

# System Logs

This chapter describes how to configure parameters related to the various types of logging and how to viewing their content. It includes the following sections:


- Feature Summary and Revision History, on page 1
- System Log Types, on page 2
- Configuring Event Logging Parameters, on page 3
- Configuring Active Logs, on page 8
- Specifying Facilities, on page 9
- Configuring Trace Logging, on page 18
- Configuring Monitor Logs, on page 18
- Viewing Logging Configuration and Statistics, on page 19
- Viewing Event Logs Using the CLI, on page 19
- Configuring and Viewing Crash Logs, on page 20
- Reducing Excessive Event Logging, on page 22
- Checkpointing Logs, on page 24
- Saving Log Files, on page 24
- Event ID Overview, on page 26


# Feature Summary and Revision History

## Summary Data

***Table 1: Summary Data***

| | |
|---|---|
| Applicable Product(s) or Functional Area | 5G-UPF |
| Applicable Platform(s) | VPC-SI<br>SMI |
| Feature Default Setting | Disabled – Configuration Required |
| Related Changes in This Release: | Not Applicable |

| | |
|---|---|
| Related Documentation | *UCC 5G UPF Configuration and Administration Guide* |

# Revision History

***Table 2: Revision History***

| Revision Details | Release |
|---|---|
| First introduced. | 2020.02.0 |

# System Log Types

There are five types of logs that can be configured and viewed on the system:

**Important** Not all Event Logs can be configured on all products. Configurability depends on the hardware platform and licenses in use.

- **Event**: Event logging can be used to determine system status and capture important information pertaining to protocols and tasks in use by the system. This is a global function that will be applied to all contexts, sessions, and processes.
- **Active**: Active logs are operator configurable on a CLI instance-by-CLI instance basis. Active logs that are configured by an administrative user in one CLI instance cannot be viewed by an administrative user in a different CLI instance. Each active log can be configured with filter and display properties that are independent of those configured globally for the system. Active logs are displayed in real time as events are generated.
- **Trace**: Trace logging can be used to quickly isolate issues that may arise for a particular connected subscriber session. Traces can be taken for a specific call identification (callid) number, IP address, mobile station identification (MSID) number, or username.
- **Monitor**: Monitor logging records all activity associated with a particular session. This functionality is available in order to comply with law enforcement agency requirements for monitoring capabilities of particular subscribers. Monitors can be performed based on a subscriber's MSID or username.
- **Crash**: Crash logging stores useful information pertaining to system software crashes. This information is useful in determining the cause of the crash.

**Important** Stateful Firewall and NAT supports logging of various messages on screen if logging is enabled for firewall. These logs provide detailed messages at various levels, like critical, error, warning, and debug. Stateful Firewall and NAT attack logs also provide information on the source IP address, destination IP address, protocol, or attack type for any packet dropped due to an attack and are also sent to a syslog server if configured in the system. For more information on logging support for Stateful Firewall and NAT, see the *Logging Support* chapter of *PSF Administration Guide* or *NAT Administration Guide*.

# Configuring Event Logging Parameters

The system can be configured to generate logs based on user-defined filters. The filters specify the facilities (system tasks or protocols) that the system is to monitor and severity levels at which to trigger the generation of the event entries.

Event logs are stored in system memory and can be viewed via the CLI. There are two memory buffers that store event logging information. The first buffer stores the active log information. The second buffer stores inactive logging information. The inactive buffer is used as a temporary repository to allow you to view logs without having data be overwritten. Logs are copied to the inactive buffer only through manual intervention.

Each buffer can store up to 50,000 events. Once these buffers reach their capacity, the oldest information is removed to make room for the newest.

To prevent the loss of log data, the system can be configured to transmit logs to a syslog server over a network interface.

## Configuring Event Log Filters

You can filter the contents of event logs at the Exec mode and Global Configuration mode levels.

### Exec Mode Filtering

These commands allow you to limit the amount of data contained in logs without changing global logging parameters.

Follow the examples below to filter logs via Exec mode commands.

#### Active Filtering

**logging active [ copy runtime filters ] [ event-verbosity** *event_level* **] [ pdu-data** *format* **] [ pdu-verbosity** *pdu_level* **]**

Notes:

- **copy runtime filters** – Copies the runtime filters and uses that copy to filter the current logging session.
- **event-verbosity** *event_level* – Specifies the level of verboseness to use in logging of events as one of:
  - *min* – Displays minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
  - *concise* – Displays detailed information about the event, but does not provide the event source within the system.
  - *full* – Displays detailed information about event, including source information, identifying where within the system the event was generated.
- **pdu-data** *format* – Specifies output format for packet data units when logged as one of:
  - *none* – raw format (unformatted).
  - *hex* – hexadecimal format
  - *hex-ascii* – hexadecimal and ASCII similar to a main-frame dump

- **pdu-verbosity** *pdu_level* – Specifies the level of verboseness to use in logging of packet data units as an integer from 1 through 5, where 5 is the most detailed.

### Disable or Enable Filtering by Instance(s)

**logging filter active facility** *facility* **level** *severity_level* **[ critical-info | no-critical-info ]**

**logging filter { disable | enable } facility** *facility* **{ all | instance** *instance_number* **}**

Notes:

- **active** – Indicates that only active processes are to have logging options set.
- **disable** – Disables logging for a specific instance or all instances. This keyword is only supported for aaamgr, hamgr and sessmgr facilities.
- **enable** – Enables logging for a specific instance or all instances. This keyword is only supported for aaamgr, hamgr and sessmgr facilities. By default logging is enabled for all instances of aaamgr, hamgr and sessmgr.
- **facility** *facility* and **level** *severity_level* – Configure the logging filter that determines which system facilities should be logged and at what levels.
- **all | instance** *instance_number* – Specifies whether logging will be disabled or enabled for all instances or a specific instance of aaamgr, hamgr or sessmgr. Run the **show session subsystem facility** *facility* command to identify specific instance numbers.

**Note** These keywords are only supported with the **disable** and **enable** keywords.

- **level** *severity_level* – Specifies the level of information to be logged from the following list which is ordered from highest to lowest:
  - critical - display critical events
  - error - display error events and all events with a higher severity level
  - warning - display warning events and all events with a higher severity level
  - unusual - display unusual events and all events with a higher severity level
  - info - display info events and all events with a higher severity level
  - trace - display trace events and all events with a higher severity level
  - debug - display all events

**Note** This keyword is only supported in conjunction with the **active** keyword.

- **critical-info** – Specifies that events with a category attribute of critical information are to be displayed. Examples of these types of events can be seen at bootup when system processes and tasks are being initiated. This is the default setting.

  **no-critical-info** – Specifies that events with a category attribute of critical information are not to be displayed.

**Note** These keywords are only supported in conjunction with the **active** keyword.

**Important** To enable logging of a single instance of a facility, you must first disable all instances of the facility (**logging filter disable facility** *facility* **all**) and then enable logging of the specific instance (**logging filter enable facility** *facility* **instance** *instance_number*. To restore default behavior you must re-enable logging of all instances (**logging filter enable facility** *facility* **all**).

You can display the instance numbers for enabled instances per facility using the Exec mode **show instance-logging** command.

## Global Configuration Mode Filtering

You can filter the contents of event logs at the Exec mode and Global Configuration mode levels.

Follow the example below to configure run time event logging parameters for the system:

```
configure
   logging filter runtime facility facility level report_level
   logging display { event-verbosity | pdu-data | pdu-verbosity }
   end
```

Notes:

- **facility** *facility* and **level** *severity_level* – Configure the logging filter that determines which system facilities should be logged and at what levels.
- Repeat for every facility that you would like to log.
- *Optional:* Configure event ID restrictions by adding the **logging disable eventid** command. The system provides the ability to restrict the sending of a specific event ID or a range of event IDs to minimize the amount of data logged to that which is most useful. Repeat to disable logging for additional event IDs or event ID ranges.
- If an administrator restricts event logging for an Event ID or Event ID range using the above command (**logging disable eventid** ), the system will generate a Critical Event log "cli 30999 critical" as well as an SNMP trap "1361 (DisabledEventIDs)" with the specific Event IDs or Event ID range that was disabled.

