You can find the most up-to-date technical documentation on our 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

© 2006–2008 VMware, Inc. All rights reserved. Protected by one or more U.S. Patent Nos. 6,397,242,
6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022,
6,944,699, 6,961,806, 6,961,941, 7,069,413, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481,
7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999,
7,278,030, 7,281,102, 7,290,253, and 7,356,679; patents pending.
VMware, the VMware “boxes” logo and design, Virtual SMP and VMotion are registered trademarks or
trademarks of VMware, Inc. in the United States and/or other jurisdictions. Microsoft is a registered
trademark of Microsoft Corporation in the United States and other countries. All other marks and
names mentioned herein may be trademarks of their respective companies.
Lab Manager is distributed with AxpDataGrid, a third-party product, copyright by Axezz, Oslo,

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

2
Contents

About This Book  13

1 Introducing Lab Manager  15
   Lab Manager Components  16
   Lab Manager Benefits and Features  17
   Understanding Lab Manager in the VMware Infrastructure Environment  18
      Using Clusters, Hosts, Resource Pools, and Datastores  18
      Using VMware Infrastructure Capabilities  19

2 Using the Lab Manager Web Console  21
   Setting Browser Options  21
   Accessing the Lab Manager Web Console  22
   Viewing Performance, Usage, and Support Information  22
   Using the Interface  24
      Using Pop-Up Menus  24
      Using Text Search Filter  24
      Using Column Sorting  25
      VMware Tools and Mouse Control  25
   Setting User Preferences  25
      Set Display, Deployment, and Lease Alert Preferences  25
      Changing Your User Password  26
   General Workflow in Lab Manager  27

3 Working with Network Templates  29
   Accessing the Network Templates Page  30
   Creating Network Templates  31
   Copying Network Templates  33
   Sharing Network Templates  33
   Modifying Network Template Properties  35
   Changing Ownership of Network Templates  35
   Deleting Network Templates  35
Lab Manager User’s Guide

Viewing IP Pool Usage for a Virtual Network 36
Adding IP Addresses to the IP Pool of a Virtual Network 37
Removing IP Addresses from the IP Pool of a Virtual Network 37

4 Working with Virtual Machines 39
Viewing the Virtual Machines in a Configuration 40
Deploying Virtual Machines 41
  Deploying Virtual Machines on High Availability Clusters 43
Undeploying Virtual Machines 43
Discarding State for Virtual Machines 44
Consolidating Virtual Machines 44
Modifying Virtual Machine Properties 45
  Modifying Virtual Machine Hard Disks 48
    Adding a Virtual Machine Hard Disk 48
    Editing a Virtual Machine Hard Disk 48
    Deleting a Virtual Machine Hard Disk 49
  Modifying Virtual Machine Network Interfaces 49
    Editing Network Interface Settings 49
    Resetting a Network Interface MAC Address 51
    Adding a Network Interface 51
    Deleting a Network Interface 52
Viewing a Virtual Machine Console 53
  Installing the ActiveX Control or VMware Remote MKS Plug-In 53
Working in a Virtual Machine Console 54
  Setting Up a Remote Desktop Connection 55
  Powering On or Powering Off a Virtual Machine 55
  Resetting a Virtual Machine 56
  Shutting Down a Virtual Machine 56
Suspending and Resuming a Virtual Machine 56
Installing VMware Tools 57
  Taking A Snapshot of a Virtual Machine 57
  Reverting to a Virtual Machine Snapshot 58
  Deleting a Virtual Machine Snapshot 58
Inserting and Swapping CDs 58
  Ejecting CDs 59
  Inserting and Swapping Floppy Disks 59
  Ejecting Floppy Disks 59
Working with BEA LiquidVMs 60
5 Working with Virtual Machine Templates 61

Accessing the VM Templates Page 62
Creating Virtual Machine Templates 64
Importing Virtual Machine Templates 66
  Importing Virtual Machine Templates from VirtualCenter 66
  Importing Virtual Machine Templates from SMB Storage 68
Saving Virtual Machines as Virtual Machine Templates 69
Cloning Virtual Machine Templates 70
Deploying Virtual Machine Templates 71
  Deploying a Virtual Machine Template with Default Settings 72
  Deploying a Virtual Machine Template with Custom Settings 72
  Deploying Virtual Machine Templates on High Availability Clusters 72
Installing a Guest Operating System 73
Installing VMware Tools 74
Customizing the Guest Operating System 79
  Prerequisites for Guest Customization 79
  Building a Microsoft Sysprep Package 80
  Choosing the Guest Customization SID Generation Tool 82
    Choosing the SID Generation Tool for Lab Manager 82
    Choosing the SID Generation Tool for a Virtual Machine Template 82
    Choosing the SID Generation Tool for a Virtual Machine 83
Disabling Guest Customization 83
  Disabling Guest Customization for a Virtual Machine Template 84
  Disabling Guest Customization for a Virtual Machine 84
Guest Customization for Windows NT and Solaris Virtual Machine Templates 85
  Customizing Guest Customization 86
  Importing Virtual Machine Templates from Lab Manager 2.x with VMware Tools and LM Tools 87
Undeploying Virtual Machine Templates 87
Sharing Virtual Machine Templates 88
Publishing Virtual Machine Templates 89
  Checking VMware Tools Status Before Publishing Virtual Machine Templates 89
  Disabling VMware Tools Check Before Publishing Virtual Machine Templates 90
  Publishing Virtual Machine Templates 91
Managing Virtual Machine Templates 91
  Unpublishing Virtual Machine Templates 91
  Exporting Virtual Machine Templates to an SMB Share 91
  Consolidating Virtual Machine Templates 92
  Discarding State for Virtual Machine Templates 93
  Modifying Virtual Machine Template Properties 93
  Modifying Virtual Machine Template Hard Disks 96
    Adding a Virtual Machine Template Hard Disk 96
    Adding SCSI Virtual Hard Disks 96
    Editing a Virtual Machine Template Hard Disk 97
    Deleting a Virtual Machine Template Hard Disk 97
  Modifying Virtual Machine Template Network Interfaces 97
    Adding a Network Interface 97
    Editing Network Interface Settings 99
    Deleting a Network Interface 100
    Resetting a Network Interface MAC Address 100
  Changing Ownership of Virtual Machine Templates 100
  Deleting Virtual Machine Templates 101

6 Working with Configurations 103
  Accessing Configurations 104
    Accessing the Workspace Page 104
    Accessing the Library Page 105
  Creating Configurations 106
  Importing Configurations from an SMB Share 109
  Cloning Configurations 110
    Cloning Workspace Configurations 110
    Cloning Library Configurations 111
  Viewing Configuration Virtual Machines and Networks 112
    Viewing Configuration Virtual Machines 112
    Viewing Configuration Networks 114
    Viewing Configuration Diagrams 115
  Changing the Virtual Machines in a Configuration 115
    Adding a Virtual Machine to a Configuration 115
    Removing a Virtual Machine from a Configuration 116
    Moving Virtual Machines to Another Configuration 117
  Changing the Networks in a Configuration 118
    Adding a Network to a Configuration 118
    Removing a Network from a Configuration 118
    Forcibly Removing a Network from a Configuration 119
Deploying Configurations 119
  Deploying a Configuration with Default Settings 120
  Deploying a Configuration with Custom Settings 120
  Deploying Configurations on High Availability Clusters 122
Working with Configuration Snapshots 123
  Taking a Configuration Snapshot 123
  Reverting to a Configuration Snapshot 123
  Deleting a Configuration Snapshot 123
Saving Configurations to the Library 124
  Adding a Configuration to the Library 124
  Cloning a Library Configuration to the Workspace 125
  Creating a LiveLink to a Configuration 126
  Deploying a Configuration from a LiveLink 126
Sharing Configurations 127
Managing Configurations 128
  Stopping Configurations 128
    Suspending a Configuration 128
    Resuming the Operation of a Suspended Configuration 128
    Powering Off a Configuration 129
    Powering On a Configuration 129
    Resetting a Configuration 129
  Undeploying Configurations 129
  Exporting Configurations 130
  Discarding State for Configurations 130
  Modifying Configuration Properties 131
  Changing Ownership of Configurations 132
  Deleting Configurations 132

7 Working with Media 133
  Accessing the Media Library 134
  Synchronizing the Media Library with Media Store Files 135
  Restricting Access to Media Files 135
  Modifying Media Properties 137
  Changing Ownership of Media Files 137

8 Administering and Monitoring Lab Manager 139
  Monitoring Lab Manager 139
    Viewing the Activity Log 140
    Viewing Job Details 140
    Viewing Deployed Virtual Machines 140
Managing Users, Groups, and Roles 142
  Managing Users 142
    Viewing Users 142
    Adding Users 144
    Disabling and Enabling Users 146
    Removing Users 146
    Modifying User Properties 147
  Viewing User Roles and Organizations 149
  Sending User Notifications 149
  Managing Stranded Users 150
    Viewing Stranded Users 150
    Transferring Ownership of Stranded User Objects 151
  Managing Groups 151
    Viewing Groups 151
    Importing LDAP Groups 152
    Removing Groups 153
    Modifying Group Properties 153
  Managing Roles and Rights 154
    Viewing Roles 155
    Adding Roles 155
    Copying Roles 156
    Deleting Roles 156
    Modifying Role Properties 156
  Managing Organizations 157
    Viewing Organizations 157
    Creating Organizations 157
    Modifying Organization Properties 159
    Disabling Organizations 160
    Removing Organizations 160
  Managing Resources 161
    Managing Resource Pools 162
      Viewing Resource Pools 162
      Attaching and Detaching Resource Pools 163
      Enabling and Disabling Resource Pools 164
      Modifying Resource Pool Properties 164
      Undeploying All Virtual Machines in a Resource Pool 165
Managing Hosts 165
  Viewing Hosts 165
  Preparing and Unpreparing Hosts 167
  Enabling and Disabling Hosts 168
  Modifying Host Properties 168
  Viewing Deployed Virtual Machines on a Host 169
  Undeploying All Virtual Machines on a Host 171
Managing Datastores 172
  Viewing Datastores 172
  Removing Datastores 173
  Enabling and Disabling Datastores 174
  Modifying Datastore Properties 175
  Viewing Virtual Machine Datastore Usage 175
  Viewing Virtual Machine Datastore Directories 177
  Deleting Expired Virtual Machines 179
  Renewing the Storage Lease for an Expired Virtual Machine 179
  Deleting Revert Points 180
  Consolidating a Virtual Machine Based on Datastore Usage 180
  Deleting a Virtual Machine or Configuration Based on Datastore Usage 181
Managing Media Stores 181
  Viewing Media Stores 181
  Adding Media Stores 182
  Synchronizing Media Stores 183
  Enabling and Disabling Media Stores 183
  Changing the Name of a Media Store 184
Managing Physical Networks 184
  Viewing Physical Networks 184
  Adding a Physical Network 185
  Viewing IP Pool Usage for a Physical Network 186
  Adding IP Addresses to the IP Pool of a Physical Network 187
  Removing IP Addresses from the IP Pool of a Physical Network 188
  Modifying Physical Network Properties 188
  Deleting a Physical Network 188
Configuring Lab Manager Settings 189
  Configuring General Settings 189
  Lab Manager Preferences 189
  Email Preferences 191
  System Alerts 192
Lab Manager User's Guide

Configuring LDAP Settings 192
   Locating an LDAP Server 193
   LDAP Connection 193
   LDAP Connector and Schema 195
   LDAP User Attributes 196
   LDAP Group Attributes 196
   Testing LDAP Settings 196
Viewing Capacity License Information 196
   Adding a Lab Manager Server Capacity License 196
Configuring Guest Customization Settings 197
Configuring SupportLink Settings 197
Configuring Resource Cleanup Settings 198
Configuring VirtualCenter Settings 199
Managing VirtualCenter and Datacenters 199
   Credential Requirements for Connecting Lab Manager to the VirtualCenter
   Server 201
Performing “Force” Operations 203
   Undeploying Virtual Machine Templates with Force 203
   Undeploying Virtual Machines with Force 204
   Deleting Published Virtual Machine Templates with Force 204

A Roles and Rights 207
   Datastore Rights 208
   General Rights 208
   Group Rights 209
   High I/O Rights 209
   Host Rights 210
   Library Configuration Rights 211
   Machine Rights 211
   Media Rights 212
   Media Store Rights 213
   Navigation Bar Rights 214
   Network Template Rights 215
   Organization Rights 215
   Physical Network Rights 216
   Resource Pool Rights 216
   Role Rights 217
   Sharing Rights 217
Contents

User Rights 218
Virtual Machine Template Rights 219
Workspace Configuration Rights 219

B Client and Browser Support 221

C Guest Operating System Support 225

D Network Fencing 229
   When to Fence Configurations 229
   Understanding Fencing 230
      Fencing Options 231
         Processor Type Incompatibility 234
      Viewing Virtual Switches for Fences 234

E Extending Guest Customization 235
   How Does Guest Customization Work? 235
      Extending Guest Customization 236

Glossary 237

Index 251
About This Book

The Lab Manager User’s Guide describes VMware® Lab Manager and its components, commands, operations, configuration, and user interface.

Intended Audience

The guide is intended for experienced developers and testers of software applications. This document assumes that the user has some familiarity with the following:

- Virtual machine technology
- Basic concepts of distributed, multitiered systems
- Current development and testing practices
- Windows and Linux operating systems

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 versions of this book and other books, go to:

http://www.vmware.com/support/pubs
Online and Telephone Support

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.html

Support Offerings

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/
Introducing Lab Manager

VMware Lab Manager is an application that runs on top of VMware Infrastructure and creates and manages ESX virtual machines. Using Lab Manager, you can create a shared virtual machine library that stores multimachine configurations in state and as a unit. Lab Manager can quickly create copies of virtual machines and run identical copies of the same virtual machine on the same network.

Lab Manager users access the library through a Web browser. Lab Manager does not require extensive knowledge of virtualization and allows users to quickly provision, share, and tear down multimachine test cases or configurations.

This chapter covers these topics:

- “Lab Manager Components” on page 16
- “Lab Manager Benefits and Features” on page 17
- “Understanding Lab Manager in the VMware Infrastructure Environment” on page 18
Lab Manager Components

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

Figure 1-1. Lab Manager Components

The Lab Manager Server provides Web and SOAP interfaces for the Lab Manager Server system.

Lab Manager client users can access the Lab Manager Web console using Microsoft Internet Explorer or Mozilla Firefox.

The Lab Manager SOAP API enables users to access Lab Manager programmatically. This allows easy integration with build management systems and with automated testing tools. See the Lab Manager SOAP API Guide.
The Lab Manager Server manages and deploys virtual machine configurations against a collection of ESX Server resource pools and shared storage attached to a VirtualCenter Server. For more information about how Lab Manager works with VirtualCenter, see “Understanding Lab Manager in the VMware Infrastructure Environment” on page 18.

Lab Manager media servers (media stores) provide users access to the operating systems and applications they need, without requiring the user to know where the media files are stored.

**Lab Manager Benefits and Features**

Lab Manager enables users to lower development, test, and integration costs, as well as tap into a shared pool of resources, eliminate manual setup, and decrease software development times.

Review these specific benefits:

- **Productivity** – Saves time when provisioning machines.
- **Process improvement** – Assists with communication between testing and development teams.
- **Server consolidation** – Includes pool and share servers, storage, and other testing and development resources.
- **Computer access** – Provides access to more computers than available physical machines.
- **Self-help** – Allows engineers to individually create, set up, and tear down configurations without relying on IT.
- **Outsourcing and distributed development** – Allows geographically dispersed teams to work on the same machines and configurations over the Internet.

Review these specific features:

- **Virtual Machine Templates** – Create new, fully configured virtual machines in seconds.
- **Configurations** – Run, manage, and monitor multiple configurations simultaneously.
- **Configuration library** – Store configurations to persistent storage for team use.
- **State capture** – Capture the live state of all the machines in a configuration. You can capture and share bugs in their running state.
- **Network fencing** – Run copies of configurations with identical network profiles simultaneously using this network isolation technology.
Resource management – Manage a pool of computing and storage resources.

Delta tree management – Save virtual machine file changes to efficient and high-performance storage.

Application integration – Integrate test applications with the Lab Manager SOAP API.

Monitoring – View and control server farm utilization in real time.

Browser access – Remotely access Lab Manager from any location.

Automation – Automate test matrices end-to-end.

Understanding Lab Manager in the VMware Infrastructure Environment

Lab Manager is an application that resides on and uses the VMware Infrastructure product.

VMware ESX provides resources to run the virtual machines. Lab Manager manages the ESX hosts through the VirtualCenter Server and the Lab Manager agent installed on those hosts.

VMware VirtualCenter Server is a control point for the datacenter and provides datacenter services such as access control, performance monitoring, and configuration. VirtualCenter also provides advanced VMware Infrastructure capabilities described in “Using VMware Infrastructure Capabilities” on page 19. ESX hosts continue to function even if the VirtualCenter Server becomes unreachable (for example, the network connection is severed).

Using Clusters, Hosts, Resource Pools, and Datastores

In the VirtualCenter Server, you can view, configure, and manage the following key elements:

- Computing and memory resources called hosts, clusters, and resource pools
- Storage resources called datastores
- Networks
- Virtual machines

See the VMware Infrastructure 3 documentation at http://www.vmware.com/support/pubs/vi_pages/vi_pubs_35.html
Hosts, clusters, and resource pools provide flexible ways to organize the aggregated computing and memory resources in the virtual environment and link them back to the underlying physical resources.

- A host represents the aggregate computing and memory resources of a physical x86 server.
- A cluster acts and can be managed much like a host. It represents the aggregate computing and memory resources of a group of physical x86 servers sharing the same network and storage arrays.
- Resource pools are partitions of computing and memory resources from a single host or a cluster. With VMware Distributed Resource Scheduler, these pools can be hierarchical and nested.

**Using VMware Infrastructure Capabilities**

Lab Manager uses VMware Infrastructure capabilities such as VMware VMotion™, VMware DRS, and VMware High Availability (HA). These are distributed services that enable efficient and automated resource management and high virtual machine availability.

Lab Manager works with virtual machines registered with VirtualCenter and VMware Infrastructure admission controls. For more information about VirtualCenter, see the VMware Infrastructure 3 documentation at http://www.vmware.com/support/pubs/vi_pages/vi_pubs_35.html
To get started with Lab Manager, it is important to be familiar with the main elements and operations of the Lab Manager Web console.

This chapter includes these topics:

- “Setting Browser Options” on page 21
- “Accessing the Lab Manager Web Console” on page 22
- “Viewing Performance, Usage, and Support Information” on page 22
- “Using the Interface” on page 24
- “Setting User Preferences” on page 25
- “General Workflow in Lab Manager” on page 27

Setting Browser Options

Review the requirements for client machines accessing the Web console in the Lab Manager Installation and Upgrade Guide. The supported browsers and operating systems are listed in Appendix B, “Client and Browser Support,” on page 221.

If you are using Internet Explorer, enable the browser settings described in the Lab Manager Installation and Upgrade Guide.
Accessing the Lab Manager Web Console

You can use either Internet Explorer or Firefox to access the Lab Manager Web console. For information on supported versions, see Appendix B, “Client and Browser Support,” on page 221.

You must have a user account that is set up by a Lab Manager administrator to log in to the Web console.

To access the Lab Manager Web console

1 On a Windows machine connected to the Internet or your local intranet, open a browser window.

2 To connect to a Lab Manager Server system, navigate to https://<Lab_Manager_Server_domain_name_or_IP_address>

   The first time you access the console, an SSL warning might appear. To avoid this warning, use a fully qualified domain name (FQDN) or ask the Lab Manager administrator for more information. An FQDN starts with the computer name followed by the DNS suffix (for example, computer_name.mydomain.com).

   To add the certificate to your trusted certificate list in Internet Explorer, click View Certificate in the SSL alert, and click Install Certificate. For information about generating a custom SSL certificate, see the Lab Manager Installation and Upgrade Guide.

3 Enter your user name and password and click Login.

   Lab Manager displays the Web console. If Lab Manager displays an error, talk to 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.

Viewing Performance, Usage, and Support Information

The Overview page is the default landing page in the Web console.

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

NOTE A Lab Manager administrator must enable SupportLink if you want to view all statistics. See “Configuring SupportLink Settings” on page 197.
To view performance, usage, and support information

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

The **Performance Summary** column includes this information:

- **Server Pool Deployments This Month** – Graphical view of virtual machine deployment for the current month.
- **Total Slots** – Number of reserved spaces across all virtual machines on the hosts.
- **Slots Used** – Number of deployed machines.
- **Slots Available** – Difference between **Total Slots** and **Slots Used**.
- **Maximum Memory** – Physical memory of the hosts.
- **Total Deployments Over Time** – Sum of all deployed virtual machines since the installation of Lab Manager.
- **Configurations in Library** – Number of virtual machine configurations stored in the configuration library.
- **Total VM Storage** – Sum of the disk space in datastore storage.
- **VMs under management** – Number of virtual machines (except routers) under Lab Manager control.
- **Disk Space used per VM** – Average disk space for each virtual machine.
  
  This entry assumes you are using dedicated datastore disk space for Lab Manager virtual machines.

The **My Lab Manager** column includes this information:

- **My Deployed VM Quota** – Number of virtual machines you are allowed to deploy. The administrator sets that limit when adding a user to Lab Manager.
- **My Stored VM Quota** – Number of virtual machines you are allowed to store. The administrator sets that limit when adding a user to Lab Manager.
- **My VMs Deployed** – Number of your deployed virtual machines.
- **My VMs Stored** – Number of virtual machines stored in the Workspace, configuration library, and virtual machine template library.

The **Documentation & Support** column provides access to documentation, video tutorials to become familiar with the product, and customer support.
You can specify a new default landing page.

**To specify the default landing page for the Web console**

- Select the **Open Workspace at Startup** check box to open the Workspace page instead of the Overview page when you launch the Web console.
- Specify a default landing page in your user preferences. See “Setting User Preferences” on page 25.

**Using the Interface**

The Lab Manager interface includes features such as pop-up menus and filters.

**Using Pop-Up Menus**

The console has pop-up menus that are similar to right-click menus and appear when you move the pointer over an object name. A name or title has a pop-up menu if an arrow appears to its right.

**To use a pop-up menu**

1. Move the pointer over an object name (for example, a virtual machine template). Lab Manager displays a menu.
2. Click an item in the menu.

**Using Text Search Filter**

Use the **Filter** button at the top of certain pages to view a subset of the information on the current page. If a page includes a long list of items, filtering can help you find the items you need. If you apply a filter to a page view, Lab Manager remembers that filter the next time you view the page. Clear the filter to view the complete list.

**To filter a page view**

On a page that supports filter, enter text in the Filter text box and click **Filter**. Lab Manager searches for objects that include the filter text in any searchable column and displays the matching objects.

Filter text is not case-sensitive. The filter text search does not recognize wildcards. If you enter a traditional wildcard, such as an asterisk (*), this function performs a literal search for an asterisk symbol.
Use the pop-up menu to the left of the Filter text box to filter based on the content of a specific column. The pop-up menu lists all searchable columns.

**To clear a page view filter**

Click clear filter.

### Using Column Sorting

Most pages in Lab Manager present data in tables. You can sort the data in each column in ascending or descending order.

**To sort a column**

Click a column heading name to sort the table.

The arrow to the right of the column name indicates whether the data appears in descending or ascending order.

### VMware Tools and Mouse Control

When moving your mouse in to and out of the virtual machine console window, you might lose the pointer. VMware Tools corrects this problem.

For details on VMware Tools, see “Installing VMware Tools” on page 74. If VMware Tools is not installed, press Ctrl + Alt to regain mouse control.

### Setting User Preferences

Each user can specify their own preferences for certain display and deployment options. These preferences are used in all of the user’s organizations.

### Set Display, Deployment, and Lease Alert Preferences

The **Defaults** tab includes default display, deployment, and lease alert preferences.

**To set display, deployment, and lease alert preferences**

1. Click the **Preferences** link in the upper-right corner of any page (next to the **Logout** link).

2. Click the **Defaults** tab.

3. Specify your display preferences:
   a. Choose the first page that appears when you log in to the Web console.
      The Overview page is the default setting.
b) Deselect the Show Page Header check box to prevent the display of the information that appears at the top of each page.

This information includes IP addresses, virtual machine descriptions, and snapshot thumbnails. Removing the header gives you more room to view the console.

c) Enter the number of rows to display on pages with data in tabular format.

The maximum number is 500. The default number is 20.

4 Specify your default deployment options:

a) Deselect the Use Server Boot Sequence check box if you do not want to use the assigned boot order to boot virtual machines in a configuration.

b) Set the default value for the delay time (or pause) between booting each virtual machine in a configuration.

Lab Manager uses this default value when you create a new configuration or adds a virtual machine to an existing configuration.

5 Specify your lease expiration alert preferences:

a) Request an email notification before a virtual machine template or configuration is undeployed. Specify the amount of time prior to expiration that you want Lab Manager to send the email.

b) Request an email notification before a virtual machine template or configuration is deleted or marked for deletion (depending on how the administrator has configured Lab Manager). Specify the amount of time prior to expiration that you want Lab Manager to send the email.

6 Click OK.

Changing Your User Password

You can only change the password for a user 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 in the upper-right corner of any page (next to the Logout link).

2 Click the Change Password tab.

3 Enter and confirm a new password and click Change Password.

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

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

The next steps might involve adding and synchronizing media stores, creating organizations, and adding users and groups to those organizations.

Once 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 configurations and their virtual machines in the Workspace, and save a configuration to the Library to share it with other users. For example, if a QA engineer is working with a configuration and finds a bug, the engineer can save it to the Library to preserve its current state. The QA engineer can then create a LiveLink to the configuration and send the LiveLink URL to a developer. The developer can now access and review the “live” configuration in the Workspace.

The following chapters provide more details on all of these operations.

You can also watch the Lab Manager videos to learn about some of the most common Lab Manager operations.

To access the Lab Manager videos

1. In the left pane of the Lab Manager Web console, click Overview.

2. Click Videos.
A network template is the 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 administrators, organization administrators, and template creators to predefine the virtual networks available for other users. A network template provides a level of control and consistency across the Lab Manager installation or within an organization.

Network templates are created and owned by a specific user, but they can be shared with other users in an organization or across the entire Lab Manager installation.

By default, only administrators, organization administrators, and template creators, can create and manage network templates. Application owners can only view network templates. To provide access to other users, see “Managing Roles and Rights” on page 154.

This chapter includes these topics:

- “Accessing the Network Templates Page” on page 30
- “Creating Network Templates” on page 31
- “Copying Network Templates” on page 33
- “Sharing Network Templates” on page 33
- “Modifying Network Template Properties” on page 35
Accessing the Network Templates Page

The Network Templates page displays a table listing network templates and providing basic information about the properties of each network template.

Use this page to add network templates to the Lab Manager environment. From the table, users with the necessary rights can copy, share, delete, and modify network templates.

To view network templates

In the left pane, click Network Templates.

A table presents basic information about each network template:

- The network template name with a pop-up menu to perform various operations on the network template.
- IP address of the default gateway for the network template.
- Subnet mask for the network template.
- Primary DNS for the network template.
- IP addressing modes available to the network template.
- The number of IP addresses defined in the network template’s IP Pool (if applicable).
- The owner of the network template.
- The organization under which the network template was created.
- Sharing information, indicating whether the network template is shared among users. Private network templates are only available to the owners.
- Total number of IP addresses in the IP pool (for networks that support IP pool).

See “Using Text Search Filter” on page 24 for information on using the Filter feature.
Chapter 3 Working with Network Templates

In the top left corner, use the drop-down menu to determine the network templates that appear on the page:

- **My Network Templates**—View only your network templates, both shared and private. This option displays all your network templates in the selected organization.

- **All Network Templates**—View your network templates, both shared and private, and network templates shared by others. This option displays all network templates in the selected organization that are available to you.

  Administrators can choose **All Network Templates** in the Global organization to view all network templates in the entire Lab Manager installation.

- **My Network Templates in Other Organizations**—This option displays all your network templates in organizations other than the selected organization. This option is not available from the Global organization or for users that are members of a single organization.

### Creating Network Templates

By default, only administrators, organization administrators, and template creators can create network templates. To provide access to other users, see “Managing Roles and Rights” on page 154. After creating a network template, you can use it to create other network templates by copying and modifying the original network template.

Use the procedure below to create a new network template in the current organization. The user who creates the network template becomes its owner.

**To create a new network template**

1. On the Network Templates page, click **New Network Template**.
2. Type a name for the network template.
3. (Optional) Type a description.
4 Select the IP addressing modes available to the network template:

- **Static - IP Pool** allows Lab Manager to pull static IP addresses from the network template IP pool.

- **DHCP** allows Lab Manager to pull IP addresses from a DHCP server. This option avoids preparing and specifying an IP address or IP range. However, you cannot connect virtual networks that use DHCP to physical networks.

- **Static - Manual** requires you to specify a static IP address when configuring the network interface for a virtual machine based on this network template. The IP address you specify cannot belong to the network template IP pool. However, if you want to connect a virtual network based on the network template to a physical network, you must have IP addresses in the IP Pool for use as virtual machine external IP addresses.

