Oracle® Communications

EAGLE Logging and Visualization Feature User's Guide

Release 47.0
F41414-01
September 2022

ORACLE

Oracle Communications EAGLE Logging and Visualization Feature User's Guide, Release 47.0

F41414-01

Contents

My Oracle Support (MOS)

My Oracle Support (MOS) is your initial point of contact for any of the following requirements:

- **Product Support**:
  The generic product related information and resolution of product related queries.
- **Critical Situations**
  A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:
  - A total system failure that results in loss of all transaction processing capability
  - Significant reduction in system capacity or traffic handling capability
  - Loss of the system's ability to perform automatic system reconfiguration
  - Inability to restart a processor or the system
  - Corruption of system databases that requires service affecting corrective actions
  - Loss of access for maintenance or recovery operations
  - Loss of the system ability to provide any required critical or major trouble notification

  Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.
- **Training Need**
  Oracle University offers training for service providers and enterprises.

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Acronyms

The following table lists the acronyms and terminology used in the document.

Table Acronyms and Terminology

Acronym	Definition
JSON	JavaScript Object Notation
ELK	Elastic-search, Log-stash, and Kibana (Elastic Stack)
UI	User Interface
SCCP	Signaling Connection Control Part
SFAPP	State-full Application
USSD	Unstructured Supplementary Service Data
GTT	Global Title Translation
IMT	Inter-processor Message Transport
OAM	Operations and Management
SM	Service Module
SS7	Signaling System Seven
STP	Signaling Transfer Point
TPS	Transactions per second
UIM	Unsolicited Information Messages
OL7	Oracle Linux version 7
VM	Virtual Machine
TCP	Transmission Control Protocol

What's New in This Guide

This section introduces the documentation updates for Release 47.0 in Oracle Communications EAGLE Logging and Visualization Feature User's Guide.

Release 47.0 -F41414-01, September 2022

- Added Setting up a TCP Connection and Log Messages and UIMs in JSON format sections to update Logging and Visualization feature.

1 Introduction

This chapter contains a brief description of the Logging and Visualization feature of the Oracle Communications EAGLE. The chapter also includes the scope, audience, and organization of the manual; how to find related publications; and how to contact Oracle for assistance.

Overview

This manual describes the Logging and Visualization feature of Oracle Communications EAGLE.

Scope and Audience

This manual is intended for those who maintain and perform administration on the EAGLE. It is assumed that the user is familiar with the SS7 network and its associated protocols. The manual describes commands used in the system, and it contains a special section on debug commands and their descriptions.

Debug commands are a special group of commands used in troubleshooting and debugging the system. These commands are intended for Customer Care Center personnel and authorized engineering personnel in the operating companies. The use of these commands is restricted to those personnel who have access to the “Debug” command class.

References

Refer to Elastic Stack and Product Documentation for information on Elastic Stack-related configuration.

2
Logging and Visualization Feature Description

This chapter provides a functional description of the Logging and Visualization feature.

Overview

EAGLE Logging and Visualization generates and sends log messages and UIMs from the SCCP and SFAPP cards to an external visualization server. The log messages and UIMs are converted into the JSON format with data enrichment for enhanced visualization.

The Logging and Visualization functionality provides the following features:

- Data storage: The Log messages and UIMs are stored with data indexing.
- Search mechanisms: Data search and data filtering are performed through data indexing.
- Dashboards: Information is displayed and analyzed through various dashboards.

In addition, it is important to note the following points with respect to the Logging and Visualization functionality:

- Supports up to 100K TPS with 9 VMs. If two or more VMs are down and not running, TPS gets reduced accordingly. Also, if EAGLE generates JSON over 100K TPS, data may be not reachable to Elastic Search.
- Does not support SLIC with GTT on IPSG application and does not support SMXG cards for visualization.
- Does not log and visualize messages for opcodes, which are not decoded on the EAGLE.

Security Support

For protection against attacks, a comprehensive approach to information security is taken.

The security of a signaling network is analyzed, which allows detection of current vulnerabilities in the network and helps in assessing information security risks.

To keep security configurations up-to-date, threats are detected early, and appropriate measures are taken. Also, it is recommended to ensure continuous monitoring and analysis of vulnerable messages that cross the network.

GSMA recommendations specify the use of a monitoring system, which can perform analysis in real time. This enables detecting phishing or anomalies in a network at an early stage.

Attacks are mostly aimed at gathering a subscriber’s information and network configuration. However, there are attacks that are likely used for fraud, traffic interception, and subscriber availability disruption.

Following are the types of attacks in a network:

- Subscriber information disclosure
- Network information disclosure

- Subscriber traffic interception
- Fraud
- Denial of service

Fraud, traffic interception, and denial of service affect subscribers directly and may lead to significant financial losses, privacy violation, and availability disruption. Subscriber information disclosure means leakage of IMSI, disclosure of location or other data. Certain methods of subscriber traffic interception allow an intruder to tap or redirect terminating and originating calls and intercept user SMS messages. Fraud attacks can be performed against both operators and subscribers.

