



Citrix XenServer Workload Balancing 6.5 Administrator's Guide

Published August 2016
1.0 Edition



Citrix XenServer Workload Balancing 6.5 Administrator's Guide

Copyright © 2016 Citrix Systems, Inc. All Rights Reserved.
Version: 6.5 Service Pack 1

Citrix, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
United States of America

Disclaimers

This document is furnished "AS IS." Citrix, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix, Inc. and its licensors, and are furnished under a license from Citrix, Inc.

Citrix Systems, Inc., the Citrix logo, Citrix XenServer and Citrix XenCenter, are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

Trademarks

Citrix®
XenServer®
XenCenter®



Contents

1. About	1
1.1. What's New in 6.5?	1
1.1.1. New Features in 6.5	1
1.2. Finding Workload Balancing Documentation	1
2. Introducing Workload Balancing	2
2.1. Workload Balancing Overview	2
2.1.1. Reports on Workloads	3
2.1.2. Workload Balancing Basic Concepts	3
2.1.3. Pool Requirements	3
3. Using Workload Balancing	4
3.1. Introduction to Basic Tasks	4
3.2. Choosing the Best Host for a VM	4
3.2.1. To start a virtual machine on the optimal server	5
3.2.1.1. To resume a virtual machine on the optimal server	6
3.3. Accepting Optimization Recommendations	7
3.3.1. To accept an optimization recommendation	7
3.3.2. Understanding WLB Recommendations under High Availability	7
4. Generating Workload Reports	9
4.1. Overview of Workload Reports	9
4.1.1. Generating and Managing Workload Balancing Reports	9
4.1.1.1. To generate a Workload Balancing report	9
4.1.1.2. To navigate in a Workload Balancing report	10
4.1.1.3. To print a Workload Balancing report	10
4.1.1.3.1. To export a Workload Balancing report	10
4.1.2. Workload Balancing Report Glossary	11
4.1.2.1. Chargeback Utilization Analysis	11
4.1.2.2. Host Health History	13
4.1.2.3. Pool Optimization Performance History	13



4.1.2.4. Pool Audit Trail	14
4.1.2.4.1. Report Contents	14
4.1.2.4.2. Audit Log Event Names	14
4.1.2.5. Pool Health	15
4.1.2.6. Pool Health History	16
4.1.2.7. Pool Optimization History	16
4.1.2.8. Virtual Machine Motion History	17
4.1.2.9. Virtual Machine Performance History	17
5. Managing Workload Balancing Features and Settings	18
5.1. Changing Workload Balancing Settings	18
5.1.1. Adjusting the Optimization Mode	19
5.1.1.1. Optimizing and Managing Power Automatically	20
5.1.1.1.1. Applying Recommendations Automatically	21
5.1.1.1.2. Enabling Workload Balancing Power Management	21
5.1.1.1.3. Designing Environments for Power Management and VM Consolidation	22
5.1.1.1.4. To apply optimization recommendations automatically	23
5.1.1.1.5. To select hosts for power management	23
5.1.1.2. Understanding When Workload Balancing Makes Recommendations	24
5.1.1.2.1. Optimization and Consolidation Process	25
5.1.1.2.2. Changing the Critical Thresholds	27
5.1.1.2.3. Tuning Metric Weightings	28
5.1.1.3. Excluding Hosts from Recommendations	29
5.1.1.3.1. To exclude hosts from Workload Balancing	30
5.1.1.4. Controlling Automated Recommendations	30
5.1.1.4.1. Setting Conservative or Aggressive Automated Recommendations	30
5.2. To Modify the Pool Audit Trail Granularity Setting	35
5.3. To View Audit Trail Reports Based on Objects Using XenCenter	35
6. Administering Workload Balancing	36
6.1. Administering and Maintaining Workload Balancing	36



6.1.1. Connecting to the Workload Balancing Virtual Appliance	36
6.1.1.1. To connect your pool to the Workload Balancing virtual appliance	37
6.1.1.2. To obtain the IP address for the WLB virtual appliance	39
6.1.1.3. Workload Balancing Access Control Permissions	39
6.1.2. Determining the Status of the Workload Balancing Virtual Appliance	40
6.1.3. Reconfiguring a Pool to Use Another WLB Appliance	40
6.1.4. Updating Workload Balancing Credentials	40
6.1.5. Changing the Workload Balancing IP Address	41
6.1.6. Stopping Workload Balancing	42
6.1.7. Entering Maintenance Mode with Workload Balancing Enabled	42
6.1.7.1. To enter maintenance mode with Workload Balancing enabled	43
6.1.8. Increasing the Workload Balancing Disk Size	43
6.1.9. Removing the Workload Balancing Virtual Appliance	43
6.1.10. Managing the Workload Balancing Database	43
6.1.10.1. Accessing the Database	44
6.1.10.2. Controlling Database Grooming	44
6.1.10.2.1. Database Grooming Parameters	45
6.1.10.3. Changing the Database Password	45
6.1.10.4. Archiving Database Data	45
6.1.10.4.1. Enabling client authentication to the database	45
6.1.10.4.2. Modifying the Database Configuration Files	46
6.1.10.5. Changing the Database Maintenance Window	47
6.1.11. Customizing Workload Balancing	48
6.2. Upgrading Workload Balancing	49
6.2.1. Upgrading Workload Balancing with Internet Access	50
6.2.2. Upgrading Workload Balancing without Direct Internet Access	50
6.2.3. Checking Workload Balancing and CentOS Version Numbers	53
7. Appendix A: XenServer Workload Balancing Troubleshooting	54
7.1. Troubleshooting Workload Balancing	54
7.1.1. General Troubleshooting Tips	54
7.1.2. Error Messages	54

7.1.3. Issues Entering Workload Balancing Credentials	54
7.1.4. Issues with Firewalls	54
7.1.5. Losing the Connection to Workload Balancing	55
7.1.6. Workload Balancing Connection Errors	55
7.1.7. Workload Balancing Stops Working	55
7.1.8. Issues Changing Workload Balancing Servers	56
8. Appendix B: Workload Balancing Commands	57
8.1. Service Commands	57
8.1.1. Logging in to the Workload Balancing Virtual Appliance	57
8.1.2. wlb restart	57
8.1.3. wlb start	57
8.1.4. wlb stop	57
8.1.5. wlb status	57
8.1.6. Modifying the Workload Balancing Configuration Options	58
8.1.7. Editing the Workload Balancing Configuration File	58
8.1.8. Increasing the Detail in the Workload Balancing Log	59
8.2. Workload Balancing XE Commands	60
8.2.1. pool-initialize-wlb	60
8.2.2. pool-param-set other-config	60
8.2.3. pool-retrieve-wlb-diagnostics	61
8.2.4. host-retrieve-wlb-evacuate-recommendations	61
8.2.5. vm-retrieve-wlb-recommendations	61
8.2.6. pool-certificate-list	61
8.2.7. pool-certificate-install	61
8.2.8. pool-certificate-sync	61
8.2.9. pool-param-set	61
8.2.10. pool-deconfigure-wlb	62
8.2.11. pool-retrieve-wlb-configuration	62
8.2.12. pool-retrieve-wlb-recommendations	62
8.2.13. pool-retrieve-wlb-report	62
8.2.14. pool-send-wlb-configuration	63



9. Appendix C: Configuring Certificates for Workload Balancing	65
9.1. Overview	65
9.2. Configuring XenServer to Verify the Self-Signed Certificate	66
9.3. Configuring XenServer to Verify a Certificate-authority Certificate	67
9.3.1. Task 1: Obtaining a Certificate-authority Certificate	67
9.3.2. Task 2: Specifying the New Certificate	68
9.3.3. Task 3: Importing the Certificate Chain into the Pool	69
Index	71



Chapter 1. About

This document explains how to run the XenServer Workload Balancing virtual appliance. To get started and import the Workload Balancing virtual appliance, see the *XenServer Workload Balancing 6.5 Quick Start Guide*.

Note:

Workload Balancing is available for XenServer Enterprise Edition customers or those who have access to XenServer through their XenDesktop entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website [here](#). For detailed information on Licensing - refer to [CTX141511 - XenServer 6.5 Licensing FAQ](#).

1.1. What's New in 6.5?

Previously removed in XenServer 6.2, Workload Balancing (WLB) is reintroduced and enhanced with XenServer 6.5.

1.1.1. New Features in 6.5

Workload Balancing 6.5 includes the following enhanced features.

- **Pool Audit Trail.** The enhanced Pool Audit Trail feature allows you to specify the granularity of the audit log report. Customers can also search and filter the audit trail logs by specific users, objects, and by time
- **Online Upgrade.** Customers can now apply upgrades directly from the live SLB Server by the yum update mechanism, or instead download the upgraded RPM packages from Citrix.com

1.2. Finding Workload Balancing Documentation

The Workload Balancing documentation also includes:

- *XenServer Workload Balancing 6.5 Quick Start* provides information about downloading and importing the Workload Balancing virtual appliance.
- In XenCenter, press F1 to access the comprehensive online help.

Chapter 2. Introducing Workload Balancing

This chapter provides introductions to the following topics:

- Workload Balancing at a high level
- Workload Reports
- Basic concepts of Workload Balancing

2.1. Workload Balancing Overview

Note:

Workload Balancing is available for XenServer Enterprise Edition customers or those who have access to XenServer through their XenDesktop entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website [here](#). For detailed information on Licensing - refer to [CTX141511 - XenServer 6.5 Licensing FAQ](#).

Workload Balancing is a XenServer component, packaged as a virtual appliance, that:

- Creates reports about VM performance in your XenServer environment
- Evaluates resource utilization and locates virtual machines on the best possible hosts in the pool for their workload's needs

Even if you do not want to use Workload Balancing to balance your virtual machines, you may want to run it anyway for the workload reporting functionality. When deployed to manage virtual machine workloads, Workload Balancing can:

- Balance virtual-machine workloads across hosts in a XenServer resource pool
- Determine the best host on which to start a virtual machine
- Determine the best host on which to resume a virtual machine that you powered off
- Determine the best host to move a virtual machine to when a host fails
- Determine the optimal server for each of the host's virtual machines when you put a host into or take a host out of Maintenance Mode

Depending on your preference, Workload Balancing can accomplish these tasks automatically or prompt you to accept its rebalancing and placement recommendations. You can also configure Workload Balancing to power off hosts automatically at specific times of day (for example, to save power at night).

Workload Balancing functions by evaluating the utilization of virtual machines across a pool and, when a host exceeds a performance threshold, relocating the VM to a less-taxed host in the pool. To rebalance workloads, Workload Balancing moves VMs to balance the resource utilization on hosts.

To ensure the rebalancing and placement recommendations align with your environment's needs, you can configure Workload Balancing to *optimize* workloads for either resource performance or to maximize the number of virtual machines that fit on hosts. These optimization modes can be configured to change automatically at predefined times or stay the same at all times. For additional granularity, you can fine-tune the weighting of individual resource metrics (CPU, network, and memory).

To help you perform capacity planning, Workload Balancing provides historical reports about host and pool health, optimization and virtual-machine performance, and virtual-machine motion history.



2.1.1. Reports on Workloads

Because Workload Balancing captures performance data, you can also use this component to generate reports, known as *Workload Reports*, about your virtualized environment.

Workload Reports provide data for a pool or host's health, for auditing, optimizations, and placement (or motion) history. Also, you can run a *chargeback* report that shows virtual machine usage and can help you measure and assign costs.

To run reports, you do not need to configure for Workload Balancing to make placement recommendations or move virtual machines. However, you do need to configure the Workload Balancing component and, ideally, set Critical thresholds to values that reflect the point at which the performance of the hosts in your pool degrades.

For more information, see [Chapter 4, Generating Workload Reports](#).

2.1.2. Workload Balancing Basic Concepts

When virtual machines are running, they consume computing *resources* on the physical host, such as CPU, Memory, Network Reads, and Network Writes. For example, some virtual machines, depending on their *workload* (that is, the applications running on a virtual machine and their user transactions), might consume more CPU resources than other virtual machines on the same host. Naturally, the combined resource consumption of all virtual machines on a host reduces the host's available resources.

Workload Balancing captures data for resource performance on virtual machines and physical hosts and stores it in a database. Workload Balancing uses this data, combined with the preferences you set, to provide optimization and placement recommendations.

Optimizations are a way in which hosts are "improved" to align with your goals: Workload Balancing makes recommendations to redistribute the virtual machines across hosts in the pool to increase either performance or density. When Workload Balancing is making recommendations, it makes them in light of its ultimate goal: to create balance or harmony across the hosts in the pool. When Workload Balancing acts on these recommendations, the action is known as an *optimization*.

Within a Workload Balancing context:

- **Performance** refers to the usage of physical resources on a host (for example, the CPU, memory, network, and disk utilization on a host). When you set Workload Balancing to maximize performance, it recommends placing virtual machines to ensure the maximum amount of resources are available for each virtual machine.
- **Density** refers to the number of virtual machines on a host. When you set Workload Balancing to maximize density, it recommends placing virtual machines to ensure they have adequate computing power so you can reduce the number of hosts powered on in a pool.

Workload Balancing does not conflict with settings you already specified for High Availability: Citrix designed these features to work together.

2.1.3. Pool Requirements

To balance a pool with Workload Balancing, the hosts in the pool must meet the requirements for XenMotion (live migration), including:

- Shared remote storage
- Similar processor configurations
- Gigabit Ethernet

If the hosts do not meet these requirements, Workload Balancing cannot migrate the virtual machines in the pool.

Chapter 3. Using Workload Balancing

This chapter provides information about the following topics:

- Using Workload Balancing to start virtual machines on the best possible host
- Accepting the recommendations Workload Balancing issues to move virtual machines to different hosts

Note:

Workload Balancing is available for XenServer Enterprise Edition customers or those who have access to XenServer through their XenDesktop entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website [here](#). For detailed information on Licensing - refer to [CTX141511 - XenServer 6.5 Licensing FAQ](#).

3.1. Introduction to Basic Tasks

Workload Balancing is a powerful XenServer component that includes many features designed to optimize the workloads in your environment, such as host power management, the ability to schedule optimization-mode changes, and running reports. In addition, you can fine-tune the criteria Workload Balancing uses to make optimization recommendations.

However, when you first begin using Workload Balancing, there are two main tasks you will probably use Workload Balancing for on a daily (or regular) basis:

- Determining the best host on which to run a virtual machine
- Accepting Workload Balancing optimization recommendations

Running reports about the workloads in your environment, which is described in [Chapter 4, *Generating Workload Reports*](#), is another frequently used task.

Determining the best host on which to run a virtual machine

Determining the host on which to start and run a virtual machine, which is known as virtual-machine placement, is handy when you want to restart a powered off virtual machine and when you want to migrate a virtual machine to a different host. Placement recommendations may also be useful in XenDesktop environments.

Accepting Workload Balancing recommendations

After Workload Balancing is running for a while, it begins to make recommendations about ways in which you can improve your environment. For example, if your goal is to improve virtual-machine density on hosts, at some point, Workload Balancing may issue a recommendation to consolidate virtual machines on a host. Assuming you are not running in automated mode, you can choose to either accept this recommendation (and apply it) or just simply ignore it.

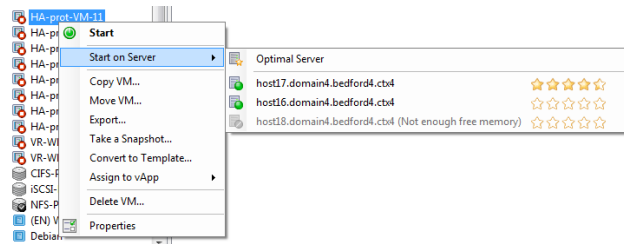
Both of these tasks, and the way in which you perform them in XenCenter, are explained in more depth in the sections that follow.

Important:

After Workload Balancing is running for a period of time, if you do not receive optimal placement recommendations, Citrix strongly recommends you evaluate your performance thresholds as described in [Section 5.1.1.2, “Understanding When Workload Balancing Makes Recommendations”](#). It is critical to set Workload Balancing to the correct thresholds for your environment or its recommendations might not be appropriate.

3.2. Choosing the Best Host for a VM

When Workload Balancing is enabled and you restart a virtual machine that is offline, XenCenter provides recommendations to help you determine the *optimal* physical host in the resource pool on which to start a virtual machine. The recommendations are also known as *star ratings* since stars are used to indicate the best host.



This illustration shows a screen capture of the Start On Server feature. More stars appear beside host17 since this is the optimal host on which to start the VM. host16 does not have any stars beside it, which indicates that host is not recommended. However, since host16 is enabled the user can select it. host18 is greyed out due to insufficient memory, so the user cannot select it.

The term *optimal* refers to the physical server best suited to hosting your workload. There are several factors Workload Balancing uses when determining which host is optimal for a workload:

- **The amount of resources available on each host in the pool.** When a pool is running in Maximum Performance mode, Workload Balancing tries to balance the virtual machines across the hosts in the pool so that all virtual machines have good performance. When a pool is running in Maximum Density mode, Workload Balancing tries to place virtual machines onto hosts as densely as possible while ensuring the virtual machines have sufficient resources.
- **The optimization mode in which the pool is running (Maximum Performance or Maximum Density).** When a pool is running in Maximum Performance mode, Workload Balancing tries to place virtual machines on hosts with the most resources available of the type the VM requires. When a pool is running in Maximum Density mode, Workload Balancing tries to place virtual machines on hosts that already have virtual machines running so that virtual machines are running on as few hosts as possible.
- **The amount and type of resources the VM requires.** After Workload Balancing has monitored a virtual machine for a while, it uses the VM metrics it gathered to make placement recommendations according to the type of resources the virtual machine requires. For example, Workload Balancing may select a host with less available CPU but more available memory if it is what the VM requires (based on its past performance history).

When Workload Balancing is enabled, XenCenter provides ratings to indicate the optimal hosts for starting a virtual machine, including when you want to start the virtual machine when it is powered off or suspended and when you want to migrate the virtual machine to a different host (Migrate and Maintenance Mode).

When you use these features with Workload Balancing enabled, host recommendations appear as star ratings beside the name of the physical host. Five empty stars indicates the lowest-rated (least optimal) server. When it is not possible to start or migrate a virtual machine to a host, when you use the menu command for one of the placement features, the host name is greyed out and the reason it cannot accept the VM appears beside it.

In general, Workload Balancing functions more effectively and makes better, less frequent optimization recommendations if you start virtual machines on the hosts it recommends (that is, by using one of the placement features to select the host with the most stars beside it).

3.2.1. To start a virtual machine on the optimal server

1. In the **Resources** pane of XenCenter, select the virtual machine you want to start.
2. From the **VM** menu, select **Start on Server** and then select one of the following:
 - **Optimal Server.** The optimal server is the physical host that is best suited to the resource demands of the virtual machine you are starting. Workload Balancing determines the optimal server based on its historical records of performance metrics and your placement strategy. The optimal server is the server with the most stars.
 - **One of the servers with star ratings** listed under the Optimal Server command. Five stars indicates the most-recommended (optimal) server and five empty stars indicates the least-recommended server.

Tip:



You can also select **Start on Server** by right-clicking the virtual machine you want to start in the **Resources** pane.

3.2.1.1. To resume a virtual machine on the optimal server

1. In the **Resources** pane of XenCenter, select the suspended virtual machine you want to resume.
2. From the **VM** menu, select **Resume on Server** and then select one of the following:
 - **Optimal Server.** The optimal server is the physical host that is best suited to the resource demands of the virtual machine you are starting. Workload Balancing determines the optimal server based on its historical records of performance metrics and your placement strategy. The optimal server is the server with the most stars.
 - **One of the servers with star ratings** listed under the Optimal Server command. Five stars indicates the most-recommended (optimal) server and five empty stars indicates the least-recommended server.

Tip:

You can also select **Resume on Server** by right-clicking the suspended virtual machine in the **Resources** pane.

3.3. Accepting Optimization Recommendations

Workload Balancing provides recommendations about ways you can migrate virtual machines to optimize your environment. Optimization recommendations appear in the **WLB** tab in XenCenter.

VM/Host	Operation	Reason
HA-prot-VM-7	Relocate from Host 17.domain4.bedford4.ctx4 to Host 16.domain4.be...	Consolidation
host17.domain4.bedford4.ctx4	Power off	Release Resource

This illustration shows a screen capture of the Optimization Recommendations list, which appears on the WLB tab. The Operation column displays the behavior change suggested for that optimization recommendation. The Reason column displays the purpose of the recommendation. This screen capture shows an optimization recommendation for a virtual machine, HA-prot-VM-7, and a host, host17.domain4.bedford4.ctx4.

Optimization recommendations are based on the:

- Placement strategy you select (that is, the optimization mode), as described in [Section 5.1.1, “Adjusting the Optimization Mode”](#).
- Performance metrics for resources such as a physical host's CPU, memory, network, and disk utilization.
- The role of the host in the resource pool. When making placement recommendations, Workload Balancing considers the pool master for virtual machine placement only if no other host can accept the workload. (Likewise, when a pool is operating in Maximum Density mode, Workload Balancing considers the pool master last when determining the order in which to fill hosts with virtual machines.)

