GETTING STARTED

Zenoss, Inc.

www.zenoss.com

Getting Started with Zenoss

Copyright © 2010 Zenoss, Inc., 275 West St. Suite 204, Annapolis, MD 21401, U.S.A. All rights reserved.

This work is licensed under a Creative Commons Attribution Share Alike 3.0 License. To view a copy of this license, visit http://creativecommons.org/licenses/by-sa/3.0/; or send a letter to Creative Commons, 171 2nd Street, Suite 300, San Francisco, California, 94105, USA.

The Zenoss logo is a registered trademark of Zenoss, Inc. Zenoss and Open Enterprise Management are trademarks of Zenoss, Inc. in the U.S. and other countries.

Flash is a registered trademark of Adobe Systems Incorporated.

Java is a registered trademark of Sun Microsystems, Inc.

Linux is a registered trademark of Linus Torvalds.

Oracle and the Oracle logo are registered trademarks of the Oracle Corporation.

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: 01-092010-3.0-v02

Chapter 1. About Zenoss

Welcome to Zenoss! This guide will help you become familiar with the interface and introduce some basic tasks.

1.1. What is Zenoss?

Zenoss is today's premier open source IT management solution. Through integrated monitoring, it enables you to manage the status and health of your infrastructure through a single, Web-based console.

The power of Zenoss starts with its in-depth Inventory and Configuration Management Database (CMDB). The system creates this database by discovering managed resources—servers, networks, and other devices—in your IT environment. The resulting environment model provides a complete inventory of your key systems, down to the level of resource components (interfaces, services, and processes, and installed software.)

With the model built, you can use the system's integrated availability and performance monitoring features to monitor and report on all aspects of your IT infrastructure. Zenoss also provides events and fault management features that tie into the CMDB. These features help drive operational efficiency and productivity by automating many of the notification, alerts, escalation, and remediation tasks you perform each day.

1.2. Quick Start

This chapter will help you quickly walk through several basic tasks that demonstrate the system's capabilities. After completing initial setup, you will learn how to:

- Add a device, and then view its status and performance details
- Set up, observe, and acknowledge an alert

The remaining guide chapters dive a little deeper into interface and system features, and show you how to:

- Configure your devices for Zenoss
- Add devices to the system through discovery, and then place them in device classes
- Monitor devices and servers
- Create and manage user accounts

1.2.1. Before You Begin

This guide assumes that you have installed the Zenoss software. If you have not, then follow the instructions in the Installation Guide (located at http://community.zenoss.org/community/documentation) to install your Zenoss instance.

To complete all the steps in this guide, you will need:

- One or more monitored targets, such as:
  - Windows Server (2000, 2003, 2008), Windows XP, Windows Vista®, Windows 7
  - Linux or other UNIX® server
  - Tomcat or other Java/JMX server
  - Any SNMP or SSH-enabled device
- For each system that will access Zenoss through a Web browser:
  - Adobe® Flash® Player
  - Firefox 3.x, or Internet Explorer 7, 8

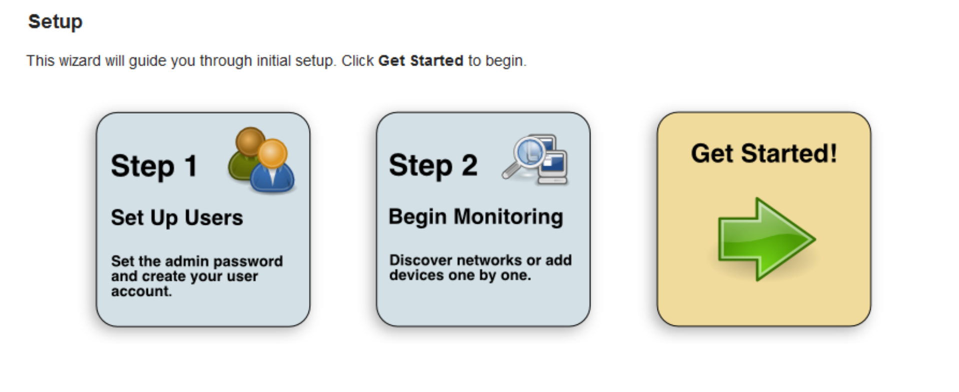
- SSH client to facilitate command line tasks

1.2.2. Perform Initial Setup

After installing, access Zenoss from your Web browser. Depending on your installation method, browse to:

- Server where Zenoss is installed, to http://xxx.xxx.xxx.xxx:8080
- URL provided in the command window (VMware installation)

The setup wizard appears.



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.

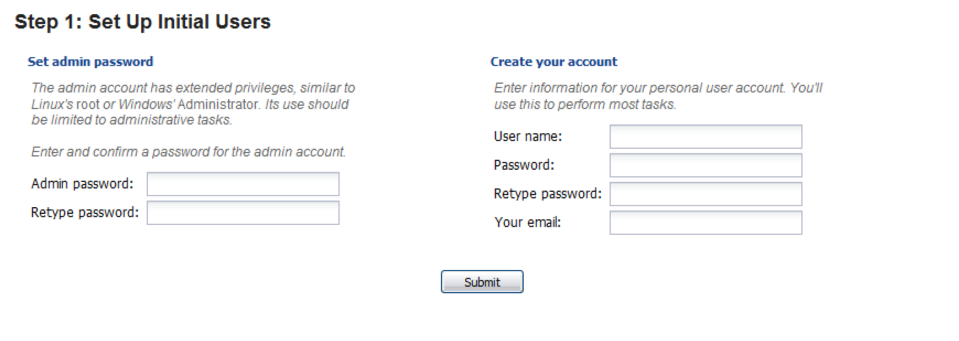
Figure 1.1. Setup Wizard

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 Step 1: Set up Initial Users panel appears.



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:

Figure 1.2. Setup Wizard: Step 1

1.2.2.1. 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.

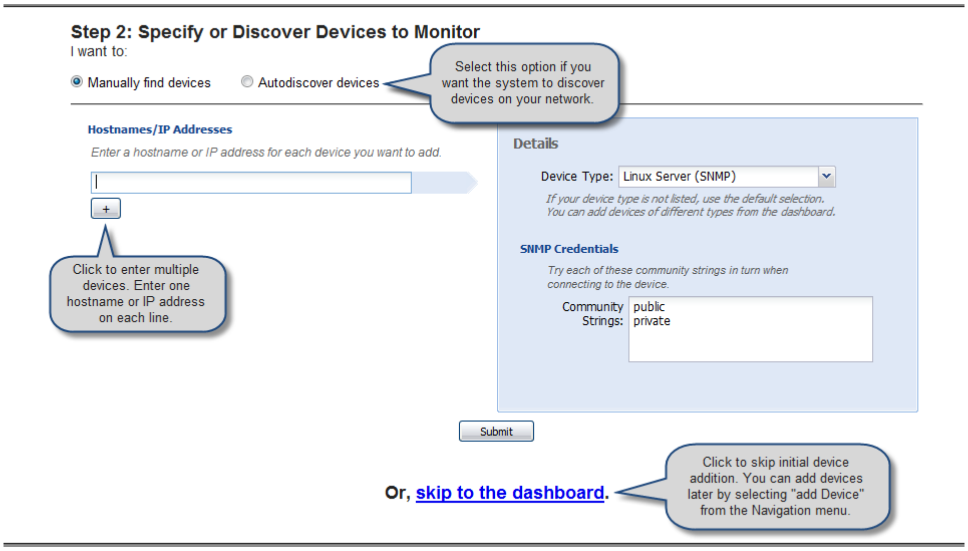
   Note

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

3. Click **Submit**.

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



Step 2: Specify or Discover Devices to Monitor

I want to:

● Manually find devices ○ Autodiscover devices

Select this option if you want the system to discover devices on your network.

Hostnames/IP Addresses

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

Click to enter multiple devices. Enter one hostname or IP address on each line.

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 dashboard.

SNMP Credentials

Try each of these community strings in turn when connecting to the device.

Community Strings: public
private

Or, skip to the dashboard.

Click to skip initial device addition. You can add devices later by selecting "add Device" from the Navigation menu.

Figure 1.3. Setup Wizard: Step 2 (Manual Add)

1.2.2.2. Add Devices

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

1.2.2.2.1. 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 Administration*.

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

   Zenoss models the devices in the background.

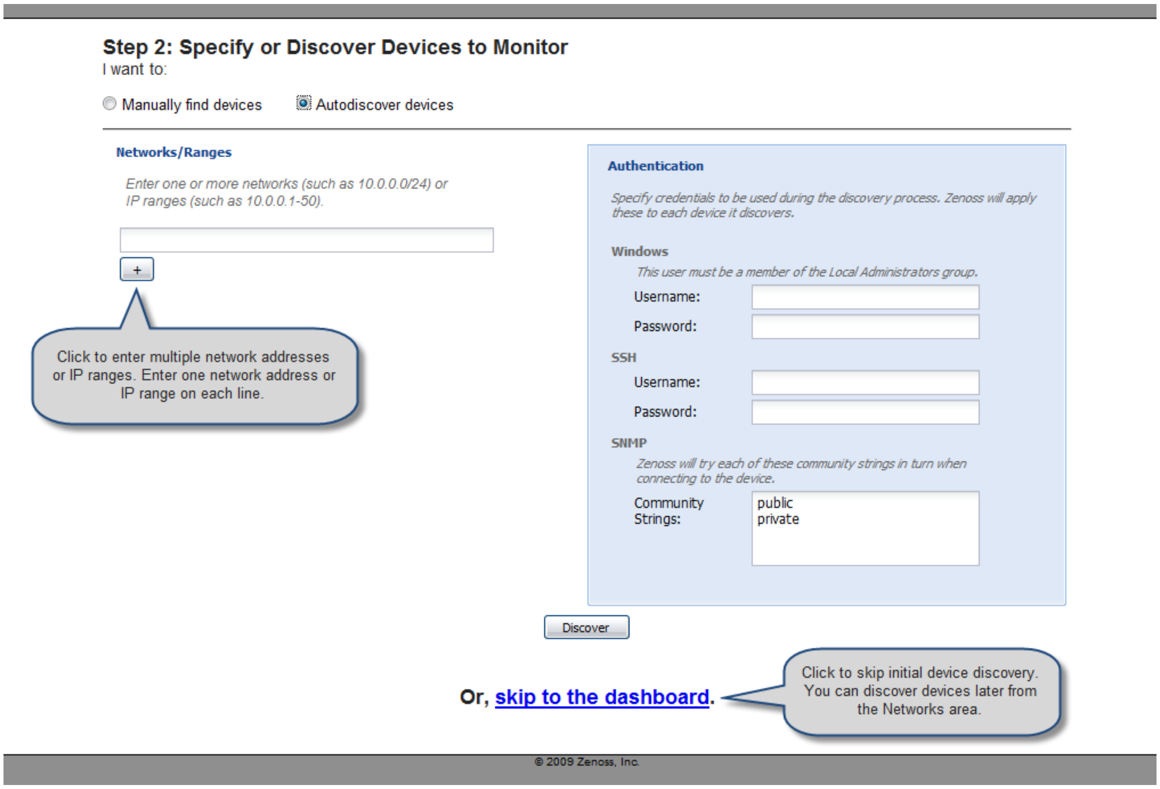
Note

You can bypass device addition through the wizard. Click **Skip to the dashboard** to go directly to the Zenoss Dashboard. Later, you can add devices by following the steps outlined in the section titled "Add and View a Device."

1.2.2.2.2. Discovering Devices

To discover devices:

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



Step 2: Specify or Discover Devices to Monitor

I want to:

○ 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).

