Zenoss Service Dynamics Resource Management Installation and Upgrade

Zenoss Service Dynamics Resource Management Installation and Upgrade

Part Number: 25-022014-4.2-v18

Preface

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

1. Audience

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. Organization

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 Resource Manager," provides procedures for installing Resource Manager on a system running Red Hat Enterprise Linux (RHEL) or Community ENTerprise Operating System (CentOS), versions 5 or 6.
- Chapter 3, "Adding a collector," provides detailed installation procedures for configuring a collector host.
- Chapter 4, "Installing a hub," provides detailed installation procedures for configuring a hub host.
- Chapter 5, "Performance Tuning," offers information and procedures to help you optimize Resource Manager performance in your environment.
- Chapters 6, 7, and 8 provide procedures for upgrading your current version of Resource Manager to this release.
- Appendix A, "Upgrading RabbitMQ Server," details procedures for upgrading RabbitMQ Server in certain non-standard conditions.
- Appendix B, "Port requirements," details the ports used by various components of Resource Manager.

3. Related guides

The Zenoss Service Dynamics documentation set includes these guides:

Table 1. Zenoss Service Dynamics Guides

Title	Description
Resource Manager Administration	Provides an overview of Resource Manager architecture and features, as well as procedures and examples to help use the system.
Resource Manager Installation and Upgrade	Provides detailed information and procedures for installing and upgrading the system.
Analytics and Optimization Installation and Administration	Provides conceptual and procedural information to help you install and use Analytics.

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

4. Additional information

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

https://support.zenoss.com

5. We welcome your comments

Zenoss welcomes your comments and suggestions about 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

This chapter describes the Resource Manager deployment architecture considerations.

1.1. Installation packages

Resource Manager is distributed as two Red Hat Package Manager (RPM) packages:

- Resource Manager RPM - The Resource Manager software and required ZenPacks
- Windows ZenPacks RPM - (Optional) The ZenPacks that enable Windows monitoring

In addition, Resource Manager incorporates a variety of third-party packages, most of which are specified as dependencies in the Resource Manager RPM package, and so are downloaded and installed automatically.

1.2. Operating system requirements

Resource Manager supports Red Hat Enterprise Linux (RHEL) and CentOS, versions 5 and 6.

The following list identifies additional operating system requirements.

- Resource Manager is not compatible with Security-Enhanced Linux (SELinux) in enforcing mode, so the installation instructions include steps to disable SELinux.

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

- Resource Manager hosts (the master host, remote hub and collector hosts) must be able to resolve their fully-qualified domain names, either through an entry in `/etc/hosts`, or through a nameserver on the network.
- The Resource Manager master host must contain an entry for `localhost` in its `/etc/hosts` file.
- In the default configuration, Resource Manager hosts must be able to download packages through the internet during installation, and to connect to other internet resources during normal operation. To configure Resource Manager to install and operate without an internet connection, contact Zenoss Support.
- Resource Manager hosts (master, data store, hubs, collectors) require Internet Protocol version 4 (IPv4) to communicate with one another.

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.

Table 1.1. Memory and CPU Requirements

Type	Minimum		Recommended		Notes
	Memory	CPU	Memory	CPU	
Master	16 GB	4 cores	32+ GB	8+ cores	Memory and CPU requirements increase with the number of datapoints, devices/components, and concurrent users.
Remote collector	8 GB	4 cores	16 GB	8 cores	SSD storage is also recommended.

Disk storage requirements are shown in the following table:

Table 1.2. Storage requirements

Type	Disk Storage
Resource Manager	50GB
Zenoss DataStore	50GB

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. Storage 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.

1.3.3. Firewall security considerations

Resource Manager relies on specific ports to communicate with remote hosts and devices. Appendix B, "Port requirements", provides comprehensive descriptions of the ports, protocols, and traffic flows associated with each Resource Manager daemon.

Because Resource Manager supports a wide variety of deployment architectures, the installation instructions do not include firewall configuration steps. Consult with your Zenoss representative to plan your deployment, and then configure Resource Manager host firewalls to support your architecture.

1.4. Server hardware configuration

1.4.1. File system configuration

Resource Manager stores 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 I/O performance. At a minimum, Zenoss recommends using a separate filesystem for `$ZENHOME/perf`, and mounting it with the `noatime` option set, so that inode access times are not updated.

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. Client and browser support

Resource Manager supports the client operating systems and web browser combinations shown in the following table:

> **Note**
>
> - The supported browsers must have Adobe® Flash® Player 11 (or a more recent version) installed.
> - Internet Explorer 10 is not supported for this release.
> - Firefox ESR 17.0.5 was not tested for this release.
> - Firefox 19.0.2 will not be supported after this release.
> - Support for Firefox 20.0 was added for this release.

Table 1.3. Client and browser support

Client OS	Supported Browsers
Windows XP Professional (with SP3)	Internet Explorer 8.0.6001.18702
Windows 7 (6.1.7601)	• Internet Explorer 9.0.8112.16421 • Firefox 19.0.2 and 20.0 • Chrome 26.0.1410.43 m
OS X Mountain Lion (10.8)	• Firefox 19.0.2 and 20.0 • Chrome 26.0.1410.43 m
Ubuntu 12.4	• Firefox 19.0.2 and 20.0 • Chrome 26.0.1410.43 m

1.6. Post-installation performance tuning

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 Resource Manager

This chapter provides detailed instructions for installing Resource Manager on RHEL or CentOS systems, versions 5 and 6.

> ### Note
>
> Resource Manager relies on specific ports to communicate with remote hosts and devices. Refer to Appendix B, "Port requirements", for information about the ports required for your deployment, and configure those ports before installing Resource Manager.

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

2.1. Check required package groups

For RHEL and CentOS 6, Resource Manager requires the package groups listed in the following table.

- Additional Development
- Base
- Console internet tools
- Debugging Tools
- Desktop Platform
- Directory Client
- E-mail server
- Fonts
- Graphical Administration Tools
- Hardware monitoring utilities
- Java Platform
- Large Systems Performance
- Legacy UNIX compatibility
- NFS file server
- Network file system client
- Networking Tools
- Performance Tools
- Perl Support
- Scientific support

- Server Platform

To determine which package groups are installed on a host, log in to the host as `root`, and enter the following command.

```
yum grouplist | less
```

Installed package groups are listed under `Installed Groups`.

If a required group is not installed, enter the following command to install it.

```
yum -y groupinstall 'package-group-name'
```

2.2. Preparation tasks

1. Log in to the Resource Manager master host as `root`, or as a user with superuser privileges.

2. Remove conflicting messaging systems.

   a. Determine whether Matahari or Qpid are installed.

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

   b. If the preceding command returns a result, remove the packages.

   ```
   yum -y erase $(rpm -qa | egrep -i "matahari|qpid")
   ```

3. Enable network traffic through required ports.

   - To enable traffic through specific ports, refer to Appendix B, "Required ports".

   - To enable traffic through all ports, enter the following commands.

   ```
   IPv4: service iptables stop; chkconfig iptables off
   IPv6: service ip6tables stop; chkconfig ip6tables off
   ```

   ### Note

   You may open all ports at this time, and then close unneeded ports later, after Resource Manager is installed.

4. Resource Manager is not compatible with Security-Enhanced Linux (SELinux) in enforcing mode. Follow these steps to disable enforcing mode.

   a. Disable enforcing mode temporarily (avoiding the need to reboot).

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

   b. Disable enforcing mode permanently by editing the `/etc/selinux/config` file.

   ```
   /bin/sed -i.bak -e 's/^SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config
   ```

5. Install Oracle Java 1.6. (Java 1.7 is not supported.)

   a. Determine whether other Java pacakges are installed.

   ```
   rpm -qa | egrep -i '(jdk|jre|java)'
   ```

   If necessary, remove the other packages.

   ```
   yum -y remove $(rpm -qa | egrep -i '(jdk|jre|java)')
   ```

   b. Download the self-installing binary of Oracle Java SE Runtime Environment 6u31 from the Java SE 6 Downloads page. The file to download is `jre-6u31-linux-x64-rpm.bin`.

   c. Add execute permission to the self-installing binary.

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

   d. Install the Oracle JRE.

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

   e. Add the JAVA_HOME environment variable to `/etc/profile`.

   ```
   echo "export JAVA_HOME=/usr/java/default" >> /etc/profile
   ```

   f. Verify the correct version is installed.

   ```
   java -version
   ```

   The preceding command should return the following output.

   ```
   java version "1.6.0_31"
   Java(TM) SE Runtime Environment (build 1.6.0_31-b04)
   Java HotSpot(TM) 64-Bit Server VM (build 20.6-b01, mixed mode)
   ```

6. Install the Zenoss dependencies repository.

   ```
   RHEL/CentOS 5: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el5.noarch.rpm
   RHEL/CentOS 6: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el6.noarch.rpm
   ```

7. Clean up `yum` caches.

   ```
   yum clean all
   ```

8. Install the Zenoss DataStore

   ### Note

   You may deploy the Zenoss DataStore on the Resource Manager master host or on a remote host. The Resource Manager master host relies on Zenoss DataStore libraries, so even if you plan to use a remote host, you must install it on the master as well.

   a. Download the Zenoss DataStore RPM file from the Zenoss Support site. Contact your Zenoss representative for login credentials.

   b. Install Zenoss DataStore.

   ```
   RHEL/CentOS 5: yum -y --nogpgcheck localinstall zends-version.el5.x86_64.rpm
   RHEL/CentOS 6: yum -y --nogpgcheck localinstall zends-version.el6.x86_64.rpm
   ```

   c. *If you are deploying Zenoss DataStore on the Resource Manager master host*, start Zenoss DataStore and configure it to start when the host starts.

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

2.3. Install and configure Resource Manager

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

1. Download the Resource Manager RPM file from the Zenoss Support site. Contact your Zenoss representative for login credentials.

2. Install Resource Manager.

   ```
   RHEL/CentOS 5: yum -y --nogpgcheck localinstall zenoss_resmgr-version.el5.x86_64.rpm
   RHEL/CentOS 6: yum -y --nogpgcheck localinstall zenoss_resmgr-version.el6.x86_64.rpm
   ```

3. Configure required services to start when the host starts, and start the services:

   ```
   for svc in rabbitmq-server memcached snmpd; do chkconfig $svc on; service $svc start; done
   ```

2.4. (Optional) Install a remote Zenoss DataStore

Follow these steps to install and configure the Zenoss DataStore to run on a remote host.

1. Log in to the Resource Manager master host as `root`, or as a user with superuser privileges.

2. Stop Zenoss DataStore, and configure it not to start when the system starts.

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

3. Switch user to `zenoss`.

   ```
   su - zenoss
   ```

4. Open `$ZENHOME/etc/global.conf.example` in a text editor and change property values as indicated in the following list.

   - `zodb-host` - Change to the hostname or IP address of the remote Zenoss DataStore host.

   - `zep-host` - Change to the hostname or IP address of the remote Zenoss DataStore host.

   - `zodb-port` - Change to `13306`.

   - `zep-port` - Change to `13306`.

   Save and close `$ZENHOME/etc/global.conf.example`.

5. Log out of the Resource Manager master host.

6. Log in to the the remote Zenoss DataStore host as `root`, or as a user with superuser privileges.

7. Download the Zenoss DataStore RPM file from the Zenoss Support site. Contact your Zenoss representative for login credentials.

8. Determine whether MySQL is installed, and if so, remove it.

   ```
   rpm -qa | grep -i mysql
   ```

   If the preceding command returns a package name, use the returned name in the following command.

   ```
   yum -y remove Package-Name
   ```

9. Enable inbound TCP traffic on port 13306, or enable traffic on all ports.

   To enable traffic on all ports, enter the following commands.

   ```
   IPv4: service iptables stop; chkconfig iptables off
   ```

```
IPv6: service ip6tables stop; chkconfig ip6tables off
```

Note

You may open all ports at this time, and then close unneeded ports later, after Zenoss DataStore is installed.

10. Disable SELinux.

```
/bin/echo 0 > /selinux/enforce
/bin/sed -i.bak -e 's/^SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config
```

11. Install Zenoss DataStore:

```
RHEL/CentOS 5: yum -y --nogpgcheck localinstall zends-Version.el5.x86_64.rpm
RHEL/CentOS 6: yum -y --nogpgcheck localinstall zends-Version.el6.x86_64.rpm
```

12. Start Zenoss DataStore and ensure it runs at system startup:

```
service zends start
chkconfig --add zends
```

13. Switch user to `zenoss`.

```
su - zenoss
```

14. Start the Zenoss DataStore command shell.

```
zends -u root
```

15. Enable remote access to the Zenoss DataStore. In the prompt that appears, enter the following commands:

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

2.5. Install MySQLTuner

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

1. Log into the Resource Manager master host as `zenoss`.

2. Change to the following directory:

```
cd $ZENHOME/bin
```

3. Retrieve the MySQLTuner script:

```
wget --no-check-certificate mysqltuner.pl
```

4. Set permissions on the file:

```
chmod 755 mysqltuner.pl
```

2.6. Install and initialize ZenUp

This release of Resource Manager includes a recommended patch set (RPS) to fix issues uncovered since it was first made available. To install and manage patch sets, Zenoss provides the Zenoss Service Dynamics ZenUp patch management tool, which must be installed and initialized before you start Resource Manager.

Follow these steps to initialize ZenUp for this release of Resource Manager.

1. Log in to the Resource Manager master host as `root`, or as a user with superuser privileges.
2. Download the following items from the https://support.zenoss.com site.
   - The ZenUp RPM file.
   - The "pristine" file for this release of Resource Manager.
   - The current RPS (`.zup`) file.

   Contact your Zenoss representative for login credentials.
3. Install ZenUp with one of the following commands:

   ```
   RHEL/CentOS 5: yum -y --nogpgcheck localinstall zenup-version.el5.x86_64.rpm
   RHEL/CentOS 6: yum -y --nogpgcheck localinstall zenup-version.el6.x86_64.rpm
   ```
4. Log in as user `zenoss`.
5. Register Resource Manager 4.2.4 with ZenUp by specifying the "pristine" file.

   ```
   zenup init zenoss_resmgr-4.2.4-XXXX-elX-pristine.tgz $ZENHOME
   ```

   The `zenup` command displays messages as it works. If you encounter an error, contact Zenoss Support.
6. Verify the result.

   ```
   zenup status
   ```

   ZenUp displays information similar to the following example.

   ```
   Product: zenoss-resmgr-4.2.4 (id = zenoss-resmgr-4.2.4)
   Home: /opt/zenoss
   Revision: 0
   Updated On: timestamp
   ```

   For more information about ZenUp, refer to *Zenoss Service Dynamics ZenUp Installation and Administration*.

2.7. Start Resource Manager

As the root user, run the following command to start the system:

```
service zenoss start
```

The startup process typically takes at least 15 minutes, and displays many messages.