The optimization recommendations display the name of the virtual machine that Workload Balancing recommends relocating, the host it currently resides on, and the host Workload Balancing recommends as the machine's new location. The optimization recommendations also display the reason Workload Balancing recommends moving the virtual machine (for example, "CPU" to improve CPU utilization). When Workload Balancing power management is enabled, Workload Balancing also displays optimization recommendations (specifically consolidation recommendation) for hosts it recommends powering on or off.

After you click **Apply Recommendations**, XenServer performs all operations listed in the **Optimization Recommendations** list.

Tip:

You can find out the optimization mode for a resource pool by selecting the pool in XenCenter and checking the **Configuration** section of the **WLB** tab.

3.3.1. To accept an optimization recommendation

1. In the **Resources** pane of XenCenter, select the resource pool for which you want to display recommendations.
2. Click the **WLB** tab. If there are any recommended optimizations for any virtual machines on the selected resource pool, they display in the **Optimization Recommendations** section of the **WLB** tab.
3. To accept the recommendations, click **Apply Recommendations**. XenServer begins performing all the operations listed in the Operations column of the **Optimization Recommendations** section.

After you click **Apply Recommendations**, XenCenter automatically displays the **Logs** tab so you can see the progress of the virtual machine migration.

3.3.2. Understanding WLB Recommendations under High Availability

If you have Workload Balancing and the XenServer High Availability feature enabled in the same pool, it is helpful to understand how the two features interact. Workload Balancing is designed not to interfere with High



Availability. If there is a conflict between a Workload Balancing recommendation and a High Availability setting, the High Availability setting always takes precedence. In practice, this means:

- When you attempt to start a virtual machine on a host, Workload Balancing will not give you star ratings if the virtual machine cannot be started on the host without violating the High Availability plan.
- Workload Balancing will not automatically power off any hosts beyond the number specified in the **Failures allowed** box in the **Configure HA** dialog.
 - However, Workload Balancing may still make recommendations to power off more hosts than the number of host failures to tolerate. (For example, Workload Balancing will still make a recommendation to power off two hosts when High Availability is only configured to tolerate one host failure.) However, when you attempt to apply the recommendation, XenCenter may display an error message stating that High Availability will no longer be guaranteed.
- When Workload Balancing is running in automated mode and has power management enabled, any recommendations that exceed the number of host failures to tolerate are ignored. In this situation, if you look in the Workload Balancing log, you will see a message that says a power-management recommendation was not applied because High Availability is enabled.

Chapter 4. Generating Workload Reports

This chapter provides information about using the Workload Balancing component to generate reports about your virtualized environment, including reports about hosts and virtual machines. Specifically, this chapter provides information about the following:

- How to generate reports
- What workload reports are available

Note:

Workload Balancing is available for XenServer Enterprise Edition customers or those who have access to XenServer through their XenDesktop entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website [here](#). For detailed information on Licensing - refer to [CTX141511 - XenServer 6.5 Licensing FAQ](#).

4.1. Overview of Workload Reports

The Workload Balancing reports can help you perform capacity planning, determine virtual server health, and evaluate the effectiveness of your configured threshold levels.

Workload Balancing lets you generate reports on three types of objects: physical hosts, resource pools, and virtual machines. At a high level, Workload Balancing provides two types of reports:

- Historical reports that display information by date
- "Roll up" style reports, which provide a summarizing overview of an area

Workload Balancing provides some reports for auditing purposes, so you can determine, for example, the number of times a virtual machine moved.

You can use the Pool Health report to evaluate the effectiveness of your optimization thresholds. While Workload Balancing provides default threshold settings, you might need to adjust these defaults for them to provide value in your environment. If you do not have the optimization thresholds adjusted to the correct level for your environment, Workload Balancing recommendations might not be appropriate for your environment.

To generate a Workload Balancing report, the pool must be running Workload Balancing. Ideally, the pool should have been running Workload Balancing for a couple of hours or long enough to generate the type of data you want to display in the reports.

4.1.1. Generating and Managing Workload Balancing Reports

This topic explains how to generate, navigate, print, and export Workload Balancing reports.

4.1.1.1. To generate a Workload Balancing report

1. In XenCenter, from the **Pool** menu, select **View Workload Reports**.

Tip:

You can also display the Workload Reports screen from the **WLB** tab by clicking the **Reports** button.

2. From the **Workload Reports** screen, select a report from the **Reports** pane.
3. Select the **Start Date** and the **End Date** for the reporting period. Depending on the report you select, you might need to specify a host in the **Host** list box.
4. Click **Run Report**. The report displays in the report window. For information about the meaning of the reports, see [Section 4.1.2, "Workload Balancing Report Glossary"](#).

4.1.1.2. To navigate in a Workload Balancing report

After generating a report, you can use the toolbar buttons in the report to navigate and perform certain tasks. To display the name of a toolbar button, pause your mouse over toolbar icon.

Table 4.1. Report Toolbar Buttons

	Document Map. Lets you display a document map that helps you navigate through long reports.
	Page Forward/Back. Lets you move one page ahead or back in the report.
	Back to Parent Report. Lets you return to the parent report when working with drill-through reports. Note: This button is only available in drill-through reports, such as the Pool Health report.
	Stop Rendering. Cancels the report generation.
	Print. Lets you print a report and specify general printing options, such as the printer, the number of pages, and the number of copies.
	Print Layout. Lets you display a preview of the report before you print it. To exit Print Layout, click the Print Layout button again.
	Page Setup. Lets you specify printing options such as the paper size, page orientation, and margins.
	Export. Lets you export the report as an Acrobat (.PDF) file or as an Excel file with a .XLS extension.
	Find. Lets you search for a word in a report, such as the name of a virtual machine.

4.1.1.3. To print a Workload Balancing report

Before you can print a report, you must first generate it.

1. (Optional.) Preview the printed document by clicking the following **Print Layout** button:



2. (Optional.) Change the paper size and source, page orientation, or margins by clicking the following **Page Setup** button:




3. Click the following **Print** button:



4.1.1.3.1. To export a Workload Balancing report

You can export a report in either Microsoft Excel or Adobe Acrobat (PDF) formats.

1. After generating the report, click the following **Export** button:
 
2. Select one of the following items from the **Export** button menu:
 - **Excel**
 - **Acrobat (PDF) file**

Note:

The data that appears between report export formats may be inconsistent, depending on the export format you select. Reports exported to Excel include all the data available for reports, including "drilldown" data, whereas reports exported to PDF and displayed in XenCenter only contain the data that you selected when you generated the report.

4.1.2. Workload Balancing Report Glossary

This topic provides information about the following Workload Balancing reports:

4.1.2.1. Chargeback Utilization Analysis

You can use the Chargeback Utilization Analysis report ("chargeback report") to determine how much of a resource (such as a physical server) a specific department in your organization used. Specifically, the report shows information about all the virtual machines in your pool, including their availability and resource utilization. Since this report shows virtual machine availability ("up time"), it can help you demonstrate Service Level Agreements compliance and availability.

The chargeback report can help you implement a simple chargeback solution and facilitate billing. To bill customers for usage of a specific resource, generate the report, save it as Excel, and then customize the spreadsheet data to include your price per unit. Alternatively, you can import the Excel data into your billing system.

If you know that you will want to bill internal or external customers for virtual machine usage, consider incorporating department or customer names in your virtual-machine naming conventions. This will make reading chargeback reports easier.

The resource reporting in the chargeback report is, in some cases, based on the allocation of physical resources to individual virtual machines.

Likewise, because XenServer lets you allocate fixed or automatic allocations of memory, the average memory data in this report is based on the amount of memory currently allocated to the virtual machine, whether it is through a fixed memory allocation or an automatically adjusting memory allocation (Dynamic Memory Control).

The chargeback report contains the following columns of data:

- **VM Name.** The name of the virtual machine to which the data in the columns in that row applies.
- **VM Uptime.** The number of minutes the virtual machine was powered on (or, more specifically, appears with a green icon beside it in XenCenter).
- **VCPU Allocation.** The number of virtual CPUs configured on the virtual machine. Each virtual CPU receives an equal share of the physical CPU(s) on the host. For example, if you configured eight virtual CPUs on a host that contains two physical CPUs and this column had "1" in it, then this value is equal to 2/16 of the total processing power on the host.
- **Minimum CPU Usage (%).** The lowest recorded value for virtual CPU utilization in the reporting period. This value is expressed as a percentage of the VM's virtual CPU capacity, and the capacity is based on the number of virtual CPUs allocated to the VM. For example, if, when you created the VM, you allocated one virtual CPU to it, **Minimum CPU Usage** represents the lowest percentage of virtual CPU usage XenServer recorded, even if it was only for a second. If you allocated two virtual CPUs to the VM, the value in this column represents the lowest usage of the combined capacity of both virtual CPUs, expressed as a percentage.

Ultimately, the percentage of CPU usage represents the lowest recorded workload that virtual CPU handled. For example, if you allocate one virtual CPU to a VM and the physical CPU on the host is 2.4 GHz, you are allocating one-eighth of 2.4 GHz to the VM. This means that if the VM's allocated capacity is 0.3GHz, or 300MHz, and the **Minimum CPU Usage** for the VM was 20%, the VM's lowest usage of the physical host's CPU during the reporting period was 60MHz.

- **Maximum CPU Usage (%).** The highest percentage of the VM's virtual CPU capacity that the VM consumed during the reporting period. The CPU capacity consumed is a percentage of the virtual CPU capacity you

allocated to the VM. For example, if, when you created the VM, you allocated one virtual CPU to it, the Maximum CPU Usage represents the highest recorded percentage of virtual CPU usage during the time reported. If you allocated two virtual CPUs to the VM, the value in this column represents the highest utilization from the combined capacity of both virtual CPUs.

- **Average CPU Usage (%).** The average amount, expressed as a percentage, of the VM's virtual CPU capacity that was in use during the reporting period. The CPU capacity is the virtual CPU capacity you allocated to the VM. If you allocated two virtual CPUs to the VM, the value in this column represents the average utilization from the combined capacity of both virtual CPUs.
- **Total Storage Allocation (GB).** The amount of disk space that is currently allocated to the VM at the time the report was run. Frequently, unless you modified it, this disk space is the amount of disk space you allocated to the VM when you created it.
- **Virtual NIC Allocation.** The number of virtual interfaces (VIFs) allocated to the VM.
- **Current Minimum Dynamic Memory (MB).**
 - **Fixed memory allocation.** If you assigned a VM a fixed amount of memory (for example, 1024MB), the same amount of memory appears in the following columns: Current Minimum Dynamic Memory (MB), Current Maximum Dynamic Memory (MB), Current Assigned Memory (MB), and Average Assigned Memory (MB).
 - **Dynamic memory allocation.** If you configured XenServer to adjust a VM's memory automatically based on a range (that is, you enabled Dynamic Memory Control), the minimum amount of memory specified in the range appears in this column. For example, if in the **Memory Settings** dialog box in XenCenter, you selected the **Automatically allocate memory within this range** option for this VM and then specified the range values as 1024MB as the minimum memory and 2048MB as the maximum memory, then 1024MB will appear in the **Current Minimum Dynamic Memory (MB)** column.
- **Current Maximum Dynamic Memory (MB).**
 - **Dynamic memory allocation.** If XenServer is set to adjust a VM's memory automatically based on a range, the maximum amount of memory specified in the range appears in this column. For example, if the memory range you provided was 1024MB minimum and 2048MB maximum, then 2048MB will appear in the **Current Maximum Dynamic Memory (MB)** column.
 - **Fixed memory allocation.** If you assign a VM a fixed amount of memory (for example, 1024MB), the same amount of memory appears in the following columns: Current Minimum Dynamic Memory (MB), Current Maximum Dynamic Memory (MB), Current Assigned Memory (MB), and Average Assigned Memory (MB).
- **Current Assigned Memory (MB).**
 - **Dynamic memory allocation.** When Dynamic Memory Control is configured, this value indicates the amount of memory XenServer is currently allocating to the VM at the time at which the report was run.
 - **Fixed memory allocation.** If you assign a VM a fixed amount of memory (for example, 1024MB), the same amount of memory appears in the following columns: Current Minimum Dynamic Memory (MB), Current Maximum Dynamic Memory (MB), Current Assigned Memory (MB), and Average Assigned Memory (MB).

Note:

If you change the VM's memory allocation immediately before running this report, the value reflected in this column reflects the new memory allocation you configured.

- **Average Assigned Memory (MB).**
 - **Dynamic memory allocation.** When Dynamic Memory Control is configured, this value indicates the average amount of memory XenServer allocated to the VM over the reporting period.
 - **Fixed memory allocation.** If you assign a VM a fixed amount of memory (for example, 1024MB), the same amount of memory appears in the following columns: Current Minimum Dynamic Memory (MB), Current Maximum Dynamic Memory (MB), Current Assigned Memory (MB), and Average Assigned Memory (MB).

Note:



If you change the VM's memory allocation immediately before running this report, the value displayed in this column may not change from what it would have previously displayed. The value in this column reflects the average over the time period.

- **Average Network Reads (BPS).** The average amount of data (in bits per second) the VM received during the reporting period.
- **Average Network Writes (BPS).** The average amount of data (in bits per second) the VM sent during the reporting period.
- **Average Network Usage (BPS).** The combined total (in bits per second) of the Average Network Reads and Average Network Writes. For example, if a VM sent, on average, 1,027 bits per second and received, on average, 23,831 bits per second over the reporting period, then the Average Network Usage would be the combined total of these two values: 24,858 bits per second.
- **Total Network Usage (BPS).** The total of all network read and write transactions in bits per second over the reporting period.

4.1.2.2. Host Health History

This report displays the performance of resources (CPU, memory, network reads, and network writes) on specific host in relation to threshold values.

The colored lines (red, green, yellow) represent your threshold values. You can use this report with the Pool Health report for a host to determine how a particular host's performance might be affecting overall pool health. When you are editing the performance thresholds, you can use this report for insight into host performance.

You can display resource utilization as a daily or hourly average. The hourly average lets you see the busiest hours of the day, averaged, for the time period.

To view report data grouped by hour, expand + **Click to view report data grouped by house for the time period** under the **Host Health History** title bar.

Workload Balancing displays the average for each hour for the time period you set. The data point is based on a utilization average for that hour for all days in the time period. For example, in a report for May 1, 2009 to May 15, 2009, the Average CPU Usage data point represents the resource utilization of all fifteen days at 12:00 hours combined together as an average. That is, if CPU utilization was 82% at 12PM on May 1st, 88% at 12PM on May 2nd, and 75% on all other days, the average displayed for 12PM is 76.3%.

Note:

Workload Balancing smooths spikes and peaks so data does not appear artificially high.

4.1.2.3. Pool Optimization Performance History

The optimization performance report displays optimization events (that is, when you optimized a resource pool) against that pool's average resource usage. Specifically, it displays resource usage for CPU, memory, network reads, and network writes.

The dotted line represents the average usage across the pool over the period of days you select. A blue bar indicates the day on which you optimized the pool.

This report can help you determine if Workload Balancing is working successfully in your environment. You can use this report to see what led up to optimization events (that is, the resource usage before Workload Balancing recommended optimizing).

This report displays average resource usage for the day; it does not display the peak utilization, such as when the system is stressed. You can also use this report to see how a resource pool is performing if Workload Balancing is not making optimization recommendations.

In general, resource usage should decline or be steady after an optimization event. If you do not see improved resource usage after optimization, consider readjusting threshold values. Also, consider whether or not the



resource pool has too many virtual machines and whether or not new virtual machines were added or removed during the time frame you specified.

4.1.2.4. Pool Audit Trail

This report displays the contents of the XenServer Audit Log, a XenServer feature designed to log attempts to perform unauthorized actions and select authorized actions, including import/export, host and pool backups, and guest and host console access. The report gives more meaningful information when XenServer administrators are given their own user accounts with distinct roles assigned to them using the Role-Based Access Control feature.

Important:

To run the audit log report, the Audit Logging feature must be enabled. By default, Audit Log is always enabled in the Workload Balancing virtual appliance.

The enhanced Pool Audit Trail feature allows you to specify the granularity of the audit log report. You can also search and filter the audit trail logs by specific users, objects, and by time. The Pool Audit Trail Granularity is set to **Minimum** by default. This option captures limited amount of data for specific users and object types. You can modify the setting at any time based on the level of detail you would require in your report. For example, set the granularity to **Medium** for a user-friendly report of the audit log. If you require a detailed report, set the option to **Maximum**.

4.1.2.4.1. Report Contents

The Pool Audit Trail report contains the following:

- Time. The time XenServer recorded the user's action.
- User Name. The name of the person who created the session in which the action was performed. In some cases, this may be the User ID
- Event Object. The object that was the subject of the action (for example, a virtual machine).
- Event Action. The action that occurred. For definitions of these actions, see Audit Log Event Names.
- Access. Whether or not the user had permission to perform the action.
- Object Name. The name of the object (for example, the name of the virtual machine).
- Object UUID. The UUID of the object (for example, the UUID of the virtual machine).
- Succeeded. This provides the status of the action (that is, whether or not it was successful).

4.1.2.4.2. Audit Log Event Names

The Audit Log report logs XenServer events, event objects and actions, including import/export, host and pool backups, and guest and host console access. The following table defines some of the typical events that appear frequently in the XenServer Audit Log and Pool Audit Trail report, and it also specifies the granularity of these events.

In the Pool Audit Trail report, the events listed in the **Event Action** column apply to a pool, VM, or host. To determine what the events apply to, see the **Event Object** and **Object Name** columns in the report. For additional event definitions, see the events section of the *Citrix XenServer Management API*.

Pool Audit Trail Granularity	Event Action	User Action
Minimum	VM.start	Started a VM
Minimum	VM.copy	Copied the specified VM, creating a new VM
Minimum	host.reboot	Restarted the XenServer host
Minimum	host-disable	Put the host into a state where no new VMs can be started

Pool Granularity	Audit Trail	Event Action	User Action
Minimum		pool.join	Instructed the host to join a new pool
Minimum		pool.join_force	Instructed (forced) the host to join a pool
Medium		SR.destroy	Destroyed the Storage Repository
Medium		SR.create	Created a new Storage Repository
Medium		VDI.snapshot	Took a read-only snapshot of the VDI, returning a reference to the snapshot
Medium		VDI.clone	Took an exact copy of the VDI returning a reference to the new disk
Medium		VIF.plug	Hot-plugged the specified VIF, dynamically attaching it to the running VM
Medium		VIF.unplug	Hot-unplugged the specified VIF, dynamically detaching it from the running VM
Maximum		auth.get_subject_identifi	Queried the external directory service to obtain the subject identifier as a string from the human-readable subject name
Maximum		task.cancel	Requested that a task be cancelled
Maximum		VBD.insert	Inserted new media into the device
Maximum		VIF.get_by_uuid	Obtained a reference to the VIF instance with the specified UUID
Maximum		VIF.get_shareable	Obtained the shareable field of the given VDI
Maximum		SR.get_all	Returns a list of all of the SRs known to the system
Maximum		pool.create_new_blob	Created a placeholder for a named binary piece of data that is associated with this pool
Maximum		host.send_debug_keys	Injected the given string as debugging keys into Xen
Maximum		VM.get_boot_record	Returned a record describing the VMs dynamic state, initialised when the VM boots and updated to reflect runtime configuration changes, for example, CPU hotplug

4.1.2.5. Pool Health

The pool health report displays the percentage of time a resource pool and its hosts spent in four different threshold ranges: Critical, High, Medium, and Low. You can use the Pool Health report to evaluate the effectiveness of your performance thresholds.

A few points about interpreting this report:

- Resource utilization in the Average Medium Threshold (blue) is the optimum resource utilization regardless of the placement strategy you selected. Likewise, the blue section on the pie chart indicates the amount of time that host used resources optimally.

- Resource utilization in the Average Low Threshold Percent (green) is not necessarily positive. Whether Low resource utilization is positive depends on your placement strategy. For example, if your placement strategy is Maximum Density and most of the time your resource usage was green, Workload Balancing might not be fitting the maximum number of virtual machines possible on that host or pool. If this is the case, you should adjust your performance threshold values until the majority of your resource utilization falls into the Average Medium (blue) threshold range.
- Resource utilization in the Average Critical Threshold Percent (red) indicates the amount of time average resource utilization met or exceeded the Critical threshold value.

If you double-click on a pie chart for a host's resource usage, XenCenter displays the Host Health History report for that resource (for example, CPU) on that host. Clicking the **Back to Parent Report** toolbar button returns you to the Pool Health history report.

If you find the majority of your report results are not in the Average Medium Threshold range, you probably need to adjust the Critical threshold for this pool. While Workload Balancing provides default threshold settings, these defaults are not effective in all environments. If you do not have the thresholds adjusted to the correct level for your environment, the Workload Balancing optimization and placement recommendations might not be appropriate. For more information, see [Section 5.1.1.2.2, "Changing the Critical Thresholds"](#).

4.1.2.6. Pool Health History

This report provides a line graph of resource utilization on all physical hosts in a pool over time. It lets you see the trend of resource utilization—if it tends to be increasing in relation to your thresholds (Critical, High, Medium, and Low). You can evaluate the effectiveness of your performance thresholds by monitoring trends of the data points in this report.

Workload Balancing extrapolates the threshold ranges from the values you set for the Critical thresholds when you connected the pool to Workload Balancing. Although similar to the Pool Health report, the Pool Health History report displays the average utilization for a resource on a specific date rather than the amount of time overall the resource spent in a threshold.

