Configure Snort to send alerts and updates to EventTracker

Version 7.x

Publication Date: July 30, 2014

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in 1998. Snort is now developed by Sourcefire.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise v7.x** and later, **Snort 2.4** and later.

Table of Contents

Abstract 1
Scope 1
Configure Snort 3
Configure Snort rules 4
Update Rules and Signature 4
Configure OinkMaster for regular updates 4
Create a cron job to daily update community.rules 4
Configure rsyslog to send Snort alerts to EventTracker server 5
Configure Virtual Switch to allow promiscuous mode 6
EventTracker Knowledge Pack (KP) 11
Categories 11
Alerts 12
Reports 123

Configure Snort

1. Login to ETVAS machine using SSH.
2. Open snort.conf in VI Editor.

   The command is vi /etc/snort/snort.conf
3. Locate and modify the following variables. This assumes the network you are going to monitor is 192.168.1.0/24

   ipvar HOME_NET 192.168.1.0/24 (Setup the network addresses you are protecting)

   ipvar EXTERNAL_NET any (Use **!#HOME_NET** to exclude from alerting)

   ipvar DNS_SERVERS [192.168.1.x] (List of **DNS** servers on your network)

   ipvar SMTP_SERVERS 192.168.1.x (List of **SMTP** servers on your network)

   ipvar HTTP_SERVERS 192.168.1.x (List of **WEB Servers** on your network)

   ipvar SQL_SERVERS 192.168.1.x (List of **SQL Servers** on your network)

   ipvar TELNET_SERVERS 192.168.1.x (List of **Telnet Servers** on your network)

   ipvar SSH_SERVERS 192.168.1.x/32 (List of **SSH Servers** on your network)

   ipvar FTP_SERVERS 192.168.1.x/32 (List of **FTP Servers** on your network)

   ipvar SIP_SERVERS 192.168.1.x/32 (List of **SIP Servers** on your network)

   NOTE:

   To enter multiple IP Address/Port you can mention it in a [] bracket i.e. [192.168.1.x/32, 10.1.1.x/32, 172.16.1.x/32]
4. Save the changes, and then close the Snort**.**
5. Restart the Snort service.

   NOTE: Now the snort events will be sent to the local rsyslog.

Configure Snort rules

The Snort rules used by us are registered version which is 30 days prior to previous paid version. Please create your valid user credentials in www.snort.org.

Update Rules and Signature

We cannot make regular update on the registered version but we can make regular update on the community rule edition which is free and is available in

/etc/snort/rules/ community.rules

These files are updated regularly by the community users.

Configure OinkMaster for regular updates

1. Edit OinkMaster configuration in VI Editor i.e. vi /etc/snort/oinkmaster.conf.
2. Modify the URL settings as given below.

   # Example for Community rules

   url = https://s3.amazonaws.com/snort-org/www/rules/community/community-rules.tar.gz

Create a cron job to daily update community.rules

1. Assuming rules directory is /etc/snort/rules.
2. Please update the rules by executing the following commands:
   # oinkmaster.pl –o /etc/snort/rules
3. Create the crontab
   $crontab –e

   0 4 * * * /etc/snort/oinkmaster.pl -o /etc/snort/rules | mail -s "oinkmaster" 123@abc.com

The above command will update community.rules file everyday at 4'oclock and send output to your Email-ID as mentioned earlier.

Configure rsyslog to send Snort alerts to EventTracker server

1. Open rsyslog.conf in VI Editor.
2. Add the information given below after the last ModLoad directive.

   # Added for ET integration with Snort

   $SystemLogRateLimitInterval 10

   $SystemLogRateLimitBurst 500
3. Using following command, add an entry to the EventTracker Manager Console.

   Syslogfacility.priority<tab>@ ip of the Eventtracker server

   For example: If Snort logs were sent as local1 and to collect all logs it will be mentioned as log_info then the following entry can be made in

   local1.info @@RemotehostIPADDRESS:Port_No

   NOTE

   Use '@@' for TCP and '@' for UDP to forward log to Remote host.
4. Save and restart the rsyslog service.