   If you select a static IP address mode, you need to enter the static mode settings and create an IP pool, otherwise skip to Step 7.

5 Enter the static mode settings:

   a Enter a subnet mask.

   b Enter a default gateway.

   c Enter a primary DNS.

   d (Optional) Enter a secondary DNS.

   e (Optional) Enter a DNS suffix.

6 Type an IP address or range and click the plus Add button to add IP addresses to the IP pool.

   You can add multiple IP addresses or ranges (contiguous or not).

   To remove an IP address or range, select the address or range and click the Remove button.

   To modify an IP address or range, select the address or range, modify it and click the Modify button.

7 Click OK.
Copying Network Templates

You can copy an existing network template to create a new network template and modify it as needed.

Lab Manager creates the new network template in the organization currently selected in the Organization drop-down menu. The user performing the copy operation becomes the owner of the new network template.

To copy an existing network template
1 On the Network Templates page, move the pointer over the network template name and choose Copy from the menu.
   Lab Manager creates an exact copy of the original network template with “(Copy)” appended to the name.
2 Modify the network template settings and click Copy.

Sharing Network Templates

When a user creates a network template in Lab Manager, the user becomes its owner. The owner, or a user with the Administrator View and Control right, can give other users access to the network template.

NOTE By default, only administrators and organizations administrators have the Administrator View and Control right.

Owners can share objects to all or specific users in the following ways, depending on their rights:

- Across the entire Lab Manager installation
- Across an organization
- Within an organization

By default, administrators and organization administrators can share in all three ways. All other types of users (except view only) can only share within their own organization.
To share a network template with other users

1 On the Network Templates page, move the pointer over the network template name and choose *Sharing* from the menu.

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

2 Click *Add Users*.

3 Choose the organization containing the users with whom you want to share the network template or choose *Global* to view users from all organizations.

4 Select who you want to share the network template with:
   - **Everyone** to share the network template with all users in the selected organization.
   - **Selected Users** to share the network template with specific users in the selected organization.

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

   When you share a network template with a specific user in an organization, the user only has access to the network template in that organization. To share a network template with a user in all the organizations to which the user belongs, choose the *Global* organization.

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

Access rights combine with a user’s existing rights to determine how the user can interact with the shared network template. Access rights cannot provide users with rights that they don’t already have based on their role.

If you are sharing the network template with users in an organization other than the one in which the network template was created, you can only grant *Read* access. Network templates created in the Global organization can only be shared with *Read* access.

6 Click *Done*. 
Modifying Network Template Properties

By default, only administrators, organization administrators, and template creators can view and edit the properties of a network template. For information on the properties, see “Creating Network Templates” on page 31.

You can also change the network template owner. See “Changing Ownership of Network Templates” on page 35.

To modify network template properties
1. On the Network Templates page, move the pointer over the network template name and choose Properties from the menu.
   You can also click the network template name.
2. Modify the properties and click Update.

Changing Ownership of Network Templates

The original owner of a network template is the user who created it. You can change the owner to assign a network template to another user in the same organization as the current owner.

To change ownership of a network template
1. On the Network Templates page, move the pointer over the network template name and choose Properties from the menu.
2. Click Change Owner.
3. Choose a new owner for the network template and click OK.
4. Click Update.

Deleting Network Templates

By default, only administrators, organization administrators, and template creators can delete network templates. After you delete a network template, you can no longer choose it as the basis for a virtual machine template or virtual machine network interface, or add it to a configuration. Existing virtual machines and configurations that rely on 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, click Network Templates.
2. Move the pointer over the network template name and choose Delete from the menu.
3. Click OK to confirm the deletion.

Viewing IP Pool Usage for a Virtual Network

You can monitor the IP pool of a virtual network that is based on a network blueprint. If a virtual network is running out of IP address, you can add more. See “Adding IP Addresses to the IP Pool of a Virtual Network” on page 37.

Every virtual machine using a static IP addressing mode for a NIC 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 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 “Lab Manager Preferences” on page 189.

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, click Workspace.
2. Move the pointer over a configuration name and choose Open from the menu.
3. In the Networks tab, move the pointer over a virtual network name and choose IP Pool from the menu.

   The IP Pool tab 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. You can see the IP address, addressing mode, machine name, configuration name, and organization and user. The Deallocate In column indicates the amount of time remaining before an unused external IP address becomes available.
Adding IP Addresses to the IP Pool of a Virtual Network

By default, only administrators, organization administrators, and template creators can add IP addresses to a virtual network.

**To add IP addresses to a virtual network**

1. In the left pane, click Network Templates.
2. Move the pointer over a network template name and choose Properties from the menu.
3. Type an IP address or IP address range in the Static IP Address Pool text box and click the Add button.
   - Lab Manager adds the IP addresses to the IP pool.
4. Click Update.

Removing IP Addresses from the IP Pool of a Virtual Network

By default, only administrators, organization administrators, and template creators can remove IP addresses from a virtual network.

**To remove IP addresses from a virtual network**

1. In the left pane, click Network Templates.
2. Move the pointer over a network template name and choose Properties from the menu.
3. Type 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 the Remove button.
   - Lab Manager removes the IP addresses from the IP pool.
4. Click Update.
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 are based on virtual machine templates that contain guest operating systems, application servers, databases, directory servers, and other infrastructures. For information on virtual machine templates, see “Working with Virtual Machine Templates” on page 61.

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

This chapter includes these topics:

- “Viewing the Virtual Machines in a Configuration” on page 40
- “Deploying Virtual Machines” on page 41
- “Undeploying Virtual Machines” on page 43
- “Discarding State for Virtual Machines” on page 44
- “Consolidating Virtual Machines” on page 44
- “Modifying Virtual Machine Properties” on page 45
- “Viewing a Virtual Machine Console” on page 53
- “Working in a Virtual Machine Console” on page 54
- “Working with BEA LiquidVMs” on page 60
Viewing the Virtual Machines in a Configuration

You can access virtual machines from the Workspace and Library pages.

On the Virtual Machines tab on the Workspace page, you can perform operations ranging from consolidating a virtual machine to viewing its properties. On the Virtual Machines tab on the Library page, you can only consolidate a virtual machine or edit its storage lease. The options in the pop-up menu for a virtual machine are contingent upon its state.

Virtual machine operations generally do not affect the guest operating system running on a virtual machine. However, editing virtual machines properties can affect the guest operating system.

To view the virtual machines in a configuration

1. In the left pane, click Workspace or Library.
2. Move the pointer over a configuration name and choose Open from the menu.
3. Click the Virtual Machines tab.

Lab Manager displays information about some of the properties of each virtual machine in the configuration, in addition to the following:

- **Console** – Displays a thumbnail icon of the virtual machine console.
- **Status** – Lists the status (deployed or undeployed) of the virtual machine.
- **External IP** – Provides the external IP address for the virtual machine if it requires one.
- **VM Template** – Indicates the virtual machine template that the virtual machine is based on.
- **Host** – Indicates the ESX 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.
  
  This column only appears for Workspace configurations.

You can modify the properties of any virtual machine in the configuration. See “Modifying Virtual Machine Properties” on page 45.
Deploying Virtual Machines

Deploying a virtual machine registers it with a resource pool and provides access to Lab Manager operations at the virtual machine console level.

This operation involves specifying a deployment lease. See “Configuring Resource Cleanup Settings” on page 198.

When you deploy an individual virtual machine from a configuration, Lab Manager deploys all physical and virtual networks associated with the configuration using the network connectivity options you select, regardless of whether the specific virtual machine you are deploying 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 deploy an individual 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. On the Workspace page, move the pointer over a configuration name and choose Open from the menu.
2. On the Virtual Machines tab, move the pointer over a virtual machine name, and choose Deploy from the menu.
3. Select the Fence Virtual Machines check box and choose 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 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 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.
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.

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

a Choose a physical network to connect to.

b Choose 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 to machines on the selected physical network, and can receive messages back on the same connection. Machines on the selected physical network cannot initiate communication to virtual machines inside the configuration.

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

6 To prevent Lab Manager from turning on virtual machines immediately after deployment, deselect the Power On Machines After Deployment check box.

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

7 Select the Force Re-customization check box to recustomize the virtual machine.

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 79.

8 Specify a time to undeploy the virtual machine and click OK.
Deploying Virtual Machines on High Availability Clusters

If you deploy a virtual machine on a cluster with VMware HA, Lab Manager uses the same calculation that VirtualCenter has for assessing free slots available in the cluster. After assessing that the hosts have enough resources, Lab Manager powers on the virtual machines. If the hosts do not meet compatibility requirements, the deploy operation fails and Lab Manager displays a message.

If you experience a failure, you need to reconfigure the resources. For information about resource management, see the Resource Management Guide for VMware Infrastructure 3.

The calculation that VirtualCenter and Lab Manager uses is conservative. If necessary, disable it in VirtualCenter to stop this calculation in Lab Manager.

To disable the calculation

1 Log in to the VMware Infrastructure Client (VI Client).
2 Right-click the cluster and select Edit Settings.
3 In the left pane of the dialog box, select VMware HA.
4 In the Admission Control section of the dialog box, select Allow virtual machines to be powered on even if they violate availability constraints and click OK.

Undeploying Virtual Machines

Undeploying a virtual machine unregisters it from VirtualCenter. You can undeploy a virtual machine and save its state or undeploy a virtual machine and discard the 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.

If an ESX host goes offline or someone manually removes a virtual machine from VirtualCenter inventory, the standard undeploy operation does not work. In these situations, see “Undeploying Virtual Machines with Force” on page 204.

To undeploy a virtual machine

1 On the Workspace page, move the pointer over a configuration name and choose Open from the menu.
2 On the Virtual Machines tab, move the pointer over the machine name and choose Undeploy - Save State or Undeploy - Discard State from the menu.

If the virtual machine is powered off, you can only choose Undeploy because no state information is available to save or discard.
Discarding State for Virtual Machines

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. On the Workspace page, move the pointer over the configuration name and choose Open from the menu.
2. On the Virtual Machines tab, move the pointer over the undeployed machine name and choose Discard State from the menu.
3. Click OK to confirm.

Consolidating Virtual Machines

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 Even if you do not have to consolidate disks, you can use this operation to move a virtual machine to a different datastore.

Consolidating a virtual machine and 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.

For information about how Lab Manager administrators can consolidate a virtual machine from the resource management area of the Web console, see “Consolidating a Virtual Machine Based on Datastore Usage” on page 180.

You can consolidate virtual machines in both Workspace and Library configurations.
To consolidate a virtual machine

1. On the Workspace or Library page, move the pointer over the configuration name and choose Open from the menu.
2. If the virtual machine is deployed, undeploy it.
3. On the Virtual Machines tab, move the pointer over the virtual machine name and choose Consolidate from the menu.
4. Choose a datastore for the consolidated virtual machine and click OK.

By default, Lab Manager selects the current datastore of the virtual machine.

Modifying Virtual Machine Properties

For virtual machines in Workspace configurations, you can modify many of the virtual machine properties. 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.

If a virtual machine is deployed, the number of properties you can modify is limited.

For information about modifying virtual machine hard disks and network interfaces, see “Modifying Virtual Machine Hard Disks” on page 48 and “Modifying Virtual Machine Network Interfaces” on page 49.

To modify virtual machine properties

1. On the Workspace page, move the pointer over the configuration name and choose Open from the menu.
2. On the Virtual Machines tab, move the pointer over the virtual machine name and choose Properties from the menu.
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 15 characters.
   - Description – (Optional) Maximum number of characters is 128.
   - Number of Virtual CPUs – Maximum number of processors is four.

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 choose 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.

- **Guest OS** – If you select a 64-bit guest operating system, the datastore must be connected to an ESX 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 VMware Infrastructure 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 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 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:**
  - **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 Reserved (Mhz)** – Minimum amount of CPU set aside for the virtual machine.
  - **CPU Limit (Mhz)** – Maximum amount of CPU available for the virtual machine.
  - **Unlimited** – Select this check box to set no CPU limit.

See the VMware Infrastructure documentation for details on CPU priorities, shares, reservations, and limits.

- **Memory information:**
  - **Memory (MB)** – Amount of RAM allocated for running 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 Reserved (MB) – Minimum amount of memory set aside for the virtual machine.

Memory Limit (MB) – Maximum amount of memory available for the virtual machine.

Unlimited – Select this check box to set no memory limit.

See the VMware Infrastructure documentation for details on memory priorities, shares, reservations, and limits.

Use Time Synchronization – Enables time synchronization between the guest (virtual machine) and ESX 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 choose None.

To use Microsoft Sysprep, you must first create a Microsoft Sysprep package for guest customization. See “Building a Microsoft Sysprep Package” on page 80.

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 VirtualCenter activity that could raise errors in Lab Manager. Click Clear All to remove system messages.

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.

Adding 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. On the Workspace page, move the pointer over the configuration name and choose Open from the menu.
2. On the Virtual Machines tab, move the pointer over the virtual machine name and choose Properties from the menu.
3. In the Hard Disk section, click Add Hard Disk.
4. Specify whether the bus type is BusLogic SCSI or LSI Logic SCSI.
5. Choose a bus number.
6. Choose a bus ID.
7. Enter the disk size (GB) and click OK.
8. Click Update.

Adding SCSI Virtual Hard Disks

If you add a SCSI hard disk to a virtual machine, you might generate an operating system error message about missing drivers for this device. If this error occurs, download and install the appropriate driver, and contact VMware for further support.

Editing 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. On the Workspace page, move the pointer over the configuration name and choose Open from the menu.
2. On the Virtual Machines tab, move the pointer over the virtual machine name and choose Properties from the menu.
3 In the Hard Disk section, click Edit.
4 Modify the bus number and bus ID and click OK.
5 Click Update.

Deleting a Virtual Machine Hard Disk
You can delete a virtual machine hard disk.

To delete a virtual machine hard disk
1 On the Workspace page, move the pointer over the configuration name and choose Open from the menu.
2 On the Virtual Machines tab, move the pointer over the virtual machine name and choose Properties from the menu.
3 In the Hard Disk section, click Delete.
4 Click OK to confirm.
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.

Editing 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 On the Workspace page, move the pointer over the configuration name and choose Open from the menu.
2 On the Virtual Machines tab, move the pointer over the virtual machine name and choose Properties from the menu.
3 In the Network Interfaces section, change any of the following settings:

- 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 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 “Adding a Network to a Configuration” on page 118.

- 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.

- Choose 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** allows Lab Manager to pull static IP addresses from the IP address pool.
  - **DHCP** allows Lab Manager to pull 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** as the IP addressing mode, type an IP address in the **IP Address** field.

4 Click **Update**.
Resetting 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. On the Workspace page, move the pointer over the configuration name and choose **Open** from the menu.
2. On the **Virtual Machines** tab, move the pointer over the virtual machine name and choose **Properties** from the menu.
3. In the Network Interfaces section, choose **Reset** from the **MAC Address** drop-down menu for the network interface you want to update.
4. Click **Update**.

Adding a Network Interface

You can add one or more virtual NICs to an undeployed virtual machine. A single virtual machine can have up to four NICs.

To add a network interface

1. On the Workspace page, move the pointer over the configuration name and choose **Open** from the menu.
2. On the **Virtual Machines** tab, move the pointer over the virtual machine name and choose **Properties** from the menu.
3. In the Network Interfaces section, 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 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 “Adding a Network to a Configuration” on page 118.
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 Choose 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** allows Lab Manager to pull static IP addresses from the IP address pool.
- **DHCP** allows Lab Manager to pull 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** as the IP addressing mode, type an IP address in the IP Address field.

5 Click **Update**.

Lab Manager generates a MAC address for the network interface.

**Deleting a Network Interface**

You can delete virtual NICs from an undeployed virtual machine.

**To delete a network interface**

1 On the Workspace page, move the pointer over the configuration name and choose **Open** from the menu.

2 On the **Virtual Machines** tab, move the pointer over the virtual machine name and choose **Properties** from the menu.

3 In the Network Interfaces section, click **Delete**.

4 Click **Update**.
Viewing a Virtual Machine Console

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

**To view an individual virtual machine console in a configuration**

1. In the left pane, click **Workspace**.
2. Use one of these methods to access a virtual machine:
   - In the **Console** column, click the thumbnail icon of a deployed virtual machine.
   - Move the pointer over the configuration name and choose **Open** from the menu. From this page, either click the thumbnail icon of a deployed virtual machine or move the pointer over the machine name and choose **View Console** or **Pop Out Console** from the menu.
3. Click in the console to work with the guest operating system.

**To view all virtual machine consoles in a configuration**

1. In the left pane, click **Workspace**.
2. Move the pointer over the configuration name and choose **Show Consoles** from the menu.
3. Click in the console to work with the guest operating system.

**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 choose **View Console** or **Pop Out Console** from the menu.

**Installing the ActiveX Control or VMware Remote MKS Plug-In**

In order to view virtual machine consoles, you must install either the ActiveX control (for Internet Explorer) or the VMware Remote MKS Plug-in (for Firefox).

The first time you view the console for a virtual machine using Internet Explorer, follow the instructions to install the ActiveX control.

The first time you view the console for a virtual machine using Firefox, the console displays a message about installing the VMware Remote MKS Plug-in.
To install the VMware Remote MKS Plug-in for Firefox

1. Click Install Plugin.
2. Click the Edit Options button in the upper-right corner.
3. Click Allow and click Close.
4. In the virtual console, click Install Plugin.
5. Click Install Now.
6. Close the dialog box and click the refresh button in the Lab Manager page.

For some versions of Firefox, you might have to restart the browser.

Working in a Virtual Machine Console

From the virtual machine console page, you can view information about a virtual machine, work with the guest operating system, and perform operations affecting the guest operating system.

The virtual machine console page displays the internal and external (if applicable) IP addresses of a virtual machine in the upper-left corner of the page. If you take a snapshot of a virtual machine, Lab Manager displays a revert point thumbnail icon of the snapshot in the upper-right corner of the page.

For configuration virtual machines only, the Configuration pop-up menu near the upper-left corner provides access other virtual machines in the same configuration. Click a thumbnail icon to see the console display, or click All Consoles to see all virtual machine consoles in a configuration. Click Configuration to view the details of virtual machines in the configuration.

From the virtual machine console page, you can send the Ctrl+Alt+Del command to the guest operating system and set up a Remote Desktop Connection to a Windows virtual machine.

You can also install VMware Tools. If the VMware Tools is not installed in a virtual machine, you can lose the mouse when navigating into and out of the console window. Press Ctrl+Alt to release the mouse cursor.
Setting Up a Remote Desktop Connection

To connect to a virtual machine remotely, the virtual machine must be running a Windows operating system and have a static IP address. You must also have network access and access permission as a Lab Manager administrator or authorized remote-access user.

To set up a remote desktop connection to a virtual machine
1. From the virtual machine console page of a Workspace configuration virtual machine, click in the console to work with the guest operating system.
2. Open the Control Panel in the guest operating system.
3. Depending on the Windows operating system, enable the remote desktop by installing Terminal Services or by navigating to the Remote tab of the System Properties dialog box.
4. On the virtual machine console page, click the Remote Desktop button.
5. Click Save and specify a location for the Remote Desktop connection file.

To access a virtual machine using Remote Desktop
2. Enter the user name and password for the guest operating system and click OK.

Powering On or Powering Off 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 choose Power On from the menu.

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 choose Power Off from the menu.
**Resetting 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 choose *Reset* from the menu.
2. Confirm the reset operation.

**Shutting 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, you might be using an old version of VMware Tools. In this case, uninstall the existing version and install VMware Tools in Lab Manager. See “Installing VMware Tools” on page 57.

**To shut down a virtual machine**

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

**Suspending and Resuming 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 VirtualCenter.

**To suspend a virtual machine**

From the virtual machine console page, move the pointer over the virtual machine name and choose *Suspend* from the menu.

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 choose **Resume** from the menu.

**Installing VMware Tools**

Lab Manager depends on the VMware Tools utility for customizing the guest operating system. VMware Tools also supports shared folders and cut and paste operations between the guest operating system and the machine from which you launch the Lab Manager Web console.

VMware Tools also allows you to move the pointer into and out of the virtual machine console window. Otherwise, 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 VMware Infrastructure 3 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**.

**Taking A Snapshot of a Virtual Machine**

A snapshot captures the state of a virtual machine at a specific point in time. After deploying a virtual machine, you can take a snapshot and revert the virtual machine to that snapshot at a later time.

Lab Manager stores the snapshot persistently with the virtual machine image. If you undeploy a virtual machine and deploy it, the snapshot remains.

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 choose **Snapshot** from the menu.
Lab Manager turns off the virtual machine for a short time and then displays the console. A thumbnail icon of the snapshot appears in the upper-right corner of the page.

**Reverting to a Virtual Machine Snapshot**

When you revert a virtual machine to a snapshot, the virtual machine loses its current state.

1. **To revert to a snapshot**
   - From the virtual machine console page, move the pointer over the virtual machine name and choose Revert from the menu.
   - Confirm 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. A thumbnail icon of the snapshot appears in the upper-right corner of the page.

**Deleting a Virtual Machine Snapshot**

Virtual machine snapshots, also known as revert points, take up space on datastores. You can free up space by deleting revert points.

1. **To delete a revert point**
   - From the virtual machine console window, move the pointer over the virtual machine name and choose Delete Revert Point from the menu.

**Inserting and Swapping CDs**

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.

1. **To insert a CD into a virtual machine**
   - From the virtual machine console page, move the pointer over the virtual machine name and choose Insert CD from the menu.
   - 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 choose Swap CD from the menu.
2. Select an ISO file from the Lab Manager media library and click OK.

Ejecting CDs

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

To eject the CD from a virtual machine

From the virtual machine console page, move the pointer over the virtual machine name and choose Eject CD from the menu.

Inserting and Swapping Floppy Disks

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 choose Insert Floppy from the menu.
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 choose Swap Floppy from the menu.
2. Select a floppy file from the media library and click OK.

Ejecting Floppy Disks

Inserting a floppy disk to a virtual machine, you can eject the floppy disk.

To eject the floppy disk from a virtual machine

From the virtual machine console page, move the pointer over the virtual machine name and choose Eject Floppy from the menu.
Working with BEA LiquidVMs

Lab Manager supports importing BEA LiquidVMs as virtual machine templates from VirtualCenter or an SMB file server. See “Importing Virtual Machine Templates” on page 66.

After you import a LiquidVM, you must do the following before you can work with a LiquidVM:

- Different versions of the WLS-VE ISO are available for different versions of LiquidVM. Make sure that the media library includes all the versions that you need.
  
  See “Managing Media Stores” on page 181

- 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.
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 quickly and easily create multiple virtual machines based on the virtual machine template without having to reinstall software or redo setup tasks on each virtual machine. Using virtual machine templates ensures that virtual machines are consistently configured across an entire organization.

By default, only administrators, organization administrators, and template creators can create virtual machine templates. These users can create a new virtual machine template, import a virtual machine template, save a Lab Manager virtual machine as a virtual machine template, and clone an existing virtual machine template.

This chapter includes these topics:

- “Accessing the VM Templates Page” on page 62
- “Creating Virtual Machine Templates” on page 64
- “Importing Virtual Machine Templates” on page 66
- “Saving Virtual Machines as Virtual Machine Templates” on page 69
- “Cloning Virtual Machine Templates” on page 70
- “Deploying Virtual Machine Templates” on page 71
- “Installing a Guest Operating System” on page 73
- “Installing VMware Tools” on page 74
- “Customizing the Guest Operating System” on page 79
- “Undeploying Virtual Machine Templates” on page 87
“Sharing Virtual Machine Templates” on page 88
“Publishing Virtual Machine Templates” on page 89
“Managing Virtual Machine Templates” on page 91

Accessing the VM Templates Page

The VM Templates page displays a table listing virtual machine templates and providing basic information about the properties of each virtual machine template.

Use this page to create, import, deploy, export, clone, share, and publish a virtual machine template. You can also access the properties of a specific virtual machine template. The options in the pop-up menu for a virtual machine template are contingent upon its state (for example, deployed or undeployed).

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

To view virtual machine templates

In the left pane, click VM Templates.

A table provides basic information about each virtual machine template:

- **Console** – Provides access to the virtual machine console through the thumbnail icon.
- **Template Name** – Provides a pop-up menu to perform operations on the virtual machine template.

  The options available in the pop-up menu for a virtual machine template depend on its state.

- **Status** – Indicates whether the virtual machine template is deployed, published, or in the midst of such operations as importing, exporting, copying, and cloning.
- **Owner** – Shows the owner of the virtual machine template.
- **Organization** – Shows the organization in which the virtual machine template was created.
- **Sharing** – Indicates whether the virtual machine template is shared among users. Private virtual machine templates are only available to the owners.
VMware Tools – Indicates the status of VMware Tools on the virtual machine template.

If VMware Tools is installed on the virtual machine template and the version meets Lab Manager requirements, **Installed** appears in the **VMware Tools** column.

If VMware Tools is installed on the virtual machine template and the version does not meet Lab Manager requirements, **Installed (Requires Update)** appears in the **VMware Tools** column.

If VMware Tools is not installed on the virtual machine template **Not Installed** appears in the **VMware Tools** column.

If Lab Manager cannot detect whether VMware Tools is installed, **Unknown** appears in the **VMware Tools** column.

For VMware Tool requirements, see “Installing VMware Tools” on page 74.

**Date Deployed** – Shows the date and time of the last deploy operation.

**Messages** – Messages or alerts about VirtualCenter activity that could raise errors in Lab Manager.

See “Using Text Search Filter” on page 24 for information on using the **Filter** feature.

In the top left corner, use the drop-down menu to determine the virtual machine templates that appear on the page:

- **My VM Templates** – View only your virtual machine templates, both shared and private. This option displays all your virtual machine templates in the selected organization.

- **All VM Templates** – View your virtual machine templates, both shared and private, and virtual machine templates shared by others. This option displays all virtual machine templates in the selected organization that are available to you.

  Administrators can choose **All VM Templates** in the Global organization to view all virtual machine templates in the entire Lab Manager installation.

- **My VM Templates in Other Organizations** – This option displays all your virtual machine templates in organizations other than the selected organization. This option is not available from the Global organization or for users that are members of a single organization.
Creating Virtual Machine Templates

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

When you create a blank template you might need to specify the deployment and storage leases. See “Configuring Resource Cleanup Settings” on page 198.

To create a blank virtual machine template

1. On the VM Templates page, click New VM Template.
2. Provide virtual machine template details:
   - **Name** – Can only contain alphanumeric characters (a-z, A-Z, 0-9), hyphens, underscores, or periods. Maximum length is 15 characters.
   - **Description** – (Optional) Maximum number of characters is 128.
   - **Datastore** – Choose a datastore for the virtual machine template.
   - **Guest OS** – This selection prepares the virtual machine template for the actual installation of the guest operating system.
     
     If you select a 64-bit guest operating system, the datastore must be connected to an ESX 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.
     
     For information on enabling an ESX host to provide 64-bit support, see the VMware Infrastructure documentation.
   - **Number of virtual CPUs** – Maximum number of processors is four.
     
     The datastore for this virtual machine template 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.
   - **Memory (MB)** – Amount of RAM allocated for running the virtual machine template.
Chapter 5 Working with Virtual Machine Templates

- **Disk Size (GB)** – The size of the virtual hard disk.
- **Bus Type** – Choose LSI LOGIC or BUS LOGIC.
- **Network** – Choose a physical or virtual network for the virtual machine template.
- **IP Address Mode** – Choose 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** allows Lab Manager to pull static IP addresses from the IP address pool.
  - **DHCP** allows Lab Manager to pull 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.
- **Deployment Lease** – Time to undeploy the virtual machine template.
- **Storage Lease** – Time to delete the virtual machine template or mark the virtual machine template for deletion.

3 Click OK.

Lab Manager creates the virtual machine template in the current organization and displays it on the VM Templates page with an Undeployed and Unpublished status.

You can now deploy the virtual machine template and install a guest operating system, VMware Tools, and applications. Next, make sure the virtual machine template meets the requirements for guest customization and complete the specific steps for Windows NT and Solaris virtual machine templates. Then, you can share the virtual machine template with other Lab Manager users and publish it to make it available to build configurations.
Importing Virtual Machine Templates

Importing a virtual machine template involves copying a virtual machine external to the Lab Manager system into the virtual machine template library. You can import an existing virtual machine from VirtualCenter or SMB storage to serve as a virtual machine template in Lab Manager.

You can import a virtual machine that is new to Lab Manager or was previously exported by Lab Manager. Lab Manager changes the MAC address of all imported virtual machines, except for those in suspended states.

The setup for the virtual machine is primarily stored in these files:

- Virtual machine disk (.vmdk) file – You can have multiple .vmdk files.
- Virtual machine configuration (.vmx for VMware) file – This file is approximately 15KB.

Lab Manager supports these types of virtual machines for import operations:

- VMware Workstation
- VMware Server
- VMware ESX
- BEA LiquidVMs that use static IP mode and DHCP mode, but not “static IP and DHCP” mode, which combines a static IP address with additional information from the DHCP server.

