Table of Contents

1 Document Overview

Author: NETIKUS.NET ltd
Date: 4th October 2006
Revision: 1.00

Documentation for the Ubuntu-based Linux Virtual Machine ESONUBU

Title	Documentation for the Ubuntu-based Linux Virtual Machine ESONUBU
Summary	This document explains how to use the Ubuntu-based ESONUBU virtual machine, which comes with a pre configured MySQL database that works out of the box with EventSentry.
Benefits	Allows EventSentry users (both trial and registered users) to take advantage of all EventSentry database-based features, without having to setup a database server and configuring the EventSentry database.
Required Software	VMWare Player (free), VMWare Workstation or VMWare Server (free)
Hardware	Not applicable
Skill Level	Beginner - Intermediate
Skills Recommended	- Basic understanding of Windows NT, 2000, 2003 or XP - Basic networking skills - Linux skills are recommended but not required
Download	http://www.eventsentry.com (accessible to EventSentry evaluation users only)

2 Document Details

Overview	This document explains how to use the ESONUBU virtual machine, which comes with a pre configured virtual machine that runs the MySQL database on Ubuntu, a Debian-based Linux distribution.
Additional Information	This virtual machine is not intended to be a permanent solution for the EventSentry database, instead we recommend that install any of the supported EventSentry databases (please see the documentation) as soon as you decide to use EventSentry in your production environment. You may use this virtual machine on a VMWare server, if you are familiar with the Linux operating system and have sufficient processing power available. The ESONUBU virtual machine also includes Nessus, a vulnerability scanner whose output files can be imported into the EventSentry database and used with the EventSentry web reports.
EventSentry	EventSentry is an event log, system and network monitoring suite that is available both as a commercial edition ("EventSentry") and a freeware edition ("EventSentry Light"). You will need either the full or trial edition of EventSentry for this guide, the light edition is not sufficient as it does not support any database-related features.
What's included?	MySQL Server for Linux MySQL Administrator Nessus Samba All EventSentry documentation in PDF format
Why?	This guide was written to help current and future EventSentry customers to become familiar with the provided virtual machine and get up to speed with EventSentry as quickly as possible.

3 EventSentry Setup

3.1 Download & Installation

Downloading EventSentry

You can skip this chapter if you have already downloaded EventSentry. If you have already purchased EventSentry then you can download the latest version from http://www.eventsentry.com/downloads_downloadnow.php.

You can download a full evaluation copy of EventSentry (will run for 45 days, extensions available) from http://www.eventsentry.com/downloads_downloadtrial.php.

You will not be able to use EventSentry Light for the functionality described in this guide, as EventSentry Light does not support any database-related features.

Installing EventSentry

After downloading the latest version, simply run the setup (**eventsentry_setup.exe**). During setup make sure that you enter the correct email (SMTP) information and select at least the "Event Log Agent" and the "Management Application". All other features are optional and can be added at a later time by running the setup again.

If you would like to record backup activity to a database then you need to make sure that you select "Database Features" and the appropriate sub feature (when using MS Access or MS SQL Server).

Testing EventSentry

After setup has completed EventSentry should automatically be configured to email you all errors, warnings and audit failures via email. To make sure that EventSentry and the email notification (aka as "target") are setup correctly, open the EventSentry management application and click on "Test Agent" in the "Service Control" container. You should receive an email with two test entries within the next minute.

Please refer to the EventSentry manual or the EventSentry knowledge base if you are experiencing difficulties setting up EventSentry.

4 Configuration

ESONUBU is designed to work out of the box on any network that supports DHCP. The following chapters outline the default configuration (default passwords, installed software) and what you need to do in order to make configuration changes, e.g. when not using DHCP.

Usernames and Passwords
Review the default usernames configured in ESONUBU.

Networking
Read this chapter if you need to view or change the network (TCP/IP) configuration.

Installed Software
What software, relevant to EventSentry and its database functionality, is installed.

4.1 Usernames and Passwords

The following usernames and passwords have been assigned to ESONUBU. You are **highly encouraged** to change these passwords if you plan on using this virtual machine in a production environment.

