EventTracker

Actionable Security Intelligence

Virtual Collection Point Configuration Guide

Publication Date: May 10, 2017

Abstract

The purpose of this document is to help users understand Virtual Collection Points (VCP) architecture and its benefits.

It also provides detailed descriptions to

- Configure Virtual Collection Points for Windows.
- Configure Windows systems to forward events through different ports.
- Configure Virtual Collection Points for SYSLOGS.
- Configure NIX systems to forward SYSLOG messages to the EventTracker Manager through different ports (default port: 514 (UDP/TCP).
- Forward incoming events as raw SYSLOG messages

Audience

Users of EventTracker monitoring large numbers of Windows and NIX systems/devices are requested to go through this document. This document will help

- Users analyze their EventTracker deployment plan and recommend the best deployment solution suitable to individual company requirements.
- Configuring your EventTracker deployment to perform at an optimal level, besides giving you deployment ideas based on the EventTracker VCP architecture.
- Garner best usage of hardware resources and bandwidth.
- Provide best performance outputs from key EventTracker Manager modules, namely, data collection, analysis and reporting.

The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Table of Contents

Virtual Collection Point

VCP stands for Virtual Collection Point. VCP is an architectural enhancement available in the EventTracker Manager using which the EventTracker can simultaneously collect event logs on multiple ports. This increases the load capacity of the product significantly while providing performance improvement to all analysis and reporting modules.

Why go for VCP?

The key benefits of using this architecture are

- Significantly faster analysis and reporting
- Best utilization of system resources and network bandwidth
- Increased load capacity

VCP is ideal for environments where many Windows and NIX systems / devices are monitored by EventTracker. Large setup is measured not only by the number of systems / devices being monitored but also the volume of events / syslogs forwarded by the monitored systems / devices.

By default, EventTracker Receiver works on

- Port 14505 (UDP/TCP) for Windows events
- Port 514 (UDP/TCP) for SYSLOGS

As a benchmark, it is recommended to opt for a VCP model deployment if EventTracker is receiving more than 250 events per second. The VCP model will balance the load and proportionately channel events / SYSLOGS coming into the EventTracker. VCP also eliminates additional hardware enhancements by optimally utilizing the single hardware/system. Last but not the least it creates significant performance improvements in the Analysis and Reporting modules of the product thereby directly saving on valuable end user time.

Implement VCP

- Identify the systems / devices that generate high volume of events / SYSLOGS baseline being 100/sec.
- Segregate those systems
- Group those systems into a manageable size
- Assign different port(s) to individual systems / devices in each group to communicate with the EventTracker Manager.

For example, consider EventTracker is monitoring 100 Windows systems. All those systems are critical and generate high volume of events that is above the baseline 500/sec. Assemble those systems into 10 groups with 10 system per group. Assign ports 14505 (default), 14515, 14525, 14535, 14545, 14555, 14565, 14575,

14585 and 14595 respectively to individual systems in each group to communicate with the EventTracker Receiver.

This way the load on Manager is balanced which ultimately enhances the performance. For detailed instructions go to appropriate sections.

Virtual Collection Points Architecture

Virtual Collection Points (VCP) enable the existing receiver to behave like a collection master without having the physical Collection Points installed. The Existing Collection Point (CP-CM model) requires physically organized Collection Points reporting to a Collection Master. CP-CM model requires several hardware facilities and a large degree of deployment difficulty.

VCP provides the solution to break down the huge volume of input events using the existing set up with minimal configuration changes, thus helps to process the received data in a short time at the reporting end.

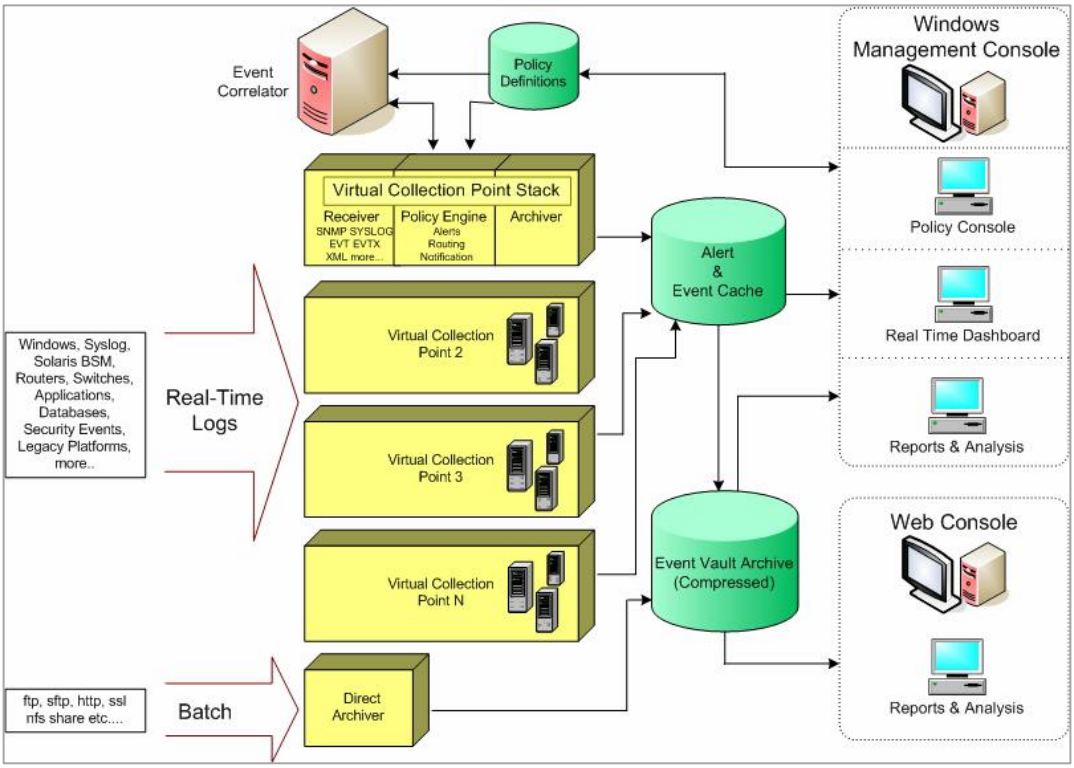

Figure 1

EventTracker behaves the same way with multiple instances of its core components. VCP should be configured in such a way that the single instance of EventTracker takes care of a group of systems.

Each EventTracker Receiver instance will receive events from their respective group of systems and maintain the respective cache.

Virtual Collection Points for SYSLOGS

EventTracker Syslog Receiver can be configured to listen on 10 UDP/TCP ports for Unix/Linux/Solaris Syslogs.

ET Modules	Suggested Trap Ports
You ought to add ports to the **Firewall exceptions** list.	
EventTracker Syslog Receivers (Incoming)	Default: 514 (UDP/TCP) for Syslogs. You can add max 10 ports for Syslogs

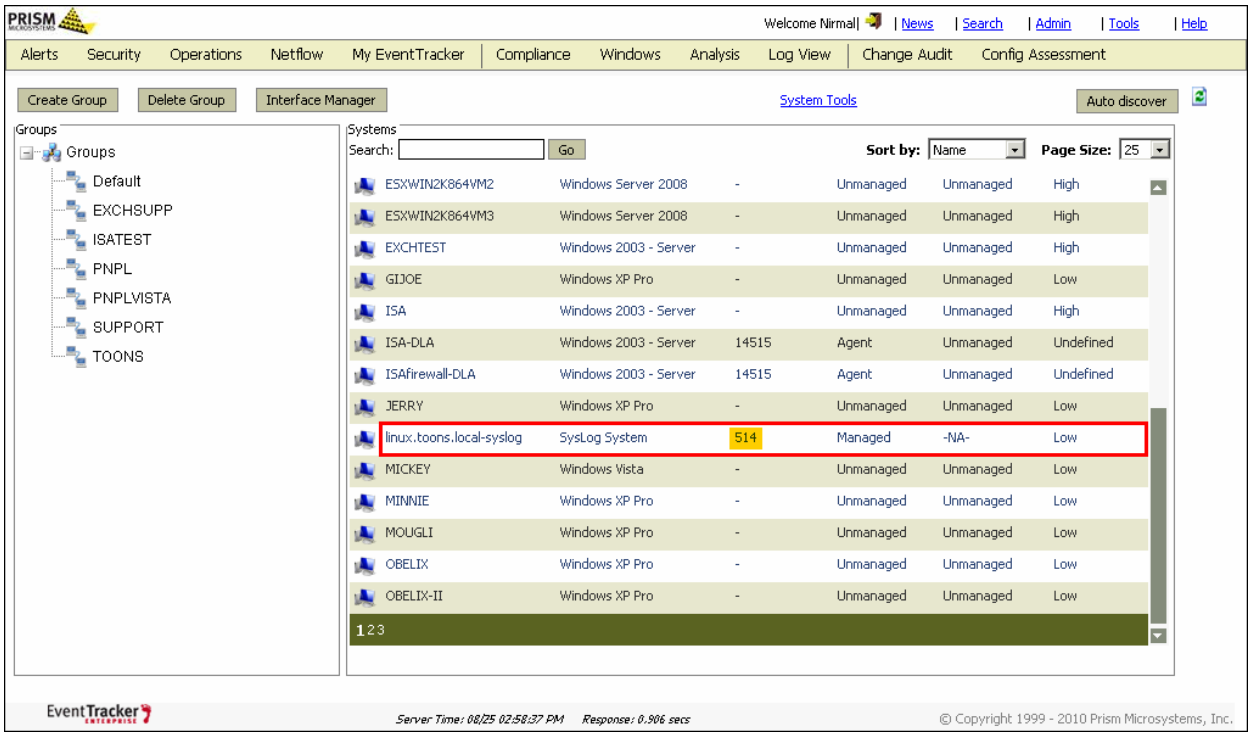

Figure 2

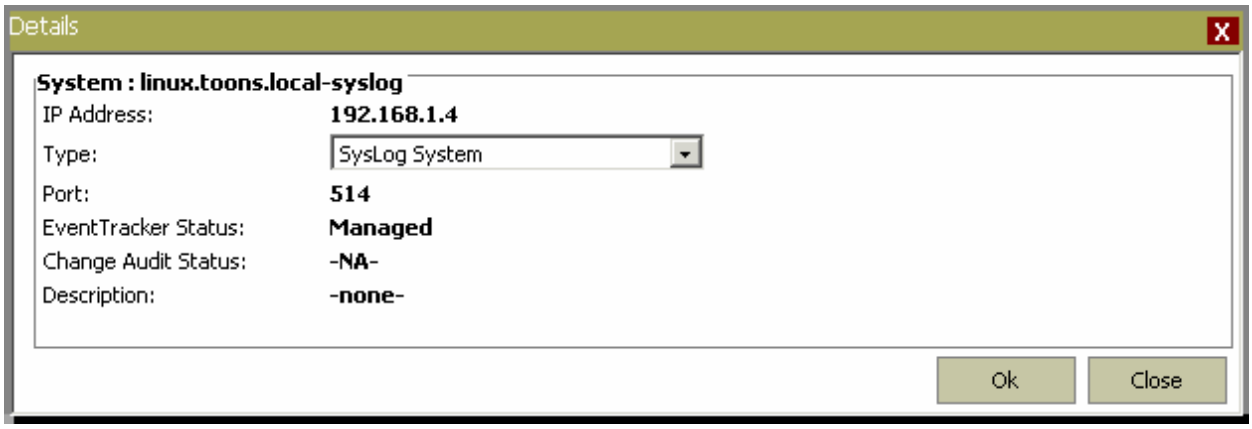

Figure 3

Configure VCP for SYSLOGS

1. Log on to EventTracker.
2. Click the **Admin** hyperlink at the upper-right corner.
3. Click **Manager**, click the **Syslog / Virtual Collection Point** tab.