Importing can take an extended period of time depending on the size of the virtual machine. By default, Lab Manager times out import operations that take longer than two hours. To modify the timeout for VirtualCenter and SMB imports, see “Lab Manager Preferences” on page 189.

Importing Virtual Machine Templates from VirtualCenter

If you have an existing virtual machine in a resource pool managed by VirtualCenter, you can import that virtual machine for use as a virtual machine template in Lab Manager.

If a virtual machine has VirtualCenter snapshot files, Lab Manager only imports the original virtual machine as a template and discards any VirtualCenter snapshot files.

Importing a virtual machine template involves specifying a deployment lease and a storage leases. See “Configuring Resource Cleanup Settings” on page 198.
To import a virtual machine template from VirtualCenter

1. In the left pane, click VM Templates.
2. Click the Import VM Template button.
3. Enter a name for the imported virtual machine template.
   The name can only contain alphanumeric characters (a–z, A–Z, 0–9), hyphens, underscores, or periods. The maximum length is 15 characters.
4. (Optional) Enter a description.
5. Select VirtualCenter and choose a virtual machine from the VirtualCenter inventory.
   Blue icons indicate available virtual machines. You can only select virtual machines that are powered off and not already under Lab Manager control.
6. Click Next.
7. Specify the networking information for each NIC in the imported virtual machine template:
   a. Selected the Connected check box to connect the virtual machine template to the network when it is deployed.
   b. Choose a default virtual or physical network.
   c. Choose a default IP addressing mode.

   Lab Manager resets the MAC address for each NIC after the import operation is complete.
8. (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.
9. Specify a time to delete the virtual machine template or mark it for deletion.
10. Specify a time to undeploy the virtual machine template.
11. Choose 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. If you move the virtual machine template it does not.
12 Select the datastore to import the virtual machine template to.

13 Click Import.

Lab Manager imports the virtual machine template into the current organization and displays it on the VM Templates page. The import process takes several minutes.

Importing Virtual Machine Templates from SMB Storage

You can import virtual machines as templates from an SMB share. Do not import virtual machine templates manually with ESX commands.

Importing from SMB requires an open SMB port on the ESX host. Although Lab Manager opens the port during installation, make sure that the port was not closed after the install. To check the port status, use the `esxcfg-firewall -q smbClient` command on each host.

Importing a virtual machine template involves specifying a deployment lease and a storage leases. See “Configuring Resource Cleanup Settings” on page 198.

To import a virtual machine template from SMB storage

1 In the left pane, click VM Templates.

2 Click the Import VM Template button.

3 Enter a name for the imported virtual machine template.

   The name can only contain alphanumeric characters (a–z, A–Z, 0–9), hyphens, underscores, or periods. The maximum length is 15 characters.

4 (Optional) Enter a description.

5 Select SMB File Server and enter the following information:

   a UNC path to the appropriate SMB share (relative to the Lab Manager Server system). 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.

   b If the UNC folder requires authentication, specify the user name and password to access the files.

6 Click Next.
7 Specify the networking information for each NIC in the imported virtual machine template:
   a Select the Connected check box to connect the virtual machine template to the network when it is deployed.
   b Choose a default virtual or physical network.
   c Choose a default IP addressing mode.
      Lab Manager resets the MAC address for each NIC after the import operation is complete.
8 (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.
      You can skip this step if you are importing a virtual machine template that was previously exported from Lab Manager. In that case, Lab Manager can detect whether or not the virtual machine template was set up for customization.
9 Specify a time to delete the virtual machine template or mark it for deletion.
10 Specify a time to undeploy the virtual machine template.
11 Select the datastore to import the virtual machine template to.
12 Click Import.
      Lab Manager imports the virtual machine template into the current organization and displays it on the VM Templates page. The import process takes several minutes.

Saving Virtual Machines as Virtual Machine Templates

You can create a virtual machine template from any virtual machine in Lab Manager. After a virtual machine in a configuration undergoes changes, such as the addition of software or altered properties, you might want to use it as the basis of a new virtual machine template. The new virtual machine template is a linked clone of the original virtual machine.

This operation involves specifying a deployment lease and a storage leases. See “Configuring Resource Cleanup Settings” on page 198.
To create a virtual machine template from an active virtual machine

1. In the left pane, click Workspace.
2. Move the pointer over the configuration name and choose Open from the menu.
3. Click the Virtual Machines tab, move the pointer over the virtual machine name, and choose Add To VM Templates from the menu.
   Lab Manager creates the virtual machine template in the current organization.
4. Specify the details of the virtual machine template and then click OK:
   a. Enter a name.
      The name can only contain alphanumeric characters (a–z, A–Z, 0–9), hyphens, underscores, or periods. The maximum length is 15 characters.
   b. (Optional) Enter a description.
   c. Specify a time to delete the virtual machine template or mark it for deletion.
   d. Specify a time to undeploy the virtual machine template.
5. In the left pane, click VM Templates.
   The VM Templates page appears with the new virtual machine template.

Cloning Virtual Machine Templates

You can create a linked clone or a full clone of a virtual machine template to take advantage of software already installed on that virtual machine template.

A linked-clone operation generates 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 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. A full-clone operation takes longer than a linked-clone operation.

Typically, you do not create full clones, except under these conditions:

- To dismantle the storage and move the virtual machine template to a different server.
- To maximize performance for virtual machines (for example, for certain production-level virtual machines).
You cannot make a full clone of a deployed virtual machine template. Linked-clone and full-clone operations involve specifying deployment and storage leases. See “Configuring Resource Cleanup Settings” on page 198.

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.

**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 choose **Clone** from the menu.
3. Enter a name.
   The name can only contain alphanumeric characters (a–z, A–Z, 0–9), hyphens, underscores, or periods. The maximum length is 15 characters.
4. (Optional) Enter a description.
5. Specify a time to delete the virtual machine template or mark it for deletion.
6. Specify a time to undeploy the virtual machine template.
7. Specify the type of clone:
   - **Linked Clone**
   - **Full Clone**
     You can specify a new datastore for the template.
8. Click **OK**.

   The new virtual machine template appears on the VM Templates page.

**Deploying Virtual Machine Templates**

Deploying a virtual machine template registers it with a resource pool and provides it access to Lab Manager operations at the virtual machine console level. To deploy a template, it must be unpublished.

When you deploy a template, you might need to specify a deployment lease. See “Configuring Resource Cleanup Settings” on page 198.
Deploying a Virtual Machine Template with Default Settings

When you deploy a virtual machine template with default settings, Lab Manager uses the default settings of the virtual machine template and the default deployment options from your user preferences. See “Setting User Preferences” on page 25.

To deploy a virtual machine template with default settings

On the VM Templates page, move the pointer over the virtual machine template name and choose Deploy with defaults from the menu.

The VM Templates page lists the virtual machine template with a Deployed and Unpublished status.

Deploying a Virtual Machine Template with Custom Settings

You can deploy a virtual machine template to a specific resource pool and specify additional deployment options.

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 choose Deploy from the menu.
2.  Select a specific resource pool or 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.
   
   Use this option when you need to manually bring up a virtual machine template.
4.  Specify a time to undeploy the virtual machine template and click OK.

The VM Templates page lists the virtual machine template with a Deployed and Unpublished status.

Deploying Virtual Machine Templates on High Availability Clusters

If you deploy a virtual machine template on a cluster with VMware HA, Lab Manager uses the same calculation that VirtualCenter uses for assessing free slots available in the cluster. After assessing that the hosts have enough resources, Lab Manager powers on the virtual machine template. If the hosts do not meet compatibility requirements, the deploy operation fails, and Lab Manager displays a message.

If you experience a failure, you need to reconfigure the resources. For information about resource management, see the Resource Management Guide for VMware Infrastructure 3.
The calculation that VirtualCenter and Lab Manager uses is conservative. If necessary, disable it in VirtualCenter to stop this calculation in Lab Manager.

**To disable the calculation**

1. Log in to the VI Client.
2. Right-click the cluster and select **Edit Settings**.
3. In the left pane of the dialog box, select **VMware HA**.
4. In the Admission Control section of the dialog box, select **Allow virtual machines to be powered on even if they violate availability constraints**.
5. Click **OK**.

**Installing a Guest Operating System**

A virtual machine template must be deployed to install an operating system on it. Installing a guest operating system requires that the appropriate ISO image file for the operating system is available in the Lab Manager media library. See “**Working with Media**” on page 133.

Installing a guest operating system on a virtual machine template resembles installing on a physical machine and takes a similar amount of time.

**To install a guest operating system on a virtual machine template**

1. On the VM Templates page, click the thumbnail icon in the **Console** column.
2. Move the pointer over the tab with the virtual machine template name and choose **Insert CD** from the menu.
3. Select an ISO file from the Lab Manager media library and click **OK**.
4. On the tab, move the pointer over the virtual machine template name and choose **Ctrl-Alt-Del** from the menu to boot from the ISO image and launch the operating system installer.
5. In the virtual machine console of the virtual machine template, enter any required information for the installation process.
Installing VMware Tools

VMware Tools supports shared folders and cut and paste operations between the guest operating system and the machine from which you launch the Lab Manager Web console. Lab Manager depends on the VMware Tools utility for customizing the guest operating system.

VMware Tools also allows you to move the pointer into and out of the virtual machine console window. Otherwise, without VMware Tools, you can lose the pointer when navigating in and out of the console window. Press Ctrl + Alt to fix the problem.

A virtual machine template must be deployed to install VMware Tools.

Installing VMware Tools takes several minutes and requires you to restart the virtual machine. For more information about the installation, see VMware Infrastructure 3 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 choose View Console from the menu.

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

3. Click Install VMware Tools.

4. From inside the guest operating system, click OK to confirm that you want to install VMware Tools and launch the InstallShield wizard.
   - If you have autorun enabled in your guest operating system (the default setting for Windows operating systems), a dialog box appears.
   - If autorun is not enabled, run the VMware Tools installer. Click Start > Run and enter D:\setup.exe, where D: is your first virtual CD-ROM drive.

5. Follow the onscreen instructions.
   - On Windows Server 2003, the SVGA driver is installed automatically, and the guest operating system uses it after it reboots.
   - After you install VMware Tools, Windows 2000 and Windows XP guest operating systems must be rebooted to use the new driver.
To install VMware Tools on a Linux guest from X with the RPM installer

1. On the VM Templates page, move the pointer over the virtual machine template name and choose View Console from the menu.

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

3. Click Install VMware Tools.
   - The remaining steps take place inside the guest operating system.

4. Do one of the following tasks:
   - If you see a VMware Tools CD icon on the desktop, double-click it, and after it opens, 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, the VMware Tools CD icon might fail to appear. In this case, continue install VMware Tools from the command line.

5. When prompted, enter the root password and click OK.
   - The installer prepares the packages.

6. Click Continue when the installer presents a dialog box that shows Completed System Preparation.
   - A dialog box appears with a progress bar. When the installer is done, VMware Tools is installed. There is no confirmation or finish button.

7. In an X terminal, as root (su -), run the following file to configure VMware Tools:
   ```bash
   ./vmware-config-tools.pl
   ```
   Respond to the questions the installer displays on the screen. Press Enter to accept the default value.

8. After the upgrade is complete, restart the network by running the following command:
   ```bash
   /etc/init.d/network restart
   ```

9. When done, exit from the root account:
   ```bash
   exit
   ```

10. In an X terminal, open the VMware Tools Properties dialog box:
    ```bash
    vmware-toolbox &
    ```
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 choose **View Console** from the menu.

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

3. Click **Install VMware Tools**.
   
The remaining steps take place inside 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), as follows.
   
   - 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, you must modify the following commands to reflect the conventions used by your distribution:
     
     ```
     mount /dev/cdrom /mnt/cdrom
     cd /tmp
     ```
   
   If you have a previous installation, delete the previous `vmware-tools-distrib` directory before installing. The location of this directory depends on where you placed it when you did the previous installation. Often it is placed in:

   /tmp/vmware-tools-distrib

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

   Depending on whether you are using the tar installer or the RPM installer, do one of the following tasks:

   - For the tar installer, at the command prompt, enter:
     
     ```
     tar zxpf /mnt/cdrom/VMwareTools-3.5.0-<xxxx>.tar.gz
     umount /dev/cdrom
     ```
   
     Where `<xxxx>` is the build/revision number of the release.
For the RPM installer, at the command prompt, enter:

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

```
umount /dev/cdrom
```

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

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 Depending on whether you are using the `tar` installer or the `RPM` installer, do one of the following tasks:

- For the `tar` installer, run the VMware Tools `tar` installer:
  ```
cd vmware-tools-distrib
./vmware-install.pl
```
  Respond to the configuration questions on the screen. Press Enter to accept the default value.

- For the `RPM` installer, configure VMware Tools:
  ```
vmware-config-tools.pl
```
  Respond to the questions the installer displays on the screen. Press Enter to accept the default value.

7 After the upgrade is complete, restart the network by running the following command:

```
/etc/init.d/network restart
```

8 Log off the root account.

```
exit
```

9 Start your graphical environment.

10 In an X terminal, open the VMware Tools Properties dialog box:
```
vmware-toolbox &
```
To install VMware Tools on a Solaris guest

1. On the VM Templates page, move the pointer over the virtual machine template name and choose View Console from the menu.

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

3. Click Install VMware Tools.

   The remaining steps take place inside the virtual machine.

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

   Usually, the Solaris volume manager—vold—mounts the CD-ROM under /cdrom/vmwaretools. If the CD-ROM is not mounted, restart the volume manager using 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, as follows:

   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

   Respond to the configuration questions on the screen. Press Enter to accept the default value.

7. Log off of the root account.

   exit

8. Start your graphical environment.

9. In an X terminal, open the VMware Tools Properties dialog box:

   vmware-toolbox &
Customizing the Guest Operating System

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

When you configure a virtual machine template with the prerequisites for guest customization and add a virtual machine to a configuration based on that virtual machine template, Lab Manager creates a package with guest customization tools. When you deploy and power on the virtual machine for the first time, Lab Manager copies the package, runs the tools, and deletes the package from the virtual machine. This process takes a few minutes.

To avoid conflicts when not using guest customization, access the virtual machine console through Lab Manager and manually set its network parameters to unique values.

You can enable or disable customization for a virtual machine template or a virtual machine. By default, Lab Manager enables guest customization when you create a new template.

Prerequisites for Guest Customization

- You must specify the correct guest operating system on the VM Template Properties page. Lab Manager uses this information to determine how to customize the operating system.

- You must install the version of VMware Tools packaged with ESX 3.5 or higher. The Lab Manager Web console also provides the correct version for installation.

If you create a virtual machine template in Lab Manager 3.0 and install VMware Tools in Lab Manager 3.0, the virtual machine template will have the correct VMware Tools version.

If you import a virtual machine as a virtual machine template to Lab Manager, 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 VMware Tools in Lab Manager.
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 87.

- The virtual machine template cannot be part of a domain.
- The virtual machine template cannot be configured as a Microsoft Cluster Service server, a Microsoft Certificate Services server, or a domain controller.
- For the following Windows guest operating systems, Lab Manager administrators must set up a Microsoft Sysprep package:
  - Microsoft Windows XP 64-bit
  - Microsoft Windows 2003 64-bit
  See “Building a Microsoft Sysprep Package” on page 80.
- Microsoft Windows NT Server 4 and Solaris virtual machine templates require additional steps.
  See “Guest Customization for Windows NT and Solaris Virtual Machine Templates” on page 85.

### Building 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), or Windows XP (32-bit) guest operating systems. You can use Microsoft Sysprep instead of SIDgen to perform guest customization in these guest operating systems.

You must use Microsoft Sysprep to perform guest customization for Windows 2003 (64-bit) and Windows XP (64-bit) guest operating systems.

Before you can use Microsoft Sysprep for guest customization, you must build a Microsoft Sysprep package that includes the Microsoft Sysprep files for all of the following guest operating systems:

- 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.
To build a Microsoft Sysprep package for guest customization

1. For each operating system, insert the Windows OS CD in the CD-ROM drive of the Lab Manager Server system.
   If you have an ISO, mount the ISO using a third-party tool.

2. Locate the DEPLOY.CAB file in the \Support\Tools directory on the CD.

3. Expand the DEPLOY.CAB file using Winzip.exe or another tool capable of reading 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 Server, copy the files to one of these directories:

   - C:\Program Files\VMware\VMware Lab Manager Server\Tools\CustomizeGuest\Windows\Sysprep\win2k3
   - C:\Program Files\VMware\VMware Lab Manager Server\Tools\CustomizeGuest\Windows\Sysprep\win2k3_64
     This location is for 64-bit Windows 2003.
   - C:\Program Files\VMware\VMware Lab Manager Server\Tools\CustomizeGuest\Windows\Sysprep\win2000
   - C:\Program Files\VMware\VMware Lab Manager Server\Tools\CustomizeGuest\Windows\Sysprep\winxp
   - C:\Program Files\VMware\VMware Lab Manager Server\Tools\CustomizeGuest\Windows\Sysprep\winxp_64
     This location is for 64-bit Windows XP.

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

6. On the Guest Customization tab, click the Build Package button.
   When complete, the Guest Customization tab indicates a package exists.
Choosing 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, a tool packaged with Lab Manager. You can also choose SIDgen or Microsoft Sysprep as the SID generation tool for an individual virtual machine or virtual machine template.

You must use Microsoft Sysprep to perform guest customization for Windows 2003 (64-bit) and Windows XP (64-bit) guest operating systems.

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.

For information about guest operating support for SIDgen and Microsoft Sysprep, see Appendix C, “Guest Operating System Support,” on page 225.

Choosing the SID Generation Tool for Lab Manager

Set the default SID generation tool to use with new virtual machine templates that require Microsoft Sysprep (Windows 2003 64-bit and Windows XP 64-bit), as well as those that support both SIDgen or Microsoft Sysprep (Windows 2000, Windows 2003 32-bit, and Windows XP 32-bit).

1. In the Lab Manager Web console, click Settings in the left pane.

2. On the Guest Customization tab, select a SID mechanism, SIDgen or Microsoft Sysprep.

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

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

   You can also select Do not change SID.

3. Click OK.

Choosing 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 “Building a Microsoft Sysprep Package” on page 80.
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 choose Properties from the menu.
3. Choose the SID mechanism.
4. Click Update.

Choosing the SID Generation Tool for a Virtual Machine

You can override the default SID generation tool specified on the Guest Customization tab for individual virtual machines. You can only use Microsoft Sysprep if you have already built a Microsoft Sysprep package. See “Building a Microsoft Sysprep Package” on page 80.

To change the SID generation tool for a virtual machine template

1. In the left pane, click Workspace.
2. Move the pointer over a configuration name and choose Open from the menu.
3. On the Virtual Machines tab, move the pointer over a virtual machine name and choose Properties from the menu.
4. Choose the SID mechanism.
5. Click Update.

Disabling Guest Customization

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

Consider disabling guest customization under these special circumstances:

- 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 225.
**Disabling 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 choose **Properties** from the menu.
3. Deselect the **Perform customization** check box.
4. Click **Update**.

**Disabling Guest Customization for a Virtual Machine**

Virtual machines in Workspace configurations get their guest customization settings from the virtual machines 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 choose **Open** from the menu.
3. On the **Virtual Machines** tab, move the pointer over a virtual machine name and choose **Properties** from the menu.
4. Deselect the **Perform customization** check box.
5. Click **Update**.
Guest Customization for Windows NT and Solaris Virtual Machine Templates

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

To complete guest customization for Windows NT virtual machine templates

1. In the left pane of the console, click VM Templates.
2. Move the pointer over the deployed virtual machine template name and choose View Console from the menu.
3. Log in to the Windows NT guest operating system.
4. Move the pointer over the virtual machine template name and choose Insert Customization CD from the menu.
   This option starts a script that copies files to the guest and makes the virtual machine template ready for customization.

To complete guest customization for Solaris virtual machine templates

1. In the left pane of the console, click VM Templates.
2. Move the pointer over the deployed virtual machine template name and choose View Console from the menu.
3. Move the pointer over the virtual machine template name and choose Insert Customization CD from the menu.
4. Log in to the Solaris guest operating system.
5. In the terminal, enter these case-sensitive commands:
   > /etc/init.d/volmgt stop
   > /etc/init.d/volmgt start
   > cp -p /cdrom/cdrom/customize-guest.sh /etc/init.d/customvm
   > cp -p /cdrom/cdrom/base64decode.awk /etc/rc2.d/
   > sh /etc/init.d/customvm install
   > eject cdrom
6. Shut down the virtual machine from inside the guest operating system:
   > shutdown -y -g0 -i5
Customizing Guest Customization

In most cases, you can achieve your goals by using Lab Manager guest customization, or by disabling guest customization and manually customizing virtual machines. In some cases however, you might want to use Lab Manager guest customization in combination with your own script.

Lab Manager provides the opportunity to add a customization script to a virtual machine template. The script runs before and after Lab Manager 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 gets called with precustomization command line parameter before the Lab Manager guest customization process begins, and the same script gets called with the postcustomization command line after the guest customization process finishes.

See “Extending Guest Customization” on page 235 for more information.

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 choose Customization Script.
3. Click Browse to locate an existing script, or type the script in the text box.
   Specify batch script for Windows guests and a shell script for UNIX guests. The script must only include text (that is, it cannot contain any 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 a previous version of Lab Manager, the virtual machine templates likely have an older version of VMware Tools, and the VMware Tools enforcement check will prevent you from publishing the virtual machine templates. Review these options:

- You can upgrade VMware Tools to the current Lab Manager version. This option allows guest customization and publishing to occur.
- If the virtual machine template has the Lab Manager LM Tools utility, you can disable the VMware Tools enforcement check, See “Disabling VMware Tools Check Before Publishing Virtual Machine Templates” on page 90. This option allows Lab Manager to customize guests according to the method used in the previous version. VMware does not recommend this approach.
- If the virtual machine template does not have the LM Tools utility and you do not upgrade VMware Tools, disable the Perform Customization setting in the virtual machine template properties. See “Disabling Guest Customization” on page 83.

Undeploying Virtual Machine Templates

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

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

If an ESX host goes offline or someone manually removes a virtual machine from VirtualCenter inventory, the standard undeploy operation does not work. See “Undeploying Virtual Machine Templates with Force” on page 203.

To undelete a virtual machine template

1. In the left pane, click VM Templates.
2. If the virtual machine template is deployed, move the pointer over the virtual machine template name and choose Undeploy - Save State or Undeploy - Discard State from the menu.
Sharing Virtual Machine Templates

When a user creates a virtual machine template in Lab Manager, the user becomes its owner. The owner, or a user with the Administrator View and Control right, can give other users access to the virtual machine template.

**NOTE** By default, only administrators and organizations administrators have the Administrator View and Control right.

Owners can share objects to all or specific users in the following ways, depending on their rights:

- Across the entire Lab Manager installation
- Between organizations
- Within an organization

By default, administrators and organization administrators can share in all three ways. All other types of users (except view only) can only share within their own organization.

**To share a virtual machine template with other users**

1. On the VM Templates page, move the pointer over the virtual machine template name and choose Sharing from the menu.

   The Sharing dialog box displays the users and organizations that currently have access to the virtual machine template (if any) and their level of access control.

2. Click Add Users.

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

4. Select who to share the virtual machine template with:

   - **Everyone** to share the virtual machine template with all users in the selected organization.
   - **Selected Users** to share the virtual machine template with specific users in the selected organization.

   Select the check box for each user you want to share the virtual machine template with.
When you share a virtual machine template with a specific user in an organization, that user only has access to the virtual machine template in that organization. To share a virtual machine template with a user in all the organizations to which the user belongs, choose the Global organization.

5 Specify the access rights for the user(s) and click OK.

Access rights combine with the rights of a user’s role to determine how a user can interact with the shared virtual machine template. Access rights cannot provide users with rights that they don’t already have based on their role.

If you are sharing the virtual machine template with users in an organization other than the one in which the virtual machine template was created, you can only grant Read access. Virtual machine templates created in the Global organization can only be shared with Read access.

6 Click Done.

## Publishing Virtual Machine Templates

Publishing a virtual machine template makes it available for use in building multimachine configurations without reinstalling software or performing setup tasks again. The use of virtual machine templates ensures that virtual machines are consistently configured with operating systems, versions, system packs, and more across an entire organization.

**NOTE** Storage leases are not applicable to published virtual machine templates. After a virtual machine template changes from a published to unpublished state, the storage lease begins. For information on leases, see “Configuring Resource Cleanup Settings” on page 198.

## Checking 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 on the status of VMware Tools on the virtual machine template and address any issues.

You cannot publish a virtual machine template that does not have VMware Tools installed, unless you deselect the Perform customization check box. See “Disabling Guest Customization” on page 83.
To check VMware Tools status

1. In the left pane, click VM Templates.

2. Check the VMware Tools column on the VM Templates page:
   - **Installed** – The virtual machine template is ready to be published.
   - **Not Installed** – If you want Lab Manager to perform guest customization, you must install VMware Tools. For installation instructions, see “Installing VMware Tools” on page 74.
   - **Installed (Requires Update)** – Deploy the virtual machine template and follow the prompts to update VMware Tools.
   - **Unknown** – Deploy the virtual machine template to allow Lab Manager to check for VMware Tools and update the information.

Disabling VMware Tools Check Before Publishing Virtual Machine Templates

By default, you cannot publish a virtual machine template that does not have a current version of VMware Tools installed. You might need to bypass this requirement in these circumstances:

- You cannot install the current version of VMware Tools because you must have special scripts in the virtual machine template for customization.
- You import virtual machine templates that have an old version of the LM Tools utility and you cannot upgrade the VMware Tools utility on those virtual machine templates.

In this case, Lab Manager recognizes the LM Tools utility 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 225.

To disable the check of VMware Tools

1. In the left pane, click Settings.


3. Click OK.
When you disable the check of VMware Tools, Lab Manager no longer prompts you to upgrade VMware Tools when publishing a virtual machine template that uses an old version.

**Publishing Virtual Machine Templates**

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 choose Publish from the menu.

**Managing Virtual Machine Templates**

You can unpublish, export, consolidate, delete, and modify virtual machine templates.

**Unpublishing Virtual Machine Templates**

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 virtual machine template name and choose Unpublish from the menu.
3. Click OK to confirm the operation.

**Exporting Virtual Machine Templates 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. To modify the timeout for SMB exports, see "Lab Manager Preferences" on page 189.
Export operations require an open SMB port on the ESX hosts. Although Lab Manager opens the port during installation, make sure that the port was not closed after the install. To check the port status, use the `esxconf-firewall-q smbClient` command on each host.

Prior to exporting a virtual machine template, Lab Manager consolidates it. This results in an increase in the disk space required to store the virtual machine template. The exported virtual machine template might also require a significant amount of disk space depending on the size of its consolidated virtual disk.

**To export a virtual machine template**

1. In the left pane, click **VM Templates**.
2. Move the pointer over the virtual machine template name and choose Export from the menu.
3. Provide the location and user credentials:
   - Enter the UNC path of the SMB share (relative to the Lab Manager Server system) where you want to store the files. A sample path is `\10.6.1.246\VMwareLM\ExportTemplates`. Use English characters for the UNC path.
   - If the UNC folder requires authentication, specify the user name and password to access the files.
4. Click **OK** and confirm to continue the export process.

**Consolidating Virtual Machine Templates**

Each time you create a linked clone of a virtual machine template, Lab Manager freezes the virtual hard disk associated with the original virtual machine 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 virtual machine 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 virtual machine template to a different datastore.

You can only consolidate virtual machine 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 virtual machine 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 virtual machine template name and choose Consolidate from the menu.

3. Select a datastore and click OK.

Discarding State for Virtual Machine Templates

When you save the state of a virtual machine template by either 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 virtual machine template name and choose Discard State from the menu.

3. Click OK to confirm.

Modifying Virtual Machine Template Properties

By default, only administrators, organization administrators, and template creators can modify the properties of a virtual machine template. Before modifying the properties of a virtual machine template, undeploy the template.

If a virtual machine template is deployed, the number of properties you can modify is limited.

For information about modifying virtual machine template hard disks and network interfaces, see “Modifying Virtual Machine Template Hard Disks” on page 96 and “Modifying Virtual Machine Template Network Interfaces” on page 97.

For information about changing a virtual machine template's owner, see “Changing Ownership of Virtual Machine Templates” on page 100.
To modify virtual machine template properties

1. On the VM Templates page, move the pointer over the virtual machine template name and choose Properties from the menu.

2. 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 15 characters.
   - **Description** – (Optional) Maximum number of characters is 128.
   - **Number of Virtual CPUs** – 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.

   - **Guest OS** – If you select a 64-bit guest operating system, the datastore must be connected to an ESX 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.

   - **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 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**:

     - **CPU Priority** – Priority for shares of CPU.
     - **CPU Shares** – Relative amount of CPU for a virtual machine based on the virtual machine template.
CPU Reserved (Mhz) – Minimum amount of CPU set aside for the virtual machine template.

CPU Limit (Mhz) – Maximum amount of CPU available for the virtual machine template.

Unlimited – Select this check box to set no CPU limit.

See the VMware Infrastructure documentation for details on priorities, shares, reservations, and limits.

Memory information:

Memory – Amount of RAM allocated for running the virtual machine template.

Memory Priority – Priority for shares of memory.

