Copyright

All content in this document, including text, graphics, logos, icons, images, and video clips, is the exclusive property of Exabeam or its content suppliers and is protected by U.S. and international copyright laws. The compilation (meaning the collection, arrangement, and assembly) of all content in this document is the exclusive property of Exabeam and is also protected by U.S. and international copyright laws. The content in this document may be used as a resource. Any other use, including the reproduction, modification, distribution, transmission, republication, display, or performance, of the content in this document is strictly prohibited.

Copyright ©2020 Exabeam, Inc. All Rights Reserved.

Trademarks

Exabeam, the Exabeam logo, Threat Hunter, Smarter SIEM, Smart Timelines and Security Management Platform are service marks, trademarks or registered marks of Exabeam, Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. The marks and logos displayed in this document may not be used without the prior written consent of Exabeam or their respective owners.

Patents

Exabeam owns, and reserves all rights for, patents for Exabeam products and services, which may be protected under registered patents as well as patents pending.

Other Policies

For information regarding Exabeam’s treatment of personally identifiable information, please review Exabeam’s current privacy policy at www.exabeam.com/privacy.
Table of Contents

1. About Exabeam Cloud Archive .................................................................................................. 4
2. Exabeam Cloud Archive Architecture ........................................................................................ 5
   2.1. Exabeam Cloud Archive Technical Specifications ........................................................... 5
3. Using Exabeam Cloud Archive To Search Your Data ................................................................. 7
   3.1. Navigating The Search Page .......................................................................................... 7
       3.1.1. Search Bar ......................................................................................................... 7
       3.1.2. Search Results Timeline ..................................................................................... 7
       3.1.3. Search Results List ............................................................................................. 8
   3.2. Export The Cloud Archive Search Result ....................................................................... 10
   3.3. Search Best Practices .................................................................................................. 11
       3.3.1. Narrowing Down The Time Range ..................................................................... 11
       3.3.2. Using Field Names And Values .......................................................................... 11
4. Technical Support Information .............................................................................................. 13
1. About Exabeam Cloud Archive

Exabeam Cloud Archive is a cloud-based log storage service that offers long-term data retention along with search capabilities. Similar to Exabeam Data Lake, Cloud Archive presents log data to the user in a clear and consumable manner. While Data Lake goes further in providing visualization, dashboards and other reporting functionalities, Cloud Archive excels in providing an affordable storage cost while preserving search capabilities.

You can use Cloud Archive to search for log events captured months or years ago, and to scan for new indicators such as IP addresses or domain names over extended periods of time. In addition, Cloud Archive makes it easier for your organization to meet multi-year log retention requirements imposed by regulations such as PCI-DSS, Sarbanes-Oxley or HIPPA.

Cloud Archive is available to Exabeam SaaS Cloud customers, and can be used with Exabeam Data Lake or Exabeam Advanced Analytics.

The Cloud Archive service is automatically provisioned as part of your Exabeam SaaS Cloud deployments and no further configuration steps are required for log data to enter the archive.
2. Exabeam Cloud Archive Architecture

Cloud Archive is a cloud native, multi-tenant, log aggregation service, designed to handle very large data volumes. As described in the diagram below, Cloud Archive directly integrates with the Exabeam SaaS Cloud infrastructure to import all received logs. Cloud Archive indexes and stores logs in a cloud native object store, then makes those logs available through its search service. Logs in Cloud Archive are parsed the same way they are in Data Lake. To ensure parsing consistency, Cloud Archive synchronizes the parser configuration with Data Lake every 24 hours.

Figure 1. Cloud Archive architecture

NOTE
Cloud Archive optimizes for storage cost and not search speed. Searches may take seconds to complete in Data Lake, but the same search query may take several minutes to complete in Cloud Archive.

2.1. Exabeam Cloud Archive Technical Specifications

Cloud Archive is an application deployed within the Exabeam Cloud Platform, which is hosted on the Google Cloud Platform.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Provider</td>
<td>Google Cloud</td>
</tr>
<tr>
<td>Geographical Regions</td>
<td>North America (us-west)</td>
</tr>
<tr>
<td></td>
<td>Europe (europe-west3, Frankfurt)</td>
</tr>
<tr>
<td>Maximum events per Second (EPS)</td>
<td>200,000 EPS per tenant</td>
</tr>
<tr>
<td>Maximum retention</td>
<td>10 years</td>
</tr>
<tr>
<td>Maximum search query length</td>
<td>1 million characters</td>
</tr>
<tr>
<td>Maximum concurrent searches</td>
<td>5 per tenant</td>
</tr>
</tbody>
</table>
Log data received by Exabeam SaaS Cloud may take up to 4 hours to appear in Cloud Archive. Analysts should account for this possible delay when looking at recent events.
3. Using Exabeam Cloud Archive to Search Your Data

This chapter walks through the process of performing a search and understanding the results. The search capabilities in Cloud Archive are designed to match those of Exabeam Data Lake. While not identical, the search syntax and user interface of Cloud Archive will be familiar to any analyst who has previously used Data Lake.