Configure Virtual Switch to allow promiscuous mode

1. Log into the **ESXi/ESX** host or **vCenter** Server using **VMware vSphere Client**.

Figure 1

2. Select the **ESXi/ESX host** in the inventory.

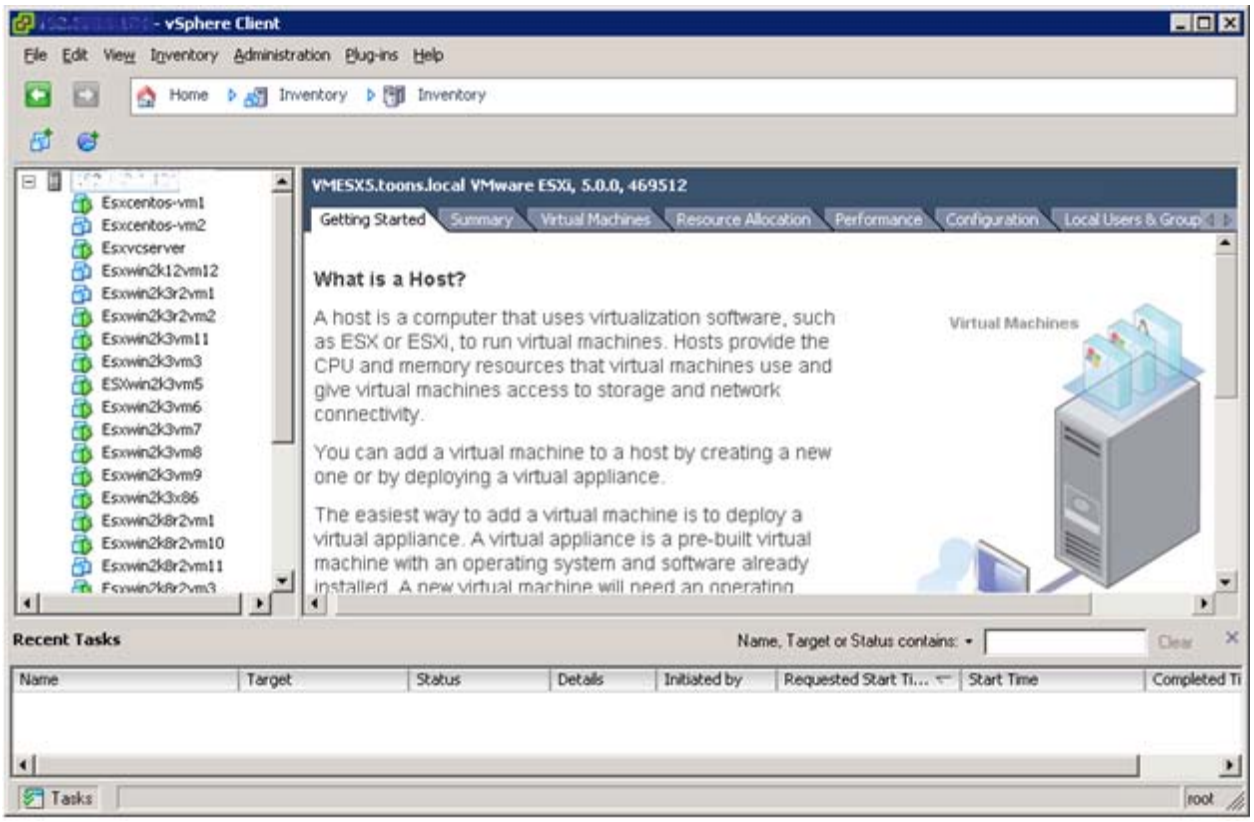

Figure 2

3. To enable promiscuous mode in virtual switch, select the **Configuration** tab, select **Networking** and then select **Properties**.