Memory Shares – Relative amount of memory for a virtual machine based on the virtual machine template.

Memory Reserved (MB) – Minimum amount of memory set aside for the virtual machine template.

Memory Limit (MB) – Maximum amount of memory available for the virtual machine template.

Unlimited – Select this check box to set no memory limit.

See the VMware Infrastructure documentation for details on priorities, shares, reservations, and limits.

Use Time Synchronization – Enables time synchronization between the guest (virtual machine template) and ESX host operating systems. You must install VMware Tools to use this option.

Perform Customization – Specifies whether guest customization is enabled.

SID mechanism – 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 choose None.

To use Microsoft Sysprep, you must first create a Microsoft Sysprep package for guest customization. See “Building a Microsoft Sysprep Package” on page 80.
Deployment Lease or Storage Lease – Time to 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 or not.

System Messages – Messages or alerts about VirtualCenter activity that could raise errors in Lab Manager.

3 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.

Adding a Virtual Machine Template Hard Disk

You can add one or more virtual hard disks (.vhd files) to a virtual machine template.

To add a virtual hard disk

1 On the VM Templates page, move the pointer over the virtual machine template name and choose Properties from the menu.

2 In the Hard Disk section, click Add Hard Disk.

3 Specify whether the bus type is BusLogic SCSI or LSI Logic SCSI.

4 Choose a bus number.

5 Choose a bus ID.

6 Enter the disk size (GB) and click OK.

7 Click Update.

Adding SCSI Virtual Hard Disks

If you add a SCSI hard disk to a virtual machine template, you might generate an operating system error message about missing drivers for this device. If this error occurs, download and install the appropriate driver, and contact VMware for further support.
Chapter 5 Working with Virtual Machine Templates

Editing 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. On the VM Templates page, move the pointer over the virtual machine template name and choose Properties from the menu.
2. In the Hard Disk section, click Edit.
3. Modify the bus number and bus ID and click OK.
4. Click Update.

Deleting a Virtual Machine Template Hard Disk
You can delete a virtual machine template hard disk.

To delete a virtual machine template hard disk
1. On the VM Templates page, move the pointer over the virtual machine template name and choose Properties from the menu.
2. In the Hard Disk section, click Delete.
3. Click OK to confirm.
4. Click Update.

Modifying Virtual Machine Template Network Interfaces
For undeployed virtual machines template, you can modify network settings, reset a MAC address, add a network interface, and delete a network interface.

Adding a Network Interface
You can add one or more virtual NICs to an undeployed virtual machine template. A single virtual machine template can have up to four NICs.

To add a network interface
1. On the VM Templates page, move the pointer over the virtual machine template name and choose Properties from the menu.
2. In the Network Interfaces section, click Add Interface.
   Lab Manager adds and connects a new virtual NIC.
3 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 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. 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.
   d Choose 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** allows Lab Manager to pull static IP addresses from the
        IP address pool.
      - **DHCP** allows Lab Manager to pull 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** as the IP addressing mode, type an IP address
      in the **IP Address** field.

4 Click **Update**.
   Lab Manager generates a MAC address for the network interface.
Editing Network Interface Settings

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 On the VM Templates page, move the pointer over the virtual machine template name and choose Properties from the menu.

2 In the Network Interfaces section, change any of the following settings:
   - 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.
   - Choose 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 allows Lab Manager to pull static IP addresses from the IP address pool.
     - DHCP allows Lab Manager to pull 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 as the IP addressing mode, type an IP address in the IP Address field.

3 Click Update.
Deleting a Network Interface

You can delete virtual NICs from an undeployed virtual machine template.

To delete a network interface

1. On the VM Templates page, move the pointer over the virtual machine template name and choose Properties from the menu.
2. In the Network Interfaces section, click Delete.
3. Click Update.

Resetting a Network Interface MAC Address

You can reset a network interface MAC address for an undeployed virtual machine template. 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. On the VM Templates page, move the pointer over the virtual machine template name and choose Properties from the menu.
2. In the Network Interfaces section, choose Reset from the MAC Address drop-down menu for the network interface you want to update.
3. Click Update.

Changing Ownership of Virtual Machine Templates

The original owner of a virtual machine template is the user who created it. You can change the owner to assign a virtual machine template to another user in the same organization as the current owner.

To change ownership of a virtual machine template

1. In the left pane, click VM Templates.
2. Move the pointer over the virtual machine template name and choose Properties from the menu.
3. Click Change Owner.
4. Choose a new owner for the virtual machine template and click OK.
5. Click Update.
Deleting Virtual Machine Templates

To delete a virtual machine template, it must be undeployed and unpublished. If you are unable to unpublish a virtual machine template, see “Deleting Published Virtual Machine Templates with Force” on page 204.

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 choose Delete from the menu.
3. Confirm the deletion.
Configurations are the core of the Lab Manager system and are composed of one or more virtual machines created from virtual machine templates. Lab You can group, deploy, save, share, and monitor multimachine configurations.

Before you can create a configuration, you must publish at least one virtual machine template.

You use the Workspace page to create and work with configurations, and you use the Library page to store configurations and move configurations to the Workspace.

This chapter includes these topics:

- “Accessing Configurations” on page 104
- “Creating Configurations” on page 106
- “Importing Configurations from an SMB Share” on page 109
- “Cloning Configurations” on page 110
- “Viewing Configuration Virtual Machines and Networks” on page 112
- “Changing the Virtual Machines in a Configuration” on page 115
- “Changing the Networks in a Configuration” on page 118
- “Deploying Configurations” on page 119
- “Working with Configuration Snapshots” on page 123
- “Saving Configurations to the Library” on page 124
- “Sharing Configurations” on page 127
- “Managing Configurations” on page 128
Accessing Configurations

You can access configurations in the Workspace and in the configuration library. You can perform configuration operations from both the Workspace and Library pages. Some operations are only available from the Workspace, some are only available from the Library, and some are available from both.

Accessing the Workspace Page

The Workspace page displays a table listing Workspace configurations and providing basic information about the properties of each configuration.

Use this page to create and import configurations. From the table, users with the necessary rights can perform configuration operations, such as deploy, clone, share, delete, and modify.

Lab Manager adds the Sample Configuration to the Workspace page 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.

To access the Workspace page

Click Workspace in the left pane.

A table presents basic information about each configuration:

- **Consoles** – Provides access to the virtual machine consoles of the configuration through the thumbnail icons.
- **Configuration Name** – Provides a pop-up menu to perform various operations on the configuration.
- **Status** – Indicates whether the configuration is deployed or in the midst of an operation.
- **Owner** – Shows the owner of the configuration.
- **Organization** – Shows the organization in which the configuration was created.
- **Sharing** – Shows whether a configuration is shared or private.
- **Connectivity** – Indicates whether a deployed configuration uses fencing or has a virtual network connected to physical network.
- **# Machines** – Shows the number of virtual machines in the configuration.
Date Deployed – Shows the date and time of the last deploy operation.

Messages – Messages or alerts about VirtualCenter activity that could raise errors in Lab Manager.

See “Using Text Search Filter” on page 24 for information on using the Filter feature.

In the top left corner, use the drop-down menu to determine the configurations that appear on the page:

- **My Configurations** – View only your configurations, both shared and private. This option displays all your configurations in the selected organization.
- **All Configurations** – View your configurations, both shared and private, and configurations shared by others. This option displays all configurations in the selected organization that are available to you.
  
  Administrators can choose **All Configurations** in the Global organization to view all configurations in the entire Lab Manager installation.
- **My Configurations in Other Organizations** – This option displays all your configurations in organizations other than the selected organization. This option is not available from the Global organization or for users that are members of a single organization.

**Accessing the Library Page**

The Library page displays a table listing library configurations and providing basic information about the properties of each configuration.

From the table, users with the necessary rights can perform configuration operations, such as clone, share, and LiveLink.

**To access the configuration library**

Click Library in the left pane.

A table presents basic information about each configuration:

- **Configuration Name** – Provides a pop-up menu to perform operations on the configuration.
- **Status** – Indicates whether the configuration is in the midst of an operation.
- **Owner** – Shows the owner of the configuration. In this case, the user who captured the configuration to the library.
- **Organization** – Shows the organization from which the configuration was captured to the library.
Sharing – Shows whether a configuration is shared or private.

Description – Shows the optional description from the capture operation.

Date Captured – Shows the date and time when the configuration was captured from the Workspace to the configuration library.

# Machines – Shows the number of virtual machines in the configuration.

Gold Master – Indicates whether or not the configuration has been labeled as a gold master. You can label important library configurations as gold masters.

See “Using Text Search Filter” on page 24 for information on using the Filter feature.

In the top left corner, use the drop-down menu to determine the configurations that appear on the page:

- **My Library Configurations** – View only your configurations, both shared and private. This option displays all your configurations in the selected organization.

- **All Library Configurations** – View your configurations, both shared and private, and configurations shared by others. This option displays all configurations in the selected organization that are available to you.

  Administrators can choose **All Library Configurations** in the Global organization to view all configurations in the entire Lab Manager installation.

- **My Library Configurations in Other Organizations** – This option displays all your configurations in organizations other than the selected organization. This option is not available from the Global organization or for users that are members of a single organization.

### Creating Configurations

A configuration consists of one or more virtual machines that are based on virtual machine templates. You can only use published virtual machine templates when building configurations.

You can create new configurations only in the Workspace. Creating a configuration involves defining configuration properties and adding virtual machines to the configuration.

Creating a configuration involves specifying a storage lease. See “Configuring Resource Cleanup Settings” on page 198.

You can also use a library configuration as the basis for a new Workspace configuration. See “Cloning a Library Configuration to the Workspace” on page 125.
To create a configuration

1. On the Workspace page, click the **New Configuration** button at the top of the page.
2. Enter a name for the configuration.
3. (Optional) Enter a description of the configuration.
4. Specify a time to delete the configuration or mark the configuration for deletion.
5. Specify the fencing policy for the configuration:
   - **Allow Fenced or Unfenced**
   - **Fenced Only**
   - **Unfenced Only**
   The default is **Allow Fenced or Unfenced**. Use the other options to require that a configuration to be deployed in fenced mode only or in unfenced mode only.
6. Choose a virtual machine template from the Template drop-down menu.
   You can choose a virtual machine template that you created or a virtual machine template that is shared with you. This virtual machine template is used as the basis for the virtual machine.
7. Enter a name for the virtual machine.
8. 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. To consolidate the chain of delta disks for a particular virtual machine to maximize performance, select the **Full Clone** check box.
   Choosing this option requires additional disk space and increases the amount of time required to add the virtual machine to the configuration.
Specify the network information for the virtual machine. Your options are based on how the virtual machine template was defined.

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 Choose a network.

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

   - **Static - IP Pool** allows Lab Manager to pull static IP addresses from the IP address pool.
   - **DHCP** allows Lab Manager to pull 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.

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

   When creating the configuration, you can add up to 20 virtual machines.

11 Click **OK**.

Lab Manager creates the configuration in the current organization and displays it on the Workspace page.
Importing Configurations from an SMB Share

You can import a configuration and all its virtual machine files from SMB share.

Import operations require an open SMB port on the ESX host. Although Lab Manager opens the port during installation, make sure that the port was not closed after the install. To check the port status, use the esxcfg-firewall –q smbClient command on each host.

Importing a configuration involves specifying a storage lease. See “Configuring Resource Cleanup Settings” on page 198.

To import a configuration

1. On the Workspace page, select the organization to which you want to import the configuration in the Organization drop-down menu.
2. Click the Import Configuration button at the top of the page.
3. Provide the import directory details:
   - UNC path of the directory (relative to the Lab Manager Server system) where the configuration file is stored. A sample path is \10.6.1.246\VMwareLM\ExportedConfigs. Use English characters for the UNC path.
   - User name and password for the import directory, if necessary.
4. Click Next.
5. Provide configuration details:
   - Name
   - (Optional) Description
   - Time to delete the configuration or mark the configuration for deletion
   - Destination datastore
6. Click Import.

When you import a configuration that you previously exported, Lab Manager sets the fencing policy for the imported configuration to Fenced Only. To modify the fencing policy, see “Modifying Configuration Properties” on page 131.
Cloning Configurations

You can clone a Workspace configuration to create a new copy of the configuration in the Workspace, or to add some or all of the virtual machines in the configuration to an existing Workspace configuration.

You can clone a Library configuration to create a new copy of the configuration in the Library. To clone a Library configuration to the Workspace, see “Cloning a Library Configuration to the Workspace” on page 125.

Cloning Workspace Configurations

You can create linked clones and full clones of Workspace configurations.

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.

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. A full-clone operation takes longer than a linked-clone operation.

Typically, you do not create full clones, except under these conditions:

- To dismantle the storage and move the configuration to a different server
- To maximize performance for virtual machines (for example, for certain production-level virtual machines)

You can clone all the virtual machines in a configuration or selected machines. You can even combine configurations by cloning some or all of the virtual machines from one Workspace configuration 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. For information about fencing, see Appendix D, “Network Fencing,” on page 229.

This operation involves specifying a storage lease. See “Configuring Resource Cleanup Settings” on page 198.

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 Workspace configuration

1. On the Workspace page, move the pointer over the configuration name and choose Clone from the menu.

2. Specify the destination:
   - New Configuration
     Enter a name, description, and storage lease.
   - Existing Configuration
     Select a configuration.

3. Specify the type of clone:
   - Linked Clone
   - Full Clone
     You cannot make a full clone of a deployed configuration.

4. Specify the virtual machines to clone:
   - All Virtual Machines
   - Selected Virtual Machines
     Select the check box for each virtual machine you want to clone. If available, you can specify a new datastore for each virtual machine you select.

5. Click OK.

Cloning Library Configurations

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 the Workspace and deploy them at the same time, duplicate IP address errors occur unless you deploy one of the configurations in fenced mode. For information about fencing, see Appendix D, “Network Fencing,” on page 229.

This operation involves specifying a storage lease. See “Configuring Resource Cleanup Settings” on page 198.
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 choose Clone to Library from the menu.
2. Enter a name.
3. (Optional) Enter a description.
4. Specify a time to delete the configuration or mark the configuration for deletion.
5. Specify the virtual machines to clone:
   - All Virtual Machines
   - Selected Virtual Machines
     Select the check box for each virtual machine you want to clone. If available, you can specify a new datastore for each virtual machine you select.
6. Click OK.

**Viewing Configuration Virtual Machines and Networks**

From the Workspace or Library, you can view information about the virtual machines and networks in the configuration and how they interact.

**Viewing Configuration Virtual Machines**

The Virtual Machines tab for a configuration displays basic information about each virtual machine in the configuration. From the tab, you can interact with the virtual machines and add virtual machines to the configuration.
To view details on the virtual machines in a configuration

1. On the Workspace or Library page, move the pointer over the configuration name and choose Open from the menu.

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 (Network)** – Lists a number for each NIC in the virtual machine and also lists the network to which the 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.

For more information about external IP addresses, see Appendix D, “Network Fencing,” on page 229.

- **VM Template** – Indicates the virtual machine template that the virtual machine is based on.
- **Host** – Indicates the ESX 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.

This column only appears for Workspace configurations.

- **Messages** – Messages or alerts about VirtualCenter activity that could raise errors in Lab Manager.
Viewing Configuration Networks

The Networks tab for a configuration displays basic information about each network in the configuration. From the tab, you can interact with the networks and add networks to the configuration.

To view details on the networks in a configuration

1. In the left pane, click Workspace or Library.
2. Move the pointer over the configuration name and choose Open from the menu.
3. 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.
  
  This column only appears for Workspace configurations.
- 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 (Used/Total) – Displays the number of IP addresses currently in use by the network and the total number of IP addresses available to the network.
Viewing Configuration Diagrams

The Configuration Diagram tab for 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. On the Workspace or Library page, move the pointer over the configuration name and choose Open from the menu.
2. Click the Configuration Diagram tab.

Changing the Virtual Machines in a Configuration

You can add virtual machines to Workspace configurations. You can also remove virtual machines and move virtual machine from one configuration to another. You cannot add, remove, or move virtual machines in the Library.

Adding a Virtual Machine to a Configuration

After you create a Workspace configuration, you can add more virtual machines at any time. You can also move an existing virtual machine from another configuration.

To add a virtual machine to a Workspace configuration

1. On the Workspace page, move the pointer over the configuration name and choose Open from the menu.
2. In the Virtual Machines tab, click the Add Virtual Machines button.
3. From the Templates drop-down menu, choose a template to use as the basis for the virtual machine.
4. Enter a name for the virtual machine.
5. 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 virtual machine template’s base disk and uses delta disks to describe the differences between the virtual machine template and the virtual machine.

This option consolidates the chain of delta disks for a particular virtual machine to maximize performance, but requires additional disk space and increases the amount of time required to add the virtual machine to the configuration.
6 Specify the network information for the virtual machine. Your options are based on how the virtual machine template was defined.
   
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 fence the configuration or connect virtual networks to physical networks.
   
b Choose a network.
   
c Choose an IP addressing mode. The available options are based on the IP addressing modes available to the selected network.
   
   ■ **Static - IP Pool** allows Lab Manager to pull static IP addresses from the IP address pool.
   
   ■ **DHCP** allows Lab Manager to pull IP addresses from a DHCP server.
   
   This option avoids specifying 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.
   
   This selection activates the IP Address text box.
   
d If you selected **Static - Manual** as the IP addressing mode, type an IP address in the **IP Address** field.
   
7 Click OK.

**Removing a Virtual Machine from a Configuration**

You can only remove undeployed virtual machines from a Workspace configuration.

To remove a virtual machine from the resource management area of the Web console, see “Deleting a Virtual Machine or Configuration Based on Datastore Usage” on page 181.
To remove a virtual machine from a Workspace configuration

1. On the Workspace page, move the pointer over the configuration name and choose Open from the menu.
2. In the Virtual Machines tab, move the pointer over the virtual machine name and choose Delete from the menu.
3. Confirm the deletion.

Moving Virtual Machines to Another Configuration

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.

You can only move virtual machines from a configuration that is undeployed. If a configuration includes both deployed and undeployed machines, you cannot move its virtual machines.

To move virtual machines to another configuration

1. On the Workspace page, move the pointer over the configuration name and choose Move from the menu.
2. Specify the destination:
   - New Configuration
     Enter a name, description, and storage lease.
   - Existing Configuration
     Select a configuration.
3. Specify the virtual machines to move:
   - All Virtual Machines
     If you move all the virtual machines in a configuration, the original configuration still exists, but it contains no virtual machines.
   - Selected Virtual Machines
     Select the check box for each virtual machine you want to move.
4. Click OK.
Changing the Networks in a Configuration

You can add networks to and remove networks from Workspace configurations. You cannot add or remove networks in the Library.

Adding a Network to a Configuration

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

You can also add a network to a configuration that no virtual machines connect to.

To add a network to a configuration

1. On the Workspace page, move the pointer over the configuration name and choose Open from the menu.

2. Click the Networks tab.

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

3. Click Add Network.

4. Choose a network and click OK.

   The list of networks includes physical networks available to your organization, as well as virtual networks you own or are shared with you.

   You can now edit the properties of a virtual machine in the configuration to use the new network. See “Modifying Virtual Machine Network Interfaces” on page 49.

Removing a Network from a 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. On the Workspace page, move the pointer over the configuration name and choose Open from the menu.

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 choose 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 in use 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, or use the Force Remove command to remove the network without reassigning virtual machine NICs.

**Forcibly Removing a Network from a Configuration**

You can forcibly remove a network that is used by a configuration. You must undeploy the configuration before you can remove the network. Virtual machines in the configuration with NICs that were connected to the removed network are disconnected and assigned to the None network.

**To forcibly remove an in-use network from a configuration**

1 On the Workspace page, move the pointer over the configuration name and choose Open from the menu.

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 choose Force Remove.

4 Click OK to confirm.

**Deploying Configurations**

Deploying a configuration registers its virtual machines on ESX hosts and provides access to Lab Manager operations at the virtual machine console level. You can deploy an entire configuration or individual virtual machines in the configuration.

You can only deploy configurations in the Workspace.

When you initially deploy a configuration based on virtual machine templates that have guest customization enabled, the configuration goes through a customization process that involves multiple reboots based on whether the virtual machines use SIDgen or Microsoft Sysprep. Do not shut down the virtual machines until the customization is complete. You can log in to the system and verify settings, such as the computer name or network values.
Deploying a configuration involves specifying a deployment lease. See “Configuring Resource Cleanup Settings” on page 198.

For information about deploying an individual virtual machine in a configuration, see “Deploying Virtual Machines” on page 41.

**Deploying a Configuration with Default Settings**

When you deploy a configuration with default settings, Lab Manager uses the default settings of the configuration and the default deployment options from your user preferences. See “Setting User Preferences” on page 25.

By default, Lab Manager configurations deploy without fencing, unless the configuration or its physical networks have fencing policy that override this default.

**To deploy a configuration with default settings**

On the Workspace page, move the pointer over the configuration name and choose Deploy with defaults from the menu.

**Deploying a Configuration with Custom Settings**

You can override the default settings of a configuration when you deploy the configuration.

**To deploy a configuration with custom settings**

1. On the Workspace page, move the pointer over the name of the configuration and choose Deploy from the menu.

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

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

   This option is only available if the configuration includes any virtual machines with NICs connected to a physical network. It also requires that the network have IP addresses available in the IP pool.

   Fencing isolates the virtual machine 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. You cannot fence a configuration if any of its virtual machines connect to a physical network using DHCP or if the configuration does not allow fencing.
Deploying a configuration in fenced mode places all the virtual machines on a single ESX host. You must have a host connected to the datastore where the virtual machine templates that serve as the basis of this configuration reside. The host must have enough resources to pass VMware Infrastructure admission controls for virtual machines.

Use the **Connectivity** drop-down menu to choose a connectivity mode for each physical network:

- **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.

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 any virtual machines with NICs connected to a virtual network.

You cannot select this option for a configuration if any of its virtual machines connect to a virtual network using DHCP. Both the virtual network and the physical network must have IP addresses available in the IP pool.

Choose a physical network to connect to and use the **Connectivity** drop-down menu to choose 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 to machines on the selected physical network, and can receive messages back on the same connection. Machines on the selected physical network cannot initiate communication to virtual machines inside the configuration.
4 Select the Use Server Boot Sequence check box if you want to use the boot sequence specified during the creation of the configuration. Otherwise, Lab Manager boots the virtual machines all at once.

5 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 bring up virtual machines. For example, you might need to ensure a database, application, and Web server are working individually rather than all at once.

6 Specify a resource pool on which to deploy the configuration, or use the default setting, Any Available.

7 Specify a time to undeploy the configuration.

The deploy options available depend on whether or not any virtual machines in the configuration are already deployed.

Deploying Configurations on High Availability Clusters

If you deploy a configuration on a cluster with VMware HA, Lab Manager uses the same calculation that VirtualCenter has for assessing free slots available in the cluster. After assessing that the hosts have enough resources, Lab Manager powers on the virtual machines. If the hosts do not meet compatibility requirements, the deploy operation fails and Lab Manager displays a message.

If you experience a failure, you need to reconfigure the resources. For information about resource management, see the Resource Management Guide for VMware Infrastructure 3.

The calculation that VirtualCenter and Lab Manager uses is conservative. If necessary, disable it in VirtualCenter to stop this calculation in Lab Manager.

To disable the calculation

1 Log in to the VMware Infrastructure Client.

2 Right-click the cluster and select Edit Settings.

3 In the left pane of the dialog box, select VMware HA.

4 In the Admission Control section of the dialog box, select Allow virtual machines to be powered on even if they violate availability constraints.

5 Click OK.
Chapter 6  Working with Configurations

Working with Configuration Snapshots

A snapshot captures the state the virtual machines in a configuration at a specific point in time. After deploying a configuration, you can take a snapshot and revert the configuration to that snapshot at a later time.

Taking a Configuration Snapshot

Lab Manager stores the snapshot persistently with the configuration. If you undeploy a configuration and deploy it, the snapshot remains. Only one snapshot of each virtual machine in a configuration can exist at a time. Taking a new snapshot replaces the previous one. You can only take a snapshot of a configuration if at least one of its virtual machines is deployed.

To take a configuration snapshot

On the Workspace page, move the pointer over the configuration name and choose Snapshot from the menu.

Lab Manager changes the status of the configuration to Setting the Revert Point. After a brief time, the configuration returns to its previous state.

Reverting to a Configuration Snapshot

When you revert a configuration to a snapshot, all the virtual machine in the configuration lose their current state.

To revert to a configuration snapshot

1  On the Workspace page, move the pointer over the configuration name and choose Revert from the menu.

2  Confirm to revert to the last snapshot of the configuration virtual machines and lose the current state of the machines.

   The status of the configuration appears as Reverting.

Deleting a Configuration Snapshot

Configuration snapshots, also known as revert points, take up space on datastores. You can free up space by deleting revert points.

To delete the revert point for a specific virtual machine in a configuration, see “Deleting a Virtual Machine Snapshot” on page 58.
To delete revert points for all virtual machines in a configuration

On the Workspace page, move the pointer over the configuration name and choose Delete Revert Point from the menu.

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

Saving Configurations to the Library

You can save a Workspace configuration to the Library to make it available to other users as the basis for new configurations. Users can clone a library configuration to the Workspace and then modify and deploy it. You can also save a configuration to the Library to create a LiveLink, which you can use to share a configuration in a specific state (for debugging purposes, for example).

Adding a Configuration to the Library

If you have a Workspace configuration that you want to use as a base configuration, you can save it to the configuration library.

When you add a configuration to the Library, Lab Manager only displays it to administrators and users in the organization currently selected in the Organization drop-down menu. Users must have the required rights to view and modify the configuration.

This operation involves specifying a storage lease. See “Configuring Resource Cleanup Settings” on page 198.

To add a configuration to the Library

1. On the Workspace page, move the pointer over the configuration name and choose Capture to Library.
2. Enter a name for the configuration.
   Use a unique naming convention to simplify identification.
3. (Optional) Enter a description.
4. Select the Gold Master check box to indicate an important or administrator-approved configuration.
5. Specify a time to delete the configuration or mark the configuration for deletion.
6. Click Capture.
Cloning a Library Configuration to the Workspace

If you have a Library configuration that you want to work with, you can clone it to the Workspace. Lab Manager creates a new configuration in the Workspace, which you can modify and deploy. The original configuration remains in the Library, so users can continue to make additional clones.

Cloning to the Workspace creates a linked clone. 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 referring back to a chain of delta disks. For each clone, Lab Manager freezes the original delta disk and creates a new one.

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

This operation involves specifying a storage lease. See “Configuring Resource Cleanup Settings” on page 198.

**To clone a configuration to the Workspace**

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

2. Specify the destination:
   - **New Configuration**
     Enter a name, description, and storage lease.
   - **Existing Configuration**
     Select a configuration.

3. Specify the virtual machines to clone:
   - **All Virtual Machines**
   - **Selected Virtual Machines**
     Select the check box for each virtual machine you want to clone.

4. Click OK.

After a brief time, an undeployed copy of the Library configuration appears in the Workspace page.
Creating a LiveLink to a Configuration

A LiveLink is the HTTP URL of a configuration in the Library. You can email this 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.

You can only create LiveLinks for shared configurations. See “Sharing Configurations” on page 127.

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 the configuration name and choose LiveLink from the menu.
   
   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 in the Attach a comment field. This note appears when a user deploys the configuration.

4. Click OK.

You can now email the LiveLink URL to another tester or developer.

Deploying a Configuration from a LiveLink

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

To deploy a configuration LiveLink

1. Invoke a LiveLink URL in a browser.
   
   If you are not logged in to the Lab Manager Web console, the login page appears. Enter your user name and password to log in.
   
   The Restore Lab Manager LiveLink page appears.

2. 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.
Sharing Configurations

When a user creates a configuration in Lab Manager, that user becomes its owner. The owner, or a user with the Administrator View and Control right, can give other users access to the configuration.

**NOTE** By default, only administrators and organizations administrators have the Administrator View and Control right.

Owners can share objects to all or specific users in the following ways, depending on their rights:

- Across the entire Lab Manager installation
- Across an organization
- Within an organization

By default, administrators and organization administrators can share in all three ways. All other types of users (except view only) can only share within their own organization.

**To share a configuration with other users**

1. On the Workspace or Library page, move the pointer over the configuration name and choose **Sharing** from the menu.

   The Sharing 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. Choose the organization containing the users with whom you want to share the configuration or choose **Global** to view users from all organizations.

4. Select who you want to share the configuration with:
   - **Everyone** to share the configuration with all users in the selected organization.
   - **Selected Users** to share the configuration with specific users in the selected organization.

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

   When you share a configuration with a specific user in an organization, that user only has access to the configuration in that organization. To share a configuration with a user in all the organizations to which they belong, choose the Global organization.
5 Specify the access rights for the users and click OK.

   Access rights combine with the rights of a user’s role to determine how a user can
   interact with the shared configuration. Access rights cannot provided users with
   rights that they don’t already have based on their role.

   If you are sharing the configuration with users in an organization other than the
   one in which the configuration was created, you can only specify Read access.
   Configurations created in the Global organization can only be shared with Read
   access.