Type / Application	Username	Password
Linux (OS)	root	`WeLoveMonitoring!`
Linux (OS)	eventsentry	`WeLoveMonitoring!`
MySQL	root	`ItStoresItAll?`
MySQL	eventsentry_svc	`ForTheAgents!`
MySQL	eventsentry_web	`ForIISWeb!`
Nessus	eventsentry	`Nessusscans.`

You cannot login to the console using the **root** user. Instead, you will have to log in using the **eventsentry** user account. You will be prompted for the root password (which, by default, is the same) whenever you attempt to make configuration changes.

Again, make sure that you change all passwords if you plan on using this virtual machine in a production environment.

4.2 Network

The network interface is configured to obtained an IP address using DHCP. If your network does not support DHCP, then you will need to manually assign an IP address to ESONUBU.

Verifying the currently active IP address

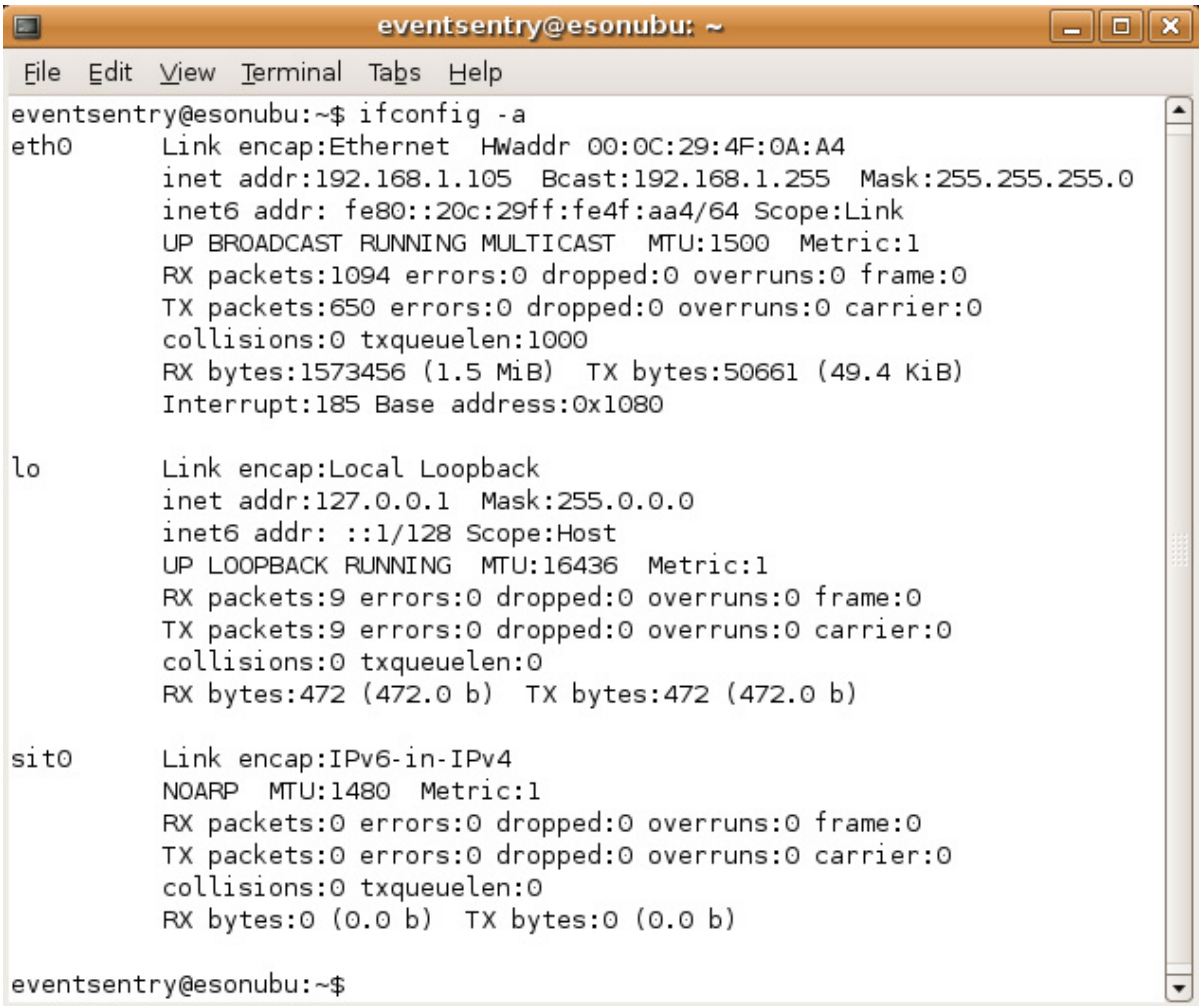
You can either view the current IP address using the command-line, or the **Network Tools** application.

