Logging Config Mode Command Reference

- logging fluent, on page 1
- logging fluent tls, on page 2
- logging fluentd, on page 2
- logging listener, on page 3
- logging loki, on page 4
- logging splunk, on page 4
- logging syslog, on page 5
- logging worker, on page 6

logging fluent

Configures Fluent Forwarding parameters.

Command Modes

Exec > Global Configuration

Syntax Description

```
logging fluent { host host_info | port port_number | protocol outbound_protocol |
 disable-tls { false | true } | disable-tls-verification { false | true
} | flush-interval flush_interval | storage-limit storage_limit }
```

host *host_info*

Specify the Fluentbit or Fluentd instance host information.

Must be a string.

port *port_number*

Specify the Fluentbit or Fluentd instance port number.

Must be an integer.

protocol *outbound_protocol*

Specify the outbound protocol.

Must be one of the following:

- **forward**

- **http**

Default Value: **http**

Usage Guidelines Use this command to configure Fluent Forwarding parameters to enable log forwarding to Fluent endpoint.

logging fluent tls

Configures TLS communciation with Splunk endpoint and TLS certification verification parameters.

Command Modes Exec > Global Configuration

Syntax Description **`tls { disable-tls { false | true } | disable-tls-verification { false | true } }`**

disable-tls { false | true}

Specify to enable or disable TLS communciation with Splunk endpoint. To enable, set to false.

Must be one of the following:

- **false**
- **true**

Default Value: false.

disable-tls-verification { false | true}

Specify to enable or disable TLS certification verification. To enable, set to false.

Must be one of the following:

- **false**
- **true**

Default Value: false.

Usage Guidelines Use this command to configure TLS communciation with Splunk endpoint and TLS certification verification parameters.

logging fluentd

Configures FluentD parameters.

Command Modes Exec > Global Configuration

Syntax Description **`fluentd workers {`** *`number_of_workers`* **`| buffer-total-limit-size`** *`buffer_size_limit`* **`| buffer-chunk-limit-size`** *`chunk_size_limit`* **`| flush-interval`** *`flush_interval`* **`}`**

buffer-chunk-limit-size *chunk_size_limit*

Specify the maximum size of each chunk in MB.

Must be an integer in the range of 1-10.

Default Value: 8

buffer-total-limit-size *buffer_size_limit*

Specify the size limitation of the buffer in GB.

Must be an integer in the range of 1-3.

Default Value: 1

flush-interval *flush_interval*

Specify the flush interval in seconds.

Must be an integer in the range of 1-10.

Default Value: 5.

workers *number_of_workers*

Specify the number of workers.

Must be an integer in the range of 1-5.

Default Value: 2

Usage Guidelines Use this command to configure FluentD parameters.

logging listener

Enables the Logs Listener for incoming logs.

Command Modes Exec > Global Configuration

Syntax Description **`listener enable external-ip`** *`ip_address`* **`udp-port`** *`port_number`* **`buffer-max-size`** *`buffer_max_size`* **`buffer-chunk-size`** *`buffer_chunk_max_size`*

enable

Specify to enable Logs Listener.

external-ip *ip_address*

Specify the exposed IP endpoint for incoming logs.

Must be an IPv4 address.

-Or-

Must be an IPv6 address.

udp-port *port_number*

Specify the Listener UDP port number.

Must be an integer.

Default Value: 514.

Usage Guidelines Use this command to enable the Logs Listener for incoming logs.

logging loki

Configures the Grafana Loki parameters.

Command Modes Exec > Global Configuration

Syntax Description **logging loki [enable | retention-period** *retention_period* **]**

enable

Specify to enable Grafana Loki Logging Visualization.

retention-period *retention_period*

Specify the retention period.

Must be a string.

Usage Guidelines Use this command to configure Grafana Loki parameters.

logging splunk

Configures Splunk endpoint.

Command Modes Exec > Global Configuration

Syntax Description **logging splunk { host** *host_info* **| port** *port_number* **| auth-token** *auth_token* **}**

auth-token *auth_token*

Specify the Splunk Authentication Token for the HTTP Event Collector interface.

Must be a string.

disable-tls { false | true}

Specify to enable or disable TLS communciation with Splunk endpoint. To enable, set to false.

Must be one of the following:

- **false**
- **true**

Default Value: false.

disable-tls-verification { false | true}

Specify to enable or disable TLS certification verification. To enable, set to false.

Must be one of the following:

- **false**
- **true**

Default Value: false.

host *host_info*

Specify the Splunk host information.

Must be a string.

port *port_number*

Specify the Splunk port number.

Must be an integer.

Usage Guidelines Use this command to configure Splunk endpoint to enable log forwarding to Splunk endpoint using HTTP Event Collector interface.

logging syslog

Configure log forwarding to the Syslog server.

Command Modes Exec > Global Configuration

Syntax Description **`logging syslog { host`** *`server_host`* **`| mode`** *`server_mode`* **`| port`** *`server_port`* **`| syslog_format`** *`syslog_format`* **`| syslog_maxsize`** *`syslog_maxsize`* **`}`**

host *server_host*

Specify the domain or IP address of the remote Syslog server.

mode *server_mode*

Specify the TCP, TLS, or UDP transport type.

port *server_port*

Specify the TCP, TLS, or UDP port of the remote Syslog server.

syslog_format *syslog_format*

Specify the *rfc3164* or *rfc5424* Syslog protocol format to use.

syslog_maxsize *syslog_maxsize*

Specify the maximum size allowed per message. The value must be an integer representing the number of bytes allowed.

Usage Guidelines Use this command to configure Fluent-bit to enable log forwarding to the Syslog server.

logging worker

Enables CEE log forwarding for Fluent Worker pods.

Command Modes Exec > Global Configuration

Syntax Description

```
logging worker [ drop-namespace-logs namespace_names | drop-pod-logs pod_names
 | exclude-logs-with-annotation true | keep-pod-logs pod_names |
keep-namespace-logs namespace_names | drop-os-service-logs [ service_names |
remove-keys [ keys ] ]
```

drop-namespace-logs *namespace_names*

Specify to drop logs by namespaces. *namespace_names* must be a regex string with selected namespace names inside double quotes.

drop-pod-logs *pod_names*

Specify to drop logs by pods. *pod_names* must be a regex string with selected pod names inside double quotes.

exclude-logs-with-annotation true

Specify to exclude logs from selected pods using annotation.

Note After adding or removing annotation from any pod, it is required to restart the fluent-worker pod for the changes to take effect.

keep-namespace-logs *namespace_names*

Specify to retain logs by namespaces. *namespace_names* must be a regex string with selected namespace names inside double quotes.

keep-pod-logs *pod_names*

Specify to retain logs by pods. *pod_names* must be a regex string with selected pod names inside double quotes.

drop-os-service-logs [*service_names*]

Specify to drop logs from selected OS services. The currently supported values for *services_names* are audit, kernel, or kubelet.

remove-keys [*keys*]

Specify to remove keys from log entries. The log entry keys to be dropped are case sensitive.

Usage Guidelines

Use this command to enable CEE log forwarding for Fluent Worker pods. The filters on Fluent worker pods that intake the logs from each node reduce the volume of logs being forwarded.