Click to enter multiple network addresses or IP ranges. Enter one network address or IP range on each line.

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

Or, skip to the dashboard.

Click to skip initial device discovery. You can discover devices later from the Networks area.

Figure 1.4. Setup Wizard: Step 2 (Discovery)

2. For each network or IP range in which you want Zenoss 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 to use on the devices it discovers. You can enter only one of each. Zenoss attempts to use the same credentials on each device it discovers within the networks or IP ranges specified.
5. Click **Discover**.

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

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

Note

You can bypass device discovery through the wizard. Click **Skip to the dashboard** to go directly to the Zenoss Dashboard. Later, you can discover devices by following the steps outlined in the section titled “Device Auto-Discovery.”

1.2.3. Add and View a Device

If you skipped initial device addition through the Setup Wizard, or want to add more devices through Zenoss’ more advanced device addition page, then follow these steps.

1.2.3.1. Add the Device

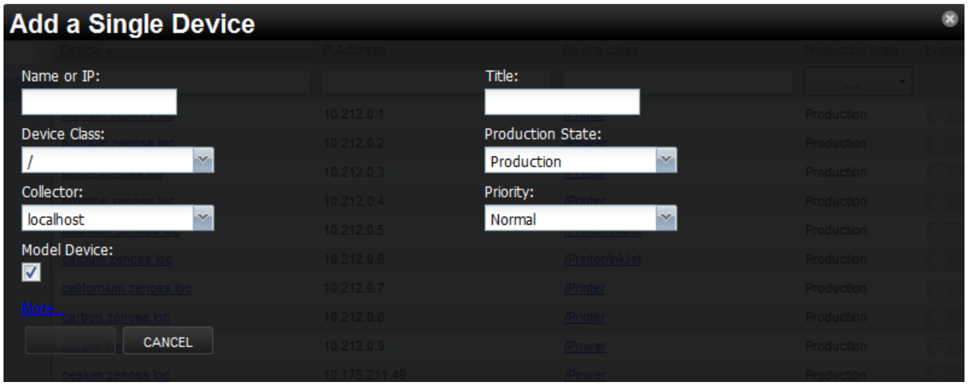
To add a device, follow these steps:

1. Navigate to Infrastructure > Devices.

   The device list appears.

2. From , select Add a Single Device.

   The Add a Single Device dialog appears.



Add a Single Device

Name or IP:

Title:

Device Class: /

Production State: Production

Collector: localhost

Priority: Normal

Model Device: ☑

Figure 1.5. Add a Single Device

3. In the dialog, click **More** to display all available fields and selections.
4. Enter the following information or make selections in the dialog:
   - **Name or IP** - Enter the fully qualified domain name or IP address of a device on your network.
   - **Device Class** - For a Windows server, select /Server/Windows/WMI. For a Linux server, select /Server/SSH/Linux.
   - **SNMP Community** - Enter the SNMP community string for this device. (Setting SNMP community strings globally is discussed later in this guide, in the section titled "Setting SNMP Community Strings Globally.")
5. Click **Add**.

Zenoss discovers the device, adds it to the list of devices, and then gathers additional details about the device to create the device model.

Note

You also can set up WMI monitoring of your Windows devices. Refer to *Zenoss Administration* for more information.

1.2.3.2. View Device Status

To view the newly added device:

1. Navigate to Infrastructure > Devices.

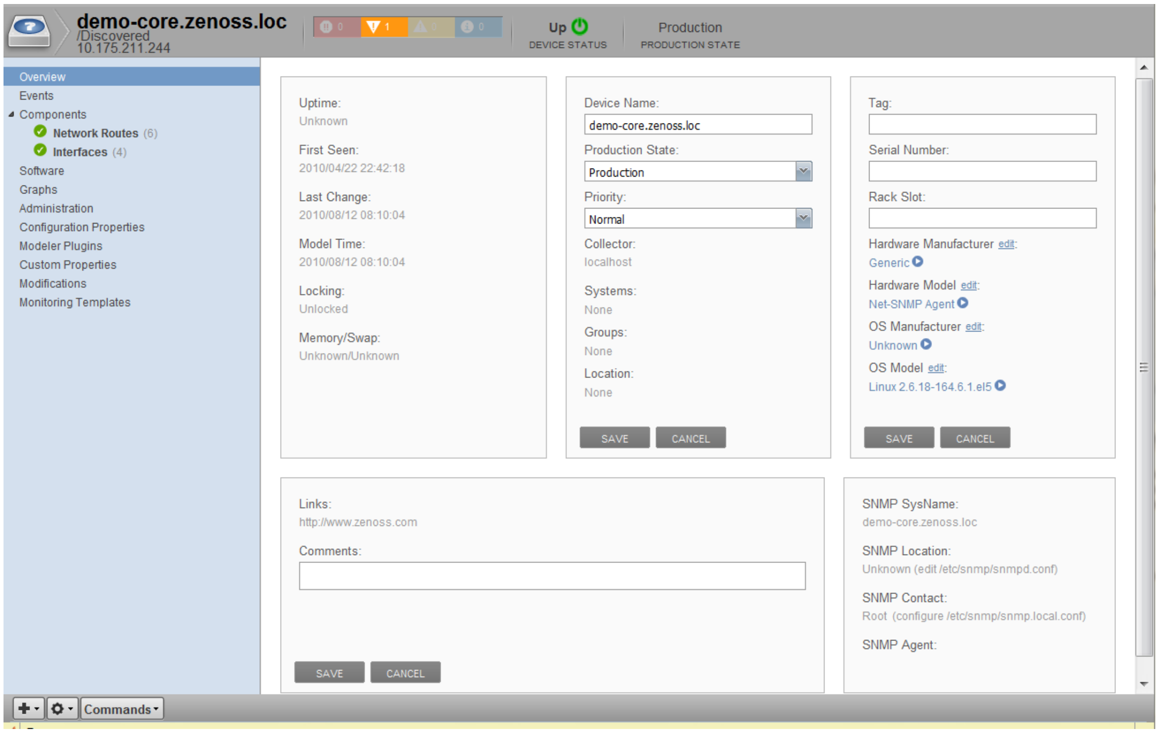
   The device list appears.

2. In the search area at the top of the Device column, type part or all of the device name.

   The system filters the list to display only those names that match the characters you enter.

3. Click the device name.

   The device overview appears.



demo-core.zenoss.loc
/Discovered
10.175.211.244

Up DEVICE STATUS

Production PRODUCTION STATE

Uptime: Unknown

First Seen: 2010/04/22 22:42:18

Last Change: 2010/08/12 08:10:04

Model Time: 2010/08/12 08:10:04

Locking: Unlocked

Memory/Swap: Unknown/Unknown

Device Name: demo-core.zenoss.loc

Production State: Production

Priority: Normal

Collector: localhost

Systems: None

Groups: None

Location: None

Tag:

Serial Number:

Rack Slot:

Hardware Manufacturer edit: Generic

Hardware Model edit: Net-SNMP Agent

OS Manufacturer edit: Unknown

OS Model edit: Linux 2.6.18-164.6.1.el5

Links: http://www.zenoss.com

Comments:

SNMP SysName: demo-core.zenoss.loc

SNMP Location: Unknown (edit /etc/snmp/snmpd.conf)

SNMP Contact: Root (configure /etc/snmp/snmp.local.conf)

SNMP Agent:

Figure 1.6. Device Overview

From here, you can view basic information about the device, or make a selection from the left panel to see more detailed information.

1.2.3.3. View Graphs

Select Graphs from the left panel to see the type of performance data that Zenoss will collect for this device. Graphs are defined at the device class level, and differ depending on the device class to which the device is assigned.

Note

Because your device is new, graphs will not immediately appear, or will contain less data than those illustrated in the following figure. You should allow up to twenty minutes for the system to gather enough data points to render graphs with content.

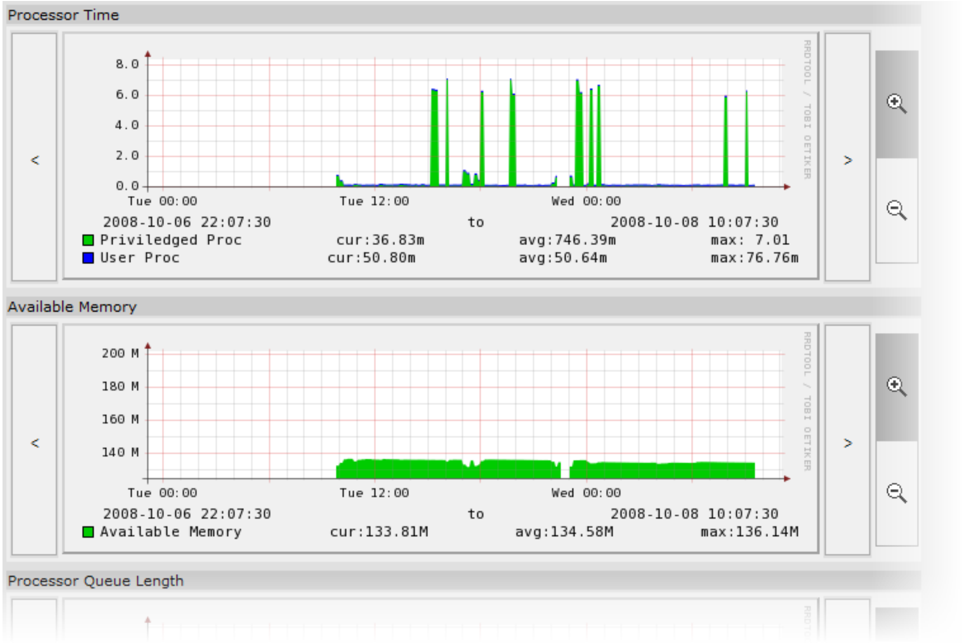

Processor Time
<
8.0
6.0
4.0
2.0
0.0
Tue 00:00
Tue 12:00
Wed 00:00
2008-10-06 22:07:30 to 2008-10-08 10:07:30
🟩 Priviledged Proc cur:36.83m avg:746.39m max: 7.01
🟦 User Proc cur:50.80m avg:50.64m max:76.76m
RRDTOOL / TOBI OETIKER
>
Available Memory
<
200 M
180 M
160 M
140 M
Tue 00:00
Tue 12:00
Wed 00:00
2008-10-06 22:07:30 to 2008-10-08 10:07:30
🟩 Available Memory cur:133.81M avg:134.58M max:136.14M
RRDTOOL / TOBI OETIKER
>
Processor Queue Length

Figure 1.7. Graphs

1.2.4. Set Up, View, and Acknowledge an Alert

Zenoss alerts are tied to user accounts or user groups, and occur when triggered by an event.

When an event is detected by the system, Zenoss categorizes it. Zenoss then examines defined *alerting rules* to determine if the event matches any filters that would create an alert.

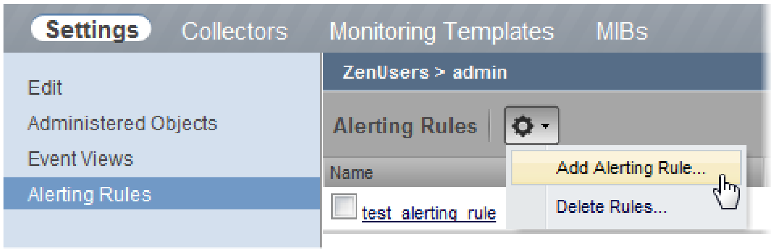
1.2.4.1. Create an Alerting Rule

To create an alerting rule:

1. From the navigation bar, select Advanced.

   The Settings page appears.