  These event logs and traps are enabled by default in this release, and cannot be disabled.
- If an administrator lowers the logging level (using the **logging filter runtime facility *facility* level *report_level*** command below the default level of "error", the system will generate a Critical Event log "cli 30998 critical" as well as an SNMP trap "1362 (LogLevelChanged)" with the specific Event IDs or Event ID range that was disabled.

  These event logs and traps are enabled by default in this release, and cannot be disabled.

The following examples show the CLI output of the traps generated when event logging or logging levels are changed.

```
show snmp trap statistics
SNMP Notification Statistics:
  ...
Trap Name                          #Gen #Disc  Disable Last Generated
---------------------------------- ----- -----  ------- --------------------
…
DisabledEventIDs                      1     0       0  2021:05:11:15:35:25
LogLevelChanged                       2     0       0  2021:05:11:15:28:03
```

```
show snmp trap history
There are x historical trap records (5000 maximum)

Timestamp                Trap Information
-------------------------
```

```
…
Thu May 11 15:28:03 2021 Internal trap notification 1362 (LogLevelChanged) Logging level
of facility resmgr is changed to critical by user #initial-config# context local privilege
 level Security Administrator ttyname /dev/pts/0 address type IPV4 remote ip address
209.165.202.129
…
Thu May 11 15:35:25 2021 Internal trap notification 1361 (DisabledEventIDs) Event IDs from
 100 to 1000 have been disabled by user adminuser context context privilege level security
 administrator ttyname tty address type IPV4 remote ip address 209.165.202.134
…
Mon May 15 10:14:56 2021 Internal trap notification 1362 (LogLevelChanged) Logging level
of facility sitmain is changed to critical by user staradmin context local privilege level
 Security Administrator ttyname /dev/pts/1 address type IPV4 remote ip address 209.165.202.120
```

# Configuring Syslog Servers

### Syslog Architecture

System Logging (syslog) is the architecture which produces and sends event information from the MSUP over the UDP transport layer to a centralized Event Message Collector. Syslog uses a client/server architecture:

- **Syslog Client:** A set of processes running on UPF, which operate as the sending device for event messages.
- **Syslog Server:** An external server configured to receive the event messages sent from the MSUP.

MSUP transports event messages using the Syslog Protocol without expecting acknowledgment of receipt. The system forwards event messages regardless if a Syslog Server is available to receive the messages.

### Configuring the System to Sent Event Messages to an External Syslog Server

Information that is generated by the run time event logging filters can be transmitted to a syslog server for permanent storage.



**Important** The data transmitted to the Syslog server is meant to be used for informational purposes. Functions such as billing and performance monitoring should not be based on syslogs.



**Important** Although the system provides the flexibility to configure syslog servers on a context-by-context basis, it is recommended that all servers be configured in the *local* context in order to isolate the log traffic from the network traffic.

Use the following example to configure syslog servers:

```
configure
   context  context_name
logging syslog ip_address [ event-verbosity { min | concise | full } |
facility facilities |  msg-format { rfc3164 | rfc5424 } | pdu-data { none
| hex | hex-ascii } | pdu-verbosity pdu_level |  port number  |  rate value
]
     end
```

**NOTES:**

- **syslog** *ip_address*: Specifies the IP address of a system log server on the network in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
- **event-verbosity { min | concise | full }**: Specifies the level of detail to use in logging of events. Detail level must be one of the following:
  - **min**: Displays minimal detail.
  - **concise**: Displays summary detail.
  - **full**: Displays full detail.
- **facility** *facilities*: Specifies the local facility for which the system logging server's logging options are applied. Local facility must be one of the following:
  - **local0**—Pertains to syslog severity level of 0, Emergency
  - **local1**—Pertains to syslog severity level of 1, Alert
  - **local2**—Pertains to syslog severity level of 2, Critical
  - **local3**—Pertains to syslog severity level of 3, Error
  - **local4**—Pertains to syslog severity level of 4, Warning
  - **local5**—Pertains to syslog severity level of 5, Notice
  - **local6**—Pertains to syslog severity level of 6, Informational
  - **local7**—Pertains to syslog severity level of 7, Debug

  Default: **local7**

  If local facility is not specified, then **local7** is applied by default.

  Multiple system log servers can share the logging options of a given local facility. This allows for the logical grouping of system log servers and the options which affect all of those associated with the same local facility.
- **msg-format { rfc3164 | rfc5424 }**: Configures the message format for each system log server as per RFC3164 or RFC5424. Default: rfc3164.

- **pdu-data { none | hex | hex-ascii }**: Specifies output format for packet data units when logged. Format must be one of the following:
  - **none**: Displays data in raw format.
  - **hex**: Displays data in hexadecimal format.
  - **hex-ascii**: Displays data in hexadecimal and ASCII format (similar to a mainframe dump).
- **pdu-verbosity** *pdu_level*: Specifies the level of verboseness to use in logging of packet data units as a value from 1 through 5, where 5 is the most detailed.
- **port** *number* : Specifies an alternate port number for the system log server. Default: 514.

  *number* must be an integer value from 1 through 65535.
- **rate** *value*: Specifies the rate at which log entries are allowed to be sent to the system log server. No more than the number specified by *value* is sent to a system log server within any given one-second interval.

  *value* must be an integer from 0 through 100000. Default: 1000
- Repeat as necessary to configure extra syslog servers. There is no limit to the number of syslog servers that can be configured.

# Configuring Active Logs

Active logs are event logs that are operator configurable on a CLI instance-by-CLI instance basis. Active logs configured by an administrative user in one CLI instance are not displayed to an administrative user in a different CLI instance. Each active log can be configured with filter and display properties that are independent of those configured globally for the system. Active logs are displayed in real time as they are generated.

Active logs are not written to the active memory buffer by default. To write active logs to the active memory buffer execute the following command in the Global Configuration mode:

```
logging runtime buffer store all-events
```

When active logs are written to the active memory buffer, they are available to all users in all CLI instances.

Use the following example to configure active logging in Global Configuration mode:

```
logging filter runtime facility facility level report_level
```

NOTES:

- Configure the logging filter that determines which system facilities should be logged and at what levels.
- Repeat for every facility that you want to log.
- *Optional:* Configure event ID restrictions by adding the **logging disable eventid** command. The system provides the ability to restrict the sending of a specific event ID or a range of event IDs to minimize the amount of data logged to that which is most useful. Repeat to disable logging for more event IDs or event ID ranges.

Once all the necessary information has been gathered, the Active log display can be stopped by entering the following command in the EXEC mode:

```
no logging active
```

# Specifying Facilities

The following facilities can be configured for logging event data:

- **a10**: A10 interface logging facility
- **a11**: A11 interface logging facility
- **a11mgr**: A11 Manager logging facility
- **aaa-client** : Accounting and authentication client logging facility
- **aaamgr**: Accounting and authentication manager logging facility
- **aaaproxy**: AAAProxy logging facility
- **aal2**: AAL2 protocol logging facility
- **acl-log**: Access Control List logging facility
- **acsctrl**: Active charging Subsystem Controller
- **acsmgr**: Active charging Subsystem Manager
- **alarmctrl**: Alarm Controller logging facility
- **alcap**: ALCAP protocol logging facility
- **alcapmgr**: ALCAPMgr logging facility
- **all**: All facilities
- **apimgr**: API Manager logging facility
- **bfd**: BFD protocol logging facility
- **bgp**: BGP protocol logging facility
- **bindmux**: IPCF BindMux Manager
- **bngmgr**: BNGMGR (BNG DemuxMgr) logging facility
- **bssap+**: Bssap+ logging facility
- **bssgp**: BSSGP Protocol logging facility
- **bulkstat**: Statistics logging facility
- **cactrl**: CACTRL application logging facility
- **callhome**: CALLHOME application logging facility
- **cap**: CAP Protocol logging facility
- **cbsmgr**: CBSMGR logging facility
- **cdf**: CDF logging facility