6 Click Done.

Managing Configurations

You can stop, undeploy, export, modify, and delete configurations.

Stopping Configurations

You can stop configurations from running using the suspend and power off operations
from the Workspace page. Undeploying a configuration also stops it from running. See
"Undeploying Configurations" on page 129.

Suspending a Configuration

Suspending a deployed configuration freezes the CPU of the virtual machines. The
virtual machines remain registered with VirtualCenter.

To suspend a configuration

On the Workspace page, move the pointer over the deployed configuration name and
choose Suspend from the menu.

Resuming the Operation of a Suspended Configuration

You can reverse a suspended state.

To resume operation of a suspended configuration

On the Workspace page, move the pointer over the deployed configuration name and
choose Resume from the menu.
Chapter 6  Working with Configurations

**Powering Off a Configuration**

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

**To power off a configuration**

On the Workspace page, move the pointer over the deployed configuration name and choose **Power Off** from the menu.

**Powering 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 a physical machine.

**To power on a configuration**

On the Workspace page, move the pointer over the deployed configuration name and choose **Power On** from the menu.

**Resetting 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**

On the Workspace page, move the pointer over the deployed configuration name and choose **Reset** from the menu.

**Undeploying Configurations**

Undeploying a configuration unregisters its virtual machines from VirtualCenter. 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 turned off, you cannot choose to save or discard state, because there is no state information to save or discard.

**To undeploy a configuration**

On the Workspace page, move the pointer over the configuration name and choose **Undeploy - Save State** or **Undeploy - Discard State** from the menu.
Exporting Configurations

You can export an undeployed configuration and all its virtual machine files from either the Workspace or Library to an SMB share. This operation requires that you have a shared folder with full control permissions at the share and file system level.

Export operations require an open SMB port on the ESX hosts. Although Lab Manager opens the port during installation, make sure that the port was not closed after the install. To check the port status, use the esxcfg-firewall -q smbClient command on each host.

Prior to exporting a configuration, Lab Manager consolidates the virtual machines in the configuration. This results in an increase in the disk space required to store the virtual machines. The exported virtual machines might also require a significant amount of disk space depending on the size of their consolidated virtual disks.

To export a configuration

1. In the left pane, click Workspace or Library.
2. Move the pointer over the configuration name and choose Export from the menu.
3. Enter the UNC path of the directory (relative to the Lab Manager Server system) where you want your configuration files stored.
   
   A sample path is \\10.6.1.246\VMwareLM\ExportConfigs. Use English characters for the UNC path.
4. Enter the user name and password for the export directory, if necessary.
5. Click OK and confirm to continue the export process.

Discarding State for Configurations

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. Lab Manager requires an available host with a compatible processor type to redeploy the configuration.

This requirement especially affects configurations that use fencing, because fencing requires that all virtual machines in the configuration are deployed on the same host. If processor incompatibility issues prevent you from deploying a configuration, you can discard the state information.

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 saved state as well.

To discard state for a configuration
1. On the Workspace or Library page, move the pointer over the undeployed configuration name and choose Discard State from the menu.
2. Click OK to confirm.

Modifying Configuration Properties
You can modify configuration properties in the Workspace or Library. Certain configuration properties can only be modified on either the Workspace or Library page. You can also change a configuration's owner. See “Changing Ownership of Configurations” on page 132.

To edit configuration properties
1. On the Workspace or Library page, move the pointer over the configuration name and choose Properties from the menu.
2. You can edit the following properties:
   - Name of the configuration.
   - Description of the configuration.
   - Whether a Library configuration is a Gold Master.
   - Deployment lease for Workspace configurations.
   - Storage lease.
   - Fencing policy.
   - Name, description, boot sequence, and boot delay for individual virtual machines in a Workspace configuration.
3. Click OK.
Changing Ownership of Configurations

The original owner of a configuration is the user who created it. You can change the owner to assign a configuration to another user in the same organization as the current owner.

To change ownership of a configuration
1. In the left pane, click Workspace or Library.
2. Move the pointer over the configuration name and choose Properties from the menu.
3. Click Change Owner.
4. Choose a new owner for the configuration and click OK.
5. Click OK.

Deleting Configurations

You can delete a configuration from the Workspace or Library. You must undeploy a configuration before you can delete it.

To delete a configuration
1. On the Workspace or Library page, move the pointer over the configuration name and choose Delete from the menu.
2. Confirm the deletion.
The media library enables you to store media image files. You can upload data (for example, 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:

- “Accessing the Media Library” on page 134
- “Synchronizing the Media Library with Media Store Files” on page 135
- “Restricting Access to Media Files” on page 135
- “Modifying Media Properties” on page 137
- “Changing Ownership of Media Files” on page 137
Accessing the Media Library

Access the Media page to work with CD, DVD, and floppy image files. Use this page to synchronize the contents of the media library with the contents of your media stores.

**To access the media library**

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

The Media page includes information about available media files:

- Name of the file and its media (in parentheses).
- The file's owner and organization.
- Sharing information, indicating whether the media is shared among users. Private media is only available to its owner.
- Type of file.
- Location of the file.

---

**NOTE** If you cannot see media files that reside on a datastore, make sure the directory containing the media (known as a media store) is enabled. See “Enabling and Disabling Media Stores” on page 183.

See “Using Text Search Filter” on page 24 for information on using the **Filter** feature.

In the top left corner, use a drop-down menu to determine the media to display:

- **My Media** – View only your media, both shared and private. This option displays all your media in the selected organization.
- **All Media** – View your media, both shared and private, and all media shared by others. This option displays all the media available to you in the selected organization.

  Administrators can choose **All Media** in the Global organization to view all media in the entire Lab Manager installation.

- **My Media in Other Organizations**– This option displays all your media in organizations other than the selected organization. This option is not available from the Global organization or for users that are members of a single organization.
Synchronizing 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 based on the latest content in the media stores, allowing users to perform ISO operations outside of the Lab Manager Web console. See “Synchronizing Media Stores” on page 183 for details on synchronizing individual media stores.

When you synchronize the media library, you become the owner of all the media that is added as a result.

Review these media file requirements:

- CD and DVD files must end with .iso.
- Floppy files must end with .img, .vfd, or .flp.

To synchronize the media library with the contents of all media stores

1. On the Media page, use the Organization drop-down menu to select the organization whose media stores that you want to synchronize.
   - Choose the Global organization to synchronize all media stores.

2. Click the Synchronize Media button.

3. Click OK to confirm.

Restricting Access to Media Files

By default, when you add media to the Lab Manager media library, the media is shared with all Lab Manager users in all organizations. You can restrict user access to media files in the following ways:

- **Organizations** – Users can only access media that is on media stores accessible from within their organization. See “Modifying Organization Properties” on page 159.

- **Sharing** – Limit the sharing properties of specific media files. Only the media owner or a user with the Administrator View and Control right, can modify media sharing properties.

**NOTE** By default, only administrators and organizations administrators have the Administrator View and Control right.
Owners can share objects to all or specific users in the following ways, depending on their rights:

- Across the entire Lab Manager installation
- Across an organization
- Within an organization

By default, administrators and organization administrators can share in all three ways. All other types of users (except view only) can only share within their own organization.

**To modify media sharing properties**

1. On the Media page, move the pointer over the media name and choose **Sharing** from the menu.

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

2. Click **Delete** to delete members.

3. Click **Add Users**.

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

5. Select who you want to share the media with:

   - **Everyone** to share the media with all users in the selected organization.
   - **Selected Users** to share the media with specific users in the selected organization.

   Select the check box for each user you want to share the media with.

   When you share a media with a specific user in an organization, that user only has access to the media in that organization. To share a media with a user in all the organizations to which the user belongs, choose the **Global** organization.
6 Specify the access rights for the user(s).

Access rights combine with the rights of a user’s role to determine how a user can interact with the shared media. Access rights cannot provide users with rights that they don’t already have based on their role.

If you chose to share the media with users in an organization other than the one in which the media was added, you can only grant Read access. Media added in the Global organization can only be shared with Read access.

7 Click Done.

Modifying 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 “Changing Ownership of Media Files” on page 137.

To modify media properties

1 On the Media page, move the pointer over a media filename and choose Properties from the menu.
2 Change the display name for the media file.
3 Enter comments on the media file.
4 Click OK.

Changing Ownership of Media Files

The original owner of a media file is the user who created it. You can change the owner to assign a media file to another user in the same organization as the current owner.

To change ownership of a media file

1 On the Media page, move the pointer over the media file name and choose Properties from the menu.
2 Click Change Owner.
3 Choose a new owner for the media file and click OK.
4 Click OK.
Use the Lab Manager Web console to manage and monitor your Lab Manager system. By default, only administrators and organization administrators can perform the operations described in this chapter.

This chapter includes these topics:

- “Monitoring Lab Manager” on page 139
- “Managing Users, Groups, and Roles” on page 142
- “Managing Organizations” on page 157
- “Managing Resources” on page 161
- “Configuring Lab Manager Settings” on page 189
- “Managing VirtualCenter and Datacenters” on page 199
- “Performing “Force” Operations” on page 203

**Monitoring Lab Manager**

Administrators and organization administrators can monitor these areas:

- **Activity Log** – View information about completed and in-progress operations in an organization or across the entire Lab Manager installation.
- **Deployed Machines** – View information about deployed virtual machines in an organization or across the entire Lab Manager installation.
Viewing the Activity Log

You can 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 administrators can see all entries. Other users can see entries about their own operations.

**To view the Activity Log**

Click Activity Log in the left pane.

The log lists activities for the currently selected organization. If you select the Global organization, 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 Owner and Organization columns provide information about who initiated a job and from which organization they initiated it.
- The job types include Configuration, Datastore, Host, Machine, Media Store, and Resource Pool.
- Job details and debugging information are available through the link in the Operation column.

Viewing Job Details

If an operation fails, you can access more information about that error from the Activity Log.

**To view details on an operation in the Activity Log**

On the Activity Log page, click the link in the Operation column.

Viewing Deployed Virtual Machines

You can view all deployed virtual machines in the Lab Manager installation or in an organization. To view the deployed virtual machines on a specific host, see “Viewing Deployed Virtual Machines on a Host” on page 169.

**To view deployed virtual machines**

Click Deployed Machines in the left pane.
The page displays a list of deployed machines for the currently selected organization. If you select the Global organization, 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.
- **VM 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 **VM Template** column.
- **Host** – Displays the ESX host name.
- **Deployed By** – Indicates the person who deployed the virtual machine.
- **Organization** – Shows the organization 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.

See “Using Text Search Filter” on page 24 for information on using the **Filter** feature.
In the top left corner, use a drop-down menu to determine the virtual machines to display:

- **My Deployed Machines** – View only your machines, both shared and private. This option displays all your deployed machines in the selected organization.

- **All Deployed Machines** – View your machines, both shared and private, and all machines shared by others. This option displays all deployed machines in the selected organization that are available to you.

Administrators can choose **All Deployed Machines** in the Global organization to view all deployed machines in the entire Lab Manager installation.

- **My Deployed Machines in Other Organizations**– This option displays all your deployed machines in organizations other than the selected organization.

This option is not available from the Global organization or for users that are members of a single organization.

### Managing Users, Groups, and Roles

An administrator or organization administrator adds users or groups to an organization and assigns each user or group a role within the organization. The organization determines which resources (resource pools, hosts, datastores, media stores, and physical networks) a user has access to, 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.

### Managing Users

Administrators and organizations administrators can view and manage users on the Users tab. Lab Manager support both LDAP users and non-LDAP users.

### Viewing Users

The Users tab displays a list of all the users (LDAP and non-LDAP) in an organization or in the entire Lab Manager installation. Users assigned the administrator role appear as members of every organization in the installation.

**NOTE** If you add an LDAP group to an organization, the members of that group do not appear on the Users tab until the first time they log in to Lab Manager.
To view users

1. In the left pane, click Users and Groups.
2. Click the Users tab.

The Users tab includes these elements:

- **Username** – Displays an icon next to the user name in this column.
  - A gray icon indicates the user is disabled and cannot log in to the Web console.
  - A blue and yellow icon indicates the user is enabled.
  - The user name for the current logged in user appears in bold text. You cannot disable or delete the current user.
  - A blue and yellow icon with a key indicates an administrator user.
  - A blue and yellow icon with a group indicates the user was added as part of an LDAP group.

- **Full Name** – The information in this field is used to indicate the owner of an object (for example, a configuration).

- **Roles** – For the Global organization, displays Administrator for users assigned to the administrator role and a dash “-” for other users. For all other organizations, displays the role(s) assigned to the user within the selected organization.

- **Deployed VM Quota** – Displays two numbers (separated by “/”). The first number indicates the number of virtual machines this user deployed. The second number indicates the number of virtual machines that the user is allowed to deploy. (The administrator sets that limit during the process of adding a user.)

- **Stored VM Quota** – Displays two numbers (separated by “/”). The first number indicates the number of virtual machine images this user stored in the configuration library. The second number indicates the total number of virtual machine images that the user is allowed to store. (The administrator sets that limit during the process of adding a user.)

**NOTE**  A user can exist in the system without an enabled status. For example, you can disable a user on extended leave.

**NOTE**  Virtual machine quota information is not displayed in the Global organization.

See “Using Text Search Filter” on page 24 for information on using the Filter feature.
Adding Users

Administrators and organization administrators can add users on the Users tab. They can also add users when creating (administrators only) or editing organizations. See “Creating Organizations” on page 157 and “Modifying Organization Properties” on page 159 for more information about adding users from the Organizations page.

The Lab Manager system can include users that exist on an LDAP server accessible to the Lab Manager server, or users that are created from the Web console. In general, VMware recommends connecting to an LDAP server to add and authenticate users. This method allows you to take advantage of user and group information that already exists, without having to recreate it in Lab Manager. See “Configuring LDAP Settings” on page 192.

Creating New Users

You can create a new non-LDAP user on the Users tab.

To create a new user

1. In the left pane, click Users and Groups.
2. Select the organization to which you want to add the user in the Organization drop-down menu.
   - Choose the Global organization to make the user available to all organizations, but assigned to none. You can assign the user to organizations later.
3. On the Users tab, click New User.
4. Do the following:
   a. Enter a user name.
      - This is the name a user logs in to the Lab Manager Web console with.
   b. Enter and confirm a password.
   c. Enter a full name.
      - All objects owned by this user display the full name in the Owner field.
   d. Enter an email address.
   e. (Optional) Enter IM and phone information.
f Choose a role for the user in the selected organization.

If you are adding a user to the Global organization, you can only choose No Role or Administrator. If you choose No Role, the user cannot log in to the Lab Manager system or access any resources until they are added to another organization.

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

h Select the Use Server Boot Sequence check box to boot virtual machines in a configuration according to the assigned boot order.

i Specify the default value for the delay time between booting each virtual machine in a configuration.

5 Click OK.

**Importing Users**

You can import LDAP users on the Users tab. You can also import any user in the Lab Manager installation (LDAP or non-LDAP) into a specific organization.

**To import a user**

1 In the left pane, click Users and Groups.

2 Select the organization to which you want to add the user in the Organization drop-down menu.

   Choose the Global organization to make the user available to all organizations, but assigned to none. You can assign the user to organizations later. See “Managing Organizations” on page 157.

3 On the Users tab, click Import Users.

4 Deselect the Show Existing Users/Groups check box to limit your search to users and groups that are not already in the organization.

5 On the Search page, type the full or partial name of the user you want to add and click Search.

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

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

   You cannot select users that are already in the organization.

7 Click the Add button.
8 Assign a role to the added users.

   If you are adding users to the Global organization, you can only choose No Role or Administrator. If you add a user who is an administrator in the Global organization, Lab Manager assigns that user the administrator role in all other organizations.

9 Click OK.

10 Repeat these steps to add more users with different roles.

**Disabling and Enabling Users**

You can only disable and enable users in the Global organization. When you disable users, they are logged out of the Lab Manager Web console and prevented from logging in again until they are enabled.

By default, only administrators can disable and enable users.

**To disable a user**

1 In the left pane, click Users and Groups.

2 Select the Global organization in the Organization drop-down menu.

3 On the Users tab, move the pointer over the user name and choose Disable from the menu.

4 Click OK to confirm the operation.

**To enable a user**

1 In the left pane, click Users and Groups.

2 Select the Global organization in the Organization drop-down menu.

3 On the Users tab, move the pointer over the user name and choose Enable from the menu.

**Removing Users**

By default, only administrators and organization administrators can remove users. Administrators can remove a user from the entire Lab Manager installation or from a specific organization. Organization administrators can only remove a user from their organization.
Removing a User from an Organization

When you remove a user from an organization, they become stranded. All of the private and shared objects (for example, media, undeployed configurations, and undeployed virtual machine templates) of the user are saved and can be reassigned a new owner by the administrator. See “Managing Stranded Users” on page 150.

To remove a user from an organization

1. In the left pane, click Users and Groups.
2. Select the organization from which you want to delete the user in the Organization drop-down menu.
3. On the Users tab, move the pointer over the user name and choose Remove from the menu.
4. Confirm the removal of the user.

Removing a User from Lab Manager

When you remove a user from the entire installation, Lab Manager removes the user from all organizations, deletes all of the private objects (for example, media, undeployed configurations, and virtual machine templates) of the user, and reassigns the shared objects to the logged in administrator.

To remove a user from Lab Manager

1. In the left pane, click Users and Groups.
2. Select the Global organization in the Organization drop-down menu.
3. On the Users tab, move the pointer over the user name, choose Disable from the menu, and click OK to confirm.
4. Move the pointer over the user name and choose Remove from the menu.
5. Confirm the removal of the user.

Modifying User Properties

By default, only administrators and organization administrators can modify user properties.

For LDAP users, you can only modify the user’s role, stored virtual machine quota, and deployed virtual machine quota.
The **Role**, **Stored VM Quota**, and **Deployed VM Quota** properties are organization-specific. If you edit these properties in any organization other than **Global**, the user’s properties are only modified for the currently selected organization. This allows a user who is a member of two organizations to have a different role or quota in each organization.

Overriding roles is especially useful for users that are part of LDAP groups. By default, all members of the group inherit the role assigned to the group. You can assign a different role to an individual group member using the **Override Inherited Roles** check box.

**To modify user properties**

1. In the left pane, click **Users and Groups**.
2. Select the organization for which you want to modify the user properties in the **Organization** drop-down menu.
   
   Choose the **Global** organization to modify the user properties for all organizations.
3. On the **Users** tab, move the pointer over the user name and choose **Properties** from the menu.
4. You can modify the following information:
   
   - **Password**.
   - **Full name, email address, and additional information about the user**.
   - **Role assigned to the user**.
     
     Select the **Override Inherited Roles** check box and choose a role. The role is specific to the selected organization. If you selected the Global organization, you can only assign the **Administrator** role.
     
     You cannot override the role for an administrator. Administrators are assigned the administrator role in all organizations.
   - **Number of virtual machine images the user is allowed to store in the configuration library**.
     
     Use an integer number to set a quota. You can leave this field blank or enter "0" to avoid setting a quota.
     
     This setting only appears for organizations other than the Global organization.
Number of virtual machines at a time the user is allowed to deploy on hosts.
Use an integer number to set a quota. You can leave this field blank or enter “0” to avoid setting a quota.
This setting only appears for organizations other than the Global organization.

5 Click OK.

**Viewing User Roles and Organizations**

You can view the roles assigned to an individual user. A user who is a member of multiple organizations can have different roles in each organization.

**To view the roles and organizations**

1 In the left pane, click Users and Groups.
2 On the Users tab, move the pointer over the user name and select Properties.
The properties page displays a list of the organizations of which the user is a member, as well as the role of the user in each organization.

**Sending User Notifications**

You can send an email notification to users in an organization or across the entire Lab Manager installation. Sending email notifications is dependent on the proper SMTP settings in the Lab Manager Web console.

**To verify SMTP settings**

1 In the left pane, click Settings.
2 Verify the information in the Email Preferences section.
3 Click Test SMTP Settings to verify the server connection works.

**To send an email notification**

1 In the left pane, click Users and Groups.
2 On the Users tab, click Send Notification.
3 Choose the recipients.

You can choose to email everyone, administrators only, or non-administrators only in the entire Lab Manager installation, or in a specific organization.

You can also choose to email all users with virtual machines deployed on a specific resource pool or with virtual machines on a specific datastore. The choices available for these last two options depend on the organization currently selected in the Organization drop-down menu.

4 Type a subject.

5 (Optional) Type a message.

6 Click Send.

Managing Stranded Users

When a user that owns objects (such as virtual machine templates, configurations, or media) is deleted, the user is considered “stranded”. When you disable an organization, all its users are stranded.

Viewing Stranded Users

Use the Stranded Users tab to view stranded users, assign their objects to a new owner, and delete the users.

To view stranded users

1 In the left pane, click Users and Groups.

2 Click the Stranded Users tab.

The Stranded Users tab includes these elements:

- **Username** – The user name of the stranded user.
- **Full Name** – The full name of the stranded user.
- **Organization** – The organization(s) of which the stranded user was a member.
- **Deployed VMs** – The number of deployed virtual machines owned by the stranded user.
- **Stored VMs** – The number of stored virtual machines owned by the stranded user.
- **Network Templates** – The number of network templates owned by the stranded user.
- **LiveLink** – The number of LiveLinks created by the stranded user. LiveLinks that have already been deployed as Workspace configurations are not included in this count, because they are owned by the user that deployed them.

- **Managed Media** – The number of media images owned by the stranded user.

  See “Using Text Search Filter” on page 24 for information on using the Filter feature.

### Transferring Ownership of Stranded User Objects

When a user gets stranded, you must reassign ownership of their objects before you can delete the user. You can reassign the objects for all stranded users or for a specific stranded user.

#### To reassign the objects of all stranded users

1. In the left pane, click **Users and Groups**.
2. Click the **Stranded Users** tab.
3. Click **Assign All To Me** to assign objects owned by stranded users to the currently logged in user.
4. Click **Delete All Empty Users** to delete users with no objects.

#### To reassign the objects of a specific stranded user

1. In the left pane, click **Users and Groups**.
2. Click the **Stranded Users** tab.
3. Move the pointer over the user name and choose **Assign Resources To Me** from the menu to assign objects owned by the stranded user to the currently logged in user.
4. Move the pointer over the user name and choose **Delete** to delete the user.

### Managing Groups

You can view and manage groups on the Groups tab. Groups and their users are defined in 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.

### Viewing Groups

The Groups tab displays all the LDAP groups in an organization or in the entire Lab Manager installation.
To view groups

In the left pane, click Users and Groups and click the Groups tab.

The Groups tab includes these elements:

- **Name** – Displays an icon next to the group name in this column.
- **Description** – Displays optional descriptive text about the LDAP group.
- **Role** – For the Global organization, displays Administrator for groups assigned to the administrator role and a dash “-” for other groups. For all other organizations, displays the role assigned to the group within the selected organization.
- **In Sync With LDAP** – A green check mark indicates whether a group is in sync with LDAP. If a group is disabled or deleted in LDAP, it is out of sync, which is indicated by a red X.

A user who is a member of an out-of-sync group, and is not a member of any other group, is considered stranded. See “Managing Stranded Users” on page 150.

See “Using Text Search Filter” on page 24 for information on using the Filter feature.

Importing LDAP Groups

By default, only administrators and organization administrators can import LDAP groups.

To import an LDAP group

1. In the left pane, click Users and Groups.
2. Select the organization to which you want to add the group in the Organization drop-down menu.
   
   Choose the Global organization to make the group available to all organizations, but assigned to none. You can assign it to organizations later. See “Managing Organizations” on page 157.
3. In the Groups tab, click Import Groups.
4. Deselect the Show Existing Users/Groups check box to limit your search to users and groups that are not already in the organization.
5. In the Search page, type the full or partial name of the group you want to add and click Search.

   Lab Manager displays the first 200 results that match the search terms.
6 Select the check box for each group you want to add.
   You cannot select group that are already in the organization.
7 Click the Add button.
8 Assign a role to the added groups.
   If you are adding groups to the Global organization, you can only choose No Role or Administrator. All members of the group are assigned the selected role. You can change the roles of individual group members later. See “Modifying User Properties” on page 147.
9 If you add a group whose members are administrators in the Global organization, Lab Manager assigns that group the administrator role in all other organizations.
10 Click OK.
11 Repeat these steps to add more groups with different roles.

**Removing Groups**

By default, only administrators and organization administrators can remove groups. Removing a group can result in stranded users. See “Managing Stranded Users” on page 150.

**To remove a group**
1 In the left pane, click Users and Groups.
2 Click the Groups tab.
3 Use the Organization drop-down menu to select the organization from which you want to remove the group.
   If you want to remove the group from all organizations, choose the Global organization.
4 Move the pointer over the group name and choose Remove from the menu.
5 Click OK to confirm the removal of the group.

**Modifying Group Properties**

By default, only administrators and organization administrators can modify group properties. You can change the description and group role.
To modify group properties

1. In the left pane, click Users and Groups.
2. Click the Groups tab.
3. Use the Organization drop-down menu to select the organization for which you want to edit the group properties.
   - If you want to edit the group properties for all organizations, choose the Global organization.
4. Move the pointer over the group name and choose Properties from the menu.
5. Change the group description and role.
   - If you are editing a group in the Global organization, you can only choose No Role or Administrator.
6. Click OK.

Managing Roles and Rights

While organizations determine which resources a user has access to, roles and rights determine what users can do with those resources. Lab Manager includes the following predefined roles with specific rights:

- **Administrator** – Includes all rights across the Lab Manager installation. Administrator users can access all organizations and perform all operations. Administrators are the only users that can access the Global organization. The administrator role is the only role that cannot be modified.
- **Organization Administrator** – Highest level of rights within an organization. Organization administrator users can do almost anything within their organization. One thing they cannot do is add or delete organization resources (datastores, media stores, resource pools, or physical networks).
- **Template Creator** – Can create virtual machine templates and configurations within an organization.
- **Application Owner** – Can create configurations within an organization.
- **User** – Can deploy and edit Workspace configurations within an organization, and also check out and LiveLink Library configurations.
- **View Only** – Can view Workspace configurations only.

See Appendix A, “Roles and Rights,” on page 207 for information about the default rights assigned to the predefined roles.
Administrators can create new roles or modify existing roles.

When a user or group is assigned to an organization, each user or group is given a role within that organization. The same user or group can have different roles in different organizations.

**Viewing Roles**

The Roles and Rights page displays a list of all the roles in the entire Lab Manager installation, regardless of which organization is selected.

**To view the roles in Lab Manager**

In the left pane, click **Roles and Rights**.

The **Roles and Rights** page includes these elements:

- **Name** – Displays the name of the role. The list includes pre-defined Lab Manager roles, as well as roles you create.

- **Description** – Displays a description of the role.

- **Organizations** – Displays organization(s) containing users assigned the role.

To view the full list of organizations containing users assigned to a role, move the pointer over the role name and choose **Properties**. Scroll to the bottom of the properties window to view the list of organizations.

See “Using Text Search Filter” on page 24 for information on using the **Filter** feature.

**Adding Roles**

By default, only administrators can add new roles. You can also create a new role by copying an existing one. See “Copying Roles” on page 156

**To add a role**

1. In the left pane, click **Roles and Rights**.
2. Click **New Role**.
3. Type a name for the new role.
4. (Optional) Enter a description for the role.
5. Assign rights to the role by selecting the check box next to each right you want to include.

See Appendix A, “Roles and Rights,” on page 207 for more information.
6. Click **OK**.
The new role appears on the Roles and Rights page. You can now assign this role to users and groups.

**Copying Roles**
You can copy an existing role (except the administrator role) to use as the basis for a new role.

**To copy a role**
1. In the left pane, click **Roles and Rights**.
2. Move the pointer over a role name and click **Copy**.
3. Type a name for the new role.
4. (Optional) Enter a description for the role.
5. Assign rights to the role by selecting and deselecting the check boxes next to each right.
   
   See Appendix A, “Roles and Rights,” on page 207 for more information.
6. Click **OK**.

The new role appears on the Roles and Rights page. You can now assign this role to users and groups.

**Deleting Roles**
By default, only administrators can delete a role. You cannot delete the administrator role, or a role that is currently in use.

**To delete a role**
1. In the left pane, click **Roles and Rights**.
2. If the Organizations column lists any organizations for the role you want to delete, view the organization properties and either reassign users to a different role, or remove the users assigned to the role.
3. Move the pointer over the role name and choose **Delete** from the menu.
4. Confirm the deletion of the role.

**Modifying Role Properties**
By default, only administrators can modify role properties. You can change the name, description, or rights of a role. The administrator role is the only role that cannot be modified.
To modify role properties
1. In the left pane, click Roles and Rights.
2. Move the pointer over the role name and choose Properties from the menu.
3. Modify the information and click OK.

Managing Organizations
Organizations determine which resources (resource pools, hosts, datastores, media stores, and physical networks) users and groups can access.

By default, only users with the Administrator role can add and delete organizations. Users with the Administrator or Organization Administrator role can edit organization properties.

Viewing Organizations
The Organizations page displays information about the organization currently selected in the Organization drop-down menu. If the Global organization is selected, Lab Manager displays information about all organizations.

