![vmware by Broadcom logo]

VMware Aria Operations for Logs 8.14

Table of Contents

Introduction

Release	Date	Build Number
VMware Aria Operations for Logs 8.14.1	23 NOV 2023	22806512

Note: If you have already upgraded from VMware Aria Operations for Logs version 8.12 or 8.12 Hot Fix 1 to version 8.14 or 8.14 with the Hot Fix, we recommend that do not upgrade to version 8.14.1. The upgrade from version 8.14 or 8.14 with the Hot Fix to version 8.14.1 can fail depending on the cluster size, which is a known issue.

Check for additions and updates to these release notes.

About VMware Aria Operations for Logs

VMware Aria Operations for Logs delivers the best real-time and archived log management, especially for VMware environments. Machine learning-based intelligent grouping and high performance search enables faster troubleshooting across physical, virtual, and cloud environments. VMware Aria Operations for Logs can analyze terabytes of logs, discover structure in unstructured data, and deliver enterprise-wide visibility using a modern web interface.

For more information, see the VMware Aria Operations for Logs product documentation.

What's New

In addition to the features and issues resolved by VMware Aria Operations for Logs 8.14, here are some of the additional upgrade issues resolved in the 8.14.1 version:

Upgrade to VMware Aria Operations for Logs 8.14

While upgrading to VMware Aria Operations for Logs 8.14, the worker nodes are not upgraded after the primary node upgrade is complete. The manual workaround described in KB-95323 is automated in the 8.14.1 release to make sure the worker nodes are upgraded successfully.

Network-related issues while upgrading from 8.12 to 8.14

While upgrading VMware Aria Operations for Logs version 8.12 to version 8.14, the primary node doesn't receive the complete network configuration. Therefore, it becomes inconsistent and blocks the rolling upgrade of the cluster. This problem primarily impacts clusters where the network is configured manually. The manual upgrade fails with similar symptoms as described in KB - 83225.

Certificate fixes while adding a new node

The newly joined node fails to apply the custom certificate uploaded to the cluster.

Active Directory user is locked after a single incorrect login attempt

When VMware Aria Operations for Logs is integrated with Active Directory and there are multiple domain controllers, a single incorrect login attempt might lock the user in Active Directory.

Compatibility

VMware Aria Operations for Logs 8.14.1 can be integrated with the following VMware products and versions:

- VMware vCenter Server 7.0 or later (FIPS mode supported).
- VMware Aria Operations 8.6 or later.

You can install and upgrade VMware Aria Operations for Logs using VMware Aria Suite Lifecycle. For more information, see the VMware Aria Suite Lifecycle Installation, Upgrade, and Management Guide.

Browser Support

VMware Aria Operations for Logs 8.14.1 supports the following browser versions. More recent browser versions also work with VMware Aria Operations for Logs, but have not been validated.

- Mozilla Firefox 80.0 and above
- Google Chrome 91.0 and above
- Safari 13.1.2 and above
- Microsoft Edge 91.0 and above

The minimum supported browser resolution is 1280 by 800 pixels.

Important: Cookies must be enabled in your browser.

VMware Aria Operations for Logs Agent Support

VMware Aria Operations for Logs Windows Agent Support

The VMware Aria Operations for Logs 8.14.1 Windows agent supports the following versions:

- Windows 10, Windows 11 (supported, but not tested)
- Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.

VMware Aria Operations for Logs Linux Agent Support

The VMware Aria Operations for Logs 8.14 Linux agent supports the following distributions and versions:

- RHEL 7, RHEL 8, and RHEL 9
- SLES 12 SP5 (supported, but not tested), and SLES 15 SP3 (supported, but not tested)
- Ubuntu 18.04, Ubuntu 20.04, and Ubuntu 22.04
- Debian 10, and Debian 11
- VMware Photon version 3, and Photon version 4 (supported, but not tested)

Upgrading from a Previous Version of VMware Aria Operations for Logs

Keep in mind the following considerations when upgrading to VMware Aria Operations for Logs 8.14.1.

Upgrade Path

You can upgrade to VMware Aria Operations for Logs 8.14.1 from version 8.12 or 8.12 Hot Fix 1. If you have already upgraded from VMware Aria Operations for Logs version 8.12 or 8.12 Hot Fix 1 to version 8.14 or 8.14 with the Hot Fix, we recommend that do not upgrade to version 8.14.1. The version 8.14 with the Hot Fix resolves the same upgrade related issues that version 8.14.1 resolves.

Starting from VMware Aria Operations for Logs version 8.14.1, the upgrade process enables secure authenticated mode for inter-node communication. However, this mode is enabled only if the rolling upgrade is successful. It is not updated in case of a manual upgrade.

> **IMPORTANT**
>
> When you upgrade from version 8.12 or 8.12 Hot Fix 1 to 8.14.1, note that:
>
> - The upgrade process automatically restarts the clusters to enable secure authenticated inter-node communication in them.
> - The `PRI` and `VERSION` prefixes are not automatically added to raw logs in your log forwarding destination when you select the RAW Protocol. You must manually select the **Adjust PRI/VERSION** option to add these prefixes. See Add a Log Forwarding Destination to learn more. This option is a temporary accommodation to support certain configurations and will be phased out in future releases of the product to uphold the principle of raw forwarding.

Important Upgrade Notes

- To upgrade to VMware Aria Operations for Logs 8.14.1, you must be running VMware Aria Operations for Logs version 8.12 or 8.12 Hot Fix 1.
- When performing a manual upgrade from the command line, you must upgrade workers one at a time. Upgrading more than one worker at the same time causes an upgrade failure.
- When you upgrade the primary node to VMware Aria Operations for Logs 8.14.1 from the user interface, a rolling upgrade occurs unless specifically disabled.
- Upgrading must be done from the primary node's FQDN. Upgrading with the Integrated Load Balancer IP address is not supported.
- VMware Aria Operations for Logs does not support two-node clusters. Add a third VMware Aria Operations for Logs node of the same version as the existing two nodes before performing an upgrade.
- Photon OS has strict rules for the number of simultaneous SSH connections. Because the MaxAuthTries value is set to 2 by default in the `/etc/ssh/sshd_config` file, the SSH connection to your VMware Aria Operations for Logs virtual appliance might fail in the presence of multiple connections, with the following message: "Received disconnect from xx.xx.xx.xxx port 22:2: Too many authentication failures". You can use any of the following workarounds for this issue:
  - Use the `IdentitiesOnly=yes` option while connecting via SSH: `#ssh -o IdentitiesOnly=yes user@ip`
  - Update the `~/.ssh/config` file to add: `Host* IdentitiesOnly yes`
  - Change the `MaxAuthtries` value by modifying the `/etc/ssh/sshd_config` file and restarting the sshd service.
- The VM's SSH fingerprint is not preserved and changes after every upgrade, which might impact the appearance and user interface for users who connect using SSH. You must accept a new SSH fingerprint after the upgrade.
- Any API traffic sent to a VMware Aria Operations for Logs instance on port 443 will be rejected. Although port 443 has never been declared for API traffic, it used to work before and will not work starting from version 8.10. Instead, use the recommended port 9543.

Internationalization Support

VMware Aria Operations for Logs 8.14.1 includes the following localization features:

- The VMware Aria Operations for Logs web user interface is localized to Japanese, French, Spanish, German, Simplified Chinese, Traditional Chinese, and Korean.
- The VMware Aria Operations for Logs web user interface supports Unicode data, including machine learning features.
- VMware Aria Operations for Logs agents work on non-English native Windows.

Limitations

VMware Aria Operations for Logs 8.14.1 has the following limitations:

General

- VMware Aria Operations for Logs does not handle non-printable ASCII characters correctly.
- VMware Aria Operations for Logs does not support printing. However, you can use the **Print** options of your browser. The printed results might vary depending on the browser that you use. We recommend Internet Explorer or Firefox for printing portions of the VMware Aria Operations for Logs user interface.
- The hosts table might display devices more than once with each in a different format, including some combination of IP address, hostname, and FQDN. For example, a device named foo.bar.com might appear as both foo and foo.bar.com. The hosts table uses the **hostname** field that is defined in the syslog RFC. If an event sent by a device over the syslog protocol does not have a hostname, VMware Aria Operations for Logs uses the source as the hostname. This might result in the device being listed more than once because VMware Aria Operations for Logs cannot determine if the two formats point to the same device.
- Adding a new index partition or deleting an existing one requires a cluster restart (restarting cluster nodes one by one) for the new configuration to become effective. However, changes in the routing filter, enabled status, and retention period for existing index partitions apply immediately (restarting the cluster is not required).
- Once activated, FIPS mode cannot be disabled.

VMware Aria Operations for Logs Windows and Linux Agents

- Non-ASCII characters in **hostname** and **source** fields are not delivered correctly when VMware Aria Operations for Logs Windows and Linux agents are running in syslog mode.

VMware Aria Operations for Logs Windows Agent

- The VMware Aria Operations for Logs Windows agent is a 32-bit application and all its requests for opening files from **C:\Windows\System32** sub-directories are redirected by WOW64 to **C:\Windows\SysWOW64**. However, you can configure the VMware Aria Operations for Logs Windows agent to collect from **C:\Windows\System32** by using the special alias **C:\Windows\Sysnative**. For example, to collect logs from their default location for the MS DHCP Server, add the following line to the corresponding section of the VMware Aria Operations for Logs Windows agent configuration file: **=C:\Windows\Sysnative\dhcp**.

VMware Aria Operations for Logs Linux Agent

- Due to an operating system limitation, the VMware Aria Operations for Logs Linux agent does not detect network outages when configured to send events over syslog.
- The VMware Aria Operations for Logs Linux agent does not support non-English (UTF-8) symbols in field or tag names.
- The VMware Aria Operations for Logs Linux agent collects hidden files and directories by default. To prevent this, you must add an **exclude=.*** option to every configuration section. The option **exclude** uses the glob pattern **.*** which represents hidden file format.
- When standard output redirection to a file is used to produce logs, the VMware Aria Operations for Logs agent might not correctly recognize event boundaries in such log files.

VMware Aria Operations for Logs Integrations

Launch in context, both from VMware Aria Operations for Logs and VMware Aria Operations, does not work for a virtual machine when the IP address of the virtual machine is not visible to the VMware Aria Operations instance and is not shown by the vCenter on the virtual machine's **VM Summary** tab. The IP address might be unavailable because of the absence of the vmware-tools utility. Older, unsupported versions or malfunctioning vmware-tools can also cause the IP address to become unavailable.

Ensure that a proper version of VMware Tools is installed on the virtual machine and that the **VM Summary** tab of the vCenter displays the IP address of the virtual machine.

Resolved Issues

Resolutions for the following issues are included in this release.

- **VMware Aria Operations for Logs cannot connect to a webhook server with a self-signed certificate.**

  You cannot integrate VMware Aria Operations for Logs with a webhook server that uses a self-signed certificate as the self-signed certificate is not trusted.

- **The triggered alert is listed in the history but not delivered to VMware Aria Operations and email.**

  After integrating the VMware Aria Operations for Logs 8.10.2 version with VMware Aria Operations, when you configure an alert, add extracted fields to the alert query, and trigger an alert, the alert is not delivered to the email recipients and to the VMware Aria Operations user interface.

- **The first token in the vCenter Server logs is truncated when forwarded from VMware Aria Operations for Logs using the Syslog format.**

  If the VMware Aria Operations for Logs forwarder is configured to use Syslog forwarding, the first token in the vCenter Server logs may be truncated at the forwarding destination.

- **The test alert sent to a webhook URL fails because of basic authentication issues.**

  When you create a webhook of **Custom** endpoint type, add basic authentication to the webhook, and then test the alert, the alert fails. This happens when the credentials are rejected because of basic authentication issues.

- **While attempting to import archived logs, the import process became stuck and never reached completion.**

  When you are importing a large number of archived events back into VMware Aria Operations for Logs, the standard log importer tool fails, and displays a message such as
  `failed to import parsed messages from 0 to 1000` in the `/var/log/loginsight/importer.log` file. Additionally, the importer does not take into account disk blocks or ingestion speed.

Known Issues

The following known issues are present in this release.

- **Failure to save a configuration when there is a long list of filters in agent groups**

  VMware Aria Operations for Logs fails to process a long list of filters in agent groups and does not save any configuration because of this issue.

  Workaround: Modify the internal configuration manually to remove or reduce the number of filters in the agent group or divide the filters into multiple agent groups.

- **VMware Aria Operations for Logs does not send more than 10 logs in webhook notifications.**

  Regardless of the **Log Payload** option, VMware Aria Operations for Logs sends only up to 10 individual notifications or 10 logs in the payload to the webhook endpoint.

  Workaround: None.

- **Users are not notified about the cloud channel integration failure**

  You do not receive any notifications regarding failures related to cloud channel integration and cloud forwarding.

  Workaround: Check the VMware Aria Operations for Logs **runtime.log** file for related issues, or check if the corresponding cloud organization is receiving the logs.

- **Inactive host notifications are sent when logs are relayed to** VMware Aria Operations for Logs **(SaaS)**

  In VMware Aria Operations for Logs, when you select the **Inactive hosts notification** check box on the **Management > Hosts** page, and select the **Relay Only** option while configuring log forwarding to VMware Aria Operations for Logs (SaaS), you receive inactive host notifications.

  The value in the **Last Received Event** column in the **Hosts** page increases with time, which indicates that a previously active host does not ingest logs anymore.

  This behavior is because log events are not considered received until the events are ingested. When you select the **Relay Only** option for cloud forwarding, a certain category of log events are never ingested (depending on your filter definition), which results in some hosts mistakenly reporting as non-ingesting and inactive.

  Workaround: None.

- **The first run for real-time alerts is delayed**

  The first run for a real-time alert is scheduled five minutes after creating or enabling the alert.

  Workaround: Wait for five minutes after creating or enabling a real-time alert for the scheduler to work as expected. After the first five minutes, the alert query is run every minute.

- **Collection from some of directories will not take place if they were created before agent start or re-configuration event**

  The logs are not collected from the newly created directories if you create the directories after re-configuring the agent.

  Workaround: To start directory monitoring, restart the service or update the agent configuration. You can update the agent configuration using the liagent.ini file or from the Server Admin Agents page.

- **No automatic upgrade for VMware Aria Operations for Logs Agent on Photon OS**

  You cannot automatically upgrade VMware Aria Operations for Logs Agent on Photon OS because Photon OS does not support the `gpg` command.

Workaround: Perform a manual upgrade.

- **SMTP configurations might not work for public mail servers through IPv6**

  SMTP configurations might not work with public email services such as Google and Yahoo, because these services leverage tighter restriction policies for IPv6.

  Workaround: Use an alternative mail server such as your corporate mail server, or create a dedicated server.

- **Integrating VMware Workspace ONE Access with VMware Aria Operations for Logs through IPv4 changes the redirect URL host to IPv6 address**

  When deploying a VMware Aria Operations for Logs virtual appliance, If you had selected the option to prefer IPv6 addresses, the redirect URL host list is always populated with IPv6 node addresses. This redirect URL does not work when integrating VMware Aria Operations for Logs with VMware Workspace ONE Access as VMware Workspace ONE Access does not support IPv6 addresses.

  Workaround: Create a different IPv4 virtual IP for the integration of VMware Aria Operations for Logs with VMware Workspace ONE Access.

- **Test connection fails for VMware Aria Operations for Logs Agent running on the Windows OS.**

  Test connection fails for VMware Aria Operations for Logs Agent running on the Windows OS, however the agent is able to successfully communicate and send logs to the VMware Aria Operations for Logs server.

  Workaround: None

Introduction

Release	Date	Build Number
VMware Aria Operations for Logs 8.14	19 OCT 2023	22564181

Check for additions and updates to these release notes.

About VMware Aria Operations for Logs

VMware Aria Operations for Logs delivers the best real-time and archived log management, especially for VMware environments. Machine learning-based intelligent grouping and high performance search enables faster troubleshooting across physical, virtual, and cloud environments. VMware Aria Operations for Logs can analyze terabytes of logs, discover structure in unstructured data, and deliver enterprise-wide visibility using a modern web interface.

For more information, see the VMware Aria Operations for Logs product documentation.

What's New

Here are some of the key highlights of the VMware Aria Operations for Logs 8.14 release:

Security Enhancements

- Inter-node communication authentication is bolstered for enhanced data protection and secure communication.
- The node joining process is security-hardened to reduce potential vulnerabilities. The existing API to add the node has been enhanced. To learn more, see KB 95121.

Content Pack Enhancements

New content packs are added to VMware Aria Operations for Logs in the 8.14 release and a few existing content packs are enhanced with bug fixes.

- New content packs:
  - OpenShift
  - Tanzu Kubernetes Grid
- Enhanced content packs:
  - VMware vSAN
  - VMware Workspace One
  - VMware Aria Suite Lifecycle

Support for Uploading Trusted Certificates via User Interface

You can now upload trusted certificates directly through the user interface. This simplifies the certificate management process. To learn more, see View and Remove SSL Certificates.

VMware NSX Advanced Load Balancer Support

VMware Aria Operations for Logs now supports the external VMware NSX Advanced Load Balancer, enabling more robust and flexible load-balancing configurations. To learn more, see the Working With VMware NSX Advanced Load Balancer documentation.

Stability Improvements

- Queries using the **=** (equality) operator are optimized both for predefined (static) and extracted (regex-based) numeric fields.
- Stability improvements are applied to log imports to ensure a seamless experience for managing and analyzing log data.

Platform Modernization

- The platform is updated to Photon 4 to provide enhanced performance and a more efficient operational experience.
- The platform is upgraded to Java Run-time Environment 11 to provide better compatibility and security features.

Security Fixes

This release resolves CVE-2023-34051, CVE-2023-34052. For more information on these vulnerabilities and their impact on VMware products, please see VMSA-2023-0021.

Compatibility

VMware Aria Operations for Logs 8.14 can be integrated with the following VMware products and versions:

- VMware vCenter Server 7.0 or later (FIPS mode supported).
- VMware Aria Operations 8.6 or later.

You can install and upgrade VMware Aria Operations for Logs using VMware Aria Suite Lifecycle. For more information, see the VMware Aria Suite Lifecycle Installation, Upgrade, and Management Guide.

Browser Support

VMware Aria Operations for Logs 8.14 supports the following browser versions. More recent browser versions also work with VMware Aria Operations for Logs, but have not been validated.

- Mozilla Firefox 80.0 and above
- Google Chrome 91.0 and above
- Safari 13.1.2 and above
- Microsoft Edge 91.0 and above

The minimum supported browser resolution is 1280 by 800 pixels.

Important: Cookies must be enabled in your browser.

VMware Aria Operations for Logs Agent Support

VMware Aria Operations for Logs Windows Agent Support

The VMware Aria Operations for Logs 8.14 Windows agent supports the following versions:

- Windows 10, Windows 11 (supported, but not tested)
- Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.

VMware Aria Operations for Logs Linux Agent Support

The VMware Aria Operations for Logs 8.14 Linux agent supports the following distributions and versions:

- RHEL 7, RHEL 8, and RHEL 9
- SLES 12 SP5 (supported, but not tested), and SLES 15 SP3 (supported, but not tested)
- Ubuntu 18.04, Ubuntu 20.04, and Ubuntu 22.04
- Debian 10, and Debian 11
- VMware Photon version 3, and Photon version 4 (supported, but not tested)

Upgrading from a Previous Version of VMware Aria Operations for Logs

Keep in mind the following considerations when upgrading to VMware Aria Operations for Logs 8.14.

Upgrade Path

You can upgrade to VMware Aria Operations for Logs 8.14 from version 8.12. Starting from VMware Aria Operations for Logs version 8.14, the upgrade process enables secure authenticated mode for inter-node communication. However, this mode is enabled only if the rolling upgrade is successful. It is not updated in case of a manual upgrade.