With the exception of the Average Free Memory graph, the data points should never average above the Critical threshold line (red). For the Average Free Memory graph, the data points should never average *below* the Critical threshold line (which is at the bottom of the graph). Because this graph displays *free* memory, the Critical threshold is a low value, unlike the other resources.

A few points about interpreting this report:

- When the Average Usage line in the chart approaches the Average Medium Threshold (blue) line, it indicates the pool's resource utilization is optimum regardless of the placement strategy configured.
- Resource utilization approaching the Average Low Threshold (green) is not necessarily positive. Whether Low resource utilization is positive depends on your placement strategy. For example, if your placement strategy is Maximum Density and most days the Average Usage line is at or below the green line, Workload Balancing might not be placing virtual machines as densely as possible on that pool. If this is the case, you should adjust the pool's Critical threshold values until the majority of its resource utilization falls into the Average Medium (blue) threshold range.
- When the Average Usage line intersects with the Average Critical Threshold Percent (red), this indicates the days when the average resource utilization met or exceeded the Critical threshold value for that resource.

If you find the data points in the majority of your graphs are not in the Average Medium Threshold range, but you are satisfied with the performance of this pool, you might need to adjust the Critical threshold for this pool. For more information, see [Section 5.1.1.2.2, "Changing the Critical Thresholds"](#).

4.1.2.7. Pool Optimization History

The Pool Optimization History report provides chronological visibility into Workload Balancing optimization activity.



Optimization activity is summarized graphically and in a table. Drilling into a date field within the table displays detailed information for each pool optimization performed for that day.

This report lets you see the following information:

- **VM Name.** The name of the virtual machine that Workload Balancing optimized.
- **Reason.** The reason for the optimization.
- **Status.** If the optimization was successful.
- **From Host.** The physical server where the virtual machine was originally hosted.
- **To Host.** The physical server where the virtual machine was migrated.
- **Time.** The time when the optimization occurred.

Tip:

You can also generate a Pool Optimization History report from the **WLB** tab by clicking the **View History** link.

4.1.2.8. Virtual Machine Motion History

This line graph displays the number of times virtual machines migrated on a resource pool over a period of time. It indicates if a migration resulted from an optimization recommendation and to which host the virtual machine moved. This report also indicates the reason for the optimization. You can use this report to audit the number of migrations on a pool.

Some points about interpreting this report:

- The numbers on the left side of the chart correspond with the number of migrations possible, which is based on how many virtual machines are in a resource pool.
- You can look at details of the migrations on a specific date by expanding the + sign in the **Date** section of the report.

4.1.2.9. Virtual Machine Performance History

This report displays performance data for each virtual machine on a specific host for a time period you specify. Workload Balancing bases the performance data on the amount of virtual resources allocated for the virtual machine. For example, if the Average CPU Usage for your virtual machine is 67%, this means that your virtual machine was using, on average, 67% of its virtual CPU for the period you specified.

The initial view of the report displays an average value for resource utilization over the period you specified.

Expanding the + sign displays line graphs for individual resources. You can use these graphs to see trends in resource utilization over time.

This report displays data for CPU Usage, Free Memory, Network Reads/Writes, and Disk Reads/Writes.

Chapter 5. Managing Workload Balancing Features and Settings

This chapter provides information about how to perform optional changes to Workload Balancing settings, including how to:

- Adjust the optimization mode
- Optimize and manage power automatically
- Change the critical thresholds
- Tune metric weightings
- Exclude hosts from recommendations
- Configure advanced automation settings and data storage
- Adjust the Pool Audit Trail granularity settings

This chapter assumes that you already connected your pool to a Workload Balancing virtual appliance. For information about downloading, importing, and configuring a Workload Balancing virtual appliance, see the *Citrix Workload Balancing 6.5 Quick Start*. To connect to the virtual appliance, see [Section 6.1.1, “Connecting to the Workload Balancing Virtual Appliance”](#).

5.1. Changing Workload Balancing Settings

After connecting to the Workload Balancing virtual appliance, you can, if desired, edit the settings Workload Balancing uses to calculate placement and recommendations.

Placement and optimization settings you can modify include changing the placement strategy, configuring automatic optimizations and power management, editing performance thresholds and metric weightings, and excluding hosts.

Workload Balancing settings apply collectively to all virtual machines and hosts in the pool.

Provided the network and disk thresholds align with the hardware in your environment, you might want to consider using most of the defaults in Workload Balancing initially.

After Workload Balancing is enabled for a while, Citrix recommends evaluating your performance thresholds and determining if you need to edit them. For example, consider if you are:

- Getting recommendations when they are not yet required. If this is the case, try adjusting the thresholds until Workload Balancing begins providing suitable recommendations.
- Not getting recommendations when you think you should receive them. For example, if your network has insufficient bandwidth and you do not receive recommendations, you might need to tweak your settings. If this is the case, try lowering the network critical thresholds until Workload Balancing begins providing recommendations.

Before you edit your thresholds, you might find it handy to generate a Pool Health report and the Pool Health History report for each physical host in the pool.

You can use the **Workload Balancing Configuration** properties in XenCenter to modify the configuration settings.

To update the credentials XenServer and the Workload Balancing server use to communicate, see [Section 8.1.7, “Editing the Workload Balancing Configuration File”](#).

To display the Workload Balancing Settings dialog box

1. In the **Infrastructure** pane of XenCenter, select XenCenter > your-pool.



2. In the **Properties** pane, click the **WLB** tab.
3. In the **WLB** tab, click **Settings**.

5.1.1. Adjusting the Optimization Mode

Workload Balancing makes recommendations to rebalance, or *optimize*, the virtual-machine workload in your environment based on a strategy for placement you select known as the *optimization mode*.

Workload Balancing lets you choose from two optimization modes:

- **Maximize Performance.** (Default.) Workload Balancing attempts to spread workload evenly across all physical hosts in a resource pool. The goal is to minimize CPU, memory, and network pressure for all hosts. When Maximize Performance is your placement strategy, Workload Balancing recommends optimization when a host reaches the High threshold.
- **Maximize Density.** Workload Balancing attempts to minimize the number of physical hosts that must be online by consolidating the active virtual machines.

When you select Maximize Density as your placement strategy, you can specify parameters similar to the ones in Maximize Performance. However, Workload Balancing uses these parameters to determine how it can pack virtual machines onto a host. When Maximize Density is your placement strategy, Workload Balancing recommends consolidation optimizations when a virtual machine reaches the Low threshold.

Workload Balancing also lets you apply these optimization modes all of the time, *Fixed*, or switch between modes for specified time periods, *Scheduled*:

- *Fixed* optimization modes set Workload Balancing to a specific optimization behavior—either to try to create the best performance or the highest density—at all times.
- *Scheduled* optimization modes let you schedule for Workload Balancing to apply different optimization modes depending on the time of day. For example, you might want to configure Workload Balancing to optimize for performance during the day when you have users connected and then, to save energy, specify for Workload Balancing to optimize for Maximum Density at night.

When you configure Scheduled optimization modes, Workload Balancing automatically changes to the optimization mode at the beginning of the time period you specified. You can configure Everyday, Weekdays, Weekends, or individual days. For the hour, you select a time of day.

To set an optimization mode for all time periods

1. In the **Resources** pane of XenCenter, select XenCenter > *your-pool*.
2. In the **Properties** pane, click the **WLB** tab.
3. On the **WLB** tab, click **Settings**.
4. In the left pane, click **Optimization Mode**.
5. In the **Fixed** section of the **Optimization Mode** page, select one of these optimization modes:
 - **Maximize Performance.** (Default.) Attempts to spread workload evenly across all physical hosts in a resource pool. The goal is to minimize CPU, memory, and network pressure for all hosts.
 - **Maximize Density.** Attempts to fit as many virtual machines as possible onto a physical host. The goal is to minimize the number of physical hosts that must be online. (Note that Workload Balancing considers the performance of consolidated VMs and issues a recommendation to improve performance if a resource on a host reaches a Critical threshold.)

To specify times when the optimization mode will change automatically

1. In the **Infrastructure** pane of XenCenter, select XenCenter > *your-pool*.



2. In the **Properties** pane, click the **WLB** tab.
3. On the **WLB** tab, click **Settings**.
4. In the left pane, click **Optimization Mode**
5. In the Optimization Mode pane, select **Scheduled**. The **Scheduled** section becomes available.
6. Click **Add New**.
7. In the **Change to** box, select one of the following modes:
 - **Maximize Performance**. Attempts to spread workload evenly across all physical hosts in a resource pool. The goal is to minimize CPU, memory, and network pressure for all hosts.
 - **Maximize Density**. Attempts to fit as many virtual machines as possible onto a physical host. The goal is to minimize the number of physical hosts that must be online.
8. Select the day of the week and the time when you want Workload Balancing to begin operating in this mode.
9. Create more scheduled mode changes (that is, "tasks") until you have the number you need. If you only schedule one task, Workload Balancing will switch to that mode as scheduled, but then it will never switch back.
10. Click **OK**.

To delete or pause a scheduled optimization mode task

1. Display the Optimization Mode dialog box by following steps 1 to 4 in the previous procedure.
2. Select the task you want to delete or disable from the Scheduled Mode Changes list.
3. Do one of the following:
 - **Delete the task permanently**. Click the **Delete** button.
 - **Stop the task from running temporarily**. Right-click the task and click **Disable**.

Tip:

You can also disable or enable tasks by selecting the task, clicking **Edit**, and selecting the **Enable Task** check box in the **Optimization Mode Scheduler** dialog.

Note:

To re-enable a task, right click the task in the **Scheduled Mode Changes** list and click **Enable**.

To edit a scheduled optimization mode task

1. Do one of the following:
 - Double-click the task you want to edit.
 - Select the task you want to edit, and click **Edit**.
2. In the **Change to** box, select a different mode or make other changes as desired.

Note:

Clicking **Cancel**, before clicking **OK**, will undo any changes you made in the **Optimization** tab, including deleting a task.

5.1.1.1. Optimizing and Managing Power Automatically

You can configure Workload Balancing to apply recommendations automatically (*Automation*) and turn hosts on or off automatically (*Power Management*). In order to power down hosts automatically (for example, during low-



usage periods), you must configure Workload Balancing to apply recommendations automatically and enable power management. Both power management and automation are described in the sections that follow.

5.1.1.1.1. Applying Recommendations Automatically

Workload Balancing lets you configure for it to apply recommendations on your behalf and perform the optimization actions it recommends automatically. You can use this feature, which is known as *Automation*, to apply any recommendations automatically, including ones to improve performance or power down hosts. However, to power down hosts as virtual-machines usage drops, you must configure automation, power management, and Maximum Density mode.

By default, Workload Balancing does not apply recommendations automatically. You must enable Automation if you want Workload Balancing to apply recommendations automatically. If you do not, you must apply recommendations manually by clicking **Apply Recommendations**.

Workload Balancing will not automatically apply recommendations to hosts or virtual machines if the recommendations conflict with High Availability settings. If a pool will become overcommitted by applying Workload Balancing optimization recommendations, XenCenter will prompt you whether or not you want to continue applying the recommendation. When Automation is enabled, Workload Balancing will not apply any power-management recommendations that exceed the number of host failures to tolerate in the High Availability plan.

When Workload Balancing is running with the Automation feature enabled, this is sometimes referred to as running in *automated mode*.

It is possible to tune how Workload Balancing applies recommendations in automated mode. For information, see [Section 5.1.1.4.1, "Setting Conservative or Aggressive Automated Recommendations"](#)

5.1.1.1.2. Enabling Workload Balancing Power Management

The term *power management* refers to the ability to turn the power on or off for physical hosts. In a Workload Balancing context, this term refers to powering hosts in a pool on or off based on the pool's total workload.

Configuring Workload Balancing power management on a host requires that:

- The hardware for the host has remote power on/off capabilities
- The Host Power On feature is configured for the host
- The host has been explicitly selected as a host to participate in (Workload Balancing) Power Management

In addition, if you want Workload Balancing to power off hosts automatically, you also need to configure Workload Balancing to:

- Apply recommendations automatically
- Apply Power Management recommendations automatically

When enabled and the pool is in Maximum Density mode, if Workload Balancing detects unused resources, it recommends powering off hosts until it eliminates all excess capacity in the pool. If Workload Balancing detects there is not sufficient host capacity in the pool to turn off hosts, it recommends leaving the hosts on until the pool's workload decreases enough to power off hosts. When you configure Workload Balancing to power off extra hosts automatically, it applies these recommendations automatically and, consequently, behaves in the same way.

When a host is set to participate in Power Management, Workload Balancing makes power-on/off recommendations as needed. If you configure Workload Balancing so that it can automatically power on hosts when you are running in Maximum Performance mode, Workload Balancing will power on one or more hosts if a resource's utilization on a host exceeds the High threshold. However, when running in Maximum Performance mode, Workload Balancing never powers off hosts after it has powered them on.

If you turn on the option to apply Power Management recommendations automatically, you do so at the pool level. However, you can specify which hosts from the pool you want to participate in Power Management.

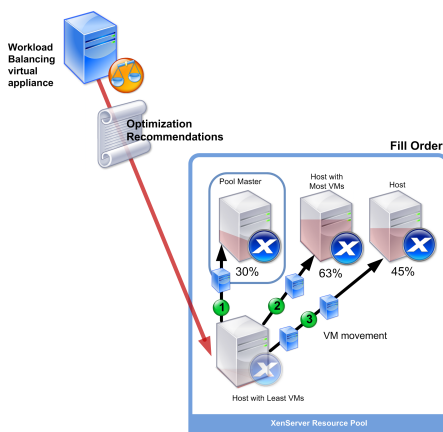
Understanding Power Management Behavior

Before Workload Balancing recommends powering hosts on or off, it selects the hosts to transfer virtual machines to (that is, to "fill"). It does so in the following order:

1. Filling the pool master since it is the host that cannot be powered off.
2. Filling the host with the most virtual machines.
3. Filling subsequent hosts according to which hosts have the most virtual machines running.

When Workload Balancing fills the pool master, it does so assuming artificially low (internal) thresholds for the master. Workload Balancing uses these low thresholds as a buffer to prevent the pool master from being overloaded.

Workload Balancing fills hosts in this order to encourage density.



This illustration shows how, when consolidating VMs on hosts in Maximum Density mode, XenServer attempts to fill the pool master first, the most loaded host second, and the least loaded host third.

If Workload Balancing detects a performance issue while the pool is in Maximum Density mode, it attempts to address the issue by recommending migrating workloads among the powered-on hosts. If Workload Balancing cannot resolve the issue using this method, it attempts to power-on a host. (Workload Balancing determines which host(s) to power-on by applying the same criteria it would if the optimization mode was set to Maximum Performance.)

When Workload Balancing is running in Maximum Performance mode, Workload Balancing recommends powering on hosts until the resource utilization on all hosts in the pool falls below the High threshold.

If, while migrating one or more virtual machines, Workload Balancing determines that increasing capacity would benefit the pool's overall performance, it powers on hosts automatically or recommends doing so.

Important:

Workload Balancing never recommends powering on a host unless Workload Balancing powered it off.

5.1.1.1.3. Designing Environments for Power Management and VM Consolidation

When you are planning a XenServer implementation and you intend to configure automatic VM consolidation and power management, consider your workload design. For example, you may want to:

- **Place Different Types of Workloads in Separate Pools.** If you have an environment with distinct types of workloads (for example, user applications versus domain controllers) or types of applications that perform better with certain types of hardware, consider if you need to locate the virtual machines hosting these workloads in different pools.

Because power management and VM consolidation are managed at the pool level, you should design pools so they contain workloads that you want consolidated at the same rate, factoring in considerations such as those discussed in [Section 5.1.1.4, “Controlling Automated Recommendations”](#).

- **Exclude Hosts from Workload Balancing.** Some hosts may need to be on at all times. See [Section 5.1.1.3, “Excluding Hosts from Recommendations”](#) for more information.

5.1.1.1.4. To apply optimization recommendations automatically

1. In the **Infrastructure** pane of XenCenter, select XenCenter > your-pool.
2. In the **Properties** pane, click the **WLB** tab.
3. In the **WLB** tab, click **Settings**.
4. In the left pane, click **Automation**.
5. Select one or more of the following check boxes:
 - **Automatically apply Optimization recommendations.** When you select this option, you do not need to accept optimization recommendations manually. Workload Balancing automatically accepts optimization and placement recommendations it makes.
 - **Automatically apply Power Management recommendations.** The behavior of this option varies according to the pool's optimization mode:
 - **Maximum Performance Mode.** When **Automatically apply Power Management recommendations** is enabled, Workload Balancing automatically powers on hosts when doing so improves host performance.
 - **Maximum Density Mode.** When **Automatically apply Power Management recommendations** is enabled, Workload Balancing automatically powers off hosts when resource utilization drops below the Low threshold (that is, Workload Balancing powers hosts off automatically during low usage periods).
6. (Optional.) Fine-tune optimization recommendations by clicking **Advanced** in the left pane of the Settings dialog and doing one or more of the following:
 - Specifying the number of times Workload Balancing must make an optimization recommendation before the recommendation is applied automatically. The default is three times, which means the recommendation is applied on the third time it is made.
 - Selecting the lowest level of optimization recommendation that you want Workload Balancing to apply automatically. The default is **High**.
 - Changing the aggressiveness with which Workload Balancing applies its optimization recommendations.

You may also want to specify the number of minutes Workload Balancing has to wait before applying an optimization recommendation to a recently moved VM.

All of these settings are explained in more depth in [Section 5.1.1.4.1, “Setting Conservative or Aggressive Automated Recommendations”](#).

7. Do one of the following:
 - If you want to configure power management, click **Automation/Power Management** and proceed to the [Section 5.1.1.1.5, “To select hosts for power management”](#).
 - If you do not want to configure power management and you are finished configuring automation, click **OK**.

5.1.1.1.5. To select hosts for power management

1. In the Power Management section, select the hosts that you want Workload Balancing to recommend powering on and off.

Note:

Selecting hosts for power management recommendations without selecting the **Automatically apply Power Management recommendations** check box results in Workload



Balancing suggesting power-management recommendations but not applying them automatically for you.

2. Click **OK**. If none of the hosts in the resource pool support remote power management, Workload Balancing displays the message, "No hosts support Power Management."

5.1.1.2. Understanding When Workload Balancing Makes Recommendations

Workload Balancing continuously evaluates the resource metrics of physical hosts and VMs across the pool(s) it is managing against *thresholds*. Thresholds are preset values that function like boundaries that a host must exceed before Workload Balancing can make an optimization recommendation. At a very high level, the Workload Balancing process is as follows:

1. Workload Balancing detects that the threshold for a resource was violated.
2. Workload Balancing evaluates if it will make an optimization recommendation.
3. Workload Balancing determines which host(s) it will recommend function as the *destination host(s)*, which is the host where Workload Balancing will recommend relocating one or more VMs.
4. Workload Balancing makes the recommendation.

After Workload Balancing determines that a host could benefit from optimization, before it makes the recommendation, it evaluates other hosts on the pool to decide (a) the order in which it should make the optimization (what hosts, what VMs) and (b) where it should recommend placing a virtual machine when it does make a recommendation. To accomplish these two tasks, Workload Balancing uses thresholds and *weightings* as follows:

- **Thresholds**, which are the boundary values Workload Balancing compares your pool's resource metrics against, are used to determine whether or not to make a recommendation and what hosts are a suitable candidate for hosting relocated virtual machines.
- **Weightings**, which are a way of ranking resources according to how much you want them to be considered, are used to determine the processing order. That is, after Workload Balancing determines it needs to make a recommendation, it uses your specifications of what resources are important to determine which hosts' performance to address first and which virtual machines to recommend migrating first.

For each resource Workload Balancing monitors, it has four levels of thresholds (Critical, High, Medium, and Low), which are discussed in the sections that follow. Workload Balancing evaluates whether to make a recommendation when a resource metric on a host:

- Exceeds the High threshold when the pool is running in Maximum Performance mode (improve performance)
- Drops below the Low threshold when the pool is running in Maximum Density mode (consolidate VMs on hosts)
- Exceeds the Critical threshold when the pool is running in Maximum Density mode (improve performance)

For example, if the High threshold for a pool running in Maximum Performance mode is set to 80%, when the CPU utilization on a host reaches 80.1%, Workload Balancing will evaluate whether or not to issue a recommendation.

When a resource violates its threshold, Workload Balancing evaluates the resource's metric against its historical performance to prevent issuing an optimization recommendation based on a temporary resource spike. To do so, Workload Balancing creates an *historically averaged utilization* metric by evaluating the data for resource utilization captured at the following times:

Data Captured	Weight
Immediately, at the time threshold was exceeded (that is, real-time data)	70%
Thirty minutes before the threshold was exceeded	25%

Data Captured	Weight
Twenty-four hours before the threshold was exceeded	5%

For example, if the CPU utilization on the host exceeds the High threshold at 12:02 PM on Thursday, Workload Balancing checks the data utilization at 11:32 AM on Thursday, and at 12:02PM on Wednesday (the previous day). If the CPU utilization is 80.1% at 12:02 PM, but only 50% at 11:32AM, and 78% at 12:32 PM on Wednesday, Workload Balancing does not make a recommendation. This is because the historically averaged utilization is 72.47%, so Workload Balancing assumes the utilization is a temporary spike. However, if the CPU utilization was 78% at 11:32AM, Workload Balancing would make a recommendation since the historically averaged utilization is 80.1%.

