Roles

	Create	Delete	Edit Properties
System Administrator	X	X	X
Administrator			
Template Creator			
Application Owner			
User			
View Only			

Resource Pool Rights

By default, only system administrators can create, delete, and edit resource pools. Other users can access resource pools that are added to their organization as resources.

Table A-19. Resource Pool Rights for Predefined Roles

	Attach	Detach	Edit Properties
System Administrator	X	X	X
Administrator			
Template Creator			
Application Owner			
User			
View Only			

Role Rights

By default, only system administrators can create, delete, and edit roles.

Table A-20. Role Rights for Predefined Roles

	Create	Delete	Edit Properties	View
System Administrator	X	X	X	X
Administrator				X
Template Creator				
Application Owner				
User				
View Only				

Sharing Rights

Based on their role and rights, users can share objects to all or specific users in the following ways:

- Across the entire Lab Manager installation
- Across organizations
- Across workspaces
- With an organization
- With a workspace

Table A-21. Sharing Rights for Predefined Roles

	Share	Share Across Installation (Read only)	Share Across Installation Users (Read Only)	Share Across Orgs (Read only)	Share Across Org Users (Read Only)	Share Across Workspaces (Read only)
System Administrator	X	X	X	X	X	X
Administrator	X	X	X	X	X	X
Template Creator	X					X
Application Owner	X					X
User	X					X
View Only						

Sharing Rights for Predefined Roles (cont'd)

	Share Across Workspaces Users (Read Only)	Share with Organizations	Share with Organizations Users	Share with Workpsace	Share with Workspace Users
System Administrator	X	X	X	X	X
Administrator	X	X	X	X	X
Template Creator	X	X	X	X	X
Application Owner	X	X	X	X	X
User	X	X	X	X	X
View Only					

When an owner shares an object with another user, the user's ability to share that object is based on the intersection of the rights of their role and the access rights assigned by the owner sharing the object.

Table A-22. Sharing Rights for Sharing Roles

Access	Sharing Across the Entire Installation	Sharing Between Organizations	Sharing Within an Organization
Full Control	X	X	X
Change			
Read			

User Rights

By default, only system administrators and administrators with rights at the organization level can create, delete, and edit users. Lab Manager also supports users created on an LDAP server.

Table A-23. User Rights for Predefined Roles

	Create	Delete	Edit Properties	Notify	View
System Administrator	X	X	X	X	X
Administrator	X	X	X	X	X
Template Creator					
Application Owner					
User					
View Only					

VM Template Rights

This table lists the rights that the predefined roles have for virtual machine templates in Lab Manager.

Table A-24. Virtual Machine Template Rights for Predefined Roles

	Create	Delete	Deploy/Undeploy	Edit Properties	View
System Administrator	X	X	X	X	X
Administrator	X	X	X	X	X
Template Creator	X	X	X	X	X
Application Owner				X	X
User					
View Only					

When an owner shares a virtual machine template with another user, the user's rights are based on the intersection of the rights of the role and the access rights assigned by the owner sharing the object.

Table A-25. Virtual Machine Template Rights for Sharing Roles

Access	Create	Delete	Deploy/Undeploy	Edit Properties
Full Control	N/A	X	X	X
Change	N/A		X	X
Read	N/A			

Workspace Configuration Rights

This table lists the rights that the predefined roles have for workspace configurations in Lab Manager.

Table A-26. Workspace Configuration Rights for Predefined Roles

	Add Machine	Create	Delete	Delete Machine	Deploy/ Undeploy Fenced	Deploy/ Undeploy Non-fenced	Edit Prop.	View
System Admin	X	X	X	X	X	X	X	X
Admin	X	X	X	X	X	X	X	X
Template Creator	X	X	X	X	X	X	X	X
App. Owner	X	X	X	X	X	X	X	X
User			X		X	X	X	X
View Only								

When an owner shares a workspace configuration with another user, the user's rights are based on the intersection of the rights of their role and the access rights assigned by the owner sharing the object.

