Zenoss®

Service Dynamics

Resource Management Installation

Zenoss, Inc.
www.zenoss.com

Zenoss Service Dynamics Resource Management Installation

Copyright © 2012 Zenoss, Inc., 275 West St. Suite 204, Annapolis, MD 21401, U.S.A. All rights reserved.

Zenoss and the Zenoss logo are trademarks or registered trademarks of Zenoss, Inc. in the United States and other countries. All other trademarks, logos, and service marks are the property of Zenoss or other third parties. Use of these marks is prohibited without the express written consent of Zenoss, Inc. or the third-party owner.

Flash is a registered trademark of Adobe Systems Incorporated.

Oracle, the Oracle logo, Java, and MySQL are registered trademarks of the Oracle Corporation and/or its affiliates.

Linux is a registered trademark of Linus Torvalds.

RabbitMQ is a trademark of VMware, Inc.

SNMP Informant is a trademark of Garth K. Williams (Informant Systems, Inc.).

Sybase is a registered trademark of Sybase, Inc.

Tomcat is a trademark of the Apache Software Foundation.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

All other companies and products mentioned are trademarks and property of their respective owners.

Part Number: 25-122012-4.2-v05

Preface

Zenoss Service Dynamics Resource Manager Installation provides detailed information and procedures you will use to install and upgrade Resource Manager for your environment.

1. Who Should Use This Guide

This guide is designed for administrators who will install and update Resource Manager.

Those installing the system should be comfortable with Linux administration, as well as networking protocols and concepts (such as SNMP and SSH). More advanced server administration skills may be required for highly available, complex, or large deployments.

2. How This Guide Is Organized

This guide is organized into these chapters:

- Chapter 1, "Installation Considerations," presents information about operating system and hardware requirements, as well as other special considerations, you should review before beginning installation.
- Chapter 2, "Installing for RHEL 5 or CentOS 5," provides procedures for installing Resource Manager on a system running Red Hat Enterprise Linux (RHEL), Version 5 or Community ENTerprise Operating System (CentOS), Version 5.
- Chapter 3, "Installing for RHEL 6 or CentOS 6," provides procedures for installing Resource Manager on a system running RHEL 6 or CentOS 6.
- Chapter 4, "Installing the RPM-Based ISO Appliance," outlines procedures for installing the RPM-based appliance in a virtual environment or on physical hardware.
- Chapter 5, "Installing Collectors and Hubs," provides detailed installation procedures for a distributed collector setup.
- Chapter 6, "Performance Tuning," offers information and procedures to help you optimize Resource Manager performance in your environment.
- Chapter 7, "Upgrading," provides procedures for upgrading your current version of Resource Manager to the current version.
- Appendix A, "Updating RabbitMQ Server for Resource Manager 4.2.3," details procedures for upgrading RabbitMQ Server in certain non-standard conditions.

3. Related Guides

The Zenoss Service Dynamics documentation set includes these guides:

Primary Audience	Title	Description
All audiences	*Resource Manager Administration*	Provides an overview of Resource Manager architecture and features, as well as procedures and examples to help use the system.
System administrators	*Resource Manager Installation*	Provides detailed information and procedures for installing and upgrading the system.
All audiences	*Analytics and Optimization Installation and Administration*	Provides conceptual and procedural information to help you install and use Analytics.
All audiences	*Impact and Event Management Installation and Administration*	Provides conceptual and procedural information to help you install and use Impact.

Primary Audience	Title	Description
All audiences	*Global Operations Management*	Provides conceptual and procedural information to help you install and use GOM.
All audiences	*Service Dynamics Release Notes*	Describes known issues, fixed issues, and late-breaking information not already provided in the Service Dynamics documentation set.
System administrators	*Resource Manager Extended Monitoring*	Provides detailed information about extending monitoring and other capabilities provided by ZenPacks.

Table 1. Zenoss Service Dynamics Guides

4. Additional Information

If you have technical questions about this product that are not answered in the product documentation, visit the Zenoss Enterprise Support Center, at:

https://support.zenoss.com

5. Zenoss Welcomes Your Comments

Zenoss welcomes your comments and suggestions on our documentation.

To share your comments, please email docs@zenoss.com. In the email, please include the document title and part number. The part number appears just below the list of trademarks at the front of each guide.

Chapter 1. Installation Considerations

Read the following sections to learn more about installation requirements for the Service Resource Management ("Resource Manager") feature of Zenoss Service Dynamics™.

1.1. Installation Artifacts

Zenoss provides two RPM Package Manager (RPM) artifacts for Resource Manager server deployment:

- Resource Manager RPM - Includes the Resource Manager software and required ZenPacks
- Windows ZenPacks RPM - (Optional) Includes ZenPacks required for Windows monitoring

For detailed information about installing the RPMs, refer to one of the following chapters in this guide:

- Installing for RHEL 5 or CentOS 5
- Installing for RHEL 6 or CentOS 6

1.2. Operating System Requirements

Resource Manager can be installed on:

- Red Hat Enterprise Linux (5 or 6)
- CentOS (5 or 6)

1.3. Hardware Requirements

Hardware requirements for Resource Manager depend on a number of factors, including I/O, memory, CPU, and the number of managed devices.

For a deployment with a low number of managed devices and data points (low I/O), only a single master is required.

For a deployment with 1000 managed devices, assuming that:

- Each managed device averages 100 data points
- Collection maximum is 250 data points per second (measured on a 15000 RPM hard drive)
- Default cycle time is 300 seconds

You could calculate hardware requirements as:

> 1000 devices x 100 data points per device = 100,000 data points
>
> 100000 / 300 seconds / 250 dps = 1.333 collectors

In this scenario, you would need one master and two collectors to prevent I/O overload.

For each use type, minimum memory and CPU requirements are shown in the following table.

Type	Memory	CPU
Master	8GB	8 cores
Remote collector	4GB	4 cores

Table 1.1. Memory and CPU Requirements

Disk storage requirements are shown in the following table:

Type	Disk Storage
Resource Manager	50GB

Type	Disk Storage
Zenoss DataStore	50GB

Table 1.2. Disk Storage Requirements

1.3.1. Large or Complex Deployments

If you are planning to monitor a large number of devices (with a significant number of data points for each device), or a network with complex topology, there are additional requirements and configurations to consider. Contact Zenoss Professional Services for deployment planning assistance.

1.3.2. Other Considerations

Resource Manager is a highly I/O-intensive application; as a result, it usually performs best when using direct, attached storage. However, an appropriately tuned SAN/NAS environment can also be used effectively with a Resource Manager installation.

1.4. Server Hardware Configuration

1.4.1. File System Configuration

Resource Manager stores gathered performance data in individual RRD files. Performance updates are 8 bytes per data point, which translates to a 4KB file system block update. Under such a high volume/low throughput usage pattern, journaled file systems can be detrimental to IO performance.

If possible, create a separate, non-journaled partition for `$ZENHOME/perf` (for RPM, `/opt/zenoss/perf`).

For more information about file system performance tuning and increasing RRD performance, read the section titled "Increasing RRD Performance" in the Performance Tuning chapter of this guide, or browse to:

http://oss.oetiker.ch/rrdtool-trac/wiki/TuningRRD

1.4.2. Deploying in a Virtualized Environment

Resource Manager is deployed successfully at many sites in a virtualized environment. However, this type of environment requires additional configuration to ensure there is no resource contention for the Resource Manager application (CPU, memory, IO). Zenoss Professional Services can provide expert assistance in this area.

1.5. Post-Installation Performance Tuning Tasks

After your installation is complete, there are several configuration settings you should adjust to maintain proper performance. Based upon the size of your planned deployment, changes to the database configuration, as well as tuning of the Zope configuration file, are required. See the chapter titled "Performance Tuning" in this guide for more information.

Chapter 2. Installing for RHEL 5 or CentOS 5

This chapter provides detailed instructions for installing Resource Manager for RHEL 5 or CentOS 5.

Before installing Resource Manager, you must:

- Ensure your system meets all requirements
- Install required software and packages

Unless otherwise directed, perform all steps as the root user.

2.1. Requirements

Ensure that your system meets all hardware requirements, and that you have correctly configured your operating system and hard drive partitions.

In addition, make sure that:

- You have disabled SELinux
- The `/opt/zenoss` directory is not a symbolic link to another location
- The umask is set to 022 (masks write permissions for group and others)
- The `/home` directory is writable by root, or the `/home/zenoss` directory exists as the zenoss user home directory
- You are connected to the Internet
- DNS is accessible

2.2. Required Software

Important! This chapter may not define all required packages for your installation options. While installing one or more software packages, you may be prompted to install additional, required software. Zenoss recommends that you install that software as directed.

The following table lists software dependencies for this Resource Manager version.

Package	Version
/bin/bash	3.2 or later
/bin/sh	
binutils	
coreutils	
cyrus-sasl-lib	2.1 or later
dmidecode	
erlang	R12B
glibc-devel	2.5 or later
gnupg	
jre	1.6 Update 31 or later (1.7 is not supported)
libaio	
libbz2.so.1()(64bit)	
libcrypto.so.6()(64bit)	
libcrypt.so.1()(64bit)	

Package	Version
libcrypt.so.1(GLIBC_2.2.5)(64bit)	
libc.so.6()(64bit)	
libc.so.6(GLIBC_2.2.5)(64bit)	
libc.so.6(GLIBC_2.3.2)(64bit)	
libc.so.6(GLIBC_2.3.4)(64bit)	
libc.so.6(GLIBC_2.3)(64bit)	
libc.so.6(GLIBC_2.4)(64bit)	
libdb-4.3.so()(64bit)	
libdl.so.2()(64bit)	
libdl.so.2(GLIBC_2.2.5)(64bit)	
liberation-fonts	
libexslt.so.0()(64bit)	
libgcc_s.so.1()(64bit)	
libgcc_s.so.1(GCC_3.0)(64bit)	
libgcj	
libgdbm.so.2()(64bit)	
libgmp.so.3()(64bit)	
libgomp	
liblber-2.3.so.0()(64bit)	
libldap_r-2.3.so.0()(64bit)	
libm.so.6()(64bit)	
libm.so.6(GLIBC_2.2.5)(64bit)	
libmysqlclient.so.18()(64bit)	
libncursesw.so.5()(64bit)	
libnsl.so.1()(64bit)	
libnsl.so.1(GLIBC_2.2.5)(64bit)	
libpanelw.so.5()(64bit)	
libpcre.so.0()(64bit)	
libprotobuf-lite.so.7()(64bit)	
libprotobuf.so.7()(64bit)	
libprotoc.so.7()(64bit)	
libpthread.so.0()(64bit)	
libpthread.so.0(GLIBC_2.2.5)(64bit)	
libpython2.7.so.1.0()(64bit)	
libreadline.so.5()(64bit)	
librrd.so.4()(64bit)	
librt.so.1()(64bit)	
libsasl2.so.2()(64bit)	
libsmi.so.2()(64bit)	
libsqlite3.so.0()(64bit)	
libssl.so.6()(64bit)	

Package	Version
libstdc++.so.6()(64bit)	
libstdc++.so.6(CXXABI_1.3)(64bit)	
libstdc++.so.6(GLIBCXX_3.4)(64bit)	
libutil.so.1()(64bit)	
libutil.so.1(GLIBC_2.2.5)(64bit)	
libxml2.so.2()(64bit)	
libxslt	1.1 or later
libxslt.so.1()(64bit)	
libz.so.1()(64bit)	
memcached	1.4.5 or later
nagios-plugins	1.4.15 or later
nagios-plugins-dig	1.4.15 or later
nagios-plugins-dns	1.4.15 or later
nagios-plugins-http	1.4.15 or later
nagios-plugins-ircd	1.4.15 or later
nagios-plugins-ldap	1.4.15 or later
nagios-plugins-ntp	1.4.15 or later
nagios-plugins-perl	1.4.15 or later
nagios-plugins-ping	1.4.15 or later
nagios-plugins-rpc	1.4.15 or later
nagios-plugins-tcp	1.4.15 or later
net-snmp	5.3.2.2-9 or later
net-snmp-utils	5.3.2.2-9 or later
openldap	2.3 or later
openssl	
patch	
pcre	6.6 or later
pkgconfig	
python	2.3.4 or later
rabbitmq-server	2.8.6 or later
readline	5.1 or later
rpmlib(CompressedFileNames)	3.0.4-1 or later
rpmlib(PayloadFilesHavePrefix)	4.0-1 or later
rpmlib(VersionedDependencies)	3.0.3-1 or later
rrdtool	1.4.7 or later
rsync	
rtld(GNU_HASH)	
shadow-utils	
sysstat	
zends	5.5.25a
zlib	1.2 or later

2.3. Prerequisite Tasks

Before installing Resource Manager, you must:

- Configure your firewall
- Remove conflicting messaging systems
- Download the Resource Manager installation files
- Install and configure the software repository, prerequisite software, and additional packages, including:
  - Oracle Java
  - Zenoss dependencies repository
  - RabbitMQ
  - memcached and snmpd
  - Zenoss DataStore

2.3.1. Configure Your Firewall

Resource Manager requires these ports be open in your firewall:

Port	Protocol	Direction to Resource Manager Server	Description
11211	TCP | UDP	Inbound	memcached
8080	TCP	Outbound	Web interface
514	UDP	Inbound	syslog
162	UDP	Inbound	SNMP Traps

Table 2.1. Ports

Alternatively, you can disable your firewall:

- For IPv4, use these commands:

```
service iptables stop
chkconfig iptables off
```

- For IPv6, use these commands:

```
service ip6tables stop
chkconfig ip6tables off
```

2.3.2. Remove Conflicting Messaging Systems

Zenoss CSA relies on the RabbitMQ messaging system. Newer versions of CentOS include alternative messaging systems (Matahari and Qpid). You must remove these messaging systems to run Zenoss CSA.

1. Use the following commands to determine if Matahari or Qpid packages are installed on your system:

```
rpm -qa | egrep -i "matahari|qpid"
```

2. Remove all listed packages:

```
yum erase Package1 Package2 ...
```

2.3.3. Download the Resource Manager Installation Files

1. Browse to the following URL:

   https://support.zenoss.com

Note

Contact your Zenoss representative for site login credentials.

2. In the Downloads area of the Home tab, locate the current Service Dynamics installation files.
3. Download the Resource Manager and (optionally) Windows ZenPacks RPM files.

2.3.4. Install Oracle Java

Follow these steps to install and configure Oracle Java.

Note

OpenJDK is not supported for Zenoss CSA. If you have OpenJDK or another Java version installed, then remove those installations before installing the required Oracle Java version.

1. Download Oracle JRE:

```
wget -O jre-6u31-linux-x64-rpm.bin \
 http://javadl.sun.com/webapps/download/AutoDL?BundleId=59622
```

2. Change mode:

```
chmod +x ./jre-6u31-linux-x64-rpm.bin
```

3. Install Oracle JRE:

```
./jre-6u31-linux-x64-rpm.bin
```

4. Add the following line to the end of the `/etc/profile` file:

```
export JAVA_HOME=/usr/java/default/bin
```

5. Verify the correct installed version (1.6 Update 31):

```
java -version
```

2.3.5. Install the Zenoss Dependencies Repository

Install the Zenoss dependencies repository:

```
rpm -ivh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el5.noarch.rpm
```

2.3.6. Install RabbitMQ

Use the following commands to install and configure RabbitMQ:

1. Install RabbitMQ:

```
yum -y install rabbitmq-server-2.8.6
```

2. Start the `rabbitmq-server` daemon and configure it to start automatically on reboot:

```
service rabbitmq-server start
chkconfig rabbitmq-server on
```

2.3.7. Install and Configure memcached and snmpd

Use these commands to install and configure the `memcached` and `snmpd` daemons:

1. Install memcached and net-snmp:

```
yum -y install memcached net-snmp net-snmp-utils
```

2. Start the `memcached` daemon and configure it to start automatically on reboot:

```
service memcached start
chkconfig memcached on
```

3. Start the `snmpd` daemon and configure it to start automatically on reboot:

```
service snmpd start
chkconfig snmpd on
```

2.3.8. Install the Zenoss DataStore

You can employ the Zenoss Datastore on a local or remote server. Resource Manager requires certain features provided by the data store, so even if you plan to use a remote server, you must install it on the local server as well. (You can, however, save resources by not running the main service.)

Perform these steps on the local Resource Manager server:

1. Browse to this URL:

   https://support.zenoss.com

   Note

   Contact your Zenoss representative for site login credentials.
2. In the Downloads area of the Home tab, locate and download the Zenoss DataStore RPM files.
3. Install the Zenoss DataStore:

```
yum --nogpgcheck localinstall zends-5.5.25a-1.Version.el5.x86_64.rpm
```

4. Start the data store and ensure it runs at system startup:

```
service zends start
chkconfig --level 2345 zends on
```

2.4. Install and Configure Resource Manager

Follow these steps to install the Resource Manager software and ZenPacks, and (optionally) a remote Zenoss DataStore.

2.4.1. Install the Resource Manager RPM

Install the Resource Manager RPM file:

```
yum -y --nogpgcheck localinstall zenoss_resmgr-Version.el5.x86_64.rpm
```

2.4.2. (Optional) Install a Remote Zenoss DataStore

Follow these optional steps to install and configure a remote data store.

1. On the local Resource Manager server:
   a. Stop the data store and configure it so that it will not run at system startup:

```
service zends stop
chkconfig --level 2345 zends off
```

   b. As the zenoss user, change the values of these entries in the `$ZENHOME/etc/global.conf.example` file:
      - zodb-host - Change the value from "localhost" to the name or IP address of the remote server.
      - zep-host - Change the value from "localhost" to the name or IP address of the remote server.
      - zodb-port - Change the value from 3306 to 13306
      - zep-port - Change the value from 3306 to 13306
2. On the remote server:
   a. Download the Zenoss DataStore RPM files.
   b. Install the Zenoss DataStore:

```
yum --nogpgcheck localinstall zends-5.5.25a-1.Version.el5.x86_64.rpm
```

c. Start the data store and ensure it runs at system startup:

```
service zends start
chkconfig --level 2345 zends on
```

d. Change to the zenoss user:

```
su - zenoss
```

e. Enter the following command:

```
zends -u root
```

f. Enable remote access to the Zenoss DataStore. In the prompt that appears, enter this series of commands:

```
grant all on *.* to 'root'@'%' with grant option;
flush privileges;
```

2.4.3. Install MySQLTuner

Follow these steps to download and install the MySQLTuner Perl script:

1. As the zenoss user, log in to a shell account on the master Resource Manager server.
2. Change to the following directory:

```
cd $ZENHOME/bin
```

3. Retrieve the MySQLTuner script:

```
wget mysqltuner.pl
```

4. Change read and execute access to the file:

```
chmod 755 mysqltuner.pl
```

2.4.4. Start the System

Run the following command to start the system:

```
service zenoss start
```

2.4.5. (Optional) Install the Windows Monitoring ZenPack

Optionally enable Windows monitoring:

1. Stop the system:

```
service zenoss stop
```

2. Install the msmonitor RPM file:

```
yum -y --nogpgcheck localinstall zenoss_msmonitor-Version.el5.x86_64.rpm
```

3. Restart the system:

```
service zenoss restart
```

2.5. Getting Started

After installation, use your Web browser to browse to the valid host name of the server where Resource Manager is installed.