Subscriber Information Disclosure

Following is the type of information that could be disclosed in a subscriber information disclosure attack:

- IMSI disclosure
- Subscriber location discovery
- Disclosure of subscriber profile information
- Cryptographic material retrieval
- Call details gathering

To obtain routing information about a subscriber during an incoming voice call, the `SendRoutingInfo` message is used. It must be transmitted only within the operator's home network.

To determine a subscriber's location, the `ProvideSubscriberInfo` message is used.

Network Information Disclosure

Network information disclosure is fraught with the leakage of SS7 network configuration data.

To obtain the relevant information, the following two messages are used:

- `AnyTimeInterrogation`
- `SendRoutingInfo`

Both of the messages allow network information disclosure.

Subscriber Traffic Interception

Following are the types of attacks in a subscriber traffic interception:

- Call redirection with interception
- SM interception/monitoring

The message `UpdateLocation` is used to inform the HLR about a change in a mobile switch. Terminating SMSs or calls are intercepted by sending a fake request to register a subscriber in an intruder's network. When a terminating call is received, the operator's network sends a request to a fake network to obtain the subscriber's

roaming number. An attacker can send the number of their telephone exchange in response, and the incoming traffic will be transmitted to the attacker's equipment. After sending another request to register the subscriber in the real network, the attacker can redirect the call to the subscriber's number. As a result, the conversation will pass through the equipment controlled by the attacker.

The same principle is used for the interception of terminating calls via `RegisterSS`. However, in such a case, terminating calls are unconditionally redirected to the intruder's telephone exchange.

Originating calls are tapped by using a similar pattern. The `InsertSubscriberData` message replaces the address of the billing platform in the subscriber's profile stored in the VLR database. When a request is sent to the changed address, the attacker first redirects the originating call to their equipment and then redirects it to the called subscriber. Therefore, the attacker can tap any conversation of the subscriber.

Fraud

Following are the categories into which a fraud can be classified:

- Illegitimate redirection of terminating or originating calls
- USSD request manipulation
- SMS message manipulation or spoofing
- Subscriber profile modification or spoofing
- Online charging evasion

Illegitimate Redirection of Terminating or Originating Calls

An attacker can redirect voice calls of subscribers to premium-rate numbers or to a third-party number. The call will be paid by the subscriber when establishing unconditional redirection, or by the operator when the subscriber is registered in a fake network and the subscriber's roaming number is spoofed.

Calls are redirected by using `UpdateLocation`, `RegisterSS`, `InsertSubscriberData` as well as by using `AnyTimeModification` that allows making changes to a subscriber.

USSD Request Manipulation

An attacker can transfer money from the account of a subscriber or an operator's partners by sending fake USSD requests using the `ProcessUnstructuredSSRequest` message. Also, `UnstructedSSNotify` is used to send notifications to subscribers from various services and the operator.

An attacker can send a fake notification on behalf of a trusted service containing instructions for the subscriber. That may include sending an SMS message to a paid number to subscribe to a service, calling a fake bank number due to suspicious transactions, or following a link to update an application.

SMS Message Manipulation or Spoofing

Phishing or ad messages can be sent on behalf of arbitrary subscribers or services using the `MT-ForwardSM` and the `MO-ForwardSM` methods.

MT-ForwardSM is designed for delivering incoming messages and can be used by attackers to generate forged incoming SMS messages. Unauthorized usage of MO-ForwardSM allows sending messages from subscribers at their expense.

Subscriber Profile Modification or Spoofing

A subscriber's profile stores data about the billing platform and service subscriptions. To bypass a billing system in real time, it is necessary to delete the subscriber's O-CSI subscription, which is used to make originating calls or to substitute the billing system address.

In order to prevent non-fare calls, O-CSI parameters imply that the call must be terminated if the billing platform is unavailable. However, this parameter can be changed, so that the call continues without addressing the platform. As a result, the legitimate platform does not receive information about the calls, and they are not billed.

Denial of Service

Following are the types of attacks in a denial of service attack:

- Service unavailability for subscriber
- Recourses depletion

If the VLR address where the subscriber is currently registered is removed from the HLR via PurgeMS initiated by a certain third-party host, terminating calls cannot be routed to the subscriber's VLR/MSC. The reason is that there is no registration address in the HLR. In such a case, originating calls are available for the subscriber because the registration record in the VLR is not changed.

Rebooting the device does not help to restore the record in the HLR, because the VLR does not initiate the UpdateLocation procedure, assuming that there are no changes in the subscriber's registration data.

