



Zenoss Core Installation and Upgrade

Release 4.2.5

Zenoss, Inc.

www.zenoss.com

Zenoss Core Installation and Upgrade

Copyright © 2014 Zenoss, Inc., 11305 Four Points Drive, Bldg 1 - Suite 300, Austin, Texas 78726, U.S.A. All rights reserved.

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

Flash is a registered trademark of Adobe Systems Incorporated.

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

Linux is a registered trademark of Linus Torvalds.

RabbitMQ is a trademark of VMware, Inc.

Red Hat and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc., in the U.S. and other countries.

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

Sybase is a registered trademark of Sybase, Inc.

Tomcat is a trademark of the Apache Software Foundation.

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

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

Part Number: 01-042014-4.2-v19

1. Installation Considerations	1
1.1. Which Installation Should You Choose?	1
1.2. Hardware Requirements	1
1.2.1. Deployments Up to 1000 Devices	1
1.2.2. Deployments Over 1000 Devices	1
1.2.3. Other Considerations	1
1.3. File System Configuration	1
1.4. Client and browser support	2
1.5. Post-Installation Performance Tuning Tasks	2
2. Installing on RHEL or CentOS	3
2.1. Requirements	3
2.2. Tasks	3
2.3. Configure Your Firewall	3
2.4. Remove Outdated Packages	4
2.5. Remove Conflicting Messaging Systems	4
2.6. Install Oracle Java	4
2.7. Disable SELinux	5
2.8. Install the Zenoss Dependencies Repository	5
2.9. Install and Configure MySQL Community Server	5
2.10. Install Zenoss Core	6
2.10.1. Download the Installation File	6
2.10.2. Install the RPM	6
2.10.3. Installing and initializing ZenUp	7
2.10.4. Start Zenoss Core and install the RPS	7
2.11. Getting Started	8
2.11.1. Set the Administrative Password and Create a User	9
2.11.2. Add Devices	10
2.11.2.1. Adding Devices Manually	10
2.11.2.2. Discovering Devices	10
3. Installing the Virtual Appliance	13
3.1. System Requirements	13
3.2. Prerequisite Tasks	13
3.3. Installing the Appliance	13
4. Performance Tuning	14
4.1. Packing the ZODB	14
4.2. Editing Archived Event Data Storage Settings	14
4.3. Memory Caching	14
4.4. Tuning MySQL	15
4.5. Increasing Maximum File Descriptors	15
5. Upgrading	16
5.1. Preparing to upgrade	16
5.2. Upgrading MySQL Server	17
5.3. Upgrading Zenoss Core	18
6. Removing an Instance	19
6.1. Before You Begin	19
6.2. Removing Zenoss Core	19

Chapter 1. Installation Considerations

Read the following sections to learn more about installation requirements for Zenoss Core.

1.1. Which Installation Should You Choose?

Zenoss Core provides these categories of artifacts for a fresh deployment:

Table 1.1. Installation Types

Artifact	Notes	Chapters
RPM (*.rpm)	Standard RPM installation. Requires a Red Hat® Enterprise Linux® (RHEL) or Community ENTerprise Operating System (CentOS)-based Linux installation, and MySQL.	"Installing on RHEL or CentOS"
Appliance	RPM installation on top of a minimal CentOS Linux installation.	"Installing the Virtual Appliance"

1.2. Hardware Requirements

You should meet these minimum hardware requirements for a single-server installation of Zenoss Core.

1.2.1. Deployments Up to 1000 Devices

Table 1.2. Hardware Requirements: Up to 1000 Devices

Deployment Size	Memory	CPU	Storage
1 to 250 devices	4GB	2 cores	1x300GB, 10K RPM drive or SSD
250 to 500 devices	8GB	4 cores	1x300GB, 10K RPM drive or SSD
500 to 1000 devices	16GB	8 cores	1x300GB, 15K RPM drive or SSD

1.2.2. Deployments Over 1000 Devices

Zenoss solutions are successfully deployed at multiple sites with tens of thousands of devices. If you are planning to monitor more than 1000 devices, or will monitor a network with complex topology, there are additional requirements and configurations to consider.

1.2.3. Other Considerations

Zenoss Core is a highly IO-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 Zenoss Core installation.