5.1.1.2.1. Optimization and Consolidation Process

The Workload Balancing process for determining potential optimizations varies according to the optimization mode (Maximum Performance or Maximum Density). However, regardless of the optimization mode, optimization and placement recommendations are made using a two-stage process:

1. Determine potential optimizations. (That is, what VMs to migrate off hosts.)
2. Determine placement recommendations. (That is, what hosts would be suitable candidates for new hosts.)

Note:

Workload Balancing only recommends migrating VMs that meet the XenServer criteria for live migration, including the destination host must have the storage the VM requires. Likewise, the destination host must have sufficient resources to accommodate adding the VM without exceeding the thresholds of the optimization mode configured on the pool (for example, the High threshold in Maximum Performance mode and the Critical threshold for Maximum Density mode).

When Workload Balancing is running in automated mode, you can tune the way it applies recommendations. See [Section 5.1.1.4.1, “Setting Conservative or Aggressive Automated Recommendations”](#) for more information.

Optimization Recommendation Process in Maximum Performance Mode

When running in Maximum Performance mode, Workload Balancing uses the following process to determine potential optimizations:

1. Every two minutes Workload Balancing evaluates the resource utilization for each host in the pool. It does so by monitoring on each host and determining if each resource's utilization exceeds its High threshold. See [Section 5.1.1.2.2, “Changing the Critical Thresholds”](#) for more information about the High threshold.

If, in Maximum Performance mode, a resource's utilization exceeds its High threshold, then Workload Balancing starts the process to determine if it wants to make an optimization recommendation. Workload Balancing determines if it should make an optimization recommendation based on whether or not doing so can ease performance constraints, such as ones revealed by the High threshold.

For example, if Workload Balancing sees that the performance of the virtual machines on Host A is being negatively affected by insufficient CPU resources, if Workload Balancing can find another host with less CPU utilization, it will recommend moving one or more virtual machines to another host.

2. If a resource's utilization on a host exceeds the relevant threshold, Workload Balancing combines the resource's current utilization with the historical data from thirty minutes ago and twenty-four hours ago to form the historically averaged utilization. If the historically averaged utilization exceeds the resource's threshold, Workload Balancing determines it will make an optimization recommendation.
3. Workload Balancing uses metric weightings to determine what hosts it should optimize first. The resource to which you have assigned the most weight is the one that Workload Balancing attempts to address first. See [Section 5.1.1.2.3, “Tuning Metric Weightings”](#) for information about metric weightings.
4. Workload Balancing determines which hosts can support the VM(s) it wants to migrate off of host(s).



Workload Balancing makes this determination by calculating the projected effect on resource utilization of placing different combinations of VMs on hosts. (Workload Balancing uses a method of performing these calculations that in mathematics is known as *permutation*.)

To do so, Workload Balancing creates a single metric or *score* to forecast the impact of migrating a VM to the host. The score indicates the suitability of a host as a home for additional VMs.

To score the host's performance, Workload Balancing combines the host's current metrics, the host's metrics from the last thirty minutes, the host's metrics from 24 hours ago, and the VM's metrics.

5. After scoring the hosts and VMs, Workload Balancing attempts to build (in essence) virtual models of what the hosts would look like with different combinations of VMs so that it can determine the best host to place the VM.

In Maximum Performance mode, Workload Balancing uses metric weightings to determine what hosts it should optimize first and what VMs on those hosts it should migrate first. Workload Balancing bases its models on the metric weightings. For example, if CPU utilization is assigned the highest importance, Workload Balancing sorts hosts and VMs to optimize first according to what hosts are most affected by CPU utilization (that is, are running closest to the High threshold for CPU utilization) and what VMs have the highest CPU utilization (or are running the closest to its High threshold).

6. Workload Balancing continues calculating optimizations. It perceives hosts as potential candidates for optimization and views VMs as candidates for migration until the *predicted resource utilization* on the VM's host drops below the configured High threshold. The term predicted resource utilization refers to the resource utilization Workload Balancing forecasts a host will have after Workload Balancing has added or removed a VM from the host.

Consolidation Process in Maximum Density Mode

Workload Balancing determines if it should make a recommendation (for consolidation) based on whether it can migrate a virtual machine off a host and still run the destination host below the Critical threshold.

1. When a resource's utilization drops below its Low threshold, Workload Balancing begins calculating potential consolidation scenarios.
2. When Workload Balancing discovers a potential way in which it can consolidate VMs on a host, it evaluates whether or not the destination host is a suitable home for the VM.
3. Like in Maximum Performance mode, Workload Balancing scores the host to determine the suitability of a host as a home for new VMs.

For example, if Workload Balancing determines that it can consolidate virtual machines on fewer hosts, before it makes an optimization recommendation, Workload Balancing checks to make sure that the resource utilization on the destination hosts will not exceed the Critical thresholds after the VMs are relocated to them.

Note:

Workload Balancing does not consider metric weightings when it makes a consolidation recommendation; it only considers metric weightings to ensure performance on hosts.

4. After scoring the hosts and VMs, Workload Balancing attempts to build (in essence) virtual models of what the hosts would look like with different combinations of VMs so that it can determine the best host to place the VM.
5. Workload Balancing calculates the effect of adding more VMs to a host until it forecasts that adding another VM to the host would cause one of its resources to exceed the Critical threshold.
6. Workload Balancing recommendations always suggest filling the pool master first since it is the host that cannot be powered off. However, Workload Balancing applies a buffer to the pool master so that it cannot be over-allocated.
7. Workload Balancing continues to recommend migrating VMs on to hosts until no hosts remain that will not exceed a Critical threshold if a VM is migrated on to them.

5.1.1.2.2. Changing the Critical Thresholds

You might want to change Critical thresholds as a way of controlling when optimization recommendations are triggered. This section provides guidance about how to modify the default Critical thresholds on hosts in the pool and how values set for Critical threshold alter High, Medium, and Low thresholds.

Workload Balancing determines whether or not to produce recommendations based on if the averaged historical utilization for a resource on a host violates its threshold. As previously discussed in [Section 5.1.1.2.1, "Optimization and Consolidation Process"](#), Workload Balancing recommendations are triggered when the High threshold in Maximum Performance mode or Low and Critical thresholds for Maximum Density mode are violated. After you specify a new Critical threshold for a resource, Workload Balancing resets the resource's other thresholds relative to the new Critical threshold. (To simplify the user interface, the Critical threshold is the only threshold you can change through XenCenter.)

The following table shows the default values for the Workload Balancing thresholds:

Metric	Critical	High	Medium	Low
CPU Utilization	90%	76.5%	45%	22.5%
Free Memory	51MB	63.75MB	510MB	1020MB
Network Reads	25MB/sec	21.25MB/sec	12.5MB/sec	6.25MB/sec
Network Writes	25MB/sec	21.25MB/sec	12.5MB/sec	6.25MB/sec

To calculate the values for all metrics except memory (that is, the High, Medium, and Low CPU, network, and disk metrics), Workload Balancing multiplies the new value for the Critical threshold with the following factors:

- **High Threshold Factor:** 0.85
- **Medium Threshold Factor:** 0.50
- **Low Threshold Factor:** 0.25

This means that if you increase, for example, the pool's Critical threshold for CPU Utilization to 95%, Workload Balancing automatically resets the High, Medium, and Low thresholds to 80.75%, 47.5%, and 23.75% respectively.

To calculate the threshold values for free memory, Workload Balancing multiplies the Critical threshold with these factors:

- **High Threshold Factor:** 1.25
- **Medium Threshold Factor:** 10.0
- **Low Threshold Factor:** 20.0

To perform this calculation for a specific threshold, multiply the factor for the threshold with the value you entered for the critical threshold for that resource:

$$\text{High, Medium, or Low Threshold} = \text{Critical Threshold} * \text{Threshold Factor}$$

For example, if you change the Critical threshold for Network Reads to 40MB/sec and you want to know its Low threshold, you multiply 40 by 0.25, which equals 10MB/sec. To obtain the Medium threshold, you multiple 40 by 0.50, and so on.

While the Critical threshold triggers many optimization recommendations, other thresholds can also trigger optimization recommendations, as follows:

- **High threshold.**

- **Maximum Performance.** Exceeding the High threshold triggers optimization recommendations to relocate a VM to a host with lower resource utilization.
- **Maximum Density.** Workload Balancing will not recommend placing a virtual machine on host if moving that VM to the host will cause the utilization of any of the host's resources to exceed the High threshold value.
- **Low threshold.**
 - **Maximum Performance.** Workload Balancing does not trigger recommendations from the Low threshold.
 - **Maximum Density.** When a metric value drops below the Low threshold, it signals Workload Balancing that hosts are being underutilized and triggers an optimization recommendation to consolidate virtual machines on fewer hosts. Workload Balancing continues to recommend moving VMs onto a host until the metric values for one of the host's resource reaches its High threshold.

However, if after a VM is relocated, a resource's utilization on the VM's new host exceeds its Critical threshold, Workload Balancing will temporarily use an algorithm similar to the Maximum Performance load-balancing algorithm to find a new host for the virtual machines. Workload Balancing continues to use this algorithm to recommend moving virtual machines until resource utilization on hosts across the pool falls below the High threshold.

5.1.1.2.2.1. To change the critical thresholds

1. In the **Infrastructure** pane of XenCenter, select XenCenter > `your-resource-pool`.
2. In the **Properties** pane, click the **WLB** tab.
3. In the **WLB** tab, click **Settings**.
4. In the left pane, select **Critical Thresholds**. These critical thresholds are used to evaluate host resource utilization.
5. In **Critical Thresholds** page, type one or more new values in the **Critical Thresholds** boxes. The values represent resource utilization on the host.

Workload Balancing uses these thresholds when making virtual-machine placement and pool-optimization recommendations. Workload Balancing strives to keep resource utilization on a host below the critical values set.

5.1.1.2.3. Tuning Metric Weightings

The way in which Workload Balancing uses metric weightings when determining which hosts and VMs to process first varies according to the optimization mode, Maximum Density or Maximum Performance.

When Workload Balancing is processing optimization recommendations, it creates an *optimization order*. To determine this, Workload Balancing ranks the hosts to address first according to which hosts have the highest metric values for whatever resource is ranked as the most important in the metric weightings page.

In general, metric weightings are mainly used when a pool is in Maximum Performance mode. However, when Workload Balancing is in Maximum Density mode, it does use metric weightings if a resource exceeds its Critical threshold.

Maximum Performance mode

In Maximum Performance mode, Workload Balancing uses metric weightings to determine (a) which hosts' performance to address first and (b) which VMs to recommend migrating first.

For example, if you rank Network Writes as the most important resource for Workload Balancing to consider—that is, you move the **Metric Weighting** slider all the way to the right (**More Important**) and you move all the other sliders to the middle—then Workload Balancing will begin addressing performance issues (that is, making optimization recommendations) on the host with the highest number of Network Writes per second first.

If you configure all resources to be equally important (that is, the **Metric Weighting** slider is in the same place for all resources), Workload Balancing addresses CPU utilization first and memory second, as these are typically the most constrained resources.



Maximum Density mode

In Maximum Density mode, Workload Balancing only uses metric weightings when a host reaches the Critical threshold—then Workload Balancing applies a Maximum Performance-like algorithm until no Hosts are exceeding the Critical thresholds. When using the Maximum Performance-like algorithm, Workload Balancing uses metric weightings to determine the optimization order in the same way as it does for Maximum Performance mode.

If two or more hosts have resource(s) exceeding their Critical thresholds, Workload Balancing verifies the importance you set for each resource before determining which host to optimize first and which VMs on that host to relocate first.

For example, your pool contains Host A and Host B, which are in the following state:

- The CPU utilization on Host A exceeds the Critical threshold for CPU, and the metric weighting for CPU utilization is set to the far right of the slider (**More Important**).
- The memory utilization on Host B exceeds the Critical threshold for memory, and the metric weighting for memory utilization is set to the far left of the slider (**Less Important**).

Workload Balancing will recommend optimizing Host A first because the resource on it that reached the Critical threshold is the resource assigned the highest weight. After Workload Balancing determines that it needs to address the performance on Host A, Workload Balancing then begins recommending placements for VMs on that host beginning with the VM that has the highest CPU utilization, since that CPU utilization is the resource with the highest weight.

After Workload Balancing has recommended optimizing Host A, it makes optimization recommendations for Host B. When it recommends placements for the VMs on Host B, it does so by addressing CPU utilization first, since CPU utilization was assigned the highest weight.

If there are additional hosts that need optimization, Workload Balancing addresses the performance on those hosts according to what host has the third highest CPU utilization.

By default, all metric weightings are set to the farthest point on the slider (**More Important**).

Note:

The weighting of metrics is relative. This means that if all of the metrics are set to the same level, even if that level is **Less Important**, they will all be weighted the same. The relation of the metrics to each other is more important than the actual weight at which you set each metric.

5.1.1.2.3.1. To edit metric weighting factors

1. Stopping
2. In the **Infrastructure** pane of XenCenter, select XenCenter > `your-resource-pool`.
3. Click the **WLB** tab, and then click **Settings**.
4. In the left pane, select **Metric Weighting**.
5. In **Metric Weighting** page, as desired, adjust the sliders beside the individual resources.

Moving the slider towards **Less Important** indicates that ensuring virtual machines always have the highest amount of this resource available is not as vital on this resource pool.

5.1.1.3. Excluding Hosts from Recommendations

When configuring Workload Balancing, you can specify that specific physical hosts are excluded from Workload Balancing optimization and placement recommendations, including Start On placement recommendations.

Situations when you may want to exclude hosts from recommendations include when:

- You want to run the pool in Maximum Density mode and consolidate and shut down hosts, but there are specific hosts you want to exclude from this behavior.
- When two virtual-machine workloads always need to run on the same host (for example, if they have complementary applications or workloads).
- You have workloads that you do not want moved (for example, a domain controller or database server).
- You want to perform maintenance on a host and you do not want VMs placed on the host.
- The performance of the workload is so critical that the cost of dedicated hardware is irrelevant.
- Specific hosts are running high-priority workloads (virtual machines), and you do not want to use the High Availability feature to prioritize these virtual machines.
- The hardware in the host is not the optimum for the other workloads in the pool.

Regardless of whether you specify a fixed or scheduled optimization mode, hosts excluded remain excluded even when the optimization mode changes. Therefore, if you only want to prevent Workload Balancing from shutting off a host automatically, consider not enabling (or deselecting) Power Management for that host instead as described in [Section 5.1.1.1, “Optimizing and Managing Power Automatically”](#).

When you exclude a host from recommendations, you are specifying for Workload Balancing not to manage that host at all. This means that Workload Balancing will not make any optimization recommendations for an excluded host. In contrast, when you do not select a host to participate in Power Management, Workload Balancing still manages the host, but it will not issue power-management recommendations for that host.

5.1.1.3.1. To exclude hosts from Workload Balancing

Use this procedure to exclude a host in a pool that Workload Balancing is managing from power management, host evacuation, placement, and optimization recommendations.

1. In the **Resources** pane of XenCenter, select XenCenter > `your-resource-pool`.
2. In the **Properties** pane, click the **WLB** tab.
3. In the **WLB** tab, click **Settings**.
4. In the left pane, select **Excluded Hosts**.
5. In **Excluded Hosts** page, select the hosts for which you do not want WLB to recommend alternate placements and optimizations.

5.1.1.4. Controlling Automated Recommendations

Workload Balancing supplies some advanced settings that let you to control how Workload Balancing applies automated recommendations. These settings appear on the **Advanced** page of the **Workload Balancing Configuration** dialog.

To display the Advanced page of the Workload Balancing Configuration dialog

1. In the **Resources** pane of XenCenter, select XenCenter > `your-resource-pool`.
2. In the **Properties** pane, click the **WLB** tab.
3. In the **WLB** tab, click **Settings**.
4. In the left pane, select **Advanced**.

5.1.1.4.1. Setting Conservative or Aggressive Automated Recommendations

When running in automated mode, the frequency of optimization and consolidation recommendations and how soon they are automatically applied is a product of multiple factors, including:

- How long you specify Workload Balancing waits after moving a VM before making another recommendation
- The number of recommendations Workload Balancing must make before applying a recommendation automatically



- The severity level a recommendation must achieve before the optimization is applied automatically
- The level of consistency in recommendations (recommended VMs to move, destination hosts) Workload Balancing requires before applying recommendations automatically

Important:

In general, Citrix recommends that you do not adjust the settings for factors without either guidance from Citrix Technical Support or significant observation and testing of your pool's behavior with Workload Balancing enabled. Incorrectly configuring these settings can result in Workload Balancing not making any recommendations.

5.1.1.4.1.1. VM Migration Interval

You can specify the number of minutes Workload Balancing must wait after the last time a particular virtual machine was moved, regardless of the cause, before Workload Balancing can generate another recommendation that includes that particular recently moved virtual machine.

The *recommendation interval* is designed to prevent Workload Balancing from generating recommendations for artificial reasons (for example, if there was a temporary utilization spike).

When Automation is configured, it is especially important to be careful when modifying the recommendation interval. If an issue occurs that leads to continuous, recurring spikes, increasing the frequency (that is, setting a lower number) can generate many recommendations and, consequently, relocations.

Note:

Setting a recommendation interval does not affect how long Workload Balancing waits to factor recently rebalanced hosts into recommendations for Start-On Placement, Resume, and Maintenance Mode.

5.1.1.4.1.2. Recommendation Count

Every two minutes, Workload Balancing checks to see if it can generate recommendations for the pool it is monitoring. When you enable Automation, you can specify the number of times a consistent recommendation must be made before Workload Balancing can automatically apply the recommendation. To do so, you configure a setting known as the *Recommendation Count*. The Recommendation Count and the Optimization Aggressiveness setting let you fine-tune the automated application of recommendations in your environment.

As described in the aggressiveness section, Workload Balancing uses the similarity of recommendations to a) vet if the recommendation is truly needed and b) determine if the destination host has stable enough performance over a prolonged period of time to accept a relocated VM (without needing to move it off the host again shortly). Workload Balancing uses the Recommendation Count value to determine a recommendation must be repeated before Workload Balancing automatically applies the recommendation.

Workload Balancing uses this setting as follows:

1. Every time Workload Balancing generates a recommendation that meets its consistency requirements, as indicated by the Optimization Aggressiveness setting, Workload Balancing increments the Recommendation Count. If the recommendation does not meet the consistency requirements, Workload Balancing may reset the Recommendation Count to zero, depending on the factors described in [Section 5.1.1.4.1.4, "Optimization Aggressiveness"](#).
2. When Workload Balancing generates enough consistent recommendations to meet the value for the Recommendation Count, as specified in the **Recommendations** text box, it automatically applies the recommendation.

If you choose to modify this setting, the value you should set varies according to your environment. Consider these scenarios:

- If host loads and activity increase extremely quickly in your environment, you may want to increase value for the Recommendation Count. Workload Balancing generates recommendations every two minutes. For



example, if you set this interval to "3", then six minutes later Workload Balancing applies the recommendation automatically.

- If host loads and activity increase gradually in your environment, you may want to decrease the value for the Recommendation Count.

Accepting recommendations uses system resources and affects performance when Workload Balancing is relocating the virtual machines. Increasing the Recommendation Count increases the number of matching recommendations that must occur before Workload Balancing applies the recommendation, which encourages Workload Balancing to apply more conservative, stable recommendations and may decrease the potential for spurious VM moves. It should be noted, however, that the Recommendation Count is set to a conservative value by default.

Because of the potential impact adjusting this setting may have on your environment, Citrix only recommends changing it with extreme caution, preferably by testing and iteratively changing the value or under the guidance of Citrix Technical Support.

5.1.1.4.1.3. Recommendation Severity

All optimization recommendations include a severity rating (Critical, High, Medium, Low) that indicates the importance of the recommendation. Workload Balancing bases this rating on a combination of factors including configuration options you set, such as thresholds and metric tunings, resources available for the workload, and resource-usage history. (The severity rating for a recommendation appears in the Optimization Recommendations pane on the **WLB** tab.)

When you configure Workload Balancing to apply recommendations automatically, you can set the minimum severity level that should be associated with a recommendation before Workload Balancing automatically applies it.

5.1.1.4.1.4. Optimization Aggressiveness

To provide additional assurance when running in automated mode, Workload Balancing has consistency criteria for accepting optimizations automatically so as to prevent moving VMs due to spikes and anomalies. In automated mode, Workload Balancing does not accept the first recommendation it produces. Instead, Workload Balancing waits to automatically apply a recommendation until a host or VM exhibits *consistent behavior over time*. The phrase consistent behavior over time refers to factors such as whether a host continues to trigger recommendations and whether the same VMs on that host continue to trigger recommendations.

Workload Balancing determines if behavior is consistent by using criteria for consistency and by having criteria for the number of times the same recommendation is made (that is, the Recommendation Count). You can configure how strictly you want Workload Balancing to apply the consistency criteria using the **Optimization Aggressiveness** setting.

While Citrix primarily designed the **Optimization Aggressiveness** setting for demonstration purposes, you can use this setting to control the amount of stability you want in your environment before Workload Balancing applies an optimization recommendation. The most stable setting (**Low** aggressiveness) is configured by default. In this context, the term *stable* refers to the similarity of the recommended changes over time, as explained throughout this section. In most environments, aggressiveness is not desirable. Consequently, **Low** is the default setting.