Command-Line

First click the terminal icon, which is the first icon in the toolbar next to "System". Then, maximize the window and enter the following command:

```
ifconfig -a
```

which will yield output similar to the one shown below:

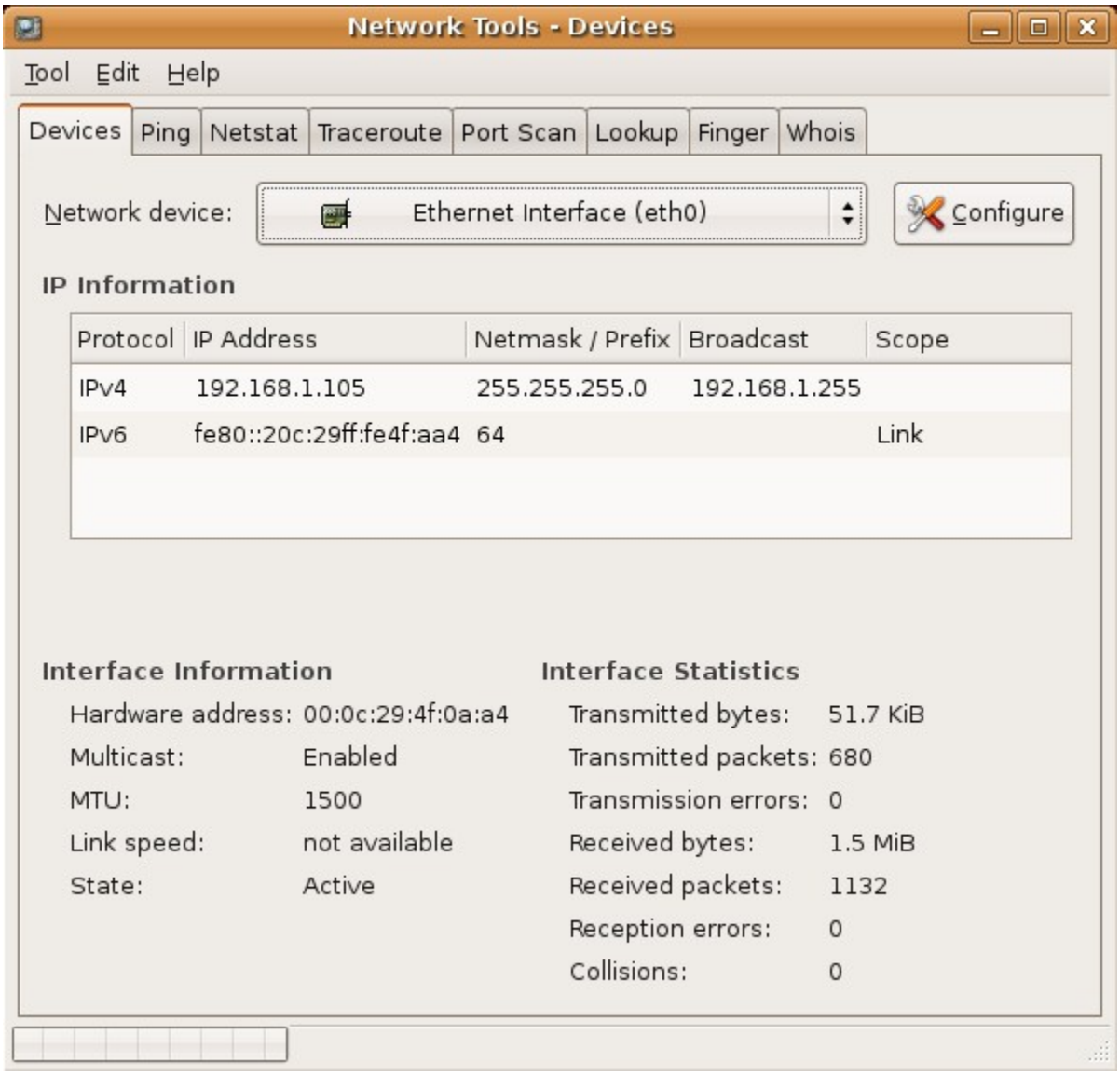


The third line from the top, in the eth0 section, shows the current IP address 192.168.1.105.