Note

Zenoss recommends that you use a hardware-based RAID 1 (mirroring) drive subsystem to protect against data loss.

1.3. File System Configuration

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

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

For more information about file system performance tuning and increasing RRD performance, browse to:

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

1.4. Client and browser support

Zenoss Core 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.

Table 1.3. Client and Browser Support

Client OS	Supported Browsers
Windows 7	<ul style="list-style-type: none"> • Internet Explorer 8 and 9 • Firefox ESR 24 and 27.0 • Chrome 32
Windows 8.1	<ul style="list-style-type: none"> • Firefox ESR 24 and 27.0 • Chrome 32
Windows Server 2012	<ul style="list-style-type: none"> • Firefox ESR 24 and 27.0 • Chrome 32
Windows Server 2012 R2	<ul style="list-style-type: none"> • Firefox ESR 24 and 27.0 • Chrome 32
OS X Mountain Lion (10.8)	<ul style="list-style-type: none"> • Firefox ESR 24 and 27.0 • Chrome 32
OS X Mavericks (10.9)	<ul style="list-style-type: none"> • Firefox ESR 24 and 27.0 • Chrome 32
Ubuntu 12.04 LTS	<ul style="list-style-type: none"> • Firefox ESR 24 and 27.0 • Chrome 32
Ubuntu 13.10	<ul style="list-style-type: none"> • Firefox ESR 24 and 27.0 • Chrome 32

1.5. Post-Installation Performance Tuning Tasks

After your installation is complete, there are several configuration settings you should adjust to obtain proper performance. Based upon the size of your planned deployment, changes to the MySQL 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 on RHEL or CentOS

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

Before installing Zenoss Core, you must:

- Ensure your system meets all requirements.
- Install prerequisite software and packages, as outlined in this chapter.

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

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

2.1. Requirements

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

In addition, make sure that:

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

2.2. Tasks

Before installing Zenoss Core, you must:

- Configure your firewall
- Remove outdated packages
- Remove conflicting messaging systems
- Install and configure software repositories, prerequisite software, and additional packages

2.3. Configure Your Firewall

Zenoss Core requires these ports be open in your firewall:

Port	Protocol	Direction to Zenoss Core Server	Description
11211	TCP UDP	Inbound	memcached

Port	Protocol	Direction to Zenoss Core Server	Description
8080	TCP	Outbound	Web interface
514	UDP	Inbound	syslog
162	UDP	Inbound	SNMP Traps
25	TCP	Inbound	zenmail

Alternatively, you can choose to disable your firewall.

For IPv4, use these commands:

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

For IPv6, use these commands:

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

2.4. Remove Outdated Packages

Zenoss Core requires at least MySQL 5.5.25, and supports later versions through 5.5.35. If you have older versions of MySQL installed, you must first remove those installations. Current data will be lost.

1. Stop the MySQL service:

```
service mysqld stop
```

2. List the MySQL packages currently installed:

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

3. Remove all listed packages:

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

4. If your version of MySQL is earlier than 5.5.25, delete the MySQL directory:

```
rm -rf /var/lib/mysql
```

If your version of MySQL is 5.5.25 or a more recent version, DO NOT delete the MySQL directory.

2.5. Remove Conflicting Messaging Systems

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

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

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

2. Remove all listed packages:

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

2.6. Install Oracle Java

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

1. Determine whether other Java packages 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)')
```

2. Download the self-installing binary of Oracle Java SE Runtime Environment 6u45 from the [Java SE 6 Downloads](#) page. The file to download is `jre-6u45-linux-x64-rpm.bin`.

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

```
chmod +x ./jre-6u45-linux-x64-rpm.bin
```

4. Install the Oracle JRE.

```
./jre-6u45-linux-x64-rpm.bin
```

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

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

6. Verify the correct version is installed.

```
java -version
```

The preceding command should return the following output.

