

# Quantar Solutions Ltd. – Network Operational Risk Manager (nORM) Monitoring System Installation and Operation Manual

*Version 2 – January 2009*

<b>1 Introduction .....</b>	<b>1</b>
<b>2 Database and File Server Installation.....</b>	<b>2</b>
<b>2.1 Basic System Installation.....</b>	<b>2</b>
2.1.1 Detailed Instructions .....	2
<b>2.2 Create shared ssh key.....</b>	<b>3</b>
2.2.1 Detailed Instructions .....	3
<b>2.3 NTP server setup.....</b>	<b>3</b>
2.3.1 Detailed Instructions .....	3
<b>2.4 Samba server setup + repository.....</b>	<b>3</b>
2.4.1 Detailed Instructions .....	3
<b>2.5 Database Configuration.....</b>	<b>4</b>
2.5.1 Detailed Instructions .....	4
<b>2.6 Cron setup + createXML configuration.....</b>	<b>4</b>
<b>2.7 Snort configuration directory + update checker cron.....</b>	<b>5</b>
2.7.1 Detailed Instructions .....	5
<b>2.8 Mappings file.....</b>	<b>5</b>
<b>3 Monitor Installation .....</b>	<b>5</b>
<b>3.1 Basic system installation.....</b>	<b>5</b>
3.1.1 Detailed Instructions .....	6
<b>3.2 NTP client to database server.....</b>	<b>6</b>
<b>3.3 Copy public key from database server.....</b>	<b>6</b>
<b>3.4 Snort installation.....</b>	<b>7</b>
3.4.1 Detailed Instructions .....	7
<b>3.5 Synchronise snort configuration.....</b>	<b>7</b>
<b>3.6 Monitor script installation.....</b>	<b>7</b>
<b>4 Operational Considerations .....</b>	<b>7</b>
<b>4.1 Mappings file.....</b>	<b>7</b>

<b>4.2 Snort Rules.....</b>	<b>7</b>
<b>5 Reference to Other Documentation.....</b>	<b>8</b>

## **1 Introduction**

This guide specifies the installation requirements for the two machines required for monitoring. The required CDs for the installation are:

- Ubuntu “Dapper” Server 6.06
- FreeBSD 6.1
- Additional Software CD containing:
  - MySQL Snort database initialisation script
  - XML creation script + library + sample mapping file
  - Initial snort configuration directory (including passive control alert)
  - Update Snort script
  - Monitor script + configuration file

The following sections describe the installation of, first, the Database and File Server and then the Monitor.

The IP address 10.0.0.1 will be used throughout this document to refer to the database server and 10.0.0.2 for the monitor. Replace these as required.

Where scripts are required to be configured, see the individual script for instructions.

## **2 Database and File Server Installation**

For additional information, beyond this guide, see:

<http://help.ubuntu.com/6.06/ubuntu.serverguide/C/index.html>

### ***2.1 Basic System Installation***

Install the basic LAMP server from the Ubuntu Dapper 6.06 disk.

Special requirements:

- Needs 2 network ports configured
  - 1 external management address

- 1 local IP address e.g. 10.0.0.1 (for connection to monitor)
- Additional package requirements
  - openssh-server (for remote management)
  - libhtml-parser-perl (for XML creation)
  - libdate-simple-perl (for date calculations)

For other package installation, see individual sections below.

### **2.1.1 Detailed Instructions**

1. Turn on machine and insert CD (making sure the machine is set to boot from CD).
2. At the Ubuntu installation menu, choose “Install a LAMP server”.
3. Choose the required language and keyboard options when prompted.
4. The basic components will then be installed.
5. If there is an available DHCP server, then the management port will be configured automatically. Otherwise, configure the network manually in the forms provided.
6. When prompted, choose an appropriate mirror of the Ubuntu archive (and give HTTP proxy information if required).
7. Select the required disk partitioning options; choosing to erase entire disk and accepting default partitioning should use the whole disk in one partition except for the swap.
8. Set clock to UTC.
9. Choose appropriate username and password.
10. The base system will then be installed (this may take some time).
11. When the installation is finished, reboot and remove the CD.
12. After the reboot, login and remove the CD option from `/etc/apt/sources.list` (i.e. comment out the line 'deb cdrom:...') and uncomment any other sources that have been commented.
13. Run: `sudo aptitude update && sudo aptitude dist-upgrade` to update the system.
14. Install the additional packages required using: `sudo aptitude install openssh-server libhtml-parser-perl libdate-simple-perl`
15. Finally, add the second network configuration in `/etc/network/interfaces`

## **2.2 Create shared ssh keys**

Create a pair of ssh keys with no password, for automated synchronisation between servers.