2. Select Users from the left panel.
3. In the list of Users, click your currently logged in user name (admin).
4. Select Alerting Rules from the left panel.
5. From the Action menu, select Add Alerting Rule.



The Add Alerting Rule dialog appears.

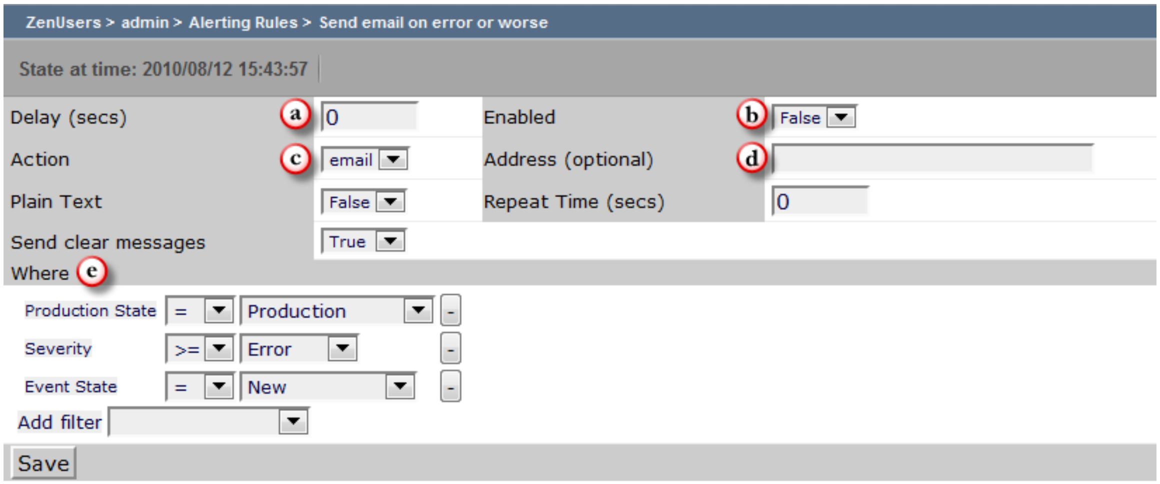
Figure 1.8. Add Alerting Rule

6. Enter a name for the alerting rule, and then click **OK**. The newly created alerting rule appears in the list.

   Note

   Zenoss recommends a descriptive naming convention for alerting rules, as multiple rules may be active at one time. For example: "Send email on error or worse."

7. Click the new rule in the list. The rule edit page appears.



ZenUsers > admin > Alerting Rules > Send email on error or worse

State at time: 2010/08/12 15:43:57

Delay (secs)	0	Enabled	False
Action	email	Address (optional)	
Plain Text	False	Repeat Time (secs)	0
Send clear messages	True		

Where

Production State	=	Production
Severity	>=	Error
Event State	=	New

Add filter

Figure 1.9. Edit Alerting Rule

8. Enter or select criteria for the rule:

   a. **Delay** - Enter a value of 0.

   b. **Enabled** - Select a value of True.

   c. **Action** - Select email to email the alert.

   d. **Address** - Optionally, enter an override email address to receive alerts. By default, Zenoss will email alerts to the address associated with your account.

   e. **Where** - Use the default information in this area:

      - **Production State = Production** - This rule applies only to devices in "Production." A device in any other state will not trigger an alert.
      - **Severity >= Error** - This rule applies only to events of severity "Error" or worse.
      - **Event State = New** - This rule applies only to new events.

9. Click **Save**.

Note

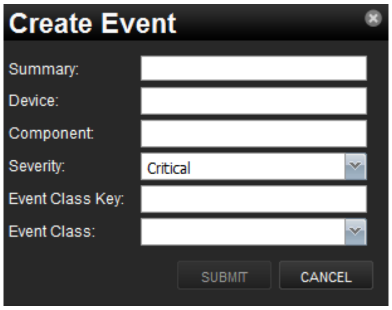
Refer to the *Zenoss Administration* guide for complete information about alerting rules, including editing alert messages and alert schedules.

1.2.4.2. Test an Alerting Rule

To test an alerting rule, create a "dummy" event in the system to trigger it. To do this:

1. From the navigation bar, select Events.
2. Click ➕ to add an event.

   The Create Event dialog appears.

   Create Event

   Summary:

   Device:

   Component:

   Severity: Critical

   Event Class Key:

   Event Class:

   Figure 1.10. Create Event Dialog
3. Complete these dialog fields:
   - **Summary** - Enter a text summary. This summary will appear in the event console.
   - **Device** - Enter the name of the device you added. The event will assert against this device.
   - **Severity** - Select Critical.
4. Click **Submit**.

   The newly created event appears in the list of events in the event console.

1.2.4.3. View the Alert Email

Note

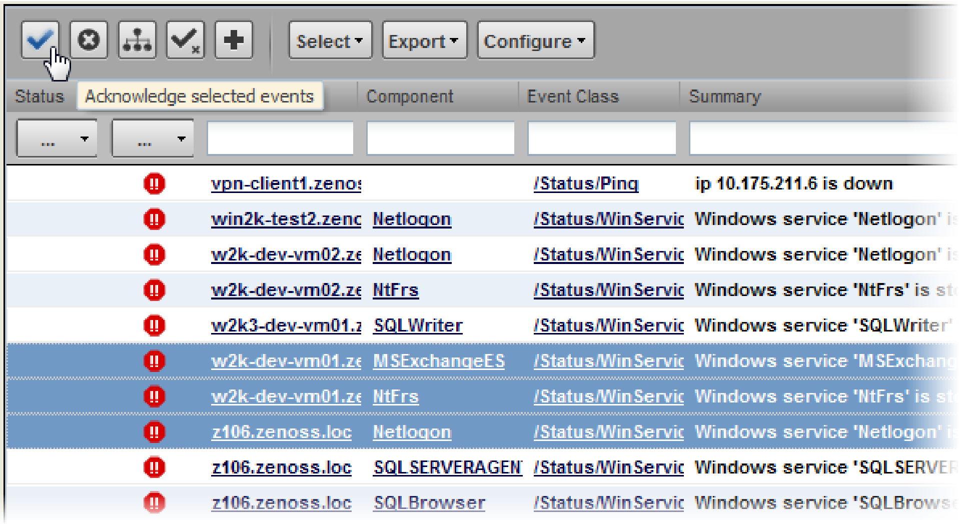
You must set up email before you can view email alerts. See the section titled Managing Zenoss Users for more information.

Check your email (either the address associated with your account, or the additional address you specified) to see notification of the event triggered by the alerting rule.

1.2.4.4. Acknowledge the Event

Acknowledging an event indicates that you are aware that the event has occurred. To acknowledge an event:

1. Select one or more events in the event console. (Ctrl-Click to select more than one event.)
2. Click ✓ (Acknowledge Event) to acknowledge the events.



Status			Component	Event Class	Summary
...	...				
	‼	vpn-client1.zenos		/Status/Ping	ip 10.175.211.6 is down
	‼	win2k-test2.zenc	Netlogon	/Status/WinServic	Windows service 'Netlogon' i
	‼	w2k-dev-vm02.ze	Netlogon	/Status/WinServic	Windows service 'Netlogon' i
	‼	w2k-dev-vm02.ze	NtFrs	/Status/WinServic	Windows service 'NtFrs' is st
	‼	w2k3-dev-vm01.z	SQLWriter	/Status/WinServic	Windows service 'SQLWriter'
	‼	w2k-dev-vm01.ze	MSExchangeES	/Status/WinServic	Windows service 'MSExchang
	‼	w2k-dev-vm01.ze	NtFrs	/Status/WinServic	Windows service 'NtFrs' is st
	‼	z106.zenoss.loc	Netlogon	/Status/WinServic	Windows service 'Netlogon' i
	‼	z106.zenoss.loc	SQLSERVERAGEN	/Status/WinServic	Windows service 'SQLSERVE
	‼	z106.zenoss.loc	SQLBrowser	/Status/WinServic	Windows service 'SQLBrows

Figure 1.11. Acknowledge Events

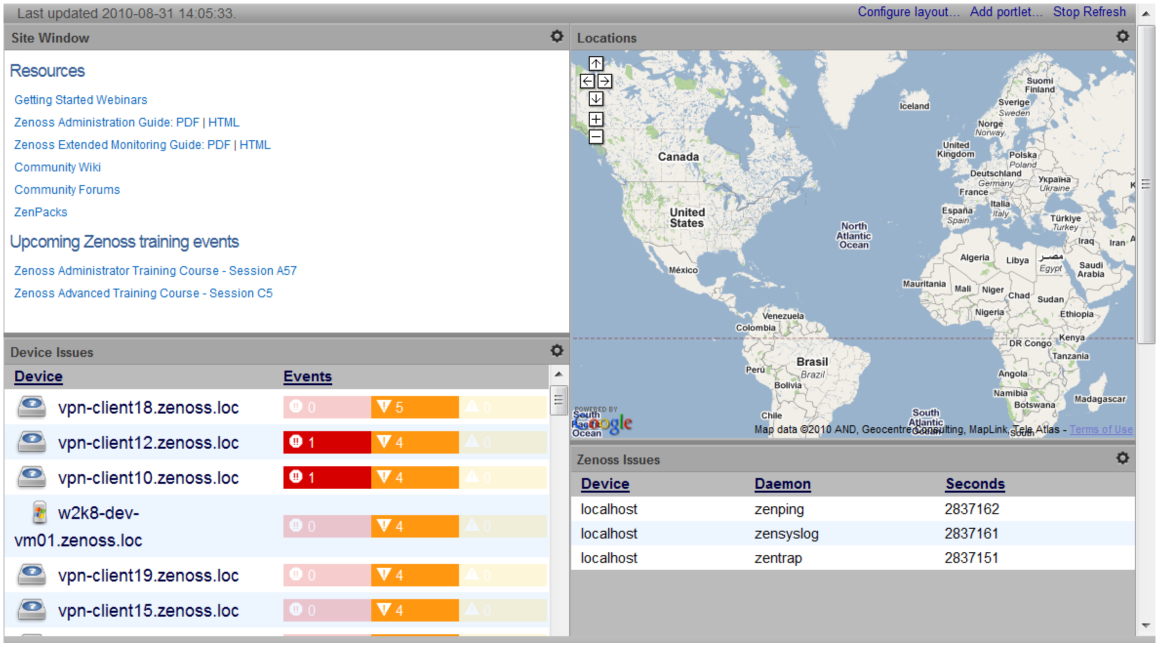
A check mark appears in the Status column next to the acknowledged event or events.

Chapter 2. Exploring Zenoss

Read this chapter to learn more about the Zenoss interface and how to customize it for your preferences.

2.1. Zenoss Dashboard

The Zenoss Dashboard provides at-a-glance information about the status of your IT infrastructure. It is the primary window into devices and events that Zenoss enables you to monitor.