- **cfctrl**: Content filtering controller
- **cfgmgr**: Config manager logging facility
- **cfmgr**: Content filtering manager
- **cgw**: Converged Gateway facility
- **chmgr**: Checkpoint Manager logging facility
- **cli**: CLI logging logging facility
- **cmp**: CMPv2 logging facility
- **confdmgr**: ConfD Manager - Proclet for communication with confd
- **connectedapps**: CONNECTEDAPPS library logging facility
- **connproxy**: Connection Proxy logging facility
- **credit-control**: Credit Control facility
- **cscf**: IMS/MMD CSCF
- **cscfcpmgr**: CSCFCPMGR logging facility
- **cscfmgr**: SIP CSCF Manager facility
- **cscfnpdb**: CSCF NPDB logging facility
- **cscfrtcp**: MS/MMD CSCF RTCP log facility
- **cscfrtp**: IMS/MMD CSCF RTP log facility
- **cscfttmgr**: SIP CSCFTT Manager facility
- **csp**: Card Slot Port controller logging facility
- **css**: CSS facility
- **css-sig**: CSS RADIUS Signaling facility
- **cx-diameter**: Cx Diameter messages
- **data-mgr**: Data Manager Framework logging facility
- **dcardctrl**: Daughtercard Controller logging facility
- **dcardmgr**: Daughtercard Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol logging facility
- **dhcpv6**: DHCPV6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages
- **diactrl**: Diactrl proclet logging

- **diameter**: Diameter endpoint logging facility
- **diameter-acct** : Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ECS Diameter signaling
- **diameter-engine** : Diameterv2 engine logging facility
- **diameter-hdd**: Diameter HDD Interface
- **diameter-svc**: Diameter Service
- **diamproxy** : DiamProxy logging facility
- **doulosuemgr**: Doulos UE Manager facility
- **dpath**: IPSEC Data Path logging facility
- **drvctrl**: Driver Controller logging facility
- **eap-ipsec** : EAP
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface Logging facility
- **egtpc**: EGTP Control plane
- **egtpmgr**: EGTP Demux manager
- **egtpu**: EGTP User plane
- **embms**: eMBMS Gateway facility
- **emctrl**: Element Manager Controller logging facility
- **epdg**: EPDG logging facility
- **event-notif** : Event Notification Interface logging facility
- **evlog**: Event-logger logging facility
- **famgr**: Foreign Agent manager logging facility
- **fapi**: VPP Fastpath API logging facility
- **femgr**: Forwarding Element Manager logging facility
- **firewall**: Firewall logging facility
- **fng**: FNG logging facility
- **gbmgr**: SGSN Gb Interface Manager facility
- **gmm**: GMM Protocol logging facility
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS-NS Protocol logging facility

- **gq-rx-tx-diameter** : Gq/Rx/Tx Diameter messages
- **gss-gcdr**: GSS GCDR facility
- **gtpc**: GTP-C Protocol logging facility
- **gtpcmgr**: GTP-C Protocol Manager logging facility
- **gtpp**: GTP-PRIME Protocol logging facility
- **gtpu**: GTP-U Protocol logging facility
- **gtpumgr**: GTPU Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages
- **gy-diameter**: Gy Diameter messages
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task process logging facility
- **hdctrl**: HD Controller logging facility
- **henbapp**: HENB App facility
- **henbgw** : HENBGW facility
- **henbgw-pws**: Henbgw Public Warning System Data logging facility
- **henbgw-sctp-acs**: HENBGW access sctp facility
- **henbgw-sctp-nw**: HENBGW network sctp facility
- **henbgwdemux**: HENBGW Demux facility
- **henbgwmgr**: ENBGW Manager facility
- **hnb-gw** : HNB-GW (3G Femto GW) logging facility
- **hnbmgr**: HNBMGR (3G Femto GW DemuxMgr) logging facility
- **hss-peer-service**: HSS Peer Service facility
- **iftask**: iftask logging facility
- **igmp**: IGMP
- **ikev2**: IKEv2
- **ims-authorizatn**: IMS Authorization Service facility
- **ims-sh**: HSS SH Service facility
- **imsimgr** : SGSN IMSI Manager facility
- **imsue**: IMSUE
- **ip-arp** : IP Address Resolution Protocol logging facility
- **ip-interface**: IP interface logging facility
- **ip-route** : IP route logging facility

- **ipms** :IPMS logging facility
- **ipne**: IPNE facility
- **ipsec**: IP Security logging facility
- **ipsecdemux**: IPsecdemux logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Service Gateway facility
- **kvstore**: KV Store facility
- **l2tp-control**: L2TP Protocol Control logging facility
- **l2tp-data**: L2TP Protocol Data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Protocol Manager logging facility
- **lagmgr**: LAGMGR logging facility
- **lcs**: LCS Service logging facility
- **ldap**: LDAP Messages
- **li**: Lawful intercept logging facility
- **linkmgr**: SGSN/SS7 Links Manager facility
- **llc**: LLC Protocol logging facility
- **lmisf**: Lmisf logging facility
- **local-policy**: Local Policy Service facility
- **location-service** : Location Service facility
- **m3ua** : M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway logging facility
- **map**: MAP Protocol logging facility
- **mcctrl**: SDN Mobility Controller - Controller logging facility
- **mcdemux**: SDN Mobility Controller - DEMUX logging facility
- **mcmgr**: SDN Mobility Controller - Manager logging facility
- **megadiammgr**: Megadiameter Manager (SLF Service)
- **mme-app**: MME application facility
- **mme-misc** : MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager facility
- **mmemgr**: MME Manager facility
- **mmgr**: Primary Manager logging facility

- **mobile-ip**: Mobile IP control logging facility
- **mobile-ip-data**: Mobile IP data logging facility
- **mobile-ipv6**: Mobile IPv6 control logging facility
- **mpls**: MPLS protocol logging facility
- **mrme**: MRME logging facility
- **mseg-app**: MSEG application logging facility
- **mseg-gtpc**: MSEG GTPC application logging facility
- **mseg-gtpu**: MSEG GTPU application logging facility
- **msegmgr**: MSEGMGR (MSEG DemuxMgr) logging facility
- **msgproxy**: Messege Proxy logging facility
- **mtp2** : MTP2 Service logging facility
- **mtp3**: MTP3 Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **nas**: NAS 4G Protocol logging facility
- **npuctrl**: Network Processor Unit Control logging facility
- **npumgr**: Network Processor Unit Manager logging facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-drv**: NPUMGR DRV logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init** : NPUMGR INIT logging facility
- **npumgr-lc**: NPUMGR LC logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **npumgr-rri** : NPUMGR RRI logging facility
- **npumgr-vpn**: NPUMGR VPN logging facility
- **npusim**: NPUSIM logging facility
- **nrfmgr**: NRF Manager logging facility
- **nsh**: NSH logging facility
- **ocsp**: OCSP logging facility
- ospf: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility

- **p2p**: Peer-to-Peer detection logging facility
- **pagingmgr**: PAGINGMGR logging facility
- **pccmgr**: IPCF PCC Manager library
- **pdg**: PDG logging facility
- **pdif**: PDIF logging facility
- **pgw**: PDN Gateway facility
- **plugin**: Plugin logging facility
- **pmm-app** : PMM application logging facility
- **ppp**: PPP link and packet logging facility
- **pppoe**: PPPOE logging facility
- **proclet-map-frwk**: Proclet mapping frameowrk logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect logging facility
- **ranap**: RANAP Protocol logging facility
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Rf Diameter messages
- **rip**: RIP protocol logging facility
- **rlf**: RLF logging facility
- **rohc**: RObust Header Compression
- **rsvp**: Reservation Protocol logging facility
- **rua**: RUA (3G Femto GW - RUA messages) logging facility
- **s102**: S102 protocol logging facility
- **s102mgr**: S102Mgr protocol logging facility
- **s1ap**: S1AP Protocol logging facility
- **sabp**: SABP logging facility
- **saegw**: SAE Gateway facility
- **sbc**: SBc protocol logging facility
- **sccp**: SCCP Protocol logging facility