Table A-27. Workspace Configuration Rights for Sharing Roles

Access	Add Machine	Create	Delete	Delete machine	Deploy/ Undeploy Fenced	Deploy/ Undeploy Nonfenced	Edit
Full Control	X	N/A	X	X	X	X	X
Change		N/A		X	X	X	
Read		N/A					

Workspace Rights

This table lists the rights that the predefined roles have for workspaces in Lab Manager.

Table A-28. Workspace Rights for Predefined Roles

	Clone To	Create	Delete	Edit Membership	Edit Prop.	Edit Resource	Move From	Move To	View
System Admin.	X	X	X	X	X	X	X	X	X
Admin.	X	X	X	X	X	X	X	X	X
Templ. Creator	X						X	X	X
App. Owner	X						X	X	X
User									X
View Only									X

Client and Browser Support

B

Lab Manager users can access the Web console from client computers running various combinations of operating systems and browsers. Depending on the operating system, Lab Manager supports Microsoft Internet Explorer, Mozilla Firefox, or both.

See Table B-1, "32-Bit Client Operating System and Web Browser Support," on page 159 and Table B-2, "64-Bit Client Operating System and Web Browser Support," on page 159.

Table B-1. 32-Bit Client Operating System and Web Browser Support

Operating System	IE 6.x	IE 7.x	IE 8.x	Firefox 2.x	Firefox 3.x
Microsoft Windows					
Server 2008	N/A	Yes	Yes	Yes	Yes
Vista	N/A	Yes	Yes	Yes	Yes
Server 2003 Standard Edition	Yes	Yes	Yes	Yes	Yes
Server 2003 Enterprise Edition	Yes	Yes	Yes	Yes	Yes
XP Professional	Yes	Yes	Yes	Yes	Yes
2000 Server	Yes	No	N/A	No	N/A
2000 Advanced Server	Yes	No	N/A	No	N/A
Red Hat Enterprise Linux					
2.1 AS/ES/WS	No	No	No	Yes	Yes
3 AS/ES/WS	No	No	No	Yes	Yes
4 AS/ES/WS	No	No	No	Yes	Yes
5 AS/ES/WS	No	No	No	Yes	Yes
SUSE Linux					
Enterprise Server 8 (SLES)	No	No	No	Yes	Yes
Enterprise Server 9 (SLES)	No	No	No	Yes	Yes
Enterprise Server 10 (SLES)	No	No	No	Yes	Yes

Table B-2. 64-Bit Client Operating System and Web Browser Support

Operating System	IE 6.x	IE 7.x	IE 8.x	Firefox 2.x	Firefox 3.x
Microsoft Windows					
Server 2008	N/A	Yes	Yes	Yes	Yes
Vista	N/A	Yes	Yes	Yes	Yes
Server 2003 Standard Edition	Yes	Yes	Yes	Yes	Yes

Table B-2. 64-Bit Client Operating System and Web Browser Support (Continued)

Operating System	IE 6.x	IE 7.x	IE 8.x	Firefox 2.x	Firefox 3.x
Server 2003 Enterprise Edition	Yes	Yes	Yes	Yes	Yes
XP Professional	Yes	Yes	Yes	No	Yes
Red Hat Enterprise Linux					
3 AS/ES/WS	No	No	No	Yes	Yes
4 AS/ES/WS	No	No	No	Yes	Yes
SUSE Linux					
Enterprise Server 9 (SLES)	No	No	No	Yes	Yes
Enterprise Server 10 (SLES)	No	No	No	Yes	Yes

Guest Operating System Support

C

Lab Manager supports a wide variety of 32-bit and 64-bit operating systems in its virtual machine templates and virtual machines. See Table C-1, "32-Bit Guest Operating System Support," on page 161 and Table C-2, "64-Bit Guest Operating System Support," on page 162.