3.1. Navigating the Search Page

3.1.1. SEARCH BAR
At the top of the page is a search bar where you can enter a simple text search or use the Lucene query syntax to search your data. Once you have entered a query, select an appropriate time range using the date and time selector located to the left of the Search button. Click Search to launch your query: the search will run and display results as soon as they are available.

![Search Bar before query input](image1)

![Search Bar before search action](image2)

![Search bar during search operation](image3)

Figure 2. Search Bar before query input

Figure 3. Search Bar before search action

Figure 4. Search bar during search operation

Searches typically take several minutes to complete, depending on the data volume, the size of the time range, and the complexity or nature of the query. Click Cancel to edit your query or interrupt the search.

3.1.2. SEARCH RESULTS TIMELINE
Once the search has completed, Cloud Archive will display a histogram chart underneath the search bar. The timeline presents the count of events over the selected time range. Click any of the bars in the chart to further filter the search. After clicking a bar, or dragging over a group of bars, click the zoom-in magnifier icon to filter the results.
The time range associated with each column dynamically adjusts based on the time range of your search. Each column may represent minutes, hours, or days in the timeline depending on how wide the search range is.

### 3.1.3. SEARCH RESULTS LIST

When you submit a search request the Timeline and Events List are updated to reflect the search results. The most recent events that match the query are displayed in the Events List.

#### 3.1.3.1. Lines Per Event

By default, the list displays the first 3 lines of each log event. Click the Lines Per Event control to change the number of lines displayed.

#### 3.1.3.2. Rows Per Page and Pager

The list displays up to 100 events by default. Click **Rows Per Page** and select the number of lines that you want to display. Alternatively, use the control on the pager to navigate the search results pages.

#### 3.1.3.3. Event Details

Click any event to reveal the full raw message of the event, along with the entire list of parsed fields for that event. The **Event Details** panel also offers controls to display or hide fields in the events list. Use the **Eye** icon to toggle whether a field is visible in the list of events.
3.1.3.4. Search Results Table

To display the search results in a tabular format, select the **Table** option in the **Event View** control. In Table view, a column is created for each visible field of the listed events. Use the Customize Fields dialog to control the visibility and order of the columns. While in Table view, click any event to display its full details in the Event Details panel.

![Figure 8. Search Results Table](image)

3.1.3.5. Field Templates

The List and Table view present a default selection of fields per event that is curated based on the event’s category. Analysts can change what fields are made visible by selecting one of the templates listed in the **Field Template** picklist. Each template provides a different selection that is appropriate for the category. Analysts can also create their own templates by clicking **Add New Field Template**.

![Figure 9. Field Template List](image)

To add a new Field Template:

1. Click **Add New Field Template**.
2. In the New Field Template dialog, select whether you would like to start from a blank template, from the currently visible fields or from one of the existing templates, then click Next.

3. In the Configure Template step, enter a name for your template and select the fields to make visible from the Available Fields and Displayed Fields lists.

4. When your configuration is complete, click Save. The new template will automatically be selected under Field Template.

Keep in mind that Field Templates are shared across analysts, new field templates created by an analyst will be visible to all other analysts in the same environment.

3.2. Export the Cloud Archive Search Result

Use Cloud Archive's export functionality to download the search results to your local computer. You can capture the results and attach them to another system, for example a ticketing system, or when you need to work with the data outside of Cloud Archive's interface.

Cloud Archive Export allows output in the following formats:

- **Raw Log (txt)** -- This format exports the events in a plain text file and separates each event by a carriage return line feed (CRLF). Use this format to attach events as evidence in a ticketing system, or to input the data into another tool such as the Exabeam Auto Parser Generator.

- **Time and Raw Log (csv)** -- This format exports the events in a comma separated value (CSV) file, where the first column includes the normalized ingestion time for the event, and the second column includes the raw message of the event. Use this format to import the search results into a spreadsheet, or into a tool that uses the time information present in the events.

The export file is compressed in gzip format. Depending on the export format selected, the file's extension will be `.txt.gz` or `.csv.gz`.

To export events:
1. After or while a search is running, click **Export Events**.

2. Fill in the export parameters and then click **Export** to apply. The compressed exported events file will be downloaded to your local computer.

Exports include up to the most recent one million events.

### 3.3. Search Best Practices

Depending on the size of your environment, the logs stored in Cloud Archive may add up to petabytes of data. Searching through this much data can take a long time. However, there are several ways to speed up the search process.

#### 3.3.1. Narrowing Down the Time Range

This may be the most straightforward approach: the longer the time range selected in the Search Bar, the more data Cloud Archive will have to search. In most cases, the search duration will grow linearly with the number of days or months Cloud Archive needs to scan.

#### 3.3.2. Using Field Names and Values

Cloud Archive stores parsed fields and their values in a separate data partition that is typically much smaller than the raw data it ingested. By using field names and values in the query string, you can help Cloud Archive find logs more efficiently.

The following query, looking for user John within the Okta logs, will run slowly because it forces Cloud Archive to look for these keywords anywhere they might exist in the raw logs.

```
Okta john
```
This query leverages field names and values to point Cloud Archive to the smaller partition and will complete faster than the previous one.

vendor:"Okta" AND user:"john"
4. Technical Support Information

To contact Exabeam Customer Success, please open a case via Community.Exabeam.com.