Monitoring your Environment

Auditing

To identify changes both expected (for tracking) or unexpected (for troubleshooting), you can view an audit trail of the Cloud Insights system events and user activities.

Viewing Audited Events

To View the Audit page, click Admin > Audit in the menu. The Audit page is displayed, providing the following details for each audit entry:

- **Time** - Date and time of the event or activity
- **User** - The User who initiated the activity
- **Role** - The user’s role in Cloud Insights (guest, user, administrator)
- **IP** - The IP address associated with the event
- **Action** - Type of activity, for example Login, Create, Update
- **Category** - The category of activity
- **Details** - Details of the activity

Displaying audit entries

There are a number of different ways to view audit entries:

- You can display audit entries by choosing a particular time period (1 hour, 24 hours, 3 days, etc.).
- You can change the sort order of entries to either ascending (up arrow) or descending (down arrow) by clicking the arrow in the column header.

By default, the table displays the entries in descending time order.

- You can use the filter fields to show only the entries you want in the table. Click the [+ ] button to add additional filters.
More on Filtering

You can use any of the following to refine your filter:

<table>
<thead>
<tr>
<th>Filter</th>
<th>What it does</th>
<th>Example</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>* (Asterisk)</td>
<td>enables you to search for everything</td>
<td>vol*rhel</td>
<td>returns all resources that start with &quot;vol&quot; and end with &quot;rhel&quot;</td>
</tr>
<tr>
<td>? (question mark)</td>
<td>enables you to search for a specific number of characters</td>
<td>BOS-PRD??-S12</td>
<td>returns BOS-PRD12-S12, BOS-PRD23-S12, and so on</td>
</tr>
<tr>
<td>OR</td>
<td>enables you to specify multiple entities</td>
<td>FAS2240 OR CX600 OR FAS3270</td>
<td>returns any of FAS2440, CX600, or FAS3270</td>
</tr>
<tr>
<td>NOT</td>
<td>allows you to exclude text from the search results</td>
<td>NOT EMC*</td>
<td>returns everything that does not start with &quot;EMC&quot;</td>
</tr>
<tr>
<td>None</td>
<td>searches for blank(NULL/None in any field where selected</td>
<td>None</td>
<td>returns results where the target field is not empty</td>
</tr>
<tr>
<td>Not *</td>
<td>as with None above, but you can also use this form to search for NULL values in text-only fields</td>
<td>Not *</td>
<td>returns results where the target field is not empty.</td>
</tr>
<tr>
<td>&quot;&quot;</td>
<td>searches for an exact match</td>
<td>&quot;NetApp*&quot;</td>
<td>returns results containing the exact literal string &quot;NetApp*&quot;</td>
</tr>
</tbody>
</table>

If you enclose a filter string in double quotes, Insight treats everything between the first and last quote as an exact match. Any special characters or operators inside the quotes will be treated as literals. For example, filtering for "" will return results that are a literal asterisk; the asterisk will not be treated as a wildcard in this case. The operators OR and NOT will also be treated as literal strings when enclosed in double quotes.

Audited Events and Actions

The events and actions audited by Cloud insights can be categorized in the following broad areas:

- **User account**: Log in, log out, role change, etc.

  Example: User Tony Lavoie logged in from 10.1.120.15, user agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36, login method(s) Cloud Central Portal Login

- **Acquisition Unit**: create, delete, etc.

  Example: Acquisition unit AU-Boston-1 removed.

- **Data Collector**: add, remove, modify, postpone/resume, change acquisition unit, start/stop, etc.

  Example: Datasource FlexPod Lab removed, vendor NetApp, model ONTAP Data Management Software, ip 192.168.106.5.
• **Application**: add, assign to object, remove, etc.

  Example: *Internal Volume ocisedev:t1appSVM01:t1appFlexVol01 added to application Test App.*

• **Annotation**: add, assign, remove, annotation rule actions, annotation value changes, etc.

  Example: *Annotation value Boston added to annotation type SalesOffice.*

• **Query**: add, remove, etc.

  Example: *Query TL Sales Query is added.*

• **Monitor**: add, remove, etc.

  Example: *Monitor Aggr Size - CI Alerts Notifications Dev updated*

• **Notification**: change email, etc.

  Example: *Recipient ci-alerts-notifications-dl created*

**Exporting Audit Events**

You can export the results of your Audit display to a .CSV file, which will allow you to analyze the data or import it into another application.

**Steps**

1. On the Audit page, set the desired time range and any filters you want. Cloud Insights will export only the Audit entries that match the filtering and time range you have set.

2. Click the *Export* button in the upper right of the table.

The displayed Audit events will be exported to a .CSV file, up to a maximum of 10,000 rows.

**Retention of Audit Data**

The amount of time Cloud Insights retains Audit data is based on your Edition:

- **Basic Edition**: Audit data is retained for 30 days
- **Standard and Premium Editions**: Audit data is retained for 1 year plus 1 day

Audit entries older than the retention time are automatically purged. No user interaction is needed.

**Troubleshooting**

Here you will find suggestions for troubleshooting problems with Audit.

<table>
<thead>
<tr>
<th>Problem:</th>
<th>Try this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>I see Audit messages telling me that a monitor has been exported.</td>
<td>Export of a custom monitor configuration is typically used by NetApp engineers during development and testing of new features. If you did not expect to see this message, please consider exploring the actions of the user named in the audited action or contact support.</td>
</tr>
</tbody>
</table>