Note

If you cannot successfully browse to your Resource Manager installation, then you may need to add an entry to your hosts file for the fully qualified domain name (FQDN) of your installation.

If you are using Internet Explorer to view the Resource Manager interface, and you have restricted the browser to trusted sites, then a warning message may appear. To prevent this, add your Resource Manager installation to the Trusted zone. These Microsoft articles provide more information on setting up trusted sites:

- Pre-Windows 7: http://support.microsoft.com/kb/174360
- Windows 7: http://windows.microsoft.com/en-US/windows7/Security-zones-adding-or-removing-web-sites

The setup wizard appears.

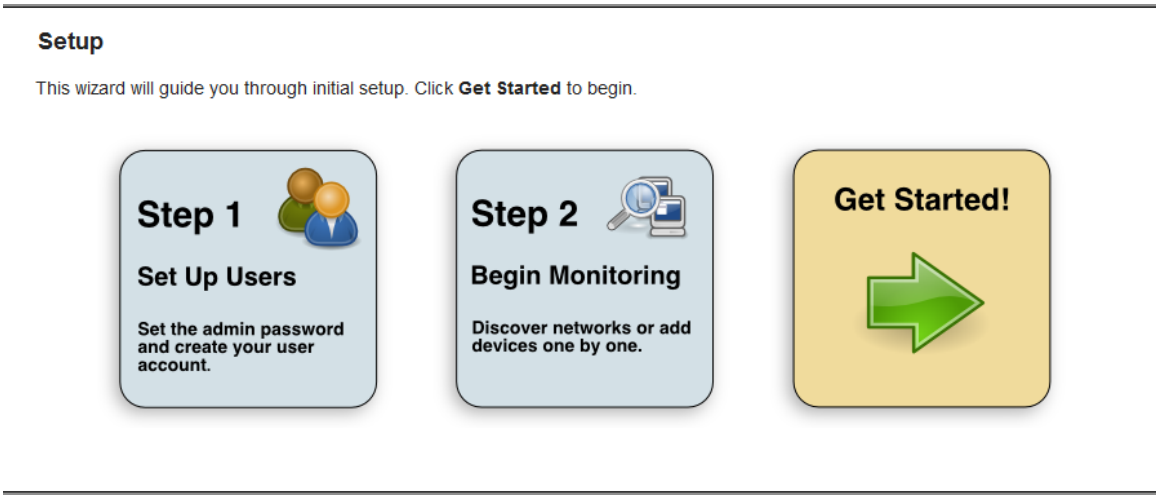

Figure 2.1. Setup Wizard

Using this wizard, you will:

- Change the admin password
- Set up an initial user
- Add some devices to the system
- Configure LDAP (optional)

From the first panel of the wizard, click **Get Started!** to begin.

The Step 1: Set up Initial Users panel appears.

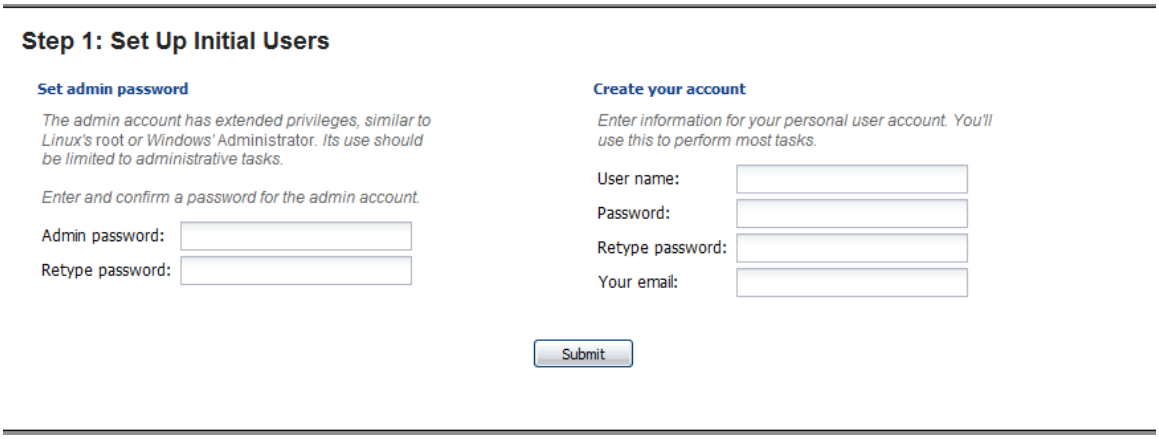

Figure 2.2. Setup Wizard: Step 1

2.5.1. Set the Administrative Password and Create a User

Follow these steps to select a password for the admin account and create your user account.

1. In the **Set admin password area**, enter and confirm a new admin password. You must enter a password value to continue.

   Note

   The Resource Manager admin account has extended privileges, and its use should be limited. Be sure to record the admin password and store it securely.

2. In the **Create your account** area, set up your Resource Manager user account. Most of the time, you will use this account to perform management tasks in Resource Manager. Enter a unique user name, password, and email address.
3. Click **Submit**.

   The Step 2: Specify or Discover Devices to Monitor panel appears.

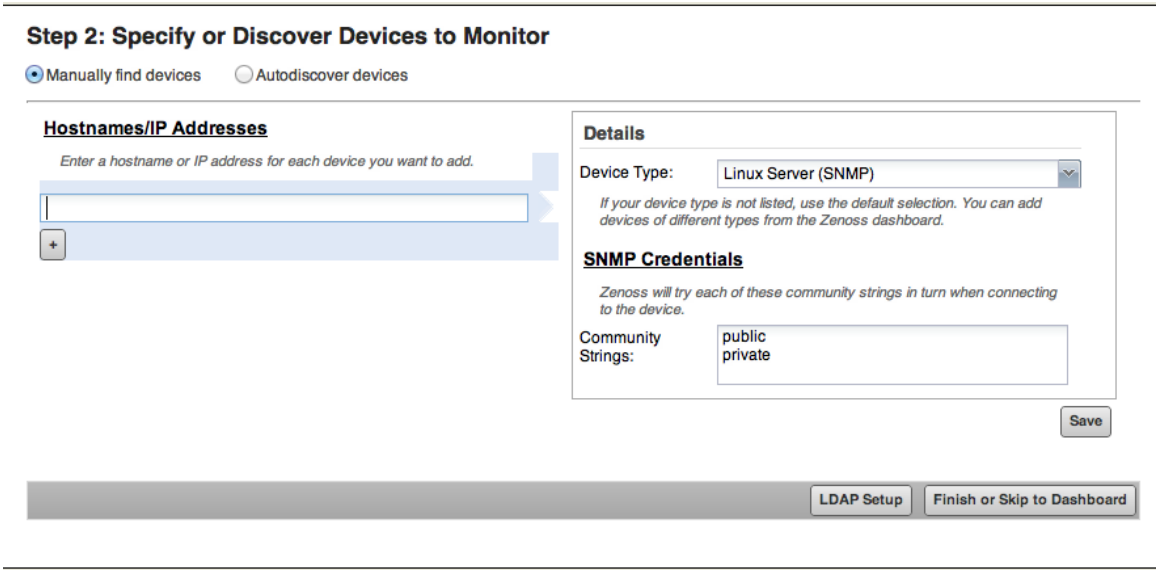

Figure 2.3. Setup Wizard: Step 2 (Manual Add)

2.5.2. Add Devices

You can add devices manually, or give Resource Manager network or IP address range information so it can discover your devices.

2.5.2.1. Adding Devices Manually

Follow these steps to manually add devices to the system. For each device you want to add:

1. Enter a fully qualified domain name or IP address
2. In the Details area, select a device type from the list. If your device type is not listed, then use the default selection. (You can change device classes for a device later, as well as add device classes.)
3. Enter the appropriate credentials used to authenticate against the device.

   Note

   For more information about setting credentials, refer to *Resource Manager Administration*.

4. To add the devices, click **Submit**.

   Resource Manager models the devices in the background.

Note

You can bypass device addition through the wizard. Click **Skip to the dashboard** to go directly to the Resource Manager Dashboard. Later, you can add devices by following the steps outlined in *Resource Manager Administration*.

2.5.2.2. Discovering Devices

To discover devices:

1. Select the **Autodiscover devices** option.

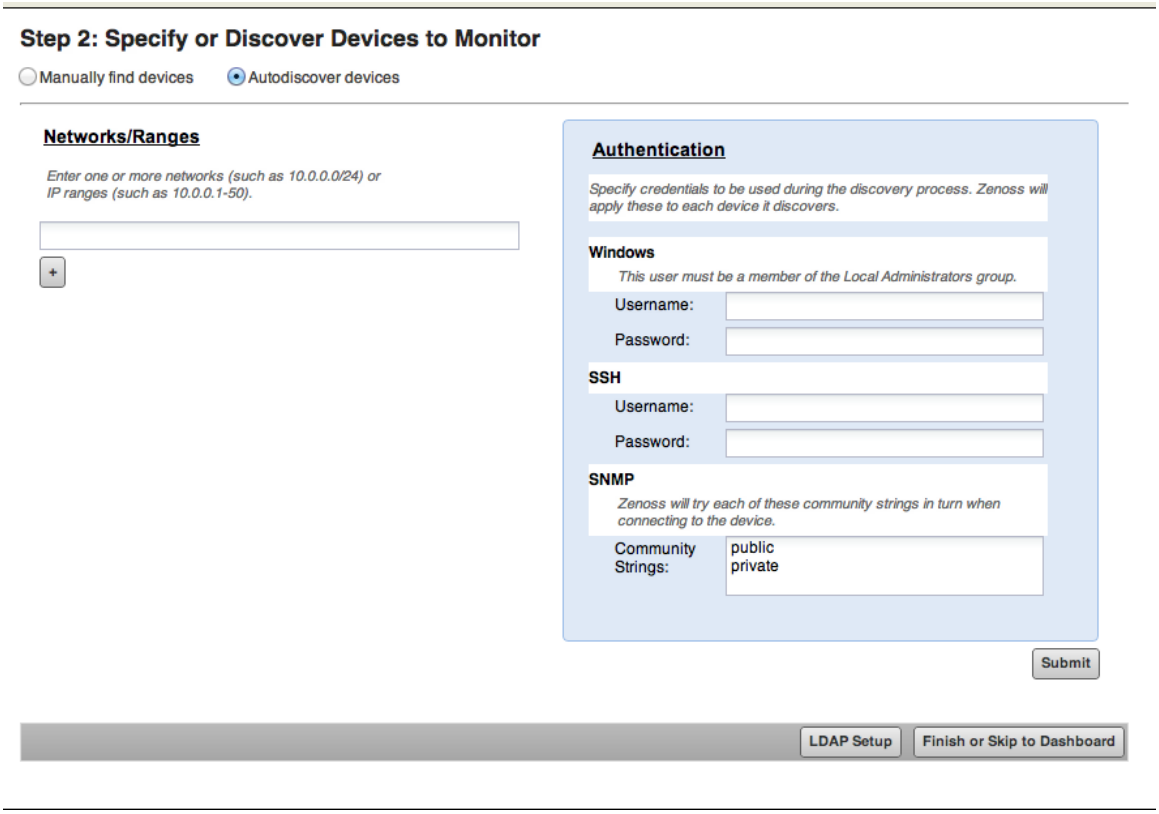

Figure 2.4. Setup Wizard: Step 2 (Discovery)

2. For each network or IP range in which you want Resource Manager to discover devices, enter an address or range. For example, you might enter a network address in CIDR notation:

   10.175.211.0/24

   or as a range of IP addresses:

   10.175.211.1-50

3. If you want to enter multiple addresses or ranges, click +. For each network, you must enter a netmask or IP range.
4. For each network or IP range, specify the Windows, SSH, or SNMP credentials you want Resource Manager to use on the devices it discovers. You can enter only one of each. Resource Manager attempts to use the same credentials on each device it discovers within the networks or IP ranges specified.
5. Click **Discover**.

   Resource Manager schedules jobs to discover devices in the networks and IP ranges you specified. (To see job status, navigate to Advanced > Settings, and then select Jobs in the left panel.)

When discovery completes, a notification message appears in the Messages portlet on the Dashboard.

Note

You can bypass device discovery through the wizard. Click **Skip to the dashboard** to go directly to the Resource Manager Dashboard. Later, you can discover devices by following the steps outlined in *Resource Manager Administration*.

2.5.2.3. LDAP Configuration

After adding or discovering devices, you can configure LDAP for single sign-on. Click **Configure LDAP** to display the LDAP Configuration wizard. For detailed setup procedures and information, see the section titled "Configuring LDAP" in *Resource Manager Administration*.

Chapter 3. Installing for RHEL 6 or CentOS 6

This chapter provides detailed instructions for installing Resource Manager for RHEL 6 or CentOS 6.

Before installing Resource Manager, you must:

- Ensure your system meets all requirements
- Install required software and packages

Unless otherwise directed, perform all steps as the root user.

3.1. Requirements

Ensure that your system meets all hardware requirements, and that you have correctly configured your operating system and hard drive partitions.

Note

Zenoss recommends that you install the CentOS 6 Basic Server package. The Minimal CentOS 6 installation lacks needed packages, such as openssh-client.

In addition, make sure that:

- You have disabled SELinux
- You have removed OpenJDK (included in the CentOS 6 Basic Server package)
- The `/opt/zenoss` directory is not a symbolic link to another location
- The umask is set to 022 (masks write permissions for group and others)
- The `/home` directory is writable by root, or the `/home/zenoss` directory exists as the zenoss user home directory
- You are connected to the Internet
- DNS is accessible

3.2. Required Software

Important! This chapter may not define all required packages for your installation options. While installing one or more software packages, you may be prompted to install additional, required software. Zenoss recommends that you install that software as directed.

The following table lists software dependencies for this version.

Package	Version
/bin/bash	3.2 or later
/bin/sh	
binutils	
dmidecode	
erlang	R12B
glibc-devel	2.5 or later
gnupg	
jre	1.6.0 or later
libaio	
libcrypto.so.10()(64bit)	

Package	Version
libcrypt.so.1()(64bit)	
libcrypt.so.1(GLIBC_2.2.5)(64bit)	
libc.so.6()(64bit)	
libc.so.6(GLIBC_2.2.5)(64bit)	
libc.so.6(GLIBC_2.3.2)(64bit)	
libc.so.6(GLIBC_2.3.4)(64bit)	
libc.so.6(GLIBC_2.3)(64bit)	
libc.so.6(GLIBC_2.4)(64bit)	
libdl.so.2(GLIBC_2.2.5)(64bit)	
liberation-fonts-common	
liberation-mono-fonts	
liberation-sans-fonts	
liberation-serif-fonts	
libexslt.so.0()(64bit)	
libgcc_s.so.1()(64bit)	
libgcc_s.so.1(GCC_3.0)(64bit)	
libgcj	
libgomp	
liblber-2.4.so.2()(64bit)	
libldap_r-2.4.so.2()(64bit)	
libm.so.6()(64bit)	
libm.so.6(GLIBC_2.2.5)(64bit)	
libncursesw.so.5()(64bit)	
libnsl.so.1()(64bit)	
libnsl.so.1(GLIBC_2.2.5)(64bit)	
libpanelw.so.5()(64bit)	
libpcre.so.0()(64bit)	
libprotobuf-lite.so.7()(64bit)	
libprotobuf.so.7()(64bit)	
libprotoc.so.7()(64bit)	
libpthread.so.0()(64bit)	
libpthread.so.0(GLIBC_2.2.5)(64bit)	
libreadline.so.6()(64bit)	
librrd.so.4()(64bit)	
librt.so.1()(64bit)	
libsasl2.so.2()(64bit)	
libsmi.so.2()(64bit)	
libssl.so.10()(64bit)	
libstdc++.so.6()(64bit)	
libstdc++.so.6(CXXABI_1.3)(64bit)	
libstdc++.so.6(GLIBCXX_3.4.10)(64bit)	

Package	Version
libstdc++.so.6(GLIBCXX_3.4.11)(64bit)	
libstdc++.so.6(GLIBCXX_3.4)(64bit)	
libstdc++.so.6(GLIBCXX_3.4.9)(64bit)	
libutil.so.1()(64bit)	
libutil.so.1(GLIBC_2.2.5)(64bit)	
libxml2.so.2()(64bit)	
libxml2.so.2(LIBXML2_2.4.30)(64bit)	
libxml2.so.2(LIBXML2_2.5.2)(64bit)	
libxml2.so.2(LIBXML2_2.5.7)(64bit)	
libxml2.so.2(LIBXML2_2.5.7)(64bit)	
libxml2.so.2(LIBXML2_2.5.8)(64bit)	
libxml2.so.2(LIBXML2_2.5.9)(64bit)	
libxml2.so.2(LIBXML2_2.6.0)(64bit)	
libxml2.so.2(LIBXML2_2.6.14)(64bit)	
libxml2.so.2(LIBXML2_2.6.15)(64bit)	
libxml2.so.2(LIBXML2_2.6.1)(64bit)	
libxml2.so.2(LIBXML2_2.6.17)(64bit)	
libxml2.so.2(LIBXML2_2.6.20)(64bit)	
libxml2.so.2(LIBXML2_2.6.21)(64bit)	
libxml2.so.2(LIBXML2_2.6.2)(64bit)	
libxml2.so.2(LIBXML2_2.6.32)(64bit)	
libxml2.so.2(LIBXML2_2.6.3)(64bit)	
libxml2.so.2(LIBXML2_2.6.5)(64bit)	
libxslt	1.1 or later
libxslt.so.1()(64bit)	
libxslt.so.1(LIBXML2_1.0.11)(64bit)	
libxslt.so.1(LIBXML2_1.0.18)(64bit)	
libxslt.so.1(LIBXML2_1.0.22)(64bit)	
libxslt.so.1(LIBXML2_1.0.24)(64bit)	
libxslt.so.1(LIBXML2_1.1.2)(64bit)	
libxslt.so.1(LIBXML2_1.1.26)(64bit)	
libxslt.so.1(LIBXML2_1.1.9)(64bit)	
libz.so.1()(64bit)	
memcached	1.4.4
nagios-plugins	1.4.15 or later
nagios-plugins-dig	1.4.15 or later
nagios-plugins-dns	1.4.15 or later
nagios-plugins-http	1.4.15 or later
nagios-plugins-ircd	1.4.15 or later
nagios-plugins-ldap	1.4.15 or later
nagios-plugins-ntp	1.4.15 or later

Package	Version
nagios-plugins-perl	1.4.15 or later
nagios-plugins-ping	1.4.15 or later
nagios-plugins-rpc	1.4.15 or later
nagios-plugins-tcp	1.4.15 or later
net-snmp	5.3.2.2-9 or later
net-snmp-utils	5.3.2.2-9 or later
ncurses	5.5 or later
openldap	2.3 or later
openssl	
patch	
pcre	6.6 or later
pkgconfig	
python	2.3.4 or later
rabbitmq-server	2.8.6 or later
readline	5.1 or later
rpmlib(CompressedFileNames)	3.0.4-1 or later
rpmlib(PayloadFilesHavePrefix)	4.0-1 or later
rpmlib(VersionedDependencies)	3.0.3-1 or later
rrdtool	1.4.7 or later
rsync	
rtld(GNU_HASH)	
shadow-utils	
sysstat	
zends	5.5.25a
zlib	1.2 or later

3.3. Prerequisite Tasks

Before installing Resource Manager, you must:

- Configure your firewall
- Remove conflicting messaging systems
- Download the installation files
- Install and configure the software repository, prerequisite software, and additional packages, including:
  - Oracle Java
  - Zenoss dependencies repository
  - RabbitMQ
  - memcached and snmpd
  - Zenoss DataStore

3.3.1. Configure Your Firewall

Resource Manager requires these ports be open in your firewall:

Port	Protocol	Direction to Resource Manager Server	Description
11211	TCP | UDP	Inbound	memcached
8080	TCP	Outbound	Web interface
514	UDP	Inbound	syslog
162	UDP	Inbound	SNMP Traps

Table 3.1. Ports

Alternatively, you can disable your firewall:

- For IPv4, use these commands:

```
service iptables stop
chkconfig iptables off
```

- For IPv6, use these commands:

```
service ip6tables stop
chkconfig ip6tables off
```

3.3.2. Remove Conflicting Messaging Systems

Zenoss CSA relies on the RabbitMQ messaging system. Newer versions of CentOS include alternative messaging systems (Matahari and Qpid). You must remove these messaging systems to run Zenoss CSA.