To view organizations
In the left pane, click Organizations.
The Organizations page includes these elements:
- Name – The name of the organization.
- Description – Optional text description of the organization.
- Enabled – Indicates whether or not the organization is enabled. If an organization is disabled, the users in that organization cannot access the organization resources until it is enabled again.

See “Using Text Search Filter” on page 24 for information on using the Filter feature.

Creating Organizations
By default, only users with the Administrator role can create new organizations.

Part of creating an organization is adding a resource pool to the organization. When you add a resource pool to an organization, Lab Manager adds all the datastores and media stores available to the resource pool to the organization. You can remove selected datastores and media stores later. See “Modifying Organization Properties” on page 159.
To add an organization

1. In the left pane, click Organizations.
2. Select the Global organization from the Organization drop-down menu.
3. Click New Organization.
4. Enter the information for the organization:
   a. Type the name of the organization.
   b. (Optional) Type a description.
5. Add resource pools to the organization.
   a. Select an available resource pool.
   b. Click the arrow to add it to the organization.
6. Add physical networks to the organization.
   a. Select an available physical network.
   b. Click the arrow to add it to the organization.
7. Add users and groups to the organization:
   a. Click Add Users and Groups.
   b. Choose whether you want to search for users, groups, or both.
   c. In the Search text box, type your search terms and click Search.
      Lab Manager displays the first 200 results that match the search terms.
   d. Select the check box for each user or group you want to add.
   e. Click the Add button.
   f. Click OK.
8. Assign each user and group a role using the drop-down menu.
9. Click OK.
Modifying Organization Properties

By default, only administrators and organization administrators can modify organization properties. Organization administrators can edit only the organizations for which they are the administrator.

**NOTE** If you just want to modify the users and groups in an organization, move the pointer over the organization name and choose Users and Groups from the menu.

**To modify organization properties**

1. In the left pane, click Organizations.
2. Move the pointer over the organization name and choose Properties from the menu.
3. Modify the organization name and description.
4. Click Edit to add or remove users and groups.
   - Lab Manager displays current users and groups and their roles. Click Delete to remove a user or group from the organization.
   - a Click Add Users and Groups to add members to the organization.
   - b Choose whether you want to search for users, groups, or both.
   - c Deselect the Show Existing Users/Groups check box to limit your search to users and groups that are not already in the organization.
   - d In the Search text box, type your search terms and click Search.
   - Lab Manager displays the first 200 results that match the search terms.
   - e Select the check box for each user or group you want to add.
   - f Click the Add button.
   - g Click OK.
   - h Assign each user and group a role using the drop-down menu and click OK.
     See “Managing Roles and Rights” on page 154.
5. Click Edit to add or remove resource pools.
6. Click Edit to add or remove datastores.
7. Click Edit to add or remove media stores.
8. Click Edit to add or remove physical networks.
9 Set the user preferences for users in this organization:
   - **Stored VM Quota** – Number of virtual machines a user can store on datastores.
   - **Deployed VM Quota** – Number of virtual machines a user can deploy at one time.

10 Click **OK**.

### Disabling Organizations

Before you can delete an organization, you must disable it. Only administrators can enable or disable an organization.

When you disable an organization, all of its users become stranded. The users’ private and shared objects (for example, media, undeployed configurations, and undeployed virtual machine templates) are saved and can be reassigned a new owner by the administrator. See “Managing Stranded Users” on page 150.

**To disable an organization**

1 In the left pane, click **Organizations**.
2 Select the **Global** organization from the **Organization** drop-down menu.
3 Move the pointer over the organization name and choose **Disable** from the menu.
4 Click **OK** to confirm.

**To enable an organization**

1 In the left pane, click **Organizations**.
2 Select the **Global** organization from the **Organization** drop-down menu.
3 Move the pointer over the organization name and choose **Enable** from the menu.

### Removing Organizations

By default, only administrators can remove an organization. Before you can remove an organization, you must disable it and reassign any objects owned by stranded users. See “Managing Stranded Users” on page 150.

**To remove an organization**

1 In the left pane, click **Organizations**.
2 Select the **Global** organization from the **Organization** drop-down menu.
3 Move the pointer over the organization name and choose **Delete** from the menu.

4 Click **OK** to confirm.

**Managing Resources**

In Lab Manager, resources (resource pools, hosts, datastores, and media stores) can be dedicated to a specific 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.

You can access the **Resource Pools**, **Hosts**, **Datastores**, **Media Stores**, and **Physical Networks** tabs on the Resources page. On each tab, you can view available resources and monitor usage. You can also add more resources.

Only administrators can add, edit, and remove resources.

Review these definitions:

- **Resource Pool** – Logical structure that allows delegation of control over the resources of a host. Resource pools compartmentalize all resources in a cluster. You can create multiple resource pools as direct children of a host or cluster and configure them. You can then delegate control over them to other individuals or organizations. The managed resources are CPU and memory from a host or cluster. Virtual machines execute in, and draw their resources from, resource pools.

- **Cluster** – Collection of ESX hosts with shared resources and a shared management interface. When you add a host to a cluster, the host’s resources become part of the cluster’s resources. A cluster manages the resources of all its hosts.

- **Host** – Physical ESX machine where virtual machines are running.

- **Datastore** – Virtual representation of combinations of underlying physical storage resources in the datacenter. These physical storage resources can come from the local SCSI disk of the server, the Fibre Channel SAN disk arrays, the iSCSI SAN disk arrays, or Network Attached Storage (NAS) arrays.

- **Media store** – Directories for media files on NFS and VMFS datastores.

- **Physical Networks** – Physical networks available to Lab Manager.

See the VMware Infrastructure 3 documentation for general information on resource pools, clusters, hosts, and datastores.
Managing Resource Pools

Lab Manager provides access to VirtualCenter resource pools. A resource pool is a logical structure that allows delegation of control over the resources of a host. Resource pools compartmentalize all resources in a cluster. In VirtualCenter, you can create multiple resource pools as direct children of a host or cluster and configure them. You can then delegate control over them to other individuals or organizations. The managed resources are CPU and memory from a host or cluster. Virtual machines execute in, and draw their resources from, resource pools.

Viewing Resource Pools

The Resource Pools tab displays all the resource pools in an organization or in the entire Lab Manager installation. Use this tab to attach a resource pool. You can also undeploy and redeploy all virtual machines associated with a resource pool, disable, enable, detach, and access properties for a resource pool.

To view resource pools

1. In the left pane, click Resources.
2. Click the Resource Pools tab.

The Resource Pools tab includes the following information:

- Name of the resource pool that provides a pop-up menu for various operations.
- Status of whether the resource pool is enabled for use.
  - The Lab Manager administrator manually enables a resource pool.
- Name of the resource pool in VirtualCenter.
- Activity and errors for the most recent operation.
- Reserved and total amount of CPU and memory for the resource pool.
  - Reserved – Amount that Lab Manager reserves for running virtual machines in both this resource pool and any child resource pool.
  - Total – Static upper-bound on usage. The value is based on the upper limit configured for the resource pool and for any parent resource pool.
- Number of virtual machines deployed on hosts in the resource pool.
  
  This number is organization-aware. For the Global organization, Lab Manager displays the total number of virtual machines deployed on hosts in the resource pool. For any other organization, Lab Manager displays the number of deployed virtual machines from configurations created in the selected organization.

- Messages or alerts about VirtualCenter activity that could raise errors in Lab Manager.

See “Using Text Search Filter” on page 24 for information on using the Filter feature.

**Attaching and Detaching Resource Pools**

If you are setting up Lab Manager for the first time, or if you need to provide more CPU and memory resources for Lab Manager virtual machines, use the **Resource Pools** tab to attach a resource pool to Lab Manager.

By default, only administrators can attach and detach resource pools.

Before you can detach a resource pool, you must disable it and undeploy all virtual machines associated with it. See “Enabling and Disabling Resource Pools” on page 164 and “Undeploying All Virtual Machines in a Resource Pool” on page 165.

**To attach a resource pool**

1. In the left pane, click **Resources**.
2. Click the **Resource Pools** tab.
3. Select the organization to which you want to add the resource pool from the **Organization** drop-down menu.

   Choose the **Global** organization to add the resource pool as a resource available to all organizations, but assigned to none. You can assign it to organizations later.

4. Click the **Attach Resource Pool** button.
5. Select the resource pool, cluster, or host from the VirtualCenter inventory.
6. (Optional) Enter a display name for the resource pool in Lab Manager.
7. Click **OK**.

If Lab Manager detects that a host is not prepared for Lab Manager (for example, it does not have an agent that Lab Manager installed on the host), a message appears asking if you want to launch the Prepare Hosts wizard or go back and select a different resource pool. See “Preparing and Unpreparing Hosts” on page 167.
If you added the resource pool to the Global organization, you can now assign it to an organization, so the virtual machines of the organization can use its resources. See “Modifying Organization Properties” on page 159.

To detach a resource pool
1  In the left pane, click Resources.
2  On the Resource Pools tab, move the pointer over the resource pool and choose Detach from the menu.
3  Click OK to confirm the operation.

Enabling and Disabling Resource Pools
Only administrators can enable and disable resource pools. Use the Disable operation to block the use of a resource pool.

To enable a resource pool
1  In the left pane, click Resources.
2  On the Resource Pools tab, move the pointer over the resource pool and choose Enable from the menu.

To disable a resource pool
1  In the left pane, click Resources.
2  On the Resource Pools tab, move the pointer over the resource pool and choose Disable from the menu.
3  Click OK to confirm the operation.

Modifying Resource Pool Properties
By default, only administrators can modify resource pool properties. You can change a resource pool's display name and description and also clear VirtualCenter messages related to a resource pool.

To modify resource pool properties
1  In the left pane, click Resources.
2  On the Resource Pools tab, move the pointer over the resource pool and choose Properties from the menu.
3 Modify the name or description.
4 Clear messages regarding VirtualCenter activity if necessary.
5 Click OK.

**Undeploying All Virtual Machines in a Resource Pool**

Administrators can undeploy all virtual machines associated with a resource pool, for example to perform maintenance. This operation undeploys the virtual machines on all hosts in the resource pool. To undeploy all virtual machines on a specific host, see “Undeploying All Virtual Machines on a Host” on page 171.

Undeploying affects anyone using the virtual machines and can result in partially deployed configurations. You must manually redeploy the undeployed virtual machines. The Undeploy all VMs operation suspends the virtual machines and saves their state.

**To undeploy all virtual machines in a resource pool**

1 In the left pane, click Resources.
2 On the Resource Pools tab, move the pointer over the resource pool and choose Disable from the menu.
3 Click OK to confirm.
4 Move the pointer over the resource pool and choose Undeploy All VMs from the menu.
   
   This operation is organization-aware. For the Global organization, Lab Manager undeploys all the virtual machines deployed on the resource pool. For any other organization, Lab Manager only undeploys the virtual machines deployed by users in the selected organization.
5 Click OK to confirm.

**Managing Hosts**

A host is an ESX server that provides CPU and memory resources for Lab Manager virtual machines. You can add VirtualCenter hosts to Lab Manager using the Resource Pools tab. See “Attaching and Detaching Resource Pools” on page 163.

**Viewing Hosts**

The Hosts tab displays all the hosts in an organization or in the entire Lab Manager installation.
To view hosts

1. In the left pane, click Resources.
2. Click the Hosts tab.

The Hosts tab includes the following information:

- Name of the ESX host that provides a pop-up menu for various operations.
- State of the host:
  - Ready – Indicates whether a host is prepared or not.
    When Lab Manager prepares a host, it completes certain tasks such as checking the ESX version and installing an agent. If the host is not prepared properly, Lab Manager cannot mark it as ready for use.
  - Available – Indicates whether a host is available or not.
    If a host is marked as unavailable, some condition exists in VirtualCenter that prevents Lab Manager from using this host.
    For example, the host could be disconnected from VirtualCenter or in maintenance mode. Refer to the Messages column for more information about why a host is unavailable.
  - Enabled – Indicates whether a host is enabled or disabled in Lab Manager.
    A user with the appropriate rights can enable and disable hosts.
- Number of virtual machines deployed on the host.
  This number is organization-aware. For the Global organization, Lab Manager displays the total number of virtual machines deployed on the host. For any other organization, Lab Manager displays the number of deployed virtual machines from configurations created in the selected organization.
- Activity and errors for the most recent operation.
- Name of the VirtualCenter cluster to which the host belongs (if applicable).
- Reserved and total amount of CPU and memory for the host.
  - Reserved – Amount that Lab Manager reserves from the resource pool for running virtual machines in both this resource pool and any child resource pool.
  - Total – Static upper-bound on usage. The value is based on the upper limit configured for the resource pool and for any parent resource pool.
Resource pools associated with the host.

Messages about VirtualCenter activity that could generates errors in Lab Manager.

From the table, you can undeploy, redeploy, and force undeploy all virtual machines on a host. Other operations include disabling and unpreparing hosts, along with accessing deployed virtual machines and properties of a host.

See “Using Text Search Filter” on page 24 for information on using the Filter feature.

Preparing and Unpreparing Hosts

Lab Manager prompts administrators to start the Prepare Hosts wizard after attaching a resource pool with hosts that are not yet prepared by Lab Manager. This preparation involves such tasks as installing an agent on the hosts.

You can also start the wizard from the Hosts tab for any hosts that are unprepared. Unprepared hosts include new hosts added to a cluster in VirtualCenter and hosts that are not prepared right after you attach a resource pool.

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.

Unprepare a host to remove it from use in the Lab Manager environment.

To prepare a host

1. Click Resources in the left pane.
2. On the Hosts tab, move the pointer over the host name and choose Prepare from the menu.
3. Provide connection details:
   a. Select or deselect the check box that specifies whether to use the same user name and password for all hosts.
   b. If you use the same user name and password for all hosts, enter the user name and password.
   c. Select the check boxes for hosts to prepare and enter individual user names and passwords if necessary.
   d. Click Next.
4. Select the datastores you want to enable for virtual machine use and click Finish.
To unprepare a host

1. Click Resources in the left pane.
2. In the Hosts tab, move the pointer over the host name to choose Unprepare from the menu.
3. Click Unprepare.

During the unprepare operation, Lab Manager tries to uninstall the Lab Manager agent. If this attempt fails, Lab Manager continues to unprepare the host and relays any errors in a message.

Enabling and Disabling Hosts

By default, only administrators can 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. If you want to perform maintenance on a host, undeploy the virtual machines. See “Undeploying All Virtual Machines on a Host” on page 171.

To enable a host

1. In the left pane, click Resources.
2. On the Hosts tab, move the pointer over the host and choose Enable from the menu.

To disable a host

1. In the left pane, click Resources.
2. On the Hosts tab, move the pointer over the host and choose Disable from the menu.
3. Click OK to confirm.

Modifying Host Properties

By default, only administrators can modify properties for ESX hosts.

To modify host properties

1. In the left pane, click Resources.
2. In the Hosts tab, move the pointer over the host and choose Properties from the menu.
3 Do any of the following and then click **OK**:

- Enter a description.
- Change the user name and password for the host.
- Change the maximum number of deployed virtual machines allowed on the host.

The **Maximum Number of VMs** field is only available for a cluster without DRS and applies to the virtual machines deployed in this Lab Manager installation. Lab Manager might raise the quota over the maximum value of 200 in certain circumstances.

- Enable different datastores for virtual machine use.
  
  You can only deploy virtual machines on the selected datastores.

- Clear messages regarding VirtualCenter activity if necessary.

The maximum quota for deployed virtual machines on a host might increase in these circumstances:

- VMotion or VMware HA failover occurs.
- If someone switches a DRS cluster to a cluster without DRS, the default quotas associated with that non-DRS cluster can negate the Lab Manager quota.

**Viewing Deployed Virtual Machines on a Host**

You can view the deployed virtual machines on a specific ESX host. To view the deployed virtual machines across all hosts, see “**Viewing Deployed Virtual Machines**” on page 140.

**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 choose **Deployed VMs** from the menu.

The Deployed Virtual Machines page displays a list of virtual machines from the currently selected organization that are deployed on the selected host. If you select the Global organization, the page lists all the virtual machines deployed on the host.

On this page, a table includes this information:

- Access to the virtual machine console through the thumbnail icon.
- Name of the virtual machine includes a pop-up menu to view the virtual machine console or undeploy the virtual machine.
■ Status indicating that the virtual machine is deployed.
■ The name of the configuration the virtual machine resides in.
   A dash in the Configuration column indicates the virtual machine is a virtual machine template.
■ NIC information for the virtual machine.
■ IP address of the virtual machine or DHCP specification.
■ External IP address for the virtual machine if it requires one.
■ 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 for a configuration or is deployed, a dash appears in the VM Template column.
■ Person who deployed the virtual machine.
■ Sharing information.
■ Date and time of deployment.
■ Messages about the virtual machine.

See “Using Text Search Filter” on page 24 for information on using the Filter feature.

In the top left corner, use a drop-down menu to determine the virtual machines to display:

■ My Deployed Machines – View only your machines, both shared and private. This option displays all your deployed machines in the selected organization.

■ All Deployed Machines – View your machines, both shared and private, and all machines shared by others. This option displays all deployed machines in the selected organization that are available to you.

   Administrators can choose All Deployed Machines in the Global organization to view all deployed machines in the entire Lab Manager installation.

■ My Deployed Machines in Other Organizations – This option displays all your deployed machines in organizations other than the selected organization. This option is not available from the Global organization or for users that are members of a single organization.
Undeploying All Virtual Machines on a Host

Administrators can undeploy all the virtual machines associated with a specific host. This is useful when you want to perform maintenance on a host.

You can either undeploy or redeploy virtual machines. Undeploying affects anyone using those virtual machines and can result in partially deployed configurations. You must manually redeploy the undeployed virtual machines. The **Undeploy all VMs** operation suspends the virtual machines and saves their state.

Redeploying first undeploys the virtual machines and then redeploys them to other available hosts. You must disable a host before you can redeploy all its virtual machines. The **Redeploy all VMs** operation suspends the virtual machines and saves their state.

When redeploying, the organization from which **Redeploy All VMs** is initiated must have access to another host that is CPU compatible with the current host and has enough capacity to deploy the virtual machines. For fenced configurations, all virtual machines in that configuration move together to another host.

**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 choose **Undeploy All VMs** from the menu.
   
   This operation is organization-aware. For the Global organization, Lab Manager undeploys all the virtual machines deployed on the host. For any other organization, Lab Manager only undeploys the virtual machines deployed by users in the selected organization.
3. Click **OK** to confirm.

**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 choose **Disable**.
3. Click **OK** to confirm.
4. Move the pointer over the host name and choose **Redeploy All VMs**.
   
   This operation is organization-aware. For the Global organization, Lab Manager redeploys all the virtual machines deployed on the host. For any other organization, Lab Manager only redeploys the virtual machines deployed by users in the selected organization.
5. Click **OK** to confirm.
Managing Datastores

A datastore provides storage resources for virtual machines. Lab Manager supports VMFS and NFS datastores, which it accesses through VirtualCenter. You can add datastores to Lab Manager by attaching them to ESX hosts in VirtualCenter.

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 host.

Datastores can also be enabled as media stores. See “Managing Media Stores” on page 181.

Viewing Datastores

The Datastores tab displays all the datastores in an organization or in the entire Lab Manager installation. Use the Datastores tab to perform datastore operations.

To view datastores

1. In the left pane, click Resources.
2. Click the Datastores tab.

The Datastores page includes the following information:

- Name of the datastore that provides a pop-up menu for various operations.
- Type of datastore (NFS or VMFS3 storage).
- State of the datastore:
  - **Connected** – Indicates whether or not a host in Lab Manager is connected to the datastore.
    You can disconnect a datastore using VirtualCenter.
  - **Enabled** – Indicates whether or not a datastore is available for use.
    You can disable the datastore to prevent users from deploying virtual machines or creating media files on the datastore.
  - **VM Creation Enabled** – Indicates whether or not you can store virtual machines on the datastore.
  - **Media Store Creation Enabled** – Indicates whether or not you can create media directories on the datastore.
    These directories are known as media stores.
  - Activity and errors for the most recent operation.
Chapter 8 Administering and Monitoring Lab Manager

- Amount of datastore disk space in use and the total amount of disk space.
- Percentage of datastore disk space used.
- Alerts on VirtualCenter activity that could generate errors in Lab Manager.
  
  For example, Lab Manager creates an installation directory for virtual machines and would generate a message if it discovers an existing directory with the same name.

See “Using Text Search Filter” on page 24 for information on using the Filter feature.

Removing Datastores

Removing a datastore deletes all its virtual machines, media stores, and media files from the Lab Manager database. By default, only administrators can remove datastores.

NOTE The operation does not delete files in the actual datastore.

Before you remove a datastore, you must do the following:

- Disconnect the datastore in VirtualCenter.
  
  For example, if the datastore is connected to three hosts managed by Lab Manager, disconnect the datastore from all three hosts through VirtualCenter.

- Disable the datastore. See “Enabling and Disabling Datastores” on page 174.

- Make sure that the media files associated with a datastore are not in use.
  
  If you remove a datastore with media stores and you add the datastore back to the Lab Manager environment at a later time, you need to recreate the media stores because the original ones are no longer available.

To remove a datastore

1. Click Resources in the left pane.

2. On the Datastores tab, move the pointer over the datastore and choose Remove from the menu.

3. Confirm the operation.
Enabling and Disabling Datastores

Administrators can enable and disable datastores for virtual machines, and datastores for media (media stores).

When you disable a datastore, the configurations associated with the datastore cannot be deployed.

You can also disable the creation of virtual machines or media stores in a datastore. When you disable virtual machine creation, the following operations cannot be performed:

- Making linked or full clones
- Taking snapshots
- Reverting snapshots
- Creating virtual machine templates or virtual machines
- Adding new virtual machines to existing configurations
- Importing virtual machines

To enable a datastore

1. In the left pane, click Resources.
2. In the Datastores tab, move the pointer over the datastore and choose Enable from the menu.

To disable a datastore

1. In the left pane, click Resources.
2. In the Datastores tab, move the pointer over the datastore and choose Disable from the menu.
3. Click OK to confirm.

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 choose Disable VM Creation from the menu.
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 choose Disable Media from the menu.

Modifying Datastore Properties

By default, only administrators can modify the properties of datastores.

To modify datastore properties

1 In the left pane, click Resources.
2 In the Datastores tab, move the pointer over the datastore and choose Properties from the menu.
3 Change the display name and disk space thresholds.
4 Clear messages regarding VirtualCenter activity if necessary, and click OK.

Viewing Virtual Machine Datastore Usage

On the Virtual Machine Datastore Usage page, administrators and organization administrators can monitor disk space usage for all virtual machines and complete maintenance tasks.

The Virtual Machine Datastore Usage page shows how much total storage (inclusive of the space occupied by hidden nodes associated with the virtual machine) can be reclaimed by deleting a virtual machine.

To access virtual machine datastore usage

1 In the left pane, click Resources.
2 On the Datastores tab, click the View Datastore Usage button.
   To view the usage of a single datastore rather than the contents of all virtual machine datastores, click the Datastores tab, move the pointer over the datastore name, and choose Open from the menu.
3 Select the organization for which you want to view datastore usage from the Organization drop-down menu.
   Choose the Global organization to view datastore usage for all organizations.
On this page, a table includes this information:

- Virtual machine name that provides a pop-up menu for operations.
- Name of the configuration containing the virtual machine.
  A dash appears in this column for virtual machine templates.
- The datastore for the virtual machine.
- Name and organization of the user who owns the virtual machine.
- Status (for example, deployed or undeployed) of the virtual machine.
- Amount of space that you can reclaim upon deleting the virtual machine.
  This space includes the area 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 “Viewing Virtual Machine DatastoreDirectories” on page 177.

**NOTE** Use the **Refresh Disk Space** button to refresh the disk space to view an
accurate estimate of the space.

- The directory ID of the revert point (if applicable).
- Number of delta disks the virtual machine relies on.
  For various changes, Lab Manager freezes the original delta disk and creates a new
  one.
  The chain length indicates how scattered the virtual machine image is across the
  directories of a datastore. Lab Manager messages the user when you need to
  consolidate a chain.
- Date to delete the virtual machine or mark it for deletion.
  This column displays the date that the virtual machine’s storage lease expires.
  Depending on the resource cleanup settings specified by the administrator,
  Lab Manager either deletes the virtual machine or marks it for deletion. See
  “Configuring Resource Cleanup Settings” on page 198.

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.
Viewing Virtual Machine Datastore Directories

The Context view provides a high level view of the dependencies between virtual machines. The Context view for a virtual machine displays a tree view of the virtual machine’s relationship to other virtual machines on which it depends (ancestor nodes) and which depend on it (child nodes). Each node in the tree represents a specific directory location on the datastore.

Lab Manager creates nodes for operations such as linked cloning. When you make a linked clone a virtual machine, Lab Manager creates a delta disk instead of 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 as a whole 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. A virtual machine with a long chain length will have a much more Context view than a virtual machine with a short chain length.

Deleting a virtual machine deletes the storage occupied by the virtual machine node and any ancestor node that can be safely deleted. Lab Manager will not delete an ancestor node under these conditions:

- The ancestor directory has other child directories dependent 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 uses 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 8-1 shows a basic example of a tree of related virtual machines and the internal nodes affected by a delete operation.

Figure 8-1. Example of Nodes Affected by a Delete Operation

If you delete node D, node B stays intact because node C and E are dependent 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).
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 the virtual machines that you can see in the Lab Manager 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.

Blue boxes indicate deployed directories, while a yellow box indicates the selected virtual machine. The default color for boxes is gray.

If you move the pointer over a box, you can see various details, including the amount of space the virtual machine or internal node consumes and the total amount of space reclaimed if the node is removed. For example, if you see Size: 277 MB (554 MB), 277 reflects the space of the selected node, and 554 is the total space. The total amount is calculated by adding the space of the node and all associated nodes to the right of the selected node.

Previously deployed and currently deployed virtual machines show when they were last deployed. Internal nodes do not display this information.

A turquoise box indicates a revert reference. This reference point implies another directory (created by a full clone operation on a different datastore) exists outside of the displayed directory tree but uses a directory linked to this revert reference as a revert point. This dependency affects your ability to delete directories.

To delete a directory linked to a revert reference, delete the virtual machine associated with the revert reference and the descendants of the directory.

**To view virtual machine datastore directories**

1. Click **Resources** in the left pane.
2. In the **Datastores** tab, click the **View Datastore Usage** button.
   - To view the usage on a single datastore, move the pointer over the datastore name and choose **Open** from the menu.
3. Click the **Refresh Disk Space** button to ensure that the data is current.
4. Move the pointer over the virtual machine name and choose **Context** from the menu.

You can use the **SSMove** utility to move an entire datastore, or a specific tree of virtual machines, to another datastore. The **SSMove** utility is available on the Lab Manager server in the following location:

[C:\]**Program Files\VMware\VMware Lab Manager Server\Tools\SSMove**
Deleting Expired Virtual Machines

When the storage lease for a virtual machine expires, Lab Manager either deletes the virtual machine or marks it for deletion, depending on the resource cleanup settings. See “Configuring Resource Cleanup Settings” on page 198.

You can delete virtual machines that are marked for deletion from the Virtual Machine Datastore Usage page.

**To delete expired virtual machines**

1. Click **Resources** in the left pane.
2. In the **Datastores** tab, click the **View Datastore Usage** button.
   - To view the usage on a single datastore, move the pointer over the datastore name and choose **Open** from the menu.
3. Click the **Refresh Disk Space** button to ensure the data is current.
   - For all virtual machines with expired storage leases, the **Status** column displays **Expired**.
4. Click the **Delete Expired VMs** button.
   - Lab Manager deletes all the undeployed virtual machines with a storage lease that expired. This operation is organization-aware. For the Global organization, Lab Manager deletes all the expired virtual machines. For any other organization, Lab Manager only deletes the expired virtual machines owned by users in the selected organization.

Renewing the Storage Lease for an Expired Virtual Machine

When the storage lease for a virtual machine expires, Lab Manager either deletes the virtual machine or marks it for deletion, depending on the resource cleanup settings. See “Configuring Resource Cleanup Settings” on page 198.

You can renew the storage lease for virtual machines that are marked for deletion from the Virtual Machine Datastore Usage page.

**To renew the storage lease for an expired virtual machine**

1. Click **Resources** in the left pane.
2. In the **Datastores** tab, click the **View Datastore Usage** button.
   - To view the usage on a single datastore, move the pointer over the datastore name and choose **Open** from the menu.
3 Click the Refresh Disk Space button to ensure the data is current.
   For all virtual machines with expired storage leases, the Status column displays Expired.
4 Move the pointer over the virtual machine name and choose Renew Storage Lease from the menu.
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. Lab Manager renews expired leases for the same length of time as the original lease (for example, 30 days).

Deleting Revert Points
Like virtual machines, revert points take up space on datastores. You can free up that space by deleting revert points.

To delete revert points
1 Click Resources in the left pane.
2 In the Datastores tab, click the View Datastore Usage button.
   To view the usage on a single datastore, move the pointer over the datastore name and choose Open from the menu.
   The Revert Dir ID lists the directory IDs of the revert points.
3 Click the Refresh Disk Space button to ensure that the data is current.
4 Move the pointer over a virtual machine name and choose Delete Revert Point from the menu.

