

Security Information and Event Management

Cloud Execution Environment

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2016–2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Scope	1
2	General	2
3	Description	3
3.1	Protocol Versions	3
3.2	Current Configuration Methods	4
4	Message and Signal Definition	6
4.1	RELP	6
4.2	Syslog	6
5	Functions and Procedure Declaration	7
5.1	RELP	7
5.2	Syslog over TCP	7
6	Constants Declarations	8
	Reference List	9



1 Scope

This document describes the interface between the external Security Information and Event Management (SIEM) systems and the Log Collector in Atlas.

The arrow between SIEM and Log Collector in Figure 1 represents the interface.

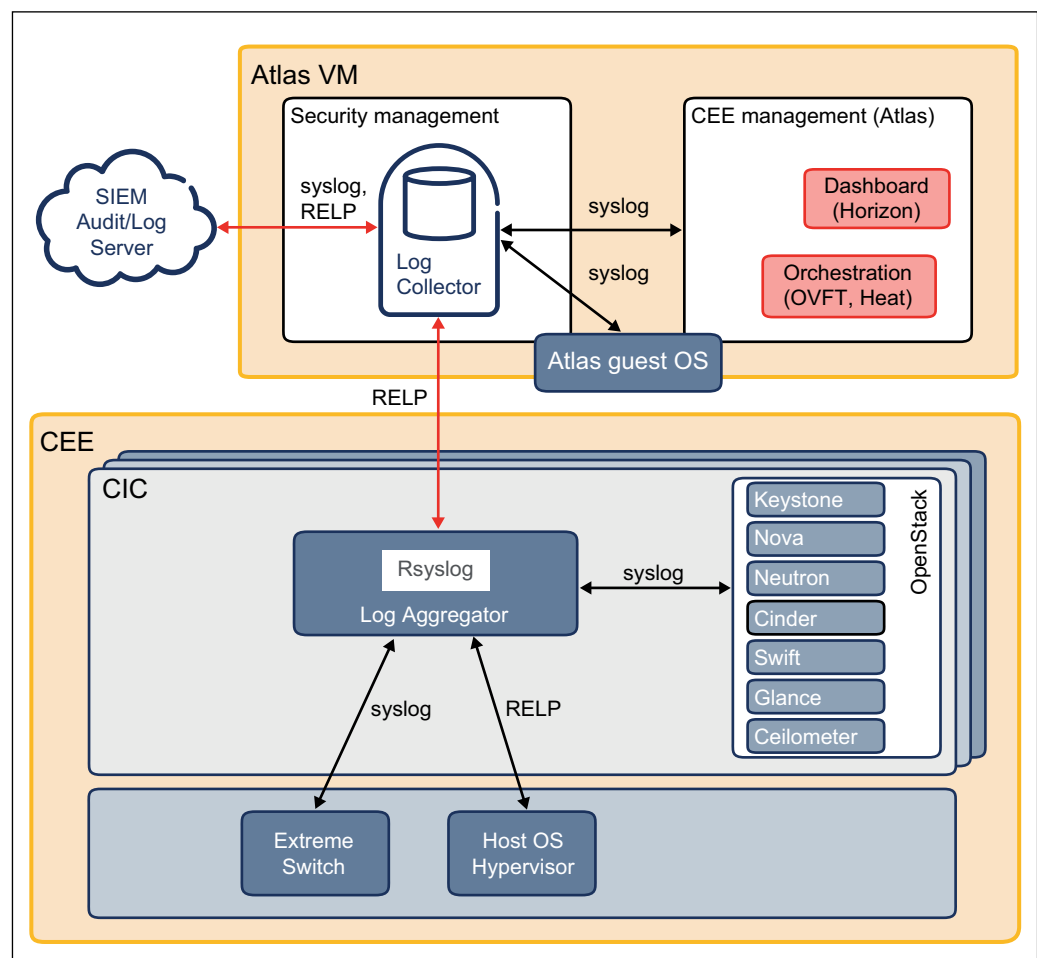


Figure 1 Security and Audit Logging



2 General

Audit events received by the Log Collector can be forwarded to one or multiple external SIEM systems for further analysis. Supported protocols for event forwarding are the Reliable Event Logging Protocol (RELP) and syslog over the Transmission Control Protocol (TCP).

Event Sources

The audit and security logging system collects logs originating from the following event sources:

- Compute nodes
- Controller nodes
- Top-of-rack switches (Extreme)

Audit and security log records from these nodes are either asynchronously pushed towards the Log Aggregator.

Log Aggregator

Security and Audit event records from the event sources are aggregated at the Log Aggregator and forwarded towards the Log Collector. The Log Aggregator functionality is performed by the `rsyslog` instance on the controllers, and it also acts as the system log. High availability of the Log-Aggregator is ensured by the HAProxy front-end that performs health check of the Log Aggregator interfaces and distributes the load among the controllers.