- **sct**: Shared Configuration Task logging facility
- **sctp**: SCTP Protocol logging facility
- **sef_ecs**: sef apis printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: Session trace logging facility
- **sfcctrl**: Service Funcion Chain Controller logging facility
- **sfcmgr**: Service Funcion Chain Manager logging facility
- **sft**: Switch Fabric Task logging facility
- **sgmbmgr**: eMBMS Gateway Demux facility
- **sgs**: SGs protocol logging facility
- **sgsn-app**: SGSN-APP interface logging facility
- **sgsn-failures**: SGSN call failures logging facility
- **sgsn-gtpc** : SGSNs GTP-C Protocol logging facility
- **sgsn-gtpu** : SGSNs GTP-U Protocol logging facility
- **sgsn-mbms-bearer** : SGSNs MBMS bearer app (SMGR) logging facility
- **sgsn-misc**: SGSN miscellaneous logging facility
- **sgsn-system** : SGSNs System Components logging facility
- **sgsn-test**: SGSN Tests logging facility
- **sgtpcmgr**: SGSN GTPC Manager facility
- **sgw**: Serving Gateway facility
- **sh-diameter** : Sh Diameter messages
- **sitmain**: System Initialization Task main logging facility
- **slmgr**: Smart License Manager logging facility
- **sls**: SLs protocol logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: SMS Service logging facility
- **sndcp**: SNDCP Protocol logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF SPR Manager library
- **srdb**: Static Rating Database

- **srp**: Service Redundancy Protocol logging facility
- **sscfnni**: SSCFNNI Protocol logging facility
- **sscop**: SSCOP Protocol logging facility
- **ssh-ipsec**: SSH IP Security logging facility
- **ssl**: SSL (Secure socket layer messages) logging facility
- **stat**: Statistics logging facility
- **supserv**: Suplementary Services logging facility
- **sx**: SX Manager logging facility
- **sxdemux**: SX Demux Manager logging facility
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **tcpdemux**: TCP Demux Manager logging facility
- **testctrl**: Test Controller logging facility
- **testmgr**: Test Manager logging facility
- **threshold**: Threshold logging facility
- **tsmon**: Traffic Steering Monitor Server facility
- **ttg**: TTG logging facility
- **tucl**: TUCL logging facility
- **udr**: UDR facility
- **uplane**: User Plane logging facility
- **user-data** : User Data logging facility
- **user-l3tunnel**: User layer-3 tunnel logging facility
- **usertcp-stack**: User Tcp Stack
- **vnfma** : VNFM Proxy Agent logging facility
- **vpn**: Virtual Private Network logging facility
- **vpp** : vpp logging facility
- **wimax-data** : WiMAX DATA
- **wimax-r6**: WiMAX R6
- **wsg**: WSG logging facility
- **x2gw-app** : X2GW application logging facility
- **x2gw-demux**: X2GW demux task logging facility

# Configuring Trace Logging

Trace logging is useful for quickly resolving issues for specific sessions that are currently active. They are temporary filters that are generated based on a qualifier that is independent of the global event log filter configured using the **logging filter** command in the Exec mode. Like event logs, however, the information generated by the logs is stored in the active memory buffer.

All debug level events associated with the selected call are stored.



**Important** Trace logs impact session processing. They should be implemented for debug purposes only.

Use the following example to configure trace logs in the Exec mode:

**logging trace { callid** *call_id* **| ipaddr** *ip_address* **| msid** *ms_id* **| username** *username* **}**

Once all of the necessary information has been gathered, the trace log can be deleted by entering the following command:

**no logging trace { callid** *call_id* **| ipaddr** *ip_address* **| msid** *ms_id* **| username** *username* **}**

# Configuring Monitor Logs

Monitor logging records all activity associated with all of a particular subscriber's sessions. This functionality is available in compliance with law enforcement agency requirements for monitoring capabilities of particular subscribers.

Monitors can be performed based on a subscriber's MSID or username, and are only intended to be used for finite periods of time as dictated by the law enforcement agency. Therefore, they should be terminated immediately after the required monitoring period.

This section provides instructions for enabling and disabling monitor logs.

## Enabling Monitor Logs

Use the following example to configure monitor log targets:

```
configure
  logging monitor { ip_addr | ipv6_addr | msid id | username name }
  end
```

Repeat to configure additional monitor log targets.

## Disabling Monitor Logs

Use the following example to disable monitor logs:

```
configure
  no logging monitor { ip_addr | ipv6_addr | msid id | username name }
  end
```

# Viewing Logging Configuration and Statistics

Logging configuration and statistics can be verified by entering the following command from the Exec mode:

```
show logging [ active | verbose ]
```

When no keyword is specified, the global filter configuration is displayed as well as information about any other type of logging that is enabled.

The following table provides information and descriptions of the statistics that are displayed when the **verbose** keyword is used.

***Table 3: Logging Configuration and Statistics Commands***

| Field | Description |
|---|---|
| **General Logging Statistics** | |
| Total events received | Displays the total number of events generated by the system. |
| Number of applications receiving events | Displays the number of applications receiving the events. |
| **Logging Source Statistics** | |
| Event sequence ids by process | Displays a list of system processes that have generated events and the reference identification number of the event that was generated. |
| Msg backlog stat with total cnt | Displays the number of event messages that have been back logged in comparison to the total number of events generated. |
| LS L2 filter drop rate | Displays the percentage of logging source (LS) layer 2 (L2) event drops. |
| Abnormal Log Source Statistics | Displays abnormal logging source (LS) statistics, if any. |
| **Runtime Logging Buffer Statistics** | |
| Active buffer | Displays the number of events currently logged in the active memory buffer and a timestamp for the oldest and most recent entries in the buffer. |
| Inactive buffer | Displays the number of events currently logged in the inactive memory buffer. |

# Viewing Event Logs Using the CLI

Event logs generated by the system can be viewed in one of the following ways:

- **From the syslog server:** If the system is configured to send logs to a syslog server, the logs can be viewed directly on the syslog server.
- **From the system CLI:** Logs stored in the system memory buffers can be viewed directly from the CLI.

- **From the console port:** By default, the system automatically displays events over the console interface to a terminal provided that there is no CLI session active.

This section provides instructions for viewing event logs using the CLI. These instructions assume that you are at the root prompt for the Exec mode.

### Procedure

**Step 1** Copy the active log memory buffer to the inactive log memory buffer.

When the active log memory buffer is copied to the inactive log memory buffer existing information in the inactive log memory buffer is deleted.

Both active and inactive event log memory buffers can be viewed using the CLI in Exec mode. However, it is preferable to view the inactive log in order to prevent any data from being over-written. The information from the active log buffer can be copied to the inactive log buffer by entering the following command:

```
logs checkpoint
```

**Step 2** View the logs by entering the following command:

```
show logs
```

# Configuring and Viewing Crash Logs



**Note** In the CN-5G 2025.02 release, crash enable URL is not configured, crash cores will be placed at `/var/lib/systemd/coredump/`

In the unlikely even of a software crash, the system stores information that could be useful in determining the reason for the crash. This information can be maintained in system memory or it can be transferred and stored on a network server.

The system supports the generation of the following two types of logs:

- **Crash log:** Crash logs record all possible information pertaining to a software crash (full core dump). Due to their size, they can not be stored in system memory. Therefore, these logs are only generated if the system is configured with a Universal Resource Locator (URL) pointing to a local device or a network server where the log can be stored.
- **Abridged crash log:** Crash event records are automatically generated when a software crash occurs and are stored in flash memory on management cards. The abridged crash log contains a list crash event records along with associated dump files. This log allows you to view event records and dump files via CLI commands.

# Crash Logging Architecture

The crash log is a persistent repository of crash event information. Each event is numbered and contains text associated with a CPU (minicore), NPU, or kernel crash. The logged events are recorded into fixed-length records and stored in /flash/crashlog2.