> **IMPORTANT**
>
> When you upgrade from the 8.12 version to 8.14, note that:
>
> - The upgrade process automatically restarts the clusters to enable secure authenticated inter-node communication in them.
> - The `PRI` and `VERSION` prefixes are not automatically added to raw logs in your log forwarding destination when you select the RAW Protocol. You must manually select the **Adjust PRI/VERSION** option to add these prefixes. See Add a Log Forwarding Destination to learn more. This option is a temporary accommodation to support certain configurations and will be phased out in future releases of the product to uphold the principle of raw forwarding.

Important Upgrade Notes

- To upgrade to VMware Aria Operations for Logs 8.14, you must be running VMware Aria Operations for Logs 8.12.
- When performing a manual upgrade from the command line, you must upgrade workers one at a time. Upgrading more than one worker at the same time causes an upgrade failure.
- When you upgrade the primary node to VMware Aria Operations for Logs 8.14 from the user interface, a rolling upgrade occurs unless specifically disabled.
- Upgrading must be done from the primary node's FQDN. Upgrading with the Integrated Load Balancer IP address is not supported.
- VMware Aria Operations for Logs does not support two-node clusters. Add a third VMware Aria Operations for Logs node of the same version as the existing two nodes before performing an upgrade.
- Photon OS has strict rules for the number of simultaneous SSH connections. Because the MaxAuthTries value is set to 2 by default in the `/etc/ssh/sshd_config` file, the SSH connection to your VMware Aria Operations for Logs virtual appliance might fail in the presence of multiple connections, with the following message: "Received disconnect from xx.xx.xx.xxx port 22:2: Too many authentication failures". You can use any of the following workarounds for this issue:
  - Use the `IdentitiesOnly=yes` option while connecting via SSH: `#ssh -o IdentitiesOnly=yes user@ip`
  - Update the `~/.ssh/config` file to add: `Host* IdentitiesOnly yes`
  - Change the `MaxAuthtries` value by modifying the `/etc/ssh/sshd_config` file and restarting the sshd service.
- The VM's SSH fingerprint is not preserved and changes after every upgrade, which might impact the appearance and user interface for users who connect using SSH. You must accept a new SSH fingerprint after the upgrade.
- Any API traffic sent to a VMware Aria Operations for Logs instance on port 443 will be rejected. Although port 443 has never been declared for API traffic, it used to work before and will not work starting from version 8.10. Instead, use the recommended port 9543.

Internationalization Support

VMware Aria Operations for Logs 8.14 includes the following localization features:

- The VMware Aria Operations for Logs web user interface is localized to Japanese, French, Spanish, German, Simplified Chinese, Traditional Chinese, and Korean.
- The VMware Aria Operations for Logs web user interface supports Unicode data, including machine learning features.
- VMware Aria Operations for Logs agents work on non-English native Windows.

Limitations

VMware Aria Operations for Logs 8.14 has the following limitations:

General

- VMware Aria Operations for Logs does not handle non-printable ASCII characters correctly.
- VMware Aria Operations for Logs does not support printing. However, you can use the **Print** options of your browser. The printed results might vary depending on the browser that you use. We recommend Internet Explorer or Firefox for printing portions of the VMware Aria Operations for Logs user interface.
- The hosts table might display devices more than once with each in a different format, including some combination of IP address, hostname, and FQDN. For example, a device named foo.bar.com might appear as both foo and foo.bar.com. The hosts table uses the **hostname** field that is defined in the syslog RFC. If an event sent by a device over the syslog protocol does not have a hostname, VMware Aria Operations for Logs uses the source as the hostname. This might result in the device being listed more than once because VMware Aria Operations for Logs cannot determine if the two formats point to the same device.
- Adding a new index partition or deleting an existing one requires a cluster restart (restarting cluster nodes one by one) for the new configuration to become effective. However, changes in the routing filter, enabled status, and retention period for existing index partitions apply immediately (restarting the cluster is not required).
- Once activated, FIPS mode cannot be disabled.

VMware Aria Operations for Logs Windows and Linux Agents

- Non-ASCII characters in **hostname** and **source** fields are not delivered correctly when VMware Aria Operations for Logs Windows and Linux agents are running in syslog mode.

VMware Aria Operations for Logs Windows Agent

- The VMware Aria Operations for Logs Windows agent is a 32-bit application and all its requests for opening files from **C:\Windows\System32** sub-directories are redirected by WOW64 to **C:\Windows\SysWOW64**. However, you can configure the VMware Aria Operations for Logs Windows agent to collect from **C:\Windows\System32** by using the special alias **C:\Windows\Sysnative**. For example, to collect logs from their default location for the MS DHCP Server, add the following line to the corresponding section of the VMware Aria Operations for Logs Windows agent configuration file: **=C:\Windows\Sysnative\dhcp**.

VMware Aria Operations for Logs Linux Agent

- Due to an operating system limitation, the VMware Aria Operations for Logs Linux agent does not detect network outages when configured to send events over syslog.
- The VMware Aria Operations for Logs Linux agent does not support non-English (UTF-8) symbols in field or tag names.
- The VMware Aria Operations for Logs Linux agent collects hidden files and directories by default. To prevent this, you must add an **exclude=.*** option to every configuration section. The option **exclude** uses the glob pattern **.*** which represents hidden file format.
- When standard output redirection to a file is used to produce logs, the VMware Aria Operations for Logs agent might not correctly recognize event boundaries in such log files.

VMware Aria Operations for Logs Integrations

Launch in context, both from VMware Aria Operations for Logs and VMware Aria Operations, does not work for a virtual machine when the IP address of the virtual machine is not visible to the VMware Aria Operations instance and is not shown by the vCenter on the virtual machine's **VM Summary** tab. The IP address might be unavailable because of the absence of the vmware-tools utility. Older, unsupported versions or malfunctioning vmware-tools can also cause the IP address to become unavailable.

Ensure that a proper version of VMware Tools is installed on the virtual machine and that the **VM Summary** tab of the vCenter displays the IP address of the virtual machine.

Resolved Issues

Resolutions for the following issues are included in this release.

- **VMware Aria Operations for Logs cannot connect to a webhook server with a self-signed certificate.**

  You cannot integrate VMware Aria Operations for Logs with a webhook server that uses a self-signed certificate as the self-signed certificate is not trusted.

- **The triggered alert is listed in the history but not delivered to VMware Aria Operations and email.**

  After integrating the VMware Aria Operations for Logs 8.10.2 version with VMware Aria Operations, when you configure an alert, add extracted fields to the alert query, and trigger an alert, the alert is not delivered to the email recipients and to the VMware Aria Operations user interface.

- **The first token in the vCenter Server logs is truncated when forwarded from VMware Aria Operations for Logs using the Syslog format.**

  If the VMware Aria Operations for Logs forwarder is configured to use Syslog forwarding, the first token in the vCenter Server logs may be truncated at the forwarding destination.

- **The test alert sent to a webhook URL fails because of basic authentication issues.**

  When you create a webhook of **Custom** endpoint type, add basic authentication to the webhook, and then test the alert, the alert fails. This happens when the credentials are rejected because of basic authentication issues.

- **While attempting to import archived logs, the import process became stuck and never reached completion.**

  When you are importing a large number of archived events back into VMware Aria Operations for Logs, the standard log importer tool fails, and displays a message such as
  `failed to import parsed messages from 0 to 1000` in the `/var/log/loginsight/importer.log` file. Additionally, the importer does not take into account disk blocks or ingestion speed.

Known Issues

The following known issues are present in this release.

- **Failure to save a configuration when there is a long list of filters in agent groups**

  VMware Aria Operations for Logs fails to process a long list of filters in agent groups and does not save any configuration because of this issue.

  Workaround: Modify the internal configuration manually to remove or reduce the number of filters in the agent group or divide the filters into multiple agent groups.

- **VMware Aria Operations for Logs does not send more than 10 logs in webhook notifications.**

  Regardless of the **Log Payload** option, VMware Aria Operations for Logs sends only up to 10 individual notifications or 10 logs in the payload to the webhook endpoint.

  Workaround: None.

- **Users are not notified about the cloud channel integration failure**

  You do not receive any notifications regarding failures related to cloud channel integration and cloud forwarding.

  Workaround: Check the VMware Aria Operations for Logs **runtime.log** file for related issues, or check if the corresponding cloud organization is receiving the logs.

- **Inactive host notifications are sent when logs are relayed to** VMware Aria Operations for Logs **(SaaS)**

  In VMware Aria Operations for Logs, when you select the **Inactive hosts notification** check box on the **Management > Hosts** page, and select the **Relay Only** option while configuring log forwarding to VMware Aria Operations for Logs (SaaS), you receive inactive host notifications.

  The value in the **Last Received Event** column in the **Hosts** page increases with time, which indicates that a previously active host does not ingest logs anymore.

  This behavior is because log events are not considered received until the events are ingested. When you select the **Relay Only** option for cloud forwarding, a certain category of log events are never ingested (depending on your filter definition), which results in some hosts mistakenly reporting as non-ingesting and inactive.

  Workaround: None.

- **The first run for real-time alerts is delayed**

  The first run for a real-time alert is scheduled five minutes after creating or enabling the alert.

  Workaround: Wait for five minutes after creating or enabling a real-time alert for the scheduler to work as expected. After the first five minutes, the alert query is run every minute.

- **Collection from some of directories will not take place if they were created before agent start or re-configuration event**

  The logs are not collected from the newly created directories if you create the directories after re-configuring the agent.

  Workaround: To start directory monitoring, restart the service or update the agent configuration. You can update the agent configuration using the liagent.ini file or from the Server Admin Agents page.

- **No automatic upgrade for VMware Aria Operations for Logs Agent on Photon OS**

  You cannot automatically upgrade VMware Aria Operations for Logs Agent on Photon OS because Photon OS does not support the `gpg` command.

Workaround: Perform a manual upgrade.

- **SMTP configurations might not work for public mail servers through IPv6**

SMTP configurations might not work with public email services such as Google and Yahoo, because these services leverage tighter restriction policies for IPv6.

Workaround: Use an alternative mail server such as your corporate mail server, or create a dedicated server.

- **Integrating VMware Workspace ONE Access with VMware Aria Operations for Logs through IPv4 changes the redirect URL host to IPv6 address**

When deploying a VMware Aria Operations for Logs virtual appliance, If you had selected the option to prefer IPv6 addresses, the redirect URL host list is always populated with IPv6 node addresses. This redirect URL does not work when integrating VMware Aria Operations for Logs with VMware Workspace ONE Access as VMware Workspace ONE Access does not support IPv6 addresses.

Workaround: Create a different IPv4 virtual IP for the integration of VMware Aria Operations for Logs with VMware Workspace ONE Access.

- **Test connection fails for VMware Aria Operations for Logs Agent running on the Windows OS.**

Test connection fails for VMware Aria Operations for Logs Agent running on the Windows OS, however the agent is able to successfully communicate and send logs to the VMware Aria Operations for Logs server.

Workaround: None

Using the VMware Aria Operations for Logs Importer (8.14)

Using the VMware Aria Operations for Logs Importer

Using the VMware Aria Operations for Logs Importer provides information about installing and running the VMware Aria Operations for Logs Importer.

The VMware Aria Operations for Logs Importer is a command-line utility used to import offline logs of historical data from local machines to the VMware Aria Operations for Logs server.

Use the Importer when you want to import logs that were collected in the past. You can import support bundles and archived logs and analyze logs from support bundles gathered from VMware Aria Operations for Logs or any VMware product.

VMware Aria Operations for Logs Importer includes the following features and capabilities.

- VMware Aria Operations for Logs Importer sends data over the ingestion API.
- It supports file log collection, including recursive directory collection.
- The Importer can read data from zip, tar, bzip, bzip2, or gz archive files. 7-Zip is not supported.
- You can stipulate that data be read recursively from a nested archive, such as a nested ZIP file, or from a directory within an archive.

Installing the VMware Aria Operations for Logs Importer

You install the VMware Aria Operations for Logs Importer Importer from an installation package you obtain from the VMware Download site. The installation packages include the MSI installer for Windows and POSIX installation packages (RPM, DEB and BIN) for Linux.

Before You Install the VMware Aria Operations for Logs Importer

Check requirements and understand importer behavior before you install the importer.

Before you install, ensure that VMware Aria Operations for Logs has access to the NFS server on which archived data is stored. If the NFS server becomes inaccessible due to network failure or errors on the NFS server, importation of archived data might fail.

When logs are extracted from a bundle during ingestion, a log bundle name is automatically determined and added as a bundle tag to all extracted logs. The tag name is the filename of the log or the directory name in case of directory sources. Bundle tags differentiate bundles on a VMware Aria Operations for Logs server.

This tag overrides any tags with the same name that are specified in the manifest file. The tag can be overridden by command line tags that use the same name.

When you use the importer, be aware of the following behaviors:

- VMware Aria Operations for Logs Importer does not check for available disk space on the VMware Aria Operations for Logs virtual appliance. Therefore, the import of archived logs might fail if the virtual appliance runs out of disk space.
- VMware Aria Operations for Logs does not display progress information during log imports. As the import of archived data is in progress, you are unable to infer from the console output how much time is left before the import finishes or how much data is already imported.

<u>**Supported Operating Systems**</u>

The VMware Aria Operations for Logs Importer is supported on the following operating systems:

- Windows 32 bit and 64 bit
- Linux 32 bit and 64 bit

The Linux version does not run on an Apple Macintosh system.

Install the VMware Aria Operations for Logs Importer

You can install VMware Aria Operations for Logs Importer on Windows and Linux. You can also install the VMware Aria Operations for Logs Importer on a VMware Aria Operations for Logs server and run it from the server.

- Verify that you can access the VMware Download site to download the VMware Aria Operations for Logs Importer.

When you install VMware Aria Operations for Logs Importer, several VMware product manifest files are also installed. You can use these files or modify them for your needs when running VMware Aria Operations for Logs Importer. These manifest files are located in `C:\Program Files (x86)\VMware\Log Insight Importer\Manifests` for Windows, and `/usr/lib/loginsight-importer/manifests` for Linux.

If you uninstall the `.bin` package, also delete the `/usr/bin/loginsight_importer` symlink.

1. Download the VMware Aria Operations for Logs Importer installation package from the VMware Download site.

   To locate the installation package, search for the relevant VMware Aria Operations for Logs version and open the corresponding download page. Under Drivers & Tools, expand the SDK section and click GO TO DOWNLOADS.

   The installation packages include the MSI installer for Windows and POSIX installation packages (RPM, DEB, and BIN) for Linux.

2. Install the tool on your system.

   After installation, the importer installation directory is added to the PATH environment variable on Windows, and a symlink to the executable file `loginsight-importer` is added to `/usr/bin/` on Linux. So the client can call `loginsight-importer` from the shell without specifying a path prefix.

   The VMware Aria Operations for Logs Importer tool is installed in the following locations.

Operating System	Filename	Installation Location
Windows	loginsight-importer.exe	C:\Program Files (x86)\VMware\Log Insight Importer
Linux	loginsight-importer	/usr/lib/loginsight-importer

Running the VMware Aria Operations for Logs Importer

When you run the importer, you must include a manifest file. The manifest file provides information about log format, the location of the data to import, and source and destination information.

About the VMware Aria Operations for Logs Importer Manifest File

VMware Aria Operations for Logs Importer uses a manifest configuration file to determine the log format and to specify the location of the data to import. The manifest file has the same format as the `liagent.ini` configuration file and is similar in structure.

Optionally, you can create your own manifest file to import arbitrary log files. One advantage of creating such a file is that you do not need to know the absolute path to the data files.

If you do not create a manifest file, VMware Aria Operations for Logs Importer uses the default manifest, which collects all `.txt` and `.log` files (`include=*.log*;*.txt*`) and applies the auto parser (extracts timestamp + kvp) on the extracted logs.

If the `liagent.ini` configuration file is used as a manifest file, VMware Aria Operations for Logs Importer extracts only the `[filelog]` sections as a manifest. All options for the `[filelog]` section are supported in VMware Aria Operations for Logs Importer.

For information about options supported in the `[filelog]` section and configuration examples, see the topic "Collect Events from a Log File" in the *Working with VMware Aria Operations for Logs Agents*.

To Create a Manifest File

You can copy and paste the contents of the agent configuration file into a new TXT file. To identify a dynamic path, remove the leading " / " before the directory path.

Specifying the Directory Path

The directory specified in the `[filelog]` section can be either relative to the source or absolute. To specify a relative path, do not include the leading slash under Linux, otherwise VMware Aria Operations for Logs Importer treats the path as absolute.

To indicate name patterns in the value of the directory key, you can use the `*` and `**` characters.

- Use `*` as a placeholder for a single directory. Use it to indicate one level of nesting with an arbitrary folder name. For example, use `directory = log_folder_*` to indicate any folder that starts with the string `log_folder_`.
- Use `**` to indicate an arbitrary level of nesting with any folder name. For example, you can use `directory = **/log` to indicate any folder with the name `log` at any level of nesting within the source directory.

Related Links

The sample VMware Aria Operations for Logs Importer manifest files provide examples of parameter configurations.

Run the VMware Aria Operations for Logs Importer to import offline logs of historical data to the VMware Aria Operations for Logs server.

VMware Aria Operations for Logs Importer Manifest File Configuration Examples

The sample VMware Aria Operations for Logs Importer manifest files provide examples of parameter configurations.

The value of the directory key must be either relative to the source or absolute. The following example shows how to collect logs from files with a `.log` extension which reside two levels lower than the source directory and name of the last folder ends with the `_log` string.

```
[filelog|importer_test]
directory=*\*_log
include=*.log
event_marker=^\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2} [A-Z]{4} LOG
```

The following example shows how to collect all files with the extension `.log` from all subfolders of the source directory including the source itself.

```
[filelog|sbimporter_test_channel]
directory = **
include = *.log
```

The following example shows how to collect logs from all files in the source directory (but not from subfolders) except files that have an `.ini` extension. We interpret files as UTF-16LE encoded.

```
[filelog|quotes_channe3]
directory=
charset=UTF-16LE
exclude=*.ini
tags={"Provider" : "Apache"}
```

The following example shows how to collect logs from all files with the extension `.log` in the source directory (but not from subfolders). The timestamp of events is parsed in the log file using the Common Log Format (CLF) parser and the extracted historical timestamp is applied. The log format parsed by the CLF parser is `2015-03-25 22:11:46,786 | DEBUG | pool-jetty-76 | AuthorizationMethodInterceptor | Authorizing method: public abstract`.

```
[filelog|vcd-container-debug]
directory=
include=*.log
parser=vcd

[parser|vcd]
base_parser=clf
format=%{%Y-%m-%d %H:%M:%S%f}t %M
```

Related Links

[About the VMware Aria Operations for Logs Importer Manifest File on page 38](#)
VMware Aria Operations for Logs Importer uses a manifest configuration file to determine the log format and to specify the location of the data to import. The manifest file has the same format as the `liagent.ini` configuration file and is similar in structure.

[Run the VMware Aria Operations for Logs Importer on page 40](#)
Run the VMware Aria Operations for Logs Importer to import offline logs of historical data to the VMware Aria Operations for Logs server.

Run the VMware Aria Operations for Logs Importer

Run the VMware Aria Operations for Logs Importer to import offline logs of historical data to the VMware Aria Operations for Logs server.

- Review About the VMware Aria Operations for Logs Importer Manifest File and create a manifest file to use with the importer. For more information, see Run the VMware Aria Operations for Logs Importer.
- If you use the `honor_timestamp` parameter, verify that you have appropriate login credentials.
- If you import a support bundle, configure `honor_timestamp` and the user name and password.

1. Start the VMware Aria Operations for Logs Importer tool by entering the following command at a command prompt.

   ```
   /usr/bin/loginsight-importer.exe
   ```

2. Enter the manifest file name at the prompt.

3. Define the configuration parameters and press **Enter**.

   The --source and --server parameters are required.

Required Parameters	Description
`--source <path>`	Specifies the path to a support bundle directory or path to a zip, gzip, bzip, bzip2, or tar archive. The value is added to all send messages as the value of the `bundle` tag.
`--server <hostname>`	Destination server hostname or IP address.