1. Use the following commands to determine if Matahari or Qpid packages are installed on your system:

```
rpm -qa | egrep -i "matahari|qpid"
```

2. Remove all listed packages:

```
yum erase Package1 Package2 ...
```

3.3.3. Download the Installation Files

1. Browse to the following URL:

   https://support.zenoss.com

   Note

   Contact your Zenoss representative for site login credentials.

2. In the Downloads area of the Home tab, locate the current Service Dynamics installation files.
3. Download the Resource Manager and (optionally) Windows ZenPacks RPM files.

3.3.4. Install Oracle Java

Follow these steps to install and configure Oracle Java.

Note

OpenJDK is not supported for Zenoss CSA. If you have OpenJDK or another Java version installed, then remove those installations before installing the required Oracle Java version.

1. Download Oracle JRE:

```
wget -O jre-6u31-linux-x64-rpm.bin \
 http://javadl.sun.com/webapps/download/AutoDL?BundleId=59622
```

2. Change mode:

```
chmod +x ./jre-6u31-linux-x64-rpm.bin
```

3. Install Oracle JRE:

```
./jre-6u31-linux-x64-rpm.bin
```

4. Add the following line to the end of the `/etc/profile` file:

```
export JAVA_HOME=/usr/java/default/bin
```

5. Verify the correct installed version (1.6 Update 31):

```
java -version
```

3.3.5. Install the Zenoss Dependencies Repository

Install the Zenoss dependencies repository:

```
rpm -ivh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el6.noarch.rpm
```

3.3.6. Install RabbitMQ

Use the following commands to install and configure RabbitMQ:

1. Install RabbitMQ:

```
yum -y install rabbitmq-server-2.8.6
```

2. Start the `rabbitmq-server` daemon and configure it to start automatically on reboot:

```
service rabbitmq-server start
chkconfig rabbitmq-server on
```

3.3.7. Install and Configure memcached and snmpd

Use these commands to install and configure the `memcached` and `snmpd` daemons:

1. Install memcached and net-snmp:

```
yum -y install memcached net-snmp net-snmp-utils
```

2. Start the `memcached` daemon and configure it to start automatically on reboot:

```
service memcached start
chkconfig memcached on
```

3. Start the `snmpd` daemon and configure it to start automatically on reboot:

```
service snmpd start
chkconfig snmpd on
```

3.3.8. Install the Zenoss DataStore

You can employ the Zenoss DataStore on a local or remote server. Resource Manager requires certain features provided by the data store, so even if you plan to use a remote server, you must install it on the local server as well. (You can, however, save resources by not running the main service.)

Perform these steps on the local Resource Manager server:

1. Browse to this URL:

   https://support.zenoss.com

   Note

   Contact your Zenoss representative for site login credentials.

2. In the Downloads area of the Home tab, locate and download the Zenoss DataStore RPM files.
3. Install the Zenoss DataStore:

```
yum --nogpgcheck localinstall zends-5.5.25a-1.Version.el6.x86_64.rpm
```

4. Start the data store and ensure it runs at system startup:

```
service zends start
chkconfig --level 2345 zends on
```

3.4. Install and Configure Resource Manager

Follow these steps to install the Resource Manager software and ZenPacks, and (optionally) a remote Zenoss DataStore.

3.4.1. Install the Resource Manager RPM

Install the Resource Manager RPM file:

```
yum -y --nogpgcheck localinstall zenoss_resmgr-Version.el6.x86_64.rpm
```

3.4.2. (Optional) Install a Remote Zenoss DataStore

Follow these steps to install and configure a remote data store.

1. On the local Resource Manager server:
   a. Stop the data store and configure it so that it will not run at system startup:

      ```
      service zends stop
      chkconfig --level 2345 zends off
      ```

   b. As the zenoss user, change the values of these entries in the `$ZENHOME/etc/global.conf.example` file:
      - zodb-host - Change the value from "localhost" to the name or IP address of the remote server.
      - zep-host - Change the value from "localhost" to the name or IP address of the remote server.
      - zodb-port - Change the value from 3306 to 13306
      - zep-port - Change the value from 3306 to 13306
2. On the remote server:
   a. Download the Zenoss DataStore RPM files.
   b. Install the Zenoss DataStore:

      ```
      yum --nogpgcheck localinstall zends-5.5.25a-1.Version.el6.x86_64.rpm
      ```

   c. Start the data store and ensure it runs at system startup:

      ```
      service zends start
      chkconfig --level 2345 zends on
      ```

   d. Change to the zenoss user:

      ```
      su - zenoss
      ```

   e. Enter the following command:

      ```
      zends -u root
      ```

   f. Enable remote access to the Zenoss DataStore. In the prompt that appears, enter this series of commands:

      ```
      grant all on *.* to 'root'@'%' with grant option;
      flush privileges;
      ```

3.4.3. Install MySQLTuner

Follow these steps to download and install the MySQLTuner Perl script:

1. As the zenoss user, log in to a shell account on the master Resource Manager server.
2. Change to the following directory:

```
cd $ZENHOME/bin
```

3. Retrieve the MySQLTuner script:

```
wget mysqltuner.pl
```

4. Change read and execute access to the file:

```
chmod 755 mysqltuner.pl
```

3.4.4. Start the System

Run the following command to start the system:

```
service zenoss start
```

3.4.5. (Optional) Install the Windows Monitoring ZenPack

Optionally enable Windows monitoring:

1. Stop the system:

```
service zenoss stop
```

2. Install the msmonitor RPM file:

```
yum -y --nogpgcheck localinstall zenoss_msmonitor-Version.el6.x86_64.rpm
```

3. Restart the system:

```
service zenoss restart
```

3.5. Getting Started

After installation, use your Web browser to browse to the valid host name of the server where Resource Manager is installed.

Note

If you cannot successfully browse to your Resource Manager installation, then you may need to add an entry to your hosts file for the fully qualified domain name (FQDN) of your installation.

If you are using Internet Explorer to view the Resource Manager interface, and you have restricted the browser to trusted sites, then a warning message may appear. To prevent this, add your Resource Manager installation to the Trusted zone. These Microsoft articles provide more information on setting up trusted sites:

- Pre-Windows 7: http://support.microsoft.com/kb/174360
- Windows 7: http://windows.microsoft.com/en-US/windows7/Security-zones-adding-or-removing-web-sites

The setup wizard appears.

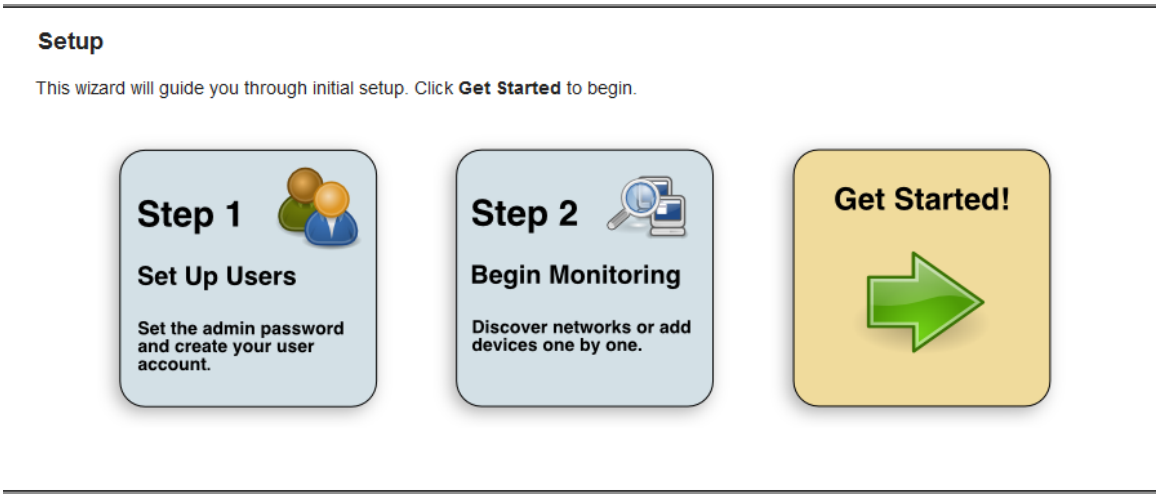

Figure 3.1. Setup Wizard

Using this wizard, you will:

- Change the admin password
- Set up an initial user
- Add some devices to the system
- Configure LDAP (optional)

From the first panel of the wizard, click **Get Started!** to begin.

The Step 1: Set up Initial Users panel appears.

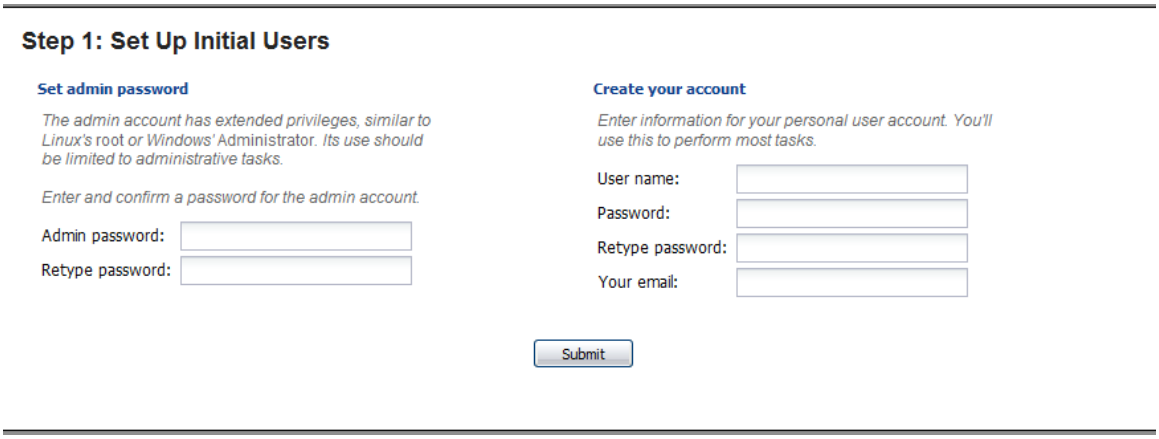

Figure 3.2. Setup Wizard: Step 1

3.5.1. Set the Administrative Password and Create a User

Follow these steps to select a password for the admin account and create your user account.

1. In the **Set admin password area**, enter and confirm a new admin password. You must enter a password value to continue.

   Note

   The Resource Manager admin account has extended privileges, and its use should be limited. Be sure to record the admin password and store it securely.

2. In the **Create your account** area, set up your Resource Manager user account. Most of the time, you will use this account to perform management tasks in Resource Manager. Enter a unique user name, password, and email address.

3. Click **Submit**.

   The Step 2: Specify or Discover Devices to Monitor panel appears.

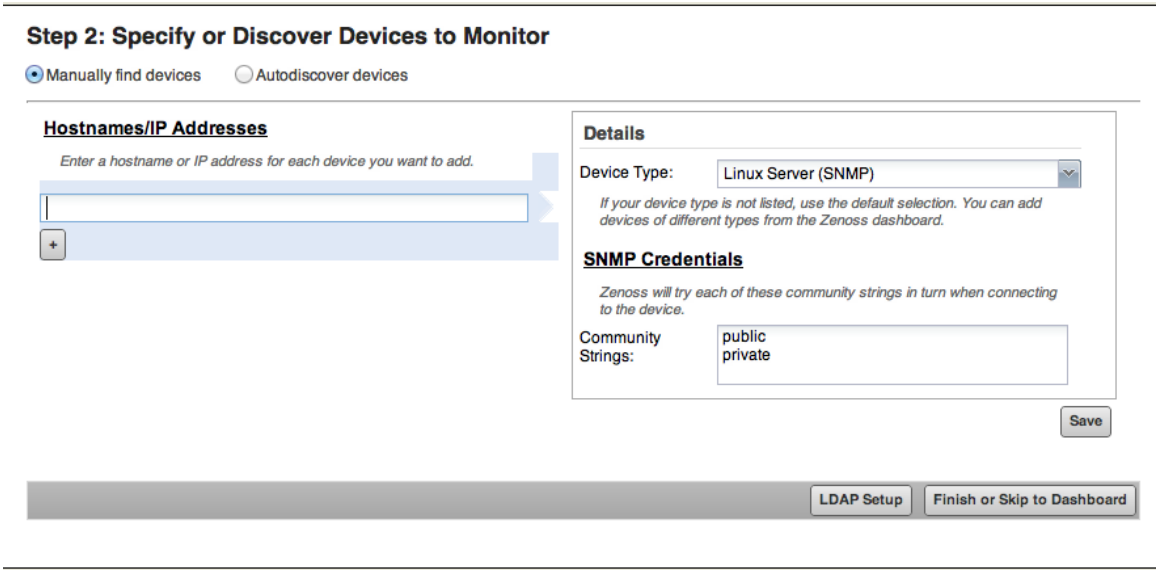

Figure 3.3. Setup Wizard: Step 2 (Manual Add)

3.5.2. Add Devices

You can add devices manually, or give Resource Manager network or IP address range information so it can discover your devices.

3.5.2.1. Adding Devices Manually

Follow these steps to manually add devices to the system. For each device you want to add:

1. Enter a fully qualified domain name or IP address
2. In the Details area, select a device type from the list. If your device type is not listed, then use the default selection. (You can change device classes for a device later, as well as add device classes.)
3. Enter the appropriate credentials used to authenticate against the device.

   Note

   For more information about setting credentials, refer to *Resource Manager Administration*.
4. To add the devices, click **Submit**.

   Resource Manager models the devices in the background.

   Note

   You can bypass device addition through the wizard. Click **Skip to the dashboard** to go directly to the Resource Manager Dashboard. Later, you can add devices by following the steps outlined in *Resource Manager Administration*.

3.5.2.2. Discovering Devices

To discover devices:

1. Select the **Autodiscover devices** option.

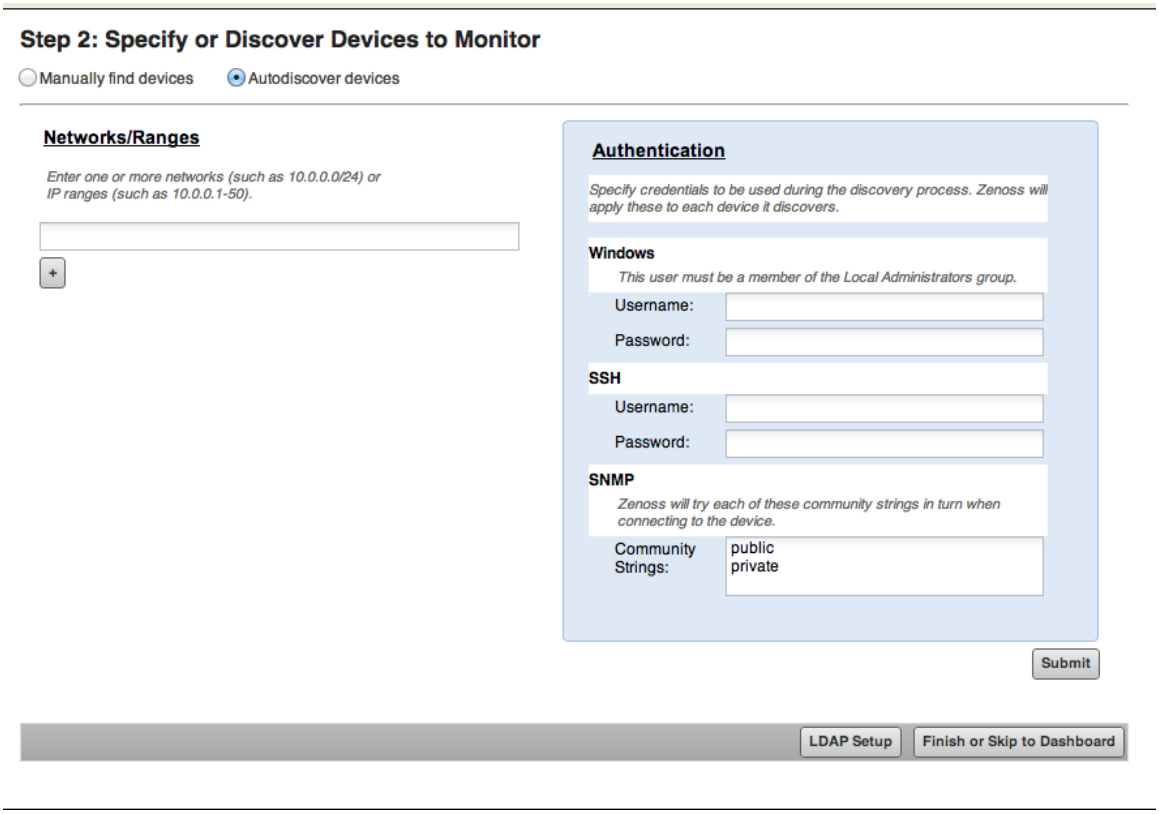

Figure 3.4. Setup Wizard: Step 2 (Discovery)

2. For each network or IP range in which you want Resource Manager to discover devices, enter an address or range. For example, you might enter a network address in CIDR notation:

   10.175.211.0/24

   or as a range of IP addresses:

   10.175.211.1-50
3. If you want to enter multiple addresses or ranges, click +. For each network, you must enter a netmask or IP range.
4. For each network or IP range, specify the Windows, SSH, or SNMP credentials you want Resource Manager to use on the devices it discovers. You can enter only one of each. Resource Manager attempts to use the same credentials on each device it discovers within the networks or IP ranges specified.
5. Click **Discover**.