Table C-1. 32-Bit Guest Operating System Support

Operating System	Virtual Machine Versions	Customization	Hot-Add Memory	Hot-Add CPU
Microsoft Windows				
Microsoft Windows 7 (experimental)	Version 7 only	Yes	Yes	Yes
Microsoft Windows Server 2008	Versions 4 and 7	Yes, Sysprep only	Yes	No
Microsoft Windows Vista	Versions 4 and 7	Yes, Sysprep only	No	No
Microsoft Windows Server 2003, Datacenter Edition	Versions 4 and 7	Yes	Yes	No
Microsoft Windows Server 2003, Enterprise Edition	Versions 4 and 7	Yes	Yes	No
Microsoft Windows Server 2003, Standard Edition	Versions 4 and 7	Yes	No	No
Microsoft Windows Server 2003, Web Edition	Versions 4 and 7	Yes	No	No
Microsoft Windows Small Business Server 2003	Versions 4 and 7	Yes	No	No
Microsoft Windows XP Professional	Versions 4 and 7	Yes	No	No
Microsoft Windows 2000 Advanced Server	Versions 4 and 7	Yes	No	No
Microsoft Windows 2000 Professional	Versions 4 and 7	Yes	No	No
Microsoft Windows 2000 Server	Versions 4 and 7	Yes	No	No
Microsoft Windows NT	Version 4 and 7	Yes, SIDgen only	No	No
Microsoft Windows 98	Version 7 only	No	No	No
Microsoft Windows 95	Version 7 only	No	No	No
UNIX/Linux				
Debian GNU/Linux 5 (experimental)	Version 7 only	No	No	No
Debian GNU/Linux 4	Version 7 only	No	No	No
FreeBSD	Version 7 only	No	No	No
Other Linux	Versions 4 and 7	No	No	No
Red Hat Enterprise Linux 5	Versions 4 and 7	Yes	No	No
Red Hat Enterprise Linux 4	Versions 4 and 7	Yes	No	No
Red Hat Enterprise Linux 3	Versions 4 and 7	Yes	No	No

Table C-1. 32-Bit Guest Operating System Support (Continued)

Operating System	Virtual Machine Versions	Customization	Hot-Add Memory	Hot-Add CPU
Red Hat Enterprise Linux 2	Versions 4 and 7	Yes	No	No
SUSE Linux Enterprise Server 10	Versions 4 and 7	Yes	No	No
SUSE Linux Enterprise Server 9	Versions 4 and 7	Yes	No	No
Ubuntu Linux	Versions 4 and 7	No	Yes	No
Solaris				
Sun Solaris 10	Versions 4 and 7	Yes	No	No
NetWare				
Novell NetWare 6	Versions 4 and 7	No	No	No
Novell NetWare 5	Versions 4 and 7	No	No	No
Other				
Other	Versions 4 and 7	No	Yes	Yes

Table C-2. 64-Bit Guest Operating System Support

Operating System	Virtual Machine Versions	Customization	Hot-Add Memory	Hot-Add CPU
Microsoft Windows				
Microsoft Windows 7 (experimental)	Version 7 only	No	Yes	Yes
Microsoft Windows Server 2008	Versions 4 and 7	Yes, Sysprep only	Yes	Yes
Microsoft Windows Server 2008 R2 (experimental)	Versions 4 and 7	Yes, Sysprep only	Yes	Yes
Microsoft Windows Vista	Versions 4 and 7	Yes, Sysprep only	No	No
Microsoft Windows Server 2003, Datacenter Edition	Versions 4 and 7	Yes, Sysprep only	Yes	No
Microsoft Windows Server 2003, Enterprise Edition	Versions 4 and 7	Yes, Sysprep only	Yes	No
Microsoft Windows Server 2003, Standard Edition	Versions 4 and 7	Yes, Sysprep only	No	No
Microsoft Windows XP Professional	Versions 4 and 7	Yes, Sysprep only	No	No
UNIX/Linux				
Debian GNU/Linux 5 (experimental)	Version 7 only	No	No	No
Debian GNU/Linux 4	Version 7 only	No	No	No
Other Linux	Versions 4 and 7	No	No	No
Red Hat Enterprise Linux 5	Versions 4 and 7	Yes	Yes	No
Red Hat Enterprise Linux 4	Versions 4 and 7	Yes	No	No
Red Hat Enterprise Linux 3	Versions 4 and 7	Yes	No	No
SUSE Linux Enterprise Server 10	Versions 4 and 7	Yes	Yes	No
SUSE Linux Enterprise Server 9	Versions 4 and 7	Yes	No	No
Ubuntu Linux	Versions 4 and 7	No	Yes	Yes
Solaris				
Sun Solaris 10	Versions 4 and 7	Yes	No	No
Other				
Other	Versions 4 and 7	No	Yes	Yes