Workload Balancing uses up to four criteria to ascertain consistency. The number of criteria that must be met varies according to the level you set in the Optimization Aggressiveness setting. The lower the level (for example, Low or Medium) the less aggressively Workload Balancing is in accepting a recommendation. In other words, Workload Balancing is stricter about requiring criteria to match (or less cavalier or aggressive) about consistency when aggressiveness is set to Low.

For example, if the aggressiveness level is set to **Low**, Workload Balancing requires that each criterion for **Low** is met the number of times specified in the **Recommendations** box (where you specify the Recommendation Count value) before automatically applying the recommendation.

For example, if you set the Recommendation Count in the **Recommendations** box to "3", you are making Workload Balancing wait until it sees all the criteria listed below for **Low** met and repeated in three consecutive recommendations. This helps ensure that the VM actually needs to be moved and that the destination host



Workload Balancing is recommending has consistently stable resource utilization over a longer period of time. It reduces the potential for a recently moved VM to be moved off a host due to host performance changes after the move. By default, this setting is set to a conservative setting (**Low**) to encourage stability.

Citrix does not recommend increasing the **Optimization Aggressiveness** setting to increase the frequency with which your hosts are being optimized. If you feel that your hosts are not being optimized quickly or frequently enough, try adjusting the Critical thresholds and comparing them against the Pool Health report.

The consistency criteria associated with the different levels of aggressiveness is the following:

Low

- All VMs in subsequent recommendations must be the same (as demonstrated by matching UUIDs in each recommendation).
- All destination hosts must be the same in subsequent recommendations
- The recommendation that immediately follows the initial recommendation must match or else the Recommendation Count reverts to 1

Medium

- All VMs in subsequent recommendations must be from the same host same; however, they can be different VMs from the ones in the first recommendation.
- All destination hosts must be the same in subsequent recommendations
- One of the next two recommendation that immediately follows the first recommendation must match or else the Recommendation Count reverts to 1

High

- All VMs in the recommendations must be from the same host same; however, the recommendations do not have to immediately follow each other.
- The host from which Workload Balancing recommended the VM move must be the same in each recommendation
- The Recommendation Count does not revert to 1 if the two recommendations that follow the first recommendation do not match

Example

The following example illustrates the way in which Workload Balancing uses the Optimization Aggressiveness setting and the Recommendation Count to determine whether or not to automatically accept a recommendation.

The first column represents the recommendation number. The second column, "Placement Recommendations," represents the placement recommendations made when Workload Balancing issued the optimization recommendation: each recommendation proposes three VM placements (moves). The third, fourth, and fifth columns represent the effect of the Optimization Aggressiveness setting on a group of placement recommendations (the group is denoted by the row, for example "Recommendation #1"). The number in the aggressiveness columns is the number of times there have been consecutive recommendation at that Optimization Aggressiveness setting. For example, 1 in the medium column for Recommendation #2 indicates that the recommendation was not consistent enough at that Optimization Aggressiveness setting and the counter was reset to 1.

For example, in the table below, when the Optimization Aggressiveness setting is set to High, the Recommendation Count continues to increase after Recommendation #1, #2, and #3—even though the same VMs are not recommended for new placements in each recommendation. Workload Balancing applies the placement recommendation with Recommendation #3 because it has seen the same behavior from that host for three consecutive recommendations.

In contrast, when set to Low aggressiveness, the consecutive recommendations count does not increase for the first four recommendations. In fact, the Recommendation Count resets to 1 with each recommendation because



the same VMs were not recommended for placements. The Recommendation Count does not start to increase until the same recommendation is made in Recommendation #5. Finally, Workload Balancing automatically applies the recommendation made in Recommendation #6 after the third time it issues the same placement recommendations.

	Placement Recommendations	High Aggressiveness Recommendation Count	Medium Aggressiveness Recommendation Count	Low Aggressiveness Recommendation Count
Recommendation #1	<ul style="list-style-type: none"> Move VM1 from Host A to Host B Move VM3 from Host A to Host B Move VM5 from Host A to Host C 	1	1	1
Recommendation #2	<ul style="list-style-type: none"> Move VM1 from Host A to Host B Move VM3 from Host A to Host C Move VM7 from Host A to Host C 	2	1	1
Recommendation #3	<ul style="list-style-type: none"> Move VM1 from Host A to Host B Move VM3 from Host A to Host C Move VM5 from Host A to Host C 	3 (Apply)	1	1
Recommendation #4	<ul style="list-style-type: none"> Move VM1 from Host A to Host B Move VM3 from Host A to Host B Move VM5 from Host A to Host C 		2	1
Recommendation #5	<ul style="list-style-type: none"> Move VM1 from Host A to Host B Move VM3 from Host A to Host B Move VM5 from Host A to Host C 		3 (Apply)	2
Recommendation #6	<ul style="list-style-type: none"> Move VM1 from Host A to Host B Move VM3 from Host A to Host B Move VM5 from Host A to Host C 			3 (Apply)

To configure VM Recommendation intervals

1. In the **Resources** pane of XenCenter, select XenCenter>your-pool.
2. In the **Properties** pane, click the **WLB** tab.
3. In the **WLB** tab, click **Settings**.
4. In the left pane, click **Advanced**.
5. In the **VM Recommendation Interval** section, do one or more of the following:
 - In the **Minutes** box, type a value for the number of minutes you want Workload Balancing to wait before making another optimization recommendation on a newly rebalanced host.
 - In the **Recommendations** box, type a value for the number of recommendations you want Workload Balancing to make before it applies a recommendation automatically.
 - Select a minimum severity level before optimizations are applied automatically.
 - Modify how aggressively Workload Balancing applies optimization recommendations when it is running in automated mode. Increasing the aggressiveness level reduces constraints on the consistency of



recommendations before automatically applying them. The Optimization Aggressiveness setting directly complements the Recommendation Count setting (that is, the **Recommendations** box).

Note:

If you type "1" for the value in the **Recommendations** setting, the Optimization Aggressiveness setting is not relevant.

5.2. To Modify the Pool Audit Trail Granularity Setting

Follow this procedure to modify the granularity settings:

1. Select the pool in the **Infrastructure** view, click the **WLB** tab, and then click **Settings**.
2. In the left pane, click **Advanced**.
3. On the Advance page, click the **Pool Audit Trail Report Granularity** drop-down list, and select an option from the list.

Important:

Select the granularity based on the your audit log requirements. For example, if you set your audit log report granularity to Minimum, the audit report only captures limited amount of data for specific users and object types. If you set the granularity to Medium, the report provides a user-friendly report of the audit log. If you choose to set the granularity to Maximum, the report will contain detailed information about the audit log report. Setting the audit log report to Maximum can cause the Workload Balancing server to use more disk space and memory.

4. To confirm your changes, click **OK**.

5.3. To View Audit Trail Reports Based on Objects Using XenCenter

Follow this procedure to run and view reports of Pool Audit Trail based on the selected object:

1. After you have set the Pool Audit Trail Granularity setting, click **Reports**. The **Workload Reports** page appears.
2. Select **Pool Audit Trail** on the left pane.
3. You can run and view the reports based on a specific Object by choosing it from the **Object** drop-down list. For example, choose **Host** from the drop-down list to get the reports based on Host alone.

Chapter 6. Administering Workload Balancing

This chapter provides information about the following topics:

- How to reconfigure a pool to use a different Workload Balancing virtual appliance
- How to disconnect a pool from Workload Balancing or temporarily stop Workload Balancing
- Database grooming
- How to change configuration options

Note:

Workload Balancing is available for XenServer Enterprise Edition customers or those who have access to XenServer through their XenDesktop entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website [here](#). For detailed information on Licensing - refer to [CTX141511 - XenServer 6.5 Licensing FAQ](#).

6.1. Administering and Maintaining Workload Balancing

After Workload Balancing has been up and running for a while, there are routine tasks that you may need to perform in order to keep Workload Balancing running optimally. These tasks may arise either as the result of changes to your environment (such as different IP addresses or credentials), hardware upgrades, or routine maintenance.

Some administrative tasks you may want to perform on Workload Balancing include:

- Connecting or reconnecting a pool to a Workload Balancing virtual appliance
- Reconfiguring a pool to use another Workload Balancing virtual appliance
- Renaming the Workload Balancing user account
- Disconnecting the Workload Balancing virtual appliance from a pool
- Removing the Workload Balancing virtual appliance
- Understanding the Role Based Access Control permissions Workload Balancing requires

Workload Balancing lets you fine-tune some aspects of its behavior through a configuration file known as the `wlb.conf` file.

This section also discusses some database administration tasks for those interested in additional ways to manage the Workload Balancing database.

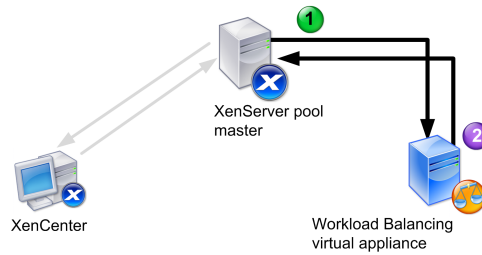
6.1.1. Connecting to the Workload Balancing Virtual Appliance

After Workload Balancing configuration, you must connect the pool you want managed to the Workload Balancing virtual appliance using either the XE commands or the **Connect to WLB Server** dialog box in XenCenter. Likewise, you might need to reconnect to the same virtual appliance at some point.

To complete the XenCenter procedure that follows, you need the:

- Host name (or IP address) and port of the Workload Balancing virtual appliance.
- Credentials for the resource pool you want Workload Balancing to monitor.

- Credentials for the account you created on the Workload Balancing virtual appliance. This is often known as the Workload Balancing user account. XenServer uses this account to communicate with Workload Balancing. You created this account on the Workload Balancing virtual appliance during Workload Balancing Configuration.



This illustration shows how (1) XenServer communicates with Workload Balancing using an account you created during Workload Balancing Configuration and (2) the Workload Balancing virtual appliance authenticates to XenServer using the credentials for the pool.

If you want to specify the Workload Balancing virtual appliance's host name for use when connecting to the Workload Balancing virtual appliance (that is, in the **Connect to WLB Server** dialog), you must first add its host name and IP address to your DNS server.

If you want to configure certificates from a certificate authority, Citrix recommends specifying an FQDN or an IP address that does not expire.

When you first connect to Workload Balancing, it uses the default thresholds and settings for balancing workloads. Automatic features, such as Automated Optimization Mode, Power Management, and Automation, are disabled by default.

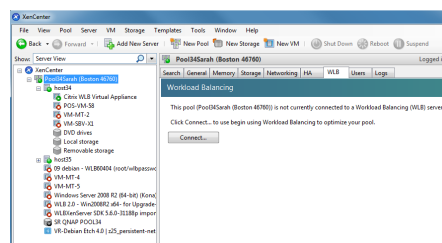
Note:

Workload Balancing is available for XenServer Enterprise Edition customers or those who have access to XenServer through their XenDesktop entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website [here](#). For detailed information on Licensing - refer to [CTX141511 - XenServer 6.5 Licensing FAQ](#).

6.1.1.1. To connect your pool to the Workload Balancing virtual appliance

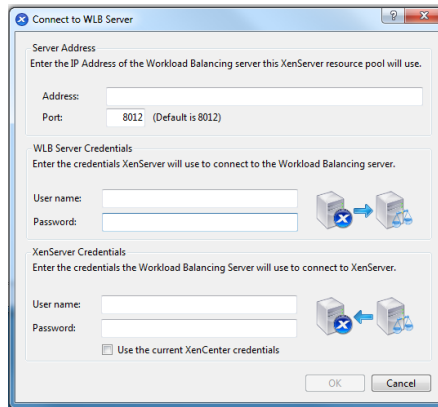
1. In the **Resources** pane of XenCenter, select XenCenter > your-resource-pool.
2. In the **Properties** pane, click the **WLB** tab.

The **WLB** tab displays the **Connect** button.



3. In the **WLB** tab, click **Connect**.

The **Connect to WLB Server** dialog box appears.



4. In the **Server Address** section, enter the following:
 - a. In the **Address** box, type the IP address or FQDN of the Workload Balancing virtual appliance (for example, your WLB-appliance-computername.yourdomain.net).

Tip:

To obtain the IP address for the WLB virtual appliance, see [Section 6.1.1.2, “To obtain the IP address for the WLB virtual appliance”](#).

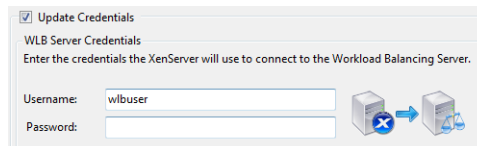
- b. Enter the port number in the **Port** box. XenServer uses this port to communicate with Workload Balancing.

By default, XenServer connects to Workload Balancing (specifically the Web Service Host service) on port 8012. If you changed the port number during Workload Balancing Configuration, you must enter that port number here.

Note:

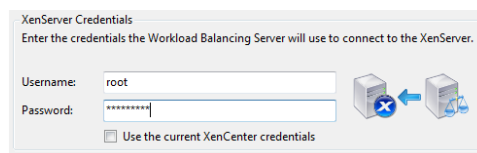
Use the default port number unless you changed it during Workload Balancing Configuration. The port number specified during Workload Balancing Configuration, in any firewall rules, and in the **Connect to WLB Server** dialog must match.

5. In the **WLB Server Credentials** section, enter the user name (for example, wlbuser) and password the XenServer pool will use to connect to the Workload Balancing virtual appliance.



This must be the account you created during Workload Balancing Configuration. By default, the user name for this account is wlbuser.

6. In the **XenServer Credentials** section, enter the user name and password for the pool you are configuring. Workload Balancing will use these credentials to connect to the XenServer hosts in that pool.



To use the credentials with which you are currently logged into XenServer, select the **Use the current XenCenter credentials** check box. If you have assigned a role to this account using the Access Control feature (RBAC), be sure the role has sufficient permissions to configure Workload Balancing. For more information, see [Section 6.1.1.3, “Workload Balancing Access Control Permissions”](#).

7. After connecting the pool to the Workload Balancing virtual appliance, Workload Balancing automatically begins monitoring the pool with the default optimization settings. If you want to modify these settings or



change the priority given to specific resources, wait at least sixty seconds (until the XenCenter Log shows discovery is finished) before proceeding and see [Section 5.1, "Changing Workload Balancing Settings"](#).

6.1.1.2. To obtain the IP address for the WLB virtual appliance

1. Select the WLB virtual appliance in the Resource pane in XenCenter, and click on the **Console** tab.
2. Log in to the appliance. Enter the VM user name (typically "root") and the root password you created when you imported the appliance.
3. Enter the following command at the prompt:

```
ifconfig
```

6.1.1.3. Workload Balancing Access Control Permissions

When Role Based Access Control (RBAC) is implemented in your environment, all user roles can display the WLB tab. However, not all roles can perform all operations. The following table lists the *minimum* role administrators require to use Workload Balancing features:

Task	Minimum Required Role
Configure, Initialize, Enable, Disable WLB	Pool Operator
Apply WLB Optimization Recommendations (in WLB tab)	Pool Operator
Modify WLB report subscriptions	Pool Operator
Accept WLB Placement Recommendations ("star" recommendations)	VM Power Admin
Generate WLB Reports, including the Pool Audit Trail report	Read Only
Display WLB Configuration	Read Only

Definition of Permissions

The following table provides additional details about permissions.

Permission	Allows Assignee To
Configure, Initialize, Enable, Disable WLB	<ul style="list-style-type: none">• Configure WLB• Initialize WLB and change WLB servers• Enable WLB• Disable WLB
Apply WLB Optimization Recommendations (in WLB tab)	<ul style="list-style-type: none">• Apply any optimization recommendations that appear in the WLB tab
Modify WLB report subscriptions	<ul style="list-style-type: none">• Change the WLB report generated or its recipient
Accept WLB Placement Recommendations ("star" recommendations)	<ul style="list-style-type: none">• Select one of the servers Workload Balancing recommends for placement ("star" recommendations)
Generate WLB Reports, including the Pool Audit Trail report	<ul style="list-style-type: none">• View and run WLB reports, including the Pool Audit Trail report

Permission	Allows Assignee To
Display WLB Configuration	<ul style="list-style-type: none"> View WLB settings for a pool as shown on the WLB tab

If a user tries to use Workload Balancing and he or she does not have sufficient permissions, a role elevation dialog appears. For more information about RBAC, see the *XenServer Administrator's Guide*.

6.1.2. Determining the Status of the Workload Balancing Virtual Appliance

Run the `service workloadbalancing status` command, as described in the [Chapter 8, Appendix B: Workload Balancing Commands](#).

6.1.3. Reconfiguring a Pool to Use Another WLB Appliance

You can reconfigure a resource pool to use a different Workload Balancing virtual appliance.

However, to prevent the old Workload Balancing virtual appliance from remaining inadvertently configured and running against a pool, you must disconnect the pool from the old Workload Balancing virtual appliance before connecting the pool to the new (or different) Workload Balancing virtual appliance.

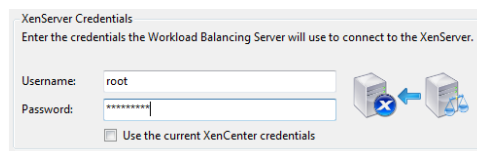
After disconnecting a pool from the old Workload Balancing virtual appliance, you can connect the pool by specifying the name of the new Workload Balancing virtual appliance. Perform the steps in the procedure that follows on the pool you want to connect to a different Workload Balancing virtual appliance.

To use a different Workload Balancing virtual appliance

1. From the **Pool** menu, select **Disconnect Workload Balancing Server** and click **Disconnect** when prompted.
2. In the **WLB** tab, click **Connect**. The **Connect to WLB Server** dialog appears.
3. In the **Address** box, type the IP address or FQDN of the new Workload Balancing server.
4. In the **WLB Server Credentials** section, enter the user name (for example, **wlbuser**) and password the XenServer pool (master) will use to connect to the Workload Balancing virtual appliance.

This must be the account you created during Workload Balancing Configuration for the new virtual appliance. By default, the user name for this account is **wlbuser**.

5. In the **XenServer Credentials** section, enter the user name and password for the pool you are configuring (typically the password for the pool master). Workload Balancing will use these credentials to connect to the hosts in the pool.



To use the credentials with which you are currently logged into XenServer, select the **Use the current XenCenter credentials** check box. If you have assigned a role to this account using the Access Control feature (RBAC), be sure the role has sufficient permissions to configure Workload Balancing. For more information, see [Section 6.1.1.3, “Workload Balancing Access Control Permissions”](#).

6.1.4. Updating Workload Balancing Credentials

Situations when you may want to update the Workload Balancing credentials include if you need to change the name of the user account XenServer uses to communicate with Workload Balancing.



After initial configuration, if you need to update the credentials XenServer and the Workload Balancing appliance use to communicate, you can do so using a three-step process:

1. Pause Workload Balancing by clicking **Pause** in the **WLB** tab.
2. Change the WLB credentials by running the `wlbconfig` command. For more information, see [Chapter 8, Appendix B: Workload Balancing Commands](#).
3. Re-enable Workload Balancing and specify the new credentials, as described in [To re-enable Workload Balancing and specify the new credentials](#).

To re-enable Workload Balancing and specify the new credentials

1. After the progress bar completes, click **Connect**.

The Connect to WLB Server dialog box appears.

2. Click **Update Credentials**.
3. In the **Server Address** section, modify the following as desired:
 - In the **Address** box, type the IP address or FQDN of the Workload Balancing appliance.
 - (Optional.) If you changed the port number during Workload Balancing Configuration, enter that port number. The port number you specify in this box and during Workload Balancing Configuration is the port number XenServer uses to connect to Workload Balancing.

By default, XenServer connects to Workload Balancing on port 8012.

Note:

Do not edit this port number unless you have changed it when you ran the Workload Balancing Configuration wizard. The port number value specified when you ran the Workload Balancing Configuration wizard and the **Connect to WLB Server** dialog must match.

4. In the **WLB Server Credentials** section, enter the user name (for example, `wlbuser`) and password the computers running XenServer will use to connect to the Workload Balancing server.
5. In the **XenServer Credentials** section, enter the user name and password for the pool you are configuring (typically the password for the pool master). Workload Balancing will use these credentials to connect to the computers running XenServer in that pool.
6. In the XenServer Credentials section, enter the user name and password for the pool you are configuring. Workload Balancing will use these credentials to connect to the computers running XenServer in that pool.

To use the credentials with which you are currently logged into XenServer, select the **Use the current XenCenter credentials** check box.

6.1.5. Changing the Workload Balancing IP Address

Situations when you may want to update the

To change the Workload Balancing IP address, do the following:

1. Stop the Workload Balancing services by running the `service workloadbalancing stop` command on the virtual appliance.
2. Change the Workload Balancing IP address by running the `ifconfig` command on the virtual appliance.
3. Re-enable Workload Balancing and specify the new IP address, as described in [To re-enable Workload Balancing and specify the new credentials](#).
4. Start the Workload Balancing services by running the `service workloadbalancing start` command on the virtual appliance.