   Resource Manager schedules jobs to discover devices in the networks and IP ranges you specified. (To see job status, navigate to Advanced > Settings, and then select Jobs in the left panel.)

   When discovery completes, a notification message appears in the Messages portlet on the Dashboard.

   Note

   You can bypass device discovery through the wizard. Click **Skip to the dashboard** to go directly to the Resource Manager Dashboard. Later, you can discover devices by following the steps outlined in *Resource Manager Administration*.

3.5.2.3. LDAP Configuration

After adding or discovering devices, you have the option to configure LDAP for single sign-on. Click **Configure LDAP** to display the LDAP Configuration wizard. For detailed setup procedures and information, see the section titled "Configuring LDAP" in *Resource Manager Administration*.

Chapter 4. Installing the RPM-Based ISO Appliance

This chapter provides instructions for installing the ISO appliance:

- In a VMware virtual environment
- On physical hardware

4.1. Installing the Appliance in a Virtual Environment

This section describes how to install a VMware-ready ISO into an ESX guest.

4.1.1. System Requirements

Refer to Chapter 1, "Installation Considerations," for minimum hardware requirements. You must configure the ESX guest according to the minimum hardware requirements for the number of devices you plan to monitor.

4.1.2. Limitations

When installing the ISOs through VMware Player or VMware Fusion, the VMware wizard will, by default, attempt to create and configure a user. To install successfully, you must de-select this option.

4.1.3. Download the Installation Files

1. Browse to the following URL:

   https://support.zenoss.com

   Note

   Contact your Zenoss representative for site login credentials.
2. In the Downloads area of the Home tab, locate the current Service Dynamics installation files.
3. Download the Resource Manager and (optionally) Windows ZenPacks RPM files.

4.1.4. Installing the Appliance

Follow these steps to download and install the appliance in a virtual environment.

1. Browse to the following URL:

   https://support.zenoss.com

   Note

   Contact your Zenoss representative for site login credentials.
2. In the Downloads area of the Home tab, locate and download this file:

   `zenoss_resmgr-`*Version*`.x86_64.vmware.iso`
3. Open your vSphere client.
4. Right-click the ESX server where you want to create the virtual machine, and then select New Virtual Machine.

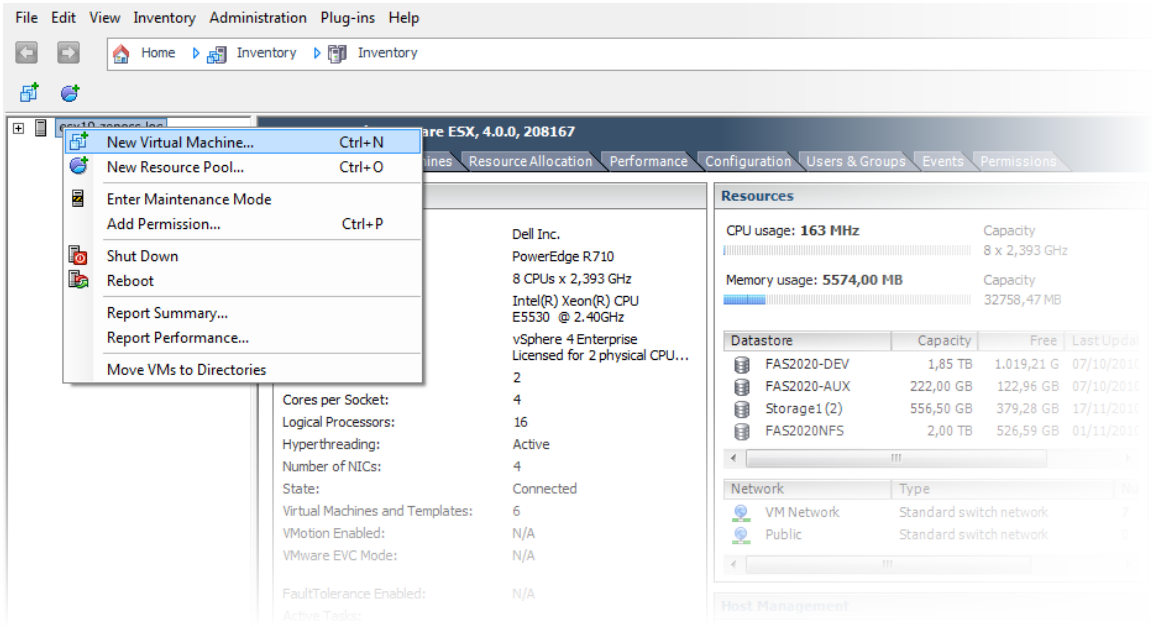

Figure 4.1. New Virtual Machine

The Create New Virtual Machine Configuration panel appears.

5. Select the Custom option, and then click **Next**.

   The Name and Location panel appears.

6. Enter a valid name for your server, and then click **Next**.

   The Datastore panel appears.

7. Select a data source on which the virtual machine will be stored, and then click **Next**.

   The Virtual Machine Version panel appears.

8. Select the Virtual Machine Version 7 option, and then click **Next**.

   The Guest Operating System panel appears.

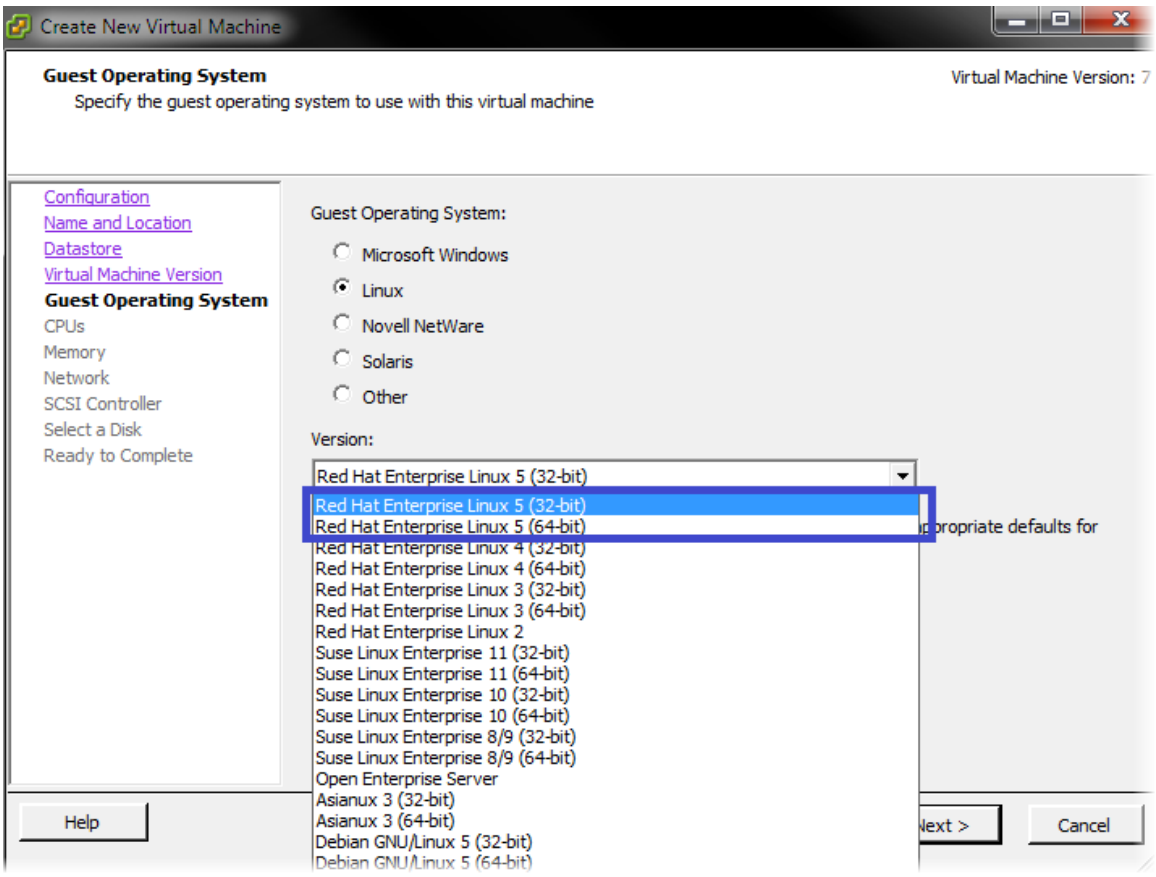

Figure 4.2. Guest Operating System Selection

9. Select Linux, and then select Red Hat Enterprise Linux 5 (64-bit). Click **Next**.

   The CPUs panel appears.

10. Select the number of virtual processors, and then click **Next**.

    The Memory panel appears.

11. Select a memory value, and then click **Next**. Refer to Chapter 1, "Installation Considerations," for recommended minimum memory configurations.

    The Network panel appears.

12. Use the default setting. Click **Next**.

    The SCSI Controller panel appears.

13. Use the default settings. Click **Next**.

    The Select a Disk panel appears.

14. Select Create a new virtual disk, and then click **Next**.

    The Create a Disk panel appears.

15. In the Capacity area, adjust the disk size. 60GB is the recommended minimum. Click **Next**.

    The Advanced Options panel appears.

16. Click **Next**, and then click **Finish**.
17. When the virtual machine is ready, right-click it, and then select Open Console.

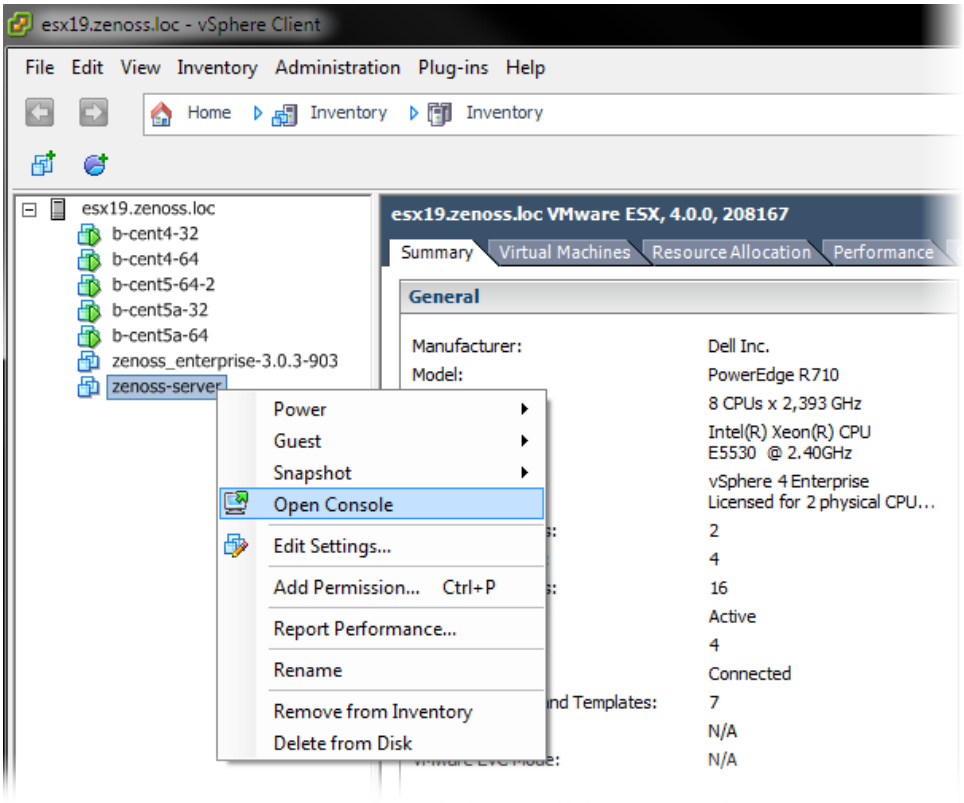

Figure 4.3. Open Console

The console starts.

18. Click **Play**, and then click the CD icon.
19. Select CD/DVD Drive 1, and then select Connect to ISO image on local disk.
20. Browse your local disk and select the ISO image, and then click **Open**.
21. Click inside the console to take control of the virtual machine, and then press [Control] + [ALT] + [INSERT] on your keyboard to reboot it and start loading the `.iso` file.

    The initial Zenoss screen appears.

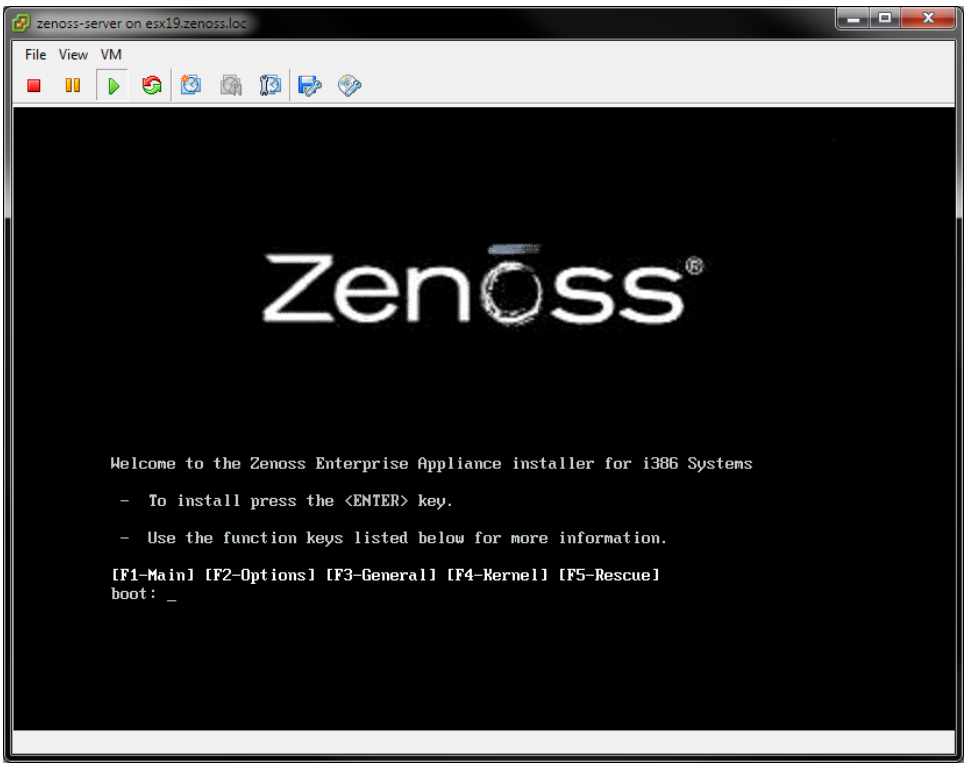

Figure 4.4. Zenoss - Initial Screen

22. Press Enter to begin installation.

    The Keyboard Type screen appears.

23. Select your keyboard, and then click **OK**.

    A warning message appears.

Figure 4.5. Warning

24. Click **Yes** (initialize the drive).

    The Partitioning screen appears.

25. Select Default Layout, and then click **Next**.

    The GRUB screen appears.

26. Click **Next**.

    The Network Devices screen appears.

27. Optionally adjust network settings, and then click **Next**.

The Timezone screen appears.

28. Select the correct timezone for your location, and then click **Next**.

    The Root Password screen appears.

29. Enter and confirm a root password, and then click **Next**.
30. The ISO installs packages and continues with installation. When installation completes, the system automatically restarts.

    After restart, the system displays a message similar to:

    ```
    Welcome to Zenoss

    To access the Zenoss Management Console, please browse to:

    http://xxx.xxx.xxx:8080
    ```

    Note

    If this message does not appear, then you may need to change the VMware player network connection option from Bridged to NAT.

31. Log in as user `root`. The default root password is `zenoss`.
32. Open a new Web browser, and then enter the URL that appears in the login screen.

    The Setup Wizard appears.

4.1.4.1. What's Next?

After installing the system, go to the section titled "Getting Started" in one of the chapters titled "Installing for RHEL or CentOS" in this guide. There you will find instructions for initial setup tasks and basic information to help you begin using the system.

4.2. Installing the Appliance on Hardware

This section describes how to install the appliance on a bare-metal server.

4.2.1. System Requirements

Refer to Chapter 1, "Installation Considerations," for minimum hardware requirements. You must size the server according to the minimum hardware requirements for the number of devices you plan to monitor.

4.2.2. Installing the Appliance

Follow these steps to download and install the appliance on physical hardware.

1. Download and save the following file from the Zenoss Support download site (http://support.zenoss.com/download):

   `zenoss_resmgr-`*Version*`.x86_64.iso`

   Note

   Contact your Zenoss representative for site login credentials.

2. Burn the `.iso` file to CD or DVD media.
3. Power on your system, place the media in the CD/DVD reader, and then reboot the system.

Note

If the system does not boot with the media, then you may need to adjust the boot order on your system BIOS setting. Make CD/DVD the first option, and then boot the system again.

The `.iso` file loads automatically and requests the following information.

a. Select the installation language, and then click **Next**.
b. Select the keyboard language, and then click **Next**.

   The Graphical Installation screen appears.
c. Select Yes to activate the hard disk, and then click **Next**.

   The Partitioning screen appears.
d. Select Default Layout, and then click **Next**.
e. Adjust network settings, and then click **Next**.
f. Set your timezone, and then click **Next**.
g. Set the password for the root account, and then click **Next**.

The ISO installs packages and continues with installation. When installation completes, the system automatically restarts.

After restart, the system displays a message similar to:

```
Welcome to Zenoss

To access the Zenoss Management Console, please browse to:

http://xxx.xxx.xxx:8080
```

4. Log in as user `root`. The default root password is `zenoss`.
5. Open a new Web browser, and then enter the URL that appears in the login screen.

   The Resource Manager Setup Wizard appears.

4.2.2.1. What's Next?

After installing the system, go to the section titled "Getting Started" in the chapter titled "Installing for RHEL 5 or CentOS 5" in this guide. There you will find instructions for initial setup tasks and basic information to help you begin using the system.