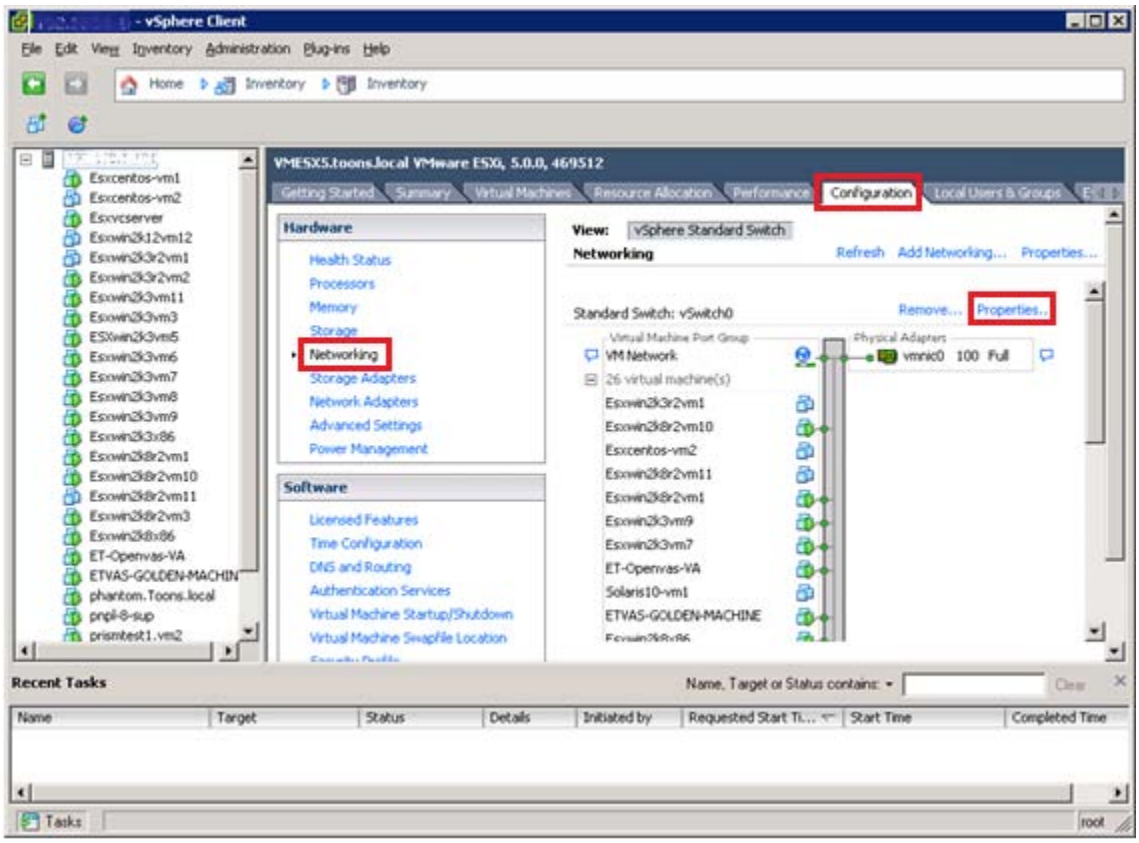

Figure 3

vSwitch0 Properties window displays.