Using Network Tools

Viewing the IP address using the Network Tools application is similarly simply, just navigate to System -> Administration and launch the Network Tools application.

On the initial dialog, change the Network device selection from Loopback Interface (lo) to Ethernet Interface (eth0). The current IP information will be shown below, similar to the screenshot below:



Changing the network configuration

If you need to change the current network configuration, then you can do this easily using the **Networking** application, which is found in the System -> Administration folder of the toolbar. We also added a shortcut to the desktop called **Configure Networking** that brings you the same application.

This application lets you configure the IP address, subnet mask, DNS servers, host name etc.. To change the IP address, select *Ethernet connection* and click Properties. For all other changes, click the appropriate tab (e.g. DNS).

If your virtual machine is configured correctly then you should be able to ping host names on your network (you can use the **Network Tools** application under System -> Administration to ping) and should also be able to ping the virtual machine from hosts in your network.

4.3 Installed Software

ESONUBU runs Ubuntu 6.06 LTS (aka *Dapper Drake*), a Debian-based Linux distribution that is available for free. We chose Ubuntu for its ease of use, appealing interface and because it is completely free of charge.

The following software is installed with ESONUBU. If software is installed as a package, then security vulnerabilities and other critical problems will most likely be updated automatically.

Software	Version	Description	Installed as Package	Required
MySQL Server	5.0.22	Free database server	yes	yes
MySQL Administrator	1.1.10	Graphical interface to administer MySQL	no	no
Nessus	2.2.6	Vulnerability scanner	yes	no
Mozilla Firefox	1.5.0.5	Web browser	yes	no
EventSentry Documentation	2.71	Entire EventSentry documentation as PDF files	no	no

5 Configuring EventSentry

If you install EventSentry with the **Setup MSSQL** or the **Setup MySQL** feature activated, then most database consolidation features will be activated by default. This means, that by default EventSentry will be writing the following information to the EventSentry database:

- All **Information**. **Warning**, **Error** and **Audit Failure** events will be written to the database
- Service status information will be recorded in the database
- Disk space information will be recorded in the database
- Software installation history is recorded in the database
- Average CPU time, memory usage and disk queue length are recorded in the database
- Process, Logon and Print tracking information is recorded in the database

If you installed EventSentry without the **Setup MSSQL** or the **Setup MySQL** feature activated then you will need to configure these features manually, after the database has been setup. Please follow the brief instructions in the following chapters to configure these features.

Please note that the following chapters only briefly cover the topics of event log and system health monitoring. For more information please see the manual or the following best practises topics:

- Event Log Consolidation
- System Health Monitoring

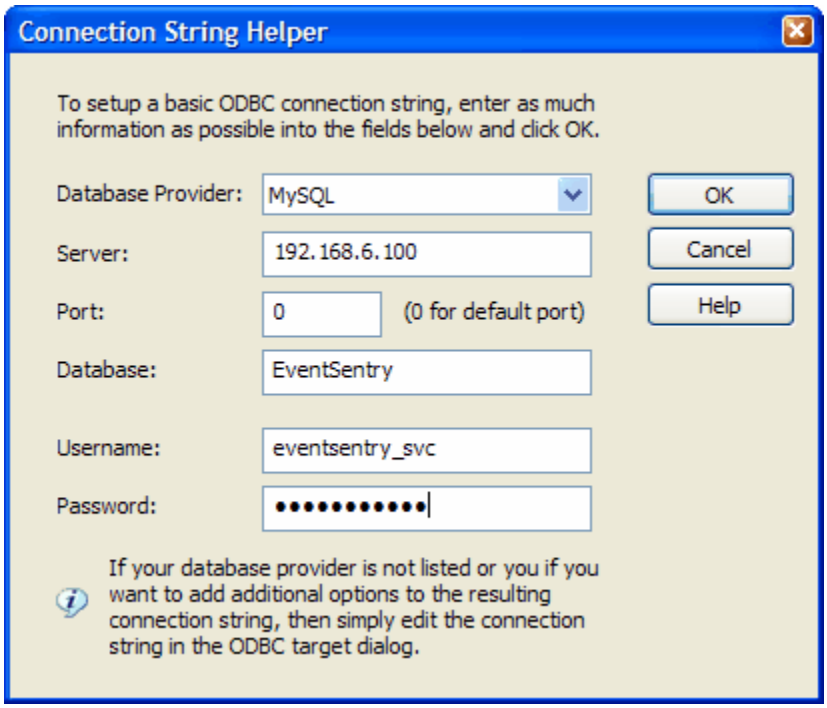
5.1 ODBC Target (Notification)