2.8. (Optional) Install the Windows Monitoring ZenPack

Log in to the Resource Manager master host as `root`, or as a user with superuser privileges.

1. Stop Resource Manager:

   ```
   service zenoss stop
   ```
2. Start the event server and its catalog service:

   ```
   su - zenoss -c "zeneventserver start; zencatalogservice start"
   ```
3. Install the Windows Monitoring RPM file:

```
RHEL/CentOS 5: yum -y --nogpgcheck localinstall zenoss_msmonitor-version.el5.x86_64.rpm
RHEL/CentOS 6: yum -y --nogpgcheck localinstall zenoss_msmonitor-Version.el6.x86_64.rpm
```

4. Start Resource Manager:

```
service zenoss start
```

2.9. Install the recommended patch set

Follow these steps to install the latest RPS (`.zup`) file for this release of Resource Manager.

1. Log in as `zenoss`, and stop Resource Manager.

   ```
   zenoss stop
   ```

   Occasionally, the stop command does not terminate all of the Resource Manager daemons. To check, enter the following command:

   ```
   pgrep -fl ${ZENHOME}
   ```

   If the `pgrep` command returns a result, kill the processes.

   ```
   pkill -f ${ZENHOME}
   ```

2. Perform a dry run of the RPS install.

   ```
   zenup install --dry-run zenoss_resmgr-version.zup
   ```

   If `zenup` completes without errors, repeat the command, without the `--dry-run` argument.

   ```
   zenup install zenoss_resmgr-version.zup
   ```

   The `zenup` command installs the RPS.

3. Start Resource Manager.

   ```
   zenoss start
   ```

2.10. Getting started

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

Note

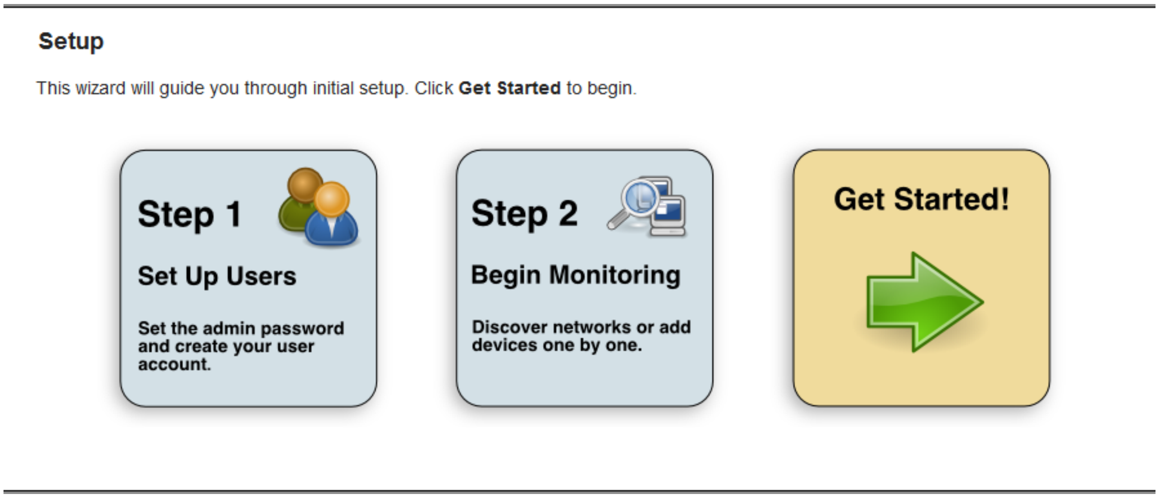
If you cannot successfully browse to your Resource Manager installation, then you may need to add an entry to your hosts file for the fully qualified domain name (FQDN) of your installation.

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



Setup

This wizard will guide you through initial setup. Click **Get Started** to begin.

Step 1

Set Up Users

Set the admin password and create your user account.

Step 2

Begin Monitoring

Discover networks or add devices one by one.

Get Started!

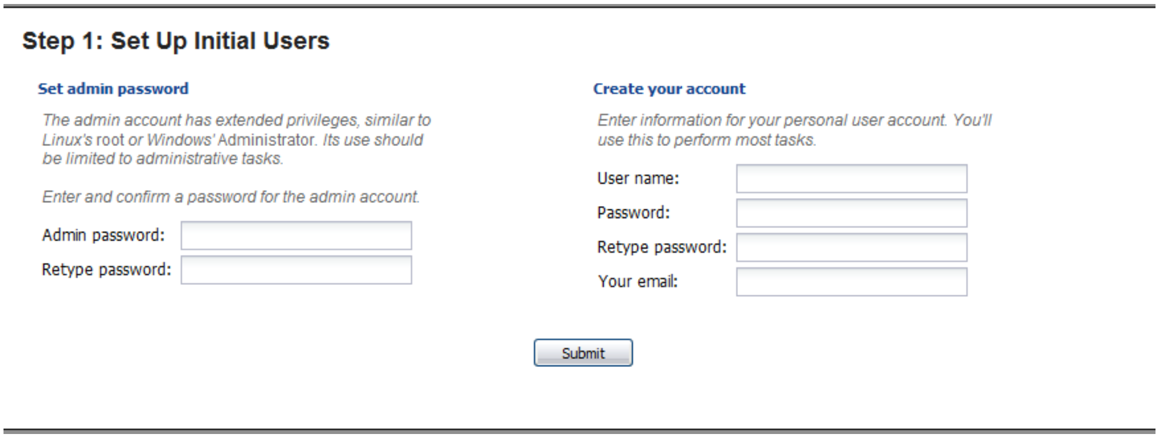
Using this wizard, you will:

- 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 Set up Initial Users panel appears.

Figure 2.2. Setup Wizard: Step 1



Step 1: Set Up Initial Users

Set admin password

The admin account has extended privileges, similar to Linux's root or Windows' Administrator. Its use should be limited to administrative tasks.

Enter and confirm a password for the admin account.

Admin password:

Retype password:

Create your account

Enter information for your personal user account. You'll use this to perform most tasks.

User name:

Password:

Retype password:

Your email:

2.10.1. Set the administrator password and create a user

Follow these steps to select a password for the administrator account (`admin`) and create a 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.

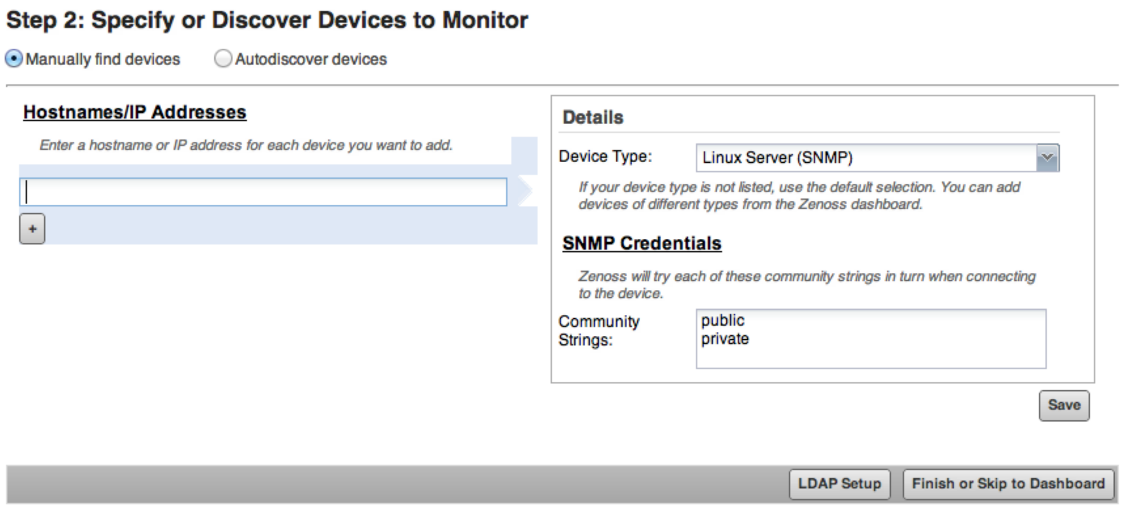
3. Click **Next**.

   The Specify or Discover Devices to Monitor panel appears.

Note

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

Figure 2.3. Setup Wizard: Step 2



Step 2: Specify or Discover Devices to Monitor

● Manually find devices ○ Autodiscover devices

Hostnames/IP Addresses

Enter a hostname or IP address for each device you want to add.

Details

Device Type: Linux Server (SNMP)

If your device type is not listed, use the default selection. You can add devices of different types from the Zenoss dashboard.

SNMP Credentials

Zenoss will try each of these community strings in turn when connecting to the device.

Community Strings: public
private

2.10.2. Add devices

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

2.10.2.1. Adding devices manually

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

1. Make sure the **Manually find devices** option is selected.

2. Enter a fully qualified domain name or IP address

3. 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.)

4. Enter the appropriate credentials used to authenticate against the device.

   ### Note

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

5. If you want to add additional domain names or IP addresses, click the + icon to add an additional row. Then, repeat steps 2-4.

6. To add the devices, click **Save**.

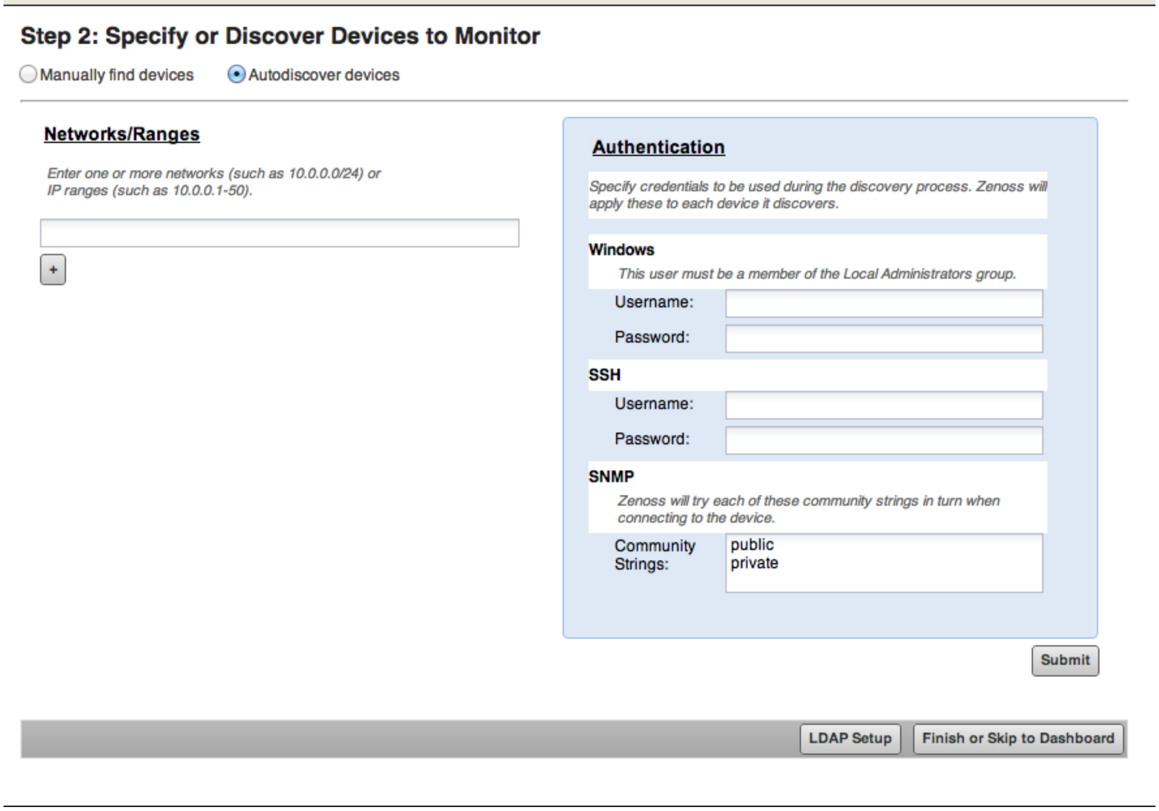
   Resource Manager models the devices in the background.

2.10.2.2. Discovering devices

To discover devices:

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

   Figure 2.4. Setup Wizard: Step 2



Step 2: Specify or Discover Devices to Monitor

○ Manually find devices ● Autodiscover devices

Networks/Ranges

Enter one or more networks (such as 10.0.0.0/24) or IP ranges (such as 10.0.0.1-50).

Authentication

Specify credentials to be used during the discovery process. Zenoss will apply these to each device it discovers.

Windows

This user must be a member of the Local Administrators group.

Username:

Password:

SSH

Username:

Password:

SNMP

Zenoss will try each of these community strings in turn when connecting to the device.

Community Strings: public
private

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 the + icon. 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 **Submit**.

   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.

2.10.2.3. 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 3. Adding a collector

This chapter describes how to add a local or remote collector to Resource Manager.

Adding local collectors to the Resource Manager master host is useful when the master host is not resource-constrained, and you would like to simplify the administration of many devices of the same type, or devices of different types with different collection cycles.

Adding remote collectors is useful when the master host is resource-constrained, and in the following types (or combinations) of environments:

- large environments (many devices)
- dense environments (devices with many components)
- distributed environments (devices are far apart, geographically or topologically)

For more information about remote collectors, refer to the chapter titled "Distributed Collector" in *Zenoss Service Dynamics Resource Management Extended Monitoring*.

> **Note**
>
> Whether local or remote, the Resource Manager master host needs an additional 500 MB of memory to efficiently manage each additional collector.

3.1. Adding a local collector

Follow these steps to deploy a local collector.

1. Log in to the Resource Manager console interface as a user with ZenManager or Manager permissions.
2. Click Advanced > Collectors.

   The console displays the deployed hubs and collectors.
3. Select the `localhost` hub.
4. From the action menu next to Zenoss Collectors, select Add Collector....

   The Add Collector page displays.
5. Select Install locally.
6. Enter a logical name for the collector in the Collector ID field.

   The name is used as the prefix of the collector's daemons on the master host. For example, if the name is `routers`, then the SNMP monitoring daemon is `routers_zenperfsnmp`.
7. Click Add Collector.

   Resource Manager submits the "Add collector" job to the jobs queue. Upon completion, the console updates the Advanced > Collectors page with an entry for the new collector.

3.2. Adding a remote collector

Resource Manager provides 3 optons for adding collector hosts, to support different security scenarios. The following table associates the security scenarios with the names of the options.

Table 3.1.

Option Name	Security Scenario	Notes
root user password	• The Resource Manager administrator has the root password of the collector host. • After the collector is added, the zenoss user on the master host can log in as root on the collector host.	After the collector is added, all communications with the collector host use keys for authentication. The collector host's root password is not stored or reused.
root user SSH keys	• The Resource Manager administrator does not have the root password of the collector host. • After the collector is added, the zenoss user on the master host can log in as root on the collector host.	After the collector is added, this option works the same way as the preceding option.
zenoss user SSH keys	• The Resource Manager administrator does not have the root password of the collector host. • The zenoss user on the master host can not log in as root on the collector host.	This is the most secure option.

