# Log Management

### Armor Knowledge Base

**Topics Discussed**


- Search for Collected Logs in AMP
- Search for Collected Logs in Kibana (BETA)
- View Logging Subagent Status
- View Log Collections Projections
- Review Log Retention Plans
- Upgrade Default Log Retention for Existing Virtual Machines
- Upgrade Default Log Retention for New Virtual Machines
- Export Logs
- Extract Logs




To fully use this screen, you must add the following permissions to your account:

- Read Log Management
- Write Log Management
- Read Log Management Plan Selection
- Write Log Management Plan Selection

You can use the **Log & Data Management** screen to:

- View collected logs in the **Search** section
- View the status of the logging subagent in the **Sources** section

By default, Armor collects and retains the following log types for 30 days:

| CentOS/RHEL | Ubuntu/Debian | Windows |
|---|---|---|
| /var/log/secure | /var/log/auth.log | System Event Log |
| /var/log/messages | /var/log/syslog | Security Event Log |
| /var/log/audit.log | | |
| /var/log/audit/audit.log | | |
| /var/log/yum.log | | |



To learn how to upgrade your default log collection plan, see Review log retention plans.

## Search for Collected Logs in AMP



The Armor Management Portal (AMP) only displays logs from the previous 30 days.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **Search**.
    - Enter separate search terms within quotation marks.
    - Enter exact search terms, including letter capitalization.

| Column | Description |
|---|---|

| | |
|---|---|
| **Date** | This column displays the date and time when Armor received the corresponding log. |
| **Source** | This data shows the IP address of the virtual machine that generated the log. |
| **Message** | This column displays the specific log message. |

To better understand how to perform successful searches, consider the following sample log message:**2019-04-08T18:46:09Z INFO No non-zero metrics in the last 30s**

In a log message, spaces between words indicates a separate search term. For instance, there are no spaces in **2019-04-08T18:46:09Z**. As a result, **2019-04-08T18:46:09Z** is considered one search term. In this example, to search for dates, you must enter the complete and exact date; you cannot perform searches with partial search terms, such as 2019-04.

| Successful search parameters | Unsuccessful search parameters | Description |
|---|---|---|
| • "2019-04-08T18:46:09Z" | • 2019<br>• 2019-04-08T18:46:09Z | If the search term contains special characters, such as a colon, then you must perform the search with quotation marks ( " " ).<br><br>Also, in this example, the complete search term is **2019-04-08T18:46:09Z**. You cannot perform a search on partial search terms, such as **2019**. |
| • "INFO" | • INF | You cannot perform a search on partial search terms. In this example, the complete search term is **INFO**, not **INF**. |
| • "metrics" "30s" | • "metrics" "30" | You can search for different search terms by separating terms with quotation marks.<br><br>In this example, the complete search term is **30s**, not **30**. You cannot perform searches with partial search terms. |
| • *zero *30 | • *zero 30 | Similar to the use of quotation marks, you can also use an asterisk ( * ) to perform a wildcard search for strings.<br><br>A wildcard search may take a few more seconds to complete. |

## Search for Collected Logs in Kibana (BETA)

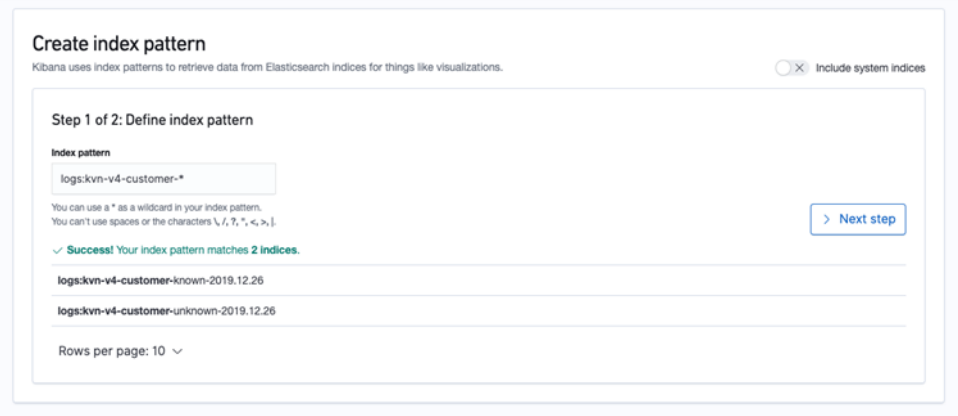
---

The **Kibana** log search feature is currently in a beta stage. **Armor has no level of support for this product during beta**. Please do **not** rely on this feature for production usage.