Options	Description
`--port <port>`	Port for connection. If not set then port 9000 is used for non-SSL connections and port 9543 is used for an SSL connection.
`--logdir <path>`	Specifies the path to the logs directory. If this is not set, the path is: `$(LOCALAPPDATA)\VMware \Log Insight Importer\log` on Windows and `~/.loginsight-importer/log` on Linux.
`--manifest <file-path>`	Specifies the path to the manifest file (.ini format). If this is not set, the `importer.ini` file in the source directory is used. If the `importer.ini` file does not exist or is not found in the source directory, VMware Aria Operations for Logs Importer applies the default (hardcoded) manifest and collects all `.txt` and `.log` files (`include=*.log*;*.txt*`), and also applies the auto parser (extracts timestamp + kvp).
`--no_ssl`	Do not use SSL for connections. This should not be set for authenticated connections (for example if --honor_timestamp is used).
`--ssl_ca_path <path>`	Path to the trusted root certificates bundle file.
`--tags <tags>`	Set tags for all sent events. For example `--tags "{ \"tag1\" : \"value1\", \"tag2\":\"value2\"}"` **NOTE** The tags option can accept `hostname` as a tag name. The value of the `hostname` tag from the command line is used instead of the FQDN of the sending machine as the value of the `hostname` field for all events extracted by VMware Aria Operations for Logs Importer. This is opposite of the tags parameter in the manifest file and extracted fields by parsers, which ignore the `hostname` field. **Note:** A log bundle name, either a filename or a directory name in case of directory sources, is automatically determined and added as a `bundle` tag to all logs extracted from that specific bundle during the ingestion. This tag helps you to differentiate bundles on the VMware Aria Operations for Logs Importer Server. A `bundle` tag overrides tags with that same name from a manifest file. But it can be overridden by command line tags, if there is one with `bundle` name.
`--username <username >`	Username for authentication. Required if `--honor_timestamp` is set.
`--password <password>`	Password for authentication. Required if `--honor_timestamp` is set. The username/password pair deactivates the allowed time-drift on VMware Aria Operations for Logs server so it is possible to import data with a historical timestamp.

Options	Description
`--honor_timestamp`	Applies the extracted timestamp. The configured parsers extract the timestamp from the log entries and the `--honor_timestamp` applies the extracted timestamp. • If the timestamp is extracted using configured parsers, then the events will have that timestamp applied. • If there is an event in the logs file, with no extracted timestamp, then the successfully extracted timestamp from the previous event in the same log file will be applied. • If no timestamp is found or parsed in the file then the `MTIME` of the log file will be applied as the timestamp. **NOTE** If a manifest file was not provided, the default hardcoded manifest that the VMware Aria Operations for Logs Importer will use has the Automatic Log parser enabled. In this case, VMware Aria Operations for Logs Importer extracts the timestamp from the log entries if the `--honor_timestamp` parameter is used.
`--debug_level <1|2>`	Increases the verbosity level of the log file. This should only be changed when troubleshooting. Under normal operations this flag should not be used.
`--help`	Display help and exit.

4. After the import is complete, press **Ctrl+C** on Windows or Linux to exit the tool.

VMware Aria Operations for Logs Importer extracts the log entries from the directories specified in the parameters. The total number of processed files, extracted log messages, sent log messages, and the run time is displayed.

From the VMware Aria Operations for Logs Explore Logs page, you can refresh the view to list the imported log events. If you imported a support bundle and used the `honor_timestamp`, the dashboard should also display the events over time.

Related Links

About the VMware Aria Operations for Logs Importer Manifest File on page 38

VMware Aria Operations for Logs Importer uses a manifest configuration file to determine the log format and to specify the location of the data to import. The manifest file has the same format as the `liagent.ini` configuration file and is similar in structure.

VMware Aria Operations for Logs Importer Manifest File Configuration Examples on page 39

The sample VMware Aria Operations for Logs Importer manifest files provide examples of parameter configurations.

Getting Started with Aria Operations for Logs (8.14)

Getting Started with VMware Aria Operations for Logs

Getting Started with VMware Aria Operations for Logs provides information about deploying and configuring VMware Aria Operations for Logs, including how to size the VMware Aria Operations for Logs virtual appliance to receive log messages.

Use this information when you want to plan or install your deployment. This information is written for experienced Linux and Windows system administrators who are familiar with virtual machine technology and data center operations. Administrators are users associated with the Super Admin role, or roles with the same permissions as the Super Admin role. For information about roles and permissions, see *Administering VMware Aria Operations for Logs*.

Before You Install VMware Aria Operations for Logs

To start using VMware Aria Operations for Logs in your environment, you must deploy the VMware Aria Operations for Logs virtual appliance and apply several basic configurations.

Supported Log Files and Archive Formats inVMware Aria Operations for Logs

You can useVMware Aria Operations for Logs to analyze unstructured or structured log data.

VMware Aria Operations for Logs accepts data from the following sources:

- Sources that support sending log streams with the syslog protocol.
- Sources that write log files and can run theVMware Aria Operations for Logs agent.
- Sources that can post log data with HTTP or HTTPS through the REST API. The API documentation is available fromVMware Aria Operations for Logs interface at `https://<operations_for_logs_host>/rest-api`.
- Historic data that was archived byVMware Aria Operations for Logs.

The vSphere log parser allows you to import vSphere log bundles inVMware Aria Operations for Logs.

> **NOTE**
> Although VMware Aria Operations for Logs can handle historic data and real-time data simultaneously, you are advised to deploy a separate instance of VMware Aria Operations for Logs to process imported log files.

See Import aVMware Aria Operations for Logs archive in *Administering VMware Aria Operations for Logs*.

Security Requirements

To ensure that your virtual environment is protected from external attacks, you must observe certain rules.

- Always install VMware Aria Operations for Logs in a trusted network.
- Always save VMware Aria Operations for Logs support bundles in a secure location.

IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of VMware Aria Operations for Logs must read the security topics in *Administering VMware Aria Operations for Logs*.

These topics provide concise references to the security features of VMware Aria Operations for Logs. Topics include the product external interfaces, ports, authentication mechanisms, and options for configuration and management of security features.

For information about securing your virtual environment, see the *VMware vSphere Security Guide* and the Security Center on the VMware Web site.

Product Compatibility

VMware Aria Operations for Logs collects data over the syslog protocol and HTTP. VMware Aria Operations for Logs can connect to vCenter Server to collect events, tasks, and alarms data; and can integrate with VMware Aria Operations to send notification events and enable launch in context. Check the *VMware Aria Operations for Logs Release Notes* for latest updates on supported product versions.

Virtual Appliance Deployment

You must deploy the VMware Aria Operations for Logs virtual appliance using vSphere. Always use a vSphere Client to connect to a vCenter Server. The VMware Aria Operations for Logs virtual appliance is deployed on an ESX/ESXi host version 5.0 or later that is managed by vCenter Server version 5.0 or later.

Syslog Feeds

VMware Aria Operations for Logs collects and analyzes syslog data over the following ports and protocols:

- 514/UDP
- 514/TCP
- 1514/TCP (SSL)

You must configure environment components such as operating systems, applications, storage, firewalls, and network devices to push their syslog feeds to VMware Aria Operations for Logs.

API Feeds

The VMware Aria Operations for Logs Ingestion API collects data over the following ports and protocols.

- 9000/TCP
- 9543/TCP (SSL)

vSphere Integration

You can configure VMware Aria Operations for Logs to pull data for tasks, events, and alarms that occurred in one or more vCenter Server instances. VMware Aria Operations for Logs uses the vSphere API to connect to vCenter Server systems and collect data.

You can configure ESXi hosts to forward syslog data to VMware Aria Operations for Logs.

For compatibility information with specific versions of vCenter Server and ESXi, see the VMware Product Interoperability Matrixes.

For information about connecting to a vSphere environment, see Connect to a vSphere Environment.

VMware Aria Operations Integration

VMware Aria Operations for Logs and VMware Aria Operations vApp or Installable can be integrated in two independent ways.

All supported versions of VMware Aria Operations support notifications as well as Launch in Context.

- VMware Aria Operations for Logs can send notification events to VMware Aria Operations.
  See Configure vRealize Log Insight to Send Notification Events to vRealize Operations.
- The launch in context menu of VMware Aria Operations can display actions related to VMware Aria Operations for Logs.
  See Enable Launch in Context for vRealize Log Insight in vRealize Operations.

Minimum Requirements

VMware distributes VMware Aria Operations for Logs as a virtual appliance in OVA file format. Various resources and applications must be available for the virtual appliance to run successfully. For the most up-to-date information about requirements, check the latest release notes.

Virtual Hardware

During deployment of the VMware Aria Operations for Logs virtual appliance, you can select from preset configuration sizes according to the ingestion requirements for your environment. The presets are certified size combinations of compute and disk resources, though you can add extra resources afterward. A small configuration, described in the following table, consumes the fewest resources while remaining supported. An extra-small configuration is also available, but it is suitable only for demos.

For complete resource requirements based on ingestion requirements, see Sizing the VMware Aria Operations for Logs Virtual Appliance.

Table 1: Preset Values for Small Configurations

Resources	Minimum Requirement
Memory	8 GB
vCPU	4
Storage Space	530 GB

Supported Browsers

You can use one of the following browsers to connect to the VMware Aria Operations for Logs web user interface. More recent browser versions also work with VMware Aria Operations for Logs, but have not been validated.

> **IMPORTANT**
> Cookies must be activated in your browser.

- Mozilla Firefox 45.0 and above
- Google Chrome 51.0 and above
- Safari 9.1 and above
- Internet Explorer 11.0 and above

> **NOTE**
>
> - Internet Explorer Document mode must be set to **Standards Mode**. Other modes are not supported.
> - **Browser Mode:** Compatibility View is not supported.
> - To use Internet Explorer with the VMware Aria Operations for Logs web client, Windows local storage integrity level must be configured as low.

Account Passwords

Type	Requirements
Root	Unless you specify a root password or use guest customization during the deployment of the OVA, the default credentials for the root user on the VMware Aria Operations for Logs virtual appliance are `root/<blank>`. You are prompted to change the root account password when you first access the VMware Aria Operations for Logs virtual appliance console. **NOTE** SSH is deactivated until you set the root password.
User Account	User accounts that you create in VMware Aria Operations for Logs 3.3 and later require a strong password. The password must be at least 8 characters long and contain one uppercase character, one lowercase character, one number, and one special character.

Integration Requirements

Product	Requirement
vCenter Server	To pull events, tasks, and alarms data from a vCenter Server, you must provide a set of user credentials for that vCenter Server. The minimum role required to register and unregister VMware Aria Operations for Logs with a vCenter Server is **Read-only**. The role must be set at the vCenter Server level and propagated to child objects. To configure ESXi hosts that a vCenter Server manages, VMware Aria Operations for Logs requires additional privileges.
vSphere ESXi	vSphere ESXi 6.0 update 1 or later is required to establish SSL connections to VMware Aria Operations for Logs.
VMware Aria Operations	To activate notification events and the launch-in-context functionality in a VMware Aria Operations instance, you must provide user credentials for that VMware Aria Operations instance.

Network Port Requirements

The following network ports must be externally accessible.

Port	Protocol
22/TCP	SSH
80/TCP	HTTP
443/TCP	HTTPS
514/UDP, 514/TCP	Syslog
1514/TCP	Syslog ingestion via SSL only
9000/TCP	VMware Aria Operations for Logs Ingestion API
9543/TCP	VMware Aria Operations for Logs Ingestion API (SSL)

Planning Your VMware Aria Operations for Logs Deployment

You can deploy VMware Aria Operations for Logs with a single node, single cluster, or cluster with forwarders.

NOTE
Starting from version 8.14, VMware Aria Operations for Logs supports VMware NSX Advanced Load Balancer. To learn more, see the Working With VMware NSX Advanced Load Balancer documentation.

Installation Through Aria Suite Lifecycle

The Aria Suite Lifecycle automates the installation, configuration, upgrade, patch, configuration management, drift remediation, and health for Aria Suite products. As an alternative to installation with VMware Aria Operations for Logs, you can install VMware Aria Operations for Logs through the Aria Suite Lifecycle. You must use Aria Suite Lifecycle 1.2 or later to install VMware Aria Operations for Logs 4.5.1 or later. See Aria Suite Lifecycle documentation for more information.

Single Nodes

A basic VMware Aria Operations for Logs configuration includes a single node. Log sources can be applications, OS logs, virtual machine logs, hosts, the vCenter Server, virtual or physical switches and routers, storage hardware, and so on. Log streams are transported to the VMware Aria Operations for Logs node using syslog (UDP, TCP, TCP+SSL) or CFAPI (the VMware Aria Operations for Logs native ingestion protocol over HTTP or HTTPS), either directly by an application, syslog concentrator, or the VMware Aria Operations for Logs agent installed on the source.

As a best practice for single-node deployments to use the VMware Aria Operations for Logs Integrated Load Balancer (ILB) and to send queries and ingestion traffic to the ILB. This does not incur overhead and simplifies configuration if you want to add nodes to create a cluster for your deployment in the future.

As a best practice, do not use single nodes for production environments.

Clusters

Production environments generally require the use of clusters. Clusters must meet the following requirements:

- Nodes in clusters must all be of the same size and in the same data center.
- The ILB used with clusters requires that nodes be in the same L2 network.
- VMware Aria Operations for Logs virtual machines must be excluded from VMware NSX Distributed Firewall Protection.
  This is because virtual IPs for clusters use a Linux Virtual Server in Direct Server Return Mode (LVS-DR) for load balancing. Direct Server Return is more efficient than routing all response traffic through a single cluster member. However, it also resembles spoofed traffic, which NSX Distributed Firewall blocks.

Sizing Clusters

A VMware Aria Operations for Logs single cluster configuration can include 3 to 18 nodes. When nodes are offline or unhealthy, the feature availability depends on the minimum number of nodes that are available for the cluster to run functionalities.

The following table lists the maximum number of nodes that can fail to maintain a healthy, active cluster:

Number of nodes in a cluster	Number of nodes that can fail
1	0
2	0
3	1
4	1
5	2
6	2
7-18	3

If the primary node is unhealthy or offline,

- You might experience certain UI limitations in accessing cluster details and statistics.
- You cannot add new nodes.
- You cannot remove existing nodes.

For information about sizing, see Sizing the VMware Aria Operations for Logs Virtual Appliance.

Clusters with Forwarders

A VMware Aria Operations for Logs cluster with forwarders configuration includes main indexing, storage, and a query cluster of three to 18 nodes using the ILB. A single log message is present in only one location within the main cluster, as for the single cluster.

The design is extended through the addition of multiple forwarder clusters at remote sites or clusters. Each forwarder cluster is configured to forward all its log messages to the main cluster and users connect to the main cluster, taking advantage of CFAPI for compression and resilience on the forwarding path. Forwarder clusters configured as top-of-rack can be configured with a larger local retention.

Cross-Forwarding for Redundancy

This VMware Aria Operations for Logs deployment scenario includes a cluster with forwarder that is extended and mirrored. Two main clusters are used for indexing, storage, and query. One main cluster is in each data center. Each is front-ended with a pair of dedicated forwarder clusters. All log sources from all top-of-rack aggregations concentrate at the forwarder clusters. You can independently query the same logs on both retention clusters.

VMware Aria Operations for Logs Integrated Load Balancer

To properly balance traffic across nodes in a cluster and to minimize administrative overhead, use the Integrated Load Balancer (ILB) for all deployments. This ensures that incoming ingestion traffic is accepted even if some VMware Aria Operations for Logs nodes are unavailable.

Sizing the VMware Aria Operations for Logs Virtual Appliance

By default, the VMware Aria Operations for Logs virtual appliance uses the preset values for small configurations.

Standalone Deployment

You can change the appliance settings to meet the needs of the environment for which you intend to collect logs during deployment.

VMware Aria Operations for Logs provides preset VM (virtual machine) sizes that you can select from to meet the ingestion requirements of your environment. These presets are certified size combinations of compute and disk resources, though you can add extra resources afterward. A small configuration is suitable only for demos.

To size virtual appliances to XL, XXL, and XXXL, see KB 80928.

Preset Size	Log Ingest Rate	Virtual CPUs	Memory	IOPS	Syslog Connections (Active TCP Connections)	Events per Second
Small	30 GB/day	4	8 GB	500	100	2000
Medium	75 GB/day	8	16 GB	1000	250	5000
Large	225 GB/day	16	32 GB	1500	750	15,000

You can use a syslog aggregator to increase the number of syslog connections that send events to VMware Aria Operations for Logs. However, the maximum number of events per second is fixed and does not depend on the use of a syslog aggregator. A VMware Aria Operations for Logs instance cannot be used as a syslog aggregator.

The sizing is based on the following assumptions.

- Each virtual CPU is at least 2 GHz.
- Each ESXi host sends up to 10 messages per second with an average message size of 170 bytes/message, which is roughly equivalent to 150 MB per day, per host.

> **NOTE**
>
> - For large installations, you must upgrade the virtual hardware version of the VMware Aria Operations for Logs virtual machine. VMware Aria Operations for Logs supports virtual hardware version 7 or later. Virtual hardware version 7 can support up to 8 virtual CPUs. Therefore, if you plan to provision 16 virtual CPUs, you must upgrade to virtual hardware version 8 or later for ESXi 5.x. You use the vSphere Client to upgrade the virtual hardware. If you want to upgrade the virtual hardware to the latest version, read and understand the information in the VMware knowledge base article Upgrading a virtual machine to the latest hardware version (1010675) .

Cluster Deployment

Use a medium configuration, or larger, for the primary and worker nodes in a VMware Aria Operations for Logs cluster. The number of events per second increases linearly with the number of nodes. For example, in a cluster of 3-18 nodes (clusters must have a minimum of three nodes), the ingestion in an 18-node cluster is 270,000 events per second (EPS), or 4 TB of events per day.

Reducing the Memory Size

Use the **Small** version of the appliance in a proof-of-concept or test environment, but not in a production environment.

VMware Aria Operations for Logs Sizing Calculator

A calculator to help you determine sizing for VMware Aria Operations for Logs and network and storage use is available. This calculator is intended for guidance only. Many environment inputs are site-specific, so the calculator necessarily uses estimations in some areas. See https://www.vmware.com/go/loginsight/calculator.

> **NOTE**
>
> The overall performance of VMware Aria Operations for Logs might degrade if forwarders are defined against the text field with complex or multiple conditions involving regular expressions, for example "`text=~"Deleting the machine`". In such cases, specifically when the overall load on the cluster is high, performance might be delayed, and disk blocks might accumulate on each node of the cluster.

IntegratingVMware Aria Operations for Logs andVMware Aria Operations

IntegratingVMware Aria Operations for Logs withVMware Aria Operations allows you to send metrics and alerts generated byVMware Aria Operations for Logs toVMware Aria Operations, and gain granular insights into your virtual infrastructure and application's performance to perform faster and efficient issue identification and resolution.

The integration betweenVMware Aria Operations for Logs andVMware Aria Operations is a two-way integration.

If you add theVMware Aria Operations integration on theVMware Aria Operations for Logs user interface, you can send alerts and metrics toVMware Aria Operations and analyze logs in theVMware Aria Operations user interface.

If you add theVMware Aria Operations for Logs integration on theVMware Aria Operations user interface, you can:

- Analyze logs on the **Log Analysis** page.
- Look for potential evidences of a problem within logs for a specific scope and time range in the **Troubleshoot Workbench** > **Logs** tab.
- View the logs for a selected object in the **Logs** tab.

To fully leverage the capabilities ofVMware Aria Operations andVMware Aria Operations for Logs, it is essential to integrate the products on both ends. By integrating the products on both ends, you can gain complete visibility into your virtual infrastructure and application's performance, allowing you to quickly identify and troubleshoot issues.