Note

When Resource Manager is started for the first time, the Distributed Collector ZenPack generates a new, unique key pair for user zenoss, with the OpenSSH **ssh-keygen** command. You may use the generated key pair to deploy a collector, or replace the pair with a new or different key pair before deploying a collector. For more information about Distributed Collector security, refer to the chapter titled "Distributed Collector" in *Zenoss Service Dynamics Resource Management Extended Monitoring*.

3.2.1. Preparing to install

The following items are required or recommended.

- Master and collector hosts must be able to resolve each others' fully-qualified domain names, either through entries in /etc/hosts, or through a nameserver on their network.
- The Linux distribution installed on the collector host must be the same as the distribution installed on the master host. The master copies binaries to the collector during installation and updates.
- Zenoss recommends using a separate filesystem for $ZENHOME/perf, and mounting it with the noatime option set, so that inode access times are not updated. Also, Resource Manager stores performance data in individual files, and makes 4 KB block updates. Under such a high volume/low throughput usage pattern, journaled file systems can be detrimental to I/O performance.

Note

If you are using the zenoss user SSH keys option, skip ahead to Zenoss user SSH keys.

If you are using the root user password option or the root user SSH keys option to add a remote collector, follow these steps to prepare a collector host.

1. Disable Security-Enhanced Linux (SELinux).

   a. Log in as `root`, or as a user with superuser privileges.

   b. Disable enforcing mode temporarily (avoiding the need to reboot) with the following command:

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

   c. Disable enforcing mode permanently by editing the `/etc/selinux/config` file with the following command:

   ```
   /bin/sed -i.bak -e 's/^SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config
   ```

2. Enable the ports identified in Appendix B, "Port requirements".

3. Determine whether OpenJDK Java is installed.

   ```
   rpm -qa | grep openjdk
   ```

   Remove it if necessary.

   ```
   yum -y remove openjdk-package-name
   ```

4. Download the self-installing RPM of Oracle Java SE Runtime Environment 6u31 from the Java SE 6 Downloads page. The file to download is `jre-6u31-linux-x64-rpm.bin`.

5. Enter the following commands to install and verify the JRE.

   ```
   chmod +x ./jre-6u31-linux-x64-rpm.bin
   ./jre-6u31-linux-x64-rpm.bin
   echo "export JAVA_HOME=/usr/java/default/bin" >> /etc/profile
   java -version
   ```

6. Install the Zenoss dependencies repository.

   ```
   RHEL/CentOS 5: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el5.noarch.rpm
   RHEL/CentOS 6: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el6.noarch.rpm
   ```

7. Clean up `yum` caches.

   ```
   yum clean all
   ```

8. Install Memcached, Net-SNMP, Redis, and RRDtool.

   ```
   yum -y install memcached net-snmp net-snmp-utils redis rrdtool-1.4.7
   ```

9. Install Nagios plugins.

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

10. Configure required services to start when the host starts, and start the services:

    ```
    for svc in memcached snmpd; do chkconfig $svc on; service $svc start; done
    ```

3.2.2. Root user password

Follow these steps to install a new collector using the root password of the collector host.

1. Log in to the Resource Manager console interface as a user with ZenManager or Manager permissions.

2. Click Advanced > Collectors.

   The console displays the deployed hubs and collectors.

3. Select the hub through which the new collector's data will flow.

4. From the action menu next to Zenoss Collectors, select Add Collector....

   The Add Collector page displays.

5. Select Install remotely.

6. Select root user password.

7. Provide values for the following fields:

   - Collector ID, the logical name of the collector.

     This name is used as the prefix for Resource Manager daemons on the collector host. For example, if the name is `denver`, then the SNMP monitoring daemon is `denver_zenperfsnmp`.

   - Host, the fully-qualified domain name or IP address of the collector host.

   - Root Password, the password of the `root` user on the collector host.

     The password is not stored or re-used; it is used only to set up SSH key authentication between the master host and the collector host.

8. Click **Add Collector**.

   Resource Manager submits the "Add collector" job to the jobs queue. Upon completion, the console updates the Advanced > Collectors page with an entry for the new collector.

3.2.3. Root user SSH keys

Follow these steps to install a new collector using the SSH authentication keys of the `zenoss` user on the master host. (You must have the `root` user password for the collector host to perform this procedure.)

1. Log in to the collector host as `root`.

2. If no SSH directory is present (`/root/.ssh`), enter the following commands:

   ```
   mkdir /root/.ssh
   chmod 700 /root/.ssh
   ```

3. If no authorized keys file is present (`/root/.ssh/authorized_keys`), enter the following commands:

   ```
   touch /root/.ssh/authorized_keys
   chmod 600 /root/.ssh/authorized_keys
   ```

4. Log in to the master host as user `zenoss` and enter the following command. Substitute the fully-qualified domain name of the collector host for *collector-host*:

   ```
   cat $HOME/.ssh/id_rsa.pub | ssh -l root \
               collector-host "cat - >> /root/.ssh/authorized_keys"
   ```

   The **ssh** command prompts you to confirm the connection.

5. Enter `yes`.

   The **ssh** command prompts you for the password of the `root` user on the collector host.

6. Enter the password.

The **ssh** command invokes **cat** to append the RSA public key of the zenoss user on the master host to the authorized keys file of the root user on the collector host. In addition, **ssh** adds the collector host to the known hosts file of the zenoss user on the master host.

7. Log in to the Resource Manager console interface as a user with ZenManager or Manager permissions.
8. Click Advanced > Collectors.

   The console displays the deployed hubs and collectors.
9. Select the hub through which the new collector's data will flow.
10. From the action menu next to Zenoss Collectors, select Add Collector....

    The Add Collector page displays.
11. Select root user SSH keys.
12. Provide values for the following fields:
    - Collector ID, the logical name of the collector.

      This name is used as the prefix for Resource Manager daemons on the collector host. For example, if the name is denver, then the SNMP monitoring daemon is denver_zenperfsnmp.
    - Host, the fully-qualified domain name or IP address of the collector host.
13. Click **Add Collector**.

    Resource Manager submits the "Add collector" job to the jobs queue. Upon completion, the console updates the Advanced > Collectors page with an entry for the new collector.

3.2.4. Zenoss user SSH keys

Perform these procedures to install a new collector using the SSH authentication keys of the zenoss user on the master host. (Someone must have root privileges on the collector host to perform the first procedure.)

Install Resource Manager on the collector host

1. Log in to the collector host as root, or as a user with superuser privileges.
2. Follow the instructions in the section titled "Prerequisite Tasks", in the chapter titled "Installing Resource Manager", with the following exceptions:
   - Do not start Zenoss DataStore.
   - Configure Zenoss DataStore not to start when the system starts:

     ```
     chkconfig zends off
     ```
3. Install the Resource Manager RPM file.

   ```
   RHEL/CentOS 5: yum -y --nogpgcheck localinstall zenoss_resmgr-version.el5.x86_64.rpm
   RHEL/CentOS 6: yum -y --nogpgcheck localinstall zenoss_resmgr-version.el6.x86_64.rpm
   ```
4. Configure required services to start when the collector host starts, and start the services:

```
for svc in memcached snmpd; do chkconfig $svc on; service $svc start; done
```

5. Configure Resource Manager not to start when the system starts:

   ```
   chkconfig zenoss off
   ```

6. Set a new password for the `zenoss` user and provide it to the person who performs the next procedure.

Deploy the collector to the collector host

1. Log in to the collector host as user `zenoss` and enter the following commands:

   ```
   cd $HOME
   mkdir .ssh
   chmod 700 .ssh
   touch .ssh/authorized_keys
   chmod 600 .ssh/authorized_keys
   ```

2. Log in to the master host as user `zenoss` and enter the following command. Substitute the fully-qualified domain name of the collector host for *collector-host*:

   ```
   cat $HOME/.ssh/id_rsa.pub | ssh -l zenoss \
               collector-host "cat - >> /home/zenoss/.ssh/authorized_keys"
   ```

   The **ssh** command prompts you to confirm the connection.

3. Enter `yes`.

   The **ssh** command prompts you for the password of the `zenoss` user on the collector host.

4. Enter the password.

   The **ssh** command invokes **cat** to append the RSA public key of the `zenoss` user on the master host to the authorized keys file of the `zenoss` user on the collector host. In addition, **ssh** adds the collector host to the known hosts file of the `zenoss` user on the master host.

5. Log in to the Resource Manager console interface as a user with ZenManager or Manager permissions.

6. Click Advanced > Collectors.

   The console displays the deployed hubs and collectors.

7. Select the hub through which the new collector's data will flow.

8. From the action menu next to Zenoss Collectors, select Add Collector....

   The Add Collector page displays.

9. Select zenoss user SSH keys.

10. Provide values for the following fields:

    - Collector ID, the logical name of the collector.

      This name is used as the prefix for Resource Manager daemons on the collector host. For example, if the name is `denver`, then the SNMP monitoring daemon is `denver_zenperfsnmp`.

    - Host, the fully-qualified domain name or IP address of the collector host.

11. Click **Add Collector**.

Resource Manager submits the "Add collector" job to the jobs queue. Upon completion, the console updates the Advanced > Collectors page with an entry for the new collector.

Chapter 4. Installing a hub

This chapter describes how to install a Resource Manager hub on a host other than the master host. The `zenhub` daemon is CPU-intensive, so off-loading it to another host is useful when the master host is resource-constrained, or in environments with multiple collectors. For more information about remote hubs, refer to the chapter titled "Distributed Collector" in *Zenoss Service Dynamics Resource Management Extended Montitoring*.

The installation process includes preparation steps on the hub host, and deployment steps through the Resource Manager console interface.

4.1. Preparing to install

The following items are required or recommended.

- Resource Manager master and hub hosts must be placed on the same subnet. If they are not, network latency negates many of the benefits of installing a hub host.

- Master and hub hosts must be able to resolve each others' fully-qualified domain names, either through entries in `/etc/hosts`, or through a nameserver on their network.

- The Linux distribution installed on the hub host must be the same as the distribution installed on the master host. The master copies binaries to the hub during installation and updates.

Follow these steps to prepare a hub host.

1. Disable Security-Enhanced Linux (SELinux).

   a. Log in as `root`, or as a user with superuser privileges.

   b. Disable enforcing mode temporarily (avoiding the need to reboot) with the following command:

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

   c. Disable enforcing mode permanently by editing the `/etc/selinux/config` file with the following command:

   ```
   /bin/sed -i.bak -e 's/^SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config
   ```

2. Enable the ports identified in Appendix B, "Port requirements".

3. Install the Zenoss dependencies repository.

   ```
   RHEL/CentOS 5: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el5.noarch.rpm
   RHEL/CentOS 6: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el6.noarch.rpm
   ```

4. Clean up `yum` caches.

   ```
   yum clean all
   ```

5. Install Memcached and Net-SNMP, configure them to start when the host starts, and start them.

   ```
   yum -y install memcached net-snmp net-snmp-utils
   for svc in memcached snmpd; do chkconfig $svc on; service $svc start; done
   ```

6. Install RRDtool.

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

7. Install Nagios plugins.

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

8. Enable access to Zenoss DataStore.

   a. Log in to the Zenoss DataStore host (which may be a host other than the Resource Manager master host) as user `zenoss`.

   b. Log in to the Zenoss DataStore server as `root`.

   ```
   zends -u root
   ```

   c. Enter the following commands at the `zends` prompt. (Replace *remote-hub* with the fully-qualified domain name of the hub host.)

   ```
   zends> GRANT SELECT on mysql.user to zenoss@'remote-hub' IDENTIFIED BY "zenoss";
   zends> GRANT ALL PRIVILEGES ON zenoss_zep.* to zenoss@'remote-hub' IDENTIFIED BY "zenoss";
   zends> GRANT ALL PRIVILEGES ON zodb.* to zenoss@'remote-hub' IDENTIFIED BY "zenoss";
   zends> FLUSH PRIVILEGES;
   zends> quit
   ```

   d. *If the Resource Manager master host is also the Zenoss DataStore host*, log in to the master host as user `zenoss`, and edit the `$ZENHOME/etc/global.conf` file. Change the values of the following properties from `localhost` to the fully-qualified domain name of the master host:

   - `zodb-host`
   - `amqphost`
   - `zep-host`
   - `zencatalogservice-uri`

4.2. Deploying a hub

Resource Manager provides 3 optons for adding hub hosts, to support different security scenarios. The following table associates the security scenarios with the names of the options.

Table 4.1.

Option Name	Security Scenario	Notes
`root user password`	• The Resource Manager administrator has the `root` password of the hub host. • After the hub is added, the `zenoss` user on the master host can log in as `root` on the hub host.	After the hub is added, all communications with the hub host use keys for authentication. The hub host's `root` password is not stored or reused.
`root user SSH keys`	• The Resource Manager administrator does not have the `root` password of the hub host. • After the hub is added, the `zenoss` user on the master host can log in as `root` on the hub host.	After the hub is added, this option works the same way as the preceding option.

Option Name	Security Scenario	Notes
`zenoss user SSH keys`	• The Resource Manager administrator does not have the `root` password of the hub host. • The `zenoss` user on the master host can not log in as `root` on the hub host.	This is the most secure option.

Note

When Resource Manager is started for the first time, the Distributed Collector ZenPack generates a new, unique key pair for user `zenoss`, with the OpenSSH **ssh-keygen** command. You may use the generated key pair to deploy a hub, or replace the pair with a new or different key pair before deploying a hub. For more information about Distributed Collector security, refer to the chapter titled "Distributed Collector" in *Zenoss Service Dynamics Resource Management Extended Montitoring*.

4.2.1. Root user password

Follow these steps to install a new hub using the root password of the hub host.

1. Log in to the Resource Manager console interface as a user with ZenManager or Manager permissions.

2. Click Advanced > Collectors.

   The console displays the deployed hubs and collectors.

3. From the action menu next to Hubs, select Add Hub....

   The Add Hub page displays.

4. Select `root user password`.

5. Provide values for the following fields:

   - Hub ID, the logical name of the hub.

     The name can be any unique combination of letters, digits, and dashes.

   - Host, the fully-qualified domain name or IP address of the hub host.

   - Root Password, the password of the `root` user on the hub host.

     The password is not stored or re-used; it is used only to set up SSH key authentication between the master host and the hub host.

   - Port, the number of the port on which the hub listens for collectors.

     The default port is 8790.

   - Hub Password, the password collectors use to log in to the hub.

     The default password is `zenoss`.

   - XML RPC Port, the port on which the hub listens for xml-rpc requests from collectors or other API clients.

     The default port is 8083.

6. Click Add Hub.

   Resource Manager submits the "Add hub" job to the jobs queue. Upon completion, the console updates the Advanced > Collectors page with an entry for the new hub.