Chapter 5. Installing Collectors and Hubs

Read this chapter for information and procedures to help you install collectors and hubs.

Note

Not all deployments will benefit from a distributed collector setup. For detailed information about deploying and using distributed collectors, refer to the chapter titled "Distributed Collector" in Zenoss Service Dynamics Resource Management Extended Monitoring.

5.1. Deploying Collectors

The following sections offer information and procedures for:

- Installing prerequisite packages
- Deploying remote collectors
- Deploying local collectors

5.1.1. Install Required Software

Before deploying, confirm that the correct versions of required software are installed.

For a list of required software and installation procedures, refer to the sections titled "Required Software" and "Prerequisite Tasks" in one of the following chapters of this guide:

- Installing for RHEL 5 or CentOS 5
- Installing for RHEL 6 or CentOS 6

5.1.2. Deploying Remote Collectors

The following sections provide detailed information needed to deploy remote collectors:

- Requirements
- Limitations
- Overriding Daemons
- Prerequisite Tasks
- Deployment

5.1.2.1. Requirements

Remote collector deployments must meet these requirements:

- The operating system running on the server to be deployed as a remote collector must be the same version and platform as that running on the Resource Manager master. (For example, if your Resource Manager master is CentOS 5 64-bit, then the collector must also be CentOS 5 64-bit.)
- The Resource Manager server host name must be a resolvable, fully qualified domain name or IP address.
- You must update all collectors after you:
  - Update your version of Resource Manager
  - Install patches
  - Install, update, or remove ZenPacks
  - Change the ZenHub port of an associated hub

5.1.2.2. Limitations

The system is not compatible with Security-Enhanced Linux (SELinux) in enforcing mode. You must disable enforcing mode for all platforms running the Resource Manager daemons (Resource Manager master, remote hubs, and remote collectors).

To disable enforcing mode:

1. Edit the /etc/selinux/config file.
2. Set the following line:

```
SELINUX=disabled
```

Note

You also can disable enforcing mode temporarily (avoiding the need to reboot) with the command:

```
echo 0 > /selinux/enforce
```

For more information about SELinux, browse to http://en.wikipedia.org/wiki/SELinux, or to the SELinux home page at http://www.nsa.gov/research/selinux/index.shtml.

5.1.2.3. Overriding Daemons on Remote Collectors

You can optionally specify which daemons are configured on a remote collector. Only the listed daemons are configured at deployment.

Before deploying the remote collector (or when reconfiguring an existing collector):

1. Create a `$ZENHOME/etc/collectordaemons.txt` file.
2. Add the names of daemons you want to configure on the remote collector. List one daemon on each line, using the real daemon name (such as zencommand or zenperfsnmp).

Note

Alternatively, you can add a `collectordaemons.txt` file on each remote machine. These files will be used instead of the file on the localhost.

5.1.2.4. Prerequisite Tasks

Before deploying a remote collector, you must:

- Configure your firewall
- Install Oracle Java
- Install the Zenoss dependencies repository
- Install RRDtool
- Install Nagios plugins

5.1.2.4.1. Configure Your Firewall

The following ports must be open in your firewall:

Port	Protocol	Direction to Resource Manager Server	Description
8080	TCP	Outbound	Web interface
514	UDP	Inbound	syslog
162	UDP	Inbound	SNMP Traps
8789	TCP	Inbound and outbound	ZenHub communication

Port	Protocol	Direction to Resource Manager Server	Description
8091	TCP	Inbound	zenrender

Table 5.1. Ports

5.1.2.4.2. Install the Zenoss Dependencies Repository

Install the Zenoss dependencies repository. Use one of the following commands.

- RHEL 5 or CentOS 5:

```
rpm -ivh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el5.noarch.rpm
```

- RHEL 6 or CentOS 6:

```
rpm -ivh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el6.noarch.rpm
```

5.1.2.4.3. Install Oracle Java

Follow these steps to install and configure Oracle Java.

Note

OpenJDK is not supported for Resource Manager. If you have OpenJDK or another Java version installed, then remove those installations before installing the required Oracle Java version.

1. Download Oracle JRE:

```
wget -O jre-6u31-linux-x64-rpm.bin \
 http://javadl.sun.com/webapps/download/AutoDL?BundleId=59622
```

2. Change mode:

```
chmod +x ./jre-6u31-linux-x64-rpm.bin
```

3. Install Oracle JRE:

```
./jre-6u31-linux-x64-rpm.bin
```

4. Add the following line to the end of the `/etc/profile` file:

```
export JAVA_HOME=/usr/java/default/bin
```

5. Verify the correct installed version (1.6 Update 31):

```
java -version
```

5.1.2.4.4. Install and Configure RRDtool

Enter the following command to install RRDtool:

```
yum -y install rrdtool-1.4.7
```

5.1.2.4.5. Install the Nagios Plugins

Enter the following command to download and install the Nagios plugins:

```
yum install nagios-plugins nagios-plugins-dig nagios-plugins-dns \
nagios-plugins-http nagios-plugins-ircd nagios-plugins-ldap \
nagios-plugins-ntp nagios-plugins-perl nagios-plugins-ping nagios-plugins-rpc \
nagios-plugins-tcp
```

5.1.2.5. Deployment

Follow these steps to deploy a remote collector:

1. Browse to the Resource Manager master, and then log in to the user interface.
2. Select Advanced > Collectors from the navigation bar.

3. Click the name of the hub for your Resource Manager master. (In a default installation, this is `localhost`.)
4. On the Overview page, select Add Collector from the Action menu.

   The Add Collector page appears. From here, you can use one of several methods to access the remote host.

5.1.2.5.1. Root User Password

Follow these steps to install a remote collector using a root password for access to the remote host.

Note

You must set a password for the root user on a server before deploying a collector to it.

1. Select the Install remotely option.
2. Select the root password option.

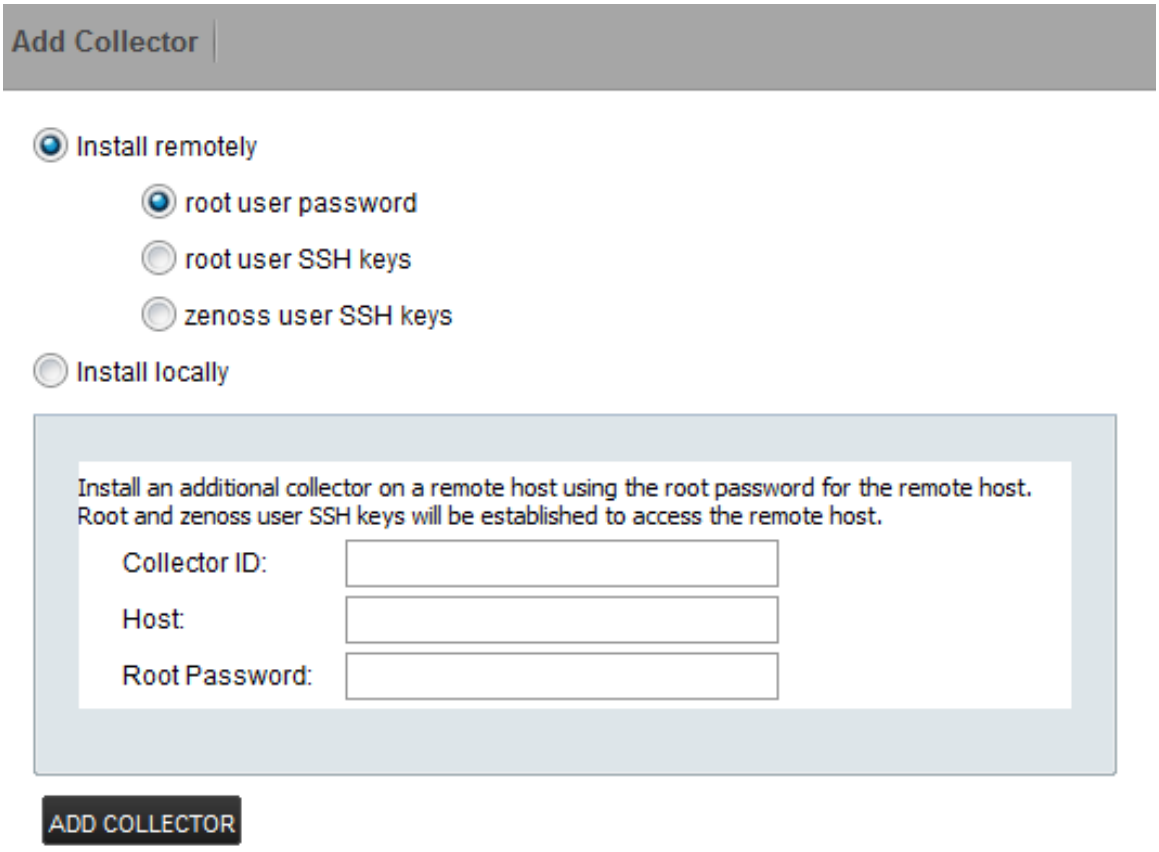

Figure 5.1. Install Remote Collector (Root Password)

3. Enter or change setup details:

Field Name	Description
Collector ID	Enter the name for the collector as it will be identified in the system. This name will be used to prefix the control scripts on the collector. If the ID is `coll1`, then scripts will be named `coll1_zenperfsnmp`.
Host	Enter the name of the host for the collector. This must be a fully qualified domain name, IP address, or resolvable host name.
Root Password	Enter the password for the root user on the Host. The root password is not stored; it is used to config-

Field Name	Description
	ure a pre-shared key between the main server and the remote collector.

Table 5.2. Add New Collector Fields

Note

If you are creating another collector on the server, enter the `localhost` rather than the IP address of the server.

4. Click **Add Collector**.

The system displays log output from the creation of the new collector. When fully configured (this may require several minutes), the system displays the final entry "navigate to *CollectorName*." Click the link to go to the overview page for the new collector.

5.1.2.5.2. Root SSH Keys

To install a remote collector, using existing root SSH keys for access to the remote host:

1. Select the Install remotely option.
2. Select the root SSH keys option.

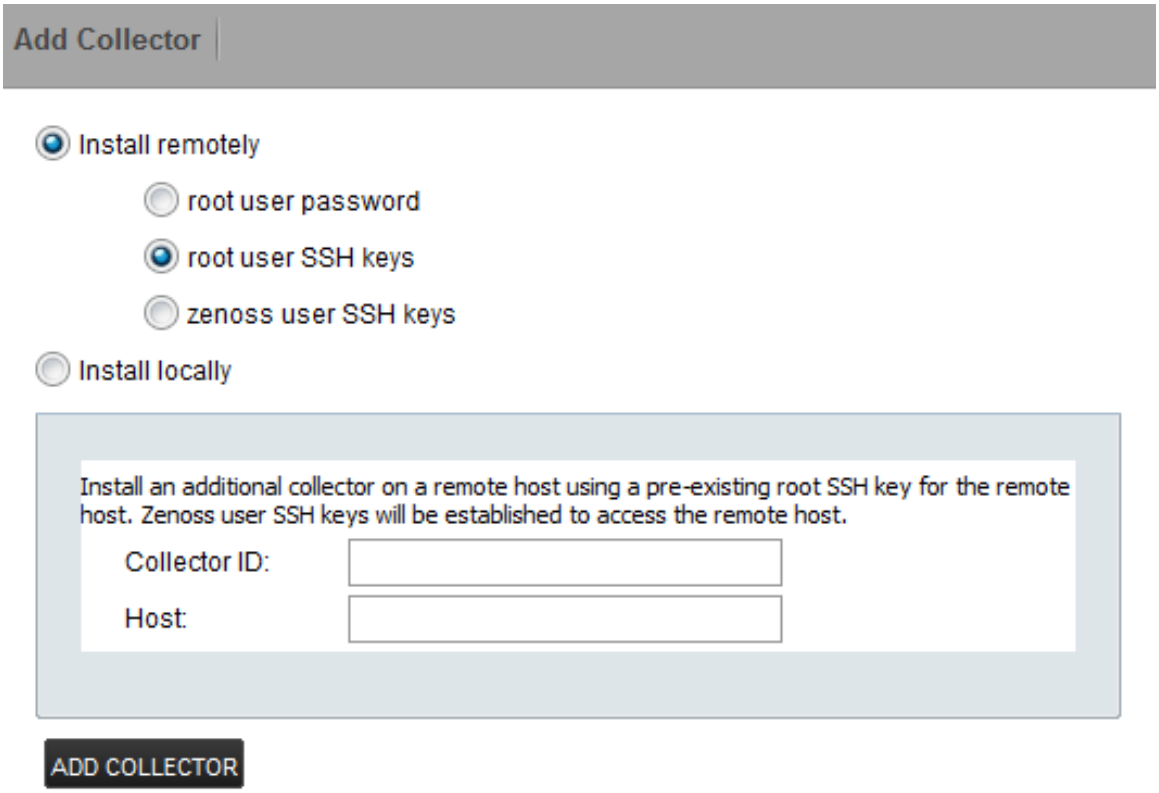

Figure 5.2. Install Remote Collector (Root SSH Keys)

3. Enter or change setup details:

Field Name	Description
Collector ID	Enter the name for the collector as it will be identified in the system. This name will be used to prefix the control scripts on the collector. If the ID is `coll1`, then scripts will be named `coll1_zenperfsnmp`.

Field Name	Description
Host	Enter the name of the host for the collector. This must be a fully qualified domain name, IP address, or resolvable host name.

Table 5.3. Add New Collector Fields

Note

If you are creating another collector on the server, enter the `localhost` rather than the IP address of the server.

4. Click **Add Collector**. The system displays log output from the creation of the new collector. When fully configured (this may require several minutes), the system displays the final entry "navigate to *CollectorName*." Click the link to go to the overview page for the new collector.

5.1.2.5.3. Resource Manager SSH Keys

If you choose to set up a collector using Resource Manager SSH keys, the system will attempt to install by using the zenoss user. To successfully install a collector using these keys (without root access), these prerequisite conditions must be met:

- zenoss user SSH keys must be set up between the Resource Manager server and the target.
- You must be running the RPM distribution.
- Resource Manager core RPM must be installed on the target (remote) machine.

Tip: When installing the RPM on the remote machine, **do not start** the system.

Follow these steps to install a remote collector, using Resource Manager SSH keys for access to the remote host.

Note

For detailed steps for creating SSH keys, see the section titled "Setting Up SSH Keys for Distributed Collector."

1. Select the Install remotely option.
2. Select the zenoss SSH Keys option.

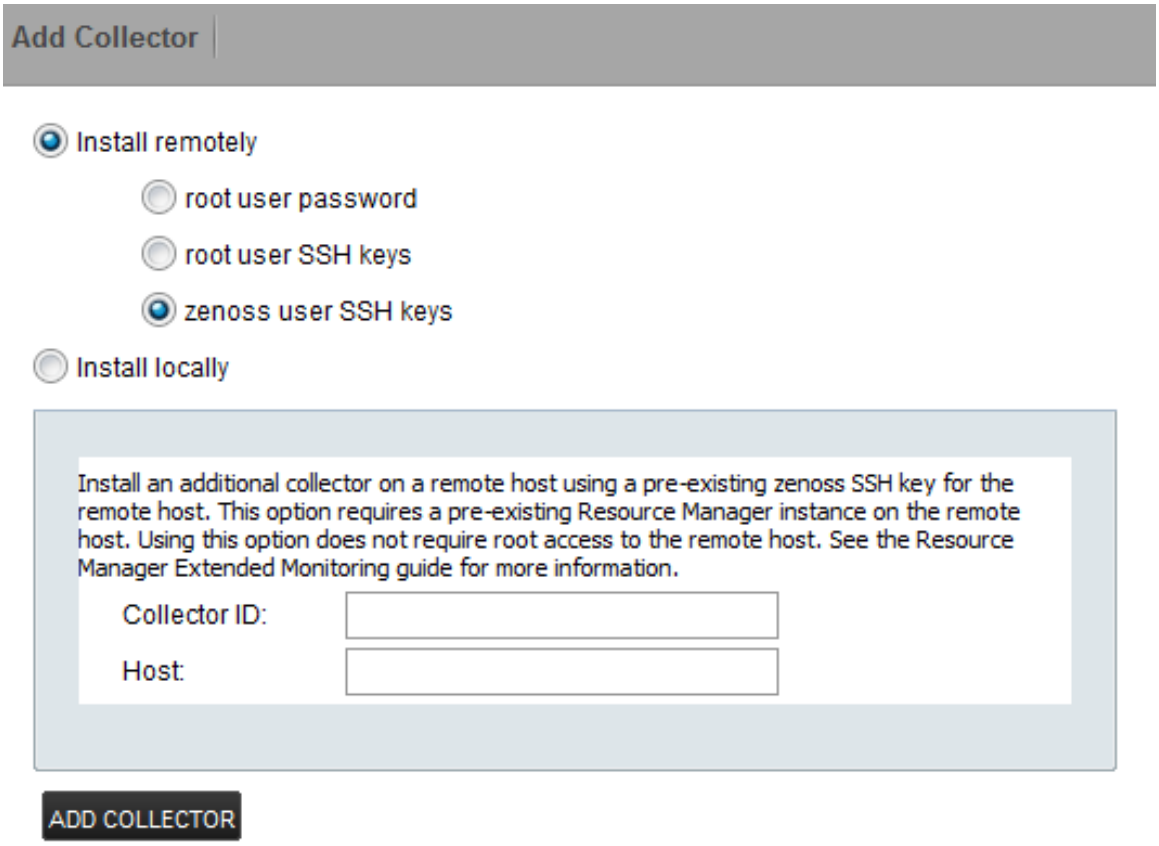

Figure 5.3. Install Remote Collector (Resource Manager SSH Keys)

3. Enter or change setup details:

Field Name	Description
Collector ID	Enter the name for the collector as it will be identified in the system. This name will be used to prefix the control scripts on the collector. If the ID is `coll1`, then scripts will be named `coll1_zenperfsnmp`.
Host	Enter the name of the host for the collector. This must be a fully qualified domain name, IP address, or resolvable host name.

Table 5.4. Add New Collector Fields

Note

If you are creating another collector on the server, enter the `localhost` rather than the IP address of the server.

4. Click **Add Collector**. The system displays log output from the creation of the new collector. When fully configured (this may require several minutes), The system displays the final entry "navigate to *CollectorName*." Click the link to go to the overview page for the new collector.

5.1.3. Deploying Local Collectors

Follow these steps to install a local collector:

1. Browse to the Resource Manager master, and then log in to the user interface.
2. Select Advanced > Collectors from the navigation bar.

3. Click the name of the hub for your Resource Manager master. (In a default installation, this is `localhost`.)
4. On the Overview page, select Add Collector from the Action menu.