Whenever a crash occurs, the following crash information is stored:

1. The event record is stored in /flash/crashlog2 file (the crash log).
2. The associated minicore, NPU, or kernel dump file is stored in the /flash/crsh2 directory.
3. A full core dump is stored in a user-configured directory.

# Configuring Software Crash Log Destinations

The system can be configured to store software crash log information to any of the following locations:

- On VPC
  - **Flash memory:** Accessible by the virtual machine
  - **USB memory stick:** Installed in the USB slot of the platform (USB slot has been enabled via the hypervisor)
- **Network Server:** Any workstation or server on the network that the system can access using the Trivial File Transfer Protocol (TFTP), the File Transfer Protocol (FTP), the Secure File Transfer Protocol (SFTP), or the Hyper-Text Transfer Protocol (HTTP); this is recommended for large network deployments in which multiple systems require the same configuration

Crash log files (full core dumps) are written with unique names as they occur to the specified location. The name format is *crash-card-cpu-time-core*. Where *card* is the card slot, *cpu* is the number of the CPU on the card, and *time* is the Portable Operating System Interface (POSIX) timestamp in hexadecimal notation.

Use the following example to configure a software crash log destination in the Global Configuration mode:

```
configure
  crash enable [ encrypted ] url crash_url
  end
```

NOTES:

- Repeat to configure additional software crash log destinations. There is no limit to the number of destinations that can be configured.

# Viewing Abridged Crash Log Information Using the CLI

You can view abridged crash information that is stored as a set of event records in flash memory on management cards (**/flash/crashlog2**). Each crash event record has an associated dump file (minicore, NPU or kernel) that can also be displayed (**/flash/crsh2**)

Follow the instructions in this section to view software crash events that have occurred on the system. These instructions assume that you are at the root prompt for the Exec mode.

### Procedure

**Step 1** View a list of software crash events by entering the following Exec mode command:

**show crash { all | list | number** *crash_num* **}**

NOTES:

- Run **show crash list** to obtain the number for a specific crash event.
- Run **show crash number** *crash_num* to display the output for the target crash event.

The resulting output may not be the same for all platforms:

Information about similar crash events is suppressed in the output of this command.

**Step 2** View the dump file associated with a specific crash event.

The information contained in the dump file helps identify and diagnose any internal or external factors causing the software to crash.

- Crash # – unique number assigned by StarOS when logging the crash event
- SW Version – StarOS build release in format: RR.n(bbbbb)
- Similar Crash Count – number of similar crashes
- Time of first crash – timestamp when first crash occurred in format: YYYY-MMM-DD+hh:mm:ss
- Failure message – text of event message
- Function – code identifier
- Process – where the crash occurred (Card, CPU, PID, etc.)
- Crash time – timestamp for when the crash occurred in the format: YYYY-MMM-DD+hh:mm:ss time zone
- Recent errno – text of most recent error number.
- Stack – memory stack information
- Last Bounce – information about the messaging received prior to the crash
- Registers – memory register contents
- Current inbound message – hexadecimal information for the current inbound message
- Address Map
- Recent heap activity (oldest first)
- Recent events (oldest first)
- Profile depth

# Reducing Excessive Event Logging

Event logging (evlogd) is a shared medium that captures event messages sent by StarOS facilities. When one or more facilities continuously and overwhelmingly keep sending a high volume of event messages, the

remaining non-offender facilities are impacted. This scenario degrades system performance, especially as the number of facilities generating logs increases.

Rate-control of event message logging is handled in the Log Source path. Essentially, every second a counter is set to zero and is incremented for each log event that is sent to evlogd. If the count reaches a threshold before the second is up, the event is sent, queued, or dropped (if the evlogd messenger queue is full).

When any facility exceeds the upper threshold set with this command for the rate of message logging and remains in the same state for prolonged interval, StarOS notifies the user through an SNMP trap or alarm.

A new threshold command allows you to specify the percentage of facility event queue full. When this threshold is exceeded, an SNMP trap and alarm are generated that specifies the offending facility.

The formats for the SNMP traps that are associated with this command are as follows:

- **ThreshLSLogsVolume**

```
<timestamp> Internal trap notification <trap_id> (ThreshLSLogsVolume) threshold
<upper_percent>%
measured value <actual_percent>% for facility <facility_name> instance <instance_id>
```

- **ThreshClearLSLogsVolume**

```
<timestamp> Internal trap notification <trap_id> (ThreshClearLSLogsVolume) threshold
<upper_percent>%
measured value <actual_percent>% for facility <facility_name> instance <instance_id>
```

If a trigger condition occurs within the polling interval, the alert or alarm is not generated until the end of the polling interval.

Both traps can be enabled or suppressed through the Global Configuration mode **snmp trap** command.

# Configuring Log Source Thresholds

There are three Global Configuration mode commands associated with configuring and implementing Log Source thresholds.

1. **threshold ls-logs-volume** – sets the parameters for the upper and lower thresholds for generating and clearing traps/alarms respectively.
2. **threshold poll ls-logs-volume interval** – establishes the polling interval for this threshold.
3. **threshold monitoring ls-logs-volume** – turns monitoring of this threshold on and off.

Use the following example to configure syslog servers:

```
configure
  [ default ] threshold ls-logs-volume upper_percent [ clear lower_percent ]
  [ default ] threshold poll ls-logs-volume interval duration
  [ no ] threshold monitoring ls-logs-volume
  end
```

Notes:

- *upper_percent* and *lower_percent* are expressed as integers from 0 to 100. Default value for *upper_percent* is 90%. If *lower_percent* is not specified, the default clear value is *upper_percent*.
- **threshold poll ls-logs-volume interval** sets the polling interval in seconds. The default interval is 300 seconds (5 minutes).

- **threshold monitoring ls-logs-volume** enables or disables this feature.

You can verify the configuration of this threshold by running the Exec mode **show threshold** command.

# Checkpointing Logs

Checkpointing identifies logged data as previously viewed or marked. Checkpointing allows you to only display log information since the last checkpoint.

Individual logs may have up to 50,000 events in the active log. Checkpointing the logs results in at most 50,000 events being in the inactive log files. This gives a maximum of 100,000 events in total which are available for each facility logged.

Checkpoint log data through the EXEC mode logs checkpoint command to set the log contents to a well-known point prior to special activities taking place. This command may also be a part of periodic regular maintenance to manage log data.

Checkpointing logs moves the current log data to the inactive logs. Only the most recently check pointed data is retained in the inactive logs. A subsequent check pointing of the logs results in the prior check pointed inactive log data being cleared and replaced with the newly check pointed data. Checkpointed log data is not available for viewing.



**Important** Checkpointing logs should be done periodically to prevent the log files becoming full. Logs which have 50,000 events logged discard the oldest events first as new events are logged.

# Saving Log Files

Log files can be saved to a file in a local or remote location specified by a URL. Use the following EXEC mode command to save log files:

**save logs** { *url* } **[ active ] ] [ inactive ] [ callid** *call_id* **]**
**[event-verbosity** *evt_verboseness* **] [ facility** *facility* **] [level** *severity_level* **]**
**[ pdu-data** *pdu_format* **] [ pdu-verbosity** *pdu_verboseness* **] [ since** *from_date_time*
**[ until** *to_date_time* **] ] [ | { grep** *grep_options* **| more** } **]**

OPTIONS:

- *url*: Specifies the location to store the log file(s). *url* may refer to a local or a remote file and must be entered in the following format.
- **active**: Saves data from active logs.
- **inactive**: Saves data from inactive logs.
- **callid** *call_id*: Specifies a call ID for which log information is to be saved as a 4-byte hexadecimal number.
- **event-verbosity** *evt_verboseness*: Specifies the level of verboseness to use in the displaying of event data as one of:

  - *min*: Logs minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
  - *concise*: Logs detailed information about the event, but does not provide the event source within the system.
  - *full*: Logs detailed information about event, including source information, identifying where within the system the event was generated.