Using SSMove

D

SSMove is a utility on the Lab Manager server that allows you to move datastores. This utility is located in `C:\Program Files\VMware\VMware Lab Manager Server\Tools\SSMove.`

This appendix includes information about preparing to use SSMove, moving a datastore, and fixing common errors that might occur.

Before You Move a Datastore

To move a datastore, you must power off virtual machines and shut down ESX hosts and the Lab Manager server.

To prepare to move a datastore

1 Back up the Lab Manager database and data on the storage servers.

See the VMware knowledge base article at http://kb.vmware.com/kb/1000023 for more information.

2 In the left pane, click **Resources**.

3 On the **Datastores** tab, click the **% Used** column heading.

You can review datastore usage and identify datastores that are at or near capacity.

4 In the left pane, click **Users and Groups**.

5 Click **Send Notification**, which prompts all users to log out of Lab Manager.

6 Undeploy the virtual machines on the datastores that you are moving.

a On the **Datastores** tab, move the pointer over the datastore name and select **Open**.

b In **Status**, move the pointer over each deployed virtual machine name and select **Undeploy - Save State** or **Undeploy - Discard State**.

7 On the **Datastores** tab, move the pointer over the datastore name and select **Disable**.

8 Click **OK**.

9 Reboot all ESX hosts.

10 Verify that the role who is performing the move is a member of the VMwareLMClientAccts local group.

a On the Lab Manager server, select **Start** > **Programs** > **Administrative Tools** > **Computer Management**.

b In the console tree, click **Groups**.

c Double-click **VMwareLMClientAccts** and click **Add** to add a member.

d Reboot the Lab Manager server.

Move a Datastore

Only system administrators can move a datastore.

To move a datastore

1 On the Lab Manager server, run `SSMove.exe`, which is located in `C:\Program Files\VMware\Vmware Lab Manager\Tools\SSMove`.

You can only run a single instance of SSMove at a time.

2 Click **Refresh Sizes** to update the used and available space information for the datastores.

3 Filter the source trees based on their datastore or size.

a Select the datastore that contains the data you want to move.

b Type a minimum tree size (GB).

4 Click **Apply**.

5 Choose a source tree to move.

a On the View Datastore Usage page, move the pointer over the virtual machine and select **Context**.

b Move the pointer over the root of the tree to display the directory path.

The directory ID of the root node is the source tree that you want to move.

6 Select the destination datastore.

The drop-down menu lists the datastores that are connected to the same ESX hosts as the source datastore and the amount of free space (GB) on the datastore.

7 Select **Move**.

SSMove moves the data from the source to the destination and reports its progress in the **Status** area.

8 Click **Exit** when the move is complete.

9 In the Lab Manager Web console, enable the datastore.

10 Notify users that they can log in to Lab Manager.

Resolving Move Errors

If errors occur during the move, this section describes how to fix them.

To resolve move errors if an error message appears

1 Read the status message.

2 Resolve the problem that prevented the move and run `SSMove.exe` again to move the remaining directories.

In the **Source Tree** drop-down menu, trees with directories that have not moved are identified as partially completed. When you select a partially moved tree, you can move the entire tree or only the remaining directories.