6.1.6. Stopping Workload Balancing

Because Workload Balancing is configured at the pool level, when you want it to stop managing a pool, you must do one of the following:

- **Pause Workload Balancing.** Pausing Workload Balancing stops XenCenter from displaying recommendations for the specified resource pool and managing the pool. Pausing is designed for a short period of time and lets you resume monitoring without having to reconfigure. When you pause Workload Balancing, data collection stops for that resource pool until you enable Workload Balancing again.
- **Disconnect the pool from Workload Balancing.** Disconnecting from the Workload Balancing virtual appliance breaks the connection between the pool and if possible, deletes the pool data from the Workload Balancing database. When you disconnect from Workload Balancing, Workload Balancing stops collecting data on the pool.

To pause Workload Balancing temporarily

1. In the **Resource** pane of XenCenter, select the resource pool for which you want to disable Workload Balancing.
2. In the **WLB** tab, click **Pause**. A message appears on the **WLB** tab indicating that Workload Balancing is currently paused.

Tip:

To resume monitoring, click the **Resume** button in the **WLB** tab.

To disconnect a pool from Workload Balancing

1. In the **Infrastructure** pane of XenCenter, select the resource pool on which you want to stop Workload Balancing.
2. From the **Infrastructure** menu, select **Disconnect Workload Balancing Server**. The **Disconnect Workload Balancing** dialog box appears.
3. Click **Disconnect** to permanently stop Workload Balancing from monitoring the pool.

Tip:

If you disconnected the pool from the Workload Balancing virtual appliance, to re-enable Workload Balancing on that pool, you must reconnect to a Workload Balancing appliance. For information, see the [Section 6.1.1, “Connecting to the Workload Balancing Virtual Appliance”](#).

6.1.7. Entering Maintenance Mode with Workload Balancing Enabled

When Workload Balancing is enabled, if you take a physical host off-line for maintenance (that is, suspend a host by entering Maintenance Mode), XenServer automatically migrates the virtual machines running on that host to their optimal hosts when available. XenServer migrates them based on Workload Balancing recommendations (performance data, your placement strategy, and performance thresholds).

If an optimal host is not available, the words **Click here to suspend the VM** appear in the **Enter Maintenance Mode** dialog box. In this case, because there is not a host with sufficient resources to run the virtual machine, Workload Balancing does not recommend a placement. You can either suspend this virtual machine or exit Maintenance Mode and suspend a virtual machine on another host in the same pool. Then, if you reenter the **Enter Maintenance Mode** dialog box, Workload Balancing might be able to list a host that is a suitable candidate for migration.

Note:



When you take a host off-line for maintenance and Workload Balancing is enabled, the words "Workload Balancing" appear in the upper-right corner of the **Enter Maintenance Mode** dialog box.

6.1.7.1. To enter maintenance mode with Workload Balancing enabled

1. In the **Resources** pane of XenCenter, select the physical host that you want to take off-line. From the **Server** menu, select **Enter Maintenance Mode**.
2. In the **Enter Maintenance Mode** dialog box, click **Enter maintenance mode**. The virtual machines running on the host are automatically migrated to the optimal host based on the Workload Balancing performance data, your placement strategy, and performance thresholds.

To take the host out of maintenance mode, right-click the host and select **Exit Maintenance Mode**. When you remove a host from maintenance mode, XenServer automatically restores that host's original virtual machines to that host.

6.1.8. Increasing the Workload Balancing Disk Size

This procedure explains how to resize the virtual disk of the Workload Balancing virtual appliance. You must shut down the virtual appliance before performing these steps. Consequently, Workload Balancing will be unavailable for approximately five minutes.

Warning:

Citrix recommends taking a snapshot of your data before performing this procedure. Incorrectly performing these steps can result in corrupting the Workload Balancing virtual appliance.

To extend the size of the Workload Balancing virtual-appliance disk

1. Shut down the Workload Balancing virtual appliance.
2. In the XenCenter resource pane, select the Workload Balancing virtual appliance (typically "Citrix WLB Virtual Appliance").
3. Click the **Storage** tab.
4. Select the "vdi_xvda" disk, and click the **Properties** button.
5. In the "vdi_xvda" **Properties** dialog, select **Size** and **Location**.
6. Increase the disk size as needed, and click **OK**.
7. Start the Workload Balancing virtual appliance and log in to it.
8. Run the following command on the Workload Balancing virtual appliance:

```
resize2fs /dev/xvda
```

9. Run the **df -h** command to confirm the new disk size.

6.1.9. Removing the Workload Balancing Virtual Appliance

Citrix recommends removing the Workload Balancing virtual appliance by using the standard procedure to delete virtual machines from XenCenter.

When you delete the Workload Balancing virtual appliance, the PostgreSQL database containing the Workload Balancing is deleted. To save this data, you must migrate it from the database before deleting the Workload Balancing virtual appliance.

6.1.10. Managing the Workload Balancing Database

The Workload Balancing database is a PostgreSQL database. PostgreSQL is an open-source enterprise-class relational database. You can find documentation for PostgreSQL by searching the web.



The following information is intended for database administrators and advanced users of PostgreSQL who are comfortable with database administration tasks. If you are not experienced with PostgreSQL, Citrix recommends that you become familiar with it before you attempt the database tasks in the sections that follow.

By default, the PostgreSQL user name is **postgres**. You set the password for this account during Workload Balancing Configuration.

The amount of historical data you can store is based on the size of the virtual disk allocated to Workload Balancing (by default 8GB) and the minimum required space, which is discussed in [Section 6.1.10.2.1, “Database Grooming Parameters”](#).

If you want to store a lot of historical data, for example if you want to enable the Pool Audit trail Report, you can do either of the following:

- Make the virtual disk size assigned to the Workload Balancing virtual appliance larger. To do so, import the virtual appliance, and increase the size of the virtual disk by following the steps in [Section 6.1.8, “Increasing the Workload Balancing Disk Size”](#).
- Create periodic duplicate back-up copies of the data by enabling remote client access to the database and using a third-party database administration tool, such as pgAdmin.

In terms of managing the database, you can control the space that database data consumes by configuring database grooming.

6.1.10.1. Accessing the Database

The Workload Balancing 6.5 virtual appliance has firewall configured in it. Before you can access database, you must add the postgresql server port to the iptables.

To open the database port in the firewall

1. From the Workload Balancing virtual appliance console, run the following command:

```
iptables -A INPUT -i eth0 -p tcp -m tcp --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

2. (Optional.) To make this configuration persist after the virtual appliance is rebooted, run the following command:

```
iptables-save > /etc/sysconfig/potables
```

6.1.10.2. Controlling Database Grooming

The Workload Balancing database is set up to automatically delete the oldest data whenever the VPX reaches the minimum amount of disk space Workload Balancing requires to run. By default, the minimum amount of required disk space is set to 1024MB.

The Workload Balancing database grooming options are controlled through the wlb.conf file.

When there is not enough disk space left on the Workload Balancing virtual appliance, Workload Balancing automatically starts grooming historical data. The process is as follows:

1. At a predefined grooming interval, the Workload Balancing data collector checks if grooming is required. Grooming is required if the database data has grown to the point where the only space that remains unused is the minimum required disk space (which is set by **GroomingRequiredMinimumDiskSizeInMB**). (You can change the grooming interval if desired using **GroomingIntervalInHour**. However, by default Workload Balancing checks to see if grooming is required once per hour.)
2. If grooming is required, Workload Balancing begins by grooming the data from the oldest day. Workload Balancing then checks to see if there is now enough disk space for it to meet the minimum disk-space requirement.
3. If the first grooming did not free enough disk space, then Workload Balancing repeats grooming up to **GroomingRetryCounter** times without waiting for **GroomingIntervalInHour** hour.

4. If the first or repeated grooming freed enough disk space, then Workload Balancing waits for **GroomingIntervallnHour** hour and returns to Step 1.
5. If the grooming initiated by the **GroomingRetryCounter** did not free enough disk space, then Workload Balancing waits for **GroomingIntervallnHour** hour and returns to Step 1.

6.1.10.2.1. Database Grooming Parameters

There are five parameters in the `wlb.conf` file that control various aspects of database grooming. They are as follows:

- **GroomingIntervallnHour**. Controls how many hours elapse before the next grooming check is done. For example, if you enter "1", Workload Balancing checks the disk space hourly. If you enter "2", Workload Balancing checks disk space every two hours to determine if grooming needs to occur.
- **GroomingRetryCounter**. Controls the number of times Workload balancing tries rerunning the grooming database query.
- **GroomingDBDataTrimDays**. Controls the number of days worth of data Workload Balancing will delete from the database each time it tries to groom data. The default value is one day.
- **GroomingDBTimeoutInMinute**. Controls the number of minutes that the database grooming will take before it times out and is canceled. If the grooming query takes longer than is expected and does not finish running within the timeout period, the grooming task is canceled. The default value is 0 minutes, which means that database grooming never times out.
- **GroomingRequiredMinimumDiskSizeInMB**. Controls the minimum amount of free space left in the virtual disk assigned to the Workload Balancing virtual appliance. When the data in the virtual disk grows to the point where there is only minimum disk size left on the virtual disk, Workload Balancing begins to trigger database grooming. The default value is 2048MB.

To edit these values, see the [Section 8.1.7, "Editing the Workload Balancing Configuration File"](#).

6.1.10.3. Changing the Database Password

While it is possible to change the database password by using the `wlb.conf` file, Citrix recommends running the `wlbconfig` command instead, as described in [Section 8.1.6, "Modifying the Workload Balancing Configuration Options"](#).

6.1.10.4. Archiving Database Data

To avoid having older historical data deleted, you can, optionally, copy data from the database for archiving. To do so, you must perform the following tasks:

1. Enable client authentication on the database.
2. Set up archiving using the PostgreSQL database administration tool of your choice.

6.1.10.4.1. Enabling client authentication to the database

While you can connect directly to the database through the Workload Balancing console, you can also use a PostgreSQL database management tool, such as the free utility `pgAdmin`, which is available on the web. After downloading a database management tool, install it on the computer from which you want to connect to the database (for example, the same laptop where you run XenCenter).

Before you can enable remote client authentication to the database, you must:

1. Modify the database configuration files, including `pg_hba.conf` file and the `postgresql.conf`, to allow connections.
2. Stop the Workload Balancing services, restart the database, and then restart the Workload Balancing services.
3. In the database-management tool, configure the IP address of the database (that is, the IP address of the Workload Balancing VPX) and the database password.

6.1.10.4.2. Modifying the Database Configuration Files

To enable client authentication on the database, you must modify two files on the Workload Balancing virtual appliance: the `pg_hba.conf` file and the `postgresql.conf` file.

To edit the `pg_hba.conf` file

1. Modify the `pg_hba.conf` file. From the Workload Balancing virtual appliance console, open the `pg_hba.conf` file with an editor, such as VI. For example:

```
vi /var/lib/pgsql/9.0/data/pg_hba.conf
```

2. If your network uses IPv4, add the IP address from the connecting computer to this file. For example:

In the configuration section, enter the following under **#IPv4 local connections**:

TYPE	DATABASE	USER	CIDR-ADDRESS	METHOD
host	all	all	0.0.0.0/0	trust

Enter your IP address in the **CIDR-ADDRESS** field.

Note:

Instead of entering `0.0.0.0/0`, you can enter your IP address and replace the last three digits with `0/24`. The trailing "24" after the / defines the subnet mask and only allows connections from IP addresses within that subnet mask.

When you enter **trust** for the **Method** field, it enables the connection to authenticate without requiring a password. If you enter **password** for the **Method** field, you must supply a password when connecting to the database.

3. If your network uses IPv6, add the IP address from the connecting computer to this file. For example:

Enter the following under **#IPv6 local connections**:

TYPE	DATABASE	USER	CIDR-ADDRESS	METHOD
host	all	all	::0/0	trust

Enter the IPv6 addresses in the **CIDR-ADDRESS** field. In this example, the `::0/0` opens the database up to connections from any IPv6 addresses.

4. Save the file and quit the editor.
5. After changing any database configurations, you must restart the database to apply the changes. Run the following command:

```
service postgresql-9.0 restart
```

To edit the `postgresql.conf` file

1. Modify the `postgresql.conf` file. From the Workload Balancing virtual appliance console, open the `postgresql.conf` file with an editor, such as VI. For example:

```
vi /var/lib/pgsql/9.0/data/postgresql.conf
```

2. Edit the file so that it listens on any port and not just the local host. For example:

- a. Find the following line:

```
# listen_addresses='localhost'
```

- b. Remove the comment symbol (#) and edit the line to read as follows:

```
listen_addresses='*'
```

3. Save the file and quit the editor.
4. After changing any database configurations, you must restart the database to apply the changes. Run the following command:

```
service postgresql-9.0 restart
```

6.1.10.5. Changing the Database Maintenance Window

Workload Balancing automatically performs routine database maintenance daily at 12:05AM GMT (00:05), by default. During this maintenance window, data collection occurs but the recording of data may be delayed. However, the Workload Balancing user interface controls are available during this period and Workload Balancing still makes optimization recommendations.

Database maintenance includes releasing allocated unused disk space and re-indexing the database. Maintenance lasts for approximately 6 to 8 minutes. In larger pools, maintenance may last longer, depending on how long Workload Balancing takes to perform discovery.

Depending on your time zone, you may want to change the time when maintenance occurs. For example, in the Japan Standard Time (JST) time zone, Workload Balancing maintenance will occur at 9:05 AM (09:05), which may conflict with peak usage in some organizations. If you want to specify a seasonal time change, such as Daylight Saving Time or summer time, you must build the change into value you enter.

To change the maintenance time

1. In the Workload Balancing console, run the following command from any directory:

```
crontab -e
```

Workload Balancing displays the following:

```
05 0 * * * /opt/citrix/wlb/wlbmaintenance.sh
```

05 0 represents the default time for Workload Balancing to perform maintenance in minutes (05) and then hours (0). (The asterisks represent the day, month, and year the job will run: do not edit these fields.) **05 0** indicates database maintenance occurs at 12:05 AM, or 00:05, Greenwich Mean Time (GMT) every night. This means, for example, that if you live in New York city in the United States, by default, the maintenance would run at 7:05 PM (19:05) during winter months and 8:05 PM in summer months.

Important:

Do not edit the day, month, and year the job will run (as represented by asterisks). Database maintenance must run daily.

2. Enter the time at which you want maintenance to occur in GMT. For example, assuming that you want the maintenance to run at midnight:

If your time zone is...	UTC Offset	Value for Maintenance to Run at 12:05 AM Local Time	Value in Daylight Saving Time
Pacific Time Zone (PST) in the United States (for example, California)	UTC-08	05 8	05 7
Japan Standard Time (JST)	UTC+09	05 15	N/A

If your time zone is...	UTC Offset	Value for Maintenance to Run at 12:05 AM Local Time	Value in Daylight Saving Time
Chinese Standard Time	UTC +08	04 15	N/A

3. Save the file and quit the editor.

6.1.11. Customizing Workload Balancing

Workload Balancing provides several methods of customization:

- **Command lines for scripting.** See the commands in [Chapter 8, Appendix B: Workload Balancing Commands](#).
- **Host Power On scripting support.** You can also customize Workload Balancing (indirectly) through the Host Power On scripting. How to create a custom script for Host Power On is documented in the *XenServer Administrator's Guide*.

6.2. Upgrading Workload Balancing

Note:

Workload Balancing is available for XenServer Enterprise Edition customers or those who have access to XenServer through their XenDesktop entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website [here](#). For detailed information on Licensing - refer to [CTX141511 - XenServer 6.5 Licensing FAQ](#).

There are two ways in which you can upgrade to Workload Balancing 6.5. You can either (a) install a new appliance or (b) use Workload Balancing functionality to upgrade the existing virtual appliance.

This section provides information about upgrading to Workload Balancing 6.5 from any version of Workload Balancing since Workload Balancing 6.1. You cannot use this procedure to upgrade Workload Balancing when it is not in a virtual appliance format (for example, Workload Balancing 2.1). Using the upgrade feature lets you retain your Workload Balancing settings and historical data.

In the virtual appliance, Workload Balancing runs on the CentOS operating system. When running the Linux upgrade command **yum update**, you have the choice of upgrading (a) both Workload Balancing and CentOS, (b) Workload Balancing only, or (c) CentOS only. These choices are specified using parameters. For the XenServer 6.5 release, Citrix recommends, if possible, upgrading both Workload Balancing and CentOS.

It is easier to upgrade Workload Balancing when you have Internet access. However, it is still possible to upgrade without Internet access, as explained in the section that follows.

Perform the following procedures on the existing Workload Balancing virtual appliance you want to upgrade. You do not need to download the latest virtual appliance from Citrix.com. This procedure applies the same updates contained in the Workload Balancing 6.5 to your existing virtual appliance.

Important:

Citrix strongly recommends that you take a snapshot of the Workload Balancing virtual appliance before you upgrade. For information about creating snapshots, see the *XenCenter Help*.

Virtual Disk Space Requirements

Upgrading the virtual appliance requires at least 582k for the GNU wget package plus the size of the download package, as follows:

- Upgrading both Workload Balancing and CentOS requires at least 145 MB
- Upgrading only Workload Balancing requires at least 55MB
- Upgrading only CentOS requires at least 100MB

When to Upgrade

Citrix suggests upgrading during a time when Workload Balancing would not typically make a lot of recommendations (low activity). Workload Balancing will be off-line until after the upgrade is complete and Workload Balancing has finished discovery.

The amount of time it takes for the appliance to begin making optimization recommendations after you upgrade it depends on the size of your pool and how long it takes for Workload Balancing to finish discovery. After discovery is complete, it takes about five minutes before Workload Balancing begins making recommendations. Discovery time varies from approximately 20 minutes to discover 200 virtual machines to 40 minutes for 800 virtual machines. This time varies according to the size of the virtual machines, hardware, and other factors. You can tell discovery is finished when the star ratings become available for the Start On server feature.

Upgrades and Certificates



If you configured certificates in Workload Balancing 6.1 or Workload Balancing 6.0.1 and you are upgrading to XenServer 6.5, you do not need to perform any additional steps to retain your certificate configuration. The upgrade scripts will upgrade your certificate configuration for you.

However, if you upgrade your virtual appliance and then b) want to configure certificates for the first time, you must use the certificate-configuration instructions in the *Workload Balancing 6.1 Administrator's Guide*.

6.2.1. Upgrading Workload Balancing with Internet Access

Upgrading with the Internet requires that you download GNU wget, an HTTP retrieval utility. You also need to download a Python script that configures a repository (add-repo.py) on your virtual appliance.

To upgrade Workload Balancing in environments with Internet access

1. If you have not done so already, log in to the Workload Balancing appliance you want to upgrade as described in [Section 8.1.1, "Logging in to the Workload Balancing Virtual Appliance"](#)
2. Install GNU wget so you can retrieve the upgrade repository installation script using HTTP:

- a. From the bash prompt, run the following command:

```
yum install wget
```

- b. During installation, wget Setup asks you to accept various prompts, such as the size of the download package and the CentOS key. Type **y** when prompted.

3. When the wget installation is complete, download "add-repo" script by running the following command:

```
wget http://updates.xensource.com/XenServer/WLB/6.5/add-repo.py
```

When this command finishes running, a message appears stating the 'add-repo.py' script is saved.

4. At the bash prompt, run the following command to create the upgrade repository on the Workload Balancing appliance:

```
python add-repo.py
```

After the script finishes, the output states "Done."

5. Do one of the following to upgrade your Workload Balancing virtual appliance:

- To upgrade both CentOS and Workload Balancing, run:

```
yum update
```

- To upgrade Workload Balancing only, run:

```
yum update citrix-wlb
```

- To upgrade CentOS only, run:

```
yum update --disablerepo=citrix-wlb
```

6. After upgrading either CentOS or Workload Balancing or both, restart the Workload Balancing virtual appliance.

Note:

After upgrading CentOS, the operating-system time changes from Coordinated Universal Time (UTC) to the local time zone. One side effect of this change is that the timestamps in the Workload Balancing log file (LogFile.log) also change from UTC time to local time. If you want to change the system time back to UTC time, run the following command in the Workload Balancing virtual appliance: **rm -rf /etc/localtime**.

6.2.2. Upgrading Workload Balancing without Direct Internet Access



Before you start this procedure, you must use a computer with Internet access to download the Workload Balancing upgrade ISO files. Depending on your environment, you may need to copy the files to a USB flash drive or a shared directory. During the procedure that follows you are instructed to copy the files to the Workload Balancing virtual appliance.

Note:

To obtain the MD5 for the ISO files, see the checksums.txt in the ISO folder (<http://updates.xensource.com/XenServer/WLB/6.5/iso/checksums.txt>).

To upgrade Workload Balancing in environments without Internet access

1. Download the Workload Balancing ISO files (wlb-6.5-upgrade.iso and CentOS-5.7-upgrade.iso) from the updates website (<http://updates.xensource.com/XenServer/WLB/6.5/iso>).
2. Using a copying utility, such as WinSCP, copy both ISO files to the /tmp/ directory on the Workload Balancing virtual appliance. The ISO files require approximately 200MB of free space on the Workload Balancing virtual appliance.
3. Create a directory to mount the ISO files:

```
mkdir /media/cdrom
```

4. Upgrade Workload Balancing:

- a. Mount the wlb-6.5-upgrade.iso to the /media/cdrom directory:

```
mount -o loop /tmp/wlb-6.5-upgrade.iso /media/cdrom
```

- b. Create the upgrade repository:

```
python /media/cdrom/add-repo.py
```

- c. Run the yum upgrade utility to upgrade Workload Balancing:

```
yum update --disablerepo=* --enablerepo=citrix-wlb-media
```

- d. Unmount the Workload Balancing ISO file:

```
umount /media/cdrom
```

- e. Clean up the yum cache:

```
rm -r /var/cache/yum/
```

5. Upgrade the CentOS operating system:

- a. Mount the CentOS-5.7-upgrade.iso to the /media/cdrom directory:

```
mount -o loop /tmp/CentOS-5.7-upgrade.iso /media/cdrom
```

- b. Install the CentOS update:

```
yum update --disablerepo=* --enablerepo=citrix-centos-media
```

- c. Unmount the CentOS ISO file:

```
umount /media/cdrom
```

6. After upgrading either CentOS or Workload Balancing or both, restart the Workload Balancing virtual appliance.

Note:

After upgrading CentOS, the operating-system time changes from Coordinated Universal Time (UTC) to the local time zone. One side effect of this change is that the timestamps in the Workload Balancing log file (LogFile.log) also change from UTC time to local time. If you want to change the system time back to UTC time, run the following command in the Workload Balancing virtual appliance: **rm -rf /etc/localtime**.



6.2.3. Checking Workload Balancing and CentOS Version Numbers

- To check the Workload Balancing virtual appliance build number, run the following command on a XenServer host in a pool being monitored by that VPX:

```
xe pool-retrieve-wlb-diagnostics | grep -i " version=" | grep -i "DwmDataColSvc.exe"
```

The Workload Balancing version number appears at the top of the output.

- To check the CentOS version number, run the following command at the bash prompt of the Workload Balancing appliance:

```
cat /etc/redhat-release
```

Chapter 7. Appendix A: XenServer Workload Balancing Troubleshooting

7.1. Troubleshooting Workload Balancing

While Workload Balancing usually runs smoothly, this series of topics provides guidance in case you encounter issues.

7.1.1. General Troubleshooting Tips

- Start troubleshooting by reviewing the Workload Balancing log files (LogFile.log and wlb_install_log.log). You can find these logs in Workload Balancing virtual appliance in this location (by default):
 - /var/log/wlb
- Check the logs in the XenCenter **Logs** tab for more (different) information.
- To check the Workload Balancing virtual appliance build number, run the following command on a XenServer host in a pool being monitored by that VPX:

```
xe pool-retrieve-wlb-diagnostics | more
```

The Workload Balancing version number appears at the top of the output.

7.1.2. Error Messages

Workload Balancing displays errors on screen as dialog boxes and as error messages in the **Logs** tab in XenCenter.

If an error message appears, review the XenCenter event log for additional information. For information about the location of this log, see the *XenCenter Help*.

7.1.3. Issues Entering Workload Balancing Credentials

If you cannot successfully enter the virtual appliance user account and password while configuring the **Connect to WLB Server** dialog, try the following:

- Make sure that Workload Balancing virtual appliance imported and was configured correctly and all of its services are running. See [Section 8.1.3, “wlb start”](#).
- Check to make sure you are entering the correct credentials. The default credentials appear in the *Workload Balancing Quick Start*.
- You can enter a host name in the **Address** box, but it must be the fully qualified domain name (FQDN) of the Workload Balancing virtual appliance (and not the host name of the physical server hosting the appliance). For example, `yourcomputername.yourdomain.net`. If you are having trouble entering a computer name, try using the Workload Balancing appliance's IP address instead.
- Verify that the host is using the correct DNS server and the XenServer host can contact Workload Balancing server using its FQDN. To do this, ping the Workload Balancing appliance using its FQDN from the XenServer host. For example, enter the following in the XenServer host console:

```
ping wlb-vpx-1.mydomain.net
```

7.1.4. Issues with Firewalls

The following error appears if the Workload Balancing virtual appliance is behind a (hardware) firewall, and you did not configure the appropriate firewall settings: "There was an error connecting to the Workload Balancing



server: <pool name> Click Initialize WLB to reinitialize the connection settings." This error may also appear if the Workload Balancing appliance is otherwise unreachable.

Resolution

If the Workload Balancing virtual appliance is behind a firewall, you must open port 8012.

Likewise, the port XenServer uses to contact Workload Balancing (8012 by default), must match the port number specified when you ran the Workload Balancing Configuration wizard.

7.1.5. Losing the Connection to Workload Balancing

If, after configuring and connecting to Workload Balancing, you receive a connection error, the credentials may no longer be valid. To isolate this issue, try:

- Verifying the credentials you entered in the **Connect to WLB Server** dialog box match the credentials:
 - You created during Workload Balancing Configuration
 - On XenServer (that is, the pool master credentials)
- Verifying the IP address or FQDN for the Workload Balancing virtual appliance that you entered in the **Connect to WLB Server** dialog box is correct.
- Verifying the user name you created during Workload Balancing Configuration matches the credentials you entered in the **Connect to WLB Server** dialog box.

7.1.6. Workload Balancing Connection Errors

If you receive a connection error in the Workload Balancing Status line on the **WLB** tab, you might need to reconfigure Workload Balancing on that resource pool.

Click the **Connect** button on the **WLB** tab and reenter the server credentials.

7.1.7. Workload Balancing Stops Working

If Workload Balancing does not work (for example, it does not let you save any changes to settings, or star ratings and/or optimization recommendations do not appear), check the Workload Balancing log file for the following error message:

```
"dwmdatacolsvc.exe: Don't have a valid pool. Trying again in 10 minutes."
```

Cause

This typically occurs in pools that have one or more problematic VMs. When VMs are problematic, this may become evident as follows:

- **Windows.** The Windows VM crashes due to a stop error ("blue screen").
- **Linux.** The Linux VM may be unresponsive in the console and typically does not shut down.

Workaround

1. Force the VM to shut down. To do so, you can do one of the following on the host with the problematic VM:
 - In XenCenter, select the VM, and then from the **VM** menu, click **Force Shutdown**.
 - Run the **vm-shutdown** xe command with the **<force>** parameter set to true as described in the *XenServer Administrator's Guide*. For example:

```
xe vm-shutdown \  
force=<true> \  
uuid=<vm_uuid> \  

```



You can find the host UUID on the **General** tab for that host (in XenCenter) or by running the **host-list** `xe` command. You can find the VM UUID on the **General** tab for the VM or by running the **vm-list** `xe` command as described in the *XenServer Administrator's Guide* .

2. In the `xsconsole` of the XenServer hosting the crashed VM or in XenCenter, migrate all of the VMs to another host, then run the **xe-toolstack-restart** command.

7.1.8. Issues Changing Workload Balancing Servers

If you connect a resource pool to a different Workload Balancing server without disconnecting from Workload Balancing, both the old and new Workload Balancing server will monitor the pool.

To solve this problem, you can either shutdown and delete the old Workload Balancing virtual appliance or manually stop the Workload Balancing services (analysis, data collector and Web service) so that it will no longer monitor the pool.

Note:

Citrix does not recommend using the **pool-deconfigure-wlb** `xe` command to disconnect a pool from the Workload Balancing virtual appliance or using the **pool-initialize-wlb** `xe` command to specify a different appliance.

Chapter 8. Appendix B: Workload Balancing Commands

This appendix provides a reference for the Workload Balancing commands that you can perform from a XenServer host or console to control Workload Balancing or configure Workload Balancing settings on the XenServer host. This appendix includes `xe` commands and service commands.

8.1. Service Commands

Run the following service commands on the Workload Balancing appliance. To do so, you must log in to the Workload Balancing virtual appliance.

8.1.1. Logging in to the Workload Balancing Virtual Appliance

Before you can run any service commands or edit the `wlb.conf` file, you must log in to the Workload Balancing virtual appliance. To do so, you must enter a user name and password. Unless you created additional user accounts on the virtual appliance, log in using the root user account. You specified this account when you ran Workload Balancing Configuration wizard (before you connected your pool to Workload Balancing). You can, optionally, use the Console tab in XenCenter to log in to the appliance.

To log in to the Workload Balancing virtual appliance

1. At the `<name-of-your-WLB-VPX>` login prompt, enter the account user name. For example, where `wlb-vpx-pos-pool` is the name of your Workload Balancing appliance:

```
wlb-vpx-pos-pool login: root
```

2. At the Password prompt, enter the password for the account:

```
wlb-vpx-pos-pool login: root
```

Note:

To log off the Workload Balancing virtual appliance, simply type **logout** at the command prompt.

8.1.2. `wlb restart`

Run the **wlb restart** command from anywhere in the Workload Balancing appliance to stop and then restart the Workload Balancing Data Collection, Web Service, and Data Analysis services.

8.1.3. `wlb start`

Run the **wlb start** command from anywhere in the Workload Balancing appliance to start the Workload Balancing Data Collection, Web Service, and Data Analysis services.

8.1.4. `wlb stop`

Run the **wlb stop** command from anywhere in the Workload Balancing appliance to stop the Workload Balancing Data Collection, Web Service, and Data Analysis services.

8.1.5. `wlb status`

Run the **wlb status** command from anywhere in the Workload Balancing appliance to determine the status of the Workload Balancing server. After you execute this command, the status of the three Workload Balancing services (the Web Service, Data Collection Service, and Data Analysis Service) is displayed.

8.1.6. Modifying the Workload Balancing Configuration Options

Many Workload Balancing configurations, such as the database and web-service configuration options, are stored in the `wlb.conf` file, a configuration file on the Workload Balancing virtual appliance.

To make it easier to modify the most commonly used options, Citrix provides a command, **wlb config**. Running the **wlb config** command on the Workload Balancing virtual appliance lets you rename the Workload Balancing user account, change its password, or change the PostgreSQL password. After you execute this command, the Workload Balancing services are restarted.

To run the wlb config command

- Run the following from the command prompt:

```
wlb config
```

The screen displays a series of questions guiding you through changing your Workload Balancing user name and password and the PostgreSQL password. Follow the questions on the screen to change these items.

Important:

Double-check any values you enter in the `wlb.conf` file: Workload Balancing does not validate values in the `wlb.conf` file. Consequently, if the configuration parameters you specify are not within the required range, Workload Balancing does not generate an error log.

8.1.7. Editing the Workload Balancing Configuration File

You can modify Workload Balancing configuration options by editing the `wlb.conf` file, which is stored in `/opt/citrix/wlb` directory on the Workload Balancing virtual appliance. In general, Citrix does not recommend changing the settings in this file without guidance from Citrix; however, there are three categories of settings you can change if desired:

- **Workload Balancing account name and password.** It is easier to modify these by running the **wlb config** command.
- **Database password.** This can be modified using the `wlb.conf` file. However, Citrix recommends modifying it through the **wlb config** command since this command modifies the `wlb.conf` file and automatically updates the password in the database. If you choose to modify the `wlb.conf` file instead, you must run a query to update the database with the new password.
- **Database grooming parameters.** You can modify database grooming parameters, such as the database grooming interval, using this file by following the instructions in the database-management section of the *Workload Balancing Administrator's Guide*. However, Citrix recommends using caution if you do so.

For all other settings in the `wlb.conf` file, Citrix currently recommends leaving them at their default, unless Citrix instructed you to modify them.

To edit the wlb.conf file

1. Run the following from the command prompt on the Workload Balancing virtual appliance (using VI as an example):

```
vi /opt/citrix/wlb/wlb.conf
```

The screen displays several different sections of configuration options.

2. Modify the configuration options, and exit the editor.

You do not need to restart Workload Balancing services after editing the `wlb.conf` file. The changes go into effect immediately after exiting the editor.

Important:



Double-check any values you enter in the `wlb.conf` file: Workload Balancing does not validate values in the `wlb.conf` file. Consequently, if the configuration parameters you specify are not within the required range, Workload Balancing does not generate an error log.

8.1.8. Increasing the Detail in the Workload Balancing Log

The Workload Balancing log provides a list of events on the Workload Balancing virtual appliance, including actions for the analysis engine, database, and audit log. This log file is found in this location: `/var/log/wlb/LogFile.log`.

You can, if desired, increase the level of detail the Workload Balancing log provides. To do so, modify the Trace flags section of the Workload Balancing configuration file (`wlb.conf`), which is found in the following location: `/opt/citrix/wlb/wlb.conf`. Enter a **1** or **true** to enable logging for a specific trace and a **0** or **false** to disable logging. For example, to enable logging for the Analysis Engine trace, enter:

```
AnalEngTrace=1
```

You may want to increase logging detail before reporting an issue to Citrix Technical Support or when troubleshooting.

Logging Option	Trace Flag	Benefit or Purpose
Analysis Engine Trace	AnalEngTrace	Logs details of the analysis engine calculations. Shows details of the decisions the analysis engine is making and potentially gain insight into the reasons Workload Balancing is not making recommendations.
Database Trace	DatabaseTrace	Logs details about database reads/writes. However, leaving this trace on will increase the log file size quickly.
Data Collection Trace	DataCollectionTrace	Logs the actions of retrieving metrics. This lets you see the metrics Workload Balancing is retrieving and inserting into the Workload Balancing data store. However, leaving this trace on will increase the log file size quickly.
Data Compaction Trace	DataCompactionTrace	Logs details about how many milliseconds it took to compact the metric data.
Data Event Trace	DataEventTrace	This trace provides details about events Workload Balancing catches from XenServer.
Data Grooming Trace	DataGroomingTrace	This trace provides details about the database grooming.
Data Metrics Trace	DataMetricsTrace	Logs details about the parsing of metric data. Leaving this trace on will increase the log-file size quickly.
Queue Management Trace	QueueManagementTrace	Logs details about data collection queue management processing. (This is for internal use.)

Logging Option	Trace Flag	Benefit or Purpose
Data Save Trace	DataSaveTrace	Logs details about the pool being saved to the database.
Score Host Trace	ScoreHostTrace	<p>Logs details about how Workload Balancing is arriving at a score for a host.</p> <p>This trace shows the detailed scores generated by Workload Balancing when it calculates the star ratings for selecting optimal servers for VM placement.</p>
Audit Log Trace	AuditLogTrace	<p>Shows the action of the audit log data being captured and written.</p> <p>(This is generally only for internal use and does not provide information that is captured in the audit log.)</p> <p>However, leaving this trace on will increase the log file size quickly.</p>
Scheduled Task Trace	ScheduledTaskTrace	<p>Logs details about scheduled tasks.</p> <p>For example, if your scheduled mode changes are not working, you might want to enable this trace to investigate the cause.</p>
Web Service Trace	WlbWebServiceTrace	Logs details about the communication with the web-service interface.

8.2. Workload Balancing XE Commands

Commands for controlling the Workload Balancing feature.

8.2.1. pool-initialize-wlb

```
pool-initialize-wlb wlb_url=<wlb_server_address> \
wlb_username=<wlb_server_username> \
wlb_password=<wlb_server_password> \
xenserver_username=<pool_master_username> \
xenserver_password=<pool_master_password>
```

Initializes the connection between the Workload Balancing server and the XenServer pool.

Note:

Initializing a pool requires running two commands. After executing the **pool-initialize-wlb** command, execute **xe pool-param-set wlb-enabled=true uuid=<pool-uuid>[]**.

8.2.2. pool-param-set other-config

Use the **pool-param-set other-config** command to specify the timeout when communicating with the Workload Balancing server. All requests are serialized, and the timeout covers the time from a request being queued to its response being completed. In other words, slow calls cause subsequent ones to be slow. Defaults to 30 seconds if unspecified or if the setting cannot be parsed.

```
xe pool-param-set other-config:wlb_timeout=<85> \
uuid=<315688af-5741-cc4d-9046-3b9cea716f69>
```



8.2.3. pool-retrieve-wlb-diagnostics

Use the **pool-retrieve-wlb-diagnostics** command to return the contents of the Workload Balancing Log file for the Workload Balancing server that the pool is currently using. This command also returns some version information.

```
xe pool-retrieve-wlb-diagnostics \
```

8.2.4. host-retrieve-wlb-evacuate-recommendations

```
host-retrieve-wlb-evacuate-recommendations uuid=<host_uuid>
```

Returns the evacuation recommendations for a host, and a reference to the UUID of the recommendations object.

8.2.5. vm-retrieve-wlb-recommendations

Returns the workload balancing recommendations for the selected VM. The simplest way to select the VM on which the operation is to be performed is by supplying the argument `vm=<name_or_uuid>`. VMs can also be specified by filtering the full list of VMs on the values of fields. For example, specifying `power-state=halted` selects all VMs whose power-state is halted. Where multiple VMs are matching, specify the option `--multiple` to perform the operation. The full list of fields that can be matched can be obtained by the command **xe vm-list params=all**. If no parameters to select VMs are given, the operation will be performed on all VMs.

8.2.6. pool-certificate-list

XenServer Workload Balancing component lets you use certificates to secure communication between XenServer pools and the Workload Balancing server. You can either use the default test certificate, which is created automatically during Workload Balancing configuration, or you can specify a certificate from a Trusted Authority.

To use a Trusted Authority certificate, the certificate must be in X.509 format and comply with the guidelines provided earlier in the *Workload Balancing Administrator's Guide*. If you want to verify the presence of a certificate from a Trusted Authority, you must:

```
pool-certificate-list
```

Lists all installed SSL certificates.

8.2.7. pool-certificate-install

```
pool-certificate-install filename=<certificatefilename>
```

Run this command on the pool to install the certificate on the Workload Balancing virtual appliance on the pool master.

8.2.8. pool-certificate-sync

```
pool-certificate-sync
```

Run this command on the pool, after running the `pool-certificate-install` command, to make sure the certificate and certificate revocation lists are synchronized from the pool master to all slaves on the pool.

8.2.9. pool-param-set

```
pool-param-set wlb-verify-cert=<true> uuid=<uuid_of_pool>
```

Run this command on the pool, after running the `pool-certificate-sync` command, to make XenServer always verify the certificate when communicating with the Workload Balancing server.

Tip:

Pressing the **Tab** key automatically populates the UUID of the pool.



8.2.10. pool-deconfigure-wlb

Permanently deletes all workload balancing configuration.

8.2.11. pool-retrieve-wlb-configuration

Prints all Workload Balancing configuration information to standard out.

8.2.12. pool-retrieve-wlb-recommendations

Prints all Workload Balancing recommendations to standard out.

8.2.13. pool-retrieve-wlb-report

Gets a Workload Balancing report of the specified type and saves it to the specified file. XenCenter uses this command when executing Workload Balancing reports. However, running this command from the CLI does not output report data in a graphical format. Outputting reports requires using the XenCenter **Pool > View Workload Reports** menu command. The available reports are:

- pool_health
- host_health_history
- optimization_performance_history
- pool_optimization_history
- pool_health_history
- vm_chargeback_history
- pool_audit_history
- vm_movement_history
- vm_performance_history

Example usage for each report type is shown below. The *utcoffset* parameter specifies the number of hours the pool's time zone is ahead or behind Coordinated Universal Time (UTC). For example, *<-5>* represents the Eastern Standard Time zone in North America, which is five hours behind UTC. The *start* parameter and *end* parameters specify the number of hours to report. For example specifying *start=-3* and *end=0* will cause Workload Balancing to report on the last three hours of activity. *LocaleCode* represents the language for the report output. You can enter either *<en>* for English or *<ja>* for Japanese.

```
xe pool-retrieve-wlb-report report=pool_health \  
LocaleCode=<en> \  
Start=<-3> \  
End=<0> \  
PoolID=<c75f9ee9-422f-9cde-4781-24f6cbd9279c> \  
UTCOffset=<-5> \  
filename=/<pool_health>.txt \  

```

```
xe pool-retrieve-wlb-report report=host_health_history \  
Start=<-3> \  
End=<0> \  
PoolID=<c75f9ee9-422f-9cde-4781-24f6cbd9279c> \  
HostID=<471626e5-8e8b-429b-9990-6013726d7e86> \  
UTCOffset=<-5> \  
filename=/<host_health_history.txt> \  

```

```
xe pool-retrieve-wlb-report report=optimization_performance_history \  
LocaleCode=<en> \  
Start=-3 \  
End=0 \  
PoolID=c75f9ee9-422f-9cde-4781-24f6cbd9279c \  
UTCOffset=-5 \  
filename=/<optimization_performance_history>.txt \  

```



```
xe pool-retrieve-wlb-report report=pool_health_history \  
LocaleCode=<en> \  
Start=<-3> \  
End=<0> \  
PoolID=<c75f9ee9-422f-9cde-4781-24f6cbd9279c> \  
UTCOffset=<-5> \  
filename=</pool_health_history>.txt \  
  
xe pool-retrieve-wlb-report report=vm_movement_history \  
LocaleCode=<en> \  
Start=<-3> \  
End=<0> \  
PoolID=<c75f9ee9-422f-9cde-4781-24f6cbd9279c> \  
UTCOffset=<-5> \  
filename=</vm_movement_history>.txt \  
  
xe pool-retrieve-wlb-report report=vm_performance_history \  
LocaleCode=<en> \  
Start=<-3> \  
End=<0> \  
PoolID=<c75f9ee9-422f-9cde-4781-24f6cbd9279c> \  
HostID=<471626e5-8e8b-429b-9990-6013726d7e86> \  
UTCOffset=<-5> \  
filename=</vm_performance_history>.txt \  
  
xe pool-retrieve-wlb-report report=pool_audit_history \  
LocaleCode=<en> \  
Start=<-3> \  
End=<0> \  
PoolID=<c75f9ee9-422f-9cde-4781-24f6cbd9279c> \  
ReportVersion=<Creedence> \  
AuditUsers=<ALL> \  
AuditObject=<ALL> \  
StartLine=<1/> \  
EndLine=<10000> \  
UTCOffset=<-5> \  
filename=</pool_audit_history>.txt \  
  
xe pool-retrieve-wlb-report report=pool_optimization_history \  
LocaleCode=<en> \  
Start=<-3> \  
End=<0> \  
PoolID=<c75f9ee9-422f-9cde-4781-24f6cbd9279c> \  
UTCOffset=<-5> \  
filename=</pool_optimization_history>.txt \  
  
xe pool-retrieve-wlb-report report=vm_chargeback_history \  
LocaleCode=<en> \  
Start=<-3> \  
End=<0> \  
PoolID=<c75f9ee9-422f-9cde-4781-24f6cbd9279c> \  
UTCOffset=<-5> \  
filename=</vm_chargeback_history>.txt
```

8.2.14. pool-send-wlb-configuration

Modifies Workload Balancing configuration settings, including thresholds, Workload Balancing power-management settings, and weightings. It is not mandatory to configure all settings with the command. You can configure only some parameters, but not all, if desired.

Before using the `pool-send-wlb-configuration` command, learn about the default values on your system by running `pool-retrieve-wlb-configuration`.

When you run the `pool-retrieve-wlb-configuration` command, additional parameters appear that are not documented in this section. Citrix does not recommend editing these parameters.