- **facility** *facility*: Specifies the facility to modify the filtering of logged information.
- **level** *severity_level*: Specifies the level of information to be logged in the following list which is ordered from highest to lowest:
  - *critical*: Logs critical events
  - *error*: Logs error events and all events with a higher severity level
  - *warning*: Logs warning events and all events with a higher severity level
  - *unusual*: Logs unusual events and all events with a higher severity level
  - *info*: Logs info events and all events with a higher severity level
  - *trace*: Logs trace events and all events with a higher severity level
  - *debug*: Logs all events
- **pdu-data** *pdu_format*: Specifies output format for the display of packet data units as one of:
  - *none* - raw format (unformatted).
  - *hex* - hexadecimal format.
  - *hex-ascii* - hexadecimal and ASCII similar to a main-frame dump.
- **pdu-verbosity** *pdu_verboseness* : Specifies the level of verboseness to use in the displaying of packet data units as a value from 1 to 5, where 5 is the most detailed.
- **since** *from_date_time*: Saves only the log information which has been collected more recently than *from_date_time*
- **until** *to_date_time*: Saves no log information more recent than *to_date_time*. Defaults to current time when omitted.
- *from_date_time* and *to_date_time* must be formatted as YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where:
  - YYYY = 4-digit year
  - MM = 2-digit month in the range 01 through 12
  - DD = 2-digit day in the range 01 through 31
  - HH = 2-digit hour in the range 00 through 23
  - mm = 2-digit minute in the range 00 through 59
  - ss = 2 digit second in the range 00 through 59

*to_date_time* must be a time which is more recent than *from_date_time*.

Using the **until** keyword allows for a time range of log information; using only the **since** keyword will display all information up to the current time.

- **grep** *grep_options* | **more**: Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command is sent.

# Event ID Overview

**Important** The use of event IDs depends on the platform type and the licenses running on the platform.

Identification numbers (IDs) are used to reference events as they occur when logging is enabled on the system. As described previously, logs are collected on a per facility basis. Each facility possesses its own range of event IDs as indicated in the following table.

***Table 4: System Facilities and Event ID Ranges***

| Facility | Description | Event ID Range |
|---|---|---|
| a10 | A10 Protocol Facility | 28000-28999 |
| a11 | A11 Protocol Facility | 29000-29999 |
| a11mgr | A11 Manager Facility | 9000-9999 |
| aaa-client | AAA Client Facility | 6000-6999 |
| aaamgr | AAA Manager Facility | 36000-36999 |
| aaaproxy | AAA Proxy Facility | 64000-64999 |
| aal2 | AAL2 Protocol Facility | 173200-173299 |
| acl-log | IP Access Control List (ACL) Facility | 21000-21999 |
| acsctrl | Active Charging Service Controller (ACSCtrl) Facility | 90000-90999 |
| acsmgr | Active Charging Service Manager (ACSMgr) Facility | 91000-91999 |
| afctrl | Ares Fabric Controller (ASR 5500 only) | 186000-186999 |
| afmgr | Ares Fabric Manager (ASR 5500 only) | 187000-187999 |
| alarmctrl | Alarm Controller Facility | 65000-65999 |
| alcap | Access Link Control Application Part (ALCAP) Protocol Facility | 160900-161399 |
| alcapmgr | ALCAP Manager Facility | 160500-160899 |
| asf | ASF Facility | 73000-73999 |
| asfprt | ASFPRT Facility | 59000-59999 |
| asngwmgr | Access Service Network (ASN) Gateway Manager Facility | 100000-100499 |
| asnpcmgr | ASN Paging/Location-Registry Manager Facility | 100500-100999 |

| Facility | Description | Event ID Range |
|---|---|---|
| bcmcs | Broadcast/Multicast Service (BCMCS) Facility | 109000-109999 |
| bfd | Bidirectional Forwarding Detection (BFD) Protocol Facility | 170500-170999 |
| bgp | Border Gateway Protocol (BGP) Facility | 85000-85999 |
| bindmux | BindMux Manager Facility [Intelligent Policy Control Function (IPCF)] | 158200-158999 |
| bngmgr | Broadband Network Gateway (BNG) Manager Facility | 182000-182999 |
| bssap | Base Station System Application Part+ (BSSAP+) Service Facilities | 131000-131199 |
| bssgp | Base Station System GPRS Protocol (BSSGP) Facility | 115050-115099 |
| callhome | Call Home Facility | 173600-173999 |
| cap | CAMEL Application Part (CAP) Facility | 87900-88099 |
| chatconf | CHATCONF Facility | 74000-74999 |
| cli | Command Line Interface (CLI) Facility | 30000-30999 |
| connproxy | Connection Proxy Facility | 190000-190999 |
| crdt-ctl | Credit Control Facility | 127000-127999 |
| csg | Closed Subscriber Groups (CSG) Facility | 188000-188999 |
| csg-acl | CSG Access Control List (ACL) Facility | 189000-189999 |
| csp | Card/Slot/Port (CSP) Facility | 7000-7999 |
| css | Content Steering Service (CSS) Facility [ESC] | 77000-77499 |
| css-sig | Content Service Selection (CSS) RADIUS Signaling Facility | 77500-77599 |
| cx-diameter | Cx Diameter Message Facility | 92840-92849 |
| dcardctrl | Daughter Card Controller Facility | 62000-62999 |
| dcardmgr | Daughter Card Manager Facility | 57000-57999 |
| demuxmgr | Demux Manager Facility | 110000-110999 |
| dgmbmgr | Diameter Gmb (DGMB) Application Manager Facility | 126000-126999 |
| dhcp | DHCP Facility | 53000-53999 |
| dhcpv6 | DHCPv6 Protocol Facility | 123000-123999 |
| dhost | Distributed Host Manager Facility | 83000-83999 |
| diameter | Diameter Endpoint Facility | 92000-92599 |
| diabase | Diabase Message Facility | 92800-92809 |
| diameter-acct | Diameter Accounting Protocol Facility | 112000-112999 |
| diameter-auth | Diameter Authentication Protocol Facility | 111000-111999 |
| diameter-dns | Diameter DNS Subsystem Facility | 92600-92699 |
| diameter-ecs | ECS Diameter Signaling Facility | 81990-81999 |

| Facility | Description | Event ID Range |
|---|---|---|
| diameter-hdd | Diameter Horizontal Directional Drilling (HDD) Interface Facility | 92700-92799 |
| diameter-svc | Diameter Service Facility | 121200-121999 |
| diamproxy | Diameter Proxy Facility | 119000-119999 |
| dpath | Data Path for IPSec Facility | 54000-54999 |
| drvctrl | Driver Controller Facility | 39000-39999 |
| ds3mgr | DS3 and DS3/E Line Card Manager Facility (part of NPU Manager Controller Facility) | 40000-40999 |
| eap-diameter | Extensible Authentication Protocol (EAP) Diameter Facility | 92870-92879 |
| eap-ipsec | EAP IPSec Facility | 118000-118999 |
| ecs-css | ACS Session Manager (ACSMgr) Signalling Interface Facility | 97000-97099 |
| edr | Event Data Record (EDR) Facility | 80000-80999 |
| egtpc | eGTP-C Facility | 141000-141999 |
| egtpmgr | eGTP Manager Facility | 143000-143999 |
| egtpu | eGTP-U Facility | 142000-142999 |
| epdg | Evolved Packet Data Gateway (ePDG) Facility | 178000-178999 |
| evlog | Event Log Facility | 2000-2999 |
| famgr | Foreign Agent (FA) Manager Facility | 33000-33999 |
| firewall | Firewall Facility | 96000-96999 |
| fng | Femto Network Gateway (FNG) Facility | 149000-149999 |
| gbrmgr | Gb-Manager Facility | 201900-202699 |
| gcdr | GGSN-Charging Data Record (G-CDR) Facility | 66000-66999 |
| gmm | GPRS Mobility Management (GMM) Facility | 88100-88299 |
| gprs-app | General Packet Radio Service (GPRS) Application Facility | 115100-115399 |
| gprs-ns | GPRS-NS Protocol Facility | 115000-115049 |
| gq-rx-tx-diameter | Gq/Rx/Tx Diameter Messages Facility | 92830-92839 |
| gss-gcdr | GTPP Storage Server GCDR Facility | 98000-98099 |
| gtpc | GTPC Protocol Facility | 47000-47999 |
| gtpcmgr | GTPC Signaling Demultiplexer Manager Facility | 46000-46999 |
| gtpp | GTP-PRIME Protocol Facility | 52000-52999 |
| gtpu | GTPU Protocol Facility | 45000-45999 |
| gtpumgr | GTPU Manager Facility | 157200-157999 |
| gx-ty-diameter | Gx/Ty Diameter Messages Facility | 92820-92829 |
| gy-diameter | Gy Diameter Messages Facility | 92810-92819 |