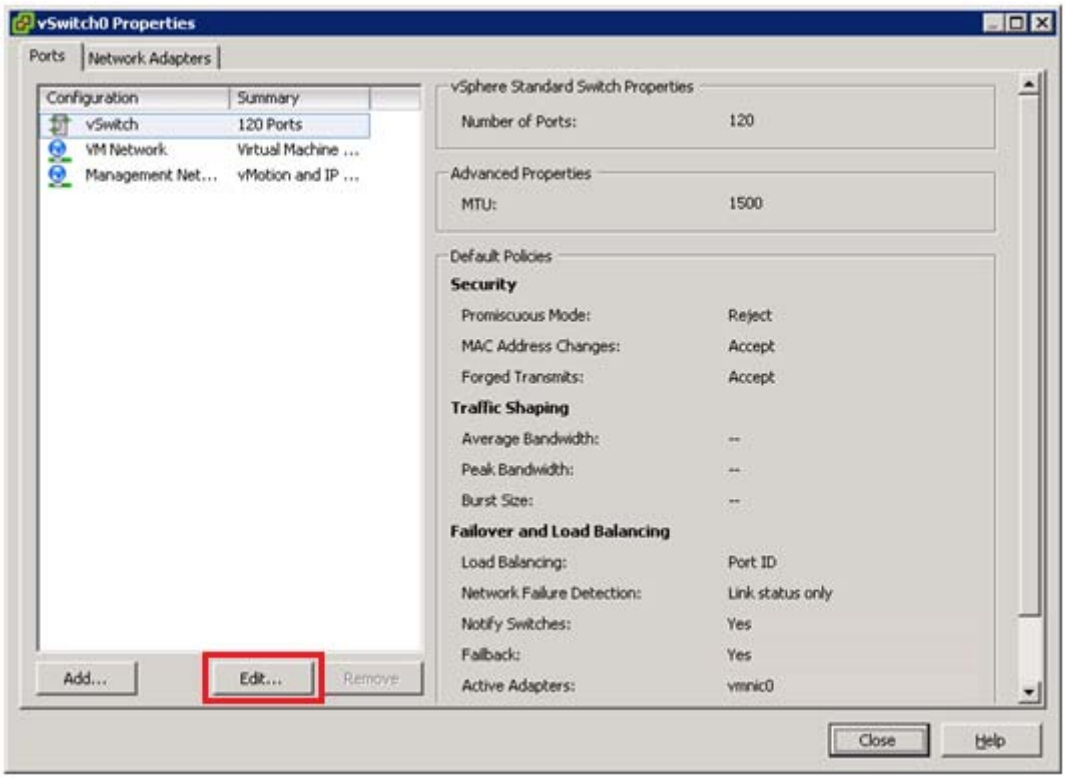

Figure 4

4. Select the required virtual switch or port group to modify and then select **Edit**.
5. Select the **Security** tab.

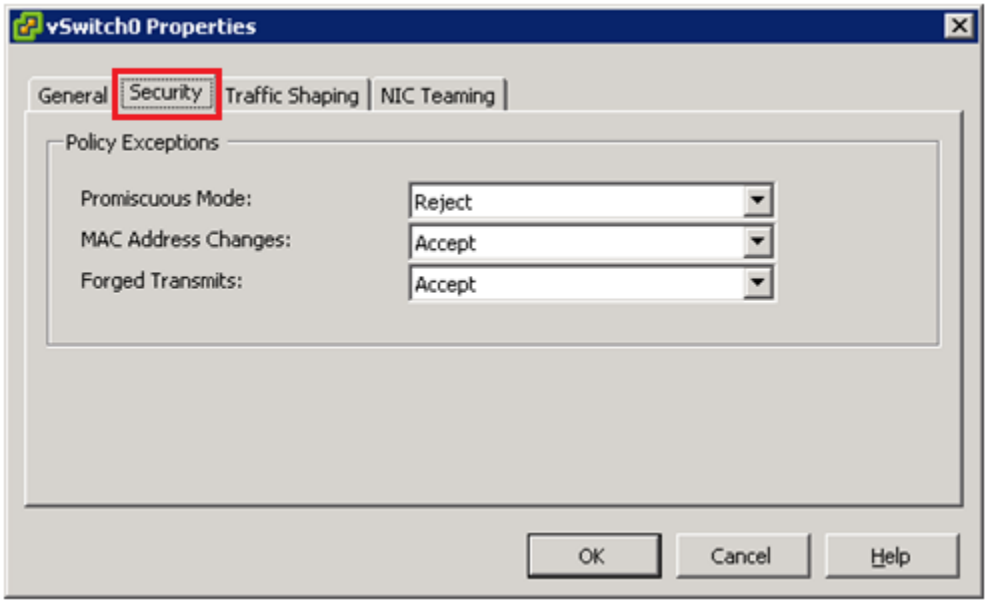

Figure 5

6. Select **Promiscuous Mode** dropdown and then select **Accept**.

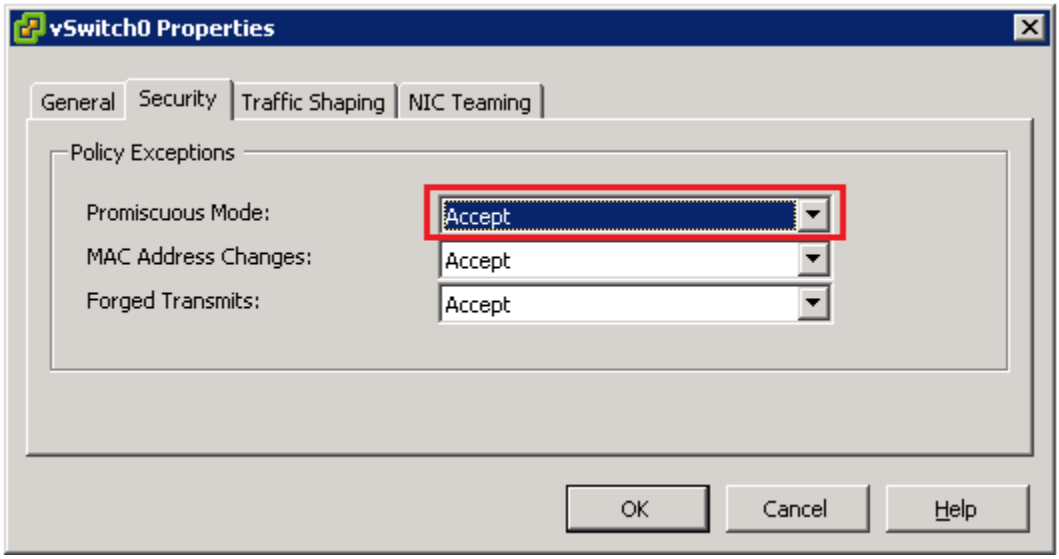

Figure 6

7. Select the **OK** button.

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker, reports and alerts can be configured. The following Knowledge Packs are available in EventTracker v7.x to support Snort monitoring.

Categories

- **Snort Database intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for database attacks.
- **Snort Denial of service alerts:** This category based report provides information related to Alerts generated by SNORT for Denial of Service attacks.
- **Snort DNS intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for DNS attacks.
- **Snort Exploit alerts:** This category based report provides information related to Alerts generated by SNORT for various types of known exploits.
- **Snort Finger intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for various types of finger attacks.
- **Snort FTP intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for FTP attack traffic.
- **Snort IMAP intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for IMAP attack traffic.
- **Snort Misc attack attempts:** This category based report provides information related to Alerts generated by SNORT for Misc. attack traffic.
- **Snort NetBIOS intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for NetBIOS attack traffic.
- **Snort NNTP intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for NNTP attack traffic.
- **Snort P2P intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for P2P attack traffic.