```
java version "1.6.0_45"  
Java(TM) SE Runtime Environment (build 1.6.0_45-b06)  
Java HotSpot(TM) 64-Bit Server VM (build 20.45-b01, mixed mode)
```

2.7. Disable SE Linux

Zenoss Core is not compatible with Security-Enhanced Linux (SELinux) in enforcing mode. Follow these steps to disable enforcing mode on the Zenoss Core host.

1. Log in as `root`, or as a user with superuser privileges.
2. Disable enforcing mode temporarily (avoiding the need to reboot) with the following command:

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

3. 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
```

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

2.8. Install the Zenoss Dependencies Repository

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
```

2.9. Install and Configure MySQL Community Server

You can install MySQL Community Server and Zenoss Core on the same host or you can install them on separate hosts.

Follow these steps to download, install, and configure MySQL Community Server:

1. Download the following Red Hat/Oracle Enterprise Linux (x86, 64-bit) RPM Packages from mysql.com/:

- Client Utilities
- MySQL Server
- Shared components

2. Install the packages with the command:

```
yum -y --nogpgcheck localinstall MySQL*
```

Important! When MySQL installation completes, it displays a message similar to "PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !" followed by directions to perform this task.

Do not set the MySQL root user password at this point in the installation process. You must install Zenoss Core before performing this task.

3. Create a file named `/etc/my.cnf` file, and then add the following lines:

```
[mysqld]
max_allowed_packet=16M
innodb_buffer_pool_size=256M
innodb_additional_mem_pool_size=20M
```

4. Run these commands to start the `mysql` daemon and to configure it to start automatically on reboot:

```
service mysql start
chkconfig --add mysql
chkconfig --level 2345 mysql on
```

5. Configure MySQL for Zenoss Core installation. Do not add a space between the single quotes in the following commands:

```
mysqladmin -u root password ''
mysqladmin -u root -h localhost password ''
```

2.10. Install Zenoss Core

Follow these steps to install Zenoss Core. Run all commands as root.

2.10.1. Download the Installation File

Download the Zenoss Core installation file from this location:

<http://community.zenoss.org/community/download>

2.10.2. Install the RPM

1. Install the RPM file:

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

2. 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
```

2.10.3. Installing and initializing ZenUp

This release of Zenoss Core 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 Core ZenUp patch management tool, which must be installed and initialized before you start Zenoss Core.

Follow these steps to initialize ZenUp for this release of Zenoss Core. For more information about ZenUp, refer to Zenoss Core ZenUp Installation and Administration.

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

- The ZenUp RPM file.
- The "pristine" file for this release of Zenoss Core.
- The current RPS (.zup) file.

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

4. Log in as user `zenoss`.

5. Register Zenoss Core with ZenUp by specifying the "pristine" file.

```
zenup init zenoss_core-4.2.5-XXXX-elX-pristine.tgz $ZENHOME
```

The `zenup` command displays messages as it works.

6. Verify the result.

```
zenup status
```

ZenUp displays information similar to the following example.

```
Product: zenoss-core-4.2.5 (id = zenoss-core-4.2.5)
Home: /opt/zenoss
Revision: 0
Updated On: timestamp
```

2.10.4. Start Zenoss Core and install the RPS

1. Log in as `root`, and start Zenoss Core.

```
service zenoss start
```

2. Stop Zenoss Core.

```
service zenoss stop
```

3. Log in as `zenoss`, and install the latest recommended patch set (RPS).

```
zenup install zenoss_core-version.zup
```

4. Start Zenoss Core.

```
zenoss start
```

2.11. Getting Started

After installation, use your Web browser to browse to the server where Zenoss Core is installed (<http://xxx.xxx.xxx.xxx:8080>).

Note

If you cannot successfully browse to your Zenoss Core 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 interface, and you have restricted the browser to trusted sites, then a warning message may appear. To prevent this, add your Zenoss Core installation to the Trusted zone. These Microsoft articles provide more information on setting up trusted sites:

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

The setup wizard appears.

Figure 2.1. Setup Wizard



Using this wizard, you will:

- Change the admin password
- Set up an initial user
- Add some devices to the system

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:

Submit

2.11.1. Set the Administrative Password and Create a User

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

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

Note

The 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 Zenoss Core user account. Most of the time, you will use this account to perform management tasks. Enter a unique user name, password, and email address.
3. Click **Next**.

The Specify or Discover Devices to Monitor panel appears.

Figure 2.3. Setup Wizard: Step 2 (Manually Find Devices)

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

2.11.2. Add Devices

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

2.11.2.1. Adding Devices Manually

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

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

Note

For more information about setting credentials, refer to *Zenoss Core Administration*.