1. ConfigureVMware Aria Operations for Logs to connect toVMware Aria Operations.

   See ConfigureVMware Aria Operations for Logs to Send Notification Events toVMware Aria Operations in *AdministeringVMware Aria Operations for Logs*.

2. ConfigureVMware Aria Operations to connect toVMware Aria Operations for Logs.

   See ConfiguringVMware Aria Operations for Logs withVMware Aria Operations in *ConfiguringVMware Aria Operations*.

You can:

- View the log analysis ofVMware Aria Operations for Logs events in theVMware Aria Operations user interface. To learn more, see Log Analysis in *ConfiguringVMware Aria Operations*.
- Activate launch in context from theVMware Aria Operations user interface. See Launch in Context fromVMware Aria Operations in *Administering VMware Aria Operations for Logs*.
- Activate launch in context from theVMware Aria Operations for Logs user interface. See Launch in Context fromVMware Aria Operations for Logs in *Administering VMware Aria Operations for Logs*.

Life Cycle of an Event

Understanding how VMware Aria Operations for Logs processes messages and events is key to using VMware Aria Operations for Logs effectively.

The life cycle of a log message or event has multiple stages including reading, parsing, ingestion, indexing, alerting, query application, archiving, and deletion.

Events and messages transition through the following stages.

1. It is generated on a device (outside of VMware Aria Operations for Logs).
2. It is picked up and sent to VMware Aria Operations for Logs in one of the following ways:
   - By a VMware Aria Operations for Logs agent using ingestion API or syslog
   - Through a third-party agent such as rsyslog, syslog-ng, or log4j using syslog
   - By custom writing to ingestion API (such as log4j appender)
   - By custom writing to syslog (such as log4j appender)
3. VMware Aria Operations for Logs receives the event.
   - If you are using the integrated load balancer (ILB), the event is directed to a single node that is responsible for processing the event.
   - If the event is declined, the client handles declines with UDP drops, TCP with protocol settings, or CFAPI with a disk-backed queue.
   - If the event is accepted, the client is notified.
4. The event is passed through the VMware Aria Operations for Logs ingestion pipeline, from which the following steps occur:
   - A keyword index is created or updated. The index is stored in a proprietary format on a local disk.
   - Machine learning is applied to cluster events.
   - The event is stored in a compressed proprietary format on the local disk in a bucket.

5. The event is queried.
    – Keyword and glob queries are matched against the keyword index.
    – Regex is matched against compressed events.
6. The event is moved to a bucket and archived.
    – A bucket is sealed and archived when it reaches 0.5 GB.
7. The event is deleted.
    – Buckets are deleted in FIFO order.

For More Information

For more information, see the VMware Technical Publications video,

Key Aspects of the Event Life Cycle

As an event ages, there are key aspects of event storage and management during the event life cycle to be aware of.

Event Storage

Each event is stored in a single on-disk bucket. When working with buckets, be aware of the following behaviors and characteristics.

*   Buckets can reach a maximum size of 0.5 GB. When a bucket reaches 0.5 GB, it is sealed and queued for archiving. After a sealed bucket is archived, it is marked as archived. An event can be retained locally and in the archives at the same time.
*   Buckets are not replicated across VMware Aria Operations for Logs nodes. If you lose a node, you lose the data on that node.
*   All buckets are stored on the `/storage/core` partition.
*   VMware Aria Operations for Logs deletes old buckets when the available space on the `/storage/core` partition is less than 3%. Deletion follows a FIFO model.
    > **NOTE**
    > A near-full `/storage/core` partition is usual and expected. That partition should never reach 100% because VMware Aria Operations for Logs manages that partition. However, do not attempt to store data on that partition because it can interfere with the deletion of old buckets.

Event Management

As you set up and configure your product, it is helpful to be familiar with the following characteristics and behaviors of VMware Aria Operations for Logs events and event management.

*   After an event is deleted locally, it can no longer be queried unless it is imported from the archive using the command-line interface.
*   After all events for a machine learning cluster are deleted from VMware Aria Operations for Logs, the cluster is removed.
*   VMware Aria Operations for Logs rebalances all incoming events fairly across nodes in the cluster. For example, even if a node is explicitly sent to an event, it might not be the node to ingest the event.
*   Event metadata is stored in a proprietary format on a single VMware Aria Operations for Logs node and not in a database.
*   An event can exist locally on a node and on the archive.

Installing VMware Aria Operations for Logs

VMware Aria Operations for Logs is delivered as a virtual appliance that you deploy in your vSphere environment.

After reviewing Sizing the Log Insight Virtual Appliance, go to Deploy the vRealize Log Insight Virtual Appliance. Whether you have a single node deployment or a clustered deployment, follow the standard OVF deployment procedure described in this section.

> **NOTE**
> You can use VMware Aria Suite Lifecycle 1.2 or later to install VMware Aria Operations for Logs 4.5.1 and later releases. See VMware Aria Suite Lifecycle documentation for more information.

Deploy the VMware Aria Operations for Logs Virtual Appliance

Download the VMware Aria Operations for Logs virtual appliance. VMware distributes the VMware Aria Operations for Logs virtual appliance as an `.ova` file. Deploy the VMware Aria Operations for Logs virtual appliance by using the vSphere Client.

- Verify that you have a copy of the VMware Aria Operations for Logs virtual appliance `.ova` file.
- Verify that you have permissions to deploy OVF templates to the inventory.
- Verify that your environment has enough resources to accommodate the minimum requirements of the VMware Aria Operations for Logs virtual appliance. See Minimum Requirements.
- Verify that you have read and understand the virtual appliance sizing recommendations. See Sizing the Virtual Appliance.

1. In the vSphere Client, select **File** > **Deploy OVF Template**.

2. Follow the prompts in the **Deploy OVF Template** wizard.

3. On the **Select Configuration** page, select the size of the VMware Aria Operations for Logs virtual appliance based on the size of the environment for which you intend to collect logs.

   Small is the minimum requirement for production environments.

   VMware Aria Operations for Logs provides preset VM (virtual machine) sizes that you can select from to meet the ingestion requirements of your environment. These presets are certified size combinations of compute and disk resources, though you can add extra resources afterward. A small configuration is suitable only for demos.

   > **NOTE**
   > If you select **Large**, you must upgrade the virtual hardware on the VMware Aria Operations for Logs virtual machine after the deployment.

4. On the Select Storage page, select a disk format.

   - **Thick Provision Lazy Zeroed** creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. The data remaining on the physical device is not erased during creation, but is zeroed out on demand later, on first write from the virtual appliance.
   - **Thick Provision Eager Zeroed** creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks.

     > **IMPORTANT**
     > Deploy the VMware Aria Operations for Logs virtual appliance with thick provisioned eager zeroed disks whenever possible for better performance and operation of the virtual appliance.
   - **Thin Provision** creates a disk in thin format. The disk expands as the amount of data saved on it increases. If your storage device does not support thick provisioning disks or you want to conserve unused disk space on the VMware Aria Operations for Logs virtual appliance, deploy the virtual appliance with thin provisioned disks.

     > **NOTE**
     > Shrinking disks on the VMware Aria Operations for Logs virtual appliance is not supported and might result in data corruption or data loss.

5. Optional: On the **Select Networks** page, set the networking parameters for the VMware Aria Operations for Logs virtual appliance. You can select the IPv4 or IPv6 protocol.

   If you do not provide network settings, such as an IP address, DNS servers, and gateway information, VMware Aria Operations for Logs uses DHCP to set those settings.

   > ⚠️ **CAUTION**
   > Do not specify more than two domain name servers. If you specify more than two domain name servers, all configured domain name servers are ignored in the VMware Aria Operations for Logs virtual appliance.

   Use a comma-separated list to specify domain name servers.

6. Optional: On the **Customize template** page, set network properties if you are not using DHCP.

   Under Application, select the **Prefer IPv6 addresses** check box if you want to run the virtual machine in a dual stack network.

   > ⚠️ **CAUTION**
   > Do not select the **Prefer IPv6 addresses** check box if you want to use pure IPv4 even with IPv6 supported in your network. Select the check box only if your network has a dual stack or pure stack support for IPv6.

7. Optional: On the **Customize template** page, select **Other Properties** and set the root password for the VMware Aria Operations for Logs virtual appliance.

   The root password is required for SSH. You can also set this password through the VMware Remote Console.

8. Follow the prompts to complete the deployment.

   For information on deploying virtual appliances, see the *VMware Aria Operations vApps Deployment and Configuration* guide.

   After you power on the virtual appliance, an initialization process begins. The initialization process takes several minutes to complete. At the end of the process, the virtual appliance restarts.

9. Navigate to the **Console** tab and verify the IP address of the VMware Aria Operations for Logs virtual appliance.

IP Address Prefix	Description
https://	The DHCP configuration on the virtual appliance is correct.
http://	The DHCP configuration on the virtual appliance failed. 1. Power off the VMware Aria Operations for Logs virtual appliance. 2. Right-click the virtual appliance and select **Edit Settings**. 3. Set a static IP address for the virtual appliance.

• If you want to configure a standalone VMware Aria Operations for Logs deployment, see Configure New Deployment. The VMware Aria Operations for Logs Web interface is available at https://*operations-for-logs-host*/ where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

Start a New VMware Aria Operations for Logs Deployment

When you access the VMware Aria Operations for Logs web interface for the first time after the virtual appliance deployment or after removing a worker node from a cluster, you must finish the initial configuration steps.

• In the vSphere Client, note the IP address of the VMware Aria Operations for Logs virtual appliance. For information about locating the IP address, see Deploy the VMware Aria Operations for Logs Virtual Appliance.
• Verify that you are using a supported browser. See Minimum Requirements.
• Verify that you have a valid license key. You can request an evaluation or permanent license key through your account on My VMware™ at https://my.vmware.com/.

- If you want to use local, vCenter Server, or Active Directory credentials to integrate VMware Aria Operations for Logs with VMware Aria Operations, verify that these users are imported in VMware Aria Operations Custom user interface. For instructions about configuring LDAP, see the VMware Aria Operations documentation.

All settings that you modify during the initial configuration are also available in the Configuration web user interface.

For information about the trace data that VMware Aria Operations for Logs might collect and send to VMware when you participate in the Customer Experience Improvement Program (CEIP), see The Customer Experience Improvement Program.

1. Use a supported browser to navigate to the web user interface of VMware Aria Operations for Logs.

   The URL format is https://*operations_for_logs-host*/, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

   The initial configuration wizard opens.

2. Click **Start New Deployment**.

3. Set the password for the administrator (user name admin) and click **Save and Continue**. Optionally, you can provide an email address for the administrator.

   The administrator is a user linked to the Super Admin role. For information about roles, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*

4. Enter the license key, click **Add License Key**, and click **Save and Continue**.

5. On the General Configuration page, enter the email address to receive system notifications from VMware Aria Operations for Logs.

6. If you are using webhooks to send notifications to VMware Aria Operations or a third-party application, enter a space-separated list of URLs in the **Send HTTP Post System Notifications To** text box.

7. Optional: To leave the CEIP, deselect the **Join the VMware Customer Experience Program** option. Click **Save and Continue**.

   > **NOTE**
   > If you join the CEIP, VMware Aria Operations for Logs uses a third-party tool called Pendo to collect analytics cookies. Pendo collects data based on your interaction with the user interface by tracking where you click, to help VMware understand how VMware Aria Operations for Logs is used. This data is used to improve the VMware services and design them better. For more information, see the Privacy Notice.

8. On the Time Configuration page, set how time is synchronized on the VMware Aria Operations for Logs virtual appliance and click **Test**.

Option	Description
NTP server (recommended)	By default, VMware Aria Operations for Logs is configured to synchronize time with public NTP servers. If an external NTP server is not accessible due to firewall settings, you can use the internal NTP server of your organization. Use commas to separate multiple NTP servers.
ESX/ESXi host	If no NTP servers are available, you can sync the time with the ESXi host where you deployed the VMware Aria Operations for Logs virtual appliance.

9. Click **Save and Continue**.

10. Optional: To enable outgoing alert and system notification emails, specify the properties of an SMTP server.

    To verify that the SMTP configuration is correct, enter a valid email address and click **Test**.VMware Aria Operations for Logs sends a test email to the address that you provided.

11. Optional: To provide a custom SSL certificate, upload a certificate file to the cluster in a PEM format. You can also view the details of the existing certificate.

    The system adds the certificate to the truststores of all the nodes of the cluster and saves it for later use.

    For information about the prerequisites of the custom SSL certificate, see Install a Custom SSL Certificate.

12. Click **Save and Continue**.

After the VMware Aria Operations for Logs process restarts, you are redirected to the **Dashboards** page of VMware Aria Operations for Logs.

- Navigate to **Integration > vSphere** and configure VMware Aria Operations for Logs to pull tasks, events, and alerts from vCenter Server instances, and to configure ESXi hosts to send syslog feeds to VMware Aria Operations for Logs.
- Assign a permanent license to VMware Aria Operations for Logs. See Assign a Permanent License to Log Insight in *Administering VMware Aria Operations for Logs.*
- Configure the VMware Aria Operations for Logs adapter in VMware Aria Operations to enable launch in context. See *Configuring VMware Aria Operations for Logs with VMware Aria Operations* in the *VMware Aria Operations Configuration Guide*.
- Install the VMware Aria Operations for Logs Windows Agent to collect events from Windows event channels, Windows directories, and flat text log files. See Installing Windows Agents in *Working with VMware Aria Operations for Logs Agents*.

Join an Existing Deployment

After you deploy and set up a standalone VMware Aria Operations for Logs node, you can deploy a new VMware Aria Operations for Logs instance and add it to the existing node to form a VMware Aria Operations for Logs cluster.

- In the vSphere Client, note the IP address of the worker VMware Aria Operations for Logs virtual appliance.
- Verify that you have the IP address or host name of the primary VMware Aria Operations for Logs virtual appliance.
- Verify that you have a user account on the primary VMware Aria Operations for Logs virtual appliance with the Super Admin role, a role that has the relevant permissions. See Create and Modify Roles for more information.
- Verify that the versions of the VMware Aria Operations for Logs primary and worker nodes are in sync. Do not add an older version VMware Aria Operations for Logs worker to a newer version VMware Aria Operations for Logs primary node.
- Synchronize the time on the VMware Aria Operations for Logs virtual appliance with an NTP server. For more information, see Synchronize the Time on the Log Insight Virtual Appliance.
- Login to the web user interface of the VMware Aria Operations for Logs primary node and generate a secure token on the **Management** > **Cluster** page.
- For information on supported browser versions, see the Release Notes.

VMware Aria Operations for Logs can scale out by using multiple virtual appliance instances in clusters. Clusters enable linear scaling of ingestion throughput, increase query performance, and allow high-availability ingestion. In cluster mode, VMware Aria Operations for Logs provides primary and worker nodes. Both primary and worker nodes are responsible for a subset of data. Primary nodes can query all subsets of data and aggregate the results. You might require more nodes to support site needs. You can use from three to 18 nodes in a cluster. This means that a fully functional cluster must have a minimum of three healthy nodes. Most nodes in a larger cluster must be healthy. For example, if three nodes of a six-node cluster fail, none of the nodes functions fully until the failing nodes are removed.

1. Use a supported browser to navigate to the web user interface of the VMware Aria Operations for Logs worker.

    The URL format is https://*operations_for_logs-host*/, where *operations_for_logs* is the IP address or host name of the VMware Aria Operations for Logs worker virtual appliance.

    The initial configuration wizard opens.

2. Click **Join Existing Deployment**.

3. Enter the following details and click **Go**.

   1. IP address or host name of the VMware Aria Operations for Logs primary node.
   2. The secure token generated on the **Management** > **Cluster** page.

   If the primary node provides an untrusted SSL certificate, a dialog box appears with the details of the certificate. Click **Accept** to send a request to the VMware Aria Operations for Logs primary node to join the existing deployment.

   If you click **Cancel**, the join request is not sent to the primary node. You must accept the certificate to ensure that the worker node joins the existing deployment.

   The worker node joins the existing deployment and VMware Aria Operations for Logs begins to operate in a cluster.

• Add more worker nodes as needed. The cluster must have a minimum of three nodes.

The Customer Experience Improvement Program

This product participates in VMware's Customer Experience Improvement Program (CEIP).

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at https://www.vmware.com/solutions/trustvmware/ceip.html.

To join or leave the CEIP for this product, see "Join or Leave the VMware Customer Experience Program" in *Administering VMware Aria Operations for Logs*.

Working with VMware Aria Operations for Logs Agents (8.14)

Working with VMware Aria Operations for Logs Agents

Working with VMware Aria Operations for Logs Agents describes how to install and configure VMware Aria Operations for Logs Agents Windows and Linux agents. It also includes troubleshooting tips.

This information is intended for anyone who wants to install, configure, or troubleshoot VMware Aria Operations for Logs Agents. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations. Administrators are users assigned the **Super Admin** role or a role that has all the permissions of the **Super Admin** role. Users assigned a role with edit access for agents can also configure VMware Aria Operations for Logs Agents.

For information about how to create configuration classes for agents with the VMware Aria Operations for Logs server, refer to *Administering VMware Aria Operations for Logs Agents*.

Overview of VMware Aria Operations for Logs Agents

A VMware Aria Operations for Logs agent collects logs from log files and forwards them to a VMware Aria Operations for Logs server or any third-party syslog destination.

Agents support syslog and the VMware Aria Operations for Logs ingestion API (cfapi protocol) and can be used with Linux or Windows platforms. You configure agents through the web interface, with the liagent.ini file on the server and client side, or as part of installation.

Agents include the following features:

- Single or group deployment
- Automatic upgrade
- Parsing that operates on log messages and extracts structured data. You can configure parsers for FileLog and WinLog collectors or both.
- Support for multi-line messages
- Native support for several log rotation schemes
- An extensive ingestion API that includes client-side compression, encryption, and the ability to add metadata to logs

The VMware Aria Operations for Logs server supports centralized configuration management and creation and management of groups of agents.

The following figure shows the elements of an agent deployment configuration.
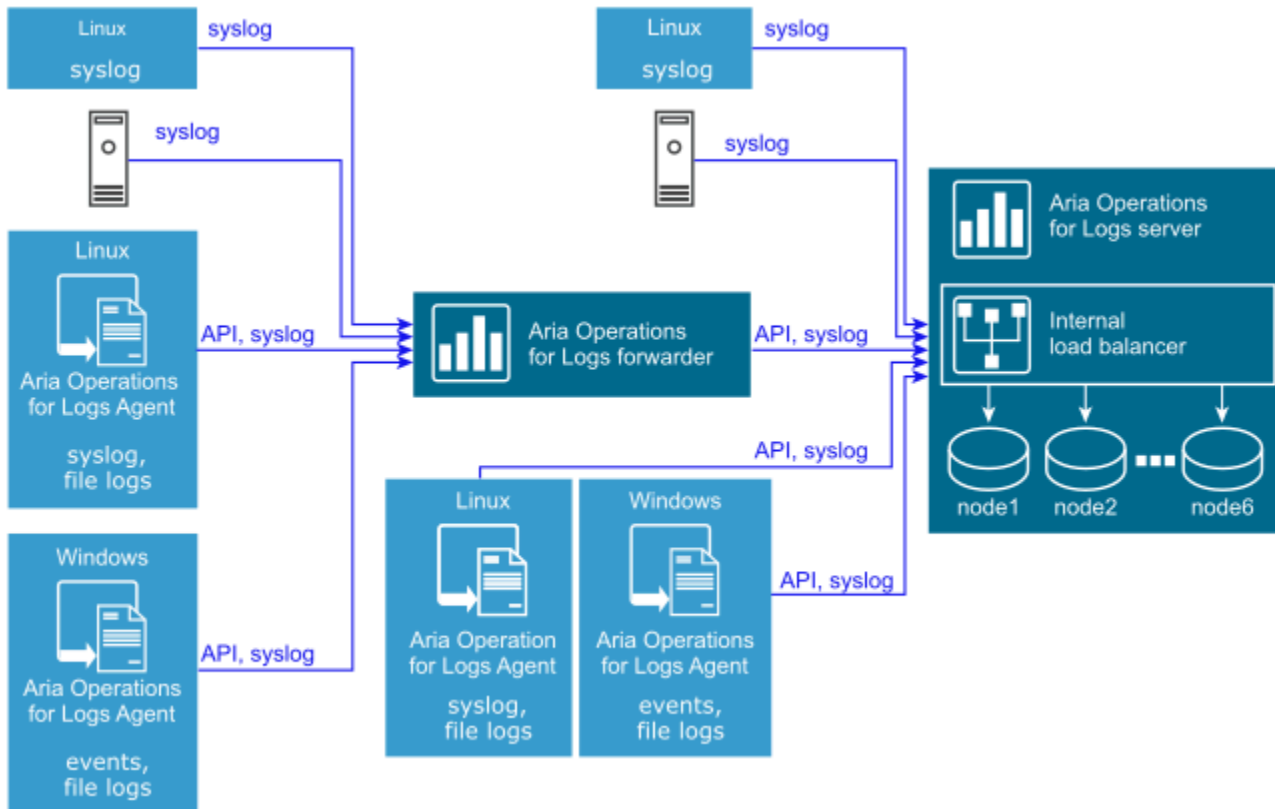
A VMware Aria Operations for Logs log forwarder is a dedicated instance of a VMware Aria Operations for Logs server whose primary job is to forward logs to a remote destination. Normally, a server instance used as a forwarder is not used for query. The forwarder uses an internal load balancer and is otherwise structured like a VMware Aria Operations for Logs server.