It is possible to restore the registration record and the subscriber's availability only by registering in the coverage area of another serving MSC. For example, first manually selecting the network of another operator and then selecting the home network again. Another method is to move to another MSC of the home network.

Supported Message Categories

This chapter mentions the message categories that are supported with EAGLE Logging and Visualization.

Category 1

This category includes messages that should only be received from within the same network and/or are unauthorized at interconnect level, and should not be sent between operators unless there is an explicit bilateral agreement between the operators to do so.

Following is the list of vulnerable category 1 opcodes:

- provideRoamingNumber

- sendParameters
- registerSS
- eraseSS
- activateSS
- deactivateSS
- interrogateSS
- registerPassword
- getPassword
- processUnstructuredSS-Data
- sendRoutingInfo
- sendRoutingInfoForGprs
- sendIdentification
- sendIMSI
- processUnstructuredSS-Request
- unstructuredSS-Request
- unstructuredSS-Notify
- anyTimeModification
- anyTimeInterrogation
- sendRoutingInfoForLCS
- subscriberLocationReport

Category 2

This category includes messages that should only be received from visiting subscribers home network. These should normally only be received from an inbound roamer's home network.

Following is the list of vulnerable category 2 opcodes:

- provideRoamingNumber
- provideSubscriberInfo
- provideSubscriberLocation
- insertSubscriberData
- deleteSubscriberData
- cancelLocation
- getPassword
- reset
- unstructuredSS-Request
- unstructuredSS-Notify
- informServiceCentre

Category 3

This category includes messages that should only be received from the subscriber's visited network. Specifically, MAP packets that are authorized to be sent on interconnects between mobile operators.

Following is the list of vulnerable category 3 opcodes:

- `updateLocation`
- `updateGprsLocation`
- `sendParameters`
- `registerSS`
- `eraseSS`
- `activateSS`
- `deactivateSS`
- `interrogateSS`
- `registerPassword`
- `processUnstructuredSS-Data`
- `mo-forwardSM`
- `mt-forwardSM`
- `beginSubscriberActivity`
- `restoreData`
- `processUnstructuredSS-Request`
- `purgeMS`
- `sendRoutingInfoForSM`
- `sendAuthenticationInfo`
- `reportSmDeliveryStatus`
- `NoteMM-Event`

3

Logging and Visualization Feature Configuration

This chapter describes the procedures for configuring the Logging and Visualization feature in the EAGLE.

Introduction

This chapter identifies the prerequisites and the procedures for configuring the EAGLE Logging and Visualization feature.

Front Panel LED Operation

On the SLIC card, the Ethernet Interface 3 (mapped to port C) is used for visualization connectivity.

The following table captures the LED operations required for the Ethernet interfaces:

Table 3-1 Front Panel LED Operation

IP Interface Status	Signaling Link/connections Status on IP Port 3 (C)	Signaling connection	
		PORT LED	LINK LED
IP Port Not configured	N/A	Off	Off
Card Inhibited			
Cable removed and/or not synced	N/A	Red	Red
Sync	Not configured	Green	Red
Sync and/or act-ip-lnk	Configured but Visualization TCP connection CLOSED (open=no) or disconnected.	Green	Red
	Visualization TCP Connection is ACTIVE (open=yes) and connected.	Green	Green
dact-ip-lnk	N/A	Green	Red

Setting up a TCP Connection

EAGLE generates log messages and UIMs in JSON format. These JSON files are sent from SCCP and SFAPP servers to an external visualization server over a TCP connection.

Perform the following steps to set up a TCP connection:

1. Configure the IP address at port C.
   ```
   Chg-ip-lnk:loc=<loc1>:port=C:ipaddr= <IP address of port C>:submask=<subnetmask>:duplex=full:speed=1000
   ```

2. Configure the default router to change the IP card (applicable only in case of a public IP address).
   `chg-ip-card:loc=<loc1>:defrouter=<defrouter IP>`
3. Assign a hostname to the IP address of port C to configure the local host (in this case, the local hostname is **hsccp**).
   `ent-ip-host:host=hsccp:ipaddr=<IP address of port C>`
4. Assign a hostname to the IP address of the visualization server to configure the remote host (in this case, the remote hostname is **Viz**).
   `ent-ip-host:host=Viz:ipaddr=<IP address of viz server>:type=remote`
5. Assign a name to configure the TCP connection (in this case, the connection name is **conn1**).
   `ent-ip-conn:prot=tcp:lhost=hsccp:lport=<local port>:rhost=Viz:rport=<remote port>:cname=conn1`
6. Change the IP connection and open the newly configured connection.
   `chg-ip-conn:cname=conn1:open=yes`

Log Messages and UIMs in JSON format

After the connection successfully gets set up, EAGLE starts transferring JSON files to external visualization server.