Log Collector

Atlas acts as the collector of all audit and security events sent by the event sources in the Cloud Execution Environment (CEE). `rsyslog` is configured to receive audit events over the RELP protocol and store them in a separate file system. The log collector listens on port 20514 for RELP connections. The incoming events are stored in a separate file system mounted at `/log-collector`. The size of the log-collector filesystem is 10% of the mounted data volume. The log file is truncated and rotated if it reaches the specified size limit.

Audit events received by the Log Collector can be forwarded to one or multiple external SIEM systems for further analysis. Supported protocols for event forwarding are RELP and syslog over TCP.

Note: There is no practical limitation to the number of external systems to which the audit events can be forwarded.



3 Description

This section describes the protocols that can be used between the Log Collector and the external SIEM systems.

RELP

RELP is a networking protocol for computer data logging in computer networks. It is based on the ideas of the syslog protocol but extends it to provide reliable delivery of event messages. It is most often used in environments where message loss is not acceptable.

RELP uses a client-server model with (mostly) fixed roles. The initiating part of the connection is called the client, the listening part is called the server.

RELP uses TCP for message transmission. This provides basic protection against message loss, but does not guarantee delivery under all circumstances. When a connection is aborted, it cannot be reliably detected if the last messages sent have actually reached their destination. Contrary to the syslog protocol, RELP works with a backchannel, over which information of messages processed by the receiver is conveyed back to the sender. This enables RELP to always know which messages have been properly received, even in the case of a connection abort.

Refer to Reference [1] for more information.

Syslog

The syslog protocol is a communication standard for sending simple messages from distributed systems and processes to the syslog server for logging and later analysis.

Refer to Reference [2] and Reference [3] for more information.

3.1 Protocol Versions

This section describes protocol versions used.

RELP

The RELP protocol version 1 is used.

The support for RELP in rsyslog is provided by the librelp library.

Syslog

The rsyslog version 8.29 is used.



3.2 Current Configuration Methods

This section describes the supported configuration modifications.

The `rsyslog` must be restarted after changing the configuration files mentioned in the following subsections to activate the changes. Use the following command:

```
service rsyslog restart
```

3.2.1 Log Rotation

Threshold for Rotation

The threshold for rotation can be configured by modifying the content of the following file:

```
/etc/rsyslog.d/40-audit.conf
```

Amount of Log Rotations

The amount of log rotations can be configured by modifying the content of the following file:

```
/opt/log-collector/conf/rotate_logs
```

To keep the size of the log-collector filesystem under the allowed 10% of the mounted data, ensure that the configured values fulfill the following rule:

```
threshold_for_rotation x amount_of_log_rotations + 1 < 10%_of_data_volume
```

3.2.2 Forwarding Events to SIEM

Address and Port

The address and port of the external SIEM can be configured by modifying the content of the following file:

```
/etc/rsyslog.d/39-siem.conf
```

Multiple SIEMs

To forward the events to more than one SIEM, multiple output actions must be configured as part of the SIEM ruleset in the config file `/etc/rsyslog.d/39-siem.conf` as shown in the example below:

```
ruleset(name="SIEM"){  
    action(type="omrelp" target="1.1.1.1" port="1111")  
    action(type="omrelp" target="relp.siem.com" port="2222")  
    action(type="omfwd" target="3.3.3.3" port="3333" protocol="tcp")  
    action(type="omfwd" target="syslog.siem.com" port="4444" protocol="tcp")  
}
```

The example configuration above will forward all the audit events to the following four remote systems:



- To 1.1.1.1, port 1111, using RELP
- To relp.siem.com, port 2222, using RELP
- To 3.3.3.3, port 3333, using syslog over TCP
- To syslog.siem.com, port 4444, using syslog over TCP



4 Message and Signal Definition

4.1 RELP

RELP employs a command-response model, that is, the client issues commands to which the server responds. Each command is assigned with a (relatively) unique, monotonically increasing ID, called the Transaction Number (TXNR). Each response must include that ID. A command and its response is called a RELP transaction.

Refer to Reference [1] for more information.

4.2 Syslog

syslog operates as a client-server protocol, that is, an application transmits logs in cleartext messages to the syslog server. syslog messages can be sent using the User Datagram Protocol (UDP) or TCP. Using the syslog protocol over TCP guarantees that the messages are delivered.

Refer to Reference [2] and Reference [3] for more information.



5 Functions and Procedure Declaration

5.1 RELP

Refer to Reference [1].

5.2 Syslog over TCP

Refer to Reference [2] and Reference [3].



6 Constants Declarations

There are no relevant constants and declarations.



Reference List

- [1] RELP – The Reliable Event Logging Protocol, Rainer Gerhards, <http://www.rsyslog.com/doc/relp.html>
- [2] RFC 5424: The Syslog Protocol, <http://tools.ietf.org/html/rfc5424>
- [3] RFC 6587: Transmission of Syslog Messages over TCP, <https://tools.ietf.org/html/rfc6587>