Consolidating a Virtual Machine Based on Datastore Usage
You can only consolidate undeployed virtual machines. For information on consolidation, see “Consolidating Virtual Machines” on page 44.

To consolidate virtual machine based on datastore usage
1 Click Resources in the left pane.
2 In the Datastores tab, click the View Datastore Usage button.
   To view the usage on a single datastore, move the pointer over the datastore name and choose Open from the menu.
3 Move the pointer over the virtual machine name and choose **Consolidate** from the menu.

4 Select a datastore and click **OK**.

You can keep the consolidated virtual machine in the current datastore (displayed in bold), or you can move the consolidated virtual machine to a different datastore.

### Deleting a Virtual Machine or Configuration Based on Datastore Usage

You can delete a specific virtual machine or the entire configuration that contains the virtual machine. To delete a virtual machine or configuration, it must be undeployed.

**To delete virtual machine or configuration based on datastore usage**

1 Click **Resources** in the left pane.

2 In the **Datastores** tab, click the **View Datastore Usage** button.

   To view the usage on a single datastore, move the pointer over the datastore name and choose **Open** from the menu.

3 Move the pointer over an undeployed virtual machine name and choose **Delete** from the menu to delete a virtual machine, or choose **Delete Configuration** to delete the entire configuration that contains the virtual machine.

4 Confirm the deletion.

### 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. See “**Synchronizing Media Stores**” on page 183.

### Viewing Media Stores

The Media Stores tab displays all the media stores in an organization or in the entire Lab Manager installation.

**To view media stores**

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

2 Click the **Media Stores** tab.
The **Media Stores** tab includes the following information:

- Name of the media store that provides a pop-up menu for various operations.
- Type of datastore (NFS of VMFS3) where the media store resides.
- State of the media store:
  - **Datapath Enabled** – Indicates whether or not the datastore where the media store resides is available for use.
  
  This setting is specified in the **Datapath** tab.
  
  - **Media Enabled** – Indicates whether or not you can use media on the media store. If you disable a media store, the Lab Manager media library will not display the files on that media store.
  
  - Amount of media store space in use and the total amount of space.
  - Percentage of media store space used.
  - Location of the media store.

Use this tab to add a media store. From the table, you can disable or remove a media store. Other operations include synchronizing the contents of the media store with the Lab Manager media library and accessing media store properties.

See “Using Text Search Filter” on page 24 for information on using the **Filter** feature.

### Adding Media Stores

By default, only administrators can 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*.

**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.

   Choose the Global organization 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 choose **Enable Media** from the menu.
4 On the **Media Stores** tab, click the **Add Media Store** button.

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 must not have the same NFS path root.

8 Click **OK**.

9 Move the pointer over the media store name and choose **Synchronize** from the menu.

**Synchronizing Media Stores**
When synchronize the contents of a media store with the Lab Manager media library, Lab Manager adds files to or deletes files from the library based on the files that currently reside on the selected media store.

To synchronize the Lab Manager media library with all media stores, see “**Synchronizing the Media Library with Media Store Files**” on page 135.

**To synchronize media with a media store**
1 Click **Resources** in the left pane.

2 In the **Media Stores** tab, move the pointer over the media store name and choose **Synchronize** from the menu.

**Enabling and Disabling Media Stores**
Administrators can enable and disable media stores. When you disable a media store, you cannot deploy configurations associated with the media store.

**To enable a media store**
1 In the left pane, click **Resources**.

2 On the **Media Stores** tab, move the pointer over the media store and choose **Enable** from the menu.
To 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 choose Disable from the menu.

3. Click OK.

Use the disable operation to block the use of a media store.

Changing the Name of a Media Store

By default, only 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. In the Media Stores tab, move the pointer over the media store and choose Properties from the menu.

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.

Viewing Physical Networks

The Physical Networks tab displays all the physical networks in an organization or in the entire Lab Manager installation.

To view physical networks

In the left pane, click Resources and click the Physical Networks tab.

The Physical Networks tab includes the following information:

- Name of the physical network that provides a pop-up menu for various operations.
- VLAN ID
- Gateway
- Subnet mask
Primary DNS

IP addressing mode

Messages

IP Pool (used/total)

Use this tab to add a physical network. From the table, you can delete a physical network, as well as access its properties and IP pool.

See “Using Text Search Filter” on page 24 for information on using the Filter feature.

Adding a Physical Network

By default, only administrators can add a physical network.

**To add a physical network**

1. In the left pane, click Resources.

2. Select the organization to which you want to add the physical network from the Organization drop-down menu.

   Choose the Global organization to add the physical network as a resource available to all organizations, but assigned to none. You can assign it to organizations later.

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

4. Type a name for the network.

   The name can only contain alphanumeric characters (a–z, A–Z, 0–9), hyphens, underscores, or periods.

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

6. Choose the IP addressing modes for the network:

   - **Static - IP Pool** allows Lab Manager to pull static IP addresses from the IP pool.

   - **DHCP** allows Lab Manager to pull IP addresses from a DHCP server.

   This option avoids specifying an IP address or IP range. However, you cannot use Lab Manager fencing or connect virtual networks to physical networks with DHCP.
- **Static - Manual** requires you to specify a static IP address when configuring the network interface for a virtual machine connected to. The IP address you specify cannot belong to the network IP pool. However, if you want to use fencing, you must have IP addresses in the IP Pool for use as virtual machine external IP addresses.

7 If you chose a static IP addressing mode, specify the static mode settings and IP pool:

a Type the subnet mask, default gateway, primary DNS, secondary DNS (optional), and DNS suffix (optional).

b Type an IP address or IP address range and click the **Add** button.

8 Select the **Allow Fenced Only** check box to require users to deploy configurations using the network in fenced mode.

Choose a fencing 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 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.

9 If you want to bind a host to a specific virtual switch, choose a virtual switch from the drop-down menu.

10 Click **OK**.

**Viewing IP Pool Usage for a Physical Network**

You can monitor the IP pool of a physical network. If a network is running out of IP addresses, you can add more. See “Adding IP Addresses to the IP Pool of a Physical Network” on page 187 for information about adding IP addresses.
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.

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 use the external IP address to access a virtual machine from outside a fenced configuration, for example. When you undeploy this configuration, Lab Manager releases the external IP addresses.

You can control the length of time Lab Manager reserves released IP addresses before returning them to the IP pool. See “Lab Manager Preferences” on page 189.

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 choose **IP Pool** from the menu.

   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. You can see the IP address, addressing mode, machine name, configuration name, and organization and user. The **Deallocate In** column indicates the amount of time remaining before an unused external IP address becomes available.

**Adding IP Addresses to the IP Pool of a Physical Network**

By default, only administrators can add IP addresses to a physical network.

**To add 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 choose **Properties** from the menu.
3 Type an IP address or IP address range in the Static IP Address Pool text box and click the Add button.

4 Click Update.

Removing IP Addresses from the IP Pool of a Physical Network
By default, only administrators can remove IP addresses from a physical network.

To remove IP addresses from 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 choose Properties from the menu.

3 Type 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 the Remove button.

   Lab Manager removes the IP address(es) from the IP pool.

4 Click Update.

Modifying Physical Network Properties
By default, only 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 choose Properties from the menu.

3 Edit the network properties.

4 Click Update.

For information about the properties of a physical network, see “Adding a Physical Network” on page 185

Deleting a Physical Network
By default, only 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 choose Delete from the menu.
3. Click OK to confirm.

Configuring Lab Manager Settings

Administrators can access the General, LDAP, License, Guest Customization, SupportLink, Resource Cleanup, and VirtualCenter tabs from the Settings link in the left pane to modify various Lab Manager settings.

Configuring General Settings

The General tab covers Lab Manager preferences, email preferences, and system alert preferences.

To access settings on the General tab

1. In the left pane, click Settings.
2. Click the General tab.
3. Modify the Lab Manager, email and system alerts preferences and click OK.

Lab Manager Preferences

Review the Lab Manager preferences:

- **Login Mode** – Lab Manager can retain the user name and password and can also log in the user.
  - **Remember User Name only** – Lab Manager retains the user name but not the password.
  - **Automatically Login** – Lab Manager logs users in when they start the Lab Manager application.

Lab Manager uses persistent cookies (physically stored in the computer hard disk) to retain the login information. If you delete the browser cookies, this information is no longer available until after you log in again.
- **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 in case an ID collision occurs.

- **Lab Manager Host IP Address** – IP address of the Lab Manager Server system.

- **Lab Manager Host Name** – DNS name of the Lab Manager Server system.

- **Session Timeout (Minutes)** – Amount of time you want the Lab Manager application to remain active without user interaction.

- **IP Release Timeout (Seconds)** – Specifies how long to reserve released IP addresses before returning them to the IP pool for use by other virtual machines.

  See “Viewing IP Pool Usage for a Physical Network” on page 186.

- **Host Refresh Frequency (Seconds)** – Frequency of checking whether ESX hosts are accessible or hung. The default is 60 seconds.

- **Host Hung Timeout (Seconds)** – Length of time to wait before marking a host as hung.

  For example, if the timeout is 20 seconds and Lab Manager pings a host every 10 seconds, Lab Manager marks the system as hung if it fails to respond for 20 seconds.

- **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 “Modifying Host Properties” on page 168.

  **Import from VirtualCenter Timeout (Minutes)** – Length of time to wait before failing an import from VirtualCenter operation. The default is 120 minutes.

  When Lab Manager imports a virtual machine from VirtualCenter, VirtualCenter clones the virtual machine. The timeout value applies to this cloning task.

- **Import/Export from SMB Timeout (Minutes)** – Length of time to wait before failing an import or export from and SMB operation. The default is 120 minutes.

  If you try to import a virtual machine with a large hard disk and the operation times out, increase this timeout.
- **Storage Server Garbage Collection Frequency (Seconds)** – 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 any 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)** – Days of log history to keep before deleting it. The default is 90 days. Specify 0 to never delete logs.

- **Activity Log History shown (Days)** – Days of log history to display in the Web console. The default is 30 days. Specify 0 to show all activity.

- **Display Background Image on Login Screen** – Specify 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.

**Email Preferences**

- **SMTP Server** – DNS host name or IP address of the mail server that Lab Manager uses for sending out emails.

- **Requires User Name** – Select if the SMTP server requires a user name and enter the user name and password for the SMTP server account.

- **Sender’s Email Address** – Email address from which Lab Manager emails are sent. Lab Manager uses the sender’s email address specified here for system alerts (see “System Alerts” on page 192) and 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.

- **Default Email Subject Prefix** – Initial text for the subject field of messages.

- **SMTP Test Destination** – Destination email address for testing SMTP settings.

- **Test SMTP Settings** – Click to verify that the server connection works.
System Alerts

Lab Manager can send system alert emails to all Lab Manager administrators or to a specified list of email addresses.

- **All Lab Manager Administrators**—Select this option to send system alerts to all administrators.
- **These Email Addresses**—Select this option to send system alerts to a specified list of email addresses. Enter comma-separated email addresses for the recipients in the text box.

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 VirtualCenter Server.
- Lab Manager detects that an ESX host is not responding or starts responding.

Configuring LDAP Settings

You can configure Lab Manager to create and authenticate user credentials against an LDAP server. This setup eases the administration of users in the system. 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.

For information on manually creating Lab Manager user accounts for non-LDAP users, see “Adding Users” on page 144.

To provide Lab Manager access to LDAP users:

- Specify the LDAP settings (described below).
- Add LDAP users or groups to a Lab Manager organization (see “Managing Organizations” on page 157).

When an LDAP user that 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 update the information in the LDAP directory. If you want to add, delete, or modify LDAP users or groups, you must do so in the LDAP directory. Lab Manager synchronizes user and group information with the LDAP directory on a regular basis.

To configure LDAP settings
1. In the left pane, click **Settings**.
2. Click the **LDAP** tab.
3. Modify the LDAP settings and click **OK**.

Locating an LDAP Server
Before entering host name and port information for your LDAP server, you can click the **Locate LDAP Server** button to have Lab Manager try to locate an available LDAP server.

When you 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** fields. If Lab Manager finds multiple LDAP servers, it chooses one based on the DNS LDAP priority and weight.

**LDAP Connection**

- **Server** – 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 requires that the Lab Manager server is in the same domain as the Active Directory domain controller and provides redundancy and load-balancing benefits.

- **Port** – If the LDAP server is listening on a non-default port, enter the port number here. For LDAP, the default port is 389; for LDAPS, the default port is 636.

- **Base Distinguished Name** – Location in the LDAP directory where Lab Manager connects.

  Lab Manager can detect the base DN if your LDAP server supports this. Leave this field blank and click **Test LDAP Settings** to determine if your server supports base DN detection.

  VMware recommends connecting at the root. In which case, you would enter the domain components only, for example: `DC=vmware,DC=com`.
To connect to a node in the tree, specify 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, the only LDAP users that can log in to Lab Manager are users in that OU. In some cases, this 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 will be able to log in to Lab Manager and access the organization. Members of the LabMan group from the DublinOffice OU will be excluded.

**Use LDAPS** – If you have an OpenLDAP server set up to support LDAPS, select LDAPS to make OpenLDAP traffic confidential and secure by using LDAP over SSL (Secure Sockets Layer). This option is only available for OpenLDAP, because Active Directory supports secure binding by default, and Lab Manager only connects to Active Directory using secure binding.

If you do not have an OpenLDAP server set up to support LDAPS, refer to your OpenLDAP documentation.

**Accept all certificates** – Allows 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 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.
Authentication Method – 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. If you choose Digest-MD5, you must provide MD5 Realm information.
- **Basic** – Choose this method for OpenLDAP with LDAPS. If you choose Basic without LDAPS, be aware that the LDAP password is sent over the network in clear text.
- **MD5 Realm** – For Digest-MD5 authentication, you must authenticate to a specific realm. Type the realm information here.
- **User Name/Password/Confirm Password** – User name and password to connect to the LDAP server.

If anonymous read support is enabled on your LDAP server, you can leave these fields blank. By default, Active Directory does not enable anonymous read, but OpenLDAP does.

- **Synchronization Every ___ (minutes)** – How often Lab Manager synchronizes with the LDAP server. The default is every 15 minutes. Synchronizing updates Lab Manager user and group information, based on changes to the LDAP directory.

To synchronize immediately, click the Synchronize LDAP button.

### LDAP Connector and Schema

- **Connector** – Choose Active Directory or OpenLDAP.

  Certain options are enabled or disabled based on your selection. For example, only Active Directory support serverless binding, and only OpenLDAP supports LDAPS.

- **LDAP Schema** – Defines the required and optional attributes for an LDAP directory entry.

  If you selected Active Directory as the connector, you can choose, **Active Directory** or **Custom** as the LDAP Schema. Choose **Active Directory**, unless you are using a custom schema.

  If you selected OpenLDAP as the connector, you can choose **Custom**, **OpenLDAP(1)**, **OpenLDAP(2)**, or **OpenLDAP(3)**. OpenLDAP(1), (2), and (3) represent the most common implementations of OpenLDAP. Check with your OpenLDAP administrator to determine which schema to choose (or if you need a custom schema). Choosing **OpenLDAP(1)** should work in most OpenLDAP environments that are not significantly customized.
The combination of connector and schema populates the fields in LDAP User Attributes and LDAP Group Attributes.

**LDAP User Attributes**

The LDAP user attributes provide Lab Manager with details about how user information is defined in the LDAP directory. This allows Lab Manager to access that information and map it to its own user database.

If your LDAP directory uses different syntax for user attributes than what is displayed, modify the information here to match the LDAP directory.

**LDAP Group Attributes**

The LDAP group attributes provide Lab Manager with details about how group information is defined in the LDAP directory. This allows Lab Manager to access that information and map it to its own group and user database.

If your LDAP directory uses different syntax for group attributes than what is displayed, modify the information to match the LDAP directory.

**Testing LDAP Settings**

After you enter your LDAP settings, use the Test LDAP Settings button to make sure attributes are mapping correctly. Lab Manager tries to connect to the LDAP server and look up information about the user entered in the User Name field. For anonymous read, you must provide a valid user name to test.

Review the LDAP settings test results and modify your connection information or attribute values if necessary.

**Viewing Capacity License Information**

The License tab show details on your Lab Manager capacity licenses, such as expiration and number of CPUs. Use this page to add a capacity license.

**Adding a Lab Manager Server Capacity License**

Lab Manager capacity is licensed on a per-processor or per-socket basis for prepared ESX hosts. You need at least two processors of available licensed capacity to prepare a dual-processor host.

You can enter multiple capacity licenses. For example, if you have one capacity license for 10 CPU and another capacity license for 10 CPU, Lab Manager is licensed for 20 CPU.
To add a capacity license

1. In the left pane, click Settings.
2. In the License tab, click the Add Capacity License button.
3. Enter the serial number and click OK.

Configuring Guest Customization Settings

For information about settings in the Guest Customization tab, see “Building a Microsoft Sysprep Package” on page 80, “Choosing the Guest Customization SID Generation Tool” on page 82, and “Disabling VMware Tools Check Before Publishing Virtual Machine Templates” on page 90.

Configuring SupportLink Settings

The Lab Manager SupportLink feature sends usage data to VMware for improved product support. VMware does not share this data with other organizations or trace any data back to individual users. During the Lab Manager installation and initialization process, the administrator initially indicates whether to enable SupportLink.

With the aid of SupportLink information, VMware can provide individualized email support with guaranteed 24-hour response time. Customers who deactivate SupportLink still have access to the Web-based support forum.

To set up SupportLink

1. In the left pane of the console, click Settings.
2. Click the SupportLink tab.
3. If VMware support requests you to collect information from your Lab Manager environment, click the Collect button.
4. Select the check box to turn on SupportLink.
5. Enter your company name and Lab Manager administrator email address.
6. Do not alter the SupportLink server unless instructed to change the name by VMware support.
7. Indicate whether to use a proxy server and specify the details.
8. If VMware support requests a test of SupportLink, click the Test Settings button to verify the connectivity to the Lab Manager SupportLink Server.
9. Click OK.
Configuring Resource Cleanup Settings

Use the Resource Cleanup tab to define the maximum deployment lease and storage lease times for virtual machine templates and configurations. The values you specify here 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 administrator changes the maximum value after the initial setting, a user can only extend an existing lease to the original value.

When a deployment lease expires, Lab Manager undeploys the configuration or virtual machine template. When a storage lease expires, Lab Manager either deletes the expired virtual machine template or configuration, or marks the virtual machine template or configuration for deletion. See “Deleting Expired Virtual Machines” on page 179.

Users can request email notification prior to lease expiration. See “Setting User Preferences” on page 25.

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 unpublished state, or a virtual machine template or virtual machine changes from a deployed to undeployed state, the storage lease begins.

A storage lease is intended to delete unused or inactive virtual machine templates. These operations renew the lease because Lab Manager identifies the virtual machine template as in use:

- Unpublish
- Clone (full or linked)
- Export
- Consolidate

Setting or changing the following properties for virtual machine templates or virtual machines renews the lease because Lab Manager identifies the virtual machine template or virtual machine as being used:

- Memory
- Use Time Synchronization
To set deployment and storage leases
1. In the left pane of the console, click Settings.
2. Click the Resource Cleanup tab.
3. Choose deployment lease maximums for Workspace configurations and VM templates.
5. Choose whether to delete or mark for deletion configurations and templates with expired storage leases.
6. Click OK.

Configuring VirtualCenter Settings

The VirtualCenter tab has settings for the VirtualCenter Server system associated with Lab Manager. See “Managing VirtualCenter and Datacenters,” for information on updating the VirtualCenter Server settings.

Managing VirtualCenter and Datacenters

From the VirtualCenter tab, you can reconnect to the VirtualCenter Server, change a port number for the VirtualCenter Server if the default port is not in use, and switch VirtualCenter systems.

If Lab Manager loses the connection to the VirtualCenter Server, Lab Manager attempts to reconnect periodically. If you want to connect immediately, you can force the connection process.

You can also switch the VirtualCenter datacenter associated with Lab Manager. Lab Manager only supports a single datacenter.

For information about user credential requirements for connecting to VirtualCenter, see “Credential Requirements for Connecting Lab Manager to the VirtualCenter Server” on page 201.

To reconnect Lab Manager to the VirtualCenter Server
1. In the left pane of the console, click Settings.
2. Click the VirtualCenter tab.
3. To force a reconnect operation, click OK.
To change the port number for the VirtualCenter Server

1. In the left pane of the console, click Settings.
2. Click the VirtualCenter tab.
3. Enter the port number.
4. Click OK.

To change the VirtualCenter system

1. Unprepare all the hosts attached to Lab Manager.
   See “Preparing and Unpreparing Hosts” on page 167.
2. Detach all the resource pools attached to Lab Manager.
   The resource pools can involve clusters and hosts. See “Attaching and Detaching Resource Pools” on page 163.
3. In the left pane, click Settings.
4. On the VirtualCenter tab, provide connection details:
   - VirtualCenter machine name or IP address
   - VirtualCenter port number
   - User name and password
5. Click OK.
6. In the left pane, click Resources.
7. Click the Attach Resource Pool button.
8. Select the resource pool associated with the new datacenter.
9. (Optional) Enter a different name for the resource pool in Lab Manager.
10. Click OK.

To change a datacenter

1. Unprepare all the hosts attached to Lab Manager.
   See “Preparing and Unpreparing Hosts” on page 167.
2. Detach all the resource pools attached to Lab Manager.
   The resource pools can involve clusters and hosts. See “Attaching and Detaching Resource Pools” on page 163.
3 In the left pane, click **Resources**.

4 On the **Resource Pools** tab, click the **Attach Resource Pool** button.

5 Select the resource pool associated with the new datacenter.

6 (Optional) Enter a different name for the resource pool in Lab Manager.

7 Click **OK**.

**Credential Requirements for Connecting Lab Manager to the VirtualCenter Server**

To set up a connection with the VirtualCenter Server, Lab Manager requires a user who is part of a role in VirtualCenter with at least the privileges listed in Table 8-1. As with other roles in VirtualCenter, you can assign Windows users or VirtualCenter users to this role.

Lab Manager requires the user to have certain permissions on objects. Any change in the role of this user to another VirtualCenter role with fewer privileges hinders Lab Manager operations. For example, assigning the user to the **No Access** role in VirtualCenter for an object, such as a resource pool, blocks the visibility of this object in a Lab Manager environment. For information on roles and setting object permissions, see VMware Infrastructure 3 documentation at [http://www.vmware.com/support/pubs/vi_pages/vi_pubs_35.html](http://www.vmware.com/support/pubs/vi_pages/vi_pubs_35.html).

If you set up the Lab Manager connection to the VirtualCenter Server with VirtualCenter administrator credentials, you have the proper credentials to make this connection.

If you set up the Lab Manager connection to the VirtualCenter Server with user credentials that do not have VirtualCenter administrator privileges, complete these tasks:

- Setting up a user role (for example, a **Lab_Manager_User** role) in VirtualCenter with the minimum privileges listed in Table 8-1.
- Add a Windows user on the VirtualCenter system to the role.
- In the **Permissions** tab of the VI Client, specify access permissions for the user to the root folder (**Hosts & Clusters** in the left pane of the VI Client) and the datacenter that works with Lab Manager. Make sure to propagate the permissions to all child objects in the datacenter.

The VI client enables you to assign permissions for objects, such as a datacenter, cluster, host, and resource pool. Lab Manager can only work with one datacenter at a time.
The privileges in Table 8-1 appear in the Edit Role dialog box of the VI Client:

Table 8-1. Required Privileges for Connecting to the VirtualCenter Server

<table>
<thead>
<tr>
<th>VI Client Privilege Category</th>
<th>Required Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Enable Methods</td>
</tr>
<tr>
<td></td>
<td>Disable Methods</td>
</tr>
<tr>
<td>Folder</td>
<td>Create Folder</td>
</tr>
<tr>
<td></td>
<td>Delete Folder</td>
</tr>
<tr>
<td></td>
<td>Rename Folder</td>
</tr>
<tr>
<td></td>
<td>Move Folder</td>
</tr>
<tr>
<td>Datastore</td>
<td>Browse Datastore</td>
</tr>
<tr>
<td></td>
<td>File Management</td>
</tr>
<tr>
<td>Network</td>
<td>Remove</td>
</tr>
<tr>
<td>Host</td>
<td>Inventory</td>
</tr>
<tr>
<td></td>
<td>Modify Cluster</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td></td>
<td>System Management</td>
</tr>
<tr>
<td></td>
<td>Network Configuration</td>
</tr>
<tr>
<td></td>
<td>Local Operations</td>
</tr>
<tr>
<td></td>
<td>Add host to VirtualCenter</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Inventory</td>
</tr>
<tr>
<td></td>
<td>Create</td>
</tr>
<tr>
<td></td>
<td>Move</td>
</tr>
<tr>
<td></td>
<td>Remove</td>
</tr>
<tr>
<td></td>
<td>Interaction</td>
</tr>
<tr>
<td></td>
<td>Select all options. For example, select Power On, Power Off, and all other options.</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td></td>
<td>Select all options. For example, select Rename, Add Existing Disk, and all other options.</td>
</tr>
</tbody>
</table>
Performing “Force” Operations

When some standard operations fail, Lab Manager administrators can forcefully undeploy or delete certain objects, such as virtual machine templates and virtual machines.

Undeploying Virtual Machine Templates with Force

If standard undeploy operations do not work, Lab Manager administrators can forcefully undeploy a virtual machine template to clean the Lab Manager database. An example of this kind of situation is when an ESX host goes offline or someone manually removes a virtual machine from VirtualCenter inventory.

The Force Undeploy option is visible even when the Undeploy, Undeploy - Save State, or Undeploy - Discard State options are available. Although it is intended for special circumstances, the Force Undeploy option produces the same results as the Undeploy - Discard State option in standard circumstances.

To forcefully undeploy a virtual machine template

1. In the left pane, click VM Templates.

2. If the virtual machine template is deployed, move the pointer over the virtual machine template name and choose Force Undeploy from the menu.
Undeploying Virtual Machines with Force

If standard undeploy operations do not work, Lab Manager administrators can forcefully undeploy a virtual machine to clean the Lab Manager database. An example of this kind of situation is when an ESX host goes offline or someone manually removes a virtual machine template from VirtualCenter inventory.

The Force Undeploy option is visible even when the Undeploy - Save State and Undeploy - Discard State options (for a single virtual machine) and Undeploy all VMs option (for all virtual machines on a host) are available. Though intended for special circumstances, the Force Undeploy option produces the same results as the Undeploy - Discard State option (for a single virtual machine) in standard circumstances.

To forcefully undeploy an individual virtual machine
1. In the left pane, click Workspace.
2. Move the pointer over the configuration name and choose Open from the menu.
3. On the Virtual Machines tab, move the pointer over the virtual machine name and choose Force Undeploy from the menu.

To forcefully undeploy all virtual machines on a host
1. In the left pane, click Resources.
2. On the Hosts tab, move the pointer over the host and choose Force Undeploy from the menu.
3. Confirm the operation.

Deleting Published Virtual Machine Templates with Force

If a standard delete operation does not work for a published virtual machine template, Lab Manager administrators can forcefully delete the virtual machine template. An example of this kind of situation is when an ESX host failure prevents you from unpublishing the virtual machine template.

The Force Delete operation cleans the virtual machine template from the Lab Manager database but not from the VirtualCenter inventory. You can manually remove the virtual machine from the VirtualCenter inventory.
To forcefully delete a published virtual machine template

1. In the left pane, click **VM Templates**.
2. Move the pointer over the published virtual machine template name and choose **Force Delete** from the menu.
3. Confirm the deletion.
Roles and Rights

Lab Manager applies the concept of roles and rights to determine which users and groups can perform which operations. See “Managing Roles and Rights” on page 154 for more information on predefined roles, creating roles, and assigning rights to roles. See “Managing Organizations” on page 157 for more information on assigning roles to users and groups.

In addition, when a user shares 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 provide users with rights that they don’t already have based on their role.

This appendix includes information about the rights assigned to Lab Manager’s predefined roles and how access rights affect users working with shared objects.

The Lab Manager pre-defined roles are:

- Administrator
- Organization Administrator
- Template Creator
- Application Owner
- User
- View Only
Datastore Rights

Only 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

<table>
<thead>
<tr>
<th>Role</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Creator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

General Rights

The Change Ownership right allows administrators to assign a new owner to Lab Manager objects (network templates, virtual machine templates, configurations, and media files) in any organization. Organization administrators can change the owner of objects in their organization.

The Administrator View and Control right allows administrators to see and interact with all objects in the Lab Manager installation; even objects that are not shared with them. It allows organization administrators to see and interact with all objects in their organization, even objects that are not shared with them.

Only administrators can modify Lab Manager’s global settings.

Table A-2. General Rights for Predefined Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Change Ownership</th>
<th>Administrator View and Control</th>
<th>Global Settings Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Template Creator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Group Rights

Only administrators and organization administrators 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.

High I/O Rights

Lab Manager restricts certain high I/O operations based on user roles.