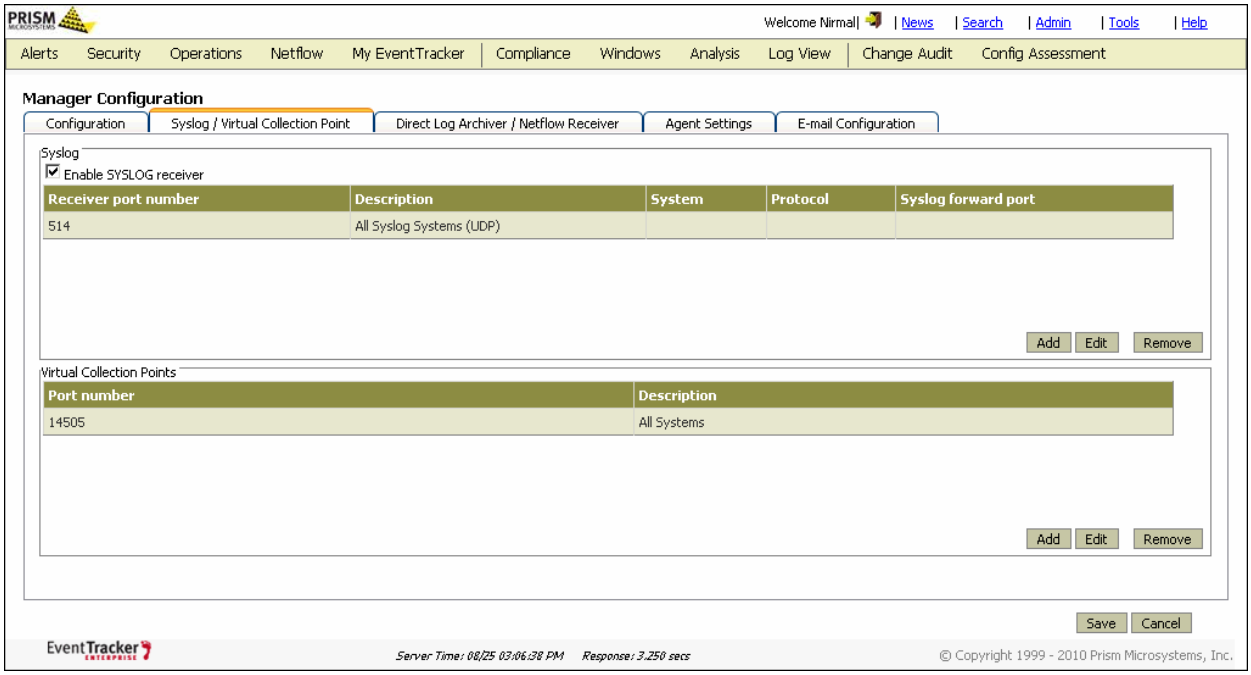

Figure 4

4. Click **Add** under Syslog.

   EventTracker displays the Syslog Receiver Port window.

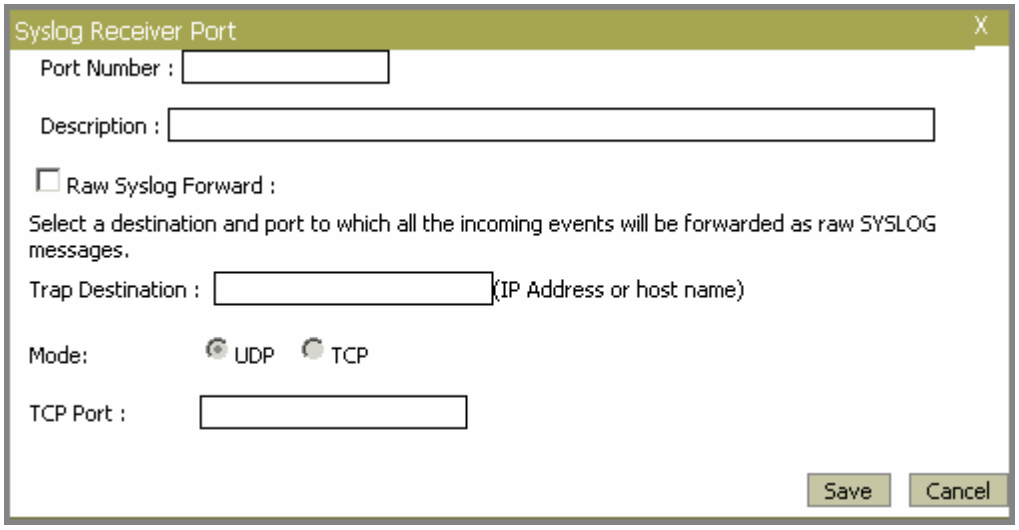

Figure 5

5. Type the UDP / TCP Port details in the **Port Number** and **Description** fields.
   This pair should be unique. Before providing the port details, refer the man pages / documents to confirm that the ports are not used by any other daemons / processes. Move the mouse pointer over the Port Number field, EventTracker displays the well-known ports in a tooltip.
6. Click **Save**.
   EventTracker adds the newly configured ports.

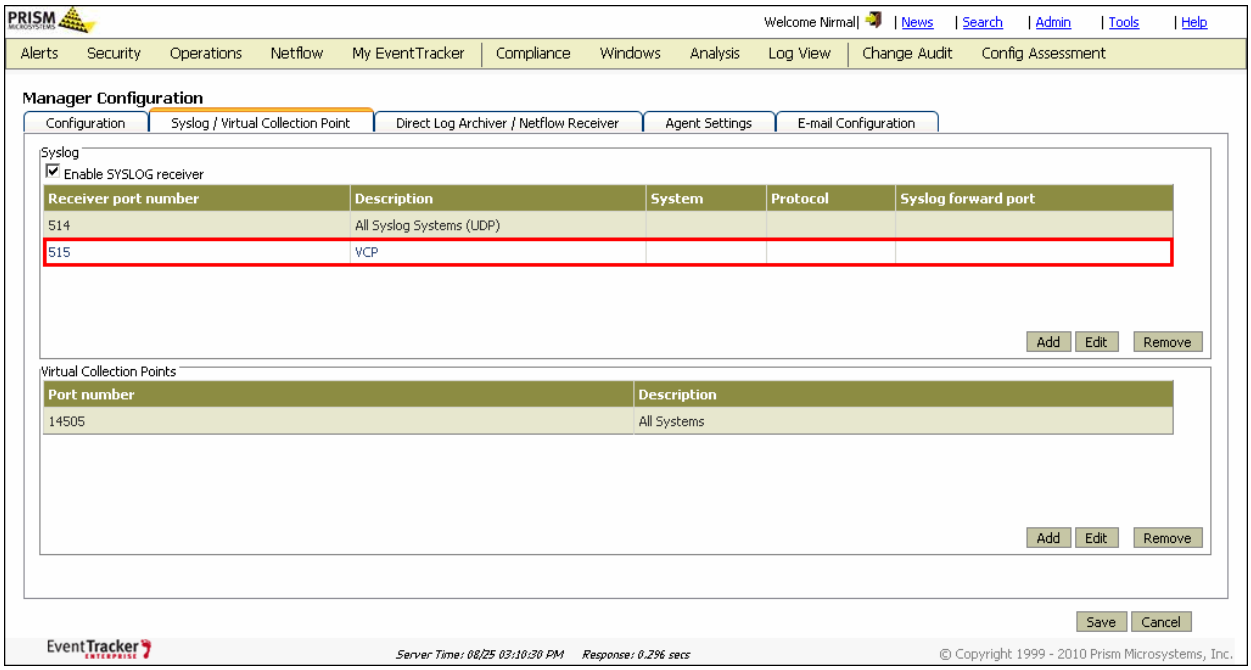

Figure 6

7. Click **Save**.
8. Add the ports to the Firewall exceptions list.
   EventTracker Manager listens on two ports 514/UDP, which is the default and 515/UDP, which is user defined.
   Group and Configure the NIX systems to forward SYSLOGS through port 514 and 515. For example, if there are 10 NIX systems in your environment, configure 5 systems to forward SYSLOGS through 514/UDP and 5 systems through 515/UDP. This enhances the performance of EventTracker Receiver.

Forward Raw Syslog Messages

This option helps to forward received Syslog messages in raw format i.e. forwarded in the same format as it is received from the source to a specified destination.

1. Select the **Raw Syslog Forward** check box.

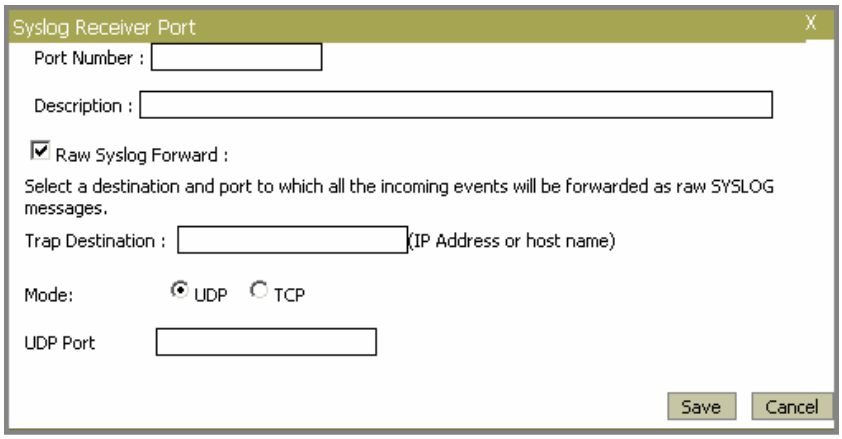

Figure 7

2. Type the name or IP address of the destination in the **Trap Destination** field.
3. Select an appropriate **Mode** of transport.
4. Enter/select an appropriate port with respect to the mode chosen.
5. Click **Save**.