- **Snort POP intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for POP attack traffic.
- **Snort Port scan alerts:** This category based report provides information related to Alerts generated by SNORT for port scan activity detected by SNORT IDS.
- **Snort RPC intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for RPC attack traffic.
- **SMTP intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for SMTP attack traffic.

- **Snort SNMP intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for SNMP attack traffic.
- **Snort Telnet intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for Telnet attack traffic.
- **Snort UNIX intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for various UNIX exploits traffic.
- **Snort Virus activity alerts:** This category based report provides information related to Alerts generated by SNORT for virus attacks.
- **Snort Web application intrusion alerts:** This category based report provides information related to Alerts generated by SNORT for Web application attacks.

Alerts

- **Snort Database intrusion alerts:** This alert is generated when Alerts generated by SNORT for database attacks.
- **Snort Virus activity alerts:** This alert is generated when Alerts generated by SNORT for virus attacks.
- **Snort DNS intrusion alerts:** This alert is generated when Alerts generated by SNORT for DNS attacks.

Reports

- **Snort: Alert Analysis Report:** This report provides information related to analysis of alerts such as attempted denial of service, potentially bad traffic, unknown traffic etc.
- **Snort: Intrusion Detected Report:** This report provides information related to intrusion detection contains details like intrusion type, intrusion classification, address and ports of both source and targets.