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

Zenoss Core models the devices in the background.

Note

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

2.11.2.2. Discovering Devices

To discover devices:

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

Figure 2.4. Setup Wizard: Step 2 (Autodiscover Devices)

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:

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

10.175.211.0/24

or as a range of IP addresses:

10.175.211.1-50

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

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

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

Note

You can bypass device discovery through the wizard. Click **Finish or Skip to Dashboard** to go directly to the Zenoss Core Dashboard. Later, you can discover devices by following the steps outlined in *Zenoss Core Administration*.

Chapter 3. Installing the Virtual Appliance

3.1. System Requirements

The system requirements for running the Virtual Appliance are largely the requirements for running the VMware Player. A typical host system used for a VMware installation should meet these specifications:

- Dual core system
- Minimum RAM - 3GB
- Available disk space - 20GB

3.2. Prerequisite Tasks

Install the VMware Player. For downloads and installation instructions, go to:

<http://www.vmware.com/products/player/>

3.3. Installing the Appliance

Follow these steps to download and install the appliance.

1. Download the Virtual Appliance file (*zenoss_core-Version-x86_64.vmware.zip*), available at this location:

<http://community.zenoss.org/community/download>

2. Unzip the file into a working directory.
3. Start the VMware Player.
4. Use the VMware Player to navigate to the directory where you unzipped the Virtual Appliance package, and then open the Virtual Appliance.

After loading the appliance, the virtual machine window displays a message similar to:

```
Welcome to Zenoss
```

```
To access the Zenoss Management Console, please browse to:
```

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

Note

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

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

The Setup Wizard appears.

Chapter 4. Performance Tuning

After installing Zenoss, you can optimize its performance by:

- Packing the ZODB
- Editing archived event data storage settings
- Setting memory caching values
- Tuning MySQL
- Increasing maximum file descriptors

Note

Performance tuning procedures assume an RPM installation. If you are using an alternate installation method, details (such as path information) likely will differ.

4.1. 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, Zenoss Core 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/zenosdbpack
```

4.2. Editing Archived Event Data Storage Settings

You can edit the default settings for archived event data to improve Zenoss Core performance. Changing these settings to values that are reasonable for your implementation will prevent the database 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 Zenoss Core 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.

4.3. 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`.

4.4. Tuning MySQL

Zenoss Core performance is directly impacted by the performance of the MySQL database that supports the event system. MySQL configuration parameters are located in the `/etc/my.cnf` file.

Zenoss recommends that you run the MySQLTuner Perl script periodically to analyze your MySQL performance. Based on the statistics it gathers, the script provides optimization recommendations.

To download the MySQLTuner script, enter this command:

```
wget http://mysqлтuner.com/mysqлтuner.pl
```

4.5. Increasing Maximum File Descriptors

A Zenoss Core 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 Zenoss Core.

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.

Chapter 5. Upgrading

This chapter provides instructions for upgrading Zenoss Core installations to version 4.2.5. You may upgrade Zenoss Core 3.2.1, 4.2.0, 4.2.3, or 4.2.4 to version 4.2.5. Version 4.2.5 requires a 64-bit platform.

Sections are presented in order, and some are optional.

Note

Version 3.2.1 upgrades only: Zenoss Core 4.2.x includes a fully redesigned event processing and storage system. Currently, upgrades do not migrate events from version 3.2.1. Instead, after the upgrade, a new, empty events database is created using the new schema.

To migrate version 3.2.1 events to version 4.2.5 as part of your upgrade, contact Zenoss Professional Services.

5.1. Preparing to upgrade

The procedure in this section prepares your installation for upgrade to version 4.2.5.

Note

Perform this procedure 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 Zenoss Core before upgrading a production environment.

1. Log in to the Zenoss Core host as user `zenoss`.
2. Stop Zenoss Core.