Configure SYSLOG Daemon

Configure SYSLOG Port

1. Log in as root.

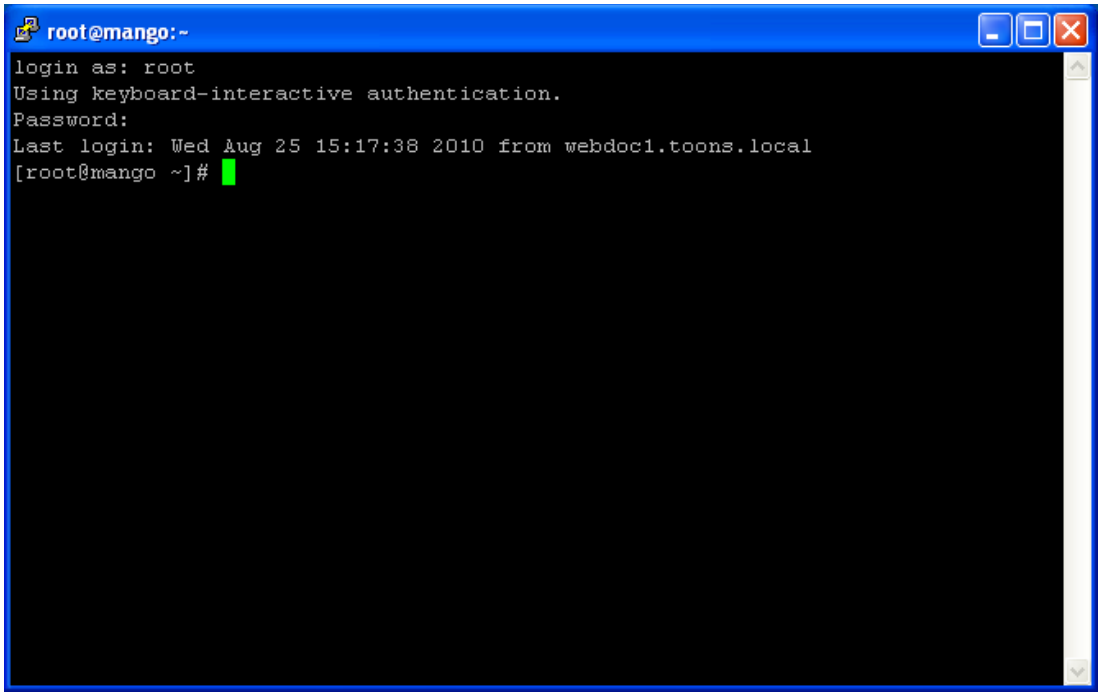

Figure 8

2. Type **cd /etc** at the command prompt.

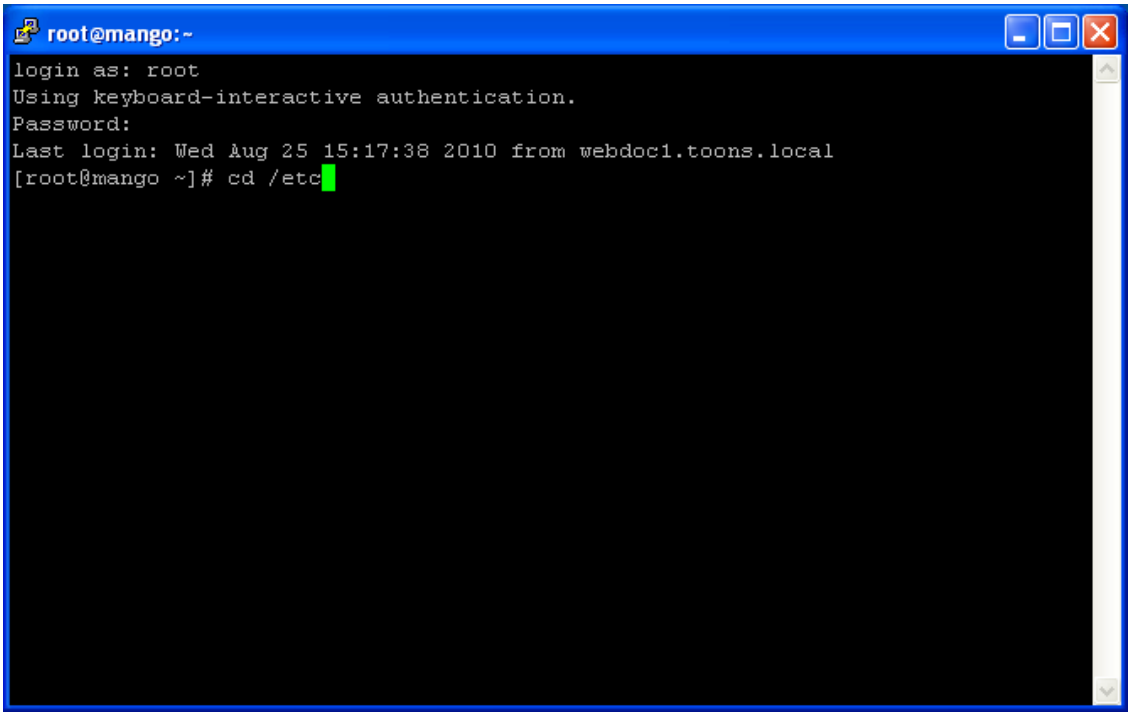

Figure 9

3. Press **ENTER** on your keyboard.
4. Type **vi services**.

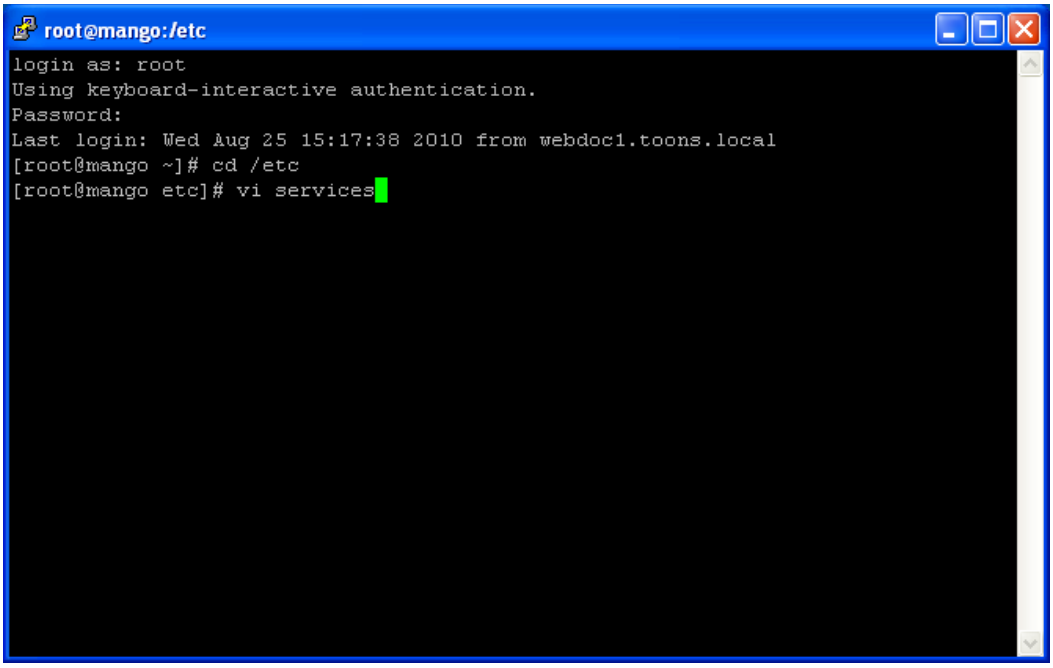

Figure 10

5. Press **ENTER** on your keyboard.
6. Press **i** on your keyboard to insert / edit the syslog port.
   For example: **syslog 514/udp** as **syslog 515/udp**.