Example of UIM in JSON format:


```
{
        "@timestamp": "2021-10-14T14:31:29.047Z",
        "CDNI": "0",
        "CDTT": "150",
        "CDNP": "6",
        "DPC": "7-030-7",
        "CDSSN": "22",
        "CDRI": "0",
        "CGRI": "1",
        "CGNAI": "",
        "CARD": "1303",
        "CDADDR": "1bb00002970025349819",
        "CGNI": "0",
        "CGPC": "3-110-5",
        "CGNP": "",
        "CGSSN": "22",
        "CGTT": "",
        "CGADDR": "",
        "GTTSET": "",
        "OPC": "3-110-5",
        "CDPC": "",
        "UIM_TEXT": "NP Circular Route detected",
        "SIO": "3",
        "CLLI": "tklc1170501",
        "UIM": "1256",
        "CDNAI": "1",
        "EC": "",
```

```
        "LSET": "ls1216i13"
        }
```

Example of log message in JSON format:

```
{
        "@timestamp": "2021-11-29T17:09:11.545Z",
        "IMSI": "22345670",
        "OPCODE": "updateLocation",
        "CDTT": "31",
        "CDLOC": "-7.92,12.57",
        "CGNAI": "",
        "CAT": "cat3.2",
        "CLLI": "tklc1181001",
        "ASUBTYPE": [      "profileDisclosure",      "callRedirection",
"callInterception",      "smInterception",      "servUnavail"
        ],
        "DISC": "no",
        "CDADDR": "22345670",
        "LSET": "ls1208",
        "ATYPE": [      "intercept",      "fraud"
        ],
        "CDCN": "Mali",
        "OPC": "7-080-7",
        "CGTT": "30",
        "CGADDR": "9899335999",
        "CDNP": "",
        "CDNAI": "",
        "DPC": "2-002-2",
        "CGCN": "Iran",
        "ClSF": "None",
        "MSISDN": "",
        "CGLOC": "51.63,36.13",
        "CGNP": "" }
```

4
Measurements

This chapter describes the measurements that can be collected and generated for Logging and Visualization and the methods that can be used for generating reports for Logging and Visualization measurements.

Logging and Visualization Measurements

Refer to *Measurements Reference* for descriptions of collection methods, measurements, and measurements reports.

Refer to *Commands User's Guide* for descriptions of the commands used to enable and turn on features, turn on measurements collection options, and schedule and generate measurements reports.

The following table lists the Logging and Visualization events:

Table 4-1 Logging and Visualization Measurements

Event Name	SYSTOT Description
VIZUIM	Total number of UIMs sent to visualization server on SCCP cards
VIZMSG	Total number of message sent to visualization server.

5
Maintenance

This chapter describes the maintenance information that is available from the EAGLE for the Logging and Visualization feature. The information includes status, alarms (UAMs), and information messages (UIMs).

Alarms

Refer to *Unsolicited Alarms and Information Messages Reference* for descriptions and corrective procedures associated with EAGLE-related alarms (**UAM**s).

UIMs

Refer to *Unsolicited Alarms and Information Messages Reference* for descriptions of EAGLE UIMs.

The following table lists the UIMs supported for the Logging and Visualization feature:

Table 5-1 Logging and Visualization UIMs

UIM #	Message Text	Output Group
1501	`Visualization connection terminated`	LINK
1502	`Visualization connection established`	LINK

The following table lists the UIM formats that are supported for visualization:

Table 5-2 UIM Format List for Visualization

UIM Format	Format Type
I12	SCCP UDT
I13	SCCP INV TCAP
I14	SCCP Class
I15	SCCP Message
I16	SCCP CDPA
I17	SCCP Routing
I18	SCMG
I38	SCCP INV LENGTH
I39	SCCP INV TCAP W/ DATA
I43	SCCP CDPA for EGTT
I44	SCCP routing for EGTT
I48	GSM MAP Screening

Table 5-2 (Cont.) UIM Format List for Visualization

UIM Format	Format Type
I91	GTT ACTION
I92	MBR MSG
I93	TCAP CDPA

Maintenance Commands

Refer to *Commands User's Guide* for complete descriptions of the commands, including parameters, valid parameter values, rules for using the commands, and output examples.

Debug Commands

The *Commands User's Guide* contains descriptions of debug commands that can be used in assessing and modifying system status and operation. Most of the debug commands are used only under the direction of Oracle support personnel.

Refer to *Commands User's Guide* for complete descriptions of the commands.

Status Reporting and Problem Identification

EAGLE commands can be used to obtain status and statistics for the EAGLE system, system devices including Service Module cards, local subsystems, and SCCP services.

Refer to *Commands User's Guide* for complete descriptions of the commands, including parameters and valid values, rules for using the commands correctly, and output examples.

Refer to *Unsolicited Alarm and Information Messages Reference* for descriptions and recovery procedures for UAMs and UIMs.