4.2.2. Root user SSH keys

Follow these steps to install a new hub using the SSH authentication keys of the `zenoss` user on the master host. (You must have the `root` user password for the hub host to perform this procedure.)

1. Log in to the hub host as `root`.

2. If no SSH directory is present (`.ssh`), enter the following commands:

   ```
   mkdir .ssh
   chmod 700 .ssh
   ```

3. If no authorized keys file is present (`.ssh/authorized_keys`), enter the following commands:

   ```
   touch .ssh/authorized_keys
   chmod 600 .ssh/authorized_keys
   ```

4. Log in to the master host as user `zenoss` and enter the following command. Substitute the fully-qualified domain name of the hub host for *hub-host*:

   ```
   cat $HOME/.ssh/id_rsa.pub | ssh -l root \
               hub-host "cat - >> /root/.ssh/authorized_keys"
   ```

   The **ssh** command prompts you to confirm the connection.

5. Enter `yes`.

   The **ssh** command prompts you for the password of the `root` user on the hub host.

6. Enter the password.

   The **ssh** command invokes **cat** to append the RSA public key of the `zenoss` user on the master host to the authorized keys file of the `root` user on the hub host. In addition, **ssh** adds the hub host to the known hosts file of the `zenoss` user on the master host.

7. Log in to the Resource Manager console interface as a user with ZenManager or Manager permissions.

8. Click Advanced > Collectors.

   The console displays the deployed hubs and collectors.

9. From the action menu next to Hubs, select Add Hub....

   The Add Hub page displays.

10. Select root user SSH keys.

11. Provide values for the following fields:

    - Hub ID, the logical name of the hub.

      The name can be any unique combination of letters, digits, and dashes.

    - Host, the fully-qualified domain name or IP address of the hub host.

- Port, the number of the port on which the hub listens for collectors.

  The default port is 8790.
- Hub Password, the password collectors use to log in to the hub.

  The default password is `zenoss`.
- XML RPC Port, the port on which the hub listens for xml-rpc requests from collectors or other API clients.

  The default port is 8083.

12. Click Add Hub.

    Resource Manager submits the "Add hub" job to the jobs queue. Upon completion, the console updates the Advanced > Collectors page with an entry for the new hub.

4.2.3. Zenoss user SSH keys

Perform these procedures to install a new hub using the SSH authentication keys of the `zenoss` user on the master host. (Someone must have `root` privileges on the hub host to perform the first procedure.)

Install Resource Manager on the hub host

1. Log in to the hub host as `root`, or as a user with superuser privileges.
2. Follow the instructions in the section titled "Prerequisite Tasks", in the chapter titled "Installing Resource Manager", with the following exceptions:
   - Do not start Zenoss DataStore.
   - Configure Zenoss DataStore not to start when the system starts:

     ```
     chkconfig zends off
     ```
3. Install the Resource Manager RPM file.

   ```
   RHEL/CentOS 5: yum -y --nogpgcheck localinstall zenoss_resmgr-version.el5.x86_64.rpm
   RHEL/CentOS 6: yum -y --nogpgcheck localinstall zenoss_resmgr-version.el6.x86_64.rpm
   ```
4. Configure required services to start when the hub host starts, and start the services:

   ```
   for svc in memcached snmpd; do chkconfig $svc on; service $svc start; done
   ```
5. Configure Resource Manager not to start when the system starts:

   ```
   chkconfig zenoss off
   ```
6. Set a new password for the `zenoss` user and provide it to the person who performs the next procedure.

Deploy the hub to the hub host

1. Log in to the hub host as user `zenoss` and enter the following commands:

   ```
   cd $HOME
   mkdir .ssh
   chmod 700 .ssh
   touch .ssh/authorized_keys
   ```

```
chmod 600 .ssh/authorized_keys
```

2. Log in to the master host as user `zenoss` and enter the following command. Substitute the fully-qualified domain name of the hub host for *hub-host*:

   ```
   cat $HOME/.ssh/id_rsa.pub | ssh -l zenoss \
               hub-host "cat - >> /home/zenoss/.ssh/authorized_keys"
   ```

   The **ssh** command prompts you to confirm the connection.

3. Enter `yes`.

   The **ssh** command prompts you for the password of the `zenoss` user on the hub host.

4. Enter the password.

   The **ssh** command invokes **cat** to append the RSA public key of the `zenoss` user on the master host to the authorized keys file of the `zenoss` user on the hub host. In addition, **ssh** adds the hub host to the known hosts file of the `zenoss` user on the master host.

5. Log in to the Resource Manager console interface as a user with ZenManager or Manager permissions.

6. Click Advanced > Collectors.

   The console displays the deployed hubs and collectors.

7. From the action menu next to Hubs, select Add Hub....

   The Add Hub page displays.

8. Select zenoss user SSH keys.

9. Provide values for the following fields:

   - Hub ID, the logical name of the hub.

     The name can be any unique combination of letters, digits, and dashes.

   - Host, the fully-qualified domain name or IP address of the hub host.

   - Port, the number of the port on which the hub listens for collectors.

     The default port is 8790.

   - Hub Password, the password collectors use to log in to the hub.

     The default password is `zenoss`.

   - XML RPC Port, the port on which the hub listens for xml-rpc requests from collectors or other API clients.

     The default port is 8083.

10. Click Add Hub.

    Resource Manager submits the "Add hub" job to the jobs queue. Upon completion, the console updates the Advanced > Collectors page with an entry for the new hub.

Chapter 5. Performance tuning

The sections in this chapter describe the options for optimizing the performance of Resource Manager.

5.1. 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**
>
> Run this command only on the Resource Manager master host (not on remote collectors).

5.2. 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.

5.3. 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.

5.3.1. Using ZenTune

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

Figure 5.1. 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 5.2. 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.

5.4. 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.

5.5. Increasing maximum file descriptors

A Resource Manager host can require in excess of 10000 open files. For optimal performance, Zenoss recommends that you increase the minimum number of open files for the zenoss user to 4096, and the maximum number of open files to a value greater than the anticipated number of open files needed by Resource Manager.

For example, to configure a host for a minimum of 4096 and a maximum of 10240 open files, follow these steps:

1. Log in to the host as root.
2. Add the minimum open files value to `/etc/security/limits.conf`:

   ```
   /bin/echo "zenoss soft nofile 4096" >> /etc/security/limits.conf
   ```

3. Add the maximum open files value:

   ```
   /bin/echo "zenoss hard nofile 10240" >> /etc/security/limits.conf
   ```

4. Add the following lines to the zenoss user's `$HOME/.bash_profile` file:

   ```
   if [ "${USER}" = "zenoss" ]; then
     ulimit -n 10240
   fi
   ```

5. Source the `$HOME/.bash_profile` file, or log in as user zenoss to use the new value.

   ### Note

   In the preceding example, the value specified with the **ulimit** command may be decreased (but not increased) without editing the `/etc/security/limits.conf` file.

5.6. 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.

Table 5.1. zenrrdcached settings

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

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

```
iostat -x 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.

5.7. 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
```

5.7.1. 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 in `messaging.conf`:

```
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
```

5.7.2. 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.

5.7.3. 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
```

5.7.4. 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).

5.8. Configuring the heartbeat monitor

The heartbeat monitor allows daemons that have connections to RabbitMQ to set up heartbeats with the message broker, and is part of Zenoss Service Dynamics Global Operations Management. 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 --amqpheartbeat option at the command line.

Note

Setting the heartbeat value to 0 turns it off.

5.9. Increasing the maximum binary message size

The default maximum size for binary messages sent to or from the catalog service is 10MB. If the modeler fails and the `zencatalogservice.log` file contains a `java.lang.OutOfMemoryError` entry, then the maximum size for binary messages most likely needs to be increased.

To increase the maximum size for binary messages, follow these steps.

1. Log in to the Resource Manager master host as `zenoss`.
2. Open the `$ZENHOME/etc/zencatalogservice.conf` file in a text editor.
3. Remove the comment character from the `vmargs` option, and then append the new maximum size setting to the line. The completed entry should match the following example:

   ```
   vmargs -server -Dcatalogservice.websocket.max_binary_message_size=20971520
   ```

   The value is specified in bytes; 20971520 bytes equals 20 MB.
4. Save and close the `$ZENHOME/etc/zencatalogservice.conf` file.
5. Restart the catalog service daemon.

   ```
   zencatalogservice restart
   ```

5.10. Normalizing data collection rates

Data collection rates are inconsistent when the number of simultaneous processes that the `zenoss` user is allowed to open is too low. Zenoss recommends that you increase the process limit for the `zenoss` user, on the Resource Manager master host and on collector hosts.

To configure a host for 102,400 simultaneous processes, follow these steps:

1. Log in to the host as `root` or as a user with superuser privilges.

2. Add the process limit value to `/etc/security/limits.conf`:

   ```
   /bin/echo "zenoss - nproc 102400" >> /etc/security/limits.conf
   ```

3. Switch user to `zenoss` and restart Resource Manager.

   ```
   su - zenoss
   zenoss restart
   ```

5.11. Adjusting RabbitMQ Server throttling

The default setting for memory-based flow-control (throttling) in RabbitMQ Server is 40% of installed RAM. When the server's memory usage exceeds this threshold, connections are temporarily blocked. Under heavy load, this behavior is sub-optimal.

For more information about RabbitMQ Server tuning, refer to the following web pages:

- http://www.rabbitmq.com/memory.html

- http://www.rabbitmq.com/configure.html

To check the current theshold setting, enter the following command:

```
service rabbitmq-server status | grep vm_memory_high_watermark
```

To disable the threshold, follow these steps.

1. Log in to the Resource Manager master host as `root` or as a user with superuser privilges.

2. Create directory `/etc/rabbitmq`, if necessary.

   ```
   test ! -d /etc/rabbitmq && mkdir -p /etc/rabbitmq
   ```

3. Change the threshold setting.

   ```
   echo "[{rabbit, [{vm_memory_high_watermark, 100}]}]." >> /etc/rabbitmq/rabbitmq.config
   ```

4. Restart RabbitMQ Server.

   ```
   service rabbitmq-server restart
   ```

Chapter 6. Upgrading Version 3.2.1

Zenoss fully supports upgrading Zenoss Enterprise 3.2.1 installations to Resource Manager version 4.2.4. However, the procedure is not documented in this guide. For more information, contact Zenoss Professional Services.

Chapter 7. Upgrading Version 4.1.1

This chapter provides instructions for upgrading Resource Manager version 4.1.1 installations to version 4.2.4. Sections are presented in order, and some are optional.

Note

- Resource Manager 4.2.4 requires a 64-bit platform. If you are upgrading from a 32-bit platform, please contact Zenoss Support for assistance.
- The instructions in this chapter assume that the hosts to upgrade can retrieve files through the internet. To upgrade hosts without internet access, contact Zenoss Support.
- This version of Resource Manager may use new or different ports than the version to upgrade. Before upgrading, review Appendix B, "Port Requirements".

Note

Perform an upgrade in a development or testing environment before performing it in a production environment. In particular, only Zenoss-maintained ZenPacks are tested and supported in an upgrade. Test all other ZenPacks for compatibility with this version of Resource Manager before upgrading a production environment.

7.1. Stopping Resource Manager

If your installation *does not* include remote hub or collector hosts, follow these steps to stop Resource Manager.

1. Log in to the master host as `zenoss`.
2. Stop all daemons.

   ```
   zenoss stop
   ```

   Occasionally, the stop command does not terminate all of the Resource Manager daemons. To check, enter the following command:

   ```
   pgrep -fl ${ZENHOME}
   ```

   If the `pgrep` command returns a result, kill the processes.

   ```
   pkill -f ${ZENHOME}
   ```

If your installation *does* include remote remote hub or collector hosts, follow these steps to stop Resource Manager.

1. Log in to the Resource Manager master host as user `zenoss`, and stop the web server daemon.

   ```
   zenwebserver stop
   ```

2. Log in to each collector host, and stop Resource Manager daemons.

   ```
   ssh root@remote-collector-host
   service zenoss stop
   exit
   ```

3. Log in to each hub host, and stop Resource Manager daemons.

   ```
   ssh root@remote-hub-host
   ```

