Lifecycle and Security Auditing

An audit event is an event that describes an action that has been taken for a cluster, host,
or user.
Minimum Required Role: Auditor (also provided by Full Administrator)
Cloudera Manager records cluster, host, license, parcel, role, and service lifecycle events
deploy, download, install, start, stop, update, upgrade, and so on), user security-related e
login failed and succeeded), and provides an audit UI and API to view, filter, and export su

Manager audit log does not track the progress or results of commands (such as starting or st
creating a directory for a service), it just notes the command that was executed and the use
the progress or results of a command, follow the procedures in the topic Viewing and Running
In CDP, Ranger performs auditing against the data access policies defined for each service.
UI and API to view, filter, and export service access audit logs. For information about audi
Ranger Auditing documentation.
Related Information
Viewing Running and Recent Commands

Viewing Audit Events

You can view audit events for a cluster, service, role, or host.

Object Procedure
Cluster 1. Click the Audits tab on the top navigation bar.

Service 1. Click the Clusters tab on the top navigation bar.

2. Select a service.
3. Click the Audits tab on the service navigation bar.

Role 1. Click the Clusters tab on the top navigation bar.

2. Select a service.
3. Click the Instances tab on the service navigation bar.
4. Select a role.
5. Click the Audits tab on the role navigation bar.

Host 1. Click the Hosts tab on the top navigation bar.

2. Select a host.
3. Click the Audits tab on the host navigation bar.

Audit event entries are ordered with the most recent at the top.

Audit Event Properties
The following properties can appear in an audit event entry:

- Date - Date and time the action was performed.
- Command - The action performed.
- Source - The object affected by the action.
- User - The name of the user that performed the action.
- IP Address - The IP address of the client that initiated the action.

- Host IP Address - The IP address of the host on which the action was performed.
- Service - The name of the service on which the action was performed.
- Role - The name of the role on which the action was performed.

Filtering Audit Events

You filter audit events by selecting a time range and adding filters. You can use the Time Range Selector or a duration link (

) to set the time range. When you select the time range, the log displays all events in that range. The time it takes to perform a search will longer time range, as the number of events to be searched will be larger.

Adding a Filter

You can filter audit events by a chosen property.

Procedure
Add the filter:

- Click the icon that displays next to a property when you hover in one of the event entries. A filter containing the property, operator, and its value is added to the list of filters at the left and Cloudera Manager redisplays all events that match the filter.
- Click the Add a filter link. A filter control is added to the list of filters.
    a. Choose a property in the drop-down list. You can search by properties such as Username, Service, Command, or Role. The properties vary depending on the service or role.
    b. If the property allows it, choose an operator in the operator drop-down list.
    c. Type a property value in the value text field. To match a substring, use the like operator and specify % around the string. For example, to see all the audit events for files created in the folder /user/joe/out specify Source l ike %/user/joe/out%.
    d. Click Search. The log displays all events that match the filter criteria.
    e. Click to add more filters and repeat steps a through d.

Removing a Filter

You can remove a filter and repeat the event search with different filter criteria.

Procedure

1. Click the at the right of the filter. The filter is removed.
2. Click Search. The log displays all events that match the filter criteria.

Downloading Audit Events

You can download audit events in CSV formats.

Procedure

1. Specify desired filters and time range.
2. Click the Download CSV button. A file with the following fields is downloaded: service, username, command, ipAddress, resource, allowed, time stamp, operationText. The structure of the resource field depends on the type of the service:
   - HDFS - A file path
   - Hive, Hue, and Impala - database:tablename
   - HBase - table family:qualifier For Hive, Hue, and Impala query and load commands, operationText is the query string. HDFS Service Audit Log

```
service,username,command,ipAddress,resource,allowed,timestamp
hdfs1,cloudera,setPermission,10.20.187.242,/user/hive,false,"2013-02-09T00
:59:34.430Z"
hdfs1,cloudera,getfileinfo,10.20.187.242,/user/cloudera,true,"2013-02-09T00
:59:22.667Z"

hdfs1,cloudera,getfileinfo,10.20.187.242,/,true,"2013-02-09T00:59:22.658Z"
```

In this example, the first event access was denied, and therefore the allowed field has the