Last updated 2010-08-31 14:05:33.
Configure layout... Add portlet... Stop Refresh
Site Window
Locations
Device Issues
Zenoss Issues
Canada
United States
México
North Atlantic Ocean
Brasil
Map data ©2010 AND, Geocentre Consulting, MapLink, Tele Atlas - Terms of Use

Resources

- Getting Started Webinars
- Zenoss Administration Guide: PDF | HTML
- Zenoss Extended Monitoring Guide: PDF | HTML
- Community Wiki
- Community Forums
- ZenPacks

Upcoming Zenoss training events

- Zenoss Administrator Training Course - Session A57
- Zenoss Advanced Training Course - Session C5

Device	Events		
vpn-client18.zenoss.loc	0	5	0
vpn-client12.zenoss.loc	1	4	0
vpn-client10.zenoss.loc	1	4	0
w2k8-dev-vm01.zenoss.loc	0	4	0
vpn-client19.zenoss.loc	0	4	0
vpn-client15.zenoss.loc	0	4	0

Device	Daemon	Seconds
localhost	zenping	2837162
localhost	zensyslog	2837161
localhost	zentrap	2837151

Figure 2.1. Zenoss Dashboard

The Dashboard can show:

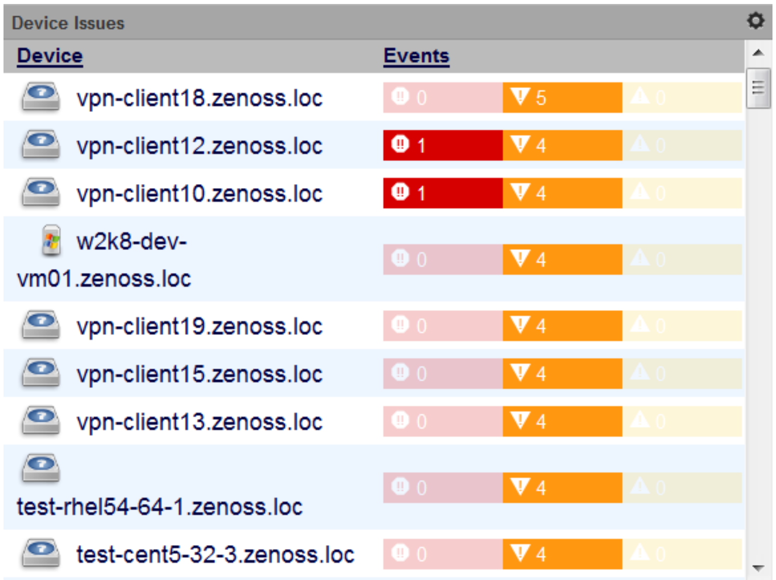
- Zenoss information resources and Web pages
- Important error-level device events
- Geographical high-level view
- "Troubled" devices

2.1.1. Portlets

The main content of the Dashboard comprises *portlets*, which provide information about the system and your infrastructure. You can display more than one of each portlet type on the Dashboard.

Portlets you can display are:

- **Device Issues** - Displays a list of devices, associated with color-coded events of error or critical severity levels. Click a device in the list to view its event log.



Device Issues

Device	Events		
vpn-client18.zenoss.loc	0	5	0
vpn-client12.zenoss.loc	1	4	0
vpn-client10.zenoss.loc	1	4	0
w2k8-dev-vm01.zenoss.loc	0	4	0
vpn-client19.zenoss.loc	0	4	0
vpn-client15.zenoss.loc	0	4	0
vpn-client13.zenoss.loc	0	4	0
test-rhel54-64-1.zenoss.loc	0	4	0
test-cent5-32-3.zenoss.loc	0	4	0

Figure 2.2. Device Issues Portlet

- **Google Maps** (device locations) - Shows configured locations and configured network connections.

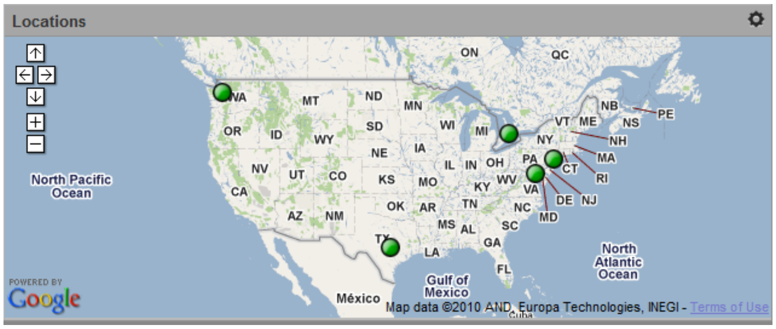
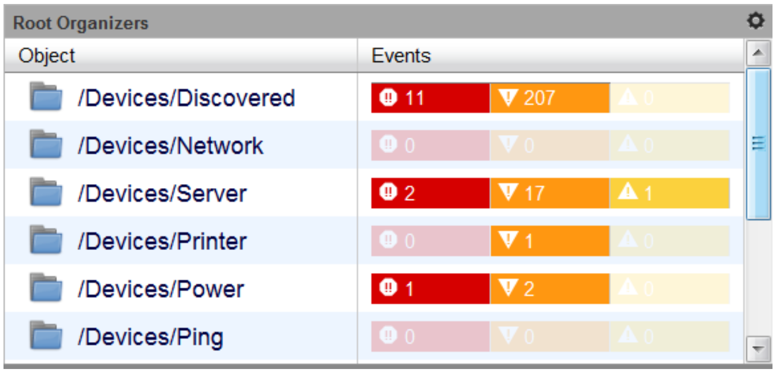


Figure 2.3. Google Maps Portlet

- **Zenoss Issues** - Contains system self-monitoring information.
- **Production States** - Shows devices assigned to a particular production state.
- **Site Window** - Initially provides links to resources such as product guides, forums, and training events.

  The URL for the default content is http://www2.zenoss.com/in-app-welcome. You can customize this portlet to display content from any URL.
- **Top Level (Root) Organizers** - Lists status for each grouping in your defined system hierarchy.



Root Organizers

Object	Events		
/Devices/Discovered	11	207	0
/Devices/Network	0	0	0
/Devices/Server	2	17	1
/Devices/Printer	0	1	0
/Devices/Power	1	2	0
/Devices/Ping	0	0	0

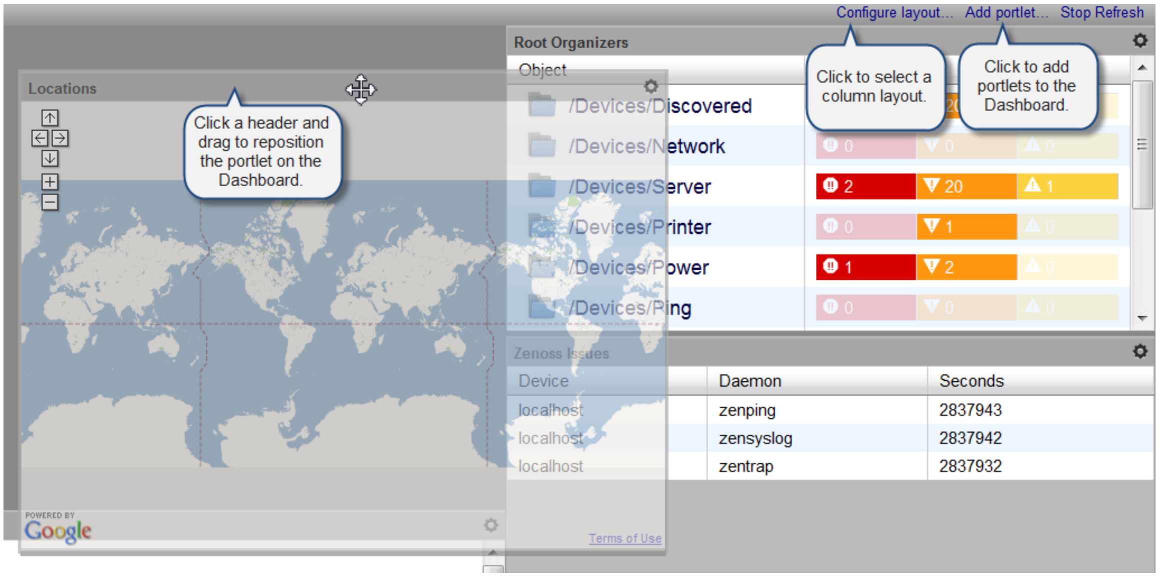
Figure 2.4. Top Level Organizers Portlet

- **Messages** - Displays system messages.
- **Object Watch List** - Allows the display of high-level status device classes, groups, systems, event classes, and locations that you select.

2.1.2. Customizing the Dashboard

You can customize the Dashboard by:

- Selecting the portlets you want to monitor
- Arranging portlets
- Changing the Dashboard column layout



Configure layout... Add portlet... Stop Refresh

Click to select a column layout.

Click to add portlets to the Dashboard.

Click a header and drag to reposition the portlet on the Dashboard.

Locations

Root Organizers

Object	Events		
/Devices/Discovered	[illegible]	20	[illegible]
/Devices/Network	0	0	0
/Devices/Server	2	20	1
/Devices/Printer	0	1	0
/Devices/Power	1	2	0
/Devices/Ping	0	0	0

Zenoss Issues

Device	Daemon	Seconds
localhost	zenping	2837943
localhost	zensyslog	2837942
localhost	zentrap	2837932

Figure 2.5. Customize Dashboard

2.1.2.1. Adding Portlets

To add a portlet to the Dashboard:

1. Click **Add portlet** (located at the top right of the Dashboard main area).

   The Add Portlet dialog appears.

2. Select a portlet.

   The portlet appears at the top right of the Dashboard main area.

To remove a portlet from the Dashboard:

1. Click * (asterisk) that appears at the top right corner of the portlet you want to remove.

   The portlet expands to show its Settings area.

2. Click **Remove Portlet**.

2.1.2.2. Arranging Portlets

To arrange portlets, click the portlet header and drag the portlet to any location on the Dashboard. Other portlets rearrange depending on the location you drop it.

2.1.2.3. Changing the Dashboard Column Layout

You can change the layout of the Dashboard to one, two, or three-column displays. For two-column display, you can additionally choose a layout that offers columns of equal or varying widths.

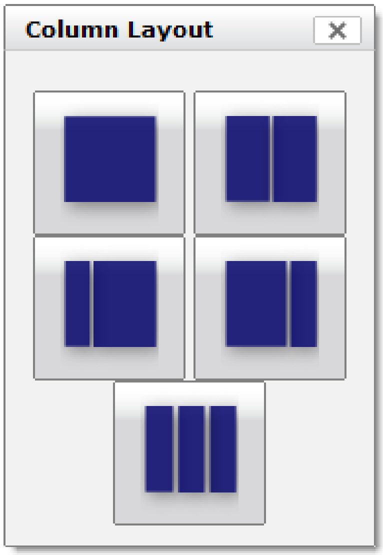


Figure 2.6. Column Layout Dialog

To change the Dashboard column layout:

1. Click Configure layout... (located at the top right of the Dashboard main area).

   The Column Layout dialog appears.

2. Click to select your preferred column layout.

Note

After selecting a new layout, you likely will need to rearrange the portlets on the Dashboard.

2.2. Navigation

The Navigation menu lets you access major system features. In addition to the Dashboard, the menu is divided among several functional areas:

- **Events** - Guides you to the event management area, where you can monitor event status, events, history, configuration properties, and event transforms. You also can track changes made to events.
- **Infrastructure** - Offers access to network infrastructure, including, devices, networks, processes, and services.
- **Reports** - Allows you to view and define reports.
- **Advanced** - Provides access to monitoring templates, collectors, MIBs, and system settings.

2.3. User Information Area

The User information area offers several selections:

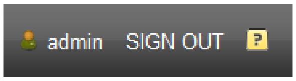


Figure 2.7. User Information Area

- **Login ID** - The ID of the user currently logged in appears at the far left of this area. Click the ID to edit user settings, such as authentication information, roles, and groups. (You also can access user settings from the Navigation bar Advanced selection.)
- **Sign Out** - Click to log out of the system.
- ? **(Help)** - Click to access community product documentation, FAQs, and HowTos, at:

  http://community.zenoss.org/community/documentation

Just below the user information area is a link to page tips, which provide helpful information about available selections.