```
service zenoss stop
exit
```

4. Log in to the Resource Manager master host as user `zenoss`, and stop all daemons.

   ```
   zenoss stop
   ```

   Occasionally, the stop command does not terminate all of the Resource Manager daemons. To check, enter the following command:

   ```
   pgrep -fl ${ZENHOME}
   ```

   If the `pgrep` command returns a result, kill the processes.

   ```
   pkill -f ${ZENHOME}
   ```

7.2. Preparing to upgrade

The procedure in this section prepares your installation for upgrade to version 4.2.4.

1. Log in to the Resource Manager master host as `zenoss`.
2. Create a backup.

   ```
   zenbackup
   ```

3. Delete the RRDtool files of a misnamed collector.

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

4. Remove the distributed ping correlation ZenPack, if present.

   a. Start the event server daemon.

      ```
      zeneventserver start
      ```

   b. Determine whether the ZenPack is installed.

      ```
      zenpack --list | grep DistributedPingCorrelation
      ```

   c. Remove the ZenPack.

      ```
      zenpack --remove=ZenPack.zenoss.DistributedPingCorrelation
      ```

   d. Stop the event server daemon.

      ```
      zeneventserver stop
      ```

5. Start a shell as `root`, or as a user with superuser privileges, and disable automatic start.

   ```
   su -
   chkconfig zenoss off
   ```

6. Create a backup of the Resource Manager software. For example:

   ```
   cd /opt/zenoss
   tar --exclude backups --exclude perf --exclude log -czf /home/zenoss/my4.1.1.tgz .
   ```

   ### Note

   This backup is important. The upgrade process does not preserve customizations to configuration files in `$ZENHOME/etc`. The customizations must be manually re-applied, after the new version is installed.

7. Back up and delete patches.

   a. Determine whether patches are installed.

   ```
   ls ./.pc ./patches ./patches-binary
   ```

   If the directories are present, Zenoss patches are installed. (Custom patches may be located elsewhere, but typically are not.) An alternative method of checking for the presence of patches is to query the `quilt` repository:

   ```
   quilt applied
   ```

   Typically, the `quilt` command displays the list of installed patches.

   b. Back up the patches.

   ```
   tar czf /home/zenoss/my4.1.1-patches.tgz ./.pc ./patches ./patches-binary
   ```

   c. Delete the patches.

   ```
   rm -rf ./.pc ./patches ./patches-binary
   ```

8. Download the self-installing RPM of Oracle Java SE Runtime Environment 6u31 from the Java SE 6 Downloads page. The file to download is `jre-6u31-linux-x64-rpm.bin`.

9. Make the RPM installer executable, install the JRE, and verify the installed version.

   ```
   chmod +x /path-to-installer/jre-6u31-linux-x64-rpm.bin
   /path-to-installer/jre-6u31-linux-x64-rpm.bin
   java -version
   ```

10. Upgrade the Zenoss dependencies repository.

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

11. Clean up `yum` caches.

    ```
    yum clean all
    ```

12. If either of the following statements are true, perform the procedure in the appendix titled "Upgrading RabbitMQ Server" before continuing:

    - You are using customized RabbitMQ Server queues.
    - You are using a server other than the Resource Manager master host for RabbitMQ Server.

    If neither of the preceding statements are true, continue to the next section.

7.3. Upgrading Zenoss DataStore

The procedure in this section upgrades Zenoss DataStore on the Resource Manager master host. (If your installation includes a remote Zenoss DataStore host, perform the procedure in the next section, too.) The Resource Manager master host needs upgraded client libraries, both to communicate with Zenoss DataStore, and to copy the libraries to remote hub and collector hosts.

Note

The Zenoss DataStore upgrade installer preserves Resource Manager data, plus any customizations it finds, in the `/opt/zends/etc/zends.cnf` file.

1. Log in to the Resource Manager master host as user `root`, or as a user with superuser privileges.

2. If necessary, stop Zenoss DataStore.

   ```
   service zends stop
   ```

3. Download the Zenoss DataStore RPM file from the https://support.zenoss.com site. Contact your Zenoss representative for login credentials.

4. Upgrade Zenoss DataStore.

   ```
   yum -y --nogpgcheck localinstall zends-version.el5.x86_64.rpm
   ```

   You may see the following warning message:

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

   If so, merge the new properties and values in `zends.cnf.rpmnew` with your customizations in `zends.cnf`.

5. Edit the `/opt/zenoss/etc/global.conf` file with the following command:

   ```
   sed -i.bak -e 's#^mysqlsocket .*$#mysqlsocket /var/lib/zends/zends.sock#' \
   /opt/zenoss/etc/global.conf
   ```

   In addition, edit the `/opt/zenoss/etc/zope.conf` file with the following command:

   ```
   sed -i.bak -re 's#([[:space:]]*)unix_socket .*$#\1unix_socket /var/lib/zends/zends.sock#' \
   /opt/zenoss/etc/zope.conf
   ```

6. If you *are not* using a remote Zenoss DataStore host, enter the following commands:

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

   If you *are* using a remote Zenoss DataStore host, enter the following command:

   ```
   chkconfig --level 2345 zends off
   ```

7.3.1. Upgrading a remote Zenoss DataStore

The procedure in this section upgrades a remote Zenoss DataStore. Perform this procedure *in addition to* upgrading Zenoss DataStore on the Resource Manager master host.

1. Log in to the remote Zenoss DataStore host as user `root`, or as a user with superuser privileges.

2. Stop Zenoss DataStore.

   ```
   service zends stop
   ```

3. Download the Zenoss DataStore RPM file from the https://support.zenoss.com site. Contact your Zenoss representative for login credentials.

4. Upgrade Zenoss DataStore.

   ```
   yum -y --nogpgcheck localinstall zends-version.el5.x86_64.rpm
   ```

   You may see the following warning message:

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

   If so, merge the new properties and values in `zends.cnf.rpmnew` with your customizations in `zends.cnf`.

5. Start Zenoss DataStore.

   ```
   service zends start
   ```

7.4. Upgrading Resource Manager

Perform the following procedure on the Resource Manager master host.

1. Download the Resource Manager RPM file from the https://support.zenoss.com site. Contact your Zenoss representative for login credentials.

2. Upgrade Resource Manager.

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

   You may see the following warnings during the upgrade process:

   ```
   warning: /opt/zenoss/bin/zenoss_init_pre saved as /opt/zenoss/bin/zenoss_init_pre.rpmsave
   warning: /opt/zenoss/bin/zenoss_upgrade_pre saved as /opt/zenoss/bin/zenoss_upgrade_pre.rpmsave
   ```

   If you are using a remote Zenoss DataStore host, or if you have made any customizations to these scripts, review the new and saved versions of the files, and merge the changes.

   If you encounter any errors during the upgrade, contact Zenoss Support.

3. Configure required services to start when the host starts, and start the services:

   ```
   for svc in rabbitmq-server memcached snmpd; do chkconfig $svc on; service $svc start; done
   ```

   Note

   Do not start Resource Manager at this time.

7.5. Post-installation steps

Perform these steps on the Resource Manager master host.

1. Log in as `zenoss`.

2. Change directory, download the MySQLTuner script, and make it executable.

   ```
   cd $ZENHOME/bin
   wget --no-check-certificate mysqltuner.pl
   chmod 755 mysqltuner.pl
   ```

3. Append at least two entries to the `$ZENHOME/etc/global.conf` file.

   - Append the following property-value pairs to `$ZENHOME/etc/global.conf`:

     ```
     amqpadminport 55672
     amqpadminusessl 0
     ```

   - *If you are using a password for the Zenoss DataStore root user*, append the following lines to `$ZENHOME/etc/global.conf`:

     ```
     zodb-admin-password root-password
     zep-admin-password root-password
     ```

     Replace *root-password* with the password of the Zenoss DataStore `root` user.

4. If your installation includes a customized `zencommand` with a hard-coded path to the former location for Nagios plugins, add a symbolic link to the new location:

   ```
   ln -s  /usr/lib64/nagios/plugins /opt/zenoss/libexec
   ```

5. If you customized configuration files in `$ZENHOME/etc`, re-apply those customizations at this time.

6. This version of Resource Manager introduces a new daemon, `zredis`, to help correlate "ping down" events. If you are using a `daemons.txt` file on the master host, add `zredis` to the file.

7. Upgrade any ZenPacks developed by you, the Zenoss community, or Zenoss Professional Services. For more information about installing and updating ZenPacks, see *Zenoss Service Dynamics Resource Management Extended Monitoring*.

   ### Note

   This step is critical. ZenPacks commonly include JavaScript-based additions or changes to the Resource Manager console, and incompatible JavaScript in outdated ZenPacks can disable the console.

8. Delete browser caches, to avoid incompatibilities in the console interface. For example, to clear the Firefox cache, press Ctrl-Shift-R.

7.6. Installing Zenoss Service Dynamics ZenUp

This release of Resource Manager includes a recommended patch set (RPS) to fix issues uncovered since it was first made available. To install and manage patch sets, Zenoss provides the ZenUp patch management tool, which must be installed before you start migrating data. For more information about ZenUp, refer to *Zenoss Service Dynamics ZenUp Installation and Administration*.

Follow these steps to install ZenUp and register Resource Manager 4.2.4.

1. Download the following items from the https://support.zenoss.com site.

   - The ZenUp RPM file.

   - The "pristine" file for Resource Manager 4.2.4.

   - The most recent RPS (`.zup`) file.

   Contact your Zenoss representative for login credentials.

2. Log in to the Resource Manager master host as `root`, or as a user with superuser privileges.

3. Install ZenUp.

   ```
   yum --nogpgcheck localinstall zenup-version.el5.x86_64.rpm
   ```

4. Log in as user `zenoss`.

5. Rename the `$ZENHOME/bin/zenquilt_update.sh` file.

   ```
   mv $ZENHOME/bin/zenquilt_update.sh $ZENHOME/bin/zenquilt_update.sh.old
   ```

6. Register Resource Manager 4.2.4 with ZenUp by specifying the "pristine" file.

   ```
   zenup init zenoss_resmgr-4.2.4-XXXX.elX-pristine.tgz $ZENHOME
   ```

   The `zenup` command displays messages as it works. If you encounter an error, contact Zenoss Support.

7. Verify the registration.

   ```
   zenup status
   ```

   ZenUp displays information similar to the following example.

```
Product: zenoss-resmgr-4.2.4 (id = zenoss-resmgr-4.2.4)
Home: /opt/zenoss
Revision: 0
Updated On: timestamp
```

7.7. Migrating data

Follow these steps to migrate 4.1.1 data to 4.2.4.

1. Log in to the Resource Manager master host as `root`, or as a user with superuser privileges.
2. Configure Resource Manager to start when the host starts, and start the migration process.

   ```
   chkconfig zenoss on
   service zenoss start
   ```

   The process takes at least 20 minutes, and displays many messages.

7.8. (Optional) Upgrading Windows Monitoring ZenPacks

To upgrade Windows Monitoring ZenPacks, follow these steps:

1. Log in to the Resource Manager master host as `root`, or as a user with superuser privileges.
2. Download the Windows Monitoring RPM file from the https://support.zenoss.com site. Contact your Zenoss representative for login credentials.
3. Stop Resource Manager.

   ```
   service zenoss stop
   ```

   Occasionally, the stop command does not terminate all of the Resource Manager daemons. To check, enter the following command:

   ```
   pgrep -fl ${ZENHOME}
   ```

   If the `pgrep` command returns a result, kill the processes.

   ```
   pkill -f ${ZENHOME}
   ```

4. Start the event server and its catalog service.

   ```
   su - zenoss -c "zeneventserver start; zencatalogservice start"
   ```

   Install the ZenPacks.

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

5. Start Resource Manager.

   ```
   service zenoss start
   ```

7.9. Apply latest recommended patch set

Follow these steps to apply the latest 4.2.4 RPS.

1. Log in as `zenoss`, and stop all daemons.

   ```
   zenoss stop
   ```

Occasionally, the stop command does not terminate all of the Resource Manager daemons. To check, enter the following command:

```
pgrep -fl ${ZENHOME}
```

If the `pgrep` command returns a result, kill the processes.

```
pkill -f ${ZENHOME}
```

2. Perform a dry run of the RPS install.

```
zenup install --dry-run zenoss_resmgr-version.zup
```

If `zenup` completes without errors, repeat the command, without the `--dry-run` argument.

```
zenup install zenoss_resmgr-version.zup
```

The `zenup` command installs the RPS.

3. Review the customizations that you saved earlier. If they are still required and their code works with the new version, apply the customizations with the ZenUp tool. For example:

```
zenup patch feature_XYZ.diff -m"add feature XYZ to 4.2.4"
```

4. Start Resource Manager.

```
zenoss start
```

7.10. Upgrading remote hubs

Perform these steps on each remote hub host to upgrade.

Note

Review the current port requirements in Appendix B, "Port Requirements", to determine whether hub hosts have new or changed port requirements.

1. Log in to the hub host as `root`, or as a user with `root` privileges.

2. Download the self-installing RPM of Oracle Java SE Runtime Environment 6u31 from the Java SE 6 Downloads page. The file to download is `jre-6u31-linux-x64-rpm.bin`.

3. Make the RPM installer executable, install the JRE, and verify the installed version.

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

4. Update the Zenoss dependencies repository.

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

5. Clean up `yum` caches.

```
yum clean all
```

6. Update Memcached, Net-SNMP, and RRDtool.

```
yum -y install memcached net-snmp net-snmp-utils rrdtool-1.4.7
```

7. Install Nagios plugins.

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

8. Configure required services to start when the host starts, and start the services:

```
for svc in memcached snmpd; do chkconfig $svc on; service $svc start; done
```

9. Log in to the Resource Manager console as a user with ZenManager or Manager permissions.

   - Select Advanced.
   - Click Collectors.
   - Select the hub to upgrade, and then select Update Hub from the Action menu.

7.11. Upgrading remote collectors

Perform these steps on each remote collector host to upgrade.

> ### Note
>
> Review the current port requirements in Appendix B, "Port Requirements", to determine whether collector hosts have new or changed port requirements.

1. Log in to the collector host as `root`, or as a user with `root` privileges.

2. Delete the RRDtool files of a misnamed collector.

```
su - zenoss -c "find $ZENHOME -name 'ifOperStatus_ifOperStatus.rrd' -delete"
```

3. Remove the `zredis` configuration file, if present.

```
su - zenoss -c "rm -f $ZENHOME/etc/zredis.conf"
```

4. Download the self-installing RPM of Oracle Java SE Runtime Environment 6u31 from the Java SE 6 Downloads page. The file to download is `jre-6u31-linux-x64-rpm.bin`.

5. Make the RPM installer executable, install the JRE, and verify the installed version.

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

6. Update the Zenoss dependencies repository.

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

7. Clean up `yum` caches.

```
yum clean all
```

8. Update Memcached, Net-SNMP, and RRDtool, and install Redis.

```
yum -y install memcached net-snmp net-snmp-utils redis rrdtool-1.4.7
```

9. Update Nagios plugins.

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

10. Configure required services to start when the host starts, and start the services:

```
for svc in memcached rabbitmq-server snmpd; do chkconfig $svc on; service $svc start; done
```

11. Log in to the Resource Manager console as a user with ZenManager or Manager permissions.

    - Select Advanced.
    - Click Collectors.
    - Select the collector to upgrade, and then select Update Collector from the Action menu.

7.12. Performance tuning

Finally, review the contents of the chapter titled "Performance Tuning". New tuning options have been added since the previous release.

Chapter 8. Upgrading Version 4.2.3

This chapter provides instructions for upgrading Resource Manager version 4.2.3 installations to version 4.2.4. Sections are presented in order, and some are optional.

Note

- The instructions in this chapter assume that the hosts to upgrade can retrieve files through the internet. To upgrade hosts without internet access, contact Zenoss Support.
- This version of Resource Manager may use new or different ports than the version to upgrade. Before upgrading, review Appendix B, "Port requirements".

Note

Perform an upgrade in a development or testing environment before performing it in a production environment. In particular, only Zenoss-maintained ZenPacks are tested and supported in an upgrade. Test all other ZenPacks for compatibility with this version of Resource Manager before upgrading a production environment.

8.1. Stopping Resource Manager

If your installation *does not* include remote hub or collector hosts, follow these steps to stop Resource Manager.

1. Log in to the master host as `zenoss`.
2. Stop all daemons.

   ```
   zenoss stop
   ```

   Occasionally, the stop command does not terminate all of the Resource Manager daemons. To check, enter the following command:

   ```
   pgrep -fl ${ZENHOME}
   ```

   If the `pgrep` command returns a result, kill the processes.

   ```
   pkill -f ${ZENHOME}
   ```

If your installation *does* include remote remote hub or collector hosts, follow these steps to stop Resource Manager.

1. Log in to the Resource Manager master host as user `zenoss`, and stop the web server daemon.

   ```
   zenwebserver stop
   ```

2. Log in to each collector host, and stop Resource Manager daemons.

   ```
   ssh root@remote-collector-host
   service zenoss stop
   exit
   ```

3. Log in to each hub host, and stop Resource Manager daemons.

   ```
   ssh root@remote-hub-host
   service zenoss stop
   exit
   ```

4. Log in to the Resource Manager master host as user `zenoss`, and stop all daemons.

```
zenoss stop
```

Occasionally, the stop command does not terminate all of the Resource Manager daemons. To check, enter the following command:

```
pgrep -fl ${ZENHOME}
```

If the `pgrep` command returns a result, kill the processes.

