Configuring Log Events

You can enable or disable the forwarding of selected log events to the Event Server.
This functionality is enabled by default, and is a service-wide setting (Enable Log Event Ca
for which monitoring is provided. You can enable and disable event capture for Cloudera Runt
Cloudera Management Service.
Important: Cloudera does not recommend logging to a network-mounted file system. If a role i
logs across the network, a network failure or the failure of a remote file system can cause
up until the network recovers.

Configuring Logs

You can configure log properties.

About this task
Minimum Required Role: Configurator (also provided by Cluster Administrator, Limited Cluste
Full Administrator)

Procedure

1. Go to a service.
2. Click the Configuration tab.
3. Select role_name (Service-Wide) Logs.
4. Edit a log property.
5. Enter a Reason for change, and then click Save Changes to commit the changes.
6. Click the Cloudera Manager logo to return to the Home page.
7. Click the icon that is next to any stale services to invoke the cluster restart wizard.

Configuring Logging Thresholds

A logging threshold determines what level of log message is reported.

About this task
Minimum Required Role: Configurator (also provided by Cluster Administrator, Limited Cluste
Full Administrator)
The available levels are:

- TRACE - Informational events finer-grained than DEBUG.
- DEBUG - Informational events useful to debug an application.
- INFO - Informational events that highlight progress at coarse-grained level.
- WARN - Events that indicate a potential problem which is handled by the application.
- ERROR - Error events that allows the application to continue running.
- FATAL - Very severe error events that typically lead the application to abort. The number of messages is greater and severity is least for TRACE. The default setting is INFO.

Procedure

1. Go to a service.
2. Click the Configuration tab.
3. Enter Logging Threshold in the Search text field.
4. For the desired role group, select a logging threshold level.
5. Enter a Reason for change, and then click Save Changes to commit the changes.
6. Click the Cloudera Manager logo to return to the Home page.
7. Click the icon that is next to any stale services to invoke the cluster restart wizard.

Configuring Log Directories

You can configure log directories for a cluster or a service.

About this task
Minimum Required Role: Configurator (also provided by Cluster Administrator, Limited Cluste
Full Administrator)

Procedure

- Do one of the following:
  - Cluster:
    - On the Home Status tab, click a cluster name.
    - Select Configuration Log Directories.
    - Edit a role_name Log Directory property.
  - Service:
    - Go to a service.
    - Click the Configuration tab.
    - Select role_name (Service-Wide) Logs.
    - Edit the Log Directory property.
- Enter a Reason for change, and then click Save Changes to commit the changes.
- Click the Cloudera Manager logo to return to the Home page.
- Click the icon that is next to any stale services to invoke the cluster restart wizard.

Enabling and Disabling Log Event Capture.....

You can enable and disable log event capture for a service.

About this task
You can also modify the rules that determine how log messages are turned into events. Editi
recommended.
For each role, there are rules that govern how its log messages are turned into events by th
the role. These are defined in the Rules to Extract Events from Log Files property.
Minimum Required Role: Configurator (also provided by Cluster Administrator, Limited Cluste

Full Administrator)

Procedure

1. Select Clusterscluster_nameservice_name.
2. Click the Configuration tab.
3. Select Scope service_name (Service-Wide).
4. Click the Monitoring category.
5. Modify the Enable Log Event Capture setting.
6. Enter a Reason for change, and then click Save Changes to commit the changes.
7. Click the Cloudera Manager logo to return to the Home page.
8. Click the icon that is next to any stale services to invoke the cluster restart wizard.

Configuring Which Log Messages Become Events

You can configure rules to determine which log messages become events.

About this task
Cloudera defines a number of rules by default. For example:

- The line {“rate”: 10, “threshold”:“FATAL”}, means log entries with severity FATAL should be forwarded as events, up to 10 a minute.
- The line {“rate”: 0, “exceptiontype”: “java.io.EOFException”}, means log entries with the exception java.io.EOFException should always be forwarded as an event. The syntax for these rules is defined in the Description field for this property: the syntax lets you create rules that identify log messages based on log4j severity, message content matching, or the exception type. These rules must result in valid JSON. Note: Editing these rules is not recommended. Cloudera Manager provides a default set of rules that should be sufficient for most users.

Minimum Required Role: Configurator (also provided by Cluster Administrator, Limited Cluste
Full Administrator)

Procedure

- Select Clusterscluster_nameservice_name.
- Click the Configuration tab.
- Enter Rules to Extract Events from Log Files in the Search text field.
- Click the Monitoring category.
- Select the role group for the role for which you want to configure log events, or search for “Rules to Extract Events from Log Files.” Note that for some roles there may be more than one role group, and you may need to modify all of them. The easiest way to ensure that you have found all occurrences of the property you need to modify is to search for the

property by name. Cloudera Manager shows all copies of the property that matches the search filter.
- In the Content field, edit the rules as needed. Rules can be written as regular expressions.
- Enter a Reason for change, and then click Save Changes to commit the changes.
- Click the Cloudera Manager logo to return to the Home page.
- Click the icon that is next to any stale services to invoke the cluster restart wizard.

Configuring Log Alerts……

```
You specify that a log event should generate an alert (by setting "alert" :true in the rule)
If you specify a content match, the entire content must match -
if you want to match on a partial string, you must
provide wildcards as appropriate to allow matching the entire string.
```