2.4. Search

A powerful search facility, enabled by the Advanced Search Enterprise ZenPack, allows you to locate devices, other system objects, and events.

Enter part or all of a name in the search box at the top right of the interface. The system displays matches, categorized by type.

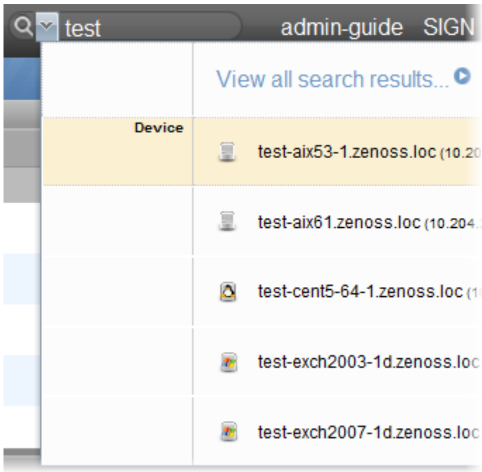

test
admin-guide SIGN
View all search results...
Device
test-aix53-1.zenoss.loc (10.20
test-aix61.zenoss.loc (10.204
test-cent5-64-1.zenoss.loc (1
test-exch2003-1d.zenoss.loc
test-exch2007-1d.zenoss.loc

Figure 2.8. Search

Click "View all search results" to display the Search Results page, which shows all results of the search. From here, you can save the search to access later. To save a search:

1. Click **Save As** (at the bottom left of the Search Results page).

   The Save Search As dialog appears.
2. Enter a name for the search, and then click **Submit**.

You can access saved searches from:

- Action menu located at the bottom of the Search Results page
- Search box located at the top of the interface. (Click the arrow, and then select Manage Saved Searches.)

For information about installing the Advanced Search ZenPack, refer to *Zenoss Extended Monitoring*.

Chapter 3. Configuring Your Devices

This chapter offers guidelines on configuring your devices to interact with Zenoss. Use the following procedures to configure access for:

- UNIX-like devices
- Windows devices

3.1. Configuring UNIX-Like Devices

Use these steps to make sure your device can communicate with Zenoss by using SNMP.

Note

Configuration details for your platform may vary. Refer to the SNMP documentation for your specific system.

1. Install NET-SNMP by using the package management mechanism supported by your UNIX (or UNIX-like) system.
2. Make sure `snmpd` is installed and running.
3. Find the `snmpd` configuration file. Generally, it is located at `/etc/snmp/snmpd.conf`.
4. Back up the file by renaming it to `snmd.conf-back`.
5. Create a new `snmpd.conf` file in the same location.
6. Edit the new file to contain this single line:

   ```
   rocommunity public
   ```

7. Restart the SNMP agent. As `root`, enter this command:

   ```
   /etc/init.d/snmpd restart
   ```

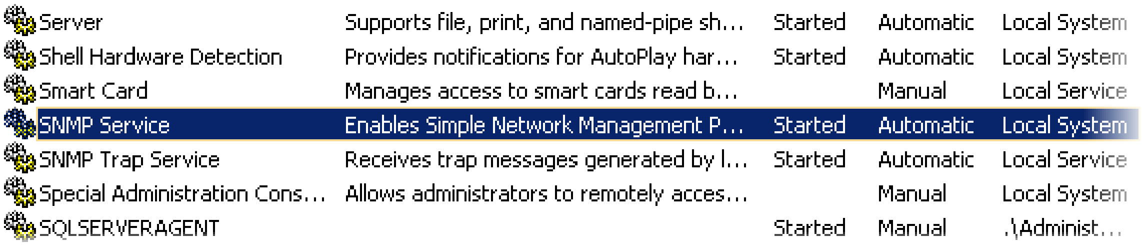
3.2. Configuring Windows Devices

For Zenoss to gather data from your Windows devices, you must configure SNMP or WMI.

3.2.1. Setting Up SNMP for Windows

To set up SNMP for Windows:

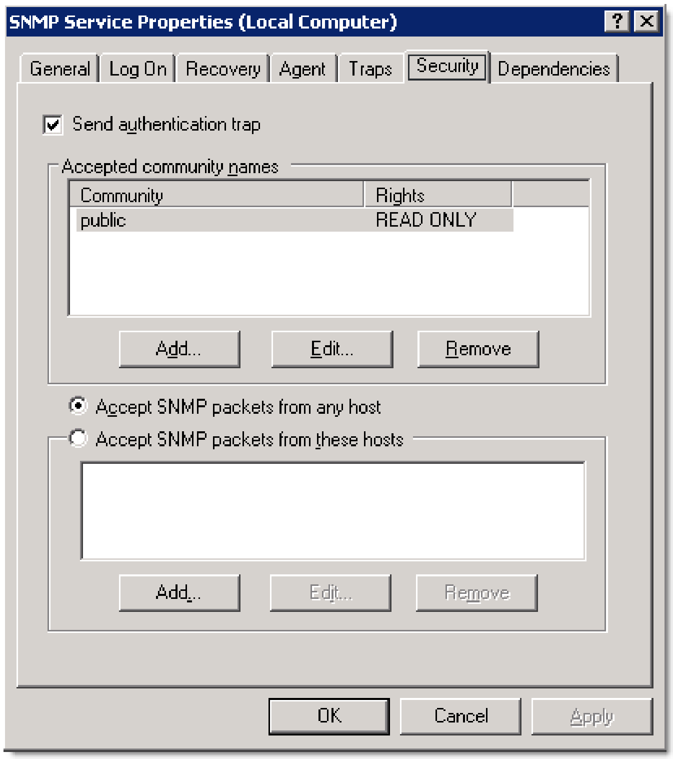
1. Go to the Windows Services list on the device you want to monitor.
2. Determine whether the target device has an SNMP agent installed and running. If so, then it will appear in the Windows Services list.



Server	Supports file, print, and named-pipe sh...	Started	Automatic	Local System
Shell Hardware Detection	Provides notifications for AutoPlay har...	Started	Automatic	Local System
Smart Card	Manages access to smart cards read b...		Manual	Local Service
SNMP Service	Enables Simple Network Management P...	Started	Automatic	Local System
SNMP Trap Service	Receives trap messages generated by l...	Started	Automatic	Local Service
Special Administration Cons...	Allows administrators to remotely acces...		Manual	Local System
SQLSERVERAGENT		Started	Manual	.\Administ...

Figure 3.1. Windows Services

3. Set access permissions to the agent. The current machine's community string should be public and allow connections from any host.



☑ Send authentication trap

Accepted community names

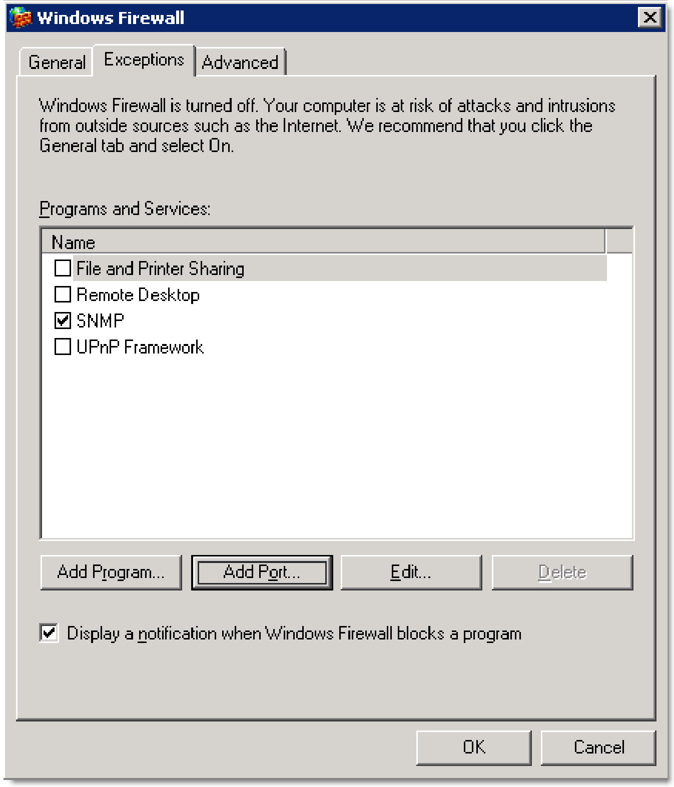
Community	Rights
public	READ ONLY

● Accept SNMP packets from any host

○ Accept SNMP packets from these hosts

Figure 3.2. SNMP Service Properties

4. Ensure that the Windows firewall allows incoming connections to the SNMP agent.



Windows Firewall is turned off. Your computer is at risk of attacks and intrusions from outside sources such as the Internet. We recommend that you click the General tab and select On.

Programs and Services:

Name

- □ File and Printer Sharing
- □ Remote Desktop
- ☑ SNMP
- □ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

Figure 3.3. Windows Firewall

Note

Running the default Microsoft SNMP agent limits the information available to you. To get the most detailed level of information from your Windows devices, Zenoss recommends that you use SNMP InformantTM™.

For more information about installing SNMP remotely on your Windows device, browse to the HowTos section of the Zenoss Web site, at this location:

http://community.zenoss.org/docs/DOC-2519

3.2.2. Setting Up WMI for Windows

Follow these steps to create an account for Zenoss to obtain WMI information from Windows devices.

1. Set up a local Windows Administrator or Domain Administrator account.

   You will use the login information for these accounts when setting the zProperties for zWinuser and zWinPassword, when adding devices to Zenoss.

2. Run one of the following commands in the console to test WMI connectivity to the device:

   - If using a Windows Domain user:

     ```
     wmic -U "DOMAIN\USER%PASSWORD" //HOST "SELECT name FROM Win32_Service"
     ```

   - If using a local Windows user account:

     ```
     wmic -U ".\USER%PASSWORD" //HOST "SELECT name FROM Win32_Service"
     ```

The system should simulate the way Zenoss collects data and intervals, and should return a list of available `perfmon` counters.

If the list does not return, make sure the user has administrator privileges on the Windows system, and then run one of the commands again.

Chapter 4. Setting Up Zenoss to Interact with Your Devices

To set up Zenoss to interact with your devices, you must:

- Set up configuration properties
- Set up SNMP communities you use in your environment

4.1. About Configuration Properties

To set up Zenoss device interaction, you configure properties for each device. Called *configuration properties*, these properties also are part of the model of the device. Use configuration properties to assign a range of device characteristics, such as:

- Collection methods
- Timeouts
- Access details (such as SSH, SNMP, and WMI)

Configuration properties can be inherited and defined at different levels of the device class hierarchy, from the general "/" class to the individual device level. The lowest point in the hierarchy where this is defined is the configuration property that is assigned to the device.

