encode
cyber threat management

Log Source Configuration Guide

Log Source Configuration Guide: Unix-Linux-BSD-OS X

Date	10/5/2019
Version	2.2
Classification	CONFIDENTIAL

Disclaimer: The information included in this document is **Confidential**. If you are not the person authorised to review it, please avoid reading, copying, distributing and transmitting its contents. Reproduction in whole or in parts is prohibited without the written consent of the copyright owner. For any questions or remarks on this document, please contact Encode,

Encode, Extrusion Testing and ENORASYS are registered trademarks of Encode and/or its affiliates.

All other product and company names may be property and/or trademarks of their respective owners.

Certificate No: PIR 0362594/A

Certificate No: 362594

Document Information	
Document Title	Log Source Configuration Guide: Unix-Linux-BSD-OS X
Classification	○ Public ○ For Internal Use Only ● Confidential ○ Strictly Confidential ○ Secret
No. pages / File size	7 pages / 1718 kB
Document Type	○ Proposal ● Deliverable ○ General

Quality Assurance

	Date	Name	Title	Completed
Issue	05/12/2018	Konstantinos Zacharos	SOC Engineer	☑
Review	05/12/2018	Thomas Ailianos	SOC Manager	☑
QA review/ Final Approval	05/12/2018	Dimitris Dorizas	MSS Manager	☑

Document History

Date	Version	Name	Notes
08/06/2015	1.0	Ioannis Vaxevanos	First Release
11/05/2018	1.5	Vasilis Rousis	General revision command history added
05/12/2018	2.0	Konstantinos Zacharos	New Template
17/12/2018	2.1	Konstantinos Zacharos	Text Changes
19/12/2018	2.2	Konstantinos Zacharos	Configuration guidelines added, minor template changes

Table of Contents

1. Introduction

1.1 Purpose of the document

This Log Source Configuration guide provides information regarding the integration of the Unix, Linux, BSD & OSX systems with the MSS/MDR Service. In the chapters below, detailed information regarding the logging enablement, optimization and formatting is provided.

1.2 Log source information

Unix/Linux-based Log Sources are a family of free and open-source software operating systems built around the Unix/Linux kernel.

1.3 Event & logging information

By integrating any of this type of log sources, Encode MSS/MDR Service will be able to monitor authentication events, system events, scheduled tasks, session-related events, etc.

1.4 Limitations

Encode Use Case Framework is based on the events that are produced by the Unix/Linux/BSD/ OSX systems. The Correlation Engine is unable to identify behaviours that are not reported by the Operating System.

1.5 Known Issues

There are no known issues for this log source.

2. Logging Configuration

2.1 Rsyslog Configuration

In order to configure your Unix Operating system using rsyslog mechanism the following steps are required:

1. Login on the system using valid credentials and escalate to a privileged user.
2. Edit the file /etc/rsyslog.conf with a text editor.
3. Append the following line usually found in the end of the configuration file.

   ```
   *.info        @@<CPE_HVEC_IP_Address>:10006
   ```

   In order to properly complete the destination IP address, please consult the field “Event Collection” on the Unix sheet.
4. Use the following command to make SELinux allow log transfer to 10006 port.

   ```
   semanage port -a -t syslogd_port_t -p tcp 10006
   ```

5. Restart the rsyslog service using the following command.

   ```
   /etc/init.d/rsyslog restart
   ```

2.2 Syslog Configuration

In order to configure your Unix Operating System using syslog mechanism the following steps are required:

1. Login on the system using valid credentials and escalate to a privileged user.
2. Edit the file /etc/syslog.conf with a text editor.
3. Append the following line at the beginning of the file under “Global Directives” section.
4. Append the following line:

   ```
   *.info        @<CPE_HVEC_IP_Address>
   ```

5. Restart the syslog service using relative command, according to the operating system type and version.

2.3 Syslog-ng Configuration

In order to configure your Unix devices using syslog-ng mechanism the following steps are required:

1. Login on the system using valid credentials and escalate to a privileged user.
2. Edit the file /etc/syslog-ng.conf with a text editor.
3. Append the following configuration:

   ```
   destination d_papertrail
   {
   network(
       “<HVEC_address>”
       port(10006)
   transport(“tcp”)
   );
   };
   log {
       source(s_sys);
       destination(d_papertrail);
   };
   ```

4. Restart the syslog-ng service using the following command.

   ```
   /etc/init.d/syslog-ng restart
   ```

2.4 Verification of configuration

In order to verify if the communication paths are enabled for syslong-ng and rsyslog configuration and the configuration is correct follow the commands below:

1. Netcat command:

```
nc -vz <CPE_HVEC_IP_Address> 10006
```

   If successful you should see a message similar to “Connection to xxx.xxx.xxx.xx 10006 port (tcp) succeeded!”

2. Tcpdump command:

```
tcpdump –i any port 10006
```

   If successful, you should see new lines created and traffic originating from the system to the relative HVEC system when trying to from another session.

3. Network Requirements

In order to complete the integration, Network Administrators should ensure that the following communication paths, to/from **Encode Customer Premises Equipment (CPE)** are properly configured as described below:

- Unix-Linux-BSD-OSX → TCP/10006 → Push Event Collector (HVEC) (for rsyslog and syslog-ng daemons)
- Unix-Linux-BSD-OSX → UDP/514 → Push Event Collector (HVEC) (for syslog daemons)

In order to identify the IP address of Encode CPEs, please consult the Scoping Worksheet in the sheet “Deployment Information”

4. Required Information

In order for the integration to complete the following information is required by Encode:

- The hostname of the server to be integrated
- The IP address of the server

Advanced Cyber Threat Management

Encode Europe
London, United Kindom

Encode Middle East
Dubai, UAE

Encode Center of Excellence
Athens, Hellas
…………………………………

encodegroup.com

Disclaimer: The information included in this document is **Confidential**. If you are not the person authorised to review it, please avoid reading, copying, distributing and transmitting its contents. Reproduction in whole or in parts is prohibited without the written consent of the copyright owner. For any questions or remarks on this document, please contact Encode,

Certificate No. PIR 0352594/A Certificate No: 397594