To resolve errors if SSmove loses data when the destination datastore is NFS

1 Run **`select display_name from datastore where sub_directory = N'/'`**

2 If Lab Manager does not display a result, continue using SSMove.

3 If there is a result, run **`Update datastore set sub_directory = N'/VM' where display_name in (select display_name from datastore where sub_directory = N'/')`**.

4 Verify whether the directory virtual machine exists on the NFS datastores.

5 If the directory does not exist, create it.

Glossary

A

Active Directory
A Microsoft directory service that stores information about the network operating system and provides services. Active Directory enables administrators to set security policies, control resources, and deploy programs across an enterprise.

You can point Lab Manager at a Microsoft Active Directory domain or domain controller to enable an entire company (or subset) of users.

ActiveX Control
An object that supports programmatic interfaces. Lab Manager prompts you to install the remote console ActiveX Control when you initially access a virtual machine console.

activity log
A display of status information about asynchronous Lab Manager tasks or jobs that do not require immediate completion.

administrator
See Lab Manager system administrator.

agent
See Lab Manager agent.

B

base disk
The original virtual hard disk from which a virtual machine is derived. Virtual machines created by linked clones in Lab Manager consist of a base disk and chain of delta disks that store the changes made to the original. This process addresses the potential disk consumption difficulties that can occur with virtual machine proliferation.

When you make a linked clone of a virtual machine, both the clone and the original use the same base disk. When you make a full clone of a virtual machine, Lab Manager consolidates the original base disk and its delta disks to create a new base disk. In this case, the original disks remain unchanged.

See also chain length, clone, delta disk.

C

chain length
The number of delta disks associated with a virtual machine. The chain length indicates how distributed a virtual machine image is across the directories of a datastore.

See also base disk, consolidate, delta disk.

clone
See linked clone, full clone.

cluster
A server group in the virtual environment. Clusters enable a high-availability solution.

compute resource
A compute resource is the cluster or host providing compute power to a resource pool. The compute resource represents the sum of all CPU and memory of all hosts under it.

configuration
A group of virtual machines that Lab Manager controls as a unit. Lab Manager can replicate these configurations on demand.

console
See Lab Manager Web console, virtual machine console.

consolidate
To combine an existing base disk and its chain of delta disks into a single base disk. Use consolidation to move a virtual machine or configuration to a new datastore.

See also base disk, chain length, delta disk.

D

datastore
Virtual representation of combinations of underlying physical storage resources in the datacenter. A datastore is the storage location (for example, a physical disk, a RAID, or a SAN) for virtual machine files.

Lab Manager stores media files and virtual machines on VMFS and NFS datastores.

delta disk
"Differencing" disk created during the cloning process. A virtual machine created as a linked clone consists of a base disk, plus a chain of one or more delta disks that store the differences between the cloned virtual machine and the original virtual machine.

See also base disk, chain length, clone.

deploy
To register a virtual machine or configuration on an ESX host. This host must have the proper CPU type, CPU numbers, and 64-bit capability, if necessary. Lab Manager manages the selection of hosts when deploying virtual machines and configurations.

deployment lease
The amount of time a virtual machine template or configuration is deployed before Lab Manager is scheduled to undeploy it.

DHCP (Dynamic Host Configuration Protocol)
A communications protocol that enables dynamic addressing. The software relieves administrators of the task of assigning an IP address to each device that connects to a network.

DNS (Domain Name System)
An Internet data query service that translates host names into IP addresses. Also called Domain Name Server or Domain Name Service.

DRS (VMware Distributed Resource Scheduler)
See VMware Distributed Resource Scheduler (DRS).

E

ESX
See VMware ESX.

export
To move a configuration or virtual machine to an SMB share.

external IP address
A unique IP address temporarily assigned to each virtual machine deployed using network fencing or connecting a virtual network to a physical network. Through these external addresses, virtual machines both inside and outside the configuration can communicate with each other.