   The Add Collector page appears.
5. Select the Install locally option.

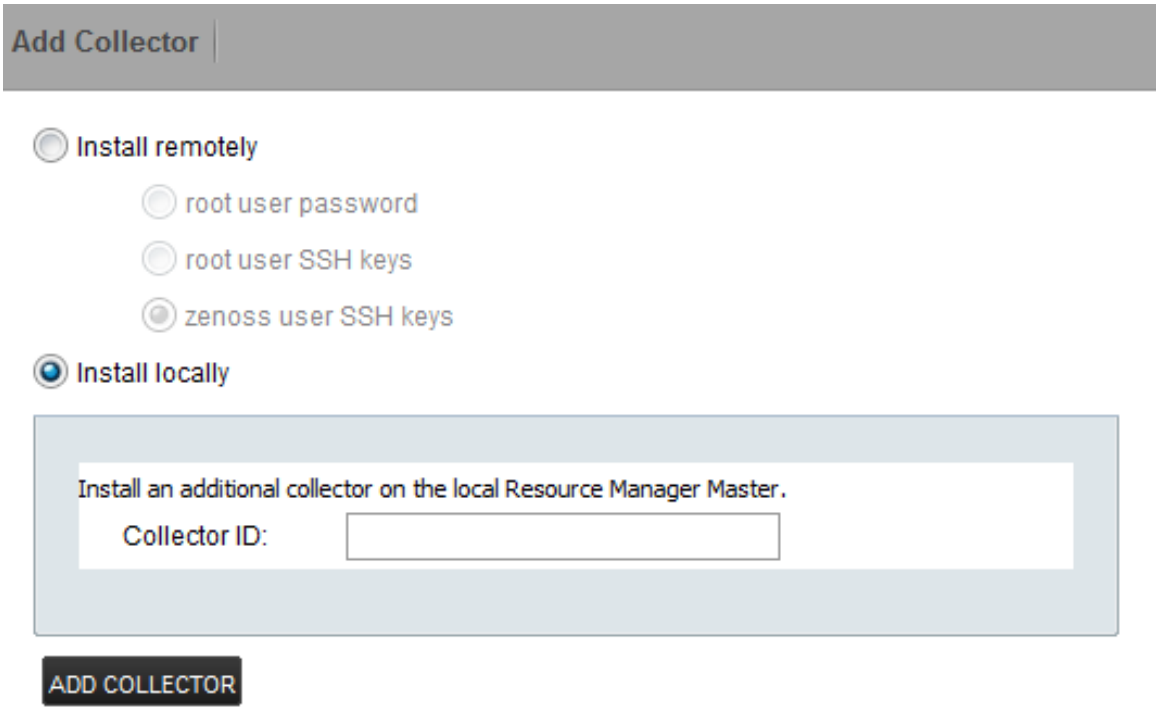

Figure 5.4. Install Locally

6. Enter or change setup details:

Field Name	Description
Collector ID	Enter the name for the collector as it will be identified in the system. This name will be used to prefix the control scripts on the collector. If the ID is `coll1`, then scripts will be named `coll1_zenperfsnmp`.

Table 5.5. Add New Collector Fields

7. Click **Add Collector**. The system displays log output from the creation of the new collector. When fully configured (this may require several minutes), click the link at the bottom of the page to go to the overview page for the new collector.

5.2. Deploying Hubs

The following sections offer information and procedures for:

- Installing prerequisite packages
- Deploying remote hubs

5.2.1. Install Prerequisite Software

Before deploying, confirm that the correct versions of required software are installed.

For a list of required software and installation procedures, refer to the sections titled "Required Software" and "Prerequisite Tasks" in one of the following chapters of this guide:

- Installing for RHEL 5 or CentOS 5
- Installing for RHEL 6 or CentOS 6

5.2.2. Deploying Remote Hubs

The following sections provide detailed information needed to deploy hubs:

- Requirements
- Limitations
- Configuring Zenoss DataStore
- Prerequisite Tasks
- Deployment

5.2.2.1. Requirements

Hub deployments must meet these requirements:

- The Resource Manager server host name must be a resolvable, fully qualified domain name or IP address.
- Any server hosting a remote hub must have the Zenoss DataStore installed (but not running). The Zenoss DataStore is needed for a client library that allows MySQL connections.
- Remote hubs need to communicate on these default Resource Manager ports:
  - Port 13306 - Zenoss DataStore
  - Port 8084 - Resource Manager events system
  - Port 5672 - Resource Manager queuing system
- You must update all hubs after you:
  - Update your version of Resource Manager
  - Install patches
  - Install, update, or remove ZenPacks

5.2.2.2. Limitations

The system is not compatible with Security-Enhanced Linux (SELinux) in enforcing mode. You must disable enforcing mode for all platforms running the Resource Manager daemons (Resource Manager master, remote hubs, and remote collectors).

To disable enforcing mode:

1. Edit the /etc/selinux/config file.
2. Set the following line:

```
SELINUX=disabled
```

Note

You also can disable enforcing mode temporarily (avoiding the need to reboot) with the command:

```
echo 0 > /selinux/enforce
```

For more information about SELinux, browse to http://en.wikipedia.org/wiki/SELinux, or to the SELinux home page at http://www.nsa.gov/research/selinux/index.shtml.

5.2.2.3. Configuring Zenoss DataStore for Remote Hubs

Hubs on remote servers need access to the Zenoss DataStore. By default this is set to localhost, but will not work for remote hubs. Distributed collector attempts to set this field to the fully qualified domain name of the Resource Manager server when it is installed. If remote hubs appear to be having trouble connecting to the

Zenoss DataStore, then check the host value in `$ZENHOME/etc/global.conf` to make sure it can be reached from the server the hub is on.

Another aspect of remote hubs connecting to the Zenoss DataStore is privileges. For a hub to connect to the database, the user specified in the `$ZENHOME/etc/global.conf file` for `mysqluser` must be granted privileges to connect to the Zenoss DataStore from the remote server. If a remote hub is logging error messages that indicate it is not allowed to connect from the given host, then these privileges are likely not set up correctly. Granting of these privileges requires a fully qualified domain name for the remote server.

Before adding a hub, ensure grants and permissions are set correctly. For your Resource Manager master, run these commands:

```
GRANT SELECT on mysql.user to zenoss@'%' IDENTIFIED BY "zenoss";
GRANT ALL PRIVILEGES ON zenoss_zep.* to zenoss@'%' IDENTIFIED BY "zenoss";
GRANT ALL PRIVILEGES ON zodb.* to zenoss@'%' IDENTIFIED BY "zenoss";
FLUSH PRIVILEGES;
```

For every remote Zenhub server, run these commands in the Zenoss DataStore, replacing *RemoteHubFQDN* with the appropriate host name for each server:

```
GRANT SELECT on mysql.user to zenoss@'RemoteHubFQDN' IDENTIFIED BY "zenoss";
GRANT ALL PRIVILEGES ON zenoss_zep.* to zenoss@'RemoteHubFQDN' IDENTIFIED BY "zenoss";
GRANT ALL PRIVILEGES ON zodb.* to zenoss@'RemoteHubFQDN' IDENTIFIED BY "zenoss";
FLUSH PRIVILEGES;
```

5.2.2.4. Prerequisite Tasks

Before deploying a remote hub, you must:

- Configure your firewall
- Install the Zenoss dependencies repository
- Install RRDtool

5.2.2.4.1. Configure Your Firewall

The following ports must be open in your firewall:

Port	Protocol	Direction to Resource Manager Server	Description
11211	TCP | UDP	Inbound	memcached
8080	TCP	Outbound	Web interface
514	UDP	Inbound	syslog
162	UDP	Inbound	SNMP Traps
8789	TCP	Inbound and outbound	ZenHub communication

Table 5.6. Ports

5.2.2.4.2. Install the Zenoss Dependencies Repository

Install the Zenoss dependencies repository. Use one of the following commands.

- RHEL 5 or CentOS 5:

  ```
  rpm -ivh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el5.noarch.rpm
  ```

- RHEL 6 or CentOS 6:

  ```
  rpm -ivh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el6.noarch.rpm
  ```

5.2.2.4.3. Install and Configure RRDtool

Enter the following command to install RRDtool:

```
yum -y install rrdtool-1.4.7
```

5.2.2.5. Deployment

When deploying a remote hub, you can select one of several options, using:

- Root password to the remote host
- Pre-existing root SSH keys
- Resource Manager SSH keys (use only for RPM installations)

To add a hub, from the main Collectors page, select Add Hub from the Action menu.

The Add Hub page appears.

5.2.2.5.1. Install Remotely (Root Password)

Follow these steps to install a remote hub, using a root password for access to the remote host.

Note

You must set a password for the root user on a server before deploying a hub to it.

1. Select the root password option.

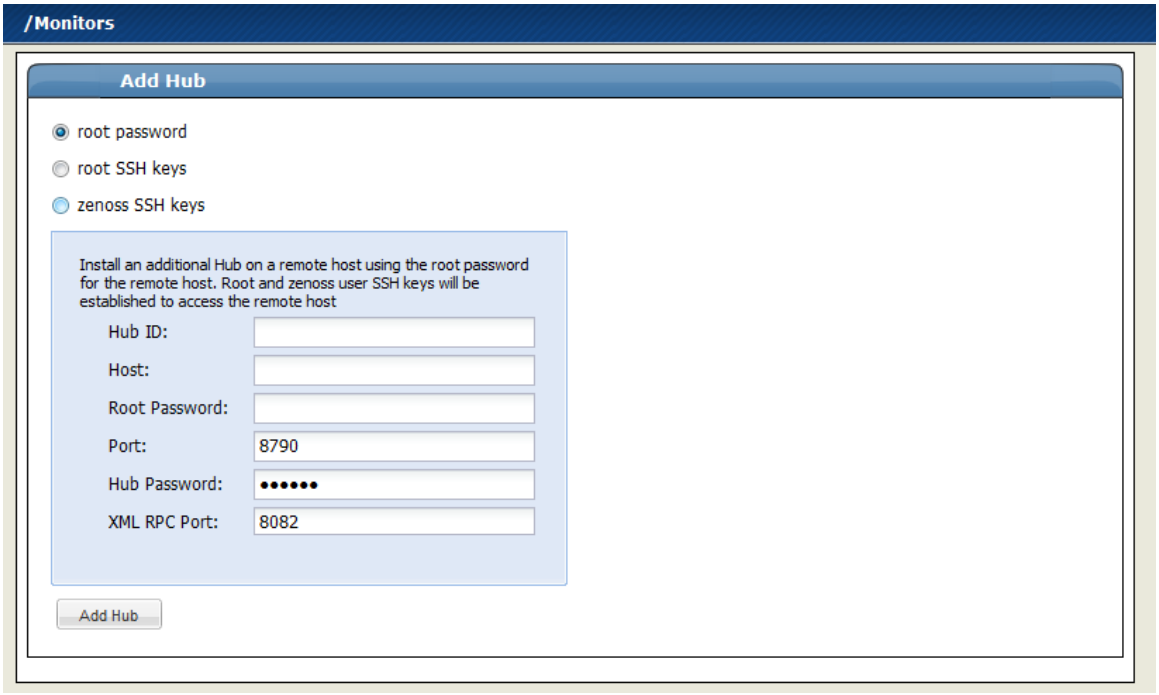

Figure 5.5. Install Remote Hub (Root Password)

2. Enter or change setup details:
   - **Hub ID** - Enter a name for the new hub. The name can be any unique combination of letters, digits, and dashes.
   - **Host** - Enter the fully qualified domain name, IP address, or resolvable host name of the server on which the new hub will run.
   - **Root Password** - Enter the root user password for the server you specified in the Host field.
   - **Port** - Enter the port number on which the hub should listen for collectors. The default port is 8790.
   - **Hub Password** - Enter the hub password that the collectors will use to log in to this hub. The default password is "zenoss."
   - **XML RPC Port** - Specify the port on which the hub should listen for xml-rpc requests from the collectors or other API clients.

3. Click **Add Hub**.

   The system displays log output from the creation of the new hub. When fully configured (this may require several minutes), click the link at the bottom of the page to go to the overview page for the new hub.

5.2.2.5.2. Install Remotely (Root SSH Keys)

To install a remote hub, using existing root SSH keys for access to the remote host:

1. Select the root SSH keys option.

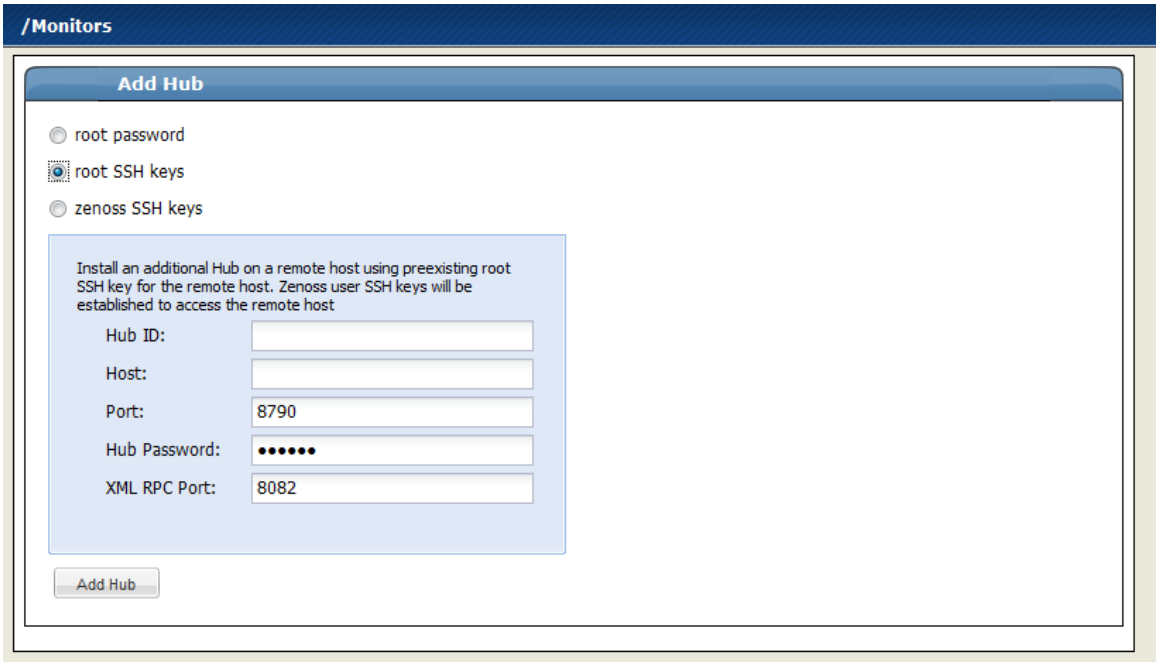

Figure 5.6. Install Remote Hub (Root SSH Keys)

2. Enter or change setup details:
   - **Hub ID** - Enter a name for the new hub. The name can be any unique combination of letters, digits, and dashes.
   - **Host** - Enter the fully qualified domain name, IP address, or resolvable host name of the server on which the new hub will run.
   - **Port** - Enter the port number on which the hub should listen for collectors. The default port is 8790.
   - **Hub Password** - Enter the hub password that the collectors will use to log in to this hub. The default password is "zenoss."
   - **XML RPC Port** - Specify the port on which the hub should listen for xml-rpc requests from the collectors or other API clients.
3. Click **Add Hub**.

   The system displays log output from the creation of the new hub. When fully configured (this may require several minutes), click the link at the bottom of the page to go to the overview page for the new hub.

5.2.2.5.3. Install Remotely (zenoss SSH Keys)

If you choose to set up a hub using zenoss SSH keys, Resource Manager will attempt to install by using the zenoss user. To successfully install a hub using these keys (without root access), these prerequisite conditions must be met:

- zenoss user SSH keys must be set up between the Resource Manager server and the target. The target must have a zenoss user.
- ZENHOME directory must be present on the remote machine.

- zensocket/pyraw must be present on the remote machine, and the setuid bits must be set.
- The nmap program must be made setuid root.

Tip: The best way to meet the prerequisite conditions is to install the Resource Manager RPM on the remote machine. After installation, **do not start** Resource Manager.

Follow these steps to install a remote hub, using Resource Manager SSH keys for access to the remote host.

Note

For detailed steps for creating SSH keys, see the section titled "Setting Up SSH Keys for Distributed Collector."

1. Select the zenoss SSH keys option.

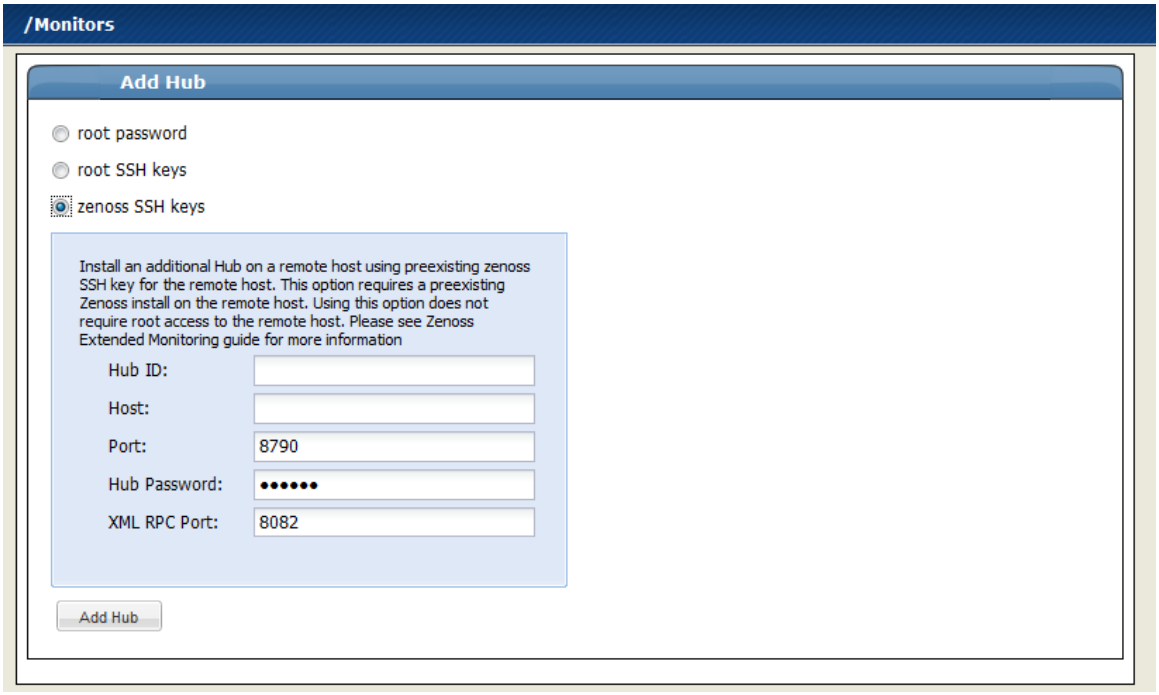

Figure 5.7. Install Remote Hub (Resource Manager SSH Keys)

2. Enter or change setup details:
   - **Hub ID** - Enter a name for the new hub. The name can be any unique combination of letters, digits, and dashes.
   - **Host** - Enter the fully qualified domain name, IP address, or resolvable host name of the server on which the new hub will run.
   - **Port** - Enter the port number on which the hub should listen for collectors. The default port is 8790.
   - **Hub Password** - Enter the hub password that the collectors will use to log in to this hub. The default password is "zenoss."
   - **XML RPC Port** - Specify the port on which the hub should listen for xml-rpc requests from the collectors or other API clients.
3. Click **Add Hub**.