| Facility | Description | Event ID Range |
|---|---|---|
| h248prt | H.248 Protocol Facility | 42000-42999 |
| hamgr | Home Agent (HA) Manager Facility | 34000-34999 |
| hat | High Availability Task (HAT) Facility | 3000-3999 |
| hdctrl | Hard Disk (HD) Controller Facility | 132000-132999 |
| hddshare | HDD Share Facility | 184000-184999 |
| henb-gw | Home eNodeB-GW Facility | 195000-195999 |
| henbapp | Home eNodeB Application Facility | 196000-196999 |
| henbgwdemux | Home eNodeB-GW Demux Facility | 194000-194999 |
| henbgwmgr | Home eNodeB-GW Manager Facility | 193000, 193999 |
| hnb-gw | Home NodeB (HNB) Gateway Facility | 151000-151999 |
| hnbmgr | HNB Manager Facility | 158000-158199 |
| hss-peer-service | Home Subscriber Server (HSS) Facility [MME] | 138000-138999 |
| igmp | Internet Group Management Protocol (IGMP) Facility | 113000-113999 |
| ikev2 | IKEv2 Facility | 122000-122999 |
| ims-authorizatn | IMS Authorization Service Library Facility | 98100-98999 |
| ims-sh | IMS SH Library Facility | 124000-124999 |
| imsimgr | International Mobile Subscriber Identity (IMSI) Manager Facility | 114000-114999 |
| imsue | IMS User Equipment (IMSUE) Facility | 144000-145999 |
| ip-arp | IP Address Resolution Protocol (ARP) Facility | 19000-19999 |
| ip-interface | IP Interface Facility | 18000-18999 |
| ip-route | IP Route Facility | 20000-20999 |
| ipms | Intelligent Packet Monitoring System (IPMS) Facility | 134000-134999 |
| ipne | IP Network Enabler (IPNE) Facility | 192000-192999 |
| ipsec | IPSec Protocol Facility | 55000-56998 |
| ipsg | IP Services Gateway (IPSG) Facility | 128000-128999 |
| ipsgmgr | IPSG Manager (IPSGMgr) Facility | 99000-99999 |
| ipsp | IP Pool Sharing Protocol (IPSP) Facility | 68000-68999 |
| kvstore | Key/Value Store (KVSTORE) Facility | 125000-125999 |
| l2tp-control | L2TP Control PDU Protocol Facility | 50000-50999 |
| l2tp-data | L2TP Data PDU Protocol Facility | 49000-49999 |
| l2tpdemux | L2TP Demux Facility | 63000-63999 |
| l2tpmgr | L2TP Manager Facility | 48000-48999 |

| Facility | Description | Event ID Range |
|---|---|---|
| lagmgr | Link Aggregation Group (LAG) Manager Facility | 179000-179999 |
| ldap | Lightweight Directory Access Protocol (LDAP) Request Facility | 160000-160499 |
| li | Lawful Intercept (LI) Log Facility | 69000-69999 |
| linkmgr | Link Manager Facility | 89500-89999 |
| llc | Logical Link-Control (LLC) Layer Facility (GPRS) | 115700-115799 |
| local-policy | Local Policy Configuration Facility | 161400-162399 |
| m3ap | M3 Application Protocol (M3AP) Facility | 211500-211999 |
| m3ua | MTP Level 3 (M3UA) Protocol Facility [SIGTRAN] | 87500-87699 |
| magmgr | Mobile Access Gateway (MAG) Manager Facility | 137500-137999 |
| map | Mobile Application Part (MAP) Protocol Facility [SS7] | 87100-87299 |
| megadiammgr | MegaDiameter Manager Facility | 121000-121199 |
| mme-app | Mobility Management Entity (MME) Application Facility | 147000-147999 |
| mme-embms | MME evolved Multimedia Broadcast Multicast Service (eMBMS) Facility | 212000-212499 |
| mme-misc | MME Miscellaneous Facility | 155800-156199 |
| mmedemux | MME Demux Manager Facility | 154000-154999 |
| mmemgr | MME Manager Facility | 137000-137499 |
| mmgr | Master Manager (MMGR) Facility | 86000-86399 |
| mobile-ip | Mobile IP (MIP) Protocol Facility | 26000-26999 |
| mobile-ip-data | MIP Tunneled Data Facility | 27000-27999 |
| mobile-ipv6 | Mobile IPv6 Facility | 129000-129999 |
| mpls | Multiprotocol Label Switching (MPLS) Facility | 163500-163999 |
| mseg-app | Mobile Services Edge Gateway (MSEG) Application Facility<br>Not supported in this release. | 172300-172999 |
| mseg-gtpc | MSEG GTPC Application Facility<br>Not supported in this release. | 172000-172199 |
| mseg-gtpu | MSEG GTPU Application Facility<br>Not supported in this release. | 172200-172299 |
| msegmgr | MSEG Manager Facility<br>Not supported in this release. | 171000-171999 |
| mtp2 | Message Transfer Part 2 (MTP2) Service Facility [SS7] | 116900-116999 |
| mtp3 | Message Transfer Part 3 (MTP3) Service Facility [SS7] | 115600-115699 |
| multicast-proxy | Multicast Proxy Facility | 94000-94999 |

| Facility | Description | Event ID Range |
|---|---|---|
| nas | Network Access Signaling (NAS) Facility | 153000-153999 |
| netwstrg | Network Storage Facility | 78000-78999 |
| npuctrl | Network Processing Unit (NPU) Control Facility | 16000-16999 |
| npudrv | NPU Driver Facility | 191000-191999 |
| npumgr | NPU Manager (NPUMGR) Facility | 17000-17999 |
| npumgr-acl | NPUMGR ACL Facility | 169000-169999 |
| npumgr-drv | NPUMGR Driver Facility | 185000-185999 |
| npumgr-flow | NPUMGR Flow Facility | 167000-167999 |
| npumgr-fwd | NPUMGR Forwarding Facility | 168000-168999 |
| npumgr-init | NPUMGR Initialization Facility | 164000-164999 |
| npumgr-lc | NPUMGR LC Facility | 180000-180999 |
| npumgr-port | NPUMGR Port Facility | 166000-166999 |
| npumgr-recovery | NPUMGR Recovery Facility | 165000-165999 |
| npumgr-vpn | NPUMGR VPN Facility | 181000-181999 |
| npusim | NPUSIM Facility | 176000-176999 |
| ntfy-intf | Event Notification Interface Facility | 170000-170499 |
| orbs | Object Request Broker (ORB) System Facility | 15000-15999 |
| ospf | Open Shortest Path First (OSPF) Protocol Facility | 38000-38999 |
| ospfv3 | OSPFv3 Protocol Facility [IPv6] | 150000-150999 |
| p2p | Peer-to-Peer (P2P) Facility | 146000-146999 |
| pccmgr | Policy Charging and Control (PCC) Manager Facility | 159000-159499 |
| pdg | Packet Data Gateway (PDG) Facility | 152010-152999 |
| pdgdmgr | PDG TCP Demux Manager (pdgdmgr) Facility (this is a customer-specific facility) | 162400-162999 |
| pdif | Packet Data Interworking Function (PDIF) Facility | 120000-120999 |
| pgw | Packet Data Network Gateway (PGW) Facility | 139000-139999 |
| pmm-app | Packet Mobility Management (PMM) Application Facility [SGSN] | 89200-89499 |
| ppp | Point-To-Point Protocol (PPP) Facility | 25000-25999 |
| pppoe | Point-to-Point Protocol over Ethernet (PPPoE) Facility | 183000-183999 |
| ptt | PTT Facility | 76000-76999 |
| push | PUSH (VPNMgr CDR Push) Facility | 133000-133999 |
| radius-acct | RADIUS Accounting Protocol Facility | 24000-24999 |
| radius-auth | RADIUS Authentication Protocol Facility | 23000-23999 |