```
pkill -f ${ZENHOME}
```

8.2. Preparing to upgrade

The procedure in this section prepares your installation for upgrade to version 4.2.4.

1. Log in to the Resource Manager master host as `zenoss`.

2. Create a backup.

   ```
   zenbackup
   ```

3. Delete the RRDtool files of a misnamed collector.

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

4. Switch user to `root`, or to a user with superuser privileges, and disable automatic start.

   ```
   su - root
   chkconfig zenoss off
   ```

5. Create a backup of the Resource Manager software. For example:

   ```
   cd /opt/zenoss
   tar --exclude backups --exclude perf --exclude log -czf /home/zenoss/my4.2.3.tgz .
   ```

6. Install the Zenoss dependencies repository, which simplifies the installation of most required packages:

   ```
   RHEL/CentOS 5: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el5.noarch.rpm
   RHEL/CentOS 6: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el6.noarch.rpm
   ```

7. Clean up `yum` caches.

   ```
   yum clean all
   ```

8. Download the self-installing RPM of Oracle Java SE Runtime Environment 6u31 from the Java SE 6 Downloads page. The file to download is `jre-6u31-linux-x64-rpm.bin`.

9. Make the RPM installer executable, install the JRE, and verify the installed version.

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

10. If either of the following statements are true, perform the procedure in the appendix titled "Upgrading RabbitMQ Server" before continuing:

    - You are using customized RabbitMQ Server queues.

    - You are using a server other than the Resource Manager master host for RabbitMQ Server.

    If neither of the preceding statements are true, continue to the next section.

8.3. Installing Zenoss Service Dynamics ZenUp

The Zenoss Service Dynamics ZenUp patch management tool replaces Quilt, and helps manage the upgrade process.

Note

If ZenUp is already installed, proceed to the section titled "Checking for customizations".

To determine whether Zenup is installed, log in as `zenoss`, and enter `zenup`. If the result is `-bash: zenup: command not found`, ZenUp is not installed.

Follow these steps to install ZenUp.

1. Download the following items from the https://support.zenoss.com site.

   - The ZenUp RPM file.
   - The "pristine" file for Resource Manager 4.2.3.

   Contact your Zenoss representative for login credentials.

2. Log in as `root`, or as a user with superuser privileges.

3. Install ZenUp with one of the following commands:

   ```
   RHEL/CentOS 5: yum -y --nogpgcheck localinstall zenup-version.el5.x86_64.rpm
   RHEL/CentOS 6: yum -y --nogpgcheck localinstall zenup-version.el6.x86_64.rpm
   ```

8.3.1. Registering Resource Manager with ZenUp

1. Log in as user `zenoss`.

2. Register Resource Manager 4.2.3 with ZenUp by specifying the "pristine" file.

   ```
   zenup init zenoss_resmgr-4.2.3-XXXX.elX-pristine.tgz $ZENHOME
   ```

   If no patches are installed, `zenup` displays only the following messages:

   ```
   Validating...
   Initializing...
   Replacing Resource Manager shebang in python files.
   Checking for zenquilt installation
   Success!
   ```

3. *If no patches are installed,* perform these steps:

   a. Delete the registration.

      ```
      zenup delete --force zenoss-resmgr-4.2.3
      ```

   b. Proceed to the section titled "Upgrading Zenoss DataStore".

   If patches are installed, proceed to the next section.

8.3.2. Checking for customizations

This procedure checks for customizations of items in the installed patch set, and of items that are not in the installed patch set.

1. Log in as `root`, or as a user with superuser privileges.

2. Back up the patches.

   ```
   cd /opt/zenoss
   tar czf /home/zenoss/my4.2.3-patches.tgz ./.pc ./patches ./patches-binary
   ```

3. Log in as user `zenoss`.

4. Download the `zencheckrps` script from the https://support.zenoss.com site. Contact your Zenoss representative for login credentials.

   ### Note

   You may place the script in any temporary location.

5. Make the script executable.

   ```
   chmod +x /path-to-script/zencheckrps
   ```

6. Start the script.

   ```
   /path-to-script/zencheckrps
   INFO: zencheckrps  date:2013-07-25-150729-CDT  uname-rm:2.6.18-348.el5 x86_64
   INFO: checking Zenoss against RPS in '/opt/zenoss' (0 args provided)
   =================================================================================
   INFO: checking 62 patches against RPS list: /opt/zenoss/patches/series.423
   INFO: compared quilt patches - found 0 differences
   =================================================================================
   INFO: checking 1 jars against RPS dir: /opt/zenoss/patches-binary
   INFO: compared jars - found 0 differences
   =================================================================================
   INFO: checking 9 ZenPacks against config: /opt/zenoss/etc/zenquilt_update.conf
   INFO: compared ZenPacks - found 0 differences
   =================================================================================
   INFO: checking compiled Javascript file: /opt/zenoss/.../zenoss-compiled.js
   INFO: compared compiled Javascript - found 0 differences
   =================================================================================
   INFO: showing version of rabbitmq-server: rabbitmq-server-2.8.6-1
   INFO: showing version of zends: zends-5.5.25a-1.r64630.el5
   INFO: showed versions of pertinent packages
   =================================================================================
   INFO: r73518 RPS version installed correctly
   ```

   The preceding result shows that none of the patches in RPS r73518 are customized. If your result shows customized patches, make a note of them.

7. Delete the `zencheckrps` script.

   ```
   rm /path-to-script/zencheckrps
   ```

8. Check for customizations that are not tracked by Quilt.

   ```
   zenup diff > $HOME/upgrade.diff
   ```

9. Review the contents of `$HOME/upgrade.diff` and make a note of any customizations.

10. Delete the ZenUp registration for Resource Manager 4.2.3.

    ```
    zenup delete --force zenoss-resmgr-4.2.3
    ```

11. Rename the `$ZENHOME/bin/zenquilt_update.sh` file.

```
mv $ZENHOME/bin/zenquilt_update.sh $ZENHOME/bin/zenquilt_update.sh.old
```

12. Log in as `root`, or as a user with superuser privileges, and delete the patches.

```
cd /opt/zenoss
rm -rf ./.pc ./patches ./patches-binary
```

8.4. Upgrading Zenoss DataStore

The procedure in this section upgrades Zenoss DataStore on the Resource Manager master host. (If your installation includes a remote Zenoss DataStore host, perform the procedure in the next section, too.) The Resource Manager master host needs upgraded client libraries, both to communicate with Zenoss DataStore, and to copy the libraries to remote hub and collector hosts.

Note

> The Zenoss DataStore upgrade installer preserves Resource Manager data, plus any customizations it finds, in the `/opt/zends/etc/zends.cnf` file.

1. Log in to the Resource Manager master host as user `root`, or as a user with superuser privileges.

2. If necessary, stop Zenoss DataStore.

```
service zends stop
```

3. Download the Zenoss DataStore RPM file from the https://support.zenoss.com site. Contact your Zenoss representative for login credentials.

4. Upgrade Zenoss DataStore.

```
RHEL/CentOS 5: yum -y --nogpgcheck localinstall zends-version.el5.x86_64.rpm
RHEL/CentOS 6: yum -y --nogpgcheck localinstall zends-version.el6.x86_64.rpm
```

You may see the following warning message:

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

If so, merge the new properties and values in `zends.cnf.rpmnew` with your customizations in `zends.cnf`.

5. If you *are not* using a remote Zenoss DataStore host, enter the following commands:

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

If you *are* using a remote Zenoss DataStore host, enter the following command:

```
chkconfig --level 2345 zends off
```

8.4.1. Upgrading a remote Zenoss DataStore

The procedure in this section upgrades a remote Zenoss DataStore. Perform this procedure *in addition to* upgrading Zenoss DataStore on the Resource Manager master host.

1. Log in to the remote Zenoss DataStore host as user `root`, or as a user with superuser privileges.

2. Stop Zenoss DataStore.

```
service zends stop
```

3. Download the Zenoss DataStore RPM file from the https://support.zenoss.com site. Contact your Zenoss representative for login credentials.

4. Upgrade Zenoss DataStore.

   ```
   RHEL/CentOS 5: yum -y --nogpgcheck localinstall zends-version.el5.x86_64.rpm
   RHEL/CentOS 6: yum -y --nogpgcheck localinstall zends-version.el6.x86_64.rpm
   ```

   You may see the following warning message:

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

   If so, merge the new properties and values in `zends.cnf.rpmnew` with your customizations in `zends.cnf`.

5. Start Zenoss DataStore.

   ```
   service zends start
   ```

8.5. Upgrading Resource Manager

Perform the following procedure on the Resource Manager master host.

1. Download the Resource Manager RPM file from the https://support.zenoss.com site. Contact your Zenoss representative for login credentials.

2. Install the Redis datastore.

   ```
   yum -y install redis
   ```

3. Upgrade Resource Manager with one of the following commands:

   ```
   RHEL/CentOS 5: rpm -Uvh zenoss_resmgr-version.el5.x85_64.rpm
   RHEL/CentOS 6: rpm -Uvh zenoss_resmgr-version.el6.x85_64.rpm
   ```

   You may see the following warnings during the upgrade process:

   ```
   warning: /opt/zenoss/bin/zenoss_init_pre saved as /opt/zenoss/bin/zenoss_init_pre.rpmsave
   warning: /opt/zenoss/bin/zenoss_upgrade_pre saved as /opt/zenoss/bin/zenoss_upgrade_pre.rpmsave
   ```

   If you are using a remote Zenoss DataStore host, or if you have made any customizations to these scripts, review the new and saved versions of the files, and merge the changes.

   If you encounter any errors during the upgrade, contact Zenoss Support.

4. Clean up `yum` caches.

   ```
   yum clean all
   ```

5. Configure required services to start when the host starts, and start the services:

   ```
   for svc in rabbitmq-server memcached snmpd; do chkconfig $svc on; service $svc start; done
   ```

   ### Note

   Do not start Resource Manager at this time.

8.5.1. Post-installation steps

Perform these steps on the Resource Manager master host.

1. Log in as `zenoss`.

2. Change directory, download the MySQLTuner script, and make it executable.

   ```
   cd $ZENHOME/bin
   wget --no-check-certificate mysqltuner.pl
   chmod 755 mysqltuner.pl
   ```

3. If your installation includes a customized `zencommand` with a hard-coded path to the former location for Nagios plugins, add a symbolic link to the new location:

   ```
   ln -s  /usr/lib64/nagios/plugins /opt/zenoss/libexec
   ```

4. This version of Resource Manager introduces a new daemon, `zredis`, to help correlate "ping down" events. If you are using a `daemons.txt` file on the master host, add `zredis` to the file.

5. Upgrade any ZenPacks developed by you, the Zenoss community, or Zenoss Professional Services. For more information about installing and updating ZenPacks, see *Zenoss Service Dynamics Resource Management Extended Monitoring Guide*.

   Note

   This step is critical. ZenPacks commonly include JavaScript-based additions or changes to the Resource Manager console, and incompatible JavaScript in outdated ZenPacks can disable the console.

6. Delete browser caches, to avoid incompatibilities in the console interface. For example, to clear the Firefox cache, press Ctrl-Shift-R.

8.5.2. Registering 4.2.4 with ZenUp

Follow these steps to register Resource Manager 4.2.4 with ZenUp.

1. Download the following items from the https://support.zenoss.com site.

   - The "pristine" file for Resource Manager 4.2.4.
   - The current RPS (`.zup`) file.

   Contact your Zenoss representative for login credentials.

2. Log in as user `zenoss`.

3. Register Resource Manager 4.2.4 with ZenUp by specifying the "pristine" file.

   ```
   zenup init zenoss_resmgr-4.2.4-XXXX.elX-pristine.tgz $ZENHOME
   ```

   The `zenup` command displays messages as it works.

4. Verify the registration.

   ```
   zenup status
   ```

   ZenUp displays information similar to the following example.

   ```
   Product: zenoss-resmgr-4.2.4 (id = zenoss-resmgr-4.2.4)
   Home: /opt/zenoss
   Revision: 0
   Updated On: timestamp
   ```

5. Log in as `root`, or as a user with superuser privileges.

6. Configure Resource Manager to start when the host starts, and start the migration process.

   ```
   chkconfig zenoss on
   service zenoss start
   ```

   The process takes at least 20 minutes, and displays many messages.

8.5.3. (Optional) Upgrading Windows Monitoring ZenPacks

To upgrade Windows Monitoring ZenPacks, follow these steps:

1. Log in to the Resource Manager master host as `root`, or as a user with superuser privileges.
2. Download the Windows Monitoring RPM file from the https://support.zenoss.com site. Contact your Zenoss representative for login credentials.
3. Stop Resource Manager.

   ```
   zenoss stop
   ```

4. Start the event server and its catalog service.

   ```
   su - zenoss -c "zeneventserver start; zencatalogservice start"
   ```

   Install the ZenPacks.

   ```
   RHEL/CentOS 5: yum -y --nogpgcheck localinstall zenoss_msmonitor-version.el5.x86_64.rpm
   RHEL/CentOS 6: yum -y --nogpgcheck localinstall zenoss_msmonitor-version.el6.x86_64.rpm
   ```

5. Start Resource Manager.

   ```
   service zenoss start
   ```

8.5.4. Installing the RPS and customizations

Follow these steps to install the current recommended patch set (RPS) as well as any customizations you discovered earlier.

1. Log in as `zenoss`, and stop all daemons.

   ```
   zenoss stop
   ```

   Occasionally, the stop command does not terminate all of the Resource Manager daemons. To check, enter the following command:

   ```
   pgrep -fl ${ZENHOME}
   ```

   If the `pgrep` command returns a result, kill the processes.

   ```
   pkill -f ${ZENHOME}
   ```

2. Perform a dry run of the RPS install.

   ```
   zenup install --dry-run zenoss_resmgr-version-SPXXX.zup
   ```

3. Install the RPS.

   - *If you used only Quilt to manage RPS updates for version 4.2.3*, enter the following command:

     ```
     zenup install --force zenoss_resmgr-version-SPXXX.zup
     ```

   - *If you used ZenUp to manage the most recent RPS updates for version 4.2.3*, enter the following command:

```
zenup install zenoss_resmgr-version-SPXXX.zup
```

The zenup command installs the RPS.

4. Review the customizations that you saved earlier. If they are still required and their code works with the new version, apply the customizations with the ZenUp tool. For example:

```
zenup patch feature_XYZ.diff -m"add feature XYZ to 4.2.4"
```

8.6. Upgrading remote hubs

Perform these steps on each remote hub host to upgrade.

Note

Review the current port requirements in Appendix B, "Port Requirements", to determine whether hub hosts have new or changed port requirements.

1. Log in to the hub host as `root`, or as a user with `root` privileges.

2. Download the self-installing RPM of Oracle Java SE Runtime Environment 6u31 from the Java SE 6 Downloads page. The file to download is `jre-6u31-linux-x64-rpm.bin`.

3. Make the RPM installer executable, install the JRE, and verify the installed version.

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

4. Update the Zenoss dependencies repository.