Agents write their own operation logs. For Windows, these logs are located in the `C:\ProgramData\VMware\Log Insight Agent\logs` directory. For Linux, the path for the operation log is `/var/log/loginsight-agent/liagent_*.log`. Log files are rotated when an agent is restarted or when the file reaches a size of 10 MB. A combined limit of 50 MB of files is kept in rotation. You cannot collect agent logs with the VMware Aria Operations for Logs agent itself.

Agents are used for real-time log collection. Use the VMware Aria Operations for Logs Importer to import historic log collections, including support bundles.

Separate installation downloads for Windows and Linux operating systems are provided.

On Windows systems, the agent runs as a Windows service and starts immediately after installation. The agent monitors application log files and Windows event channels, pools for collecting related Windows system logs. Collected logs are forwarded to VMware Aria Operations for Logs servers or third-party syslog destinations.

On Linux systems, the agent runs as a daemon and starts immediately after installation. The VMware Aria Operations for Logs Linux agent collects logs from log files on Linux machines and forwards them to VMware Aria Operations for Logs servers or syslog destinations. Debian, Red Hat, and Linux binary installation packages are available.

Log Rotation Schemes Supported by VMware Aria Operations for Logs Agents

VMware Aria Operations for Logs agents support several log rotation schemes.

Log rotation ensures that log files do not grow infinitely. There are several log rotation schemes, each designed for a particular set of use cases. VMware Aria Operations for Logs includes native support for the following schemes.

Table 2: Supported Log Rotation Schemes

Log rotation scheme	Description
create-new	New log files are created when a size or time limit is reached. The logger process stops writing to the current log file and directs log output to a newly created file. No existing file is renamed or touched in any other way.
rename-recreate	An external utility such as logrotate renames the log file when a size or time limit is reached. The logger process then creates a log file with the previous name.
copy-truncate	An external utility such as logrotate copies the log file when a size or time limit is reached. The log process renames the copied file and truncates the original file so that its size becomes 0. The logger process can continue to write logs to the original file.

Installing or Upgrading VMware Aria Operations for Logs Agents

You can install or upgrade VMware Aria Operations for Logs agents on Windows machines or Linux machines, including machines with third-party log management systems.

Agents collect logs and forward them to the VMware Aria Operations for Logs server. During installation, you can specify parameters for the server, port, and protocol settings or keep the default settings. For the installation instructions, navigate to **Log Sources > Agents** and click **LI Agent**.

You can upgrade agents using the same methods you use for installation, or you can use auto-upgrade. Auto-upgrade propagates upgrades to agents when you deploy a new version of VMware Aria Operations for Logs. See Automatic Update for vRealize Log Insight Agents for more information. Upgrade is not available for Linux binary packages.

<u>**Hardware Support**</u>

To install and run a VMware Aria Operations for Logs agent, your hardware must support the minimum parameters required for hosts or machines that support x86 and x86_64 architecture and MMX, SSE, SSE2, and SSE3 instruction sets.

<u>**Platform Support**</u>

Operating System	Processor Architecture
Windows 7, Windows 8, Windows 8.1, and Windows 10	x86_64, x86_32
Windows Server 2008, Windows Server 2008 R2,	x86_64, x86_32
Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019	x86_64
RHEL 5, RHEL 6, RHEL 7, RHEL 7, and RHEL 9	x86_64, x86_32
SuSE Enterprise Linux (SLES) 11 SP3 and SLES 12 SP1	x86_64
Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04	x86_64
VMware Photon, version 1 revision 2, version 2, and version 3	x86_64

Linux Notes

If you implement a default installation of the VMware Aria Operations for Logs Linux Agent for a user without root privileges, the default configuration might create problems with the data collection. The agent does not log a warning that the subscription to the channel is unsuccessful, and files in the collection do not have read permissions. The message `Inaccessible log file ... will try later` is repeatedly added to the log. You can comment out the default configuration that is causing the problem or change the user permissions.

If you use an rpm or DEB package to install Linux agents, the init.d script named `liagentd` is installed as part of the package installation. The bin package adds the script, but does not register it. You can register the script manually.

You can verify that the installation was successful by running the (/sbin/) service `liagentd` status command.

Related Links

Download Agent Installation Files on page 60

The first step to setting up a VMware Aria Operations for Logs agent is to download an agent installation package for your platform.

Download Agent Installation Files

The first step to setting up a VMware Aria Operations for Logs agent is to download an agent installation package for your platform.

All packages downloaded from the VMware Aria Operations for Logs server agent page include the destination hostname appended to the package name. The server.hostname is applied during an initial installation for the MSI, RPM, and DEB agents. If a hostname is present in the configuration file, or if you are running the package by the hostname parameter, the embedded server hostname is ignored.

1. Expand the main menu and navigate to **Management > Agents**.

2. Scroll to the bottom of the screen and click **Download VMware Aria Operations for Logs Agent Version x.x.x**.

3. Download an installation package by selecting it from the pop-up menu and clicking **Save**.

Option	Description
Windows MSI	Installation package for a Windows platform (32-bit/64-bit)
Linux RPM	Installation package for a Linux Red Hat, openSuSE (32-bit/64-bit), or VMware Photon platform
Linux DEB	Installation package for a Linux Debian platform (32-bit/64-bit)
Linux BIN	Self-installing package for Linux (32-bit/64-bit). A package management system is not required.

Use the downloaded files to deploy the VMware Aria Operations for Logs agent.

Related Links

Installing or Upgrading VMware Aria Operations for Logs Agents on page 59

You can install or upgrade VMware Aria Operations for Logs agents on Windows machines or Linux machines, including machines with third-party log management systems.

Installing Windows Agents

You can install an agent on a single machine through an installation wizard or through the command-line, or you can deploy multiple instances of an agent by using a script.

Upgrading Windows Agents

You can upgrade a Windows agent by applying an upgrade file using any of the methods you can use to install. You can also choose to use the auto-upgrade feature to upgrade your agents in the background.

Install or Update the VMware Aria Operations for Logs Windows Agent with the Installation Wizard

You can install or upgrade a Windows agent on a single machine with the installation wizard.

- Verify that you have a copy of the VMware Aria Operations for Logs Windows agent `.msi` file. See Download Agent Installation Files.
- Verify that you have permissions to perform installations and start services on the Windows machine.

1. Log in to the Windows machine on which to install the VMware Aria Operations for Logs Windows agent.

2. Change to the directory where you have the VMware Aria Operations for Logs Windows agent `.msi` file.

3. Double-click the VMware Aria Operations for Logs Windows agent `.msi` file, accept the terms of the License Agreement, and click **Next**.

4. Enter the IP address or host name of the VMware Aria Operations for Logs server and click **Install**.

   The wizard installs or updates the VMware Aria Operations for Logs Windows agent as an automatic Windows Service under the Local System service account.

5. Click **Finish**.

Configure the VMware Aria Operations for Logs Windows agent by editing `liagent.ini` file. See Configuring Log Insight Windows Agent After Installation.

Install or Update the VMware Aria Operations for Logs Windows Agent from the Command Line

You can install or update the Windows agent from the command line.

- Verify that you have a copy of the VMware Aria Operations for Logs Windows agent `.msi` file. See Download Agent Installation Files.
- Verify that you have permissions to perform installations and start services on the Windows machine.
- If you use the silent installation options /quiet or /qn, verify that you run the installation as an administrator. If you are not an administrator and run silent installation, the installation does not prompt for administrator privileges and fails. Use the logging option and parameters /lxv* *file_name* for diagnostic purposes.

You can use the default or specify a service account, and use command-line parameters to specify server, port, and protocol information. For MSI command-line options, see the Microsoft Developer Network (MSDN) Library website and search for MSI command-line options.

1. Log in to the Windows machine on which to install or update the VMware Aria Operations for Logs Windows agent.

2. Open a **Command Prompt** window.

3. Change to the directory where you have the VMware Aria Operations for Logs Windows agent `.msi` file.

4. Install or update with default values with a command of the following form. Replace *version-build_number* with your version and build number.

   The `/quiet` option runs the command silently, and the `/lxv` option creates a log file in the current directory.

```
        Drive:\path-to-msi_file>VMware-Log-Insight-Agent-version-build-num-
  ber.msi
  /quiet /lxv* li_install.log
```

5. Optional: Specify a user service account for the VMware Aria Operations for Logs Windows agent service to run under.
   Drive:*path-to-msi_file*>VMware-Log-Insight-Agent-*.msi SERVICEACCOUNT=domain*user*
   SERVICEPASSWORD=*user_password*

   > **NOTE**
   > The account supplied in the SERVICEACCOUNT parameter is granted with the **Log On As a Service** right and full-write access to the %ProgramData%\\VMware\\Log Insight Agent directory. If the supplied account does not exist, it is created. The user name must not exceed 20 characters. If you do not specify a SERVICEACCOUNT parameter, the VMware Aria Operations for Logs Windows agent service is installed or updated under the LocalSystem service account.

6. Optional: You can specify values for the following command-line options as needed.

Option	Description
SERVERHOST=*hostname*	IP address or host name of the virtual appliance.
SERVERPROTO=*protocol*	Protocol that the agent uses to send log events to the server. The possible values are cfapi and syslog. The default is cfapi.
SERVERPORT=*portnumber*	Communication port that the agent uses to send log events to the or third party server. By default the agent uses the appropriate port based on the options that are set for SSL and the protocol. See default port values provided in the list below. You need to specify the port option only if it's different from these defaults. • cfapi with SSL activated: 9543 • cfapi with SSL deactivated: 9000 • syslog with SSL activated: 6514 • syslog with SSL deactivated: 514
SERVICEACCOUNT=*account-name*	User service account under which the VMware Aria Operations for Logs Windows Agent service is run. **NOTE** The account supplied in the SERVICEACCOUNT parameter must have the **Log On As a Service** privilege and write access to %ProgramData%\\VMware\\Log Insight Agent directory so that the installer runs correctly. If you do not specify a SERVICEACCOUNT parameter, the VMware Aria Operations for Logs Windows agent service is installed under the LocalSystem service account.
SERVICEPASSWORD=*password*	Password for the user service account.
AUTOUPDATE={yes|no}	Activate or deactivate auto-update for the agent. You must also activate auto-update from the server to fully activate auto-update. The default is yes.
LIAGENT_SSL={yes|no}	Activate secure connection. If SSL is activated, the agent uses TLS 1.2 protocol to communicate to the server. The default is yes.

The command installs or updates the VMware Aria Operations for Logs Windows agent as a Windows service. The VMware Aria Operations for Logs Windows agent service starts when you start the Windows machine.

Verify that the command-line parameters you set are applied correctly in the liagent.ini file. See Configuring Log Insight Windows Agent After Installation.

Related Links

When you install VMware Aria Operations for Logs agents from the command line, you can include options to configure your deployment during installation. These options correspond to settings in the `liagent.ini` file.

Deploy the VMware Aria Operations for Logs Windows Agent to Multiple Machines

You can perform a mass deployment of the VMware Aria Operations for Logs Windows Agent on target computers in a Windows domain.

Create a Transform File to Deploy Multiple VMware Aria Operations for Logs Windows Agents

As part of deploying multiple agents, you must create a transform file that specifies configuration parameters for deployment. The .mst transform file is applied to the .msi file when you install agents. Parameters include the destination server for the agents and the communication protocol, port, and user account for installing and starting the VMware Aria Operations for Logs agent service.

- Verify that you have a copy of the VMware Aria Operations for Logs Windows `.msi` file. See Download Agent Installation Files.
- Download and install the Orca database editor. See https://learn.microsoft.com/en-us/windows/win32/msi/orca-exe.

Parameters include the destination server for the agents and the communication protocol, port, and user account for installing and starting the VMware Aria Operations for Logs agent service.

1. Open the VMware Aria Operations for Logs Windows agent `.msi` file in the Orca editor and select **Transform** > **New Transform**.

2. Edit the Property table and add necessary parameters and values for a customized installation or upgrade.

   Figure 1: Property Table
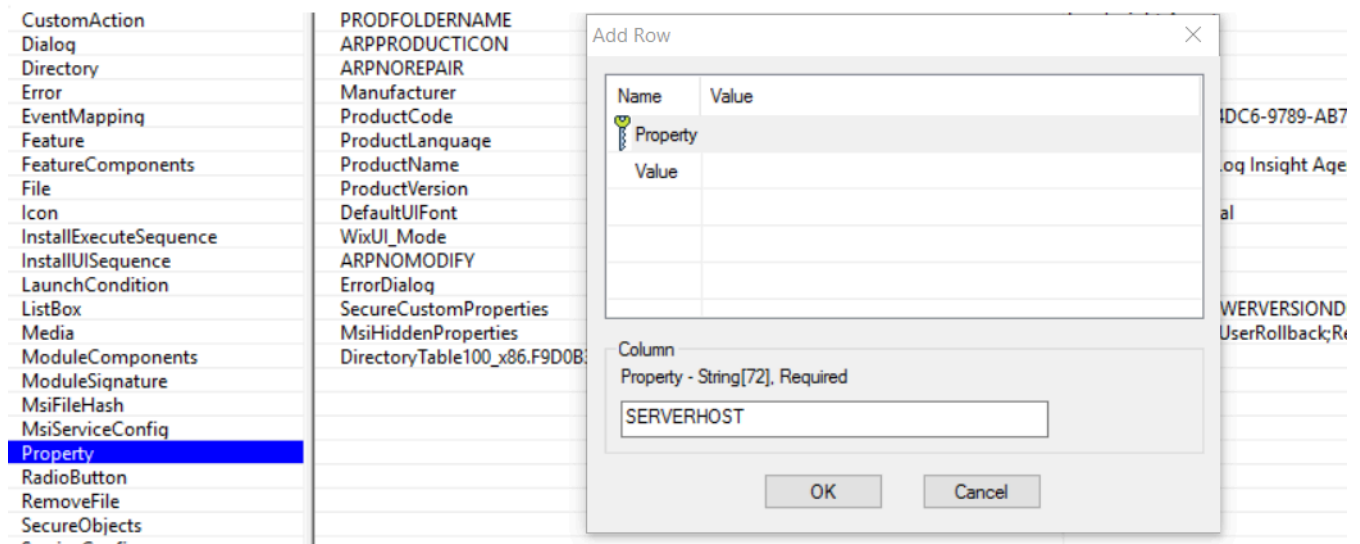
   a) Click **Property**.
   b) From the **Table** drop-down menu, select **Add Row**.
   c) Enter a property name and value in the Add Row dialog box.

   Parameters are shown in the following table.

Parameter	Description
`SERVERHOST`	IP address or host name of the virtual appliance.

Parameter	Description
	The default is `loginsight`.
`SERVERPROTO`	Protocol that the agent uses to send log events to the server. The possible values are `cfapi` and `syslog`. The default is cfapi.
`SERVERPORT`	Communication port that the agent uses to send log events to the or third party server. By default the agent uses the appropriate port based on the options that are set for SSL and the protocol. See default port values provided in the list below. You need to specify the port option only if it's different from these defaults. • cfapi with SSL activated: 9543 • cfapi with SSL deactivated: 9000 • syslog with SSL activated: 6514 • syslog with SSL deactivated: 514
`SERVICEACCOUNT`	User service account under which the VMware Aria Operations for Logs Windows Agent service is run. **NOTE** The account supplied in the `SERVICEACCOUNT` parameter must have the **Log On As a Service** privilege and write access to `%ProgramData%\VMware\Log Insight Agent` directory so that the installer runs correctly. If you do not specify a `SERVICEACCOUNT` parameter, the VMware Aria Operations for Logs Windows agent service is installed under the LocalSystem service account.
`SERVICEPASSWORD`	Password for the user service account.
`AUTOUPDATE`	Activate or deactivate auto-update for the agent. You must also activate auto-update from the server to fully activate auto-update. The default is yes.
`LIAGENT_SSL`	Activate secure connection. If SSL is activated, the agent uses TLS 1.2 protocol to communicate to the server. The default is yes.

3. Select **Transform** > **Generate Transform** and save the `.mst` transform file.

Use the `.msi` and `.mst` files to deploy the VMware Aria Operations for Logs Windows agent.

Deploy VMware Aria Operations for Logs Windows Agent on Multiple Targets

You can deploy VMware Aria Operations for Logs Windows agent on multiple target computers in a Windows domain.

- Verify that you have an administrator account or an account with administrative privileges on the domain controller.
- Verify that you have a copy of the VMware Aria Operations for Logs Windows agent `.msi` file. See Download Agent Installation Files.
- Familiarize yourself with the procedures described in http://support.microsoft.com/kb/887405 and http://support.microsoft.com/kb/816102.

For more information about why you need to reboot the client machine twice, see http://support.microsoft.com/kb/305293.

1. Log in to the domain controller as an administrator or a user with administrative privileges.

2. Create a distribution point and copy the VMware Aria Operations for Logs Windows agent `.msi` file to the distribution point.

3. Open the **Group Policy Management** Console and create a **Group Policy Object** to deploy the VMware Aria Operations for Logs Windows agent `.msi` file.

4. Edit the **Group Policy Object** for software deployment and assign a package.

5. Optional: If you generated an `.mst` file before deployment, select the `.mst` configuration file on the **Modifications** tab of the **GPO Properties** window. and use the Advanced method to edit a Group Policy Object to deploy the `.msi` package.

6. Optional: Upgrade the VMware Aria Operations for Logs Windows agent.
   a) Copy the upgrade `.msi` file to the distribution point.
   b) Click the **Upgrade** tab on the Group Policy Object **Properties** window.
   c) Add the initially installed version of the `.msi` file in the Packages that this package will upgrade section.

7. Deploy the VMware Aria Operations for Logs Windows agent to specific security groups that include the domain users.

8. Close all Group Policy Management Console and Group Policy Management Editor windows on the domain controller and restart the client machines.

   If Fast Login Optimization is enabled, reboot the client machines twice.

9. Verify that VMware Aria Operations for Logs Windows agent is installed on the client machines as a local service.

   If you configured SERVICEACCOUNT and SERVICEPASSWORD parameters for using an `.mst` file to deploy multiple instances of VMware Aria Operations for Logs Windows agent, verify that VMware Aria Operations for Logs Windows agent is installed on the client machines under the user account that you specified.

If the deployment is not successful, see Mass Deployment of the Log Insight Windows Agent is Not Successful to troubleshoot issues.

