McAfee Enterprise Security Manager

Data Source Configuration Guide

Data Source: *Infoblox NIOS*

September 2, 2014

Important Note:

The information contained in this document is confidential and proprietary.

Please do not redistribute without permission.

Table of Contents

1 Introduction

This guide details how to configure Infoblox NIOS to send syslog data in the proper format to the ESM.

2 Prerequisites

McAfee Enterprise Security Manager Version 9.0.0 and above.

In order to configure the Infoblox NIOS syslog service, appropriate administrative level access is required to perform the necessary changes documented below.

3 Specific Data Source Configuration Details

3.1 Infoblox NIOS Configuration

1. From the Grid perspective, click *grid* ->**Edit** -> **Grid Properties**
   Or
   From the Device perspective, click *hostname* -> **Edit -> Device Properties**
2. In Grid or Device editor, click **Monitoring**, and then enter the following:
   - **Enable external syslog server**: Select this check box to enable the Infoblox device to send messages to the specified syslog server.
   - **Syslog Server Group**: Define one or more syslog servers: click **Add**, enter the following, then click **OK**:
     - **Server Address**: Enter the IP address of the syslog server.
     - **Connection Type:** Specify whether the device uses TCP or UDP to connect to the external syslog server.
     - **Port:** Specify the destination port number. (Standard port is 514)
     - **Out Interface:** Specify the interface through which the device sends syslog messages to the syslog server.
     - **Severity Filter:** Choose a filter from the drop-down list.
     - **Message Source:** Specify which syslog messages the device sends to the external syslog server:
       - **Internal:** Device sends the syslog messages that it generates.
       - **External:** Device sends the syslog messages that it receives from other devices, such as syslog servers and routers.
       - **Any:** Device sends both internal and external syslog messages.
     - **Copy audit log messages to syslog:** Select the check box for the Infoblox device to include audit log messages among the messages it sends to the syslog server. This function can be helpful for monitoring administrative activity on multiple devices from a central location.
     - **Audit Log Facility:** Choose the facility where you want the syslog server to sort the audit log messages.
3. Click the Save icon to save your settings.

Configuring Syslog for a Grid Member

1. From the Grid perspective, click **+** (for *grid*) -> **+** (for **Members**) -> *member* -> **Edit** -> **Member Properties.**
2. In the *Grid Member* editor, click **Monitoring**, and enter the following:
   - **Override grid syslog settings:** Select the check box to override grid-level syslog settings and apply member-level settings.
   - **Enable external syslog server:** Select the check box to enable the Infoblox device to send messages to a specified syslog server.
   - **Syslog Server Group:** To define one or more syslog servers, click **Add**, enter the following, and then click **OK**:
     - **Server Address:** Type the IP address of a syslog server.
     - **Connection Type:** Specify whether the device uses TCP or UDP to connect to the external syslog-server.
     - **Port:** Specify the destination port number.

        - **Out Interface:** Specify the interface through which the device sends syslog messages to the syslog server.
        - **Severity Filter:** Choose a filter from the drop-down list.
    - **Message Source:** Specify which syslog messages the device sends to the external syslog server:
        - **Internal:** The device sends the syslog messages that it generates.
        - **External:** The device sends the syslog messages that it receives from other devices
        - **Any:** The device sends both internal and external syslog messages.

- **Enable syslog proxy:** Select this check box to enable the device to receive syslog messages from other devices, such as syslog servers and routers, and then forward these messages to an external syslog server.
- **Enable listening on TCP:** Select this check box if the device uses TCP to receive messages from other devices.
    - **Port:** Enter the port number through which the device receives syslog messages from other devices.
- **Proxy Client Access Control:** Click **Add**, enter the following in the *Access Control* Item dialog box, and then click **OK:**
    - **IP Address option:** Select **IP Address** if you are adding the IP address of a device, or select **Network** if you are adding the network address of a group of devices.
        - **Address:** Enter the IP address of the device or network.
        - **Subnet Mask:** If you entered a network IP address, you must also enter its subnet mask.

3. Click the **Save** icon to save your settings.

3.2 McAfee Receiver Configuration

After successfully logging into the McAfee ESM console the data source will need to be added to a McAfee Receiver in the ESM hierarchy.

1. Select the Receiver you are applying the data source setting to.
2. Select the Receiver properties.
3. From the Receiver Properties listing, select “Data Sources”.
4. Select “Add Data Source”.

   OR

1. Select the Receiver you are applying the data source setting to.
2. After selecting the Receiver, select the “Add Data Source” icon.

Data Source Screen Settings

1. Data Source Vendor – Infoblox
2. Data Source Model – NIOS (ASP)
3. Data Format – Default
4. Data Retrieval – Default
5. Enabled: Parsing/Logging/SNMP Trap – Parsing
6. Name – Name of data source
7. IP Address/Hostname – The IP address and host name associated with the data source device.
8. Syslog Relay – None
9. Mask – 32
10. Require Syslog TLS – Enable to require the Receiver to communicate over TLS.
11. Support Generic Syslogs – Do nothing
12. Time Zone – Time zone of data being sent.

Note – Refer to Appendix A for details on the Data Source Screen options

4 Appendix A - Generic Syslog Configuration Details

Once you select the option to add a data source, you are taken to the “Add Data Source” menu. The general options for adding a data source are shown. As you select different options, additional parameters may show. Each of these parameters will be examined in more detail.

1. Use System Profiles – System Profiles are a way to use settings that are repetitive in nature, without having to enter the information each time. An example is WMI credentials, which are necessary to retrieve Windows Event Logs if WMI is the chosen mechanism.
2. Data Source Vendor – List of all supported vendors.
3. Data Source Model – List of supported products for a vendor.
4. Data Format – “Data Format” is the format the data is in. Options are “Default”, “CEF”, and “MEF”.

   Note – If you choose CEF it will enable the generic rule for CEF and may not parse data source-specific details.
5. Data Retrieval – “Data Retrieval” allows you to select how the Receiver is going to collect the data. Default is over syslog.
6. Enabled: Parsing/Logging/SNMP Trap – Enables parsing of the data source, logging of the data source, and reception of SNMP traps from the data source. If no option is checked, the settings are saved to the ESM, but not written to the Receiver or utilized. Default is to select “Parsing”.
7. Name – This is the name that will appear in the Logical Device Groupings tree and the filter lists.
8. IP Address/Hostname – The IP address and host name associated with the data source device.
9. Syslog Relay – “Syslog Relay” allows data to be collected via relays and bucketed to the correct data source. Enable syslog relay on relay sources such as Syslog-NG.
10. Mask – Enables you to apply a mask to an IP address so that a range of IP addresses can be accepted.
11. Require Syslog TLS – Enable to require the receiver to communicate over TLS.
12. Support Generic Syslog – “Generic Syslog” allows users to select “Parse generic syslog” or “Log ‘unknown syslog event”. Both these options will create an alert for an auto-learned syslog event if there is no parsing rule.
13. Time Zone - If syslog events are sent in a time zone other than GMT, you need to set the time zone of the data source so the date on the events can be set accordingly.
14. Interface – Opens the receiver interface settings to associate ports with streams of information.
15. Advanced – Opens advanced settings for the data source.

5 Appendix B - Troubleshooting

- If a data source is not receiving events, verify that the data source settings have been written out and that policy has been rolled out to the Receiver.
- If you see errors saying events are being discarded because the “Last Time” value is more than one hour in the future, or the values are incorrect, you may need to adjust the “Time Zone” setting.