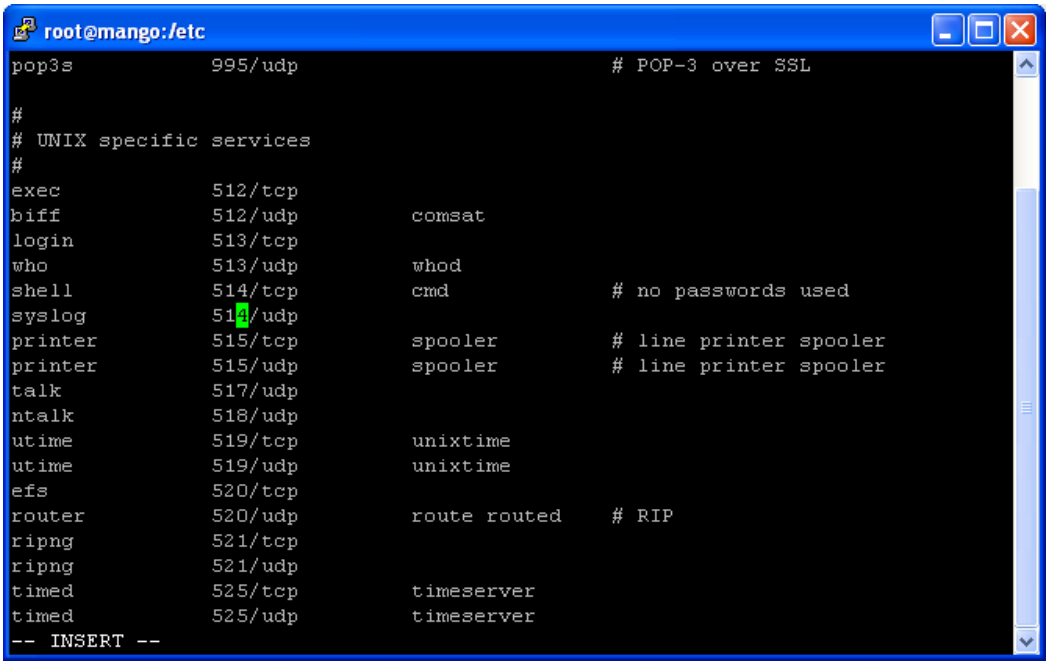

Figure 11

7. Press **ESC** on your keyboard.
8. Type **:wq** on your keyboard to save the changes.

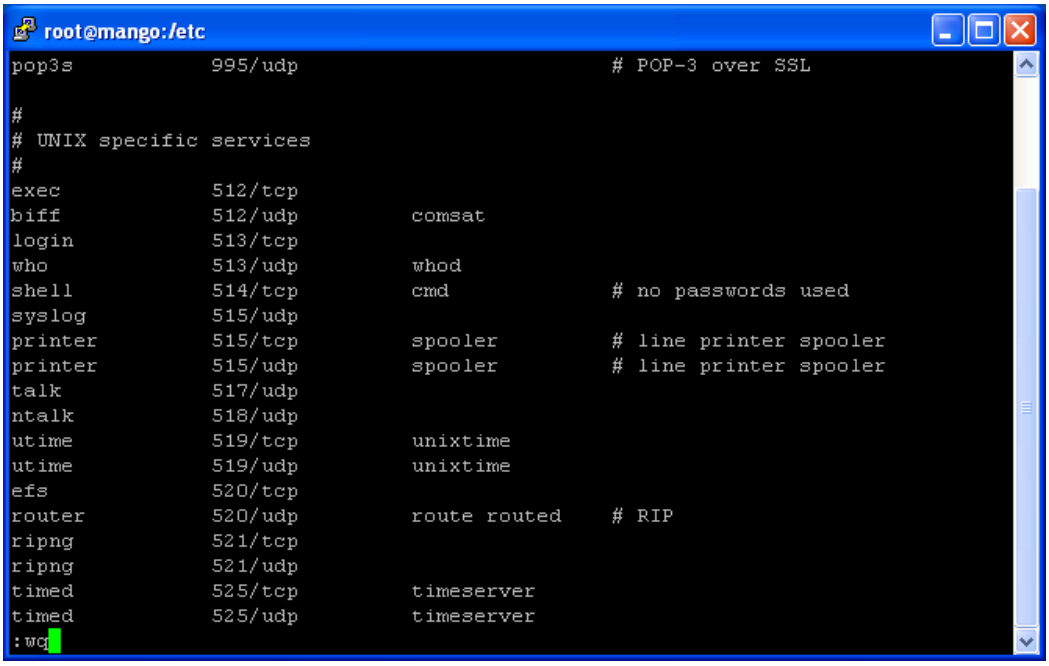

Figure 12

9. Press **ENTER** on your keyboard.

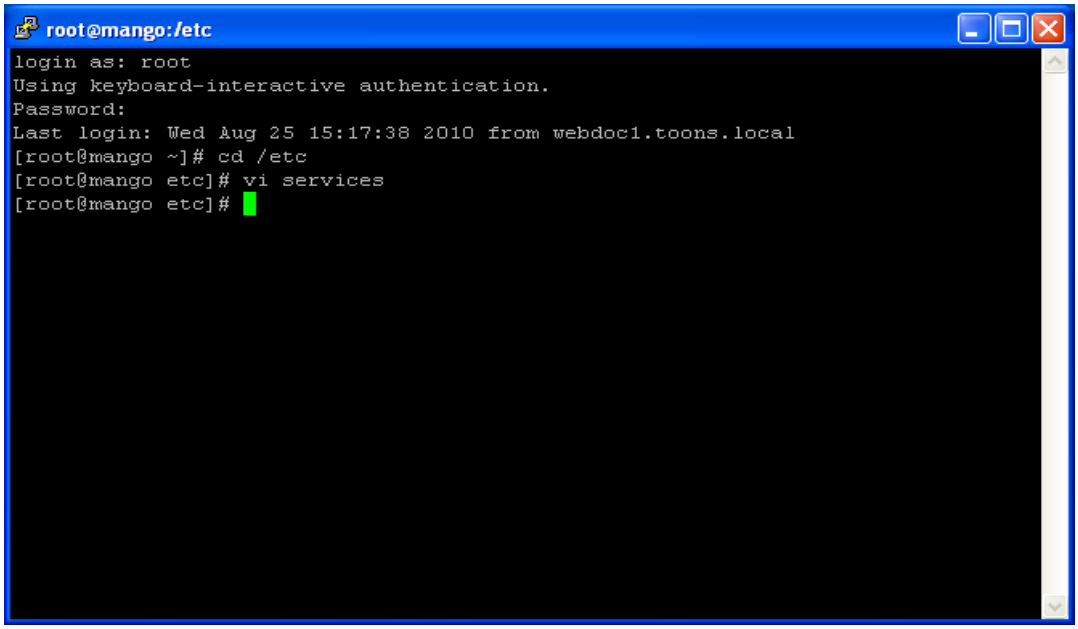

Figure 13

10. Type **./init.d/syslog restart** to restart the syslog daemon.

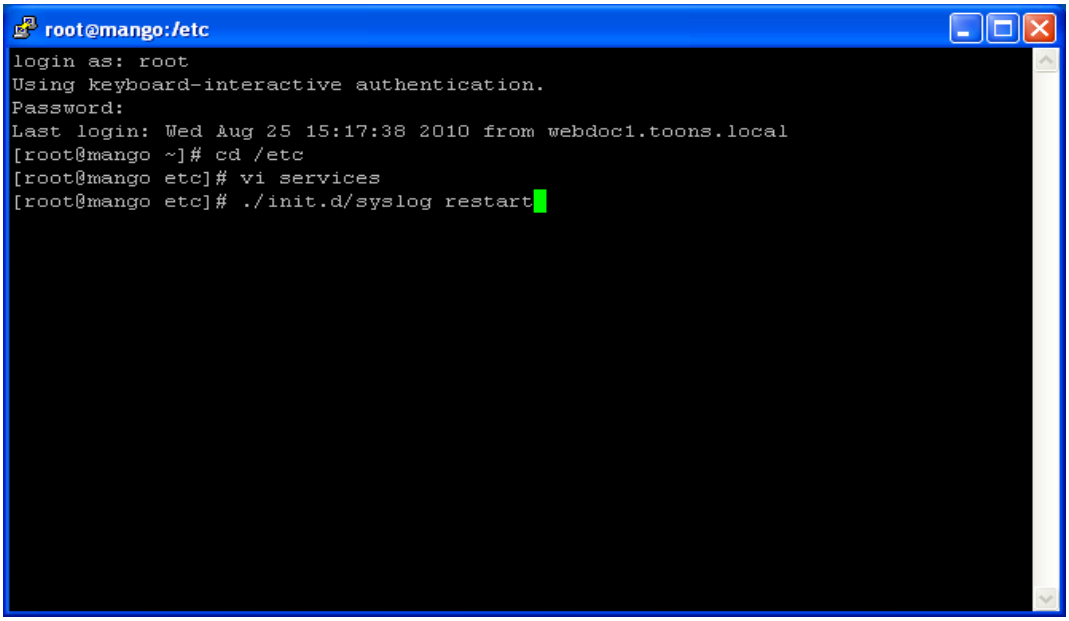

Figure 14

11. Press **ENTER** on your keyboard.

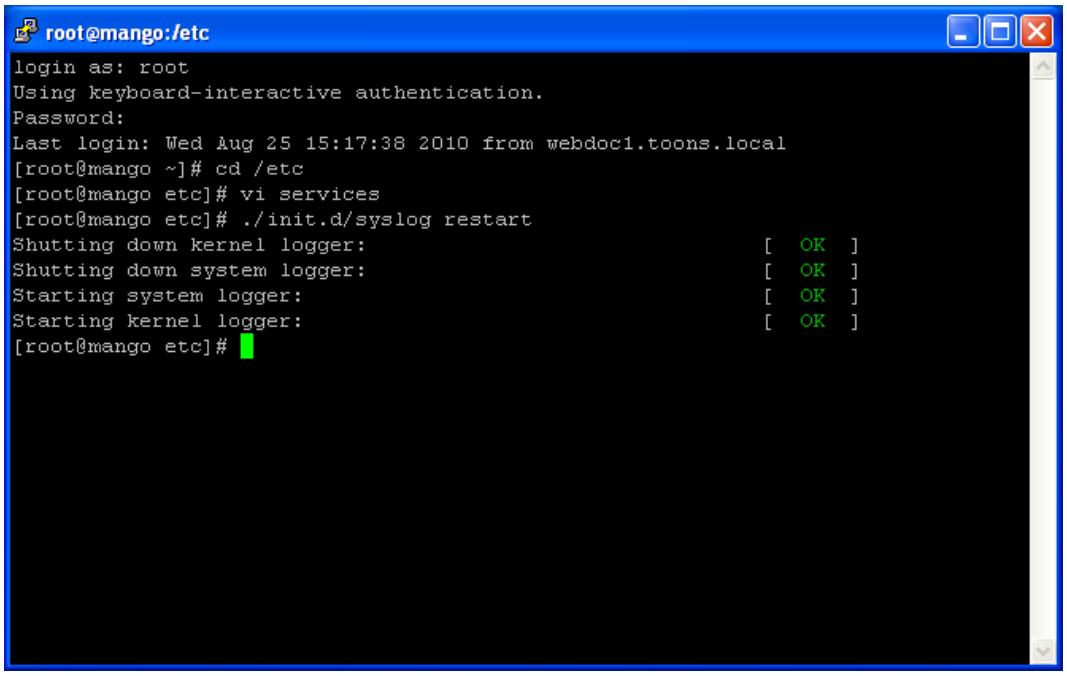

Figure 15

Edit SYSLOG Configuration

1. Type **vi syslog.conf** at the command prompt.

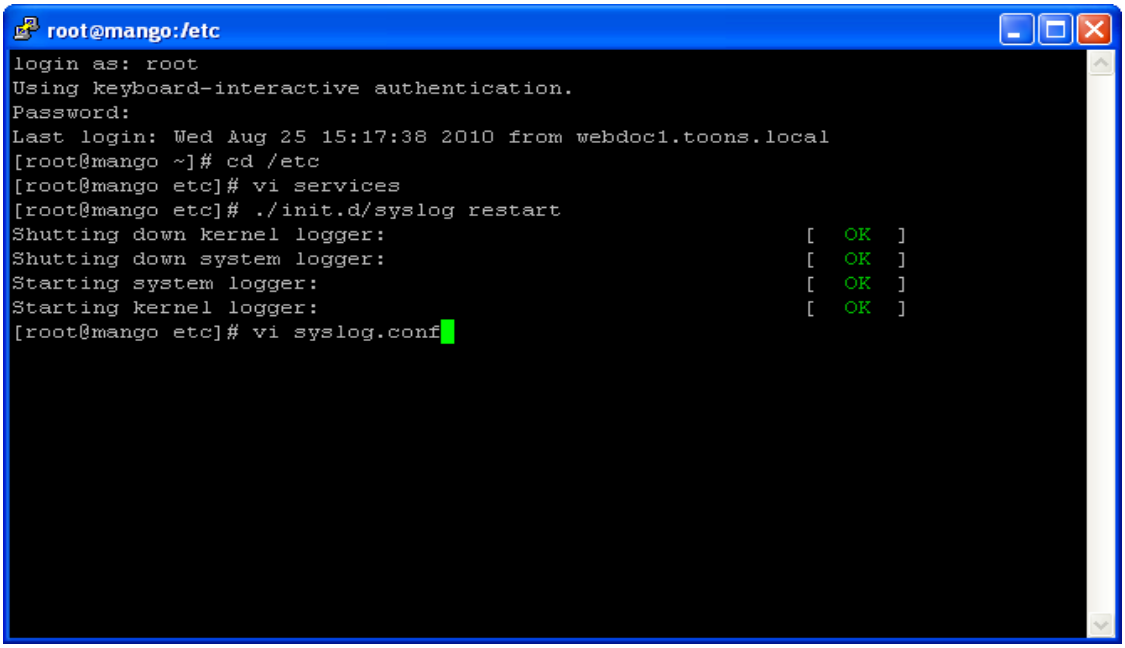

Figure 16

2. Press **ENTER** on your keyboard.

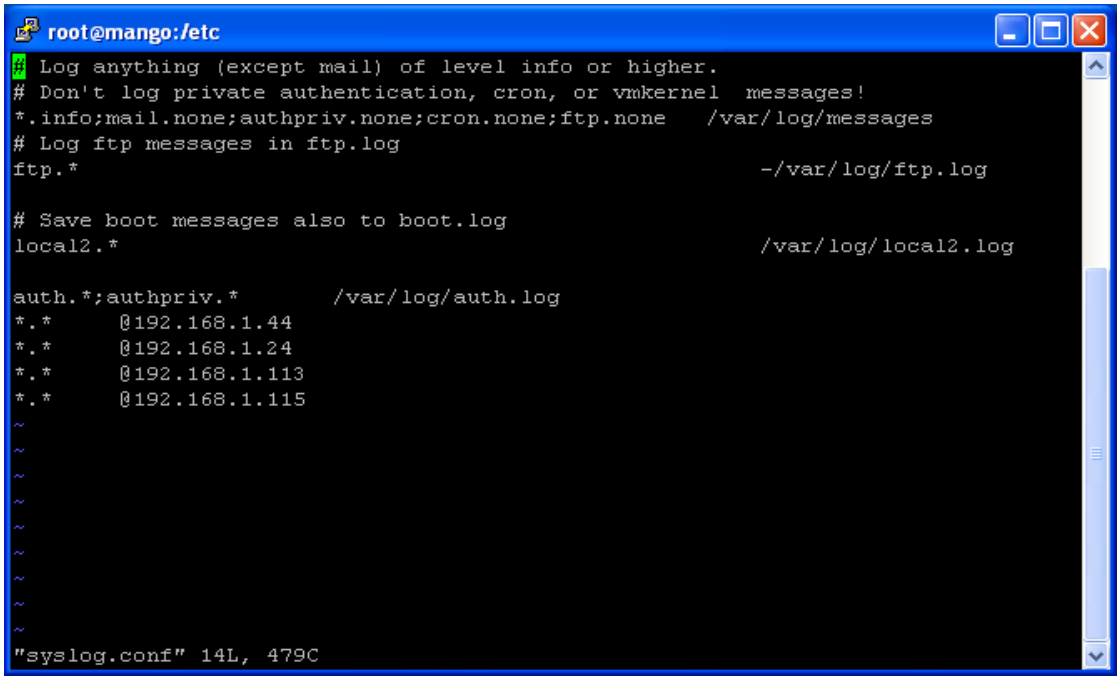

Figure 17

3. Press **I** on your keyboard to insert.
4. Type ***.* @IP address**

- *.* @192.168.1.19
- Type “asterisk’ followed by a “period’ and an “asterisk’
- Press **TAB** on your keyboard.
- Type “at the rate” symbol followed by IP address of the EventTracker server.
- *.* signifies all Syslog messages will be forwarded to the destination computer.