Install or Update the VMware Aria Operations for Logs Linux Agent RPM package

You can install or update the VMware Aria Operations for Logs Linux agent as a root or non-root user and you can set configuration parameters during installation. After installation, you can verify the installed version.

- Read about installation defaults and how to change them at Command-line Options for VMware Aria Operations for Logs Agent Installation on Linux .
- Log in as **root** or use `sudo` to run console commands.
- The VMware Aria Operations for Logs Linux agent needs access to syslog and networking services to function. Install and run the VMware Aria Operations for Logs Linux agent on runlevels 3 and 5. If you want the VMware Aria Operations for Logs Linux agent to work under other runlevels, configure the system appropriately.

1. You can install or upgrade an agent from the console.

   - To install the VMware Aria Operations for Logs Linux agent with default configuration settings, open a console and run the following command.

     ```
     rpm -i VMware-Log-Insight-Agent-<version-and-build-number>.rpm
     ```

   - To upgrade the agent without changing current configuration settings, open a console and run the following command.

     ```
     rpm -Uhv VMware-Log-Insight-Agent-<version-and-build-number>.rpm
     ```

2. Optional: You can override the default configuration values for installation or the current configuration values during an update. You do this by specifying options as part of the install or upgrade command.

   ```
   sudo <OPTION=value> rpm -i <version-and-build-number>.rpm
   ```

3. Optional: Verify the installed version by running the following command.

   ```
   rpm -qa | grep Log-Insight-Agent
   ```

   Linux Agent Install and Update Examples

   - The following command installs the VMware Aria Operations for Logs agent for a Linux RPM distribution. It installs the agent on a separate server, assigns a non-default port number, and creates a VMware Aria Operations for Logs agent user.

     ```
     sudo SERVERHOST=myagentserver SERVERPORT=1234 LIAGENTUSER=liagent rpm -i VMware-Log-Insight-Agent-44.1234.rpm
     ```

   - The following command updates the agent with the given rpm file. Current agent configuration is unchanged.

     ```
     rpm -Uhv VMware-Log-Insight-Agent-44.1234.rpm
     ```

Related Links

Command-line Options for VMware Aria Operations for Logs Agent Installation on Linux on page 71

When you install VMware Aria Operations for Logs agents from the command line, you can include options to configure your deployment during installation. These options correspond to settings in the `liagent.ini` file.

Install or Update the VMware Aria Operations for Logs Linux Agent DEB Package

You can install or update the VMware Aria Operations for Logs Linux agent DEB (Debian) package from the command line or through the debconf database. After installation, you can verify the installed version.

- Read about installation defaults and how to change them at Agent Installation Options.
- Log in as **root** or use `sudo` to run console commands.
- Verify that the VMware Aria Operations for Logs Linux agent has access to syslog and networking services to function. By default, the VMware Aria Operations for Logs Linux agent runs on runlevels 2, 3, 4, and 5 and stops on runlevels 0, 1, and 6.
- For more information and examples, see Customizing Your Agent Installation for Debian Linux.

1. To install or update the VMware Aria Operations for Logs Linux agent, open a console and run the `dpkg -i`*`package_name`* command.

    The *`package_name`* consists of the prefix `vmware-log-insight-agent-` and the version build number of your download version.

    The following command form installs the package with default values.
    ```
    dpkg -i vmware-log-insight-agent-VERSION-BUILD_NUMBER_all.deb
    ```

2. Optional: Verify the installed version by running the following command:
    ```
    dpkg -l | grep -i vmware-log-insight-agent
    ```

    - Configure the connection protocol from the command line.

        To override the default connection protocol, use the SERVERPROTO variable as shown in the following example:
        ```
        sudo SERVERPROTO=syslog dpkg -i vmware-log-insight-agent-<version-and-build-number>_all.deb
        ```

Related Links

When you install VMware Aria Operations for Logs agents from the command line, you can include options to configure your deployment during installation. These options correspond to settings in the `liagent.ini` file.

Customizing Your Agent Installation for Debian Linux

You can customize you installation by using command options to override the current configuration values for installation or by configuring the debconf database.

Customization from the Command Line

To configure your installation from the command line, use a command of the following form:
```
sudo <OPTION=value> dpkg  -i vmware-log-insight-agent-<version-and-build-number>_all.deb
```

For a complete list of options, see Command-line Options for VMware Aria Operations for Logs Agent Installation on Linux .

The following examples show some show some typical configurations done from the command line.

- Specify a target VMware Aria Operations for Logs server.
- To set the target during installation, run the `sudo` command and replace hostname with the IP address or hostname of the VMware Aria Operations for Logs server as shown in the following example:
    ```
    sudo SERVERHOST=hostname dpkg -iv mware-log-insight-agent-<version-and-build-number>_all.deb
    ```

    Unless you enabled the `--force-confold` flag during installation, whenever you update to a newer version, the system prompts you to keep or replace the liagent.ini configuration file. The following system message appears:

```
Configuration file `/var/lib/loginsight-agent/liagent.ini'
 ==> Modified (by you or by a script) since installation.
 ==> Package distributor has shipped an updated version.
   What would you like to do about it ?  Your options are:
    Y or I  : install the package maintainer's version
    N or O  : keep your currently-installed version
       D    : show the differences between the versions
       Z    : start a shell to examine the situation
 The default action is to keep your current version.
 *** liagent.ini (Y/I/N/O/D/Z) [default=N] ?
```

To preserve the existing configuration, use [default=N]. The additional parameters passed from the command line are still applied.

- Configure the connection protocol.
  To override the default connection protocol, use the SERVERPROTO variable as shown in the following example:

  ```
  sudo SERVERPROTO=syslog dpkg -i vmware-log-insight-agent-<version-and-build-number>_all.deb
  ```

- Configure the connection port.
  To override the default connection port, provide a value for the SERVERPORT variable to the installer as shown in the following example:

  ```
  sudo SERVERPORT=1234 dpkg -i vmware-log-insight-agent-<version-and-build-number>_all.deb
  ```

- Run the agent as a non-root user.
  To run the VMware Aria Operations for Logs Linux agent as a **non-root** user, run the `sudo` command.

  ```
  sudo LIAGENTUSER=liagent dpkg -i vmware-log-insight-agent-<version-build-number>_all.deb
  ```

If the specified user does not exist, the VMware Aria Operations for Logs Linux agent creates the user account during the installation. The created account is not deleted after uninstallation. If you install the Linux agent with the LIAGENTUSER=*non_root_user* parameter and try to upgrade with the LIAGENTUSER=*non_root_user2* parameter, a conflict occurs. Warnings appear because the *non_root_user2* user does not have the permissions of the *non_root_user* user.

DEB Package Customization Options for the debconf Database

The agent DEB package can also be configured through the debconf database. The following table shows supported debconf options and corresponding VMware Aria Operations for Logs agent DEB installer options:

Command-line Options	Debconf Options	Description
SERVERHOST=*hostname*	vmware-log-insight-agent/ serverhost	IP address or host name of the virtual appliance. The default is `loginsight`.
SERVERPROTO={cfapi|syslog}	vmware-log-insight-agent/ serverproto	Protocol that the agent uses to send log events to the server. The possible values are `cfapi` and `syslog`. The default is cfapi.

Command-line Options	Debconf Options	Description
`SERVERPORT=`*`portnumber`*	vmware-log-insight-agent/serverport	Communication port that the agent uses to send log events to the or third party server. By default the agent uses the appropriate port based on the options that are set for SSL and the protocol. See default port values provided in the list below. You need to specify the port option only if it's different from these defaults. • cfapi with SSL activated: 9543 • cfapi with SSL deactivated: 9000 • syslog with SSL activated: 6514 • syslog with SSL deactivated: 514
`LIAGENT_INITSYSTE` `M={init|systemd}`	log-insight-agent/init_system	During install time, the agent automatically detects the type of init system for the machine you are installing the agent on. You can override this behavior by specifying the type of system value with this option. There are two types of supported init systems: `init` and `systemd`.
`LIAGENT_AUTOUPDATE={yes|no}`	vmware-log-insight-agent/auto_update	Activate or deactivate auto-update for the agent. You must also activate auto-update from the server to fully activate auto-update. The default is yes. Auto-update is not supported for Linux BIN packages.
`LI_AGENT_RUNSERVICES`	vmware-log-insight-agent/init_system	Immediately after the installation, the services `liagentd` (agent) and `liupdaterd` (updater) are started by default. You can prevent them from starting by setting the LIAGENT_RUNSERVICES debconf parameter to `no`. The default is yes. The only accepted values are `yes` and `no`; **1** or **0** are not supported values.
`LIAGENT_SSL`	vmware-log-insight-agent/ssl	C
`LIAGENTUSER=`*`user-account-name`*	vmware-log-insight-agent/liagentuser	Specifies an account under which the agent is run. If the user does not exist, the installer creates it as a regular user. If the specified user account does not exist, the VMware Aria Operations for Logs Linux agent creates the user account during the installation. The created account is not deleted after uninstallation. By default the agent is installed to run as a root user. If you install the agent with the `LIAGENTUSER=`*`non_r`* *`oot_user`* parameter and try to upgrade with `LIAGENT` `USER=`*`non_root_user2`*, a conflict occurs. Warnings appear because *`non_root_user2`* user does not have the permissions of the user *`non_root_user`*. The created user is not removed during uninstall. It can be removed manually. This parameter is intended for the agent service only. The updater service is always running as a root user.

Install the VMware Aria Operations for Logs Linux Agent Binary Package

Installing the binary package includes changing the .bin file to an executable file and then installing the agent.

- Download and copy the VMware Aria Operations for Logs Linux Agent `.bin` package to the target Linux machine.
- Verify that the VMware Aria Operations for Logs Linux Agent has access to syslog and networking services.
- Read about default configuration values and how to change them at installation. See Command-line Options for VMware Aria Operations for Logs Agent Installation on Linux .

Upgrading the .bin package is not officially supported. If you used the .bin package to install an existing VMware Aria Operations for Logs Linux Agent,make a backup copy of the `liagent.ini` file located in `/var/lib/loginsight-agent` directory to keep the local configuration. After you have a backup copy, manually uninstall the VMware Aria Operations for Logs Linux Agent. See Manually Uninstall the VMware Aria Operations for Logs Linux Agent bin package.

If you use the .bin package to install Linux agents, the `init.d` script named `liagentd` is installed as part of the package installation, but the package does not register the script. You can register the script manually.

You can verify that the installation is successful by running `(/sbin/)service liagentd status` command.

1. Open a console and run the `chmod` command to change the `.bin` file to an executable file.

   Replace *filename-version* with the appropriate version.

   ```
   chmod +x filename-version.bin
   ```

2. From a command prompt, run the `./filename-version.bin` command to install the agent.

   Replace *filename-version* with the appropriate version.

   ```
   ./filename-version.bin
   ```

3. Optional: To set the target VMware Aria Operations for Logs server during installation, run the `sudo SERVERHOST=hostname ./filename-version.bin` command.

   Replace *hostname* with the IP address or hostname of the VMware Aria Operations for Logs server.

   ```
   sudo SERVERHOST=hostname ./filename-version.bin
   ```

4. Optional: To override the default connection protocol use the SERVERPROTO variable as shown in the following example:

   ```
   sudo SERVERPROTO=syslog ./filename-version.htm
   ```

5. Optional: To override the default connection port provide a value for the SERVERPORT variable to the installer as shown in the following example:

   ```
   sudo SERVERPORT=1234 ./filename-version.htm
   ```

6. Optional: To run the VMware Aria Operations for Logs Linux Agent as a **non-root** user run the `sudo` command.

   ```
   sudo LIAGENTUSER=liagent ./filename-version.bin
   ```

   If the specified user does not exist, the VMware Aria Operations for Logs Linux Agent creates the user account during the installation. The created account is not deleted after uninstallation. If you install the VMware Aria Operations for Logs Linux Agent with the `LIAGENTUSER=`*non_root_user* parameter and try to upgrade with the `LIAGENTUSER=`*non_root_user2* parameter, a conflict occurs and warnings appear because the *non_root_user2* user does not have the permissions of the *non_root_user* user.

Related Links

When you install VMware Aria Operations for Logs agents from the command line, you can include options to configure your deployment during installation. These options correspond to settings in the `liagent.ini` file.

Command-line Options for VMware Aria Operations for Logs Agent Installation on Linux

When you install VMware Aria Operations for Logs agents from the command line, you can include options to configure your deployment during installation. These options correspond to settings in the `liagent.ini` file.

The following options can be used during installation to configure VMware Aria Operations for Logs agents that run on Linux systems.

Option	Description
`SERVERHOST=`*hostname*	IP address or host name of the virtual appliance. The default is `loginsight`.
`SERVERPROTO={cfapi|syslog}`	Protocol that the agent uses to send log events to the server. The possible values are `cfapi` and `syslog`. The default is cfapi.
`SERVERPORT=`*portnumber*	Communication port that the agent uses to send log events to the or third party server. By default the agent uses the appropriate port based on the options that are set for SSL and the protocol. See default port values provided in the list below. You need to specify the port option only if it's different from these defaults. • cfapi with SSL activated: 9543 • cfapi with SSL deactivated: 9000 • syslog with SSL activated: 6514 • syslog with SSL deactivated: 514
`LIAGENT_INITSYSTEM={init|systemd}`	During install time, the agent automatically detects the type of init system for the machine you are installing the agent on. You can override this behavior by specifying the type of system value with this option. There are two types of supported init systems: `init` and `systemd`.
`LIAGENT_AUTOUPDATE={yes|no}`	Activate or deactivate auto-update for the agent. You must also activate auto-update from the server to fully activate auto-update. The default is yes. Auto-update is not supported for Linux BIN packages.
`LIAGENT_SSL={yes|no}`	Activate secure connection. If SSL is activated, the agent uses TLS 1.2 protocol to communicate to the server. The default is yes.
`LIAGENTUSER=`*user-account-name*	Specifies an account under which the agent is run. If the user does not exist, the installer creates it as a regular user. If the specified user account does not exist, the VMware Aria Operations for Logs Linux agent creates the user account during the installation. The created account is not deleted after uninstallation. By default the agent is installed to run as a root user. If you install with the `LIAGENTUSER=`*non_root_user* parameter and try to upgrade with `LIAGENTUSER=`*non_root_user2*, a conflict occurs. Warnings appear because *non_root_user2* user does not have the permissions of the user *non_root_user* The created user is not removed during uninstall. It can be removed manually. This parameter is intended for the agent service only. The updater service is always running as a root user.

Related Links

You can install or update the Windows agent from the command line.

You can install or update the VMware Aria Operations for Logs Linux agent as a root or non-root user and you can set configuration parameters during installation. After installation, you can verify the installed version.

You can install or update the VMware Aria Operations for Logs Linux agent DEB (Debian) package from the command line or through the debconf database. After installation, you can verify the installed version.

Installing the binary package includes changing the .bin file to an executable file and then installing the agent.

Automatic Update for VMware Aria Operations for Logs Agents

The auto-update feature for VMware Aria Operations for Logs agents allows active agents to check, download, and automatically update based on the agent install packages from the VMware Aria Operations for Logs server.

You can enable auto-update from the server for all agents, or from clients for individual agent instances. Agents must have an active status and be version 4.3 or later.

Auto-update is not supported for Linux BIN packages.

Deactivate or Activate Auto-Update for Individual Agents

You can enable or deactivate auto-update for individual agents by editing the client-side configuration file for that agent.

Agents must be version 4.3 or later.

By default, auto-update is enabled from the client side for an agent.

1. Open the local `liagent.ini` file in an editor.

2. Locate the `[update]` section.
   It looks similar to the following example.
   ```
   [update]
   ; Do not change this parameter
   package_type=msi
   ; Enable automatic update of the agent. If enabled:
   ; the agent will silently check for updates from the server and
   ; if available will automatically download and apply the update.
   ; auto_update=yes
   ```

3. To deactivate auto-update, uncomment `auto_update=yes` and change it to `auto_update=no`.

   > **NOTE**
   > Auto-update for agents is enabled by default. So, the default value for `auto_update` is "yes", even when commented.

4. Save and close the `liagent.ini` file.

Configuring VMware Aria Operations for Logs Agents

After you have deployed an agent, you can configure it to send logs to the VMware Aria Operations for Logs server that you select, specify communication protocols, and set other parameters.

Use these instructions as required to configure your agents to your requirements.

Configure the VMware Aria Operations for Logs Windows Agent

You can configure the VMware Aria Operations for Logs Windows Agent after you install it. Edit the `liagent.ini` file to configureVMware Aria Operations for Logs Windows Agent to send logs to a VMware Aria Operations for Logs, set the communication protocol and port, add Windows event channels, and configure flat file log collection. The file is located in the `%ProgramData%\VMware\Log Insight Agent` directory.

Related Links

You can configure the VMware Aria Operations for Logs Linux Agent after you install it.

You can provide the information that an agent sends to a destination with the filter option in the `[server|<dest_id>]` section of your local `liagent.ini` file.

You can configure multiple VMware Aria Operations for Logs agents.

You can forward logs collected by an agent to up to three destinations. A destination can include VMware Aria Operations for Logs servers or forwarder, or third-party log management solutions.

You can override the default values of the agent configuration file with common parameter values that apply for each agent configuration section for Windows or Linux agents.

Agent-side log parsers extract structured data from raw logs before delivering to the VMware Aria Operations for Logs server. Using log parsers, VMware Aria Operations for Logs can analyze logs, extract information from them, and show those results on the server. Log parsers can be configured for both Windows and Linux VMware Aria Operations for Logs Agents.

Default Configuration of the VMware Aria Operations for Logs Windows Agent

After installation, the `liagent.ini` file contains pre-configured default settings for the VMware Aria Operations for Logs Windows Agent.

VMware Aria Operations for Logs Windows Agent liagent.ini Default Configuration

If you use non-ASCII names and values, save the configuration as UTF-8.

If you are using central configuration, the final configuration is this file joined with settings from the server to form the `liagent-effective.ini` file.

You may find it more efficient to configure the settings from the server's agents page.

```
; Client-side configuration of VMware Log Insight Agent.
; See liagent-effective.ini for the actual configuration used by VMware Log Insight Agent.

[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
;hostname=LOGINSIGHT

;Enables or deactivates centralized configuration from the vRealize Log Insight server.
;When enabled, agent configuration changes made to the liagent.ini file on the server
;are joined with the settings in this file. to this agent. Accepted values are yes or no and  0 or 1.
```

```
;The default is yes.
;
;central_config=yes
;

; Set protocol to use:
; cfapi - Log Insight REST API
; syslog - Syslog protocol
; If omitted the default value is cfapi
;
;proto=cfapi

; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 514
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
;port=9000

;ssl - enable/deactivate SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is no.
;ssl=no

; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30

; FIPS mode.
; Possible values are 1 or 0. If omitted the default value is 1.
; ssl_fips_mode=1

[storage]
;max_disk_buffer - max disk usage limit (data + logs) in MB:
; 100 - 2000 MB, default 200
;max_disk_buffer=2000

[logging]
;debug_level - the level of debug messages to enable:
;   0 - no debug messages
;   1 - trace essential debug messages
;   2 - verbose debug messages (will have negative impact on performance)
;debug_level=0
;
;The interval in minutes to print statistics
;stats_period=15

[update]
; Do not change this parameter
package_type=msi

; Enable automatic update of the agent. If enabled:
; the agent will silently check for updates from the server and
; if available will automatically download and apply the update.
;auto_update=yes
```

```
[winlog|Application]
channel=Application
raw_syslog=no

[winlog|Security]
channel=Security

[winlog|System]
channel=System
```

Parameter	Default Value	Description
hostname	LOGINSIGHT	IP address or host name of the virtual appliance. The default is loginsight.
central_config	yes	Activate or deactivate centralized configuration for this agent. When centralized configuration is deactivated, the agent ignores configuration provided by the server. Accepted values are yes , no ,1 , or 0 . The default value is yes .
proto	cfapi	Protocol that the agent uses to send log events to the server. The possible values are cfapi and syslog . The default is cfapi.
port	9543, 9000, 6514, and 514	Communication port that the agent uses to send log events to the or third party server. By default the agent uses the appropriate port based on the options that are set for SSL and the protocol. See default port values provided in the list below. You need to specify the port option only if it's different from these defaults. • cfapi with SSL activated: 9543 • cfapi with SSL deactivated: 9000 • syslog with SSL activated: 6514 • syslog with SSL deactivated: 514
ssl	yes	Enables or deactivates SSL. The default value is yes. When ssl is set to yes, if you do not set a value for the port, the port is automatically picked up as 9543.
max_disk_buffer	200	The maximum disk space in MB that the VMware Aria Operations for Logs Windows Agent uses to buffer events and its own logs. When the specified max_disk_buffer is reached, the agent begins to drop new incoming events.