F

fencing
An architecture that isolates virtual machine configurations while allowing full network access. Fencing enables you to work with live instances of identical configurations on the same network simultaneously.

force delete
To forcefully delete a virtual machine when an ESX host failure prevents the Lab Manager administrator from deleting the virtual machine.

The operation cleans the virtual machine from the Lab Manager database but not from the VirtualCenter inventory. You can manually remove the virtual machine from the VirtualCenter inventory.

force undeploy
To forcefully undeploy a virtual machine after situations such as an ESX host goes permanently offline or someone manually removes a virtual machine from VirtualCenter inventory.

FQDN (fully qualified domain name)
The name of a host that includes the host name and the domain name. For example, the FQDN of a host named `esx1` in the domain `vmware.com` is `esx1.vmware.com`.

full clone
(n.) Full copy of the consolidated sum of delta disks and base disk of a virtual machine. Full cloning takes a significantly longer time than linked cloning.

(v.) To make a full copy of the consolidated sum of delta disks and base disk of a virtual machine.

See also linked clone, base disk.

G

guest customization
Lab Manager customization of the network settings inside the guest operating system of a virtual machine. These settings include the machine name, IP settings, and Security Identifier (SID) for Windows guest operating systems.

Lab Manager creates a package with the guest customization tools. When you power on a virtual machine for the first time, Lab Manager copies the package, runs the tools, and deletes the package from the virtual machine.

Without guest customization, the virtual machine uses the settings of the virtual machine template it is based on. This situation can create machine name and network conflicts when you deploy more than one virtual machine created from the same virtual machine template at the same time.

guest operating system
An operating system that runs inside a virtual machine.

H

host
The physical computer on which the virtual machines managed by Lab Manager reside.

I

import
To copy a configuration from an SMB share, or to copy a virtual machine from an SMB share or VirtualCenter.

internal IP address
A preconfigured IP address for a virtual machine in a configuration. Internal IP addresses remain static across cloning activity.

IP pool
A range of IP addresses set aside for use by physical and virtual networks in Lab Manager.

ISO
An exact representation of a CD or DVD, including its content and logical format.

L

Lab Manager system administrator
In most organizations, the highest level administrator who is likely to map to the VMware Infrastructure system administrator role. The responsibilities of the Lab Manager system administrator span the entire Lab Manager installation. Only Lab Manager system administrators can attach resources.

Lab Manager agent
Software installed on the ESX host that facilitates a connection to the Lab Manager Server system. Lab Manager installs the agent during the process of preparing a host.

Lab Manager Server
Component of the Lab Manager environment installed with the Lab Manager Server software.

Lab Manager Web console
A browser-based interface that provides access to all Lab Manager operations.

LDAP (Lightweight Directory Access Protocol)
A protocol that enables you to locate organizations, individuals, or other resources from a server.

lease
See deployment lease, storage lease.

linked clone
(n.) A duplicate of a virtual machine that uses the same base disk as the original, with a chain of delta disks, to keep track of the differences between the original and the clone.

(v.) To generate a "quick" copy by creating a delta disk instead of copying an entire virtual hard disk. This operation addresses virtual machine proliferation by using "referential provisioning," a process that involves storing new changes but referring back to a chain of delta disks. For each clone, Lab Manager freezes the original delta disk and creates a new one.

See also full clone, base disk, chain length.

M

MAC (Media Access Control) address
A hardware address that identifies each virtual or physical network adapter.

media store
A directory for media files on a datastore.

Microsoft Sysprep
A Microsoft utility for changing the SID of operating systems. You can build a Microsoft Sysprep package for guest customization in Lab Manager.

See Security Identifier (SID).

N

network fencing
See fencing.

NFS (Network File System)
A protocol that supports sharing of files, printers, and other resources. Lab Manager can use NFS datastores for media and virtual machine storage.

NIC (Network Interface Card)
An expansion board that provides a dedicated connection between a computer and a network. Also called a network adapter.