   The system displays log output from the creation of the new hub. When fully configured (this may require several minutes), click the link at the bottom of the page to go to the overview page for the new hub.

5.2.3. Setting Up SSH Keys for Distributed Collector

Follow these instructions to create SSH keys for use when setting up hubs and collectors.

These instructions assume you are using openssh. For more information, refer to the ssh-keygen man pages.

1. Use the following commands to generate an openssh RSA key pair for the zenoss user:

```
mkdir $HOME/.ssh
ssh-keygen -t rsa -f $HOME/.ssh/id_rsa -P "
```

2. Lock down the key pair:

```
chmod 700 $HOME/.ssh
chmod go-rwx $HOME/.ssh/*
```

3. Copy the generated public key `$HOME/.ssh/id_rsa.pub` file to the remote machine. On the remote machine, add the public key to the `authorized_keys` file in the account the user wants to log in to by using the SSH key.
   a. If `$HOME/.ssh` does not exist on the target machine, then create it with these commands:

```
mkdir ~/.ssh
chmod 700 ~/.ssh
```

   b. Add the key:

```
cat id_rsa.pub >> $HOME/.ssh/authorized_keys
chmod 600 $HOME/.ssh/authorized_keys
```

Note

You cannot use keys with a pass phrase with Resource Manager.

Chapter 6. Performance Tuning

After installing Resource Manager, you can optimize its performance by:

- Packing the ZODB
- Editing archived event data storage settings
- Running ZenTune
- Setting memory caching values
- Increasing maximum file descriptors
- Increasing RRD performance
- Configuring the messaging system
- Configuring the heartbeat monitor

6.1. Packing the ZODB

The Zope Object Database (ZODB) keeps records of all transactions performed. As these records accumulate, the database file grows over time.

To keep the database running efficiently, Resource Manager runs a weekly `cron` job to regularly remove old transactions. You also can initiate this process at any time; as the zenoss user, use the following command:

```
$ZENHOME/bin/zenossdbpack
```

Note

You should run this command only on the system master (not on remote collectors).

6.2. Editing Archived Event Data Storage Settings

You can edit the default settings for archived event data to improve Resource Manager performance. Changing these settings to values that are reasonable for your implementation will prevent the Zenoss DataStore from filling up your hard drive. An extremely large database also can have a negative impact on performance.

To change the settings for length of time Resource Manager archives event data:

1. Select Advanced, and then select Events from the left panel.

   The Event Configuration page appears.
2. Adjust values as desired for these configuration settings:
   - **Delete Archived Events Older Than** (days) - By default, this is set to 90 days. Accepted values are between 1 and 1000 days.
   - **Event Time Purge Interval** (days) - By default, this is set to 7 days. Accepted values are between 1 and 250 days.
3. Click **Save** to save your changes.

6.3. ZenTune

The ZenTune "tuning advisor" analyzes your system configuration and makes recommendations for better performance. The feature is implemented through the ZenPacks.zenoss.AutoTune ZenPack.

6.3.1. Using ZenTune

To access ZenTune, select Advanced > Tuning from the Resource Manager interface.

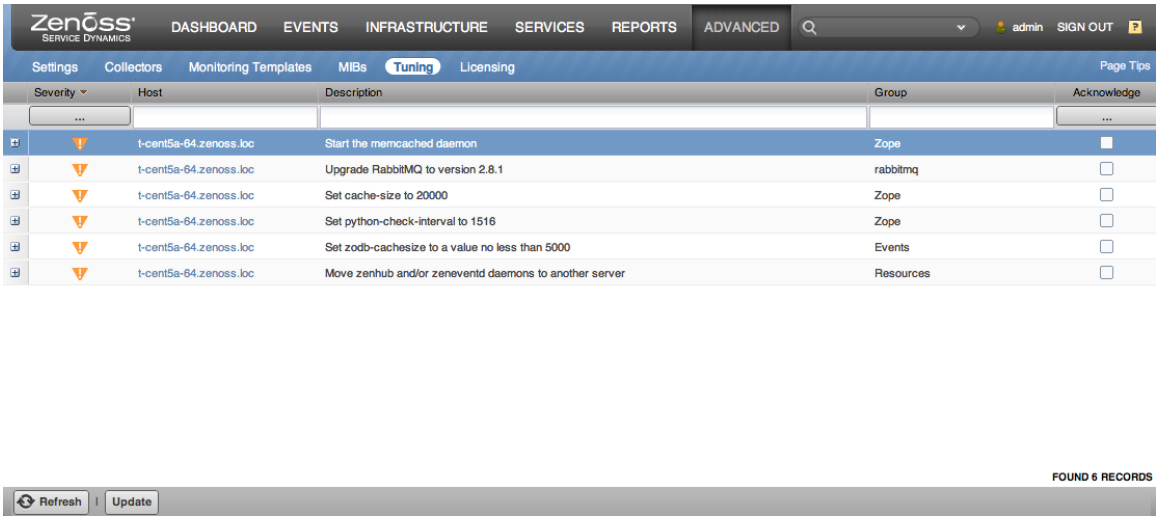

Figure 6.1. ZenTune

To run ZenTune, click **Update** (located at the bottom left of the page).

ZenTune returns information about current and optimal values for several configuration parameters. Click + to the left of each item to display recommendations, if any, for configuration changes.

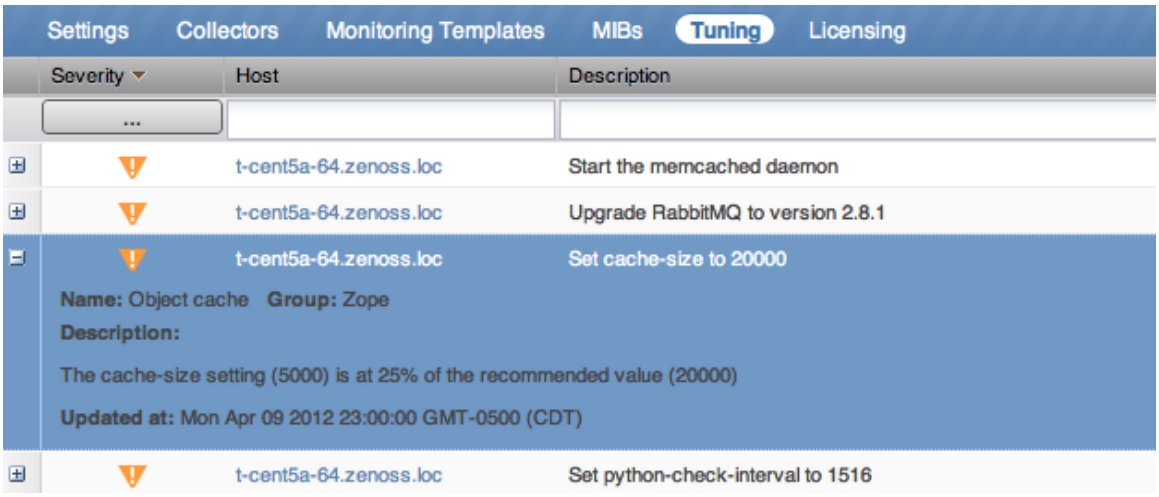

Figure 6.2. ZenTune Issue Detail

To refresh the view, click **Refresh**. (This does not run ZenTune again.)

To filter the list of displayed items, select Not Acknowledged, Acknowledged, or both in the Acknowledge column. To acknowledge one or more items, select the option in the Acknowledge column.

You also can filter the display by severity, host, and description.

6.4. Memory Caching

Zenoss recommends that you set the CACHESIZE value in`/etc/sysconfig/memcached` to a minimum of 1024, and ideally double the size of the cache-local-mb value in `zope.conf`.

Run memcached as close to the master as possible, as zopectl and zeneventd are its biggest users. In very large database scenarios (for example, 500,000 items in the global catalog), run other instances of memcached on the hubs, and update `global.conf` on those boxes to point there instead of to the master.

6.5. Increasing Maximum File Descriptors

A Resource Manager server can require in excess of 10000 open files. For optimal performance, Zenoss recommends that you increase the maximum number of file descriptors in your Linux system configuration:

1. Edit the `/etc/sysctl.conf` file:

   ```
   vi /etc/sysctl.conf
   ```

2. Add this line to the file:

   ```
   fs.file-max = Number
   ```

   where *Number* represents a number in excess of the anticipated number of open files needed by Resource Manager (for example, 10240).

3. Save and close the configuration file.
4. Verify the new setting with this command:

   ```
   sysctl fs.file-max
   ```

Note

Alternatively, you can edit the `/etc/security/limits.conf` file and add the line:

```
zenoss  -   nofile   Number
```

6.6. Increasing RRD Performance

You can increase RRD performance by tuning `zenrrdcached`. Adjust one or more of the following settings in the `$ZENHOME/etc/zenrrdcached.conf` file.

Resource Manager Setting	rrdcached Setting	Default Value (in seconds)
write_threads	-t	4
write_timeout	-w	300
write_delay	-z	0
flush_timeout	-f	3600

Table 6.1. zenrrdcached Settings

To determine how to adjust these settings, you can use the following command, which indicates load on the disk subsystem:

```
iostat -dx 10
```

If iowait times are above 50 percent, then the disk is likely overtaxed. A further indicator of performance degradation is if you see gaps in performance graphs.

Increasing the values of write_timeout and write_delay to some multiple of the polling period (by default, 5 minutes) will decrease the number of random IOPS due to writing performance data.

6.7. Configuring the Messaging System

You can configure several aspects of the messaging system by making changes to the `messaging.conf` configuration file.

After making a change, you must:

- Drop any queues modified
- Restart the processes that consume messages from the modified queues

To drop queues, use the `zenqdelete` script:

```
$ zenqdelete zenoss.queues.zep.rawevents
```

To get queue names, use `rabbitmqctl`:

```
$ rabbitmqctl list_queues -p /zenoss
```

6.7.1. Message Persistence

You can configure whether messages published to a given exchange:

- Exist only in memory (and are lost if Rabbit fails), or
- Are persisted to disk (and recoverable)

Non-persistent messages are much faster, and do not consume disk space if a queue backs up.

To change default message persistence, edit the value of the following line:

```
exchange.default.delivery_mode = Value
```

where possible values are:

- 1 - Do not persist to disk
- 2 - Persist to disk (the default value)

Examples

To prevent unprocessed events from being saved to disk before being processed by `zeneventd`, uncomment the line:

```
# exchange.$RawZenEvents.delivery_mode = 1
```

To prevent processed events from being saved to disk before being de-duped and persisted by `zeneventserver`, uncomment the line:

```
# exchange.$ZepZenEvents.delivery_mode = 1
```

To prevent heartbeats from being saved to disk before being handled by `zeneventserver`, uncomment the line:

```
# exchange.$Heartbeats.delivery_mode = 1
```

6.7.2. Message Compression

You can configure whether messages published to a given exchange should be compressed. To change default message compression, edit the value of the following line:

```
exchange.default.compression = Value
```

where possible values are:

- deflate - Use DEFLATE algorithm
- none - Do not compress messages

By default, all messages published to all exchanges are compressed.

6.7.3. Message TTL

You can configure the time-to-live value (TTL) of messages published to a queue, setting them to expire if they have not been delivered to a client within a given time.

To change default message TTL, edit the following line:

```
queue.default.x-message-ttl = Value
```

where *Value* is a value in milliseconds. By default, messages expire after one day (86400000 milliseconds).

Examples

To cause unprocessed events to expire if they have not been processed within one hour (for example, if `zeneventd` backs up in an event storm), uncomment the line:

```
# queue.$RawZenEvents.x-message-ttl = 3600000
```

To cause processed events to expire if they have not been persisted within one hour (for example, if `zeneventd` backs up in an event storm), uncomment the line:

```
queue.$ZepZenEvents.x-message-ttl = 3600000
```

6.7.4. Queue Expiration

You can configure unused queues to be deleted automatically after a period of time. "Unused" means that the queue has no consumers, and has not been re-declared.

To change default queue expiration, edit the following line:

```
queue.default.x-expires = Value
```

where *Value* is a value in milliseconds. By default, queues expire after one day (86400000 seconds).

6.8. Configuring the Heartbeat Monitor

The heartbeat monitor allows daemons that have connections to RabbitMQ to set up heartbeats with the message broker. Configuration options allow you to specify how often the message broker should expect to receive heartbeats from the consumers created by the daemon. If three intervals pass without the message broker receiving a heartbeat, the broker will disconnect the consumer.

You may want to configure the interval if you are fine-tuning a high availability environment and encountering issues with consumers not disconnecting quickly enough from RabbitMQ when a failover scenario occurs.

By default, a heartbeat is sent every 60 seconds. You can modify this default in two ways:

- Modify the value of the amqpheartbeat setting (by default, 60), in the `$ZENHOME/etc/zengomd.conf` file.
- Use the -b or --zmqpheartbeat option at the command line.

Note

Setting the heartbeat value to 0 turns it off.

Chapter 7. Upgrading

Use the instructions in this chapter to upgrade your Resource Manager instance.

Note

Unless otherwise directed, perform all commands as the root user.

7.1. Upgrade Paths

The current version of Resource Manager requires a 64-bit platform. If you are upgrading from a 32-bit platform version, please contact Zenoss Support for assistance with your upgrade.

The following table lists supported upgrade paths for this version of Resource Manager:

If your current version is:	You can upgrade directly to this version:
Zenoss Enterprise 3.2.1	Resource Manager 4.2.3
Resource Manager 4.1.1 + recommended patches	Resource Manager 4.2.3
Resource Manager 4.2.2	Resource Manager 4.2.3

Table 7.1. Upgrade Paths

7.2. Before Upgrade

Before starting upgrade, review the information in the following sections (as applicable to your upgrade):

- Resource Manager 4.2.2 to Resource Manager 4.2.3
- Resource Manager 4.1.1 to Resource Manager 4.2.3
- Zenoss Enterprise 3.2.1 to Resource Manager 4.2.3
- All upgrade paths

7.2.1. Resource Manager 4.2.2 to Resource Manager 4.2.3

When upgrading from Resource Manager 4.2.2 to Resource Manager 4.2.3, you must use RPM (instead of YUM).

7.2.2. Resource Manager 4.1.1 to Resource Manager 4.2.3

For upgrades from Resource Manager 4.1.1 to Resource Manager 4.2.3:

- When updating to the required version of RabbitMQ Server (Version 2.8.6), Zenoss recommends that you follow alternate installation procedures if:
  - You use custom queues
  - Your installation includes Zenoss Service Dynamics Impact and Optimization
  - You want to independently update RabbitMQ Server (without upgrading Resource Manager)

  These procedures are outlined in the appendix in this guide titled "Updating RabbitMQ Server for Resource Manager 4.2.3."
- You must remove all `ifOperStatus_ifOperStatus.rrd` perf files. As the zenoss user, run this command on each server with perf files:

```
find $ZENHOME -name "ifOperStatus_ifOperStatus.rrd" -delete
```

7.2.3. Zenoss Enterprise 3.2.1 to Resource Manager 4.2.3

For upgrades from Zenoss Enterprise 3.2.1 to Resource Manager 4.2.3:

- Zenoss Resource Manager includes a fully redesigned event processing and storage system. Upgrades to Resource Manager do not automatically migrate events from Zenoss Enterprise 3.2.1. A new, empty event table is created in the new schema after upgrade.

  If you want to migrate events to Resource Manager as part of your upgrade, then a managed migration path is available. Zenoss recommends you contact Zenoss Professional Services for assistance, and then create an output file of your current MySQL events database.

  To create the output file, enter this command:

  ```
  mysqldump -u root -p [ROOT_PASSWORD] events | gzip -c > zenoss_events.sql.gz
  ```

- If upgrading from Zenoss Enterprise 3.2.1, do not remove your current MySQL installation. (You can remove MySQL after upgrade is complete.)

7.2.4. All Upgrade Paths

For all upgrade paths:

- Back up your data files.

  Do this as the `zenoss` user, following the instructions outlined in the section titled "Back Up Resource Manager Data" in the *Resource Manager Administration* guide.

- Download the Resource Manager installation files:
  1. Browse to the following URL:

     https://support.zenoss.com

     Note

     Contact your Zenoss representative for site login credentials.
  2. In the Downloads area of the Home tab, locate the current Service Dynamics installation files.
  3. Download the Resource Manager and (optionally) Windows ZenPacks RPM files.
- Ensure that all dependencies and the correct versions of required software are installed. As part of the upgrade, you may need to:
  - Remove conflicting messaging systems
  - Install and configure software repositories, prerequisite software, and additional packages. These include:
    - Oracle Java
    - Zenoss dependencies repository
    - RabbitMQ
    - memcached and snmpd

  For installation procedures and a list of required software versions, see one of the following chapters in this guide:
  - Installing for RHEL 5 or CentOS 5
  - Installing for RHEL 6 or CentOS 6
- When upgrading with a remote Zenoss DataStore configured, any modifications made to `$ZENHOME/bin/zenoss_init_pre` or `$ZENHOME/bin/zenoss_upgrade_pre` are preserved automatically as part of the upgrade. Modified versions are backed up to `zenoss_init_pre.rpmsave` and `zenoss_upgrade_pre.rpmsave`, respectively.

You must merge any changes to these settings into the `zenoss_init_pre` and `zenoss_upgrade_pre` files before starting the system for the first time.

- If you do not plan to install the Windows Monitoring ZenPack (by installing the msmonitor RPM, as described in the section titled "Install the Windows Monitoring ZenPack"), then you must manually remove these ZenPacks:
  - ZenPacks.zenoss.ZenWinPerf
  - ZenPacks.zenoss.WinModelerPlugins
  - ZenPacks.zenoss.ActiveDirectory
  - ZenPacks.zenoss.IISMonitor
  - ZenPacks.zenoss.MSExchange
  - ZenPacks.zenoss.MSMQMonitor
  - ZenPacks.zenoss.MSSQLServer

  To see a list of all currently installed ZenPacks, as the zenoss user, enter:

  ```
  zenpack --list
  ```

  To remove a ZenPack, as the zenoss user, enter:

  ```
  zenpack --remove=ZenPacks.zenoss.Name
  ```
- During upgrade, you will stop any installed remote hubs. Do not restart these hubs after upgrading the master system. The hubs are automatically restarted after they are upgraded (later in the process).