If you upgraded to Lab Manager 3.0 from a Lab Manager 2.5.x installation for which the Hide High I/O Operations from User setting was enabled, the upgrade wizard removes all high I/O rights from the Template Creator and Application Owner roles.

---

**Table A-2. General Rights for Predefined Roles (Continued)**

<table>
<thead>
<tr>
<th>Role</th>
<th>Change Ownership</th>
<th>Administrator View and Control</th>
<th>Global Settings Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>User View Only</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table A-3. Group Rights for Predefined Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**Table A-4. High I/O Rights for Predefined Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Import</th>
<th>Export</th>
<th>Full Clone</th>
<th>Consolidate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Template Creator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
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-4. High I/O Rights for Predefined Roles (Continued)**

<table>
<thead>
<tr>
<th>Role</th>
<th>Import</th>
<th>Export</th>
<th>Full Clone</th>
<th>Consolidate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Owner</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table A-5. High I/O Rights for Sharing Roles**

<table>
<thead>
<tr>
<th>Access</th>
<th>Import</th>
<th>Export</th>
<th>Full Clone</th>
<th>Consolidate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>NA</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Change</td>
<td>NA</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Read</td>
<td>NA</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

**Host Rights**

**Table A-6. Host Rights for Predefined Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Edit</th>
<th>Enable/Disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Creator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Owner</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Library Configuration Rights

Table A-7. Library Configuration Rights for Predefined Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
<th>Clone to Workspace</th>
<th>LiveLink</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Template Creator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Application Owner</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>User</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When an owner shares a Library 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-8. Library Configuration Rights for Sharing Roles

<table>
<thead>
<tr>
<th>Access</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
<th>Clone to Workspace</th>
<th>LiveLink</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>NA</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Change</td>
<td>NA</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Read</td>
<td>NA</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Machine Rights

Table A-9. Machine Rights for Predefined Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Edit</th>
<th>Edit Memory</th>
<th>Edit Network</th>
<th>Edit Boot Sequence and Delay</th>
<th>Edit CPU</th>
<th>Edit Hard Disk Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Template Creator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
The Edit column above 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-9. Machine Rights for Predefined Roles (Continued)**

<table>
<thead>
<tr>
<th>Access</th>
<th>Edit Memory</th>
<th>Edit Network</th>
<th>Edit Boot Sequence and Delay</th>
<th>Edit CPU</th>
<th>Edit Hard Disk Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Owner</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>User</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table A-10. Machine Rights for Sharing Roles**

<table>
<thead>
<tr>
<th>Access</th>
<th>Edit Memory</th>
<th>Edit Network</th>
<th>Edit Boot Sequence and Delay</th>
<th>Edit CPU</th>
<th>Edit Hard Disk Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Change</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Read</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Media Rights**

**Table A-11. Media Rights for Predefined Roles**

<table>
<thead>
<tr>
<th>Access</th>
<th>Edit</th>
<th>Synchronize</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Template Creator</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Application Owner</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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-12. Media Rights for Sharing Roles**

<table>
<thead>
<tr>
<th>Access</th>
<th>Edit</th>
<th>Synchronize</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Read</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Media Store Rights**

Only administrators can create, delete, and edit media stores. Other users can access media stores that are added to their organization as resources.

**Table A-13. Media Store Rights for Predefined Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Creator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Navigation Bar Rights

Access to certain areas of the Lab Manager Web console navigation bar is restricted based on the role of the logged in user.

Table A-14. Navigation Bar Rights for Predefined Roles

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Administrator</th>
<th>Organization Administrator</th>
<th>Template Creator</th>
<th>Application Owner</th>
<th>User</th>
<th>View Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Preferences</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Workspace</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Library</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VM Templates</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Network Templates</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Activity Log</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Deployed Machines</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Users and Groups</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Resources</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Organizations</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Roles and Rights</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Feature Request</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>About</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Network Template Rights

Administrators, organization administrators, and templates creators can create, delete, and edit network templates.

Table A-15. Network Template Rights for Predefined Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Administrator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Creator</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Application Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Access</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>NA</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Change</td>
<td>NA</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Read</td>
<td>NA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Organization Rights

Only administrators can create and delete organizations.

Table A-17. Organization Rights for Predefined Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Edit</th>
<th>Edit Membership</th>
<th>Edit Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Creator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Physical Network Rights

Only administrators can create, delete, and edit physical networks. Other users can access physical networks that are added to their organization as resources.

<table>
<thead>
<tr>
<th>Role</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Creator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Resource Pool Rights

Only administrators can create, delete, and edit resource pools. Other users can access resource pools that are added to their organization as resources.

<table>
<thead>
<tr>
<th>Role</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Creator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Role Rights

Only administrators can create, delete, and edit roles.

Table A-20. Role Rights for Predefined Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Creator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sharing Rights

Based on their role, a user can share objects to all or specific users in the following ways:

- Across the entire Lab Manager installation
- Between organizations
- Within an organization

Table A-21. Sharing Rights for Predefined Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Share</th>
<th>Sharing Across the Entire Installation (Read only)</th>
<th>Sharing Between Organizations (Read only)</th>
<th>Sharing Within an Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Template Creator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Application Owner</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Access</th>
<th>Sharing Across the Entire Installation</th>
<th>Sharing Between Organizations</th>
<th>Sharing Within an Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Change</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**User Rights**

Only administrators and organization administrators can create, delete, and edit users. Lab Manager also supports users created on an LDAP server.

**Table A-23. User Rights for Predefined Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
<th>Notify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Template Creator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Owner</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Virtual Machine Template Rights

Table A-24. VM Template Rights for Predefined Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
<th>Deploy/Undeploy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Creator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Application Owner</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Only</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When an owner shares a virtual machine 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-25. VM Template Rights for Sharing Roles

<table>
<thead>
<tr>
<th>Access</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
<th>Deploy/Undeploy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>NA</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Change</td>
<td>NA</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Read</td>
<td>NA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Workspace Configuration Rights

Table A-26. Workspace Configuration Rights for Predefined Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
<th>Add Machine</th>
<th>Delete Machine</th>
<th>Deploy/Undeploy Fenced</th>
<th>Deploy/Undeploy Nonfenced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Organization Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Template Creator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Application Owner</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
<th>Add Machine</th>
<th>Delete Machine</th>
<th>Deploy/Undeploy Fenced</th>
<th>Deploy/Undeploy Nonfenced</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View Only</th>
<th>Create</th>
<th>Delete</th>
<th>Edit</th>
<th>Add Machine</th>
<th>Delete Machine</th>
<th>Deploy/Undeploy Fenced</th>
<th>Deploy/Undeploy Nonfenced</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table A-26. Workspace Configuration Rights for Predefined Roles (Continued)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>NA</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>NA</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read</td>
<td>NA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The following tables list browsers and operating systems for client machines accessing the Lab Manager Web console.

**Table B-1. 32-Bit Client Operating System and Web Browser Support**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>IE 6.0</th>
<th>IE 7.0</th>
<th>Firefox 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft Windows</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vista</td>
<td>N/A</td>
<td>Yes</td>
<td>Experimental</td>
</tr>
<tr>
<td>Server 2003 Standard Edition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>R2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server 2003 Enterprise Edition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>R2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>XP Professional</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2000 Server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP3</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SP4</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2000 Advanced Server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP3</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SP4</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
**Table B-1. 32-Bit Client Operating System and Web Browser Support (Continued)**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>IE 6.0</th>
<th>IE 7.0</th>
<th>Firefox 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Red Hat Enterprise Linux</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1 AS/ES/WS</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>3 AS/ES/WS</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>4 AS/ES/WS</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>5 AS/ES/WS</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SUSE Linux</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Server 8 (SLES)</td>
<td>SP4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Enterprise Server 9 (SLES)</td>
<td>SP3</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Enterprise Server 10 (SLES)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Table B-2. 64-Bit Client Operating System and Web Browser Support**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>IE 6.0</th>
<th>IE 7.0</th>
<th>Firefox 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft Windows</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vista</td>
<td>N/A</td>
<td>Yes</td>
<td>Experimental</td>
</tr>
<tr>
<td>Server 2003 Standard Edition</td>
<td>SP1</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SP2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>R2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server 2003 Enterprise Edition</td>
<td>SP1</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SP2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>R2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>XP Professional</td>
<td>SP1</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SP2</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Red Hat Enterprise Linux</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 AS/ES/WS</td>
<td>Update 7</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Update 8</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>4 AS/ES/WS</td>
<td>Update 2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Update 3</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Update 4</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table B-2. 64-Bit Client Operating System and Web Browser Support (Continued)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>IE 6.0</th>
<th>IE 7.0</th>
<th>Firefox 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUSE Linux</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Server 9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(SLES) SP3</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Enterprise Server 10 RTM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(SLES)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
The following tables list uniprocessor (UP) and multiprocessor (MP) operating systems, and the SIDgen and Microsoft Sysprep components of guest customization.

Although Lab Manager uses guest customization on both Windows and UNIX-based guest operating systems to configure network settings, these tables address only the Windows-specific support for the SIDgen and Microsoft Sysprep components of guest customization.

Table C-1. 32-Bit Guest Operating System Support

<table>
<thead>
<tr>
<th>Operating System</th>
<th>UP</th>
<th>MP</th>
<th>SIDgen Support (Windows Only)</th>
<th>Microsoft Sysprep Support (Windows Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server 2008 RTM</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Vista</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server 2003 Standard Edition SP1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>R2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server 2003 Enterprise Edition SP1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>R2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server 2003 Web Edition SP1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table C-1. 32-Bit Guest Operating System Support (Continued)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>UP</th>
<th>MP</th>
<th>SIDgen Support (Windows Only)</th>
<th>Microsoft Sysprep Support (Windows Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>XP Professional SP1</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2000 Server SP2</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2000 Server SP3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2000 Server SP4</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2000 Advanced Server SP3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2000 Terminal Services SP4</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NT 4.0 Server SP6a</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 AS/ES/WS Update 1</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3 AS/ES/WS Update 7</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>4 AS/ES/WS Update 2</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>4 AS/ES/WS Update 3</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>4 AS/ES/WS Update 4</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>5 AS/ES/WS</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>SUSE Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Server 9 (SLES)</td>
<td>SP3</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Enterprise Server 10 (SLES)</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Solaris</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 Update 3</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Table C-2. 64-Bit Guest Operating System Support

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft Windows</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server 2008 RTM</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Vista RTM</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Server 2003 Enterprise Edition 64-bit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP1</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SP2</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>R2</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Server 2003 Standard Edition 64-bit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP1</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SP2</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>R2</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>XP Professional x64 Edition</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP1</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SP2</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Red Hat Enterprise Linux</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 64-bit Update 7</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Update 8</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>4 64-bit Update 2</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Update 3</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Update 4</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>SUSE Linux</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Server 9, 64-bit (SLES)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP3</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Enterprise Server 10, 64-bit (SLES)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTM</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Solaris</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 Update 3</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Network Fencing

Lab Manager uses network fencing, an architecture that isolates or “fences” virtual machine configurations while allowing full network access. Fencing enables you to work with live instances of the same configuration on the same physical network.

For example, when you want to have concurrent development or testing on the same configuration, you can duplicate or clone the configuration and avoid any IP or MAC address collision with this technology.

This appendix includes these topics:

- “When to Fence Configurations” on page 229
- “Understanding Fencing” on page 230
- “Viewing Virtual Switches for Fences” on page 234

When to Fence Configurations

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.

With fencing, engineers can run multiple, independent tests on a configuration deployed multiple times. Fencing is particularly useful when a developer needs to examine a bug without interrupting or stopping ongoing testing on a configuration. Lab Manager also enables you to reproduce the bug at a later time if the developer is unavailable.
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.

**Understanding Fencing**

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 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 Options” on page 231.

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

**Figure D-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 Options**

You can deploy fenced configurations in three ways:

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

*Figure D-2. Allow In and Out Fencing Mode*
- **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 in 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 D-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 D-4. Block In and Out Fencing Mode**

This 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.
**Processor Type Incompatibility**

Deploying a configuration in fenced mode hosts all the virtual machines on a single ESX host. You must have a host connected to the datastore where the virtual machine templates that serve as the basis of this configuration reside. The host must have sufficient resources, such as memory, CPU, and fences.

If you deploy a configuration, perform an operation that saves the state of the configuration (for example, suspend or capture to library), and then redeploy the configuration with fencing (which requires hosting all virtual machines on the same physical machine), you might have a situation where the only hosts available are ones with incompatible processor types. The captured memory requires a particular processor type and if there are no compatible hosts available, you cannot deploy the configuration.

To address this situation, discard the state information for the configuration and redeploy. See “Discarding State for Configurations” on page 130.

**Viewing Virtual Switches for Fences**

You can use the VI Client in the ESX host to see the virtual switches or networks that Lab Manager creates for each fence.

**To view virtual switches for fences**

1. Navigate to the **Configuration** tab of the VI Client.
2. Click the **Networking** link in the **Hardware** list to view virtual switches.

   For information about using the VI Client, see VMware Infrastructure 3 documentation.

---

**CAUTION**  Do not connect the virtual switches that Lab Manager creates to an external network. Lab Manager needs these virtual switches for deploying fenced configurations.
Enabling guest customization allows Lab Manager to customize the network settings for a virtual machine made from a virtual machine template. For general information on guest customization, see “Customizing the Guest Operating System” on page 79.

In some cases, you might want to extend the customization, using a customization script. For example, the script could check for viruses or start and stop processes. You can add a customization script to any virtual machine template.

This appendix covers these topics:
- “How Does Guest Customization Work?” on page 235
- “Extending Guest Customization” on page 236

How Does Guest Customization Work?

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 what 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 Workspace 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 host
1. From the ESX host system, open the .vmx file.
2. Find the machine.id line.

If you install VMware Tools, you can also 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 Web console, click Workspace in the left pane.
2. Move the pointer over the configuration name and choose Open from the menu.
3. Move the pointer over the deployed virtual machine name and choose View Console.
4. Search for machine.id from inside the guest operating system:
   - From the command prompt on a Linux guest OS, type:
     
     ```bash
     # 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:
     
     ```cmd
     >VMwareService.exe -cmd machine.id.get
     ```

The following is an examples of a machine.id line:

```plaintext
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=10.115.127.254&bootproto_1=static&ip_1=1.1.1.100&netmask_1=255.255.0.0&gateway_1=1.1.1.1&primaryNic=0&suffix_0=eng.vmware.com&primaryNic=0&computerName=Config10VM1&UseSysPrep=No&bitMask=11&markerid=504810238&reconfigToken=411678171
```

### Extending Guest Customization

Although you cannot modify the Lab Manager guest customization script, you can add your own customization script to any virtual machine template. That script runs before and after the Lab Manager guest customization script.

To attach your own customization script to a virtual machine template, see “Customizing Guest Customization” on page 86.
Glossary

A

Active Directory
A Microsoft directory service that stores information about users, computers, and the Windows operating system. 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 administrator.

agent
See Lab Manager agent.

B

base disk
The original virtual hard disk from which a virtual machine is derived. Virtual machines creates by linked clones in Lab Manager are comprised of a base disk and chain of delta disks that store the changes made to the original. This “referential provisioning” process addresses the potential disk consumption difficulties that come 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.
**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.

**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.

**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).

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.
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, including both 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.

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 administrator**
The highest level administrator who is likely to map to the VMware Infrastructure administrator role in most organizations. The responsibilities of the Lab Manager administrator span the entire Lab Manager installation. Only Lab Manager 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 combined 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.

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).

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.”

Prepare Hosts wizard
A wizard that prepares ESX hosts for Lab Manager use after attaching a resource pool. The wizard installs the Lab Manager agent on the hosts and collects information on user names, passwords, virtual switches, and datastores.

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.

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.

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.

SSL (Secure Sockets Layer)
A Web server uses this protocol to establish a secure connection with the browser.

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.

suspend
To save the current state of a running virtual machine or configuration. To return a suspended virtual machine or configuration to operation, use the resume feature. See also resume.

Sysprep
See Microsoft Sysprep.

TCP/IP (Transmission Control Protocol/Internet Protocol)
The de facto 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.
**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.

**VirtualCenter**
See VMware VirtualCenter (VirtualCenter), virtual machine disk (.vmdk).

**VirtualCenter 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. VirtualCenter Server is the working core of VirtualCenter.

See also VMware VirtualCenter (VirtualCenter).

**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. The file contains details about the virtual hardware and other configuration areas.

**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 VirtualCenter agent, and VirtualCenter 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 VirtualCenter 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 Infrastructure.

Lab Manager requires ESX hosts.

VMware High Availability (VMware HA)
Supports distributed availability services in an environment that includes ESX and VirtualCenter. If you configured VMware HA and one of the hosts managed by VirtualCenter 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 Infrastructure
A software suite, including ESX and VirtualCenter, 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 VirtualCenter (VirtualCenter), VMware ESX.

VMware Infrastructure Client (VI Client)
A user interface that runs locally in a Windows machine and provides access to the virtual machine’s display. VI Client runs on a networked machine that does not need to be the same machine as the VirtualCenter 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, the VMware Tools control panel, and support for such features as shared folders, drag-and-drop in Windows guests, shrinking virtual disks, time synchronization with the host, VMware Tools scripts, and connecting and disconnecting devices while the virtual machine is running.

Guest customization in Lab Manager requires VMware Tools.

**VMware VirtualCenter (VirtualCenter)**

A software component of VMware Infrastructure for deploying and managing virtual machines across the datacenter. With VirtualCenter, 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

A
accessing
  configurations 104
  media library 134
  network templates 30
  virtual machine consoles 53
  virtual machine templates 62
  virtual machines 40
Active Directory 192
ActiveX control 53
activity log 140
adding
  capacity licenses 196
  groups 152, 158
  IP addresses 37, 187
  media stores 182
  members 158
  network interfaces to virtual machines 51, 97
  networks to configurations 118
  organizations 157
  physical networks 185
  roles 155
  SCSI virtual hard disks 48, 96
  users 144, 158
  virtual hard disks to virtual machines 48, 96
  virtual machines to configurations 115, 117
  virtual machines to existing configurations 115
  virtual machines to new configurations 107
administration
  force operations 203
  of datastores 172–181
  of groups 151–154
  of hosts 165–171
  of Lab Manager settings 189–199
  of media stores 181–184
  of organizations 157–161
  of physical networks 184–189
  of resource pools 162–165
  of roles 154–157
  of users 142–151
attaching resource pools 163
B
BEA LiquidVM 60
C
capturing configurations 124
CD images
  ejecting from virtual machines 59
  inserting into virtual machines 58
  requirements 135
  swapping 58
changing owner
  configurations 132
  media 137
  network templates 35
  virtual machine templates 100
cloning
  configurations 110, 111
  virtual machine templates 70
clusters, defining 161
column sorting 25
configuration library
  accessing 105
configurations
  accessing 104
  accessing the configuration library 105
  adding virtual machines 115
capturing 124
changing owner 132
cloning 110, 111
cloning to the Workspace 125
creating 106
creating LiveLinks 126
defining 103
deleting 132, 181
deploying 119
deploying in fenced mode 41, 120, 231
deploying on clusters with VMware HA 122
discarding state 130
editing properties 131
exporting 130
forced deployment modes 107
full cloning 110
importing 109
linked cloning 110
moving virtual machines 117
powering off 129
powering on 129
properties 131
removing virtual machines 116
resetting 129
resuming operation of 128
reverting to snapshots 123
sharing 127
suspending 128
taking snapshots 123
undeploying 129
configurations, sample in Lab Manager 104
consolidating
  virtual machine templates 92
  virtual machines 44, 180
copying network templates 33
creating
  configurations 106
  LiveLinks 126
  network templates 31
  virtual machine templates 64
D
datacenters, managing 199
datastores
  adding media storage 182
  defining 161
  disabling 174
  editing properties 175
  enabling 174
  properties 175
  removing 173
  viewing virtual machine datastore usage 175
Datastores tab 172
deleting
  configurations 132, 181
  expired virtual machines 179
groups 153
network templates 35
physical networks 188
published virtual machine templates after host failure 204
revert points 58, 123, 180
roles 156
users 146
virtual machine templates 101
virtual machines 116, 181
Deployed Virtual Machines page 140
deploying
configurations 119
configurations on clusters with VMware HA 122
virtual machine templates 71
virtual machine templates on clusters with VMware HA 72
virtual machines 41
virtual machines on clusters with VMware HA 43
deployment lease alerts 26
deployment leases 47, 96, 122, 198
detaching resource pools 163
directed deployment 72, 122
disabling
datastores 174
guest customization 83
hosts 168
media stores 183
organizations 160
resource pools 164
users 146
version check of VMware Tools 90
discard state 44, 93, 130

E
editing
configuration properties 131
datastore properties 175
group properties 153
host properties 168
media properties 137
media store properties 184
network templates 35
organization properties 159
physical network properties 188
resource pool properties 164
role properties 156
user properties 147
virtual hard disks 48, 97
virtual machine properties 45
virtual machine template properties 93
email alerts 192
e-mail notifications 149
e-mail preferences 191
enabling
datastores 174
hosts 168
media stores 183
resource pools 164
users 146
exporting
configurations 130
virtual machine templates 91
F
fencing, see network fencing
filtering the Web console view 24
Firefox support 221
floppy files
ejecting from virtual machines 59
inserting into virtual machines 59
requirements 135
swapping 59
force operations 203
forced deployment modes 107
G
General tab 189
glossary 237
Gold Master 106, 124, 131
groups
adding 152, 158
deleting 153
Lab Manager User's Guide

editing properties 153
viewing 151
Groups page 151
guest customization
building a Microsoft Sysprep package 80
disabling 83
extending the customization 235
guest operating system support 225
installing VMware Tools 57
prerequisites 79
setting up 79–82
settings in virtual machine properties 47
settings in virtual machine template properties 95
steps for Windows NT and Solaris virtual machine templates 85
guest operating systems
32 and 64-bit support 225
customizing 79–82
installing 73
requirements 225

hosts
defining 161
disabling 168
editing properties 168
enabling 168
preparing 167
properties 168
unpreparing 167
viewing deployed virtual machines 169
Hosts tab 165

importing
configurations 109
LDAP groups 152
virtual machine templates 66
installing
guest operating systems 73
VMware Tools 74
Internet Explorer support 221
IP addressing modes 32, 50, 52, 98, 99, 108, 185
IP pool
adding IP addresses 32, 37, 187
viewing IP address usage 36, 186

Lab Manager
benefits and features 17
client user 16
components 17
in a VMware Infrastructure environment 18
introducing 15
Lab Manager Server 16
LM Tools 235
Managed Server 16
SOAP API 16
Web console 16
Lab Manager agent
installing 167
uninstalling 168
Lab Manager Server about 16
LDAP
authenticating users 192
settings 192
testing settings 196
LDAP tab 192
LDAPS 194
lease alerts 26
leases
  cleanup date 176
  deployment 47, 96, 122, 198
  Resource Cleanup tab 198
  storage 47, 89, 96, 198
  system-wide settings 198
Library page 105
License tab 196
licenses
  adding capacity 196
LiquidVM 60
LiveLinks
  creating 126
  restoring 126
LM Tools
  defining 235
M
MAC addresses
  generating 190
  resetting 51, 100
Managed Server
  about 16
media
  about 133
  accessing the library 134
  adding media stores 182
  changing owner 137
  editing properties 137
  restricting access 135
  sharing 135
  synchronizing Lab Manager with media stores 135
Media page 134
media stores
  adding 182
  defining 161
  disabling 183
  editing properties 184
  enabling 183
Media Stores tab 181
Microsoft Active Directory 192
Microsoft Internet Explorer support 221
Mozilla Firefox support 221
N
network fencing
  defining 229
  deployment options 41, 120
  how it works 230
  options 231
  physical network options 186
  processor incompatibility 234
  reasons for 229
  viewing virtual switches 234
network interfaces, adding 51, 97
network templates
  accessing 30
  changing owner 35
  copying 33
  creating 31
  defining 29
  deleting 35
  editing properties 35
  sharing 33
Network Templates page 30
networks
  adding to configurations 118
  physical 184
  removing from configurations 118
  virtual 29
NICs, adding 51, 97
O
OpenLDAP 192
organizations
adding 157
adding members 158
disabling 160
editing properties 159
viewing 157
Organizations page 157
Overview page 22
P
physical networks
adding 185
deleting 188
editing properties 188
removing IP addresses 37, 188
pop-up menus 24
powering off
configurations 129
virtual machines 55
powering on
configurations 129
virtual machines 55
preparing hosts 167
prerequisites for guest customization 79
properties
of configurations 131
of datastores 175
of groups 153
of hosts 168
of media 137
of media stores 184
of network templates 35
of organizations 159
of physical networks 188
of resource pools 164
of roles 156
of users 147
of virtual machine templates 93
of virtual machines 45
publishing virtual machine templates 89
R
redeploying all virtual machines 171
remote desktop connections 55
removing
datastores 173
IP addresses 37, 188
networks from configurations 118
organizations 160
renewing storage leases 179
requirements
CD images 135
client machines accessing Web console 221
floppy files 135
for VirtualCenter credentials 201
guest operating systems 225
remote desktop connections 55
resetting
configurations 129
MAC addresses 51, 100
virtual machines 56
Resource Cleanup tab 198
resource pools
attaching 163
defining 161
detaching 163
disabling 164
editing properties 164
enabling 164
viewing 162
Resource Pools page 162
resource usage, monitoring 175
restricting access to media 135
resuming
  operation of configurations 128
  operation of virtual machines 56
revert points
  creating 57, 123
  deleting 58, 123, 180
roles
  adding 155
  deleting 156
  editing properties 156
  viewing 155
Roles page 155
S
sharing
  configurations 127
  media 135
  network templates 33
  virtual machine templates 88
shutting down
  virtual machines 56
SMB
  exporting configurations 130
  exporting virtual machine templates 91
  import/export timeout 190
  importing configurations 109
  importing virtual machine templates 68
snapshots
  of configurations 123
  of virtual machines 57
  reverting to 57, 123
SOAP API
  about 16
  SSMove utility 178
storage lease alerts 26
storage leases 47, 89, 96, 198
storage leases, renewing 179
stranded users 150
Stranded Users page 150
SupportLink tab 197
suspending
  configurations 128
  virtual machines 56
synchronizing media library with media store files 135
system alerts 192
U
undeploying
  all virtual machines 165, 171
  configurations 129
  virtual machine templates 87
  virtual machine templates after standard attempt fails 203
  virtual machines 43
unpreparing hosts 167
unpublishing virtual machine templates 91
User Preferences page 25
users
  adding 144, 158
  authenticating with LDAP 192
  defining roles 145
  deleting 146
  disabling 146
  editing properties 147
  enabling 146
  managing 142
  properties 147
  setting preferences 25
  viewing 142
Users page 142
V

virtual hard disks
  adding 48, 96
  adding SCSI disks 48, 96
  editing 48, 97
Virtual Machine Datastore Usage page 175

virtual machine template consoles 53
virtual machine templates
  accessing 62
  accessing virtual machine consoles 53
  adding virtual hard disks 48, 96
  changing owner 100
  cloning 70
  consolidating 92
  creating 64
  creating by importing virtual machines 66
  creating from active virtual machines 69
  defining 61
  deleting 101
  deleting after ESX host failure 204
  deploying 71
  discarding state 93
  editing properties 93
  exporting 91
  importing 66
  installing guest operating systems 73
  installing VMware Tools 74
  leases 89, 96
  properties 93
  publishing 89
  sharing 88

undeploying 87
undeploying with force 203
unpublishing 91

virtual machine templates, sample in Lab Manager 62
virtual machines
  accessing 40
  accessing the console 53
  accessing the console for the first time 53
  adding to configurations 115, 117
  adding virtual hard disks 48, 96
  changing MAC addresses 51, 100
  consolidating 44, 180
  creating virtual machine templates from 69
  defining 39
  deleting 116, 181
  deploying 41
  deploying on clusters with VMware HA 43
  discarding state 44
  editing properties 45
  ejecting CD images 59
  ejecting floppy files 59
  inserting CD images 58
  inserting floppy files 59
  installing ActiveX 53
  installing VMware Remote MKS Plugin 53
  installing VMware Tools 57
  leases 47, 122, 198
  moving from one datastore to another 181
  performing guest customization 57
  powering off 55
  powering on 55
  properties 45
redeploying all 171
remote desktop connections 55
removing from a configuration 116
resetting 56
resuming operation of 56
reverting to snapshots 57
shutting down 56
suspending 56
swapping CD images 58
swapping floppy files 59
taking snapshots 57
undeploying 43
undeploying all 165, 171
undeploying with force 204
viewing datastore usage 175
viewing storage usage 175
Virtual Machines tab 40
virtual switches, viewing 234
VirtualCenter
connecting to Lab Manager 201
importing virtual machine templates from 66
managing in a Lab Manager environment 199
timeout for import operations 190
VirtualCenter tab 199
VM Templates page 62
VMware Infrastructure
leveraging services 19
working with Lab Manager 18
VMware Remote MKS Plugin 53
VMware Tools
and mouse control 25
disabling version check prior to publishing 90
installing 57, 74
required for guest customization 79
W
Web console
about 16
access requirements 221
browser and client machine support 221
column sorting 25
filtering the view 24
pop-up menus 24
WLS-VE 60
Workspace page 104