### **2.2.1 Detailed Instructions**

Run the following command:

```
ssh-keygen -t dsa
```

(using the default file names and no password)

The public key will later be copied to the monitor.

## ***2.3 NTP server setup***

Setup an NTP server to keep the time of the monitor updated.

### **2.3.1 Detailed Instructions**

Install the NTP server:

```
sudo aptitude install ntp-server
```

The change the default server in `/etc/ntp.conf` from `ntp.ubuntu.com` if required.

If the server (or any other settings) is changed, then restart NTP:

```
sudo /etc/init.d/ntp-server restart
```

## ***2.4 Samba server setup + repository***

Create a directory to store the XML files in.

Install a Samba Server to prove access to the directory.

### **2.4.1 Detailed Instructions**

First make a directory for the XML files:

```
mkdir /mypath/xmlfiles
```

Then install Samba:

```
sudo aptitude install samba
```

Create a password for the current user:

```
smbpasswd
```

Edit the configuration file `/etc/samba/smb.conf` changing the workgroup to the required group, making sure the user is not in the invalid list and added the share point e.g.:

```
[share]  
path = /mypath/xmlfiles
```

comment = shared xml files  
browseable = yes  
writable = no

Comment out any other share definitions.

Finally, restart Samba:

```
sudo /etc/init.d/samba restart
```

## **2.5 Database Configuration**

Setting up the database:

- Add remote access to connect from monitor
- Create snort user
- Create snort database and import structure
- Grant permissions for snort user on database

### **2.5.1 Detailed Instructions**

Edit the MySQL configuration file `/etc/mysql/my.cnf` and remove the line:

```
bind-address = 127.0.0.1
```

Restart MySQL:

```
sudo /etc/init.d/mysql restart
```

Run MySQL:

```
mysql
```

Enter the following sequence of commands:

```
create user snort identified by 'password'; (replacing password)
create database snort;
use snort;
source /pathto/create_mysql (The initialisation script on the CD)
grant all on snort.* to snort@localhost identified by 'password';
grant all on snort.* to snort@10.0.0.2 identified by 'password';
flush privileges;
```

## **2.6 Cron setup + createXML configuration**

Copy the `createXML.pl` script and library file from the CD and edit the configuration options inside the script. Then add an item to cron, to run the script once a week.

### **Detailed Instructions**

Edit the crontab:

```
crontab -e
```

And add the following line:

```
* * * * 1 cd createXMLpath && ./createXML.pl
```

This runs the createXML.pl script from its local directory every Monday.

## ***2.7 Snort configuration directory + update checker cron***

Copy the snort configuration directory from the CD provided (and edit the snort.conf output line, if necessary), also copy the update\_snort.pl script (and edit the options as required). Add a line into the crontab to check for update requests at the desired interval.

### **2.7.1 Detailed Instructions**

Edit the file snortconf/snort.conf and change the following line as required:

```
output database: alert, mysql, user=snort password=password dbname=snort  
host=10.0.0.1
```

Edit the crontab:

```
crontab -e
```

Add the following line (example for hourly checking):

```
0 * * * * cd updatesnortpath && ./update_snort.pl >/dev/null
```

## ***2.8 Mappings file***

In addition, it is necessary to enter the desired mappings from snort alerts to local target systems in the mappings file. See Operations below.

## **3 Monitor Installation**

For additional information, beyond this guide, see: <http://www.freebsd.org/docs.html>  
The monitor should ideally be configured to use RAID0 for the hard disk drives (to maximise disk write speed for capturing network traffic) before beginning this installation process.