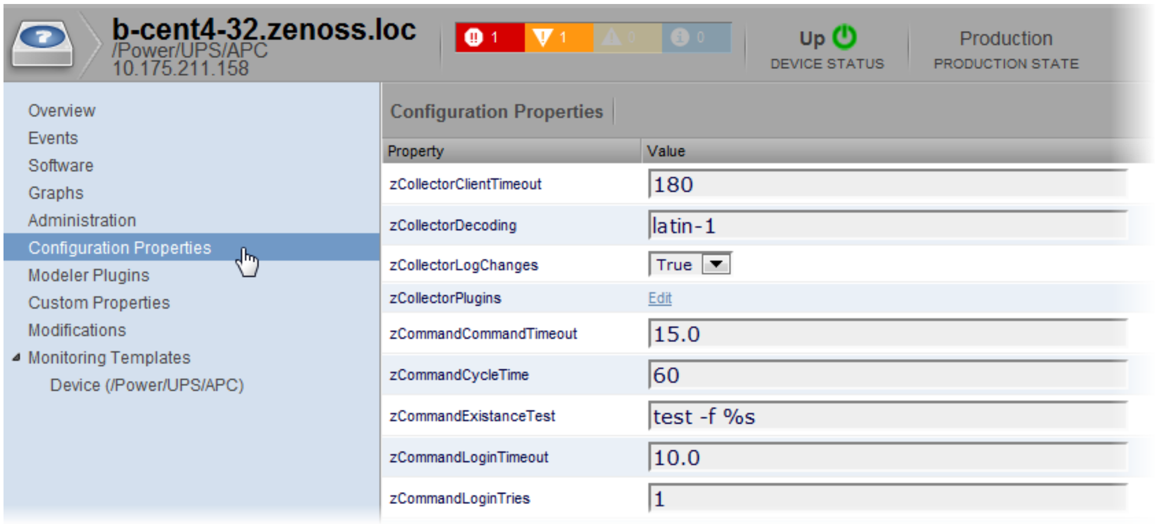
4.1.1. Accessing Configuration Properties

To view configuration properties:

1. From the menu bar, select Infrastructure.

   The device list appears.
2. Click a device in the list.

   The device overview page appears.
3. In the left panel, select Configuration Properties.



Property	Value
zCollectorClientTimeout	180
zCollectorDecoding	latin-1
zCollectorLogChanges	True
zCollectorPlugins	Edit
zCommandCommandTimeout	15.0
zCommandCycleTime	60
zCommandExistanceTest	test -f %s
zCommandLoginTimeout	10.0
zCommandLoginTries	1

Figure 4.1. Configuration Properties Selection

4.2. Setting SNMP Community Strings Globally

To set up SNMP communities to be used in your environment:

1. From the menu bar, select Infrastructure.
2. In the left panel, click **Details**.
3. In the left panel, click Configuration Properties.

4.3. Windows Configuration Properties

If you plan to use WMI monitoring, then you must set additional configuration properties after the device is added. This ensures that Zenoss can access all of the modeling information and collect performance data.

To set the Windows user name and password for a device:

1. Click the device in the device list.

   The device overview page appears.
2. In the left panel, select Configuration Properties
3. Scroll down to the zWinPassword and zWinUser configuration properties and enter appropriate information.
4. Click **Save**.

For more information about configuration properties, refer to the *Zenoss Administration* guide.

Chapter 5. Devices and Device Organizers

In Quick Start, you learned how to add a Windows device to Zenoss. Read this chapter to learn about:

- Adding other device types
- Discovering devices in your network
- Using device classes to optimize available monitoring information for each type of device on your network

5.1. Adding Other Device Types

The information that Zenoss collects differs depending on the device class. Add one or more devices to see how information is collected for other device types, and how that information differs depending on the assigned device class. For example, add:

- Linux server in the /Server/Linux device class
- Microsoft Exchange Server in the /Server/Windows/WMI/MS-Exchange device class
- Active Directory Server in the /Server/Windows/WMI/Active Directory device class
- Microsoft SQL Server in the /Server/Windows/WMI/MS-SQL device class

After adding these devices, navigate to each device in Zenoss and view the data being collected.

5.2. Discovering Devices

You can provide network or IP address range information so that the system can discover your devices.

Follow these steps to discover devices:

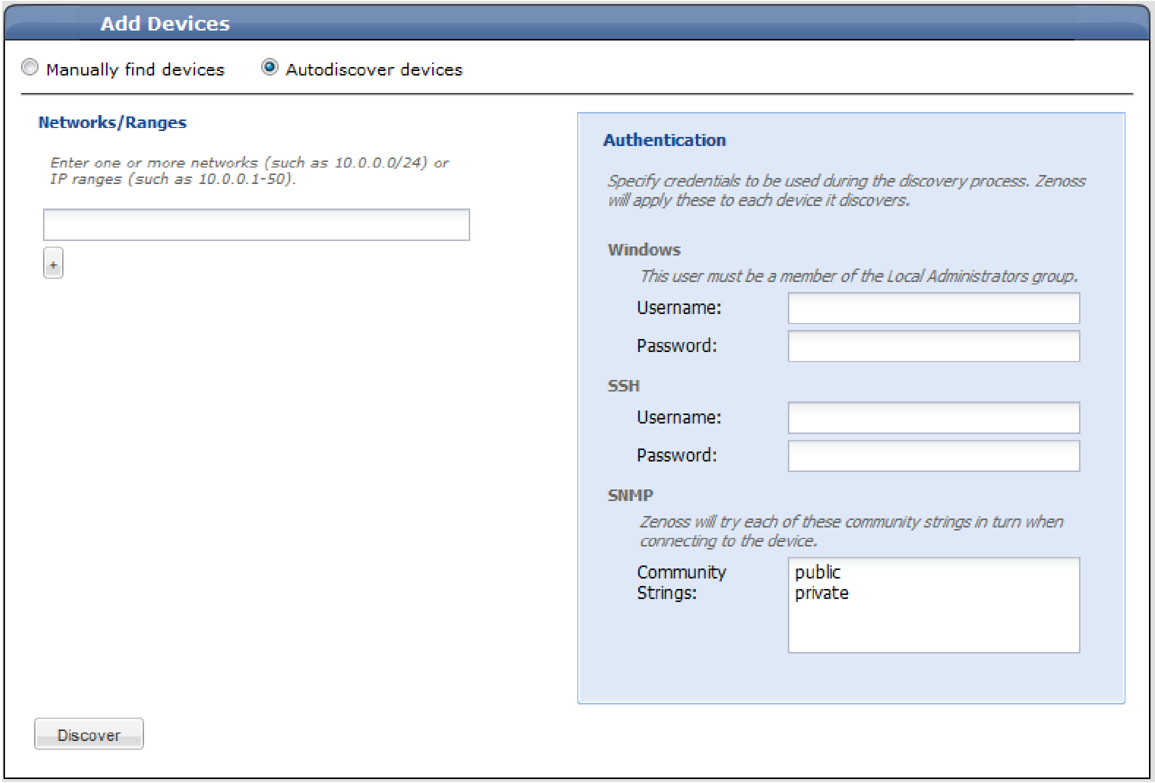
1. From the navigation bar, select Infrastructure.

   The Devices page appears.

2. Select Add Multiple Devices from ⊞ (Add Devices).

   The Add Devices panel appears.

3. Select the **Autodiscover devices** option.



Add Devices

○ 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

Figure 5.1. Add Multiple Devices (Discover)

4. For each network or IP range in which you want Zenoss 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 a range of IP addresses:

   10.175.211.1-50

5. If you want to enter multiple addresses or ranges, click +. For each network, you must enter a netmask or IP range.

6. For each network or IP range, specify the Windows, SSH, or SNMP credentials you want Zenoss to use on the devices it discovers. You can enter only one of each. Zenoss will attempt to use the same credentials on each device it discovers within the networks or IP ranges specified, but will not try to automatically classify the devices.

7. Click **Discover**.

   The discovery process iterates through every IP address in the networks and IP ranges you specify, adding each device that responds to a ping request. Further, the process adds information to any device that responds to an SNMP, WMI, or SSH request.

Zenoss places discovered routers in the device path /Network/Router. Devices are placed in the /Discovered device class.

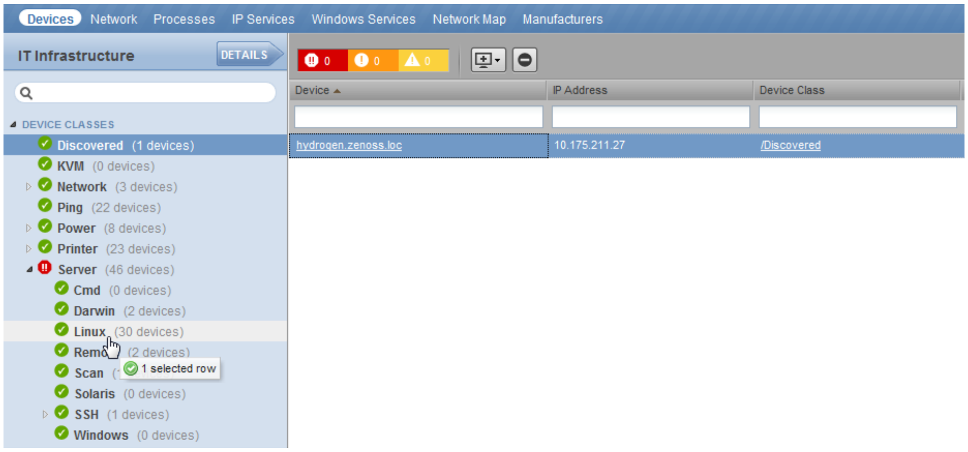
5.2.1. Classifying Discovered Devices

Once discovery is complete, you must move discovered devices (placed, by default, in the /Discovered class) to an appropriate device class in the hierarchy. Moving devices to their correct hierarchy location makes it possible for monitoring to begin.

Servers are organized by operating system. If the system discovers Windows devices, for example, you might choose to relocate them to /Server/Windows. Similarly, you might choose to classify discovered Linux devices in /Server/Linux (if you want to monitor and model using SNMP), or /Server/SSH/Linux (if you want to monitor and model using SSH).

To classify discovered devices:

1. Select one or more discovered devices (highlight one or more rows) in the device list.
2. Drag the selected devices to the new device class in the tree view.



Device ▲	IP Address	Device Class
hydrogen.zenoss.loc	10.175.211.27	/Discovered

Figure 5.2. Classifying Discovered Devices

   The Move Devices dialog appears.

3. Click **OK**.

   The list of devices refreshes, and the devices now appear in the newly selected class.

5.2.2. Updating Device Authentication Details

For each device added to the database and set to its proper device class, the system may require additional or different authentication information before it can gather device information and monitor the device.

For example, for a device in the /Server/Windows class, you must supply your Windows user name and password before the system can monitor the device. To do this:

1. Click a device name in the devices list.

   The Device summary page appears.

2. Select Configuration Properties from the left panel.
3. Set the user name and password values in the zWinUser and zWinPassword configuration properties.
4. Click **Save**.

Similarly, for a device in the /Server/SSH/GenericLinux class, you must supply your SSH user name and password. Set these values in the device's zCommandUsername and zCommandPassword configuration properties.

Tip

After making changes, you should remodel the device to ensure the authentication changes are valid.

5.2.3. Adding Information to a Device Record

You may want to add details about a discovered device.

To add information:

1. Click a device name in the devices list.

   The Device summary page appears. Values that appear in text fields can be edited.
2. Enter or change information in one or more fields, and then click **Save** to save your changes.

5.3. Creating and Using Organizers

Within Zenoss you can create organizers. Organizers let you monitor devices in logical groups, such as:

- Systems
- Groups
- Locations

A device can be a member of many groups or systems, but can be in only one location.

Use this procedure to add a system to the list of organizers, and then add devices to that system.

1. From the menu bar, select Infrastructure.

   The device list appears.
2. Click the Systems organizer in the tree view.
3. Click + to add a system.

   The Add System dialog appears.
4. Enter a name and description for the system, and then click **Submit**.

   The system is added.
5. Drag one or more devices from the device list to the system.

5.3.1. Adding and Nesting Locations

Use the following procedure to create a location, and then move and nest that location.

The locations you add using this procedure are the same locations that Zenoss uses when creating a Google map of your devices. You can use locations to add Google maps addresses.