7.3. Update the Zenoss DataStore

The Zenoss DataStore update process is configured to preserve your existing Resource Manager database files and any customizations you may have made to the `/opt/zends/etc/zends.cnf` file.

Perform these steps on the local Resource Manager server:

1. Browse to this URL:

   https://support.zenoss.com

   Note

   Contact your Zenoss representative for site login credentials.
2. In the Downloads area of the Home tab, locate and download the Zenoss DataStore RPM files.
3. Stop Resource Manager:

   ```
   service zenoss stop
   ```
4. Stop remote hubs, if any:

   ```
   service zenoss stop
   ```
5. Stop the Zenoss DataStore:

   ```
   service zends stop
   ```
6. Install the Zenoss DataStore.
   - For RHEL 5 or CentOS 5 systems:

     ```
     yum --nogpgcheck localinstall zends-5.5.25a-1.Version.el5.x86_64.rpm
     ```
   - For RHEL 6 or CentOS 6 systems:

     ```
     yum --nogpgcheck localinstall zends-5.5.25a-1.Version.el6.x86_64.rpm
     ```

7. *If upgrading from Version 4.1.1*, edit the `opt/zenoss/etc/global.conf` file and set the value of the mysql-socket option to:

   ```
   /var/lib/zends/zends.sock
   ```

8. *If upgrading from Version 4.1.1*, edit the `/opt/zenoss/etc/zope.conf` file and set the value of the unix_socket option (listed in two places in the file) to:

   ```
   /var/lib/zends/zends.sock
   ```

9. Start the data store and ensure it runs at system startup:

   ```
   service zends start
   chkconfig --level 2345 zends on
   ```

During Zenoss DataStore update, if you see the following warning message:

```
warning: /opt/zends/etc/zends.cnf created as /opt/zends/etc/zends.cnf.rpmnew
```

then you must manually merge updates from `zends.cnf.rpmnew` into your customized `zends.cnf` file.

In the following example scenario, merge of the `zends.cnf` file is required after update:

```
ZenDS RPM upgrade to version 5.5.25a-1.r64630.el5
Giving ZenDS 5 seconds to exit gracefully

  Updating       : zends                      1/2Executing post-installation steps
Updating vm.swappiness
vm.swappiness = 0

Successfully upgraded Zenoss DataStore under /opt/zends.

The default configuration is located here:
        /opt/zends/etc/zends.cnf

Before starting Zenoss, update the mysqlsocket option
in /opt/zenoss/etc/global.conf and the unix_socket option
(two places) in /opt/zenoss/etc/zope.conf to the value /var/lib/zends/zends.sock.
```

7.4. Update and Configure Resource Manager

Follow these steps to update the Resource Manager software and ZenPacks, and (optionally) a remote Zenoss DataStore.

7.4.1. Update the Resource Manager RPM

Install the Resource Manager RPM file.

- For upgrades from Version 4.2.2 to Version 4.2.3:
  - RHEL 5 or CentOS 5 systems:

    ```
    rpm -Uvh zenoss_resmgr-Version.el5.x86_64.rpm
    ```

  - RHEL 6 or CentOS 6 systems:

    ```
    rpm -Uvh zenoss_resmgr-Version.el6.x86_64.rpm
    ```

- All other upgrade paths:
  - RHEL 5 or CentOS 5 systems:

    ```
    yum -y --nogpgcheck localinstall zenoss_resmgr-Version.el5.x86_64.rpm
    ```

  - RHEL 6 or CentOS 6 systems:

    ```
    yum -y --nogpgcheck localinstall zenoss_resmgr-Version.el6.x86_64.rpm
    ```

7.4.2. (Optional) Install a Remote Zenoss DataStore

Follow these optional steps to install and configure a remote data store.

1. On the local Resource Manager server:
   a. Stop the data store and configure it so that it will not run at system startup:

      ```
      service zends stop
      chkconfig --level 2345 zends off
      ```

   b. Change the values of these entries in the `$ZENHOME/etc/global.conf.example` file:
      - zodb-host - Change the value from "localhost" to the name or IP address of the remote server.
      - zep-host - Change the value from "localhost" to the name or IP address of the remote server.
      - zodb-port - Change the value from 3306 to 13306
      - zep-port - Change the value from 3306 to 13306
2. On the remote server:
   a. Download the Zenoss DataStore RPM files.
   b. Install the Zenoss DataStore.
      - For RHEL 5 or CentOS 5 systems:

        ```
        yum --nogpgcheck localinstall zends-5.5.25a-1.Version.el5.x86_64.rpm
        ```

      - For RHEL 6 or CentOS 6 systems:

        ```
        yum --nogpgcheck localinstall zends-5.5.25a-1.Version.el6.x86_64.rpm
        ```

   c. Start the data store and ensure it runs at system startup:

      ```
      service zends start
      chkconfig --level 2345 zends on
      ```

   d. Change to the zenoss user:

      ```
      su - zenoss
      ```

   e. Enter the following command:

      ```
      zends -u root
      ```

   f. Enable remote access to the Zenoss DataStore. In the prompt that appears, enter this series of commands:

      ```
      grant all on *.* to 'root'@'%' with grant option;
      flush privileges;
      ```

7.4.3. Install MySQLTuner

Follow these steps to download and install the MySQLTuner Perl script:

1. As the zenoss user, log in to a shell account on the master Resource Manager server.
2. Change to the following directory:

   ```
   cd $ZENHOME/bin
   ```

3. Retrieve the MySQLTuner script:

   ```
   wget mysqltuner.pl
   ```

4. Change read and execute access to the file:

   ```
   chmod 755 mysqltuner.pl
   ```

7.4.4. Update Port Information

If upgrading from Version 3.2.1 and if not using a remote Zenoss DataStore, you must update port information for the following entries in the `/opt/zenoss/etc/global.example` file:

- zodb-port - Change the value from 3306 to 13306.
- zep-port - Change the value from 3306 to 13306.

7.4.5. Start the System

Run the following command to start the system:

```
service zenoss start
```

7.4.6. (Optional) Install the Windows Monitoring ZenPack

Optionally enable Windows monitoring:

1. Stop the system:

   ```
   service zenoss stop
   ```

2. Install the msmonitor RPM file.
   - For RHEL 5 or CentOS 5 systems:

     ```
     yum -y --nogpgcheck localinstall zenoss_msmonitor-Version.el5.x86_64.rpm
     ```

   - For RHEL 6 or CentOS 6 systems:

     ```
     yum -y --nogpgcheck localinstall zenoss_msmonitor-Version.el6.x86_64.rpm
     ```

3. Restart the system:

   ```
   service zenoss restart
   ```

4. Log in to your Resource Manager instance to confirm correct operation.
5. Delete the browser cache on each user machine used to access Resource Manager. (For example, if using Firefox, press Ctrl-Shift-R to clear your cache.)

7.5. Update Custom ZenPacks

After upgrading, you must update any ZenPacks developed by you, the Zenoss community, or Zenoss Professional Services. For more information about installing and updating ZenPacks, see the *Resource Manager Extended Monitoring* guide.

7.6. Update Collectors and Hubs

For each machine that houses a remote collector or remote hub (zenhub), you must:

- Install required prerequisites (if not already installed)
- Update the collector or hub manually from the Resource Manager user interface

7.6.1. Remote Hubs

For RHEL or CentOS, to update remote hubs:

1. Install Oracle Java Version 1.6u31 or later.
2. Install the Zenoss DataStore RPM.
3. Stop the remote hub:

   ```
   service zenoss stop
   ```

4. On the remote hub server, run these commands:

   ```
   service zends stop
   chkconfig zends off
   ```

   Note

   Resource Manager requires certain features provided by the Zenoss DataStore, so you cannot remove the Zenoss DataStore completely. You can, however, save resources by not running the main service.

5. Update the remote hub. From the user interface Navigation menu:
    a. Select Advanced > Settings.
    b. Click Collectors.
    c. Select the remote hub, and then select Update Hub from the Action menu.

7.6.2. Remote Collectors

For RHEL or CentOS, to update remote collectors:

1. Install Oracle Java Version 1.6u31 or later.
2. Update remote collectors (and any local collectors). From the user interface Navigation menu:
    - Select Advanced > Settings.
    - Click Collectors.
    - Select the collector, and then select Update Collector from the Action menu.

Appendix A. Updating RabbitMQ Server for Resource Manager 4.2.3

A.1. About

This document provides information and procedures for updating RabbitMQ Server for systems upgrading from Zenoss Resource Manager Version 4.x to Version 4.2.3. Using this information, you will update RabbitMQ Server to Version 2.8.6 or later.

You should follow these procedures if:

- You use custom queues
- Your installation includes Zenoss Service Dynamics Impact and Optimization
- You want to independently update RabbitMQ Server (without upgrading Resource Manager)

Zenoss strongly recommends that you read this document completely before starting the procedures.

A.1.1. Resource Manager Master Connected to Internet

If your Resource Manager master has Internet connectivity, then follow these steps to update RabbitMQ Server:

1. Enter one of the following commands to upgrade to the latest Zenoss dependencies repository:
   - For RHEL 5 or CentOS 5:

     ```
     rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el5.noarch.rpm
     ```
   - For RHEL 6 or CentOS 6:

     ```
     rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el6.noarch.rpm
     ```
2. Verify that you have visibility on version 2.8.6 of RabbitMQ Server from the zenossdeps-update repository:

   ```
   yum list rabbitmq-server
   ```

   You should see output similar to:

   ```
   ...
       Installed Packages
       rabbitmq-server.noarch   2.1.0-1.el5              installed
       Available Packages
     >>rabbitmq-server.noarch   2.8.6-1                  zenossdeps-update-repo
   ```
3. Quiesce all Resource Manager components (remote collectors, hubs, and the Resource Manager master). Enter the following commands:

On the Resource Manager master

```
zenwebserver stop
```

On each remote collector

```
ssh zenoss@remote-collector
zenoss stop
```

On each remote hub

```
ssh zenoss@remote-hub
zenoss stop
```

On the Resource Manager master

```
ssh root@master
```

```
service zenoss stop
```

4. Examine the RabbitMQ queues:

```
rabbitmqctl list_queues -p /zenoss
Your output should be similar to:
Listing queues ...
zenoss.queues.modelrequests.vmware 0
zenoss.queues.zep.migrated.summary 0
zenoss.queues.hub.invalidations.localhost:8789 0
zenoss.queues.zep.migrated.archive 0
zenoss.queues.hub.collectorcalls.localhost:8789 0
zenoss.queues.zep.rawevents 0
zenoss.queues.zep.heartbeats 0
zenoss.queues.zep.zenevents 0
zenoss.queues.zep.signal 0
zenoss.queues.zep.modelchange 0
...done.
```

Warning

Upgrading RabbitMQ will erase all exchanges and queries. All messages that have not been consumed will be lost. If you notice any non-zero queues, then contact Zenoss Support before continuing.

If you have customizations or ZenPacks that are not Zenoss-supported and use RabbitMQ, ensure that all of the messages in the relevant queues are consumed before continuing upgrade. Consult the provider of the customizations for help regarding the sensitivity of lost messages.

5. Enter the following commands to quiesce RabbitMQ:

```
service rabbitmq-server stop
service rabbitmq-server status
```

You should see output similar to:

```
Status of all running nodes...
Error: no_nodes_running
```

6. Perform the RabbitMQ upgrade:

```
yum upgrade rabbitmq-server
```

7. Start the RabbitMQ server:

```
service rabbitmq-server start
```

8. Create a script to restore the RabbitMQ configuration for use with Resource Manager:
   a. Create a file named `configure_amqp.sh`.
   b. Add the following content to the file:

```
#!/bin/sh

RABBITMQ_USER=zenoss
RABBITMQ_PASS=zenoss
RABBITMQ_VHOST=/zenoss

configure_amqp() {
RABBITMQCTL="`which rabbitmqctl`"
if [ ! -z "$RABBITMQCTL" ]; then
local user_exists=`"$RABBITMQCTL" -q list_users | awk '{print $1}' |\
 grep '^'"$RABBITMQ_USER"'$'`
if [ -z "$user_exists" ]; then
echo "Adding RabbitMQ user: $RABBITMQ_USER"
"$RABBITMQCTL" -q add_user "$RABBITMQ_USER" "$RABBITMQ_PASS"
fi
local vhost_exists=`"$RABBITMQCTL" -q list_vhosts | awk '{print $1}' |\
 grep '^'"$RABBITMQ_VHOST"'$'`
if [ -z "$vhost_exists" ]; then
echo "Adding RabbitMQ vhost: $RABBITMQ_VHOST"
```

```
"$RABBITMQCTL" -q add_vhost "$RABBITMQ_VHOST"
fi
local perm_exists=`"$RABBITMQCTL" -q list_user_permissions -p "$RABBITMQ_VHOST" \
 "$RABBITMQ_USER"`
if [ -z "$perm_exists" ]; then
echo "Setting RabbitMQ permissions for user: $RABBITMQ_USER"
"$RABBITMQCTL" -q set_permissions -p "$RABBITMQ_VHOST" "$RABBITMQ_USER" '.*' '.*' '.*'
fi
else
echo "Unable to find rabbitmqctl. Please refer to the installation"
echo "guide for instructions on configuring RabbitMQ."
fi
}
configure_amqp
```

9. Change permissions, and then run the configuration script:

```
chmod +x ./configure_amqp.sh
./configure_amqp.sh
```

10. Restart all Resource Manager components. Enter one or more of the following commands:

On the Resource Manager master

```
service zenoss start
```

On each remote hub

```
ssh zenoss@remote-hub
zenoss start
```

On each remote collector

```
ssh zenoss@remote-hub
zenoss start
```

A.1.2. Resource Manager Master Not Connected to Internet

If your Resource Manager master does not have Internet connectivity, then follow these steps to upgrade RabbitMQ Server:

1. From a staging server with Internet access, enter one of the following commands:
   - For RHEL 5 or CentOS 5:

     ```
     wget http://deps.zenoss.com/yum/4.2.x/centos/5/updates/x86_64/\
     rabbitmq-server-2.8.6-1.noarch.rpm
     ```

   - For RHEL 6 or CentOS 6:

     ```
     wget http://deps.zenoss.com/yum/4.2.x/centos/6/updates/x86_64/\
     rabbitmq-server-2.8.6-1.noarch.rpm
     ```

2. Copy the `rabbitmq-server-2.8.6-1.noarch.rpm` file to the Resource Manager master.
3. Quiesce all Resource Manager components (remote collectors, hubs, and the Resource Manager master). Enter the following commands:

On the Resource Manager master

```
zenwebserver stop
```

On each remote collector

```
ssh zenoss@remote-collector
zenoss stop
```

On each remote hub

```
ssh zenoss@remote-hub
zenoss stop
```

On the Resource Manager master

```
ssh root@master
service zenoss stop
```

4. Examine the RabbitMQ queues:

```
rabbitmqctl list_queues -p /zenoss
Your output should be similar to:
Listing queues ...
zenoss.queues.modelrequests.vmware 0
zenoss.queues.zep.migrated.summary 0
zenoss.queues.hub.invalidations.localhost:8789 0
zenoss.queues.zep.migrated.archive 0
zenoss.queues.hub.collectorcalls.localhost:8789 0
zenoss.queues.zep.rawevents 0
zenoss.queues.zep.heartbeats 0
zenoss.queues.zep.zenevents 0
zenoss.queues.zep.signal 0
zenoss.queues.zep.modelchange 0
...done.
```

Warning

Upgrading RabbitMQ will erase all exchanges and queries. All messages that have not been consumed will be lost. If you notice any non-zero queues, then contact Zenoss Support before continuing.

If you have customizations or ZenPacks that are not Zenoss-supported and use RabbitMQ, ensure that all of the messages in the relevant queues are consumed before continuing upgrade. Consult the provider of the customizations for help regarding the sensitivity of lost messages.

5. Enter the following commands to quiesce RabbitMQ:

```
service rabbitmq-server stop
service rabbitmq-server status
```

You should see output similar to:

```
Status of all running nodes...
Error: no_nodes_running
```

6. Perform the RabbitMQ upgrade on the Resource Manager master:

```
yum localupdate rabbitmq-server-2.8.6-1.noarch.rpm
```

7. Start the RabbitMQ server:

```
service rabbitmq-server start
```

8. Create a script to restore the RabbitMQ configuration for use with Resource Manager:
   a. Create a file named `configure_amqp.sh`.
   b. Add the following content to the file:

```
#!/bin/sh

RABBITMQ_USER=zenoss
RABBITMQ_PASS=zenoss
RABBITMQ_VHOST=/zenoss

configure_amqp() {
RABBITMQCTL="`which rabbitmqctl`"
if [ ! -z "$RABBITMQCTL" ]; then
```

```
local user_exists=`"$RABBITMQCTL" -q list_users | awk '{print $1}' |\
 grep '^'"$RABBITMQ_USER"'$'`
if [ -z "$user_exists" ]; then
echo "Adding RabbitMQ user: $RABBITMQ_USER"
"$RABBITMQCTL" -q add_user "$RABBITMQ_USER" "$RABBITMQ_PASS"
fi
local vhost_exists=`"$RABBITMQCTL" -q list_vhosts | awk '{print $1}' |\
 grep '^'"$RABBITMQ_VHOST"'$'`
if [ -z "$vhost_exists" ]; then
echo "Adding RabbitMQ vhost: $RABBITMQ_VHOST"
"$RABBITMQCTL" -q add_vhost "$RABBITMQ_VHOST"
fi
local perm_exists=`"$RABBITMQCTL" -q list_user_permissions -p "$RABBITMQ_VHOST" \
 "$RABBITMQ_USER"`
if [ -z "$perm_exists" ]; then
echo "Setting RabbitMQ permissions for user: $RABBITMQ_USER"
"$RABBITMQCTL" -q set_permissions -p "$RABBITMQ_VHOST" "$RABBITMQ_USER" '.*' '.*' '.*'
fi
else
echo "Unable to find rabbitmqctl. Please refer to the installation"
echo "guide for instructions on configuring RabbitMQ."
fi
}
configure_amqp
```

9. Change permissions, and then run the configuration script:

```
chmod +x ./configure_amqp.sh
./configure_amqp.sh
```

10. Restart all Resource Manager components. Enter one or more of the following commands:

On the Resource Manager master

```
service zenoss start
```

On each remote hub

```
ssh zenoss@remote-hub
zenoss start
```

On each remote collector

```
ssh zenoss@remote-hub
zenoss start
```