5. Press **ESC** on your keyboard.
6. Type **:wq** to save the changes.
7. Press **ENTER** on your keyboard.
8. Type **./init.d/syslog restart** to restart the syslog daemon.
9. Click **ENTER** on your keyboard.

Verification

Open the Task Manager to verify EventTracker Receiver spawned a new process EtReceiver-S-515.exe.

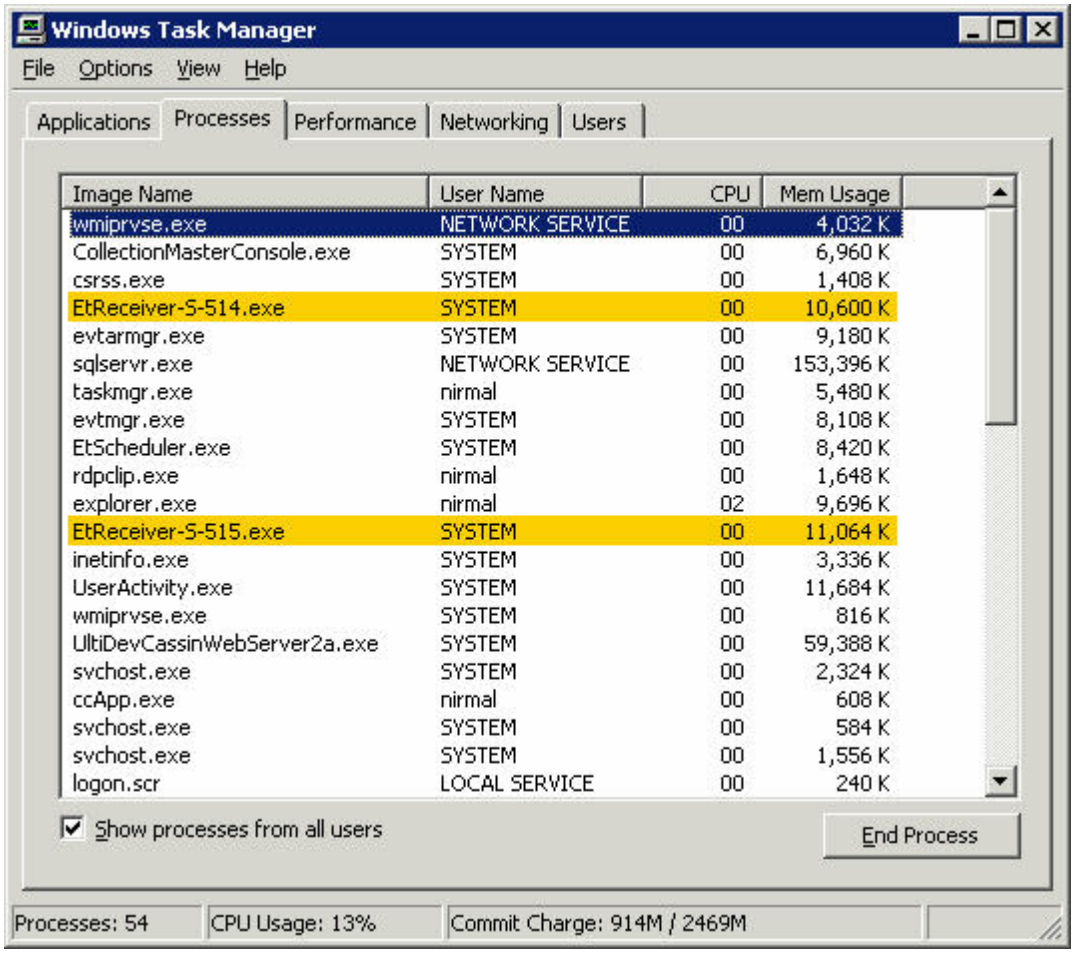

Figure 18

1. Open the System Manager to verify EventTracker Receiver receives SYSLOG messages at the configured port 515/UDP.

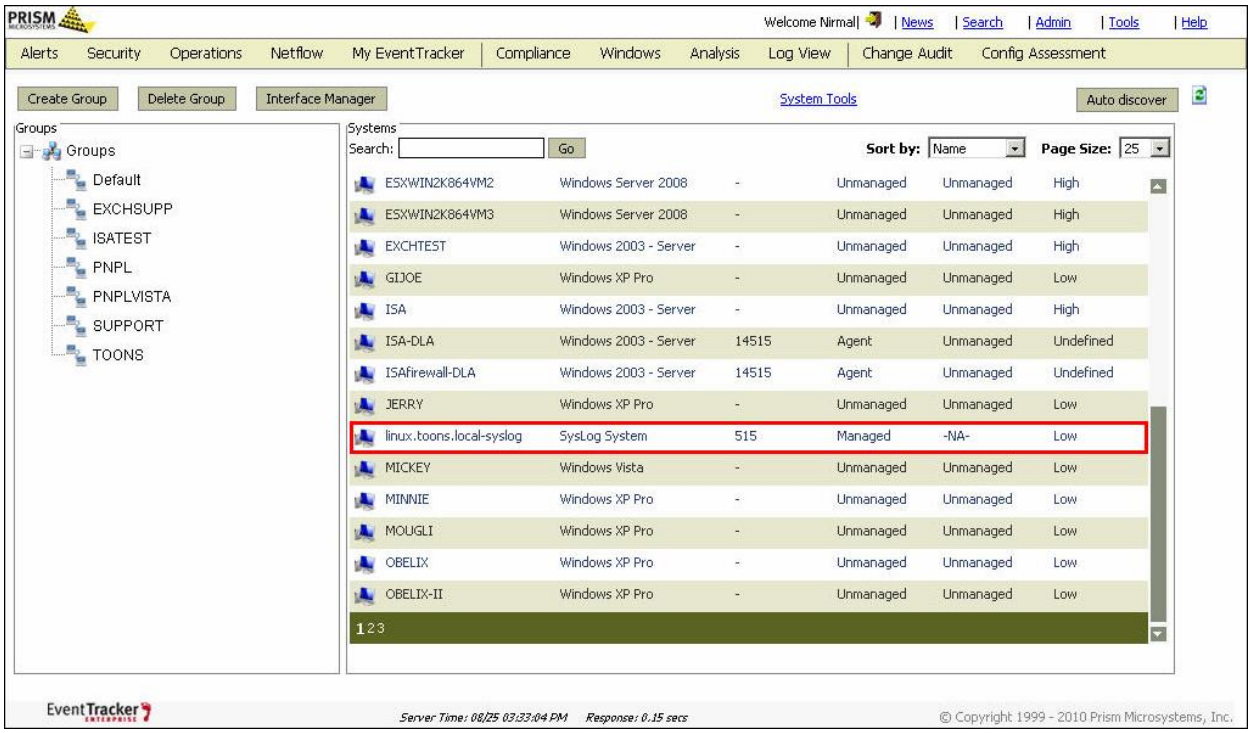

Figure 19

2. Click **Log View** on the EventTracker home page.
3. Select the Syslog system from the System(s) drop-down list.

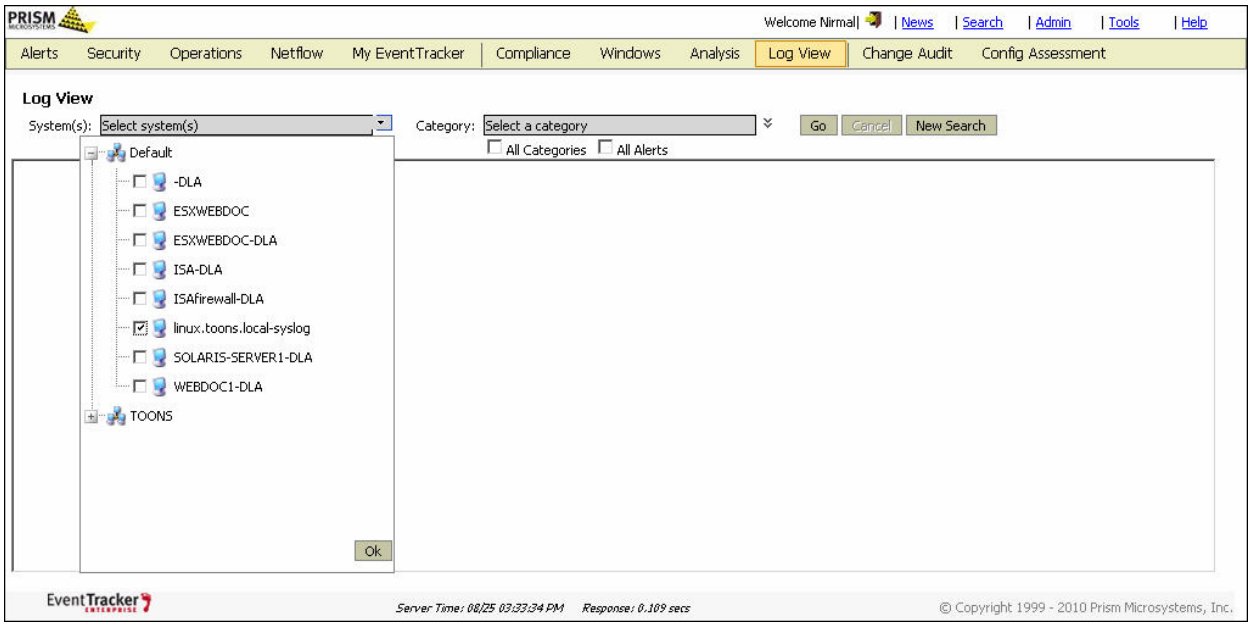

Figure 20

4. Select the **Syslog** -> ***All Syslog events** Category from the Category drop-down list.

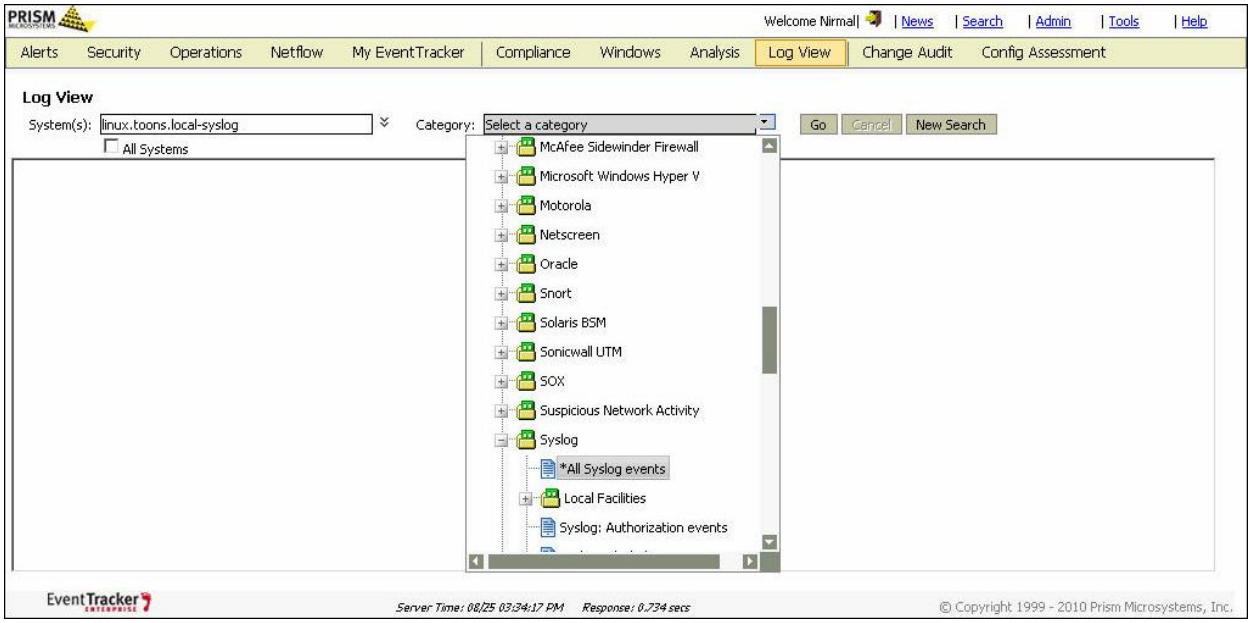

Figure 21

5. Click **Go**.

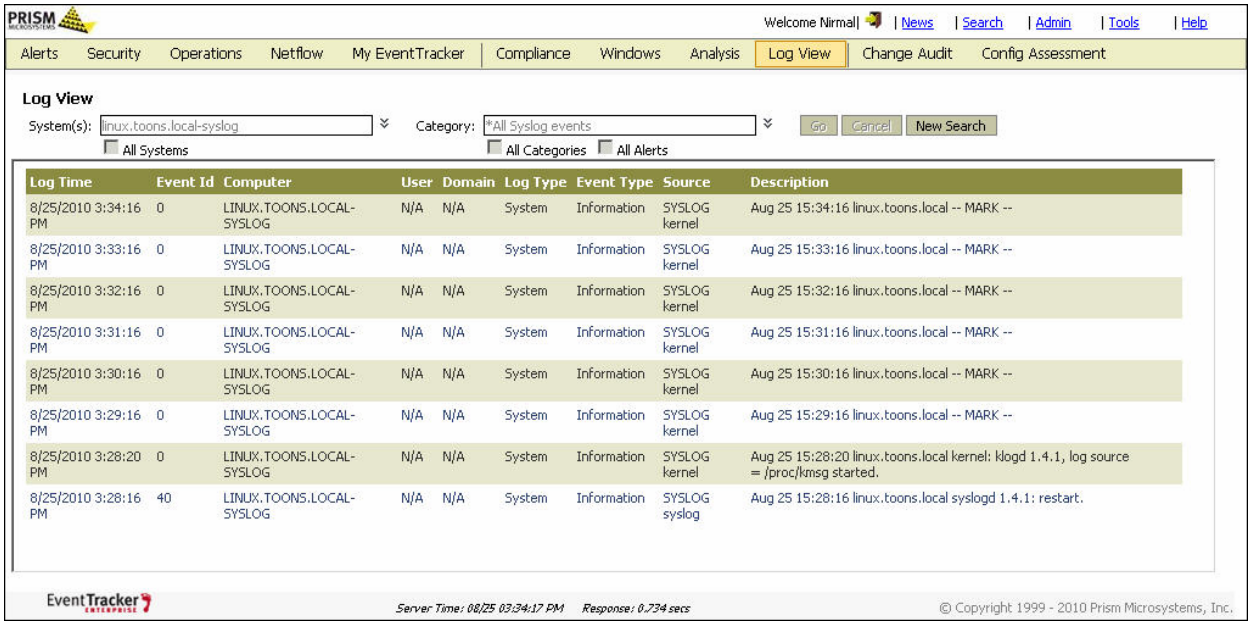

Figure 22

Virtual Collection Points for Windows

EventTracker Receiver can be configured to listen on 10 ports for Windows.

ET Modules	Suggested Trap Ports
You ought to add ports to the **Firewall exceptions** list.	
EventTracker Syslog Receivers (Incoming)	14505 default port.14515, 14525, 14535, 14545, 14555, 14565, 14575, 14585, 14595 (max 10 ports).

