Log Management

Armor Knowledge Base

Topics Discussed

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

- Read LogManagement
- Write LogManagement
- 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

⚠ 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 column displays the name 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 • 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 (" "). 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. 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. A wildcard search may take a few more seconds to complete.

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. 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. 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. • **Online** indicates the agent has sent logs within the past hour. • **Warning** indicates the agent in the past 24 hours has sent logs that exceeds the 7-day moving average by 10% or more. • **Critical** indicates the agent has not sent logs within the past hour. • **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. By default, users are automatically subscribed to this plan. ⚠ To make sure that you do not pass the default log collection limit, Armor recommends that you review the: • **Daily Log Storage Usage** graph in the **Summary** section • **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. 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:** After you select this plan, existing virtual machines will not be automatically enrolled in this plan; you must update each virtual machine separately. To learn more, see Upgrade log retention for **existing** virtual machines. ⚠ **For future virtual machines:** After you select this plan, new virtual machines will be automatically enrolled in this plan. 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 Log Service Status

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.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **Log Sources**.
4. (Optional) Use the filter function to customize the data displayed.
5. Under the table, click **CSV.**
6. 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
Vm Name	This data shows the name of the Armor Agent.
Last Log Date	This data shows the last date that Armor received logs. A blank entry indicates that the action has never taken place.
Vm Provider	This data shows if you are an **Anywhere** or **Complete** user. If Armor cannot determine your specific environment, such as AWS or Azure, then by default, this entry will say **Anywhere**.
Vm Location	This data shows the virtual data center that hosts your data.
Retention	This data shows how long the logs are stored in the Armor user interface.
Average Size	This data shows the average log size.
Agent	This data shows the status of your Armor Agent.

Status	**Online** - This status means the Armor Agent is active and has sent logs within the last hour. **Warning** - This status means the previous 24-hour log volume has exceeded the 7-day moving average by 10% or more. **Critical** - This status means the Armor Agent has not sent logs within the last hour. **Offline** - This status means that the Armor Agent, and possibly the virtual machine, is offline.

Troubleshooting

Search section or Sources section

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

- The selected date range does not contain any data.
- The virtual machine may be powered off.
- You do not have permission to view log data.
    - 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.

Retention Plan section

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:

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

Related Documentation

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

Was this helpful?

Your Rating: ☆☆☆☆☆ Results: ★★★★★ 4 rates