P

privilege
Authorization to perform a specific action or set of actions on a managed object or group of managed objects.

publish
To make a Lab Manager virtual machine template available for use in creating configurations.

R

ready
Indicates an ESX host is available for use. Certain host states are documented that affect this status.

referential provisioning
A process for linked clones that involves storing new changes but referring back to a chain of delta disks. For each clone, Lab Manager freezes the original delta disk and creates a new one.

A linked clone operation generates a "quick" copy by creating a delta disk instead of copying an entire virtual hard disk.

reset
To restart a virtual machine and clear the machine state. This operation can occur at the virtual machine or configuration level.

resource pool
A division of computing resources used to manage allocations between virtual machines.

resume
To return a virtual machine or configuration to operation from its suspended state. When you resume a suspended virtual machine or configuration, all applications are in the same state they were when the virtual machine or configuration was suspended.

See also Suspend.

revert
To return the virtual machine to an earlier state captured in a snapshot.

revert point
The state of a virtual machine as captured by a snapshot at a specific point in time. You can restore the status of an active virtual machine to its revert point.

S

SAN (storage area network)
A large-capacity network storage device that can be shared among multiple VMware ESX hosts. Shared storage (for example, SAN or NAS) is required for VMotion.

Security Identifier (SID)
A unique name in a Microsoft Windows environment used to identify an object.

See Microsoft Windows documentation.

SID
See Security Identifier (SID).

SIDgen
A tool packaged with Lab Manager that changes the SID for virtual machines.

SMB (Server Message Block)
A network protocol for exchanging files between computers. You can use SMB with Windows and Linux operating systems.

SMP (Symmetric Multiprocessing)
The technology that enables you to assign two virtual processors to a virtual machine on any host machine that has at least two logical processors.

SMTP (Simple Mail Transfer Protocol)
A protocol that facilitates email transmissions between servers.

SMTP Server
A system running email server software that accepts email from within your enterprise. Lab Manager must connect to an SMTP server to send email alerts.

snapshot
A reproduction of the virtual machine or configuration as it was when you took the snapshot, including the state of the data on all the virtual disks and power state (on, off, or suspended).

Lab Manager stores the snapshot with the configuration or virtual machine image. Only one snapshot is active at a time. The most recent snapshot replaces the previous one.

You can revert the configuration or virtual machine to a snapshot. If you undeploy a virtual machine and deploy it, the snapshot remains.

storage lease
The amount of time an unused virtual machine template or configuration exists on a datastore before Lab Manager deletes it or marks it for deletion. This affects only unpublished virtual machine templates.

Sysprep
See Microsoft Sysprep.

Suspend
A state in which settings are preserved and actions are no longer performed. To turn off a virtual machine while preserving the current state of a running virtual machine. See also resume.

T

TCP/IP
The set of protocols that is the language of the Internet, designed to enable communication between networks regardless of the computing technologies that they use. TCP connects hosts and provides a reliable exchange of data streams with guaranteed delivery. IP specifies the format of packets and handles addressing.

template
See virtual machine template.

U

undeploy
To unregister a virtual machine or configuration from an ESX host. This operation makes the resources associated with that virtual machine available for use by the rest of the virtual environment.

unprepare
To remove an ESX host from use in the Lab Manager environment. This operation uninstalls the Lab Manager agent.

V

vCenter
See VMware vCenter (vCenter), virtual machine disk (.vmdk).

vCenter Server
A service that acts as a central administrator for VMware servers connected on a network. This service directs actions on the virtual machines and the virtual machine hosts. vCenter Server is the working core of vCenter.