### ***3.1 Basic system installation***

Install base system of FreeBSD 6.1 using Kern-developer with ports option.  
Special requirements:

- 3 network ports:

- 1 active port with no IP (Intel NIC)
  - 1 local connection e.g. 10.0.0.2 (for communicating with database)
  - 1 external connection (for installation - can be disabled after initial installation)
- Additional packages:
    - bash-3.1.10-1 (or equivalent)
    - Change default shell to bash, for root user
    - Permit SSH access as root

### 3.1.1 Detailed Instructions

1. Turn on the machine and insert FreeBSD installation disk.
2. Choose “Boot FreeBSD [default]” when prompted.
3. Next the machines hardware is automatically detected. This may take some time.
4. When prompted, choose the appropriate regional settings.
5. At the “sysinstall Main Menu” choose “Express” installation.
6. At the disk partitioning menu, use the default settings buy pressing 'A' then 'Q' on both pages. Also, choose the “BootMgr” option to install the FreeBSD Boot Manager.
7. Choose the “kern-developer” distribution and choose “yes” when prompted to install ports.
8. At “Installation Media”, select HTTP and then choose an appropriate site.
9. Configure the management network interface; this can be done automatically if DHCP if available.
10. The installation will now continue. This may take some time, depending on the network bandwidth and machine specification.
11. Select the following package: shells->bash\_3.1.10-1 (or equivalent)
12. After giving a root password, check the sshd option to enable remote access.
13. The basic installation should now be complete. The computer will reboot. Remove the CD.
14. After the reboot, login as root and change the default shell to bash: `chsh -s /usr/local/bin/bash root`
15. Edit `/etc/ssh/sshd_config` and uncomment the line `#PermitRootLogin` and change the 'no' to 'yes'. Then restart the ssh daemon: `/etc/rc.d/sshd restart`
16. Finally, configure the monitoring card in `/etc/rc.conf`

### **3.2 NTP client to database server**

To configure the NTP client edit /etc/ntp.conf and put in the following lines:

```
server 10.0.0.1 primary
driftfile /var/db/ntp.drift
```

Restart the NTP daemon:

```
/etc/rc.d/ntpd restart
```

Finally, add the following line to /etc/rc.conf to ensure NTP is started when the machine boots:

```
ntpd_enabled="YES"
```

### **3.3 Copy public key from database server**

Copy the public key from the database server e.g.:

- mkdir ~/.ssh
- scp user@10.0.0.1:~/.ssh/id\_dsa.pub ~/.ssh/authorized\_keys

### **3.4 Snort installation**

Compile snort from ports with MySQL support and install.

- Make log directory /var/log/snort

#### **3.4.1 Detailed Instructions**

1. Set the http\_proxy environment variable if required.
2. cd /usr/ports/security/snort
3. make (check the MySQL option, when prompted)
4. Snort will now be compiled. There may be several messages saying that sources cannot be found; this is only a problem if the compilation fails.
5. make install (to install the build of snort)
6. mkdir /var/log/snort

### **3.5 Synchronise snort configuration**

Type (all on one line):

- rsync -ave ssh --delete user@10.0.0.1:/pathto/snortconf/ /usr/local/etc/snort

### **3.6 Monitor script installation**

Copy the monitor script (gather.sh) from the CD.

The script can either be run manually or installed into the rc.d directory to be run automatically when the monitor is booted.

## **4 Operational Considerations**

### **4.1 Mappings file**

The file is a simple CSV file with one line per threat. Each line has five values:

- SID – the unique identification number assigned to this threat by SNORT1
- Alert – the name of the threat also provided by SNORT, but can be changed by the Administrator.
- Target – the Target attribute as needed by nORM's Threat tag and is provided manually by the administrator. The default value is "Unknown".
- Category – the Category attribute as required by nORM's Threat tag, again provided by the administrator. The default value is "Indiscriminate".
- Severity – the SeverityScore attribute as required by nORM's Threat tag. The default value automatically calculated from the SNORT priority value. The mapping from SNORT to nORM is 1 → 10, 2 → 7, 3 → 4, 4 → 1.

In order to determine appropriate values for this file please refer to the Mapping Targets document.

### **4.2 Snort Rules**

To update snort rules:

1. Download the latest ruleset from <http://www.snort.org/>
2. Unpack the file
3. Copy the rules directory to /pathto/snortconf on the database machine
4. Execute the synchronisation command from section 3.5

## **6 Reference to Other Documentation**

See also the Mapping Targets Document (January 2009)