Configure Virtual Collection Points for Windows

1. Log on to EventTracker.
2. Click the **Admin** hyperlink at the upper-right corner.
3. Click **Manager** on the Control Panel.
4. Click the **Syslog / Virtual Collection Point** tab.
5. Click **Add** under **Virtual Collection Points**.
   EventTracker displays the Receiver Port pop-up window.
6. Type the port number and description in the **Port Number** and **Description** fields.
   Before typing the port numbers, refer the man pages / documents to confirm that the ports are not used by any other services / processes.

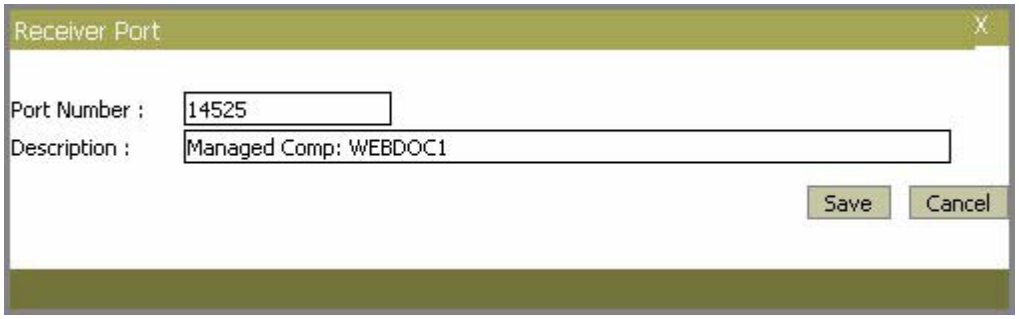

Figure 23

7. Click **Save**.
   EventTracker adds the newly configured ports.

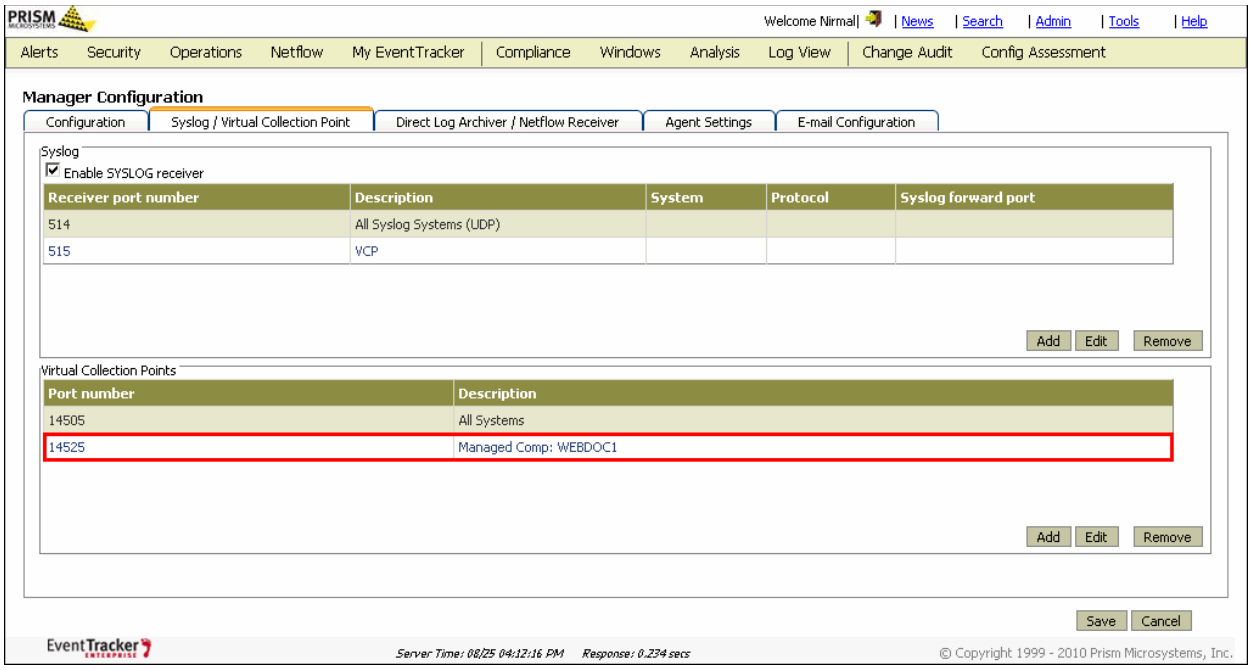

Figure 24

8. Click **Save** on the Manager Configuration page.
9. Add the ports to the Firewall exceptions list.
   EventTracker Manager listens on two ports 14505, which is the default and 14525, which is user defined.

Configure EventTracker Agents to Forward Events on Different Ports

Group and Configure the Windows systems to forward events through port 14505 and 14525. For example, if there are 10 Windows systems in your environment, configure 5 systems to forward events through 14505 and 5 systems through 14515. This enhances the performance of EventTracker Receiver.