```
RHEL/CentOS 5: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el5.noarch.rpm
RHEL/CentOS 6: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el6.noarch.rpm
```

5. Update Memcached, Net-SNMP, and RRDtool.

```
yum -y install memcached net-snmp net-snmp-utils rrdtool-1.4.7
```

6. Clean up `yum` caches.

```
yum clean all
```

7. Install Nagios plugins.

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

8. Configure required services to start when the host starts, and start the services:

```
for svc in memcached snmpd; do chkconfig $svc on; service $svc start; done
```

9. Log in to the Resource Manager console as a user with ZenManager or Manager permissions.

   - Select Advanced.
   - Click Collectors.
   - Select the hub to upgrade, and then select Update Hub from the Action menu.

8.7. Upgrading remote collectors

Perform these steps on each remote collector host to upgrade.

Note

Review the current port requirements in Appendix B, "Port Requirements", to determine whether collector hosts have new or changed port requirements.

1. Log in to the collector host as `root`, or as a user with `root` privileges.
2. Delete the RRDtool files of a misnamed collector.

   ```
   su - zenoss -c "find $ZENHOME -name 'ifOperStatus_ifOperStatus.rrd' -delete"
   ```

3. Download the self-installing RPM of Oracle Java SE Runtime Environment 6u31 from the Java SE 6 Downloads page. The file to download is `jre-6u31-linux-x64-rpm.bin`.
4. Make the RPM installer executable, install the JRE, and verify the installed version.

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

5. Update the Zenoss dependencies repository.

   ```
   RHEL/CentOS 5: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el5.noarch.rpm
   RHEL/CentOS 6: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el6.noarch.rpm
   ```

6. Update Memcached, Net-SNMP, and RRDtool, and install Redis.

   ```
   yum -y install memcached net-snmp net-snmp-utils redis rrdtool-1.4.7
   ```

7. Clean up `yum` caches.

   ```
   yum clean all
   ```

8. Update Nagios plugins.

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

9. Configure required services to start when the host starts, and start the services:

   ```
   for svc in memcached rabbitmq-server snmpd; do chkconfig $svc on; service $svc start; done
   ```

10. Log in to the Resource Manager console as a user with ZenManager or Manager permissions.
    - Select Advanced.
    - Click Collectors.
    - Select the collector to upgrade, and then select Update Collector from the Action menu.

8.8. Performance tuning

Finally, review the contents of the chapter titled "Performance Tuning". New tuning options have been added since the previous release.

Appendix A. Upgrading RabbitMQ Server

This appendix describes how to upgrade RabbitMQ Server without upgrading Resource Manager. Follow these procedures if your Resource Manager deployment relies on custom queues, or if RabbitMQ Server is deployed off-host (not on a Resource Manager host).

Unless otherwise instructed, perform all steps in this procedure as `root`, or as a user with superuser privileges.

A.1. Prepare to upgrade

1. Log in to the host to upgrade as `root`, or as a user with superuser privileges.

2. *If you are upgrading a RabbitMQ Server instance on a Resource Manager host*, upgrade the Zenoss dependencies repository.

   ```
   RHEL/CentOS 5: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el5.noarch.rpm
   RHEL/CentOS 6: rpm -Uvh http://deps.zenoss.com/yum/zenossdeps-4.2.x-1.el6.noarch.rpm
   ```

   If you are upgrading an off-host RabbitMQ Server instance, download the RabbitMQ RPM file.

   ```
   RHEL/CentOS 5: wget http://deps.zenoss.com/yum/4.2.x/centos/5\
      /os/x86_64/rabbitmq-server-2.8.6-1.noarch.rpm
   RHEL/CentOS 6: wget http://deps.zenoss.com/yum/4.2.x/centos/6\
      /os/x86_64/rabbitmq-server-2.8.6-1.noarch.rpm
   ```

A.2. Stop Resource Manager

If your installation **does not** include remote hub or collector hosts, follow these steps to stop Resource Manager.

1. Log in to the Resource Manager master host as `zenoss`.

2. Stop all daemons.

   ```
   zenoss stop
   ```

   Occasionally, the stop command does not terminate all of the Resource Manager daemons. To check, enter the following command:

   ```
   pgrep -fl ${ZENHOME}
   ```

   If the `pgrep` command returns a result, kill the processes.

   ```
   pkill -f ${ZENHOME}
   ```

If your installation **does** include remote remote hub or collector hosts, follow these steps to stop Resource Manager.

1. Log in to the Resource Manager master host as user `zenoss`, and stop the web server daemon.

   ```
   zenwebserver stop
   ```

2. Log in to each collector host, and stop Resource Manager daemons.

   ```
   ssh root@remote-collector-host
   service zenoss stop
   ```

```
exit
```

3. Log in to each hub host, and stop Resource Manager daemons.

```
ssh root@remote-hub-host
service zenoss stop
exit
```

4. Log in to the Resource Manager master host as user `zenoss`, and stop all daemons.

```
zenoss stop
```

   Occasionally, the stop command does not terminate all of the Resource Manager daemons. To check, enter the following command:

```
pgrep -fl ${ZENHOME}
```

   If the `pgrep` command returns a result, kill the processes.

```
pkill -f ${ZENHOME}
```

A.3. Stop RabbitMQ Server

1. Check 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 erases 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 use RabbitMQ and are not Zenoss-supported, ensure that all of the messages in the relevant queues are consumed before continuing this upgrade. Consult the provider of the customizations for help regarding the sensitivity of lost messages.

2. Stop RabbitMQ.

```
service rabbitmq-server stop
```

3. Verify that RabbitMQ is stopped.

```
service rabbitmq-server status
```

   You should see output similar to:

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

A.4. Upgrade RabbitMQ Server

1. *If you are upgrading a RabbitMQ Server instance on a Resource Manager host*, use the Zenoss dependencies repository.

   ```
   yum upgrade rabbitmq-server
   ```

   If you are upgrading an off-host RabbitMQ Server instance, use the local RabbitMQ RPM file.

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

2. Start RabbitMQ Server.

   ```
   service rabbitmq-server start
   ```

3. Create a script named `configure_amqp.sh`, and add the following content to it

   ```
   #!/bin/sh

   RABBITMQ_USER=zenoss
   RABBITMQ_PASS=zenoss
   RABBITMQ_VHOST=/zenoss
   RABBITMQCTL="`which rabbitmqctl`"

   configure_amqp() {
     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
   }

   if [ -z "$RABBITMQCTL" ]; then
     echo "Unable to find rabbitmqctl. Please refer to the installation"
     echo "guide for instructions on configuring RabbitMQ."
     exit
   fi