To search for logs in **Kibana**, you must have the **Read Log Search** permission assigned to your account.

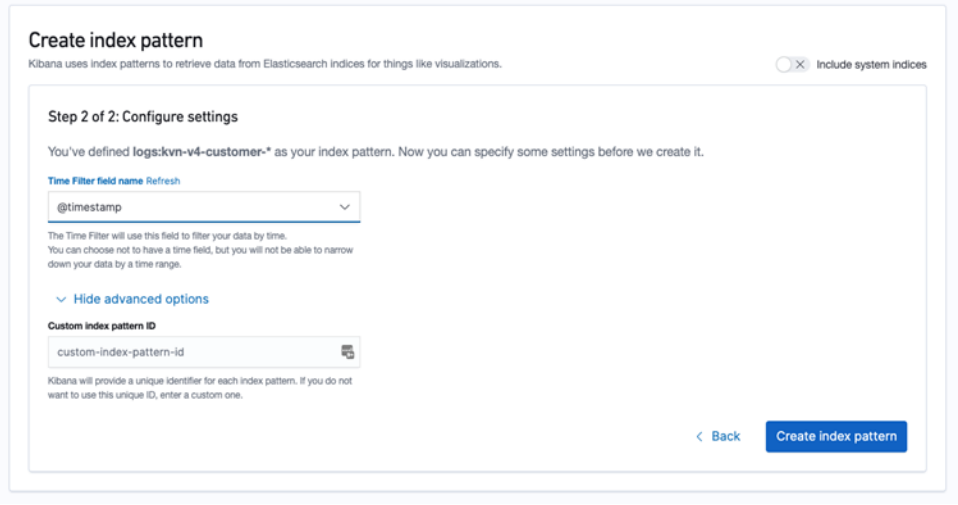
1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log Search - BETA**.
    a. You will be redirected to the **Kibana** log search tool.
3. Create an **Index Pattern**

a. Enter **logs:kvn-v4-customer-*** to the index pattern field.




b. Select **Next Step**

c. In **advanced options** drop-down, select "**@timestamp**" for **Time Filter** field name.




d. Select **Create index pattern**

4. In the left-hand navigation, at the bottom of the screen, click the **Expand** icon.
5. Click **Discover** to take you to the log search screen.

> ⚠ The banner at the top of the screen indicates that you are accessing the **Armor Kibana Beta**.
>
> To hide the banner, click **Dismiss**. Once you dismiss the banner, it will be permanently hidden from your view.

### Troubleshooting

**Request Timeout Error**

1. A query request will timeout in **Kibana** after 30 seconds, and return an **Error in visualization**. If you receive this error, retry the request. If the error is still returned, try adjusting your filter.

For more information on how to use the **Kibana** tool, visit the Kibana documentation.

## View Logging Subagent Status

You can use these instructions to review the logging status of your virtual machines. Specifically, you can verify if your virtual machine is sending logs to Armor.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **Agent Sources.**

| Column | Description |
|---|---|
| **Name** | This column displays the name of the virtual machine or instance that contains the Armor agent.<br><br>You can click a specific virtual machine to access the **Virtual Machines** screen. |
| **Type** | This column displays if the virtual machine or instance has been converted to a log collecting device, also known as **Log Relay**. |
| **Last Log Received** | This column displays the date and time when Armor last received a log. |
| **Retention Type** | This column displays the length of time that Armor keeps logs.<br>By default, the Armor Management Portal (AMP) retains log status and details for the previous 30 days. To review logs older than 30 days for a specified instance, see Review log retention plans. |
| **Average Size** | This column displays the average size of the collected logs. |
| **Log Status** | This column displays the status of the logging subagent.<br><br>1. **Online** indicates the agent has sent logs within the past hour.<br>2. **Warning** indicates the agent in the past 24 hours has sent logs that exceeds the 7-day moving average by 10% or more.<br>3. **Critical** indicates the agent has not sent logs within the past hour.<br>4. **Offline** indicates the agent (or the instance) is offline. |

## View Log Collections Projections

You can use these instructions to review AMP's prediction regarding future log collection. You can use this information to estimate log collection cost.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **Retention Plan**.
4. In the bottom of the screen, review the **Total Log Storage** graph.
    - The dotted line indicates AMP's prediction for your future log collections.