| Facility | Description | Event ID Range |
|---|---|---|
| radius-coa | RADIUS Change of Authorization (CoA) and Disconnect Facility | 70000-70999 |
| ranap | Radio Access Network Application Part (RANAP) Facility | 87700-87899 |
| rct | Recovery Control Task (RCT) Facility | 13000-13999 |
| rdt | Redirector Task (RDT) Facility | 67000-67999 |
| resmgr | Resource Manager (RM) Facility | 14000-14999 |
| rf-diameter | Rf Diameter Messages Facility | 92860-92869 |
| rip | Routing Information Protocol (RIP) Facility | 35000-35999 |
| rohc | Robust Header Compression (ROHC) Protocol Facility | 103000-103999 |
| rsvp | RSVP Protocol Facility | 93000-93999 |
| rua | RANAP User Adaptation (RUA) Protocol Facility | 152000-152009 |
| s1ap | S1 Application Protocol (S1AP) Facility | 155200-155799 |
| saegw | System Architecture Evolution Gateway Facility | 191000-191999 |
| sccp | Signalling Connection Control Part (SCCP) Protocol Facility [SS7] | 86700-86899 |
| sct | Shared Configuration Task (SCT) Facility | 32000-32099 |
| sctp | Stream Control Transmission Protocol (SCTP) Protocol Facility | 87300-87499 |
| sess-gr | SESS-GR Facility | 77600-77999 |
| sessctrl | Session Controller Facility | 8000-8999 |
| sessmgr | Session Manager Facility | 10000-12999 |
| sesstrc | Session Trace Facility | 155000-155199 |
| sft | Switch Fabric Task (SFT) Facility | 58000-58999 |
| sgs | SGs Interface Protocol Facility [MME] | 173000-173199 |
| sgsn-app | SGSN Application Interface Facility | 115900-115999 |
| sgsn-failures | SGSN Call Failures Facility | 89100-89199 |
| sgsn-gtpc | SGSN GTP-C Protocol Facility | 116000-116599 |
| sgsn-gtpu | SGSN GTP-U Protocol Facility | 86900-87099 |
| sgsn-mbms-bearer | SGSN MBMS Bearer Application (SMGR) Facility | 116600-116799 |
| sgsn-misc | SGSN Miscellaneous Facility | 88800-89099 |
| sgsn-system | SGSN System Components Facility | 86400-86499 |
| sgsn-test | SGSN Tests Facility | 88700-88799 |
| sgsn2 | SGSN2 Facility | 114000-117999 |
| sgtpcmgr | SGSN GTP-C (SGTPC) Manager Facility | 117000-117999 |
| sgw | Serving Gateway (SGW) Facility | 140000-140999 |

| Facility | Description | Event ID Range |
|---|---|---|
| sh-diameter | Sh Diameter Messages Facility | 92850-92859 |
| sipcdprt | SIPCDPRT Facility | 95000-95999 |
| sitmain | System Initiation Task (SIT) Main Facility | 4000-4999 |
| sm-app | Short Message Service (SMS) Facility | 88300-88499 |
| sms | SMS Service Facility | 116800-116899 |
| sndcp | Sub Network Dependent Convergence Protocol (SNDCP) Facility | 115800-115899 |
| snmp | Simple Network Management Protocol (SNMP) Facility | 22000-22999 |
| sprmgr | Subscriber Policy Register (SPR) Manager Facility | 159500-159999 |
| srdb | Static Rating Database Facility | 102000-102999 |
| srp | Service Redundancy Protocol (SRP) Facility | 84000-84999 |
| sscfnni | SSCFNNI Protocol Facility [ATM] | 115500-115599 |
| sscop | SSCOP Protocol Facility [ATM] | 115400-115499 |
| ssh-ipsec | SSH IP Security Facility | 56999-56999 |
| ssl | SSL Facility (this is a customer-specific facility) | 156200-157199 |
| stat | Statistics Facility | 31000-31999 |
| system | System Facility | 1000-1999 |
| tacacs+ | TACACS+ Protocol Facility | 37000-37999 |
| taclcp | TACLCP Facility | 44000-44999 |
| tcap | Transaction Capabilities Application Part (TCAP) Protocol Logging Facility [SS7] | 86500-86699 |
| testctrl | Test Controller Facility | 174000-174999 |
| testmgr | Test Manager Facility | 175000-175999 |
| threshold | Threshold Facility | 61000-61999 |
| ttg | Tunnel Termination Gateway (TTG) Facility | 130000-130999 |
| tucl | TCP/UDP Convergence Layer (TUCL) Facility [SS7] | 88500-88699 |
| udr | User Data Record (UDR) Facility | 79000-79999 |
| user-data | User-Data Facility | 51000-51999 |
| user-l3tunnel | User L3 Tunnel Facility | 75000-75999 |
| usertcp-stack | User TCP Stack Facility | 173300-173499 |
| vim | Voice Instant Message (VIM) Facility | 60000, 60999 |
| vinfo | VINFO Facility | 82000, 82999 |
| vmgctrl | Virtual Media Gateway (VMG) Controller Facility | 41000, 41999 |
| vmgctxmgr | VMG Context Manager Facility | 43000, 43999 |

| Facility | Description | Event ID Range |
|---|---|---|
| vpn | Virtual Private Network (VPN) Facility | 5000-5999 |
| wimax-data | WiMAX DATA Facility | 104900-104999 |
| wimax-r6 | WiMAX R6 Protocol (Signaling) Facility | 104000-104899 |

# Event Severities

The system provides the flexibility to configure the level of information that is displayed when logging is enabled. The following levels are supported:

- **critical:** Logs only those events indicating a serious error has occurred that is causing the system tor a system component to cease functioning. This is the highest severity level.
- **error:** Logs events that indicate an error has occurred that is causing the system or a system component to operate in a degraded state. This level also logs events with a higher severity level.
- **warning:** Logs events that may indicate a potential problem. This level also logs events with a higher severity level.
- **unusual:** Logs events that are very unusual and may need to be investigated. This level also logs events with a higher severity level.
- **info:** Logs informational events and events with a higher severity level.
- **trace:** Logs events useful for tracing and events with a higher severity level.
- **debug:** Logs all events regardless of the severity.

Each of the above levels correspond to the "severity" level of the event ID. Therefore, only those event IDs with a "severity" level equal to the logging level are displayed.

# Understanding Event ID Information in Logged Output

This section explains the event information that is displayed when logging is enabled.

The following displays a sample output for an event that was logged.

```
2011-Dec-11+5:18:41.993 [cli 30005 info] [8/0/609 cli:8000609 _commands_cli.c:1290] [software
 internal system] CLI session ended for Security Administrator admin on device /dev/pts/2
```

The following table describes the elements of contained in the sample output.

***Table 5: Event Element Descriptions***

| Element | Description |
|---|---|
| 2011-Dec-11+5:18:41.993 | Date/Timestamp indicating when the event was generated |

| Element | Description |
|---|---|
| [cli 30005 info] | Information about the event including:<br>• The facility the event belongs to<br>• The event ID<br>• The event's severity level<br>In this example, the event belongs to the CLI facility, has an ID of 3005, and a severity level of "info". |
| [8/0/609 cli:8000609 _commands_cli.c:1290] | Information about the specific CLI instance. |
| [software internal system] | Indicates that the event was generated because of system operation. |
| CLI session ended for Security Administrator admin on device /dev/pts/2 | The event's details. Event details may, or may not include variables that are specific to the occurrence of the event. |