```
zenoss stop
```

3. Create a backup with the `zenbackup` command. For more information about `zenbackup`, refer to the *Zenoss Core Administration* guide.

Note

If you are upgrading version 3.2.1, do not include the events database in the backup. For example:

```
zenbackup --no-events
```

4. Create a backup of the Zenoss Core software. For example:

```
cd $ZENHOME  
tar --exclude backups --exclude perf --exclude log -czf $HOME/myZenoss.tgz ./*
```

5. *If you are upgrading version 4.2.3 or 4.2.4,* you must install the ZenUp patch management tool before upgrading. For more information, refer to the *Zenoss Core ZenUp Installation and Administration* guide. When you are finished installing ZenUp, resume this procedure at the next step.
6. Switch user to `root`, or to a user with superuser privileges, and 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. Upgrade Java.

- a. Download the self-installing RPM of Oracle Java SE Runtime Environment 6u45 from the [Java SE 6 Downloads](#) page. The file to download is `jre-6u45-linux-x64-rpm.bin`.
- b. Make the RPM installer executable, install the JRE, and verify the installed version.

```
chmod +x ./jre-6u45-linux-x64-rpm.bin
./jre-6u45-linux-x64-rpm.bin
java -version
```

- c. Remove the older version of Java.

```
yum -y remove jre-1.6.0_31-fcs.x86_64
```

5.2. Upgrading MySQL Server

The procedure in this section removes MySQL Server and then installs the updated release.

1. Log in as `root`, or as a user with superuser privileges.
2. Stop MySQL Server.

```
service mysql stop
```

Note

For older releases of MySQL Server, the daemon is `mysqld`, not `mysql`.

3. Determine which MySQL packages are installed.

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

Remove package(s) as necessary.

```
rpm -e --nodeps package-name
```

4. Download the following Red Hat/Oracle Enterprise Linux (x86, 64-bit) RPM Packages of MySQL Community Server, version 5.5.35, from [mysql.com](#):

- MySQL Server
- Client Utilities
- Shared components

5. Clean `yum` caches and metadata, and then install the MySQL Server packages.

```
yum clean all
yum -y --nogpgcheck localinstall MySQL*
```

6. Start MySQL Server.

```
service mysql start
```

7. Upgrade the existing databases.

```
mysql_upgrade
```

8. Set MySQL Server to start when the system starts, restart it, and set the root password for the Zenoss Core upgrade.

```
chkconfig --add mysql
chkconfig --level 2345 mysql on
service mysql restart
mysqladmin -u root password ''
mysqladmin -u root -h localhost password ''
```

9. *If you are upgrading version 3.2.1*, log in to MySQL Server and drop the events database.

```
mysql -u root
mysql> drop database events;
mysql> quit
```

5.3. Upgrading Zenoss Core

Follow these steps to upgrade the Zenoss Core package.

1. Log in as `root`, or as a user with superuser privileges.
2. Download the Zenoss Core package from community.zenoss.org
3. *If you are upgrading version 4.2.0 or 4.2.3*, follow these steps.

- a. Install the Redis datastore.

```
yum -y install redis
```

- b. Upgrade Zenoss Core with one of the following commands:

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

4. *If you are upgrading version 4.2.4*, enter one of the following commands.

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

5. *If you are upgrading version 3.2.1*, install the package:

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

6. 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
```

7. Configure Zenoss Core to start when the host starts, and start the migration process.

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

The migration process typically lasts at least 20 minutes.

8. Install the ZenUp patch management tool. For more information, refer to the *Zenoss Core ZenUp Installation and Administration* guide.
9. Install the latest recommended patch set (RPS) with the ZenUp tool.
10. Install upgraded versions of any ZenPacks you may have removed earlier.
11. Delete the browser cache on each user machine used to access Zenoss Core. (For example, if using Firefox, press Ctrl-Shift-R to clear your cache.)

Chapter 6. Removing an Instance

6.1. Before You Begin

Before removing your Zenoss Core instance, you may want to save data files. For information about saving your files, refer to the backup and archive instructions in *Zenoss Core Administration*.

Use the instructions in the following section to remove a Zenoss Core instance.

6.2. Removing Zenoss Core

Use these instructions to remove an RPM installation and all of its components from your system.

1. Enter the following command:

```
yum erase zenoss
```

2. Then enter:

```
rm -rf /opt/zenoss  
userdel zenoss
```

3. Open the command line MySQL client, as root:

```
mysql -u root
```

4. Enter the following commands at the MySQL prompt:

```
drop database events;  
drop user 'zenoss'@'localhost';
```