McAfee Enterprise Security Manager Data Source Configuration Guide

Data Source: *Vormetric Data Security Manager*

February 16, 2016

Table of Contents

1 Introduction

This guide details how to configure Vormetric Data Security to send syslog data in the proper format to the McAfee Event Receiver.

2 Prerequisites

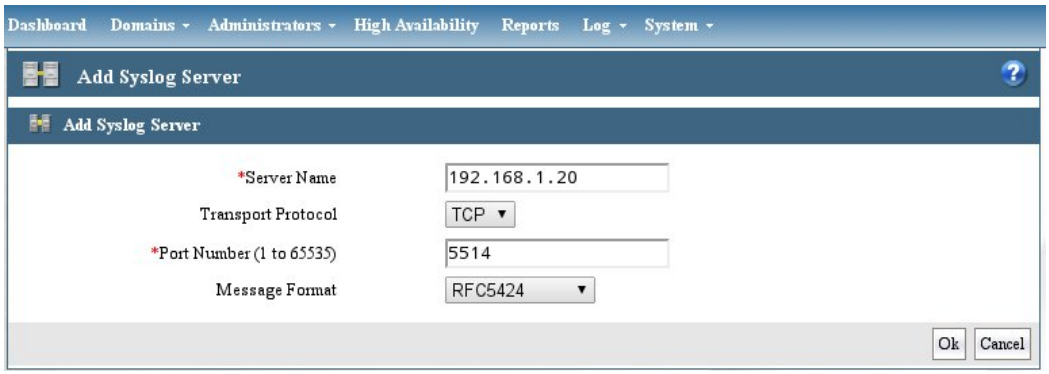
McAfee Enterprise Security Manager Version 9.2.0 and above.

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

3 Specific Data Source Configuration Details

3.1 Vormetric Data Security 5.2 Configuration

1. Within the DSM product, select **Log > Syslog** and add the required information.



You will need to check **Syslog Enabled** via **System > General Preferences** on the **System** tab.

2. Syslog server for DSM logging will need to be configured for each Domain.

3.2 McAfee Event Receiver Configuration

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

1. Select the desired McAfee Event Receiver.
2. Click the **Properties** icon.
3. From the Receiver Properties listing, select **Data Sources**.
4. Click **Add**.
   OR
1. Select the desired McAfee Event Receiver.
2. Click the **Add Data Source** icon.

Data Source Screen Settings

1. Data Source Vendor – Vormetric
2. Data Source Model – Data Security (ASP)
3. Data Format – Default
4. Data Retrieval – Default
5. Enabled: Parsing/Logging/SNMP Trap – Defaults
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 Data Source Event to McAfee Field Mappings

4.1 Log Format

The expected format for this device is not available.

4.2 Log Sample

These are sample logs from a Vormetric Data Security device:

```
<30>1 2013-06-29T18:44:42.420Z 10.10.10.1 vee-FS 0 CGP2601I [CGP@21513
sev="INFO" msg="Audit access" cat="[AUDIT]" pol="aria256_on_host"
uinfo="cfd,uid=100,gid=10{staff}"
sproc="/opt/VRTSfssdk/5.0/src/vxfsio/cache/obj64/cache_advisory"
act="write_app" gp="/vor/guard" filePath="/symtest" key="aria256_on_host"
denyStr="PERMIT" showStr="Code (1M)"]

<14> Jan 06 05:31:03 cpu.mydom.com CEF:0|Vormetric,
Inc.|dsm|5.2.0.1|DAO0048I|update host|3|cs4Label=logger cs4=DAO spid=4322
rt=1388986263954 dvchost=cpu.mydom.com suser=USER_1 shost=test_cpu
```

4.3 Mappings

The table below shows the mappings between the data source and McAfee ESM fields.

Log Fields	McAfee ESM Fields
filePath	Destination_Filename
cat	Category
url	URL
Message ID	Signature ID
sev	Severity
msg, Action	Message
user, suser, admin, uinfo	Source User
shost	Host, Source IP
dvchost	Destination_Hostname
sproc, Process	Application
act	Event Subtype, Command
denyStr	Event Subtype
spt	Source Port
count	Event Count
cs1_policy, policy, pol	Policy_Name, Command
“faked as USERNAME” from suser	User_Nickname

showStr, reason	Reason
rt	First Time, Last Time
key	Registry_Key
Res	Object

5 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.

6 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.
- When creating custom Advanced Syslog Parser rules, the “Key” and “Value” table located within the “Parsing” tab will display potential field mappings based on the log text within the “Sample Log Data” section. None of the data from the “Key” and “Value” table is populated by default. Actual field assignments are set within the “Field Assignment” tab by dragging and dropping the key onto the desired field.
- Note that when analyzing log data details, and selecting the “Custom Types” tab, some fields may not be present if that specific field data is absent from the received logs.