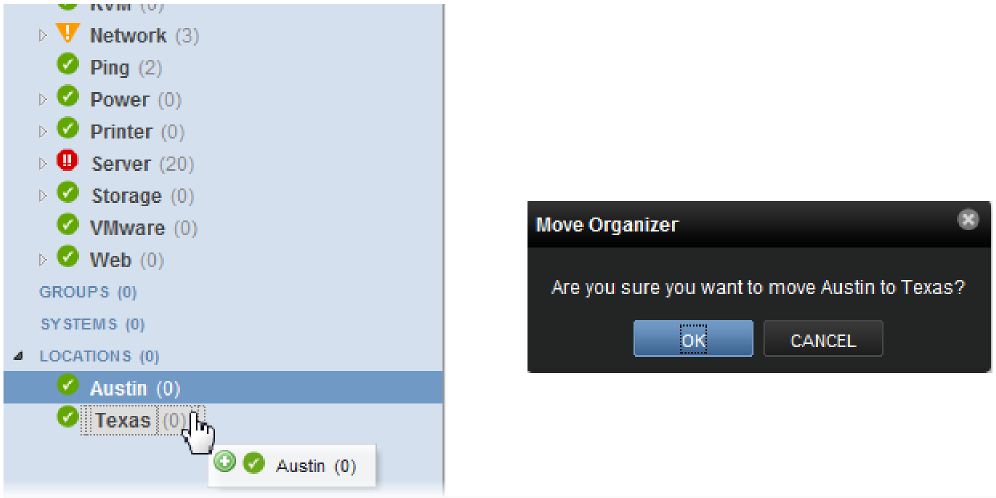
1. From the menu bar, select Infrastructure.

   The device list appears.
2. Click the Locations organizer in the tree view.
3. Click + to add a location.

The Add Location dialog appears.

4. Enter a name, description, and address (or zip code) for the location, and then click **Submit**.
5. To nest one location under another, drag it in the tree view.

   A confirmation dialog appears.



Move Organizer

Are you sure you want to move Austin to Texas?

Figure 5.3. Move Location

6. Click **OK**.

5.3.2. Displaying Locations on the Dashboard

To display locations on the Dashboard:

1. From the Dashboard, click the Add portlet link located near the top right of the page.
2. Select Top Level Organizers from the list of options.

   The Root Organizers portlet appears on the Dashboard.
3. Click the indicator at the top right of the portlet to open the portlet list of options.
4. From the Root Organizer list of options, select Locations.
5. Click **Save Settings**.

   The portlet displays the status for the locations you have entered.

Note

You also will use these locations when creating a Google map.

Chapter 6. Performance Monitoring

Read this chapter for information about monitoring:

- Windows server
- Tomcat (or other Java/JMX) server

6.1. Monitor a Windows Server

The Windows Performance (ZenWinPerf) Enterprise ZenPack allows agentless performance monitoring of Windows servers. It provides a data source, WinPerf, that uses a Windows performance counter rather than an SNMP OID to specify the value to collect. WinPerf data sources are processed by the `zenwinperf` daemon.

For more information about the Windows Performance ZenPack, refer to the *Zenoss Extended Monitoring* guide.

6.2. Monitor a Tomcat (or Other Java/JMX) Server

Use the instructions in this section to prepare for and set up monitoring of a Tomcat or other Java/JMX server.

6.2.1. Device Preparation for the Tomcat Server

When you start your Tomcat server, you must enable JMX access with these commands:

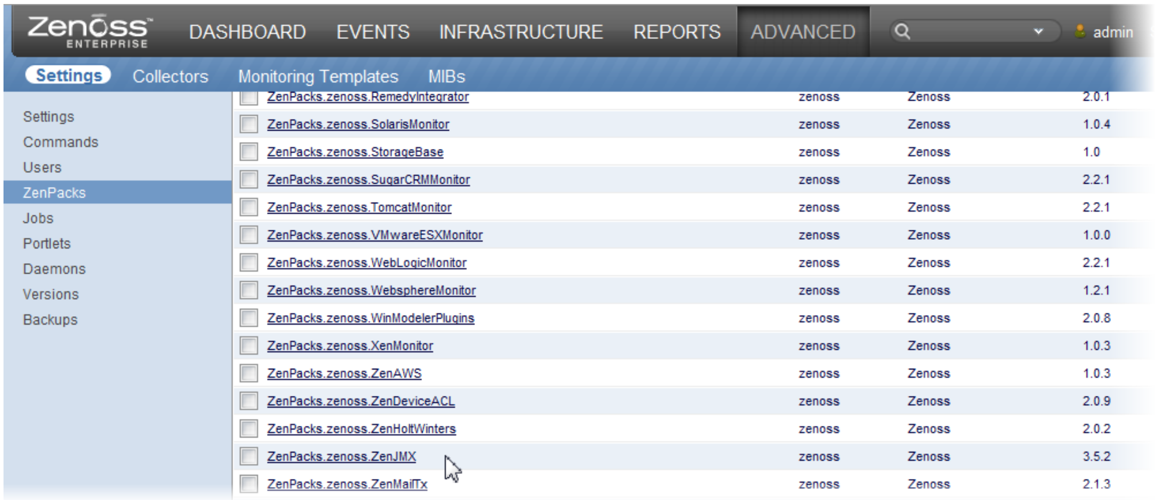
```
JAVA_OPTS="-Dcom.sun.management.jmxremote.port=12346"
JAVA_OPTS="${JAVA_OPTS} -Dcom.sun.management.jmxremote.authenticate=false"
JAVA_OPTS="${JAVA_OPTS} -Dcom.sun.management.jmxremote.ssl=false"  \
 export JAVA_OPTS
```

Note

If you prefer to use a WebLogic or JBoss server, see the configuration notes located at:

http://dev.zenoss.org/trac/browser/trunk/zenpacks/ZenPacks.zenoss.ZenJMX/notes.txt

Look at the list of loaded Zen Packs to verify that the ZenJMX ZenPack is installed. Select Advanced > Settings from the menu bar, and then select ZenPacks in the left panel.



□	ZenPacks.zenoss.RemedyIntegrator	zenoss	Zenoss	2.0.1
□	ZenPacks.zenoss.SolarisMonitor	zenoss	Zenoss	1.0.4
□	ZenPacks.zenoss.StorageBase	zenoss	Zenoss	1.0
□	ZenPacks.zenoss.SugarCRMMonitor	zenoss	Zenoss	2.2.1
□	ZenPacks.zenoss.TomcatMonitor	zenoss	Zenoss	2.2.1
□	ZenPacks.zenoss.VMwareESXMonitor	zenoss	Zenoss	1.0.0
□	ZenPacks.zenoss.WebLogicMonitor	zenoss	Zenoss	2.2.1
□	ZenPacks.zenoss.WebsphereMonitor	zenoss	Zenoss	1.2.1
□	ZenPacks.zenoss.WinModelerPlugins	zenoss	Zenoss	2.0.8
□	ZenPacks.zenoss.XenMonitor	zenoss	Zenoss	1.0.3
□	ZenPacks.zenoss.ZenAWS	zenoss	Zenoss	1.0.3
□	ZenPacks.zenoss.ZenDeviceACL	zenoss	Zenoss	2.0.9
□	ZenPacks.zenoss.ZenHoltWinters	zenoss	Zenoss	2.0.2
□	ZenPacks.zenoss.ZenJMX	zenoss	Zenoss	3.5.2
□	ZenPacks.zenoss.ZenMailTx	zenoss	Zenoss	2.1.3

Figure 6.1. Loaded ZenPacks

6.2.2. Monitoring the Tomcat Server

Use these instructions to set up Zenoss to monitor a Tomcat server.

1. Add the Java server device to your preferred device class.

   Tip

   You might, for example, set up a Java Servers class under the Server device class and add the device in that location.

2. When adding the device, de-select the Model option (In this case, the SNMP model will not add significant additional information.)
3. Navigate to the newly added Java server device.
4. In the left panel, select Device under Monitoring Templates.
5. From the Action menu, select Bind Templates.

   The Bind Templates dialog appears.

6. Select the ZenJMX template (loaded with the ZenJMX ZenPack) from the Available list and move it to the Selected list, and then click **Save**.

   The ZenJMX monitoring template is added to the list of monitoring templates.

6.2.2.1. Change Data Source Parameters

In the next set of steps, you will change some of the parameters of the data sources. These data sources are provided through Java, and must be fine-tuned for Zenoss. These sample steps illustrate changing the Heap memory Data Source.

1. Select the ZenJMX monitoring template in the left panel.
2. In the Data Sources area, double-click ZenJMX Heap Memory.

   The Edit Data Source dialog appears.

3. Ensure that the Enabled option is selected.
4. In the JMX Connection and Metadata Information area, make sure that the value of the Management Port field is set to the same value as the management port on your Java server.
5. In the JMX Remote Authentication Information area, make sure that:
   a. If you have remote authentication enabled on your server, you have also enabled it in Zenoss.
   b. Zenoss and server values match.
6. Click **Save**.

To see where the JMX information appears in the device model, navigate to the device through the device list, and then click Graphs in the left panel.

These performance graphs should appear on the page:

- ZenJMX Non-Heap Memory
- ZenJMX Heap Memory
- ZenJMX Open File Descriptors
- ZenJMX Thread Count

The graphs are created by ZenJMX. When they are initially loaded, they will not display actual data.

6.2.2.2. Collecting and Displaying Data

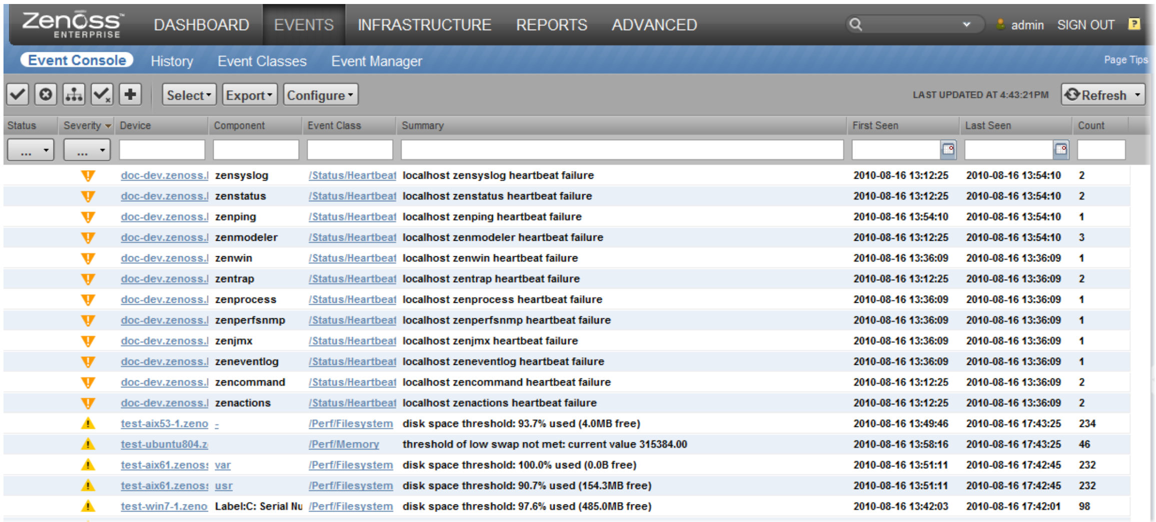
You must restart the ZenJMX daemon to being collecting and displaying data. To restart the daemon:

1. From the menu bar, select Advanced.
2. In the left panel, select Daemons.
3. Next to the `zenjmx` entry, click **Restart**.