```
pool-send-wlb-configuration  
[config:HostMemoryThresholdCritical=<HostCpuThresholdCritical=value>\  
config:HostMemoryThresholdHigh=<HostMemoryThresholdHigh=value>\  
config:HostPifReadThresholdCritical=<HostPifReadThresholdCritical=value>\  
config:HostPifReadThresholdHigh=<HostPifReadThresholdHigh=value>\ config:set_host_configuration=<true |  
false> ...\]
```

Use the **pool-send-wlb-configuration** command with the arguments *<ParticipatesInPowerManagement>* and *<set_host_configuration>* to configure Workload Balancing's Host Power Management feature.

```
xe pool-send-wlb-configuration \  
config:<host_21_> \  
ParticipatesInPowerManagement=<true> \  
config:set_host_configuration=<true>
```

Chapter 9. Appendix C: Configuring Certificates for Workload Balancing

This chapter provides information about two optional tasks for securing certificates:

- Configuring XenServer to verify a certificate from a Trusted Authority
- Configuring XenServer to verify the default Citrix WLB self-signed certificate

Important:

Certificate configuration has changed for this release. If you upgraded a Workload Balancing Balancing 6.x virtual appliance to Workload Balancing 6.5 and you did not have certificates configured before the upgrade, you must use the certificate instructions in the *Workload Balancing 6.0 Administrator's Guide* (and not this guide) if you configure certificates.

9.1. Overview

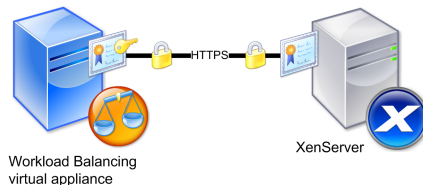
XenServer and Workload Balancing communicate over HTTPS. Consequently during Workload Balancing Configuration, the wizard automatically creates a self-signed test certificate. This self-signed test certificate lets Workload Balancing establish an SSL connection to XenServer.

Note:

The self-signed certificate is a placeholder to facilitate HTTPS communication and is not from a trusted certificate authority. For added security, Citrix recommends using a certificate signed from a trusted certificate authority.

By default, Workload Balancing creates this SSL connection with XenServer automatically. You do not need to perform any certificate configurations during or after configuration for Workload Balancing to create this SSL connection. However, to use a certificate from another certificate authority, such as a signed one from a commercial authority, you must configure Workload Balancing and XenServer to use it.

Regardless of what certificate Workload Balancing uses, by default, XenServer does not validate the identity of the certificate before it establishes connection to Workload Balancing. To configure XenServer to check for a specific certificate, you must export the root certificate that was used to sign the certificate, copy it to XenServer, and configure XenServer to check for it when a connection to Workload Balancing is made. In this scenario, XenServer acts as the client and Workload Balancing acts as the server.



This illustration shows how XenServer verifies that a specific certificate is present before it lets the Workload Balancing virtual appliance establish a connection to it over SSL. In this case, the real certificate (the certificate with the private key) is on the Workload Balancing server and the certificate that was used to sign it, is on the XenServer pool master.

Depending on your security goals, you can either:

- Configure XenServer to verify the self-signed test certificate. See [Section 9.2, “Configuring XenServer to Verify the Self-Signed Certificate”](#).



- Configure XenServer to verify a certificate from a trusted certificate authority. See [Section 9.3, “Configuring XenServer to Verify a Certificate-authority Certificate”](#).

9.2. Configuring XenServer to Verify the Self-Signed Certificate

You can configure XenServer to verify that the Citrix WLB self-signed certificate is authentic before XenServer permits Workload Balancing to connect.

Important:

To verify the Citrix WLB self-signed certificate, you must connect to Workload Balancing using its host name. To find the Workload Balancing host name, run **hostname** command on the virtual appliance.

If you want to configure Workload Balancing to verify the Citrix WLB self-signed certificate, perform the steps in the procedure that follows.

To configure XenServer to verify the self-signed certificate

1. Copy the self-signed certificate from the Workload Balancing virtual appliance to the pool master. The Citrix WLB self-signed certificate is stored at `/etc/ssl/certs/server.pem`. Run the following on the pool master to copy the certificate:

```
scp root@<wlb-ip>:/etc/ssl/certs/server.pem .
```

2. If you receive a message stating that the authenticity of `<wlb-ip>` cannot be established, type **yes** to continue.
3. Enter Workload Balancing virtual appliance root password when prompted, the certificate will be copied to current directory.
4. Install the certificate. Run the **pool-certificate-install** command from the directory where you copied the certificate. For example:

```
xe pool-certificate-install filename=server.pem
```

5. Verify the certificate was installed correctly by running the **pool-certificate-list** command on the pool master:

```
xe pool-certificate-list
```

If you installed the certificate correctly, the output of this command includes the exported root certificate (for example, `server.pem`). Running this command lists all installed SSL certificates, including the certificate you just installed.

6. Synchronize the certificate from the master to all hosts in the pool by running the **pool-certificate-sync** command on the pool master:

```
xe pool-certificate-sync
```

Running the **pool-certificate-sync** command on the master synchronizes the certificate and certificate revocation lists on all the pool servers with the master. This ensures all hosts in the pool use the same certificate(s).

There is no output from this command. However, the next step does not work if this one did not work successfully.

7. Instruct XenServer to verify the certificate before connecting to the Workload Balancing virtual appliance. Run the following command on the pool master:

```
xe pool-param-set wlb-verify-cert=<true> uuid=<uuid_of_pool>
```

Tip:

Pressing the **Tab** key automatically populates the UUID of the pool.



8. (Optional.) To verify this procedure worked successfully, perform the following steps:
 - a. To test if the certificate synchronized to the other hosts in pool, run the **pool-certificate-list** command on those hosts.
 - b. To test if XenServer was set to verify the certificate, run the **pool-param-get** command with the `param-name=<wlb-verify-cert>` parameter. For example:

```
xe pool-param-get param-name=<wlb-verify-cert> uuid=<uuid_of_pool>
```

9.3. Configuring XenServer to Verify a Certificate-authority Certificate

You can configure XenServer to verify a certificate signed by a trusted certificate authority.

For trusted authority certificates, XenServer requires an exported certificate or certificate chain (the intermediate and root certificates) in .pem format that contains the public key.

If you want Workload Balancing to use a trusted authority certificate, do the following:

1. Obtain a signed certificate from the certificate authority. See [Section 9.3.1, “Task 1: Obtaining a Certificate-authority Certificate”](#).
2. Follow the instructions in [Section 9.3.2, “Task 2: Specifying the New Certificate”](#) to specify and apply the new certificate.
3. Install the obtained certificates and enable certificate verification on the pool master. See [Section 9.3.3, “Task 3: Importing the Certificate Chain into the Pool”](#).

Before beginning these tasks, make sure:

- You know the IP address for the XenServer pool master.
- XenServer can resolve the Workload Balancing host name. (For example, you can try pinging the Workload Balancing FQDN from the XenServer console for the pool master.)

Important:

If you want to use an IP address to connect to Workload Balancing, you must specify that IP address as the Subject Alternative Name (SAN) when you create the certificate.

9.3.1. Task 1: Obtaining a Certificate-authority Certificate

To obtain a certificate from a certificate authority, you must generate a Certificate Signing Request (CSR). Generating a CSR for the Workload Balancing virtual appliance is two-task process. You must (1) create a private key and (2) use that private key to generate the CSR. You must perform both of these procedures on the Workload Balancing virtual appliance.

Guidelines for Specifying the Common Name

The Common Name (CN) you specify when creating a CSR must exactly match the FQDN of your Workload Balancing virtual appliance and the FQDN or IP address you specified in the **Address** box in the **Connect to WLB Server** dialog box.

To ensure the name matches, specify the Common Name using one of these guidelines:

- Specify the same information for the certificate's Common Name as you specified in the **Connect to WLB Server** dialog. For example, if your Workload Balancing virtual appliance is named “wlb-vpx.yourdomain,” specify “wlb-vpx.yourdomain” in the **Connect to WLB Server** and provide “wlb-vpx.yourdomain” as the Common Name when creating the CSR.
- If you connected your pool to Workload Balancing using an IP address, use the FQDN as the Common Name and specify the IP address as a Subject Alternative Name (SAN). However, this may not work in all situations.

Note:



Certificate verification is a security measure designed to prevent unwanted connections. As a result, Workload Balancing certificates must meet strict requirements or the certificate verification will not succeed and XenServer will not allow the connection. Likewise, for certificate verification to succeed, you must store the certificates in the specific locations in which XenServer expects to find the certificates.

To create a private key file

1. Create a private key file:

```
openssl genrsa -des3 -out <privatekey.pem> 2048
```

2. Remove the password:

```
openssl rsa -in <privatekey.pem> -out <privatekey.nop.pem>
```

Note:

If you enter the password incorrectly or inconsistently, you may receive some messages indicating there is a user interface error. You can ignore the message and just rerun the command to create the private key file.

To generate the CSR

1. Generate the CSR:

- a. Create the CSR using the private key:

```
openssl req -new -key <privatekey.nop.pem> -out <csr>
```

- b. Follow the prompts to provide the information necessary to generate the CSR:

Country Name. Enter the SSL Certificate country codes for your country. For example, CA for Canada or JM for Jamaica. You can find a list of SSL Certificate country codes on the web.

State or Province Name (full name). Enter the state or province where the pool is located. For example, Massachusetts or Ontario.

Locality Name. The name of the city where the pool is located.

Organization Name. The name of your company or organization.

Organizational Unit Name. Enter the department name. This field is optional.

Common Name. Enter the FQDN of your Workload Balancing server. This must match the name the pool uses to connect to Workload Balancing.

Email Address. This email address is included in the certificate when you generate it.

- c. Provide optional attributes or click **Enter** to skip providing this information.

The CSR request is saved in the current directory and is named `csr`.

2. Display the CSR in the console window by running the following commands in the Workload Balancing appliance console:

```
cat csr
```

3. Copy the entire Certificate Request and use the CSR to request the certificate from the certificate authority.

9.3.2. Task 2: Specifying the New Certificate

Use this procedure to specify Workload Balancing use a certificate from a certificate authority. This procedure installs the root and (if available) intermediate certificates.

To specify a new certificate

1. Download the signed certificate, root certificate and, if the certificate authority has one, the intermediate certificate from the certificate authority.
2. If you did not download the certificates to the Workload Balancing virtual appliance. Do one of the following:
 - a. If you are copying the certificates from a Windows computer to the Workload Balancing appliance, use WinSCP or another copying utility, to copy the files.

For the host name, you can enter the IP address and leave the port at the default. The user name and password are typically root and whatever password you set during configuration.

- b. If you are copying the certificates from a Linux computer to the Workload Balancing appliance, use SCP or another copying utility, to copy the files to the directory of your choice on the Workload Balancing appliance. For example:

```
scp <root_ca.pem> root@<wlb-ip>: /<path_on_your_WLB>
```

3. On the Workload Balancing virtual appliance, merge contents of all the certificates (root certificate, intermediate certificate (if it exists), and signed certificate) into one file. For example:

```
cat <signed_cert.pem> <intermediate_ca.pem> <root_ca.pem> > <server.pem>
```

4. Rename the existing certificate and key using the move command:

```
mv /etc/ssl/certs/server.pem /etc/ssl/certs/server.pem_orig
mv /etc/ssl/certs/server.key /etc/ssl/certs/server.key_orig
```

5. Copy the merged certificate:

```
mv <server.pem> /etc/ssl/certs/server.pem
```

6. Copy the private key created in [this step](#):

```
mv <privatekey.nop.pem> /etc/ssl/certs/server.key
```

7. Make the private key readable only by root. Use **chmod** command to fix permissions.

```
chmod 600 /etc/ssl/certs/server.key
```

8. Restart stunnel:

```
killall stunnel
stunnel
```

9.3.3. Task 3: Importing the Certificate Chain into the Pool

After obtaining certificates, you must import (install) the certificates onto the XenServer pool master and synchronize the hosts in the pool to use those certificates. Then, you can configure XenServer to check the certificate's identity and validity each time Workload Balancing connects to a XenServer host.

1. Copy the signed certificate, root certificate and, if the certificate authority has one, the intermediate certificate from the certificate authority onto the XenServer pool master.
2. Install the root certificate on the pool master:

```
xe pool-certificate-install filename=<root_ca>.pem
```

3. If applicable, install the intermediate certificate on the pool master:

```
xe pool-certificate-install filename=<intermediate_ca>.pem
```

4. Verify both the certificates installed correctly by running this command on the pool master:

```
xe pool-certificate-list
```

Running this command lists all installed SSL certificates. If the certificates installed successfully, they appear in this list.

5. Synchronize the certificate on the pool master to all hosts in the pool:

```
xe pool-certificate-sync
```

Running the **pool-certificate-sync** command on the master synchronizes the certificates and certificate revocation lists on all the pool servers with the pool master. This ensures all hosts in the pool use the same certificates.

6. Instruct XenServer to verify a certificate before connecting to the Workload Balancing virtual appliance. Run the following command on the pool master:

```
xe pool-param-set wlb-verify-cert=<true> uuid=<uuid_of_pool>
```

Tip:

Pressing the **Tab** key automatically populates the UUID of the pool.

7. If, before you enabled certificate verification, you specified an IP address in the **Connect to WLB** dialog, you may be prompted to reconnect the pool to Workload Balancing.

In this case, specify the **FQDN** for the Workload Balancing appliance in the **Address** box in the **Connect to WLB** dialog—exactly as it appears in the certificate's Common Name (CN). (You must enter the FQDN since the Common Name and the name XenServer uses to connect must match.)

Troubleshooting Tips

- If, after configuring certificate verification, the pool cannot connect to Workload Balancing, check to see if the pool can connect if you turn certificate verification off (by running `xe pool-param-set wlb-verify-cert=<true> uuid=<uuid_of_pool>`). If it can connect with verification off, the issue is in your certificate configuration. If it cannot connect, the issue is in either your Workload Balancing credentials or your network connection.
- Some commercial certificate authorities, such as Verisign, provide tools to verify the certificate installed correctly. Consider running these tools if these procedures fail to help isolate the issue. If these tools require specifying an SSL port, specify port 8012 or whatever port you set during Workload Balancing Configuration.
- If, after following these procedures, an error message appears on the **WLB** tab stating, "There was an error connecting to the WLB server," there may be a conflict between the Common Name in the certificate and the name of the Workload Balancing virtual appliance. The Workload Balancing virtual-appliance name and the Common Name of the certificate must match exactly.

Index

A

- adjusting
 - optimization mode, 19
- aggressiveness
 - configuring, 32
- automated recommendations
 - advanced settings, 30
 - controlling, 30
 - overview, 21
- automatic
 - optimization acceptance, 21

C

- certificates
 - certificate authority certificate, verifying, 67
 - certificate chain, importing, 69
 - Certificate Signing Request, generating, 67
 - configuring, 65
 - new, specifying, 68
 - self-signed, verifying, 66
- changing
 - PostgreSQL account, 58
 - WLB server, 40
 - Workload Balancing account, 58
- commands
 - Workload Balancing, 57
- configuring
 - critical thresholds, 27
 - power management, 20
- connecting
 - pool to WLB, 36
- consolidation process
 - Maximum Density Mode, 26
- critical thresholds
 - configuring, 27
 - default settings, 27
- customizing
 - Workload Balancing, 48

D

- database
 - archiving, 45
 - changing account, 58
 - changing maintenance time, 47
 - client authentication, 45
 - configuration files, 46
 - grooming, 44, 58
 - grooming parameters, 45
 - managing, 43
 - password, 45
 - pg_hba.conf file, 46
 - postgresql.conf file, 46
- disconnecting
 - Workload Balancing, 42

- disk size
 - increasing, 43
- displaying
 - settings dialog, 18

E

- enabling
 - power management, 21
- excluding
 - hosts from recommendations, 29

F

- fixed optimization mode
 - configuring, 19

H

- High Availability
 - interaction with WLB, 7

I

- IP address
 - changing Workload Balancing, 41
 - obtaining for WLB, 39

L

- logging in
 - Workload Balancing appliance, 57
- logs
 - enabling traces, 58
 - increasing detail in logs, 59

M

- Maximum Density Mode
 - consolidation process, 26
- Maximum Performance Mode
 - recommendation process, 25
- metric weightings
 - configuring, 28

O

- optimal server
 - resuming VM on, 6
 - starting, 5
- optimization mode
 - fixed mode, 19
 - scheduled mode, 19
 - scheduling, 19
 - settings, 19
- optimization recommendations
 - accepting, 7
 - how WLB makes, 24
- options
 - configuring, 18

P

- pausing
 - Workload Balancing, 42



- PostgreSQL
 - changing password, 58
- power management
 - configuring, 20
 - enabling, 21

R

- RBAC
 - Workload Balancing, 39
- recommendation count
 - setting, 31
- recommendation process
 - Maximum Performance Mode, 25
- recommendation severity
 - setting, 32
- recommendations
 - accepting, 7
 - accepting, optimization, 7
 - excluding hosts from, 29
- reconfiguring
 - pool to use different WLB server, 40
- renaming
 - WLB user account, 58
- reports
 - Chargeback, 11
 - generating, 9
 - glossary, 11
 - Host Health History, 13
 - introduction, 3
 - overview, 9
 - Pool Health, 15
 - Pool Health History, 16
 - Pool Optimization History, 16
 - Pool Optimization Performance History, 13
 - Virtual Machine Motion History, 17
 - Virtual Machine Performance History, 17
- requirements
 - Workload Balancing, 3
- resource utilization
 - process for evaluating, 24

S

- scheduled optimization mode
 - configuring, 19
- scheduling
 - optimization mode, 19
- securing
 - Workload Balancing, 65
- settings
 - configuring, 18, 18
 - displaying dialog, 18
- star ratings, 4
- stopping
 - Workload Balancing, 42

T

- trace flags

- increasing detail in logs, 59
- troubleshooting
 - connection to WLB, 55
 - error messages, 54
 - firewalls, 54
 - issues changing servers, 56
 - overview, 54
 - recommendations, stop, 55
 - WLB credentials, 54
- Trusted Authority certificates
 - configuring, 65

U

- uninstalling
 - Workload Balancing, 43
- updating credentials
 - Workload Balancing, 40
- upgrading
 - CentOS, 49
 - Internet access, with, 50
 - Internet access, without, 50
- user accounts
 - setting permissions, 39

V

- virtual disk size
 - increasing, 43
- VM migration interval
 - setting, 31
- VM placement
 - how to start VM, 5
 - overview, 4

W

- wlb config
 - running (proc.), 58
- wlb.conf
 - changing, 58
 - editing (proc.), 58
- wlbconf
 - editing (proc.), 58
- wlbconfig
 - running command, 58
- Workload Balancing
 - administering, 36
 - administering, overview, 36
 - commands, 57
 - configuring, 18, 18
 - customizing, 48
 - disconnecting, 42
 - IP address, 39
 - Maintenance Mode, 42
 - overview, 2
 - pausing, 42
 - reports, 9
 - requirements, 3
 - settings, 18, 18



- stopping, 42
- uninstalling, 43
- using, 4
- Workload Balancing account
 - changing, 58
- Workload Balancing commands
 - wlb restart, 57
 - wlb start, 57
 - wlb status, 57
 - wlb stop, 57
- workload reports
 - Chargeback, 11
 - generating, 9
 - glossary, 11, 11
 - Host Health History, 13
 - introduction, 3
 - overview, 9
 - Pool Health, 15
 - Pool Health History, 16
 - Pool Optimization History, 16
 - Pool Optimization Performance History, 13
 - Virtual Machine Motion History, 17
 - Virtual Machine Performance History, 17