See also VMware vCenter (vCenter).

virtual hardware
The devices that make up a virtual machine. The virtual hardware includes the virtual disk, removable devices such as the DVD-ROM/CD-ROM and floppy drives, and the virtual Ethernet adapter.

virtual machine
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. Multiple virtual machines can operate on the same host system concurrently.

virtual machine configuration file (.vmx)
A file containing a virtual machine configuration. This `.vmx` file is created after you create a virtual machine. It is used to identify and run a specific virtual machine.

virtual machine console
An interface to a virtual machine within the larger Lab Manager Web console. Use the virtual machine console to run programs within it or modify guest operating system settings. Lab Manager provides operations ranging from the installation of VMware Tools to media file activity for the guest operating system to snapshots of virtual machines.

virtual machine disk (.vmdk)
A file or set of files that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system.

virtual machine template
A master image of a virtual machine that typically includes a specified operating system and virtual counterparts to hardware components. A virtual machine template can include an installed guest operating system and a set of applications.

virtual router
A virtual machine that specifically routes packets between other virtual machines. Lab Manager configures the virtual router when you deploy a fenced configuration and deletes it when you undeploy the configuration.

Lab Manager does not create a virtual router for the Block In and Out fencing mode.

virtual switch
A virtualized network switch used by ESX to manage traffic between virtual machines, the service console, and the physical network adapters on the ESX host.

VMFS (Virtual Machine File System)
A file system that is optimized for storing virtual machines. One VMFS partition is supported per SCSI storage device or LUN. Different versions of ESX might use different versions of VMFS. For example, VMFS3 was introduced with ESX Server 3.

VMkernel
In ESX, a high-performance hypervisor that occupies the virtualization layer and manages most of the physical resources on the hardware, including memory, physical processors, storage, and networking controllers.

VMotion
A feature that enables you to move running virtual machines from one ESX system to another without interrupting service. It requires licensing on both the source and target hosts. VMotion is activated by the vCenter agent, and vCenter Server centrally coordinates all VMotion activities. *See also* virtual machine disk (.vmdk).

VMware Distributed Resource Scheduler (DRS)
A feature that balances virtual machine workloads across ESX hosts using the vCenter and VMotion products. VMware DRS detects when virtual machine activity saturates an ESX host and triggers automated VMotion live migrations, moving running virtual machines to other ESX nodes so that all resource commitments are met.

VMware ESX
A virtualization layer run on physical servers that abstracts processor, memory, storage, and networking resources into multiple virtual machines. ESX is a component of VMware vSphere.

Lab Manager requires ESX hosts.

VMware High Availability (VMware HA)
Supports distributed availability services in an environment that includes ESX and vCenter. If you configured VMware HA and one of the hosts managed by vCenter Server goes down, all virtual machines on that host are immediately restarted on another host.

See also DRS (VMware Distributed Resource Scheduler), virtual machine disk (.vmdk).

VMware vSphere
A software suite, including ESX and vCenter, that virtualizes servers, storage, and networking and enables multiple unmodified operating systems and their applications to run independently in virtual machines while sharing physical resources. The suite delivers comprehensive virtualization, management, resource optimization, application availability, and operational automation capabilities.

See also VMware vCenter (vCenter), VMware ESX.

VMware vSphere Client
A user interface that runs locally in a Windows machine and provides access to the virtual machine's display. vSphere Client runs on a networked machine that does not need to be the same machine as the vCenter Server.

VMware Remote MKS Plugin
An application that embeds in the browser to facilitate interaction with a remote machine. This application sends mouse, keyboard, and screen data back and forth across the network.

VMware Tools
A suite of utilities and drivers that enhances the performance and functionality of your guest operating system. Key features of VMware Tools include some or all of the following, depending on your guest operating system: an SVGA driver, a mouse driver, and the VMware Tools control panel.

Guest customization in Lab Manager requires VMware Tools.

VMware vCenter (vCenter)
A software component of VMware vSphere for deploying and managing virtual machines across the datacenter. With vCenter, datacenters can instantly provision servers, globally manage resources, and eliminate scheduled downtime for hardware maintenance.

See also virtual machine disk (.vmdk).

.vmx
See virtual router.

Index

D

E

F

G

H

I

L

R

S

T

U

V

W