Chapter 7. Event Management

The event console enables you to view and manage events. It displays the repository of all events that are detected by the system.

To access the event console, select Events from the menu bar.



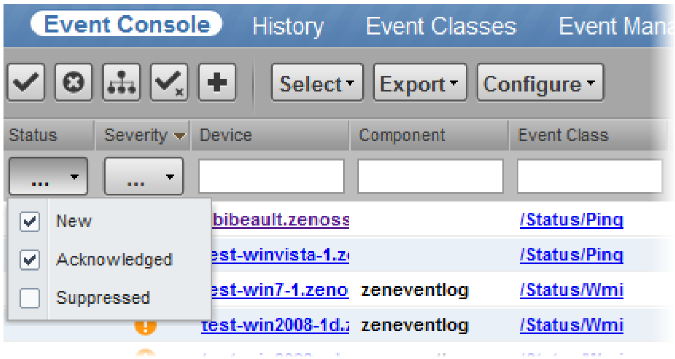
Status	Severity	Device	Component	Event Class	Summary	First Seen	Last Seen	Count
	!	doc-dev.zenoss.l	zensyslog	/Status/Heartbeat	localhost zensyslog heartbeat failure	2010-08-16 13:12:25	2010-08-16 13:54:10	2
	!	doc-dev.zenoss.l	zenstatus	/Status/Heartbeat	localhost zenstatus heartbeat failure	2010-08-16 13:12:25	2010-08-16 13:54:10	2
	!	doc-dev.zenoss.l	zenping	/Status/Heartbeat	localhost zenping heartbeat failure	2010-08-16 13:54:10	2010-08-16 13:54:10	1
	!	doc-dev.zenoss.l	zenmodeler	/Status/Heartbeat	localhost zenmodeler heartbeat failure	2010-08-16 13:12:25	2010-08-16 13:54:10	3
	!	doc-dev.zenoss.l	zenwin	/Status/Heartbeat	localhost zenwin heartbeat failure	2010-08-16 13:36:09	2010-08-16 13:36:09	1
	!	doc-dev.zenoss.l	zentrap	/Status/Heartbeat	localhost zentrap heartbeat failure	2010-08-16 13:12:25	2010-08-16 13:36:09	2
	!	doc-dev.zenoss.l	zenprocess	/Status/Heartbeat	localhost zenprocess heartbeat failure	2010-08-16 13:36:09	2010-08-16 13:36:09	1
	!	doc-dev.zenoss.l	zenperfsnmp	/Status/Heartbeat	localhost zenperfsnmp heartbeat failure	2010-08-16 13:36:09	2010-08-16 13:36:09	1
	!	doc-dev.zenoss.l	zenjmx	/Status/Heartbeat	localhost zenjmx heartbeat failure	2010-08-16 13:36:09	2010-08-16 13:36:09	1
	!	doc-dev.zenoss.l	zeneventlog	/Status/Heartbeat	localhost zeneventlog heartbeat failure	2010-08-16 13:36:09	2010-08-16 13:36:09	1
	!	doc-dev.zenoss.l	zencommand	/Status/Heartbeat	localhost zencommand heartbeat failure	2010-08-16 13:12:25	2010-08-16 13:36:09	2
	!	doc-dev.zenoss.l	zenactions	/Status/Heartbeat	localhost zenactions heartbeat failure	2010-08-16 13:12:25	2010-08-16 13:36:09	2
	⚠	test-aix53-1.zeno	-	/Perf/Filesystem	disk space threshold: 93.7% used (4.0MB free)	2010-08-16 13:49:46	2010-08-16 17:43:25	234
	⚠	test-ubuntu804.z		/Perf/Memory	threshold of low swap not met: current value 315384.00	2010-08-16 13:58:16	2010-08-16 17:43:25	46
	⚠	test-aix61.zenos:	var	/Perf/Filesystem	disk space threshold: 100.0% used (0.0B free)	2010-08-16 13:51:11	2010-08-16 17:42:45	232
	⚠	test-aix61.zenos:	usr	/Perf/Filesystem	disk space threshold: 90.7% used (154.3MB free)	2010-08-16 13:51:11	2010-08-16 17:42:45	232
	⚠	test-win7-1.zeno	Label:C: Serial Nu	/Perf/Filesystem	disk space threshold: 97.6% used (485.0MB free)	2010-08-16 13:42:03	2010-08-16 17:42:01	98

Figure 7.1. Event Console

7.1. Sorting and Filtering Events

Zenoss lets you sort and filter events that appear in the event console. You can sort events by any column that appears. To sort events, click a column header. Clicking the header toggles between ascending and descending sort order.

Filter options appear below each column header.



☑ New
☑ Acknowledged
☐ Suppressed

Device	Component	Event Class
bibeault.zenoss		/Status/Ping
est-winvista-1.z		/Status/Ping
est-win7-1.zeno	zeneventlog	/Status/Wmi
test-win2008-1d.:	zeneventlog	/Status/Wmi

Figure 7.2. Filter Events

You can filter the events that appear in the list in several ways, depending on the field type. Date fields (such as First Seen and Last Seen) allow you to enter a value or use a date selection tool to limit the list. For other fields, such as Device, Component, and Event Class, enter a match value to limit the list.

To clear filters, select **Configure > Clear filters**.

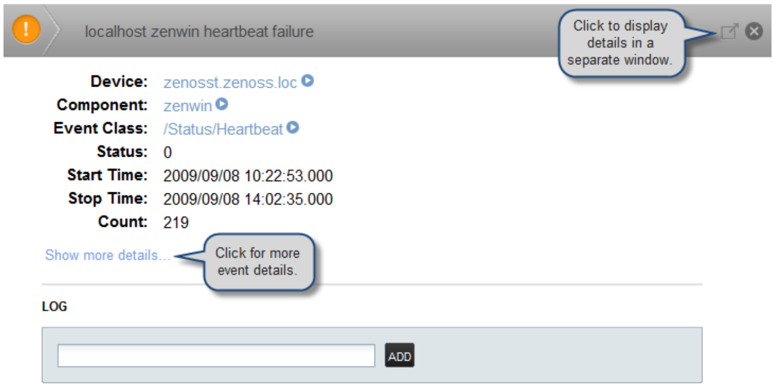
7.2. Viewing Event Details

You can view details for any event in the system. To view details, double-click an event row.

Note

Do not double-click on or near the device name, component, or device class in the row. Doing this displays details about that entity, rather than about the event.

The Event Detail area appears.



localhost zenwin heartbeat failure

Click to display details in a separate window.

Device:	zenosst.zenoss.loc
Component:	zenwin
Event Class:	/Status/Heartbeat
Status:	0
Start Time:	2009/09/08 10:22:53.000
Stop Time:	2009/09/08 14:02:35.000
Count:	219

Show more details...

Click for more event details.

LOG

Figure 7.3. Event Details

To see more information about the event, click Show more details.

You can use the Log area to add specific information about the event. Enter details, and then click **Add**.

7.3. Selecting and Managing Events

Select and manage events from the event console. To select one or more events, you can:

- Click a row to select a single event
- Ctrl-Click rows to select multiple events
- Click Select to select all, none, new, or suppressed events

After selecting an event, you can:

- Acknowledge the event
- Close the event (move it to history)
- Map the event, associating it with a specific event class
- Return the event to New status (revoke its Acknowledged status)

You also can add events from the event console.

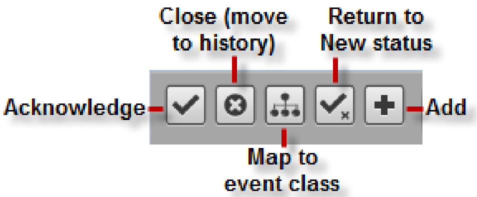


Figure 7.4. Event Management Options

7.4. Creating Test Events

While most events are generated by the devices in your system, Zenoss also provides the ability to generate test events. This feature is helpful when you are testing or trying a new setup.

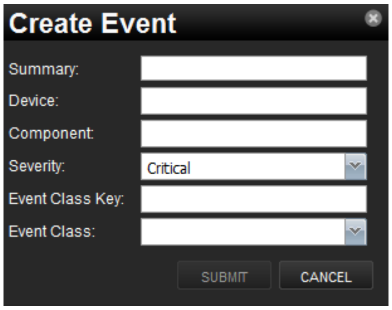
To create a test event:

1. From the menu bar, select Events.

   The event console appears.

2. Click + (Add Event).

   The Create Event dialog appears.

   Severity: Critical

   Figure 7.5. Create Event Dialog

3. Enter and select details about the test event and device you want to test, and then click **Submit**. The event appears in the system according to the criteria you set.

Chapter 8. Managing Zenoss Users

Zenoss user accounts associate rules and permission, and alerting rule behavior, with a specific user. Along with assigned permissions, user accounts comprise login and contact information for a user.

Use the following procedures to:

- Create a user account
- Edit user account details

8.1. Creating User Accounts

To create a Zenoss user account:

1. Log in as a user with administrative privileges.
2. From the menu bar, select Advanced.

   The Settings page appears.
3. In the left panel, select Users.
4. From the Action menu, select Add User.

   The Add User dialog appears.
5. Enter a user name and email address for the user account.
6. Click **OK**. The newly created user appears in the list.

8.2. Editing User Account Details

To edit user account details:

1. Click the user name in the Users list.

   The User details page appears.
2. Enter or select details for the user account.
3. Enter your administrative password to confirm changes to the account, and then click **Save**.

Chapter 9. Troubleshooting Device Connectivity Issues

If your Zenoss instance relies on SNMP to collect information from remote systems, use these tips and tricks to identify and help solve SNMP issues with the devices on your network.

9.1. Identifying SNMP Agent Issues

Make sure an SNMP agent is running and accessible from the Zenoss server. To check, run this command on the Zenoss server:

```
$ snmpwalk -c YOUR_COMMUNITY_STRING -v1 YOUR_DEVICE_IP
```

Tip

If you do not know your community string, try `public`.

If the system returns this string, then the device is responding to your SNMP request:

```
Timeout: No response from xxx.xxx.xxx.xxx
```

9.2. Resolving Linux SNMP Issues

Depending on your device platform, there are several reasons that the device may not be responding to the request. To resolve this problem, you can:

- Check permissions on the agent side
- Ensure that there is an SNMP daemon running on the target device. To determine if the daemon is running, issue this command:

  ```
  netstat -an | grep -i udp
  ```

  If you see an entry that looks like this, then the agent is running but Zenoss cannot get the information for another reason:

  ```
  udp 0.0.0.0:161 0.0.0.0:*
  ```

  If the SNMP daemon is running, but the configuration does not allow connections, then add this line to the `/etc/snmp/snmpd.conf` file to grant read access to Zenoss:

  ```
  rocommunity public
  ```
- Check firewalls

  There may be a firewall on the target device, or between the Zenoss server and the target device. Use the `tcpdump` command to debug this issue.

  Note

  Refer to the *Zenoss Administration* guide for information about using Zenoss through a firewall.

Appendix A. Zenoss Resources

For more information and help, go to one of these Zenoss information resources on the Web.

- **Zenoss Product Guides**

  http://community.zenoss.org/community/documentation
- **Zenoss Wiki**

  http://community.zenoss.org/community/documentation/wiki
- **Zenoss FAQ**

  http://community.zenoss.org/docs/DOC-2445
- **Zenoss User Forums**

  http://community.zenoss.org/community/forums
- **Zenoss Blog**

  http://community.zenoss.org/blogs/zenossblog