## Review Log Retention Plans

| Plan name | Log retention rate | Description |
|---|---|---|
| **Log Management Essentials** | 30 days | This plan collects and stores your **default log types** for 30 days, which you can view in AMP.<br><br>By default, users are automatically subscribed to this plan.<br><br>⚠ To make sure that you do not pass the default log collection limit, Armor recommends that you review the:<br><br>1. **Daily Log Storage Usage** graph in the **Summary** section<br>2. **Total Log Storage** graph in the **Retention Plan** section |
| **Compliance Professional** | 13 months | This plan collects and stores your **default log types** for 13 months at an additional cost.<br><br>Logs from the previous 30 days are visible in AMP; however, to view logs older than 30 days, you must send a support ticket. |

| | | |
|---|---|---|
| | | **For existing virtual machines:**<br><br>After you select this plan, existing virtual machines will not be automatically enrolled in this plan; you must update each virtual machine separately.<br><br>To learn more, see Upgrade log retention for **existing** virtual machines.<br><br>**For future virtual machines:**<br><br>After you select this plan, new virtual machines will be automatically enrolled in this plan.<br><br>To learn more, see Upgrade log retention for **new** virtual machines. |

## Upgrade Default Log Retention for Existing Virtual Machines

You can use these instructions to upgrade the default log retention rate for an existing virtual machine.

In order to add and update your plan, you must have the following permissions assigned to your account:

- Read Log Management Plan Selection
- Write Log Management Plan Selection
- Read LogManagement
- Write LogManagement

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **Agent Sources**.
4. Locate and hover over the desired virtual machine.
5. Click the vertical ellipses.
6. Select **Upgrade Plan**.
7. Review the pricing information, and then select **Upgrade Local Storage Plan**.
8. (Optional) Repeat these steps for additional existing virtual machines.

## Upgrade Default Log Retention for New Virtual Machines

You can use these instructions to update the default log retention plan for future virtual machines. In short, after you perform this step, any virtual machine you create afterwards will be automatically enrolled in the 13-month log retention plan.

For pricing information, please contact your account manager.

Existing virtual machines will not be upgraded. To upgrade the log retention rate for existing virtual machines, you must update each existing virtual machine individually.

To learn more, see Upgrade log retention for **existing** virtual machines.

In order to add and update your plan, you must have the following permissions assigned to your account:

- Read Log Management Plan Selection
- Write Log Management Plan Selection
- Read LogManagement
- Write LogManagement

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **Retention Plan**.

4. For **Compliance Professional**, click **Choose This**.
5. Review the product information, and then click **Select Plan**.
    - Now when you create a virtual machine, the machine will be automatically enrolled in this updated log retention plan.
    - To learn how to create a virtual machine, see ANYWHERE Virtual Machines or Virtual Machines.

## Export Logs

You can export the logs that are displayed in the Armor Management Portal (AMP) to analyze offline or to provide to an auditor.

This file export will only contain logs from the previous 30 days, up to 10,000 messages.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **Search**.
4. (Optional) Use the filter function to customize the data displayed.
5. Under the table, click **CSV.**
    - You have the option to export all data (**All**) or only the data that appears on the current screen (**Current Set**).

| Data Type | Data Detail |
|---|---|
| **Date** | This data shows the date and time when Armor received the corresponding log. |
| **Source** | This data shows the IP address of the virtual machine that generated the log. |
| **Message** | This data shows the specific log message. |

## Extract Logs

Customers who are enrolled in Armor's 13-month log retention plan can request to have logs extracted through Armor Support after 40 days of log collection.

> For more information on log retention plans, see Review log retention plans.

To learn how to submit a request to Armor Support, see Create a support ticket.

Review the following requirements before submitting your log extraction request to Armor Support.

### Review Requirements

| Requirement Type | Description |
|---|---|
| **Supported Storage Methods** | **s3 bucket**<br>1. A globally unique S3 bucket name must be provided to Armor Support<br>2. Access to the S3 bucket must be provided (IAM)<br>a. Access keys<br>3. File type: JSON<br><br>**Physical hard drive**<br>1. File type: JSON |
| **Unsupported Storage Methods** | Armor does not support the following storage methods:<br>1. Azure Blobs<br>2. GCP Storage<br>3. CSV format (Excel) |

### Troubleshooting

If you do not see any data in the **Search** section or the **Sources** section of the **Log & Data Management** screen, consider that:

1. The selected date range does not contain any data.
2. The virtual machine may be powered off.
3. You do not have permission to view log data.
    a. You must have the **ReadLogManagement** permission enabled to view log data. Contact your account administrator to enable this permission. To learn how to update your permissions, see Roles and Permissions.

If you cannot add or update your plan, consider that you do not have permission to update your plans. You must have the following permissions enabled:

1. Read Log Management Plan Selection
2. Write Log Management Plan Selection
3. Read LogManagement
4. Write LogManagement

## Related Documentation

To learn how to collect and send additional log types to AMP, see Introduction to Log Relay.