Parameter	Default Value	Description
debug_level	0	Defines the log details level. See Define Log Details Level in the VMware Aria Operations for Logs Agents.
channel	Application, Security, System	The Application, Security, and System Windows Event Log channels are commented by default; the VMware Aria Operations for Logs Windows Agent does not collect logs from these channels. See Collect Logs from Windows Events Channels .
raw_syslog	no	For agents that use the syslog protocol, allows the agent to collect and send raw syslog events. The default is no, which means collected events are transformed with user-specified syslog attributes. Activate this option to collect log events without any syslog transformations. Accepted values are yes or 1 and no or 0.
ssl_fips_mode	1	Enables or deactivates FIPS mode for the VMware Aria Operations for Logs Windows Agent through the liagent.ini file. Accepted values are 1 and 0.

Collect Logs from Windows Events Channels

You can add a Windows event channel to the VMware Aria Operations for Logs Windows Agent configuration. The VMware Aria Operations for Logs Windows Agent will collect the log events and send them to the VMware Aria Operations for Logs server.

Log in to the Windows machine on which you installed the VMware Aria Operations for Logs Windows agent and start the services manager to verify that the VMware Aria Operations for Logs agent service is installed.

Field names are restricted. The following names are reserved and cannot be used as field names.

- event_type
- hostname
- source
- text

1. Navigate to the program data directory of the VMware Aria Operations for Logs Windows agent.
   %ProgramData%\VMware\Log Insight Agent

2. Open the liagent.ini file in any text editor.

3. Add the following parameters and set the values for your environment.

Parameter	Description
[winlog| section_name]	A unique name for the configuration section.
channel	The full name of the event channel as shown in the Event Viewer built-in Windows application. To copy the correct channel name, right-click a channel in Event Viewer, select **Properties** and copy the contents of **Full Name** field.
enabled	An optional parameter to enable or deactivate the configuration section. The possible values are yes or no (case-insensitive). The default value is yes.

Parameter	Description
`tags`	Optional parameter to add custom tags to the fields of collected events. Define tags using JSON notation. Tag names can contain letters, numbers, and underscores. A tag name can only begin with a letter or an underscore and cannot exceed 64 characters. Tag names are not case-sensitive. For example, if you use `tags={"tag_name1" : "tag value 1", "Tag_Name1" : "tag value 2" },Tag_Name1` is ignored as a duplicate. You cannot use `event_type` and `timestamp` as tag names. Any duplicates within the same declaration are ignored. If the destination is a syslog server, tags can override the APP-NAME field. For example, tags={"appname":"VROPS"}.
`whitelist, blacklist`	Optional parameters to explicitly include or exclude log events. **NOTE** The `blacklist` option only works for fields; it cannot be used to block text.
`exclude_fields`	(Optional) A parameter to exclude individual fields from collection. You can provide multiple values as a semicolon separated list. For example, `exclude_fields=EventId; ProviderName`

```
[winlog|section_name]
channel=event_channel_name
enabled=yes_or_no
tags={"tag_name1" : "Tag value 1", "tag_name2" : "tag value 2" }
```

4. Save and close the `liagent.ini` file.

Configurations

See the following `[winlog|` configuration examples.

```
[winlog|Events_Firewall ]
channel=Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
enabled=no
[winlog|custom]
channel=Custom
tags={"ChannelDescription": "Events testing channel"}
```

Set up Filtering for Windows Event Channels

You can set up filters for Windows Event channels to explicitly include or exclude log events.

Log in to the Windows machine on which you installed the VMware Aria Operations for Logs Windows agent and start the services manager to verify that the VMware Aria Operations for Logs agent service is installed.

You use the `whitelist` and `blacklist` parameters to evaluate a filter expression. The filter expression is a Boolean expression that consists of event fields and operators.

> **NOTE**
> The `blacklist` option only works for fields; it cannot be used to block text.

- The `whitelist` parameter collects only log events for which the filter expression evaluates to non-zero. If you omit this parameter, the value is an implied 1.
- The `blacklist` parameter excludes log events for which the filter expression evaluates to non-zero. The default value is 0.

For a complete list of Windows event fields and operators see Event Fields and Operators.

1. Navigate to the program data directory of the VMware Aria Operations for Logs Windows agent.
   ```
   %ProgramData%\VMware\Log Insight Agent
   ```

2. Open the `liagent.ini` file in any text editor.

3. Add a `whitelist` or `blacklist` parameter in the `[winlog|]` section.
   For example
   ```
   [winlog|unique_section_name]
   channel = event_channel_name
   blacklist = filter_expression
   ```

4. Create a filter expression from Windows events fields and operators.
   For example
   ```
   whitelist = level > WINLOG_LEVEL_SUCCESS and level < WINLOG_LEVEL_INFO
   ```

5. Save and close the `liagent.ini` file.

Filter Configurations

You can configure the agent to collect only error events, for example
```
[winlog|Security-Error]
channel = Security
whitelist = Level == WINLOG_LEVEL_CRITICAL or Level == WINLOG_LEVEL_ERROR
```
You can configure the agent to collect only VMware Network events from Application channel, for example
```
[winlog|VMwareNetwork]
channel = Application
whitelist = ProviderName == "VMnetAdapter" or ProviderName == "VMnetBridge" or ProviderName == "VM-
netDHCP"
```
You can configure the agent to collect all events from Security channel except particular events, for example
```
[winlog|Security-Verbose]
channel = Security
blacklist = EventID == 4688 or EventID == 5447
```

Event Fields and Operators

Use the Windows event fields and operators to build filter expressions.

Filter Expression Operators

Operator	Description
==, !=	equal and not equal. Use with both numeric and string fields.
>=, >, <, <=	greater or equal, greater than, less than, less than or equal. Use with numeric fields only.
&, |, ^, ~	Bitwise AND, OR, XOR and complement operators. Use with numeric fields only.
and, or	Logical AND and OR. Use to build complex expressions by combining simple expressions.
not	Unary logical NOT operator. Use to reverse the value of an expression.
()	Use parentheses in a logical expression to change the order of evaluation.

Windows Event Fields

You can use the following Windows event fields in a filter expression.

Field name	Field type
Hostname	string
Text	string
ProviderName	string
EventSourceName	string
EventID	numeric
EventRecordID	numeric
Channel	string
UserID	string
Level	numeric You can use the following predefined constants • WINLOG_LEVEL_SUCCESS = 0 • WINLOG_LEVEL_CRITICAL = 1 • WINLOG_LEVEL_ERROR = 2 • WINLOG_LEVEL_WARNING = 3 • WINLOG_LEVEL_INFO = 4 • WINLOG_LEVEL_VERBOSE = 5
Task	numeric
OpCode	numeric
Keywords	numeric You can use the following predefined bit masks • WINLOG_KEYWORD_RESPONSETIME = 0x0001000000000000; • WINLOG_KEYWORD_WDICONTEXT = 0x0002000000000000; • WINLOG_KEYWORD_WDIDIAGNOSTIC = 0x0004000000000000; • WINLOG_KEYWORD_SQM = 0x0008000000000000; • WINLOG_KEYWORD_AUDITFAILURE = 0x0010000000000000; • WINLOG_KEYWORD_AUDITSUCCESS = 0x0020000000000000; • WINLOG_KEYWORD_CORRELATIONHINT = 0x0040000000000000; • WINLOG_KEYWORD_CLASSIC = 0x0080000000000000;

Examples

Collect all critical, error and warning events

```
[winlog|app]
channel = Application
whitelist = level > WINLOG_LEVEL_SUCCESS and level < WINLOG_LEVEL_INFO
```

Collect only Audit Failure events from Security channel

```
[winlog|security]
channel = Security
whitelist = Keywords & WINLOG_KEYWORD_AUDITFAILURE
```

Collect Log Events from a Log File

You can configure the VMware Aria Operations for Logs Windows agent to collect log events from one or more log files.

Log in to the Windows machine on which you installed the VMware Aria Operations for Logs Windows agent and start the services manager to verify that the VMware Aria Operations for Logs agent service is installed.

Field names are restricted. The following names are reserved and cannot be used as field names.

- `event_type`
- `hostname`
- `source`
- `text`

You can have up to three destinations for agent information and filter the information before it is sent. See Forwarding Logs from a VMware Aria Operations for Logs Agent.

> **NOTE**
> - Monitoring a large number of files, such as a thousand or more, leads to higher resource utilization by the agent and impacts the overall performance of the host machine. To prevent this, configure the agent to monitor only the necessary files using patterns and globs, or archive the old log files. If monitoring a large number of files is a requirement, consider increasing the host parameters such as CPU and RAM.
> - The agent can collect from encrypted directories, but only if it is run by the user who encrypted the directory.
> - The agent supports only static directory structures. If the directories have been renamed or added, you must restart the agent to start monitoring these directories, provided the configuration covers the directories.

1. Navigate to the program data directory of the VMware Aria Operations for Logs Windows agent.
   `%ProgramData%\VMware\Log Insight Agent`

2. Open the `liagent.ini` file in any text editor.

3. Locate the [server|<dest_id>] section of the file. Add configuration parameters and set the values for your environment.
   ```
   [filelog|section_name]
   directory=path_to_log_directory
   include=glob_pattern
   ...
   ```

Parameter	Description
`[filelog| section_name ]`	A unique name for the configuration section.
`directory=full-path-to-log-file`	The full path to the log file directory. Glob patterns are supported. Example configurations: • To collect from all sub-directories of `D:\Logs\new_test_logs` directory, use `directory=D:\Logs\new_test_logs\*` • If your sub-directories have their own sub-directories, use the following configuration to monitor all sub-directories `directory=D:\Logs\new_test_logs\*\*`

Parameter	Description
	NOTE To limit the number of files and directories and avoid high resource consumption, you cannot define a directory glob for either the first or second level directories such as: `directory=c:/tmp/*` or `directory=c:\Logs\*` . The directory path must be at least two levels.
	You can define a path to a non-existing directory, and the agent will collect the log files in that directory once the directory and files are created.
	You can define the same directory under one or more different configuration sections, to collect logs from the same file multiple times. This process makes it possible to apply different tags and filters to the same source of events. **NOTE** If you use identical configurations for these sections, duplicated events are observed on the server side.
`include=file_name; ...`	(Optional) The name of a filename or a file mask (glob pattern) from which to collect data. You can provide values as a semicolon separated list. The default value is `*`, which means that all files are included. The parameter is case-sensitive. A file mask (glob pattern) can be used to group files that follow the same naming convention, as well as within a single filename. For example, filenames that include spaces, such as `vRealize Ops Analytics.log` and `vRealize Ops Collector.log`, can be specified with `vRealize? Ops?Analytics*.log` or `vRealize*.log`. By using file masks, you can specify filenames that are acceptable for agent configuration under Linux and Windows hosts. By default `.zip` and `.gz` files are excluded from collection. **IMPORTANT** If you are collecting a rotated log file, use the `include` and `exclude` parameters to specify a glob pattern that matches both the primary and the rotated file. If the glob pattern matches only the primary log file, the VMware Aria Operations for Logs agents might miss events during rotation. The VMware Aria Operations for Logs agents automatically determine the correct order of rotated files and sends events to theVMware Aria Operations for Logs server in the right order. For example, if your primary log file is named `myapp.log` and rotated logs are `myapp.log.1` and `myapp.log.2` and so on, you can use the following `include` pattern: `include= myapp.log;myapp.log.*`
`exclude=regular_expression`	(Optional) A filename or file mask (glob pattern) to exclude from collection. You can provide values as a semicolon separated list. The default value is empty, which means that no file is excluded.
`event_marker=regular_expression`	(Optional) A regular expression that denotes the start of an event in the log file. If omitted defaults to newline. The

Parameter	Description
	expressions you type must use the Perl regular expressions syntax.
	NOTE Symbols, for example quotation marks (" "), are not treated as wrappers for regular expressions. They are treated as part of the pattern.
	Since the VMware Aria Operations for Logs agent is optimized for real-time collection, partial log messages written with an internal delay may be split into multiple events. If log file appending stops for more than 200 ms without a new observed `event_marker`, the partial event is treated as complete, parsed, and delivered. This timing logic is non-configurable and has priority over the `event_marker` setting. Log file appenders should flush full events.
enabled=yes|no	(Optional) A parameter to activate or deactivate the configuration section. The possible values are `yes` or `no`. The default value is `yes`.
charset=*char-encoding-type*	(Optional) The character encoding of the log files that the agent monitors. Possible values are: • `UTF-8` • `UTF-16LE` • `UTF-16BE` The default value is `UTF-8`.
tags=*{"tag-name" : "tag-value", ...}*	(Optional) A parameter to add custom tags to the fields of collected events. Define tags using JSON notation. Tag names can contain letters, numbers, and underscores. A tag name can only begin with a letter or an underscore and cannot exceed 64 characters. Tag names are not case-sensitive. For example, if you use tags={"tag_name1" : "tag value 1", "Tag_Name1" : "tag value 2" }, Tag_Name1 is ignored as a duplicate. You cannot use event_type and timestamp as tag names. Any duplicates within the same declaration are ignored. If the destination is a syslog server, tags can override the APP-NAME field. For example, tags={"appname":"VROPS"}.
exclude_fields	(Optional) A parameter to exclude individual fields from collection. You can provide multiple values as a semicolon- or comma-separated list. For example, • `exclude_fields=hostname; filepath` • `exclude_fields=type; size` • `exclude_fields=type, size`
raw_syslog=Yes|No	For agents that use the syslog protocol, this option allows the agent to collect and send raw syslog events. The default is No, which means collected events are transformed with user-specified syslog attributes. Activate this option to collect events without any syslog transformations.

Configurations

```
[filelog|vCenterMain]
directory=C:\ProgramData\VMware\VMware VirtualCenter\Logs
```

```
include=vpxd-*.log
exclude=vpxd-alert-*.log;vpxd-profiler-*.log
event_marker=^\d{4}-\d{2}-\d{2}[A-Z]\d{2}:\d{2}:\d{2}\.\d{3}
[filelog|ApacheAccessLogs]
enabled=yes
directory=C:\Program Files (x86)\Apache Software Foundation\Apache2.2\logs
include=*.log
exclude=*_old.log
tags={"Provider" : "Apache"}
[filelog|MSSQL]
directory=C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log
charset=UTF-16LE
event_marker=^[^\s]
```

Set up Windows Log File Channel Filtering

You can set up filters for Windows log files to explicitly include or exclude log events.

Log in to the Windows machine on which you installed the VMware Aria Operations for Logs Windows agent and start the services manager to verify that the VMware Aria Operations for Logs agent service is installed.

You use the `whitelist` and `blacklist` parameters to evaluate a filter expression. The filter expression is a Boolean expression that consists of event fields and operators.

> **NOTE**
> The `blacklist` option only works for fields; it cannot be used to block text.

- The `whitelist` parameter collects only log events for which the filter expression evaluates to non-zero. If you omit this parameter, the value is an implied 1.
- The `blacklist` parameter excludes log events for which the filter expression evaluates to non-zero. The default value is 0.

For a complete list of Windows event fields and operators see Event Fields and Operators.

1. Navigate to the program data directory of the VMware Aria Operations for Logs Windows agent.
   ```
   %ProgramData%\VMware\Log Insight Agent
   ```

2. Open the `liagent.ini` file in any text editor.

3. Add a `whitelist` or `blacklist` parameter in the `[filelog|]` section.
   For example:
   ```
   [filelog|apache]
   directory = path_to_log_directory
   include = glob_pattern
   blacklist = filter_expression
   ```

4. Create a filter expression from Windows events fields and operators.
   For example
   ```
   whitelist = myServer
   ```

5. Save and close the `liagent.ini` file.

   ### Filter Configurations

   You can configure the agent to collect only Apache logs where the server_name is
   ```
   [filelog|apache]
   directory=C:\Program Files\Apache Software Foundation\Apache2.4\logs
   include=error.log
   parser=clf
   ```

```
whitelist = server_name == "sample.com"
blacklist = remote_host == "127.0.0.1"
```

Forward Logs to the VMware Aria Operations for Logs Windows Agent

You can forward logs from Windows machines to a machine where the VMware Aria Operations for Logs Windows Agent is running.

See Collect Logs from Windows Events Channels .

You can use Windows Log Forwarding to forward logs from multiple Windows machines to a machine on which the VMware Aria Operations for Logs Windows Agent is installed. You can then configure the VMware Aria Operations for Logs Windows Agent to collect all forwarded logs and send them to a VMware Aria Operations for Logs server.

Get familiar with Windows Log Forwarding. See http://technet.microsoft.com/en-us/library/cc748890.aspx and http://msdn.microsoft.com/en-us/library/windows/desktop/bb870973(v=vs.85).aspx.

1. Add a new section to the VMware Aria Operations for Logs Windows Agent configuration to collect logs from the Windows event channel that receives forwarded logs.

    The default channel name is ForwardedEvents.

2. Set up Windows Log Forwarding.

Go to the VMware Aria Operations for Logs Web user interface and verify that forwarded logs are arriving.

Configure the VMware Aria Operations for Logs Linux Agent

You can configure the VMware Aria Operations for Logs Linux Agent after you install it.

You can use the centralized Agent Configuration to set up the agent to send log events to a VMware Aria Operations for Logs server, specify the communication protocol and port, and configure flat file log collection. For the location of the `liagent.ini` file, see Define Log Details Level in the VMware Aria Operations for Logs Agents.

Related Links

Configure the VMware Aria Operations for Logs Windows Agent on page 73

You can configure the VMware Aria Operations for Logs Windows Agent after you install it. Edit the `liagent.ini` file to configureVMware Aria Operations for Logs Windows Agent to send logs to a VMware Aria Operations for Logs, set the communication protocol and port, add Windows event channels, and configure flat file log collection. The file is located in the `%ProgramData%\VMware\Log Insight Agent` directory.

Filtering Log Events from VMware Aria Operations for Logs Agents on page 93

You can provide the information that an agent sends to a destination with the filter option in the `[server|<dest_id>]` section of your local `liagent.ini` file.

Centralized Configuration of VMware Aria Operations for Logs Agents on page 94

You can configure multiple VMware Aria Operations for Logs agents.

Forwarding Logs from a VMware Aria Operations for Logs Agent on page 97

You can forward logs collected by an agent to up to three destinations. A destination can include VMware Aria Operations for Logs servers or forwarder, or third-party log management solutions.

Using Common Values for Agent Configuration on page 104

You can override the default values of the agent configuration file with common parameter values that apply for each agent configuration section for Windows or Linux agents.

Parsing Logs on page 105

Agent-side log parsers extract structured data from raw logs before delivering to the VMware Aria Operations for Logs server. Using log parsers, VMware Aria Operations for Logs can analyze logs, extract information from them, and show

those results on the server. Log parsers can be configured for both Windows and Linux VMware Aria Operations for Logs Agents.

Default Configuration of the VMware Aria Operations for Logs Linux Agent

After installation, the `liagent.ini` file contains preconfigured default settings for the VMware Aria Operations for Logs Linux Agent.

