

Logs

The Logs page presents log information for Hadoop services, filtered by service, role, host, log level (severity).

To configure logs, see the topic [Configuring Log Events](#).

Viewing Logs

You can view logs that contain information such as warnings, errors, and more.

Procedure

1. Select [Diagnostics Logs](#) on the top navigation bar.
2. Click [Search](#). The logs for all roles display. If any of the hosts cannot be searched, an error message notifies you of the error and the host(s) on which it occurred.

Logs List

Log results are displayed in a list.

The logs list contains the following columns:

- Host - The host where this log entry appeared. Clicking this link will take you to the [Host Status](#) page.
- Log Level - The log level (severity) associated with this log entry.
- Time - The date and time this log entry was created.
- Source - The class that generated the message.
- Message - The message portion of the log entry. Clicking [View Log File](#) displays the [Log Details](#) page, which presents a display of the full log, showing the selected message (highlighted) and the 100 messages before and after it in the log. If there are more results than can be shown on one page (per the [Results per Page](#) setting you selected), [Next](#) and [Prev](#) buttons let you view additional results. [Related Information](#) [Managing Hosts Log Details](#)

Filtering Logs

You filter logs by selecting a time range and specifying filter parameters.

About this task

You can use the [Time Range Selector](#) or a duration link (

) to set the time range. See [for details](#). However,

logs are, by definition, historical, and are meaningful only in that context. So the [Time Machine](#) at a specific point in time, is not available on this page. The [Now](#) button () is available.

Procedure

1. Specify any of the log filter parameters:

- Search Phrase - A string to match against the log message content. The search is case-insensitive, and the string can be a regular expression, such that wildcards and other regular expression primitives are supported.
- Select Sources - A list of all the service instances and roles currently instantiated in your cluster. By default, all services and roles are selected to be included in your log search; the All Sources checkbox lets you select or

clear all services and roles in one operation. You can expand each service and limit the search by selecting or clearing individual roles.

- Hosts - The hosts to be included in the search. As soon as you start typing a hostname, Cloudera Manager provides a list of hosts that match the partial name. You can add multiple names, separated by commas. The default is to search all hosts.
 - Minimum Log Level - The minimum severity level for messages to be included in the search results. Results include all log entries at the selected level or higher. This defaults to WARN (that is, a search will return log entries with severity of WARN, ERROR, or FATAL only).
 - Additional Settings
 - Search Timeout - A time (in seconds) after which the search will time out. The default is 20 seconds.
 - Results per Page - The number of results (log entries) to be displayed per page.
2. Click Search. The Logs list displays the log entries that match the specified filter.

Log Details

The Log Details page presents a portion of the full log, showing the selected message (highlighted) before and after it in the log.

The Log Details page shows you:

- The host
- The role
- The full path and name of the log file you are viewing.
- Messages before and after the one you selected. The log displays the following information for each message:
 - Time - the time the entry was logged
 - Log Level - the severity of the entry
 - Source - the source class that logged the entry
 - Log Message

You can switch to display only messages or all columns using the buttons. In addition, from the Log Details page you can:

- View the log entries in either expanded or contracted form using the buttons to the left of the date range at the top of the log.
- Download the full log using the Download Full Log button at the top right of the page.
- View log details for a different host or for a different role on the current host, by clicking the Change... link next to the host or role at the top of the page. In either case this shows a pop-up where you can select the role or host you want to see.

Viewing the Cloudera Manager Server Log

To help you troubleshoot problems, you can view the Cloudera Manager Server log. You can view the log on the Cloudera Manager Server Logs page or in specific pages for the log.

Viewing Cloudera Manager Server Logs in the Logs Page

You can view Cloudera Manager Server logs in the Logs page.

Procedure

1. Select DiagnosticsLogs on the top navigation bar.
2. Next to Sources, select the Cloudera Manager Server checkbox and deselect the other options.
3. Adjust the search criteria and click Search. Related Information Logs

Viewing the Cloudera Manager Server Log

You can access the Cloudera Manager Server Log through the Diagnostics menu or the server host page.

Procedure

1. Select DiagnosticsServer Log on the top navigation bar.
2. Optionally, you can view the Cloudera Manager Server log at `/var/log/cloudera-scm-server/cloudera-scm-server.log` on the Server host.

Viewing the Cloudera Manager Agent Logs

To help you troubleshoot problems, you can view the Cloudera Manager Agent logs. You can view the logs on the Cloudera Manager Agent Logs page or in specific pages for the logs.

Viewing Cloudera Manager Agent Logs in the Logs Page

You can view the Cloudera Manager Agent logs in the Logs page.

Procedure

1. Select DiagnosticsLogs on the top navigation bar.
2. Click Select Sources to display the log source list.
3. Uncheck the All Sources checkbox.

4. Click to the left of Cloudera Manager and select the Agent checkbox.
5. Click Search. Related Information Logs

Viewing the Cloudera Manager Agent Log

You can view the Cloudera Manager Agent log through the Hosts page.

Procedure

1. Click the Hosts tab.
2. Click the link for the host where you want to see the Agent log.
3. In the Details panel, click the Details link in the Host Agent field.
4. Click the Agent Log link. You can also view the Cloudera Manager Agent log at `/var/log/cloudera-scm-agent/cloudera-scm-agent.log` on the Agent hosts.

Managing Disk Space for Log Files

All CDH cluster hosts write out separate log files for each role instance assigned to the host. You can monitor and manage the disk space used by these roles and configure log rotation to prevent roles from consuming too much disk space.

Related Information

Managing Role Groups

Disk Space Requirements

For each role assigned to a host, you should generally provision 2GB of disk space for log files. This is based on the default values of configuration properties that set the maximum log file size (2GB) and the maximum number of files (10). To calculate the disk space required for each host, multiply the size of the log file by the configured maximum number of logs. Perform this calculation for each role and add them together. (Note that Gateway roles do not generate log files.)

To determine the roles assigned to each host, open the Cloudera Manager Admin Console and go to Hosts, and expand the list of roles in the Roles column.

Managing Log Files

To manage log file configurations for all role instances of a service:

1. Go to Service NameConfiguration.
2. Select CategoryLogs.
3. Edit the logging parameters.
4. Click Save Changes. Note: You can also manage these configurations using Role Groups, which you can use to configure similar hosts with the same configuration values.

There are the parameters you use to manage log files:

Table 8: Log File Properties

Property Description Default Value

Role Type Max Log Size Maximum size for a log file before the log file rolls over into a new file.

200 MB

Role Type Maximum Log File Backups Maximum number of rolled-over log files to retain.

10

Role Type Log Directory The path to the directory where the log files are saved.

/var/log/log_file_name

Role Type Logging Threshold
(not available for all roles)

Logging level to limit the number of entries saved in the log file.

Depends on the role.