   configure_amqp
   ```

   The script creates the RabbitMQ configuration Resource Manager requires.

4. Change permissions, and then run the script.

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

A.5. Start Resource Manager

1. Log in to the Resource Manager master host as `zenoss`.

2. Start Resource Manager.

   ```
   zenoss start
   ```

3. Start remote hubs, if any.

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

4. Start remote collectors, if any.

   ```
   ssh zenoss@remote-collector
   zenoss start
   ```

Appendix B. Port requirements

This appendix details the network ports and protocols that Resource Manager needs to function properly. The exact requirements for a specific installation depend on how its components are distributed and/or replicated from the master host, and what classes of devices are being monitored. In most cases, the port numbers used by Resource Manager daemons are set by their configuration file(s) in **`$ZENHOME/etc`**. Some monitoring templates use a configuration property to specify the target port on monitored devices.

In the default, single-server installation, all communication among components is through the loopback network (lo) and local (“unix”) sockets.

This appendix describes the ports used by a standard Resource Management installation with the Windows Monitoring ZenPack installed. For ZenPacks not included in the standard installation, consult the *Resource Management Extended Monitoring* guide, or the individual ZenPack’s documentation.

Browser Connections to the Zenoss Web Server

By default, the Resource Manager web server load balancer (nginx) listens on TCP port 8080, but can be configured to accept requests on the default HTTP port (80), the HTTPS port (443), or an arbitrary port.

Zenoss Administrator’s / Operator’s Browser to Zenoss UI					
Description	**Port**	**Proto**	**Direction**	**Source / Destination**	**Notes**
Web UI	8080*	TCP	OUT	nginx	*Port number is configurable.
Google Maps portlet (Dashboard)	80 (HTTP)	TCP	OUT	callhome.zenoss.com, *Various Google sites*	This portlet can be removed.
Default site portlet (Dashboard)	80 (HTPP)	TCP	OUT	www2.zenoss.com	This portlet can be removed or reconfigured to access another website.

Port Requirements for Prerequisite Software

Resource Manager depends on various third-party software packages, some of which include daemons that must be accessible either locally, over the network, or both. By default, all Resource Manager software and its dependencies are installed initially on the Resource Manager master host. For increased performance, some of the third-party daemons can be run on a separate, dedicated (physical or virtual) server, noted as “off-host” in the table below.

Port Requirements for Prerequisite Software

Daemon	Port	Proto	Dir	Source / Destination	Notes
(*bind*)	53 (DNS)	UDP	OUT	*DNS Server(s)*	Very strongly recommended.
ntpd	123 (NTP)	UDP	IN/OUT	*Zenoss servers, network time servers*	Strongly recommended for Zenoss instances with more than one server. Should be run on all Zenoss hosts.
memcached	11211 (memcache)	TCP	IN	zenactiond, zeneventserver, zenhub, zenjobs, zope	Required on the master server and every remote hub.
rabbitmq	5672 (AMQP)	TCP	IN	zenactiond, zencatalogservice, zeneventd, zeneventserver, zenhub, zenjobs, zope	One RabbitMQ instance (or cluster) is required for each Zenoss instance. Can be run off-host.
sshd	22 (SSH)	TCP	IN	*ssh client, Zenoss master server*	Inbound access is required on all Zenoss servers.
(*various*)	22 (SSH)	TCP	OUT	*Zenoss master server*	Outbound SSH access is required on the master host.
zends (mysql)	`/var/lib/zends/zends.sock` 13306	unix TCP	— IN	zenactiond, zencatalogservice, zeneventd, zeneventserver, zenhub, zenjobs, zope	One instance is required. The object database and event database can be located on separated instances. Local connections use the unix socket. Remote connections conventionally go to TCP port 13306. Can be run off-host.

Event Server Daemons

The daemons listed below are required. They are normally run on the master host. As noted below, some of them can be moved to a different dedicated (physical or virtual) host ("off-host"), and others may be run ("replicated") on additional hosts but still require an instance running on the master host.

Note that by default, the master host also runs the Hub and Collector daemons detailed in subsequent sections.

Event Server Daemons

Daemon	Port	Proto	Dir	Source / Destination	Notes
nginx	8080 (HTTP) 8090 (HTTP) 8091 (HTTP) 9081[1] (HTTP)	TCP TCP TCP TCP	IN OUT OUT OUT	(*browser*) zenhub zenrender zope	Can be replicated (with zope) on additional servers to off-load report generation.
zenactiond	25 (SMTP) 5672 (AMQP) 11211 (memcache) 13306[2]	TCP TCP TCP TCP	OUT OUT OUT OUT	(SMTP daemon) rabbitmq memcached zends	
zencatalogservice	8085 13306[2]	TCP TCP	IN OUT	zope, zenjobs, zenhub zends	
zeneventd	5672 (AMQP) 11211 (memcache) 13306	TCP TCP TCP	OUT OUT OUT	rabbitmq memcached zends	Can be moved or replicated off-host.
zeneventserver	8084 5672 (AMQP) 13306[2]	TCP TCP TCP	IN OUT OUT	zope, zenhub rabbitmq zends	Can be moved off-host.
zenjobs	5672 (AMQP) 8085 13306[2]	TCP TCP TCP	OUT OUT OUT	rabbitmq zencatalogservice zends	
zenjserver	8700	TCP	IN	zope	
zentune	5672 (AMQP) 8084 11211 (memcache) 13306[2]	TCP TCP TCP TCP	OUT OUT OUT OUT	rabbitmq zeneventserver memcached zends	
zope (runzope)	9081[1] 25 (SMTP) 5672 (AMQP) 8084 8700 11211 (memcache) 13306[2]	TCP TCP TCP TCP TCP TCP TCP	IN OUT OUT OUT OUT OUT OUT	nginx (*SMTP daemon*) rabbitmq zeneventserver zenjserver memcached zends	Can be replicated (with nginx) on additional hosts to off-load report generation.

1. For performance, Resource Manager normally runs multiple instances of the Zope daemon (two, by default). Each instance is automatically configured with a unique incoming HTTP port. By default, the initial instance listens on port 9081 and each additional instance uses the port number equal to that of the previous instance plus one (9082, 9083, etc.). See the *zenwebserver* chapter of the *Resource Management Extended Monitoring* guide for information on how to manage the number of concurrent Zope servers.
2. Local connections to ZenDS are through the `/var/lib/zends/zends.sock` unix socket.

Hub Daemons

The zenhub daemon must run on every hub host.

Hub Daemons

Daemon	Port	Proto	Dir	Source / Destination	Notes
zenhub	8081[1]	TCP	IN	*collector daemons*	XML-RPC
	8090	TCP	IN	nginx	Graph rendering
	8789[1]	TCP	IN	*collector daemons*	“ZenHub”
	5672 (AMQP)	TCP	OUT	rabbitmq	
	8084	TCP	OUT	zeneventserver	
	8085	TCP	OUT	zencatalogservice	
	11211 (memcache)	TCP	OUT	memcached	
	13306	TCP	OUT	zends	
zentune	5672 (AMQP)	TCP	OUT	rabbitmq	
	8084	TCP	OUT	zeneventserver	
	11211 (memcache)	TCP	OUT	memcached	
	13306	TCP	OUT	zends	

1. The “ZenHub” and XML-RPC port numbers are specified when the hub is created. They default to the lowest port numbers greater than 8789 and 8081, respectively, which are not being used by an existing hub.

Collector Daemons

Note that all collector daemons must be able to connect to their hub’s “ZenHub” and XML-RPC ports, which usually vary from hub to hub. Most collector daemons do not need to be run if they are not required for monitoring the devices assigned to the collector.

Daemons marked with a dagger (†) must be run on every collector host.

Collector Daemons

Daemon	Port	Proto	Dir	Source / Destination	Notes
zencommand	22 (SSH) *	TCP	OUT	*monitored devices*	*See note 1.
zeneventlog	135 (EPMAP)	TCP	OUT	*monitored devices*	*See notes 2 and 3.
	*	TCP	IN/OUT	*monitored devices*	
zenjmx	*	TCP	OUT	monitored devices	*See note 4.
zenmailtx	25 (SMTP)	TCP	OUT	*outgoing SMTP server*	
	110 (POP3)	TCP	OUT	*monitored POP3 service*	
zenmodeler†	*	*	OUT	*monitored devices*	*The port(s) and protocol(s) used for device modeling are determined by which modeler plugins have been enabled for the device(s) being modeled.
zenperfsnmp	161 (SNMP)	UDP	—	*monitored devices*	

Collector Daemons

Daemon	Port	Proto	Dir	Source / Destination	Notes
zenping	echo request echo-reply	ICMP ICMP	OUT IN	*monitored devices* *monitored devices*	Devices with a non-empty IP address will periodically be probed by the zenping daemon by default. Set the **zPingMonitorIgnore** configuration property to **true** (checked) to prevent this behavior.
zenprocess	161 (SNMP)	UDP	—	*monitored devices*	
zenrender†	8091	TCP	IN	nginx	
zenrrdcached†	**$ZENHOME/var/rrdcached.sock**	unix	—		
zenstatus	*	TCP	OUT	*monitored devices*	*zenstatus attempts to open a TCP connection to the port defined for each monitored IP Service on each device where the service is monitored.
zensyslog	514 (Syslog)	UDP	IN	*monitored devices*	
zentune	13306	TCP	OUT	*zends*	
zentrap	162 (SNMPTrap)	UDP	IN	*monitored devices*	
zenucsevents	80 (HTTP)	TCP	OUT	*monitored devices*	
zenvcloud	443 (HTTPS)	TCP	OUT	*monitored devices*	
zenvmwareevents	443 (HTTPS) or 80 (HTTP)	TCP	OUT	*monitored devices*	
zenvmwaremodeler	443 (HTTPS) or 80 (HTTP)	TCP	OUT	*monitored devices*	
zenvmwareperf	443 (HTTPS) or 80 (HTTP)	TCP	OUT	*monitored devices*	
zenwebtx	80 (HTTP)	TCP	OUT	*monitored devices*	
zenwin	135 (EPMAP) *	TCP TCP	OUT IN/OUT	*monitored devices* *monitored devices*	*See note 2.
zenwinperf	445 (MS-DS)	TCP	OUT	*monitored devices*	
zredis	16379	TCP	IN	*Zenoss master server and collector servers*	Required on the master host and every remote collector.

1. **zencommand**: In addition to running commands on monitored devices, the zencommand daemon is also used to run commands (for example, Nagios plugins) on the collector. Those commands often then connect to the monitored device. See the **Additional Monitoring Port Usage** section below for more information.
2. **zeneventlog**, **zenwin**: These daemons use Windows RPC to communicate with the WMI service on the remote device. By default, Windows RPC allocates a dynamic port, in addition to port 135, in the range of 49152–65535 or 1025–5000 depending on the version of Windows. See the *Service overview and network port requirements for Windows* Microsoft support article for more information.
3. **zeneventlog**: This daemon will attempt to monitor the Windows event logs of any devices where the **zWmiMonitorIgnore** configuration property is set to **False** (unchecked) and the **zWinEventlog** configuration property is set to **True** (checked), which is the default configuration on the **/Server/Windows** device class.
4. **zenjmx**: The zenjmx daemon provides monitoring of remote Java® applications using Java Monitoring Extensions (JMX) using either RMI (Remote Method Invocation) or JMXMP (JMX Messaging Protocol). Device class specific configuration properties are used to define the remote port and authentication credentials.

   Note that the RMI protocol requires a second connection that, by default, goes to a dynamically allocated (essentially random) port number. See the *Java 2 Platform Standard Edition* chapter in the *Resource Manager Extended Monitoring* guide for more information.

Resource Manager Collectors by Device Class

This table details the collector daemons invoked by default on devices in each device class. The listed port numbers are for outgoing connections from the collector to the monitored device. See the **Collector Daemons** section above for additional information about a specific daemon.

Device classes marked with a dagger (**†**) are used primarily as containers for sub-classes (or other special purposes). Zenoss recommends that you do not add devices to these classes, but to an appropriate subclass instead.

Collector to Monitored Devices by Device Class

Device Class	Port	Proto	Daemon / Notes
/**Devices**†	161 (SNMP)	UDP	zenperfsnmp
/Devices/**AWS**†	161 (SNMP)	UDP	zenperfsnmp
/Devices/AWS/**EC2**	443 (HTTPS) or 80 (HTTP)	TCP	zencommand
/Devices/**CiscoUCS**	80 (HTTP)*	TCP	zenucsevents *The destination port number is specified when the device is added and is maintained in the **zCiscoUCSManagerPort** configuration property.
/Devices/**Discovered**†	161 (SNMP)	UDP	zenperfsnmp Devices are normally added to this class by the auto-discovery process. Modeling uses the SNMP, SSH, and WMI protocols.
/Devices/**HTTP**	80 (HTTP)*	TCP	zencommand Invokes the **`check_http`** Nagios plugin *The port number can be changed in the HttpMonitor data source of the HttpMonitor monitoring template.
/Devices/**KVM**	161 (SNMP)	UDP	zenperfsnmp
/Devices/**Network**†	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/**BIG-IP**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/**Check Point**	161 (SNMP) 22 (SSH)	UDP TCP	zenperfsnmp zencommand
/Devices/Network/Check Point/**SPLAT**	161 (SNMP) 22 (SSH)	UDP TCP	zenperfsnmp zencommand
/Devices/Network/**Cisco**†	161 (SNMP)	UDP	zenperfsnmp Some Cisco devices can be configured to send SNMP traps and syslog messages to their Zenoss collector. See **zensyslog** and **zentrap** in the previous section.
/Devices/Network/Cisco/**6500**	161 (SNMP) 22 (SSH)	UDP TCP	zenperfsnmp zencommand
/Devices/Network/Cisco/6500/**VSS**	161 (SNMP) 22 (SSH)	UDP TCP	zenperfsnmp zencommand
/Devices/Network/Cisco/**ACE**	161 (SNMP) 80 (HTTP)	UDP TCP	zenperfsnmp zencommand
/Devices/Network/Cisco/**ASA**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Cisco/**ASR**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Cisco/ASR/**1000**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Cisco/ASR/**9000**	161 (SNMP) 23 (TELNET)	UDP TCP	zenperfsnmp zencommand
/Devices/Network/Cisco/**CatOS**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Cisco/**Codec**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Cisco/**FWSM**	161 (SNMP)	UDP	zenperfsnmp

Collector to Monitored Devices by Device Class

Device Class	Port	Proto	Daemon / Notes
/Devices/Network/Cisco/**IDS**	443 (HTTPS)	TCP	zencommand
/Devices/Network/Cisco/**MDS**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Cisco/MDS/**9000**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Cisco/**Nexus**	161 (SNMP) 22 (SSH)	UDP TCP	zenperfsnmp zenmodeler (NETCONF over SSH)
/Devices/Network/Cisco/Nexus/**1000V**	161 (SNMP) 22 (SSH)	UDP TCP	zenperfsnmp zenmodeler (NETCONF over SSH)
/Devices/Network/Cisco/Nexus/**5000**	161 (SNMP) 22 (SSH)	UDP TCP	zenperfsnmp zenmodeler (NETCONF over SSH)
/Devices/Network/Cisco/Nexus/**7000**	161 (SNMP) 22 (SSH)	UDP TCP	zenperfsnmp zenmodeler (NETCONF over SSH)
/Devices/Network/Cisco/**VSG**	161 (SNMP) 22 (SSH)	UDP TCP	zenperfsnmp zenmodeler (NETCONF over SSH)
/Devices/Network/Cisco/**WLC**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/**Juniper**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Juniper/**M10i**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/**NetScreen**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/**Router**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Router/**Cisco**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Router/**Firewall**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Router/**RSM**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Router/**TerminalServer**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/**Switch**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Switch/**Nortel**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Network/Switch/**Passport**	161 (SNMP)	UDP	zenperfsnmp
/Devices/**Ping**	Echo request Echo reply	ICMP	zenping Devices in this class will only be monitored for up / down status. See **zenping** in the previous section.
/Devices/**Power**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Power/**UPS**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Power/UPS/**APC**	161 (SNMP)	UDP	zenperfsnmp
/Devices/**Printer**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Printer/**InkJet**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Printer/**Laser**	161 (SNMP)	UDP	zenperfsnmp
/Devices/**Server**†	161 (SNMP)	UDP	zenperfsnmp
/Devices/Server/**Cmd**	22 (SSH)	TCP	zencommand This device class is deprecated; use one of the sub-classes of **/Devices/Server/SSH/** instead.
/Devices/Server/**Darwin**	161 (SNMP)	UDP	zenperfsnmp, zenprocess
/Devices/Server/**JBoss**	161 (SNMP) * 9999 (REMOTING-JMX)	UDP TCP TCP	zenperfsnmp, zenprocess zenjmx *The port number used for JMX monitoring is set by the **zJBossJmxManagementPort** configuration property. See **zenjmx** in the previous section.
/Devices/Server/**Linux**	161 (SNMP)	UDP	zenperfsnmp, zenprocess
/Devices/Server/**Remote**	161 (SNMP)	UDP	zenperfsnmp, zenprocess
/Devices/Server/**Scan**	*	TCP	zenstatus
/Devices/Server/**Solaris**	161 (SNMP)	UDP	zenperfsnmp, zenprocess

Collector to Monitored Devices by Device Class

Device Class	Port	Proto	Daemon / Notes
/Devices/Server/**SSH**†	—	—	
/Devices/Server/SSH/**AIX**	22 (SSH)	TCP	zencommand
/Devices/Server/SSH/**HP-UX**	22 (SSH)	TCP	zencommand
/Devices/Server/SSH/**Linux**	22 (SSH)	TCP	zencommand
/Devices/Server/SSH/**Solaris**	22 (SSH) 161 (SNMP)	TCP TCP	zencommand zenperfsnmp
/Devices/Server/**Tomcat**	161 (SNMP) *	UDP TCP	zenperfsnmp, zenprocess zenjmx *The port number used for JMX monitoring is set by the **zTomcatJmxManagementPort** configuration property. See zenjmx in the previous section.
/Devices/Server/Virtual Machine **Host**†	161 (SNMP)	UDP	zenperfsnmp, zenprocess
/Devices/Server/Virtual Machine Host/**ESX**	161 (SNMP)	UDP	zenperfsnmp, zenprocess
/Devices/Server/Virtual Machine Host/**EsxTop**	161 (SNMP) 443 (HTTPS)	UDP TCP	zenperfsnmp zencommand Invokes the **`resxtop`** command on the collector. resxtop is part of the VMware vSphere CLI. resxtop connects to the monitored device using HTTPS.
/Devices/Server/Virtual Machine Host/**Xen**	161 (SNMP) 22 (SSH)	UDP TCP	zenperfsnmp zencommand
/Devices/Server/**WebLogic**	161 (SNMP) *	UDP TCP	zenperfsnmp, zenprocess zenjmx *The port number used for WebLogic monitoring is set by the **zWebLogicJmxManagementPort** configuration property. See **zenjmx** in the previous section.
/Devices/Server/**Windows**	161 (SNMP) 135 (EPMAP), *	UDP TCP	zenperfsnmp zeneventlog
/Devices/Server/Windows/**WMI**	135 (EPMAP), * 445 (MS-DS)	TCP TCP	zeneventlog, zenwin zenwinperf
/Devices/Server/Windows/WMI/**Active Directory**	135 (EPMAP), * 445 (MS-DS)	TCP TCP	zeneventlog, zenwin zenwinperf
/Devices/Server/Windows/WMI/**MSExchange**	135 (EPMAP), * 445 (MS-DS)	TCP TCP	zeneventlog, zenwin zenwinperf
/Devices/Server/Windows/WMI/**MSSQLServer**	135 (EPMAP), * 445 (MS-DS)	TCP TCP	zeneventlog, zenwin zenwinperf
/Devices/**Storage**†	161 (SNMP)	UDP	zenperfsnmp
/Devices/Storage/**Brocade**	161 (SNMP)	UDP	zenperfsnmp
/Devices/Storage/**NetApp**	161 (SNMP) 22 (SSH)	UDP TCP	zenperfsnmp zencommand
/Devices/**vCloud**	443 (HTTPS)	TCP	zenvcloud
/Devices/**VMware**	443 (HTTPS) or 80 (HTTP)	TCP	zenvmwaremodeler, zenvmwareevents, zenvmwareperf
/Devices/**Web**†	161 (SNMP)	UDP	zenperfsnmp
/Devices/Web/**SugarCRM**	80 (HTTP)	TCP	zenwebtx

Additional Monitoring Port Usage

Additional monitoring functionality can be added to a device or device class by binding the appropriate monitoring template or adding a data source to an already bound template. This table shows the port numbers used when specific monitoring capabilities are applied. See the *Resource Manager Extended Monitoring* guide for more information.

Additional Monitoring Port Usage

Description	Port	Proto	Direction	Collector Daemon	Notes
Apache HTTP Server™ Monitoring	80 (HTTP)	TCP	OUT	zencommand	Provided by the **Apache** monitoring template.
DNS Monitoring	53 (Domain)	UDP	OUT	zencommand	Provided by the **DigMonitor** and **DnsMonitor** monitoring templates. Invokes the **`check_dig`** or **`check_dns`** Nagios plugin respectively.
FTP Service Monitoring	21 (FTP)	TCP	OUT	zencommand	Provided by the **FtpMonitor** monitoring template. Invokes the **`check_ftp`** Nagios plugin.
IRC Service Monitoring	6667 (IRCD)	TCP	OUT	zencommand	Provided by the **IRCD** monitoring template. Invokes the **`check_ircd`** Nagios plugin.
Jabber® Service Monitoring	5223	TCP	OUT	zencommand	Provided by the **JabberMonitor** monitoring template. Invokes the **`check_jabber`** Nagios plugin.
LDAP Response Time Monitoring	389 (LDAP)	TCP	OUT	zencommand	Provided by the **LDAPServer** monitoring template. Invokes the **`check_ldap`** or **`check_ldaps`** Nagios plugin.
Microsoft Message Queuing (MSMQ) Monitoring	445 (MS-DS)	TCP	OUT	zenwinperf	Provided by the **MSMQQueue** monitoring template.
Microsoft Internet Information Services (IIS) Monitoring	445 (MS-DS)	TCP	OUT	zenwinperf	Provided by the **IIS** monitoring template.
MySQL® Monitoring	3306	TCP	OUT	zencommand	Provided by the **MySQL** monitoring template.
Network News Transport Protocol (NNTP) Monitoring	119 (NNTP) or 563 (NNTPS)	TCP	OUT	zencommand	Provided by the **NNTPMonitor** monitoring template. Invokes the **`check_nntp`** or **`check_nntps`** Nagios plugin.
Network Time Protocol (NTP) Monitoring	123 (NTP)	UDP	OUT	zencommand	Provided by the **NTPMonitor** monitoring template. Invokes the **`check_ntp`** Nagios plugin.
SQL Transactions	*	TCP	OUT	zencommand	Provided by the **SQL** data source type. *The destination port number depends on the SQL server and is specified in the data source properties.
WebSphere® Application Server	80 (HTTP)*	TCP	OUT	zenwebtx	Provided by the **Websphere** monitoring template. *A custom port number can be set in the **Initial URL** data source property.