VMware Aria Operations for Logs Linux Agent liagent.ini Default Configuration

If you use non-ASCII names and values, save the configuration as UTF-8.

If you are using central configuration, the final configuration is this file joined with settings from the server to form the liagent-effective.ini file.

You may find it more efficient to configure the settings from the server's agents page.

```
[server]
; Hostname or IP address of your Log Insight server / cluster load balancer. Default:
;hostname=LOGINSIGHT

;Enables or deactivates centralized configuration from the vRealize Log Insight server.
;When enabled, agent configuration changes made to the liagent.ini file on the server
;are joined with the settings in this file. to this agent. Accepted values are yes or no and  0 or 1.
;The default is yes.
;
;central_config=yes
;
;
; Protocol can be cfapi (Log Insight REST API), syslog. Default:
;proto=cfapi

; Log Insight server port to connect to. Default ports for protocols (all TCP):
; syslog: 514; syslog with ssl: 6514; cfapi: 9000; cfapi with ssl: 9543. Default:
;port=9543

; SSL usage. Default:
;ssl=yes
; Example of configuration with trusted CA:
;ssl=yes
;ssl_ca_path=/etc/pki/tls/certs/ca.pem

; Time in minutes to force reconnection to the server.
; This option mitigates imbalances caused by long-lived TCP connections. Default:
;reconnect=30

; FIPS mode.
; Possible values are 1 or 0. If omitted the default value is 1.
; ssl_fips_mode=1

[logging]
; Logging verbosity: 0 (no debug messages), 1 (essentials), 2 (verbose with more impact on performance).
; This option should always be 0 under normal operating conditions. Default:
```

```
;debug_level=0

[storage]
; Max local storage usage limit (data + logs) in MBs. Valid range: 100-2000 MB.
;max_disk_buffer=2000

; Uncomment the appropriate section to collect system logs
; The recommended way is to enable the Linux content pack from LI server
;[filelog|syslog]
;directory=/var/log
;include=messages;messages.?;syslog;syslog.?
```

Parameter	Default Value	Description
hostname	LOGINSIGHT	IP address or host name of the virtual appliance. The default is `loginsight`.
central_config	yes	Activate or deactivate centralized configuration for this agent. When centralized configuration is deactivated, the agent ignores configuration provided by the server. Accepted values are `yes` , `no` ,`1` , or `0` . The default value is `yes` .
proto	cfapi	Protocol that the agent uses to send log events to the server. The possible values are `cfapi` and `syslog` . The default is cfapi.
port	9543, 9000, 6514, and 514	Communication port that the agent uses to send events to the VMware Aria Operations for Logs server. The default values are 9543 for cfapi with SSL enabled, 9000 for cfapi with SSL deactivated, 6514 for syslog with SSL enabled and 514 for syslog with SSL deactivated.
ssl	yes	Enables or deactivates SSL. The default value is yes. When `ssl` is set to yes, if you do not set a value for the port, the port is automatically picked up as 9543.
max_disk_buffer	200	The maximum disk space in MB that the VMware Aria Operations for Logs Linux Agent uses to buffer events and its own logs. When the specified `max_disk_buffer` is reached, the agent begins to drop new incoming events.
debug_level	0	Defines the log details level. See Define Log Details Level in the VMware Aria Operations for Logs Agents.
ssl_fips_mode	1	Enables or deactivates FIPS mode for the VMware Aria Operations for Logs Linux Agent through the `liagent.ini` file. Accepted values are 1 and 0.

Collect Log Events from a Log File

You can configure the VMware Aria Operations for Logs Linux agent to collect log events from one or more log files.

- Log in as **root** or use `sudo` to run console commands.
- Verify that the VMware Aria Operations for Logs Linux agent is installed and running. Log in to the Linux machine on which you installed the VMware Aria Operations for Logs Linux agent, open a console, and run `pgrep liagent`.

By default the VMware Aria Operations for Logs Linux agent collects hidden files created by applications or editors. The hidden filenames start with a period. You can prevent the VMware Aria Operations for Logs Linux agent from collecting hidden files by adding an exclude parameter, `exclude=.*`.

Field names are restricted. The following names are reserved and cannot be used as field names.

- `event_type`
- `hostname`
- `source`
- `text`

You can specify up to three destinations for agent information and filter the information before it is sent. See Forwarding Logs from a VMware Aria Operations for Logs Agent

> **NOTE**
> Monitoring a large number of files, such as a thousand or more, leads to a higher resource utilization by VMware Aria Operations for Logs Agent and impacts the overall performance of the host machine. To prevent this, configure the agent to monitor only the necessary files using patterns and globs, or archive the old log files. If monitoring a large number of files is a requirement, consider increasing the host parameters such as CPU and RAM.

1. Open the `/var/lib/loginsight-agent/liagent.ini` file in any text editor.

2. Locate the [server|<dest_id>] section of the file. Add configuration parameters and set the values for your environment.

```
[filelog|section_name]
directory=path_to_log_directory
include=glob_pattern
...
```

Parameter	Description
`[filelog| section_name ]`	A unique name for the configuration section.

`directory=full-path-to-log-file`	The full path to the log file directory. Glob patterns are supported. Example configurations:
	
	• To collect from all sub-directories of `D:\Logs\new_test_logs`directory, use `directory=D:\Logs\new_test_logs\*`
	• If your sub-directories have their own sub-directories, use the following configuration to monitor all sub-directories `directory=D:\Logs\new_test_logs\*\*`
	
	    NOTE
	    To limit the number of files and directories and avoid high resource consumption, you cannot define a directory glob for either the first or second level directories such as: `directory=c:/tmp/*` or `directory=c:\Logs\*` . The directory path must be at least two levels.

Parameter	Description
	You can define a path to a non-existing directory, and the agent will collect the log files in that directory once the directory and files are created.
	You can define the same directory under one or more different configuration sections, to collect logs from the same file multiple times. This process makes it possible to apply different tags and filters to the same source of events.
	NOTE If you use identical configurations for these sections, duplicated events are observed on the server side.
`include=file_name; ...`	(Optional) The name of a filename or a file mask (glob pattern) from which to collect data. You can provide values as a semicolon separated list. The default value is `*`, which means that all files are included. The parameter is case-sensitive.
	A file mask (glob pattern) can be used to group files that follow the same naming convention, as well as within a single filename. For example, filenames that include spaces, such as `vRealize Ops Analytics.log` and `vRealize Ops Collector.log`, can be specified with `vRealize? Ops?Analytics*.log` or `vRealize*.log`. By using file masks, you can specify filenames that are acceptable for agent configuration under Linux and Windows hosts.
	By default `.zip` and `.gz` files are excluded from collection.
	IMPORTANT If you are collecting a rotated log file, use the `include` and `exclude` parameters to specify a glob pattern that matches both the primary and the rotated file. If the glob pattern matches only the primary log file, the VMware Aria Operations for Logs agents might miss events during rotation. The VMware Aria Operations for Logs agents automatically determine the correct order of rotated files and sends events to theVMware Aria Operations for Logs server in the right order. For example, if your primary log file is named `myapp.log` and rotated logs are `myapp.log.1` and `myapp.log.2` and so on, you can use the following `include` pattern: `include= myapp.log;myapp.log.*`
`exclude=regular_expression`	(Optional) A filename or file mask (glob pattern) to exclude from collection. You can provide values as a semicolon separated list. The default value is empty, which means that no file is excluded.
`event_marker=regular_expression`	(Optional) A regular expression that denotes the start of an event in the log file. If omitted defaults to newline. The expressions you type must use the Perl regular expressions syntax.
	NOTE Symbols, for example quotation marks (`"  "`), are not treated as wrappers for regular expressions. They are treated as part of the pattern.

Parameter	Description
	Since the VMware Aria Operations for Logs agent is optimized for real-time collection, partial log messages written with an internal delay may be split into multiple events. If log file appending stops for more than 200 ms without a new observed `event_marker`, the partial event is treated as complete, parsed, and delivered. This timing logic is non-configurable and has priority over the `event_marker` setting. Log file appenders should flush full events.
`enabled=yes|no`	(Optional) A parameter to activate or deactivate the configuration section. The possible values are `yes` or `no`. The default value is `yes`.
`charset=char-encoding-type`	(Optional) The character encoding of the log files that the agent monitors. Possible values are: • `UTF-8` • `UTF-16LE` • `UTF-16BE` The default value is `UTF-8`.
`tags={"tag-name" : "tag-value", ...}`	(Optional) A parameter to add custom tags to the fields of collected events. Define tags using JSON notation. Tag names can contain letters, numbers, and underscores. A tag name can only begin with a letter or an underscore and cannot exceed 64 characters. Tag names are not case-sensitive. For example, if you use tags={"tag_name1" : "tag value 1", "Tag_Name1" : "tag value 2" }, Tag_Name1 is ignored as a duplicate. You cannot use event_type and timestamp as tag names. Any duplicates within the same declaration are ignored. If the destination is a syslog server, tags can override the APP-NAME field. For example, tags={"appname":"VROPS"}.
`exclude_fields`	(Optional) A parameter to exclude individual fields from collection. You can provide multiple values as a semicolon- or comma-separated list. For example, • `exclude_fields=hostname; filepath` • `exclude_fields=type; size` • `exclude_fields=type, size`
`raw_syslog=Yes|No`	For agents that use the syslog protocol, this option allows the agent to collect and send raw syslog events. The default is No, which means collected events are transformed with user-specified syslog attributes. Activate this option to collect events without any syslog transformations.

3. Save and close the `liagent.ini` file.

Configurations

```
[filelog|messages]
directory=/var/log
include=messages;messages.?

[filelog|syslog]
directory=/var/log
include=syslog;syslog.?
```

```
[filelog|Apache]
directory=/var/log/apache2
include=*
```

Filter Log Events

You can filter all collected log events on the VMware Aria Operations for Logs Linux agent based on their field values to specify which log events to pick or drop. You can use the `whitelist` and `blacklist` collector options to define filters.

- Log in as **root** or use `sudo` to run console commands.
- Log in to the Linux machine on which you installed the VMware Aria Operations for Logs Linux agent, open a console and run `pgrep liagent` to verify that the VMware Aria Operations for Logs Linux agent is installed and running.

> **TIP**
> By default theVMware Aria Operations for Logs Linux agent collects hidden files created by programs or editors. The hidden file names start with a period. You can prevent the VMware Aria Operations for Logs Linux agent from collecting hidden files, by adding an exclude `exclude=.*` parameter.

For each log event, the collector evaluates the `whitelist` and `blacklist` filter expression. If the `whitelist` expression evaluates to true and the `blacklist` expression evaluates to false or cannot be evaluated, the event moves to the queue for further processing. In any other case, the collector drops the event. The default value of the `whitelist` expression is true and the default value of the `blacklist` expression is false.

> **TIP**
> The `Filelog` collector provides fewer fields for filtering. To obtain fields for filtering, you can parse the logs. For more information, see Parsing Logs.

A `whitelist` or `blacklist` filter is a set of variables, literals, and operators that evaluates to a single logical or integer value. You use the log event fields as variables and double quoted strings and numbers as literals. For information about the operators that you can use within a filter expression, see Event Fields and Operators.

> **NOTE**
> - If you compare a number with a string or if the comparison involves numerical strings, each string is converted to a number and the comparison is performed numerically. For example:
>   - The expression `whitelist = 123.0 == "000123"` evaluates to true.
>   - The expression `whitelist = "00987" == "987.00"` evaluates to true.
>   - In the expression `whitelist = response_size >= "12.12"` , if the `response_size` field has a numeric value, the expression is evaluated numerically. If the response size is greater than 12.12, the expression is true, else it is false.
>   - In the expression `whitelist = "09123" < "234"` , both the string literals are converted to numeric values and the expression evaluates to false.
> - If one of the string operands cannot be converted to numeric values, both the operands are converted to string. A simple case-sensitive lexicographical comparison is performed. For example:
>   - The expression `whitelist = "1234a" == "1234A"` is a string comparison that evaluates to false.
>   - The expression `whitelist = 4 < "four"` converts 4 to "4" and evaluates to true.
>   - In the expression `whitelist = response_size > "thousand"` , the value of the `response_size` field is converted to a string value, which evaluates the expression to false.
> - If a filter expression evaluates to an integer value, it is treated as false if it is 0 and true otherwise.
>   For example, the expression `whitelist = some_integer & 1` evaluates to true if the `some_integer` field has a least significant bit set and false otherwise.

For a complete list of log event fields and operators see Collect Log Events from a Log File.

In this example, you collect Apache access logs from the file `/var/log/httpd/access`. Some sample logs from the file are:

- `127.0.0.1 - frank [10/Oct/2016:13:55:36 +0400] "GET /apache_pb.gif HTTP/1.0" 200 2326`
- `198.51.100.56 - john [10/Oct/2016:14:15:31 +0400] "GET /some.gif HTTP/1.0" 200 8270`
- `198.51.100.12 - smith [10/Oct/2016:14:15:31 +0400] "GET /another.gif HTTP/1.0" 303 348`
- `198.51.100.32 - test [10/Oct/2016:15:22:55 +0400] "GET /experimental_page.gif HTTP/1.0" 400 46374`
- `127.0.0.1 - test [10/Oct/2016:15:22:57 +0400] "GET /experimental_page2.gif HTTP/1.0" 301 100`

1. Define a parser for the logs, as shown in the following snippet:

   ```
   [parser|apache-access]
   base_parser=clf
   format=%h %l %u %t \"%r\" %s %b
   ```

   The parser that you have defined extracts the `remote_host`, `remote_log_name`, `remote_auth_user`, `timestamp`, `request`, `status_code`, and `response_size` fields for every log event collected from the file `/var/log/httpd/access`. You can use these fields to filter events.

2. Open the `/var/lib/loginsight-agent/liagent.ini` file in any text editor.

3. Define a `Filelog` section in the file to collect and parse logs, as shown in the following snippet:

   ```
   [filelog|apache-access]
   directory = /var/log/httpd/
   include = access
   parser = apache-access
   ```

4. Filter log events according to your requirement.

   - To collect logs where the HTTP status is 200, you can define a `whitelist` in the `Filelog` section as shown in the following snippet:

     ```
     [filelog|apache-access]
     directory = /var/log/httpd/
     include = access
     parser = apache-access
     whitelist = status_code == 200
     ```

     The `whitelist` expression evaluates to true only for the first and second log events from the sample logs and the collector picks these events.

     If the `status_code` field does not exist in the log event because it is not present in the log or is not parsed, the `whitelist` expression cannot be evaluated, which means it evaluates to false and collector drops the event.

   - To drop a log event that you are not interested in, you can use the `blacklist` option. For example, if you are not interested in local traffic, you can block the local IP as shown in the following snippet:

     ```
     [filelog|apache-access]
     directory = /var/log/httpd/
     include = access
     parser = apache-access
     blacklist = remote_host == "127.0.0.1"
     ```

     The collector picks the second, third, and fourth log events from the sample logs.

   - To filter log events based on more than one predicate, you can use `or` and `and` operators. For example, you can drop events generated from a local IP or events generated by test users from any host that you do not require, as shown in the following snippet:

     ```
     [filelog|apache-access]
     directory = /var/log/httpd/
     ```

```
include = access
parser = apache-access
blacklist = remote_host == "127.0.0.1" or remote_auth_user == "test"
```

Using the `or` operator evaluates the `blacklist` expression to true to skip an unwanted log event. The expression instructs the collector to drop the event if the `remote_host` field value is "127.0.0.1" or the `remote_auth_user` field value is "test".

The collector picks the second and the third log events from the sample logs.

- To drop log events generated from a local IP by test users, you can use `and` in the `blacklist` expression, as shown in the following snippet:

```
[filelog|apache-access]
directory = /var/log/httpd/
include = access
parser = apache-access
blacklist = remote_host == "127.0.0.1" and remote_auth_user == "test"
```

The collector drops the fifth log event from the sample logs.

- You can use `whitelist` and `blacklist` filters together. For example, if you require log events where the response size is greater than 1024 bytes but you do not require events that originated from a local host, you can use the following snippet:

```
[filelog|apache-access]
directory = /var/log/httpd/
include = access
parser = apache-access
whitelist = response_size > 1024
blacklist = remote_host == "127.0.0.1" or remote_host == "localhost"
```

The collector picks the second log event from the sample logs.

Collecting Events from `journald`

Beginning with VMware Aria Operations for Logs 4.6, agents can read logs from the `journald` system service for log data in Linux distributions running `systemd`. `journald` is now the default standard for logging in `systemd`-based Linux platforms. The `journald` configuration section supports the following options:

`journal_files`

The journal files to monitor. The following values are supported:

Value	Description
all	Open and monitor all the available journal files.
local	Monitor and read only the journal files generated on the local machine.
runtime	Monitor and read only the volatile journal files, excluding the files in the persistent storage.
system	Monitor and read only the system services and kernel journal files.
user	Monitor and read only journal files of the current user.

`fetch_fields`

The fields to fetch with the message from the journal log entries. The value for this option is a case-insensitive list of field names separated by comma. The following values are supported:

Value	Description
pri_severity,pri_facility,syslog_identifier	Default value for this option.
*	Fetch all the fields.
all	Do not fetch any fields.

Filtering Log Events from VMware Aria Operations for Logs Agents

You can provide the information that an agent sends to a destination with the filter option in the `[server|<dest_id>]` section of your local `liagent.ini` file.

The option is of the following form:

```
filter = {collector_type; collector_filter; event_filter}
```

Filter type	Description
collector_type	A comma-separated list that defines the collector types. Supported values are filelog or winlog. If no value is provided, all collector types are used.
collector_filter	Specifies the name of a collector section in a regex format. For example, `vcops_.*` refers to all collector sections that begin with "vcops_".
event_filter	Filters for log event fields use the same syntax as an acceptlist or a denylist in collector sections. An agent sends only log events that evaluate the expression to True or a non-zero value. An empty event_filter always evaluates to True. To use event_filter on log events, you must have a parser defined in appropriate collector sections for field extraction. If an expression cannot be evaluated due to absence of fields in the collected log event, then the event is dropped.

More than one filter expression can be specified by separating them with a comma as shown in the following example:

```
filter=
{winlog;Micr.*;},{filelog;apache-access;level=="error"}
```

If a message meets more than one set of filter criteria for a destination target, it is sent only once.

Table 3: Syntax Examples

Filter	Meaning
filter= {winlog;Microsoft.*;}	Sends log events from winlog collectors only if the event name begins with "Microsoft".
filter= {winlog;Microsoft.*; eventid == 1023}	Sends log events from winlog collectors only if the event name begins with "Microsoft" and Event ID equal to 1023.
filter= {;.*;}	Default filter value. Sends all log events from all sources.
filter= {winlog;.*;}	Sends all log events from winlog sections.
filter= {filelog;syslog;facility<5}	Sends log events from [filelog|syslog] section if facility less than 5. [filelog|syslog] sections must have a parser that extracts the facility field. Otherwise, all events are skipped.
filter= {;;}	Matches no log events. Use this syntax to deactivate log forwarding.

The following example adds a filter to the configuration of the second destination of the previous example.

```
; The second destination receives just syslog events through the plain syslog protocol.
[server|syslog-audit]
hostname=third_party_audit_management.eng.vmware.com
proto=syslog
ssl=no
filter= {filelog; syslog; }
```

The next example uses a more complex filter expression.

```
; This destination receives vRealize Operations events if they have the level field equal
;to "error" or "warning" and they are collected by sections whose name begins with "vrops-"

[server|licf-prod1]
hostname=vrops-errors.licf.vmware.com
filter= {; vrops-.*; level == "error" || level == "warning"}
```

More than one filter expression can be specified by separating them with a comma as shown in the following example.

```
filter= e.
{winlog;Micr.*;},{filelog;apache-access;level=="error"}
```

Related Links

You can configure the VMware Aria Operations for Logs Windows Agent after you install it. Edit the `liagent.ini` file to configureVMware Aria Operations for Logs Windows Agent to send logs to a VMware