An ODBC target **is needed by all features** that forward information (e.g. event logs, service status) to the database. The ODBC target essentially tells EventSentry where to find the database server, the name of the EventSentry database and what the login information is. This ODBC target is then referenced by filters and system health features.

If you do not have a database notification target yet, then you can create one by right-clicking the **Notifications (Targets)** container and clicking **Add**. Specify a name for the target (e.g. MySQL DB) and click the **ODBC** tab.

You can either point to the EventSentry database using a connection string or a System DSN. A connection string is **almost always** the preferred method, since selecting a System DSN requires you to configure this System DSN on every computer that is to communicate with the database through EventSentry.

To create a connection string, click the **Create** button and enter the relevant information into the *Connection String Helper* dialog:



Enter the following information into this dialog to point to the MySQL database on your ESONUBU virtual machine:

Database Provider:	MySQL
Server:	IP Address of your VM (more information)
Port:	0
Database:	EventSentry
Username:	eventsentry_svc
Password:	See "Usernames and Passwords"

5.2 Event Log Consolidation

In order to forward events log entries to a database you will need to create a new filter package (or use an existing one) and create a filter. A filter package is necessary since all filters need to be contained in filter packages, and the filter itself tells EventSentry which events to forward to the database.

Configure the filter itself according to your requirements (e.g. which logs and severities to forward to the database), but make sure that you add the ODBC target to the list of targets.

> ⚠ In most cases one filter will be sufficient (e.g. when you consolidate all Audit Failures to the database), but you might have to create multiple filters if your requirements are more complex.

Please see Event Log Consolidation in the **best practises** guide for more information.

5.3 System Health and Tracking

System Health

The following system health features support logging of information to the EventSentry database:

- Service monitoring
- Disk space monitoring
- Software installation monitoring
- Performance monitoring

If you are working with a default installation of EventSentry, then chances are that most system health monitoring objects are already configured and active. Expand the System Health Packages container to find out which system health packages are installed. Expand the individual packages to see which monitoring objects they contain. If a particular object does not exist, then you can **right-click the package** and select **Add** and select a health-monitoring object.

You can either specify the ODBC target at the object level (e.g. in the service monitoring object), or at the package level. It is recommended that you **set the ODBC target on the package level** since this makes administration significantly easier. An ODBC target set at the package level will automatically apply to all objects of that package, so add as many objects as needed to the package.

You will still have to configure some options on the object-level, for example how often disk space information is to be written to the database. See Health Packages in the official documentation for more information.

Make sure that you don't forget to assign any package, whether is a filter package, health package or tracking package, to the appropriate group and/or computer.

Tracking

All tracking features of EventSentry require a database, they cannot be used without a database. Just like with system health monitoring, you can either specify the ODBC target at the object level (e.g. in the logon tracking object), or at the package level. I recommend that you set the ODBC target on the package level since this makes administration significantly easier. An ODBC target set at the package level will automatically apply to all objects of that package, so add as many objects as needed to the package.

5.4 Important Information

Please check the following steps to make sure that EventSentry is deployed correctly in your network:

1. Once you configured EventSentry properly, make sure that all packages are properly assigned and save the configuration.

2. If you haven't done so already, **install the EventSentry agents** on the remote hosts by selecting "Remote -> Install Agent(s)" from the main menu.

3. If agents are already installed, push the configuration through the "Remote -> Update Configuration" main menu option.

4. Since EventSentry **utilizes ODBC** in order to talk to the database, all the computers on your network that need to write data to the ESONUBU database server will need to have the MySQL ODBC drivers installed. Please see Rolling out the MySQL ODBC Driver for more information on how to automate this process.