- Open the etagentconfig.ini of the remote system.
  For example, **etaconfig.ini.WEBDOC1** from the EventTracker installation folder…\Program Files\Prism Microsystems\EventTracker\AgentConfig

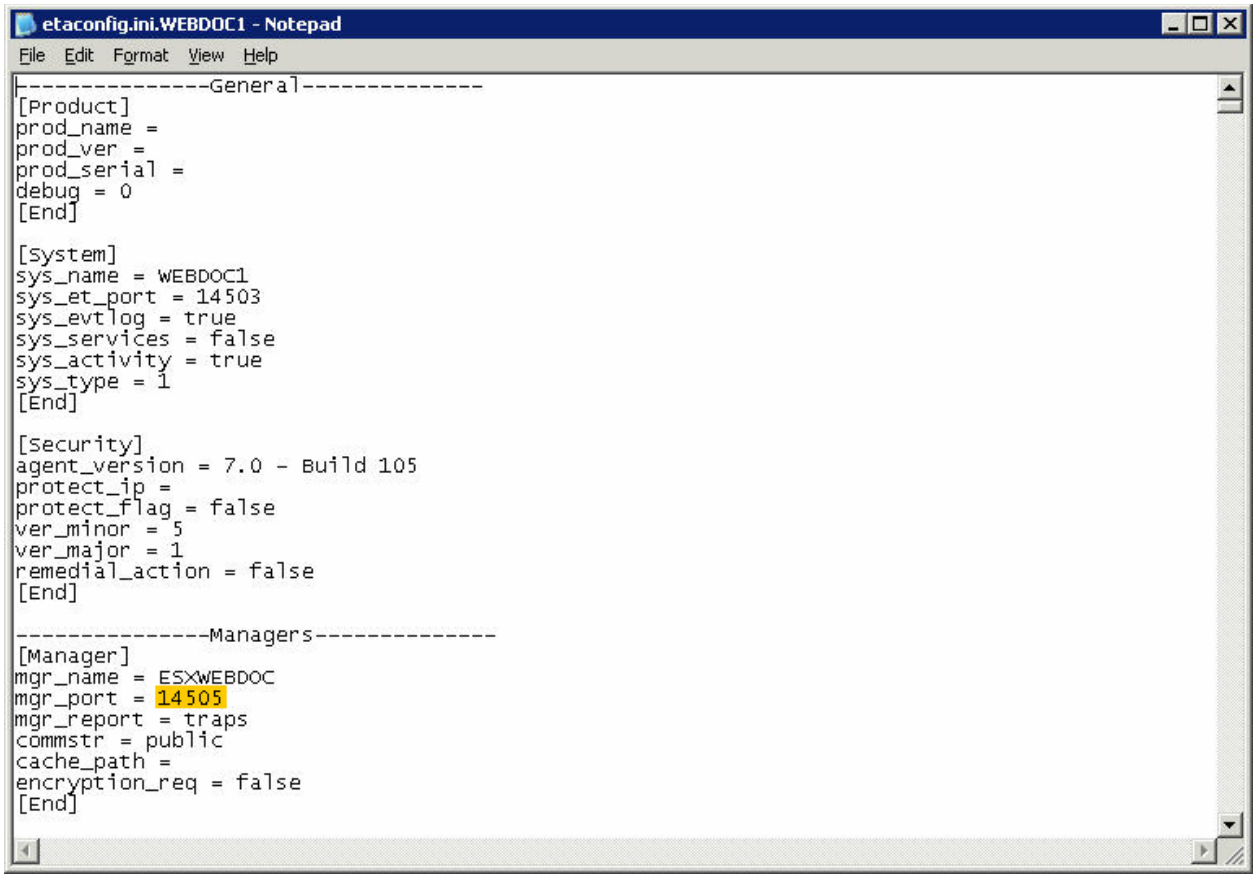

Figure 25

It is clear from figure above, by default, remote agent communicates with the Manager through port 14505. When you change the port number through Agent Configuration window, EventTracker updates this field with the new value.

1. Double-click **EventTracker Agent Configuration** on the desktop Control Panel.
2. Select a managed system from the **Select Systems** drop-down list.

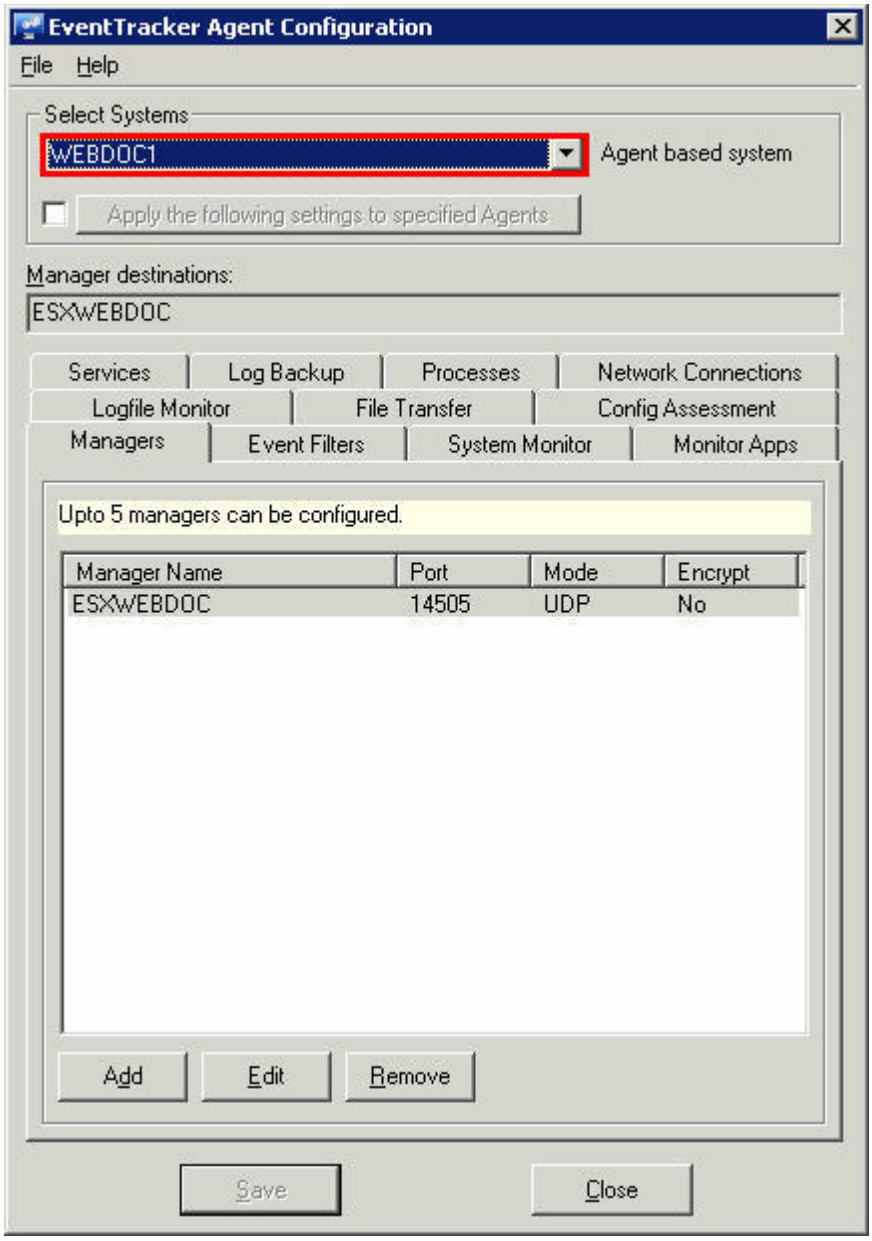

Figure 26

3. Select the Manager Name and then click **Edit**.
   EventTracker displays the Edit Destination window.

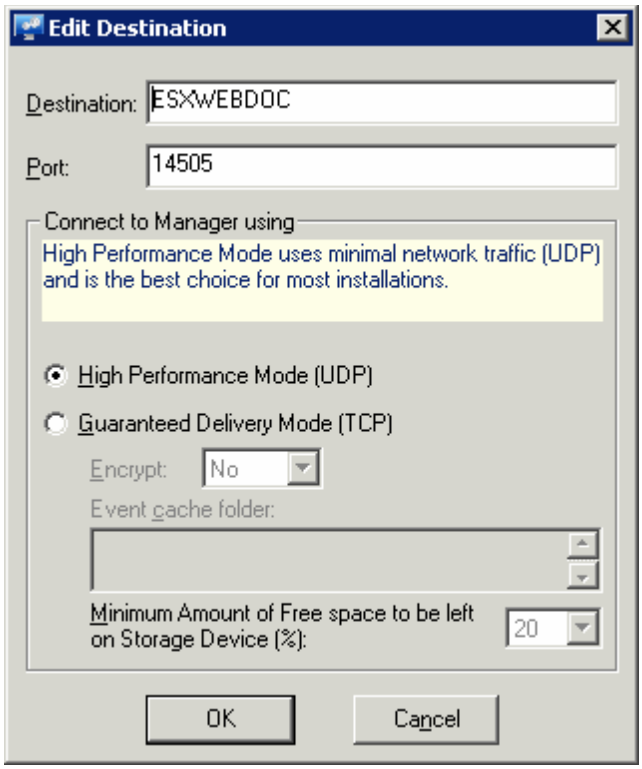

Figure 27

4. Type the port number as 14525 in the **Port** field and then click **OK**. EventTracker updates the port number.

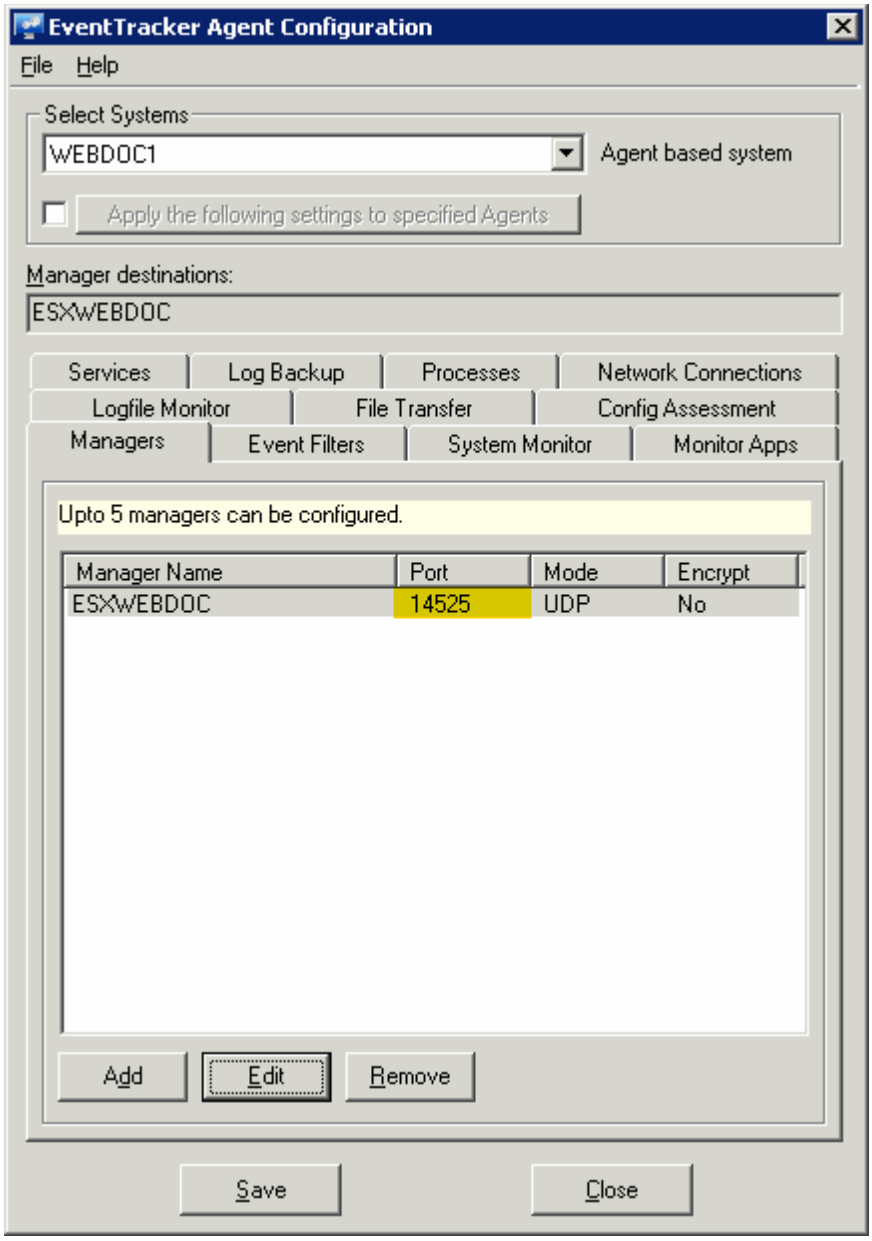

Figure 28

5. Click **Save** and then click **Close**.
   Open etaconfig.ini.WEBDOC1 from the location mentioned earlier to check if EventTracker has updated the mgr_port with new port number.

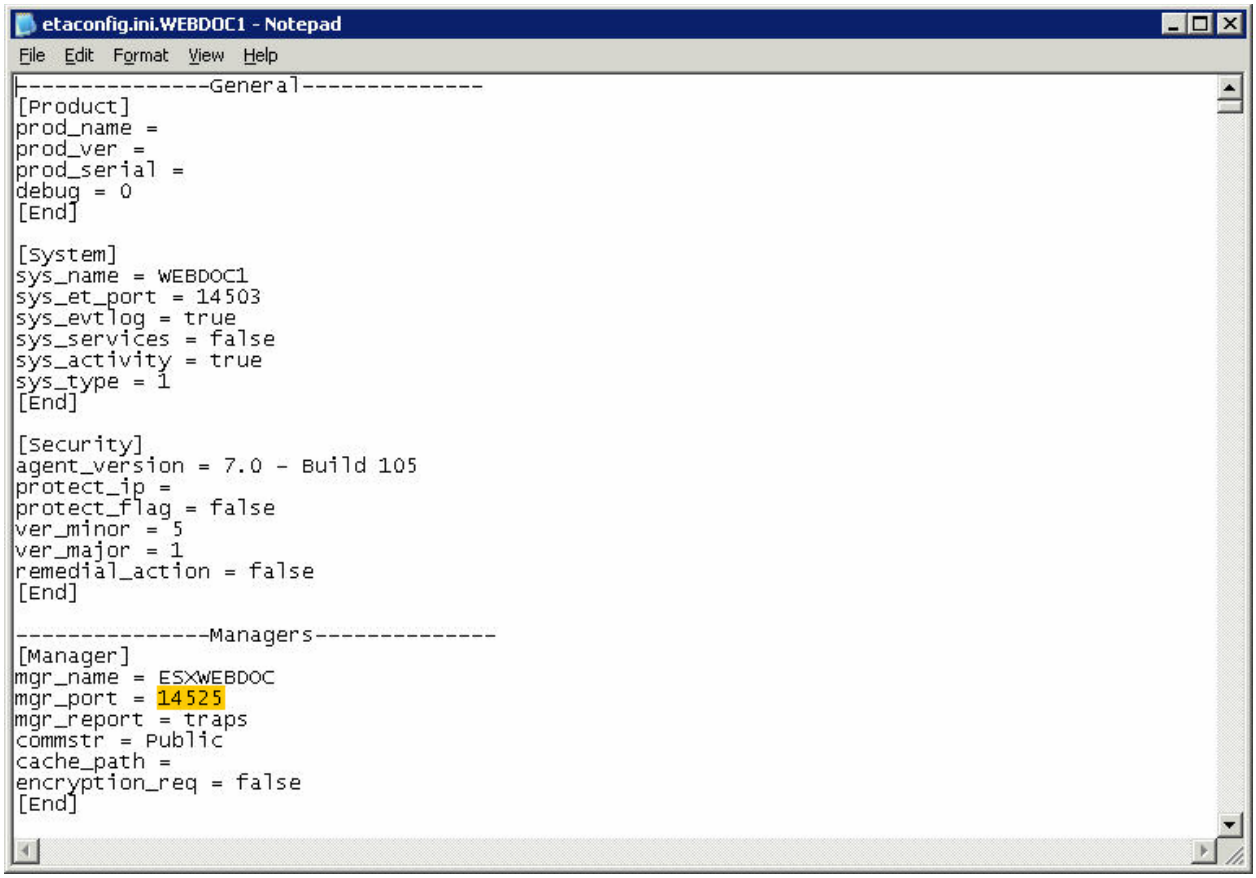

Figure 29

Verification

- Open the Task Manager to verify EventTracker Receiver spawned a new process EtReceiver-W-14525.exe.

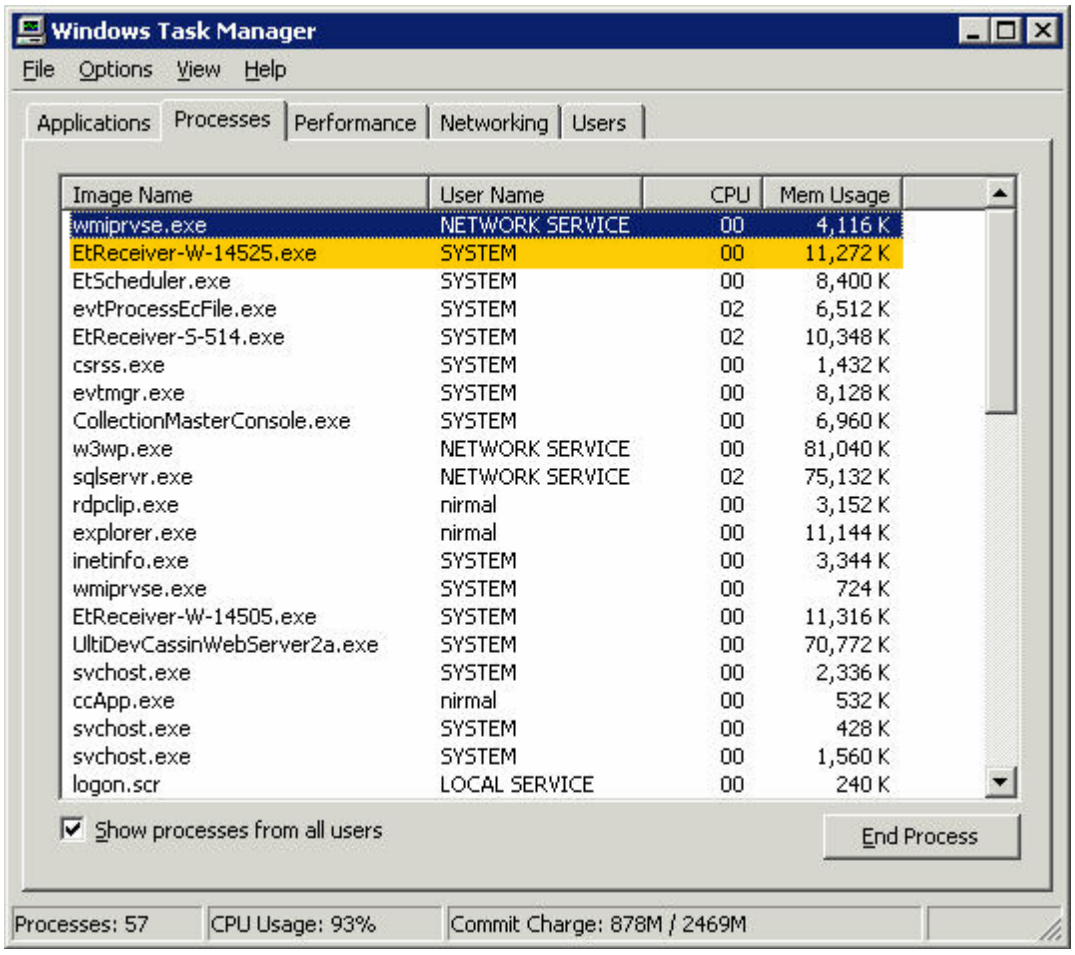

Figure 30

- Open the System Manager to verify EventTracker Receiver receives Windows events at the configured port 14525.

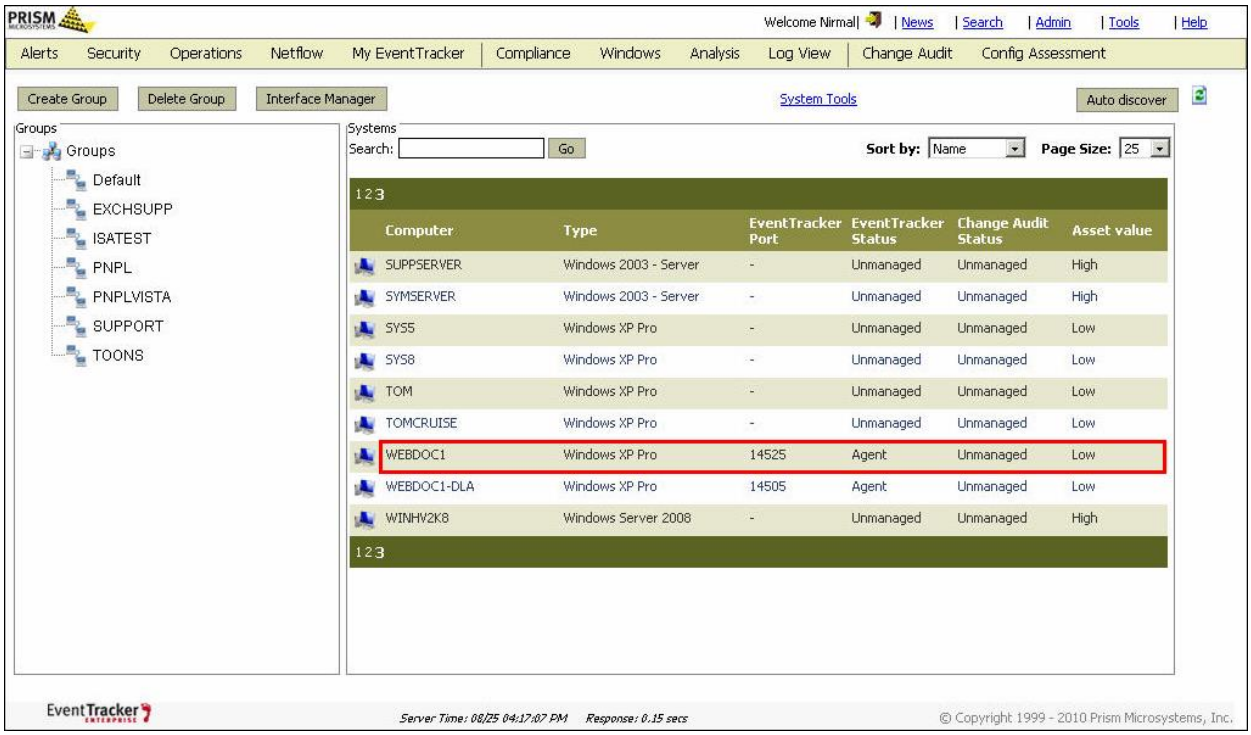

Figure 31

Summary

Success of any application depends on performance optimization and load balancing, EventTracker is no exception.

Implementing Virtual Collection Points will give the following benefits

- Significantly faster analysis and reporting
- Best utilization of system resources and network bandwidth
- Increased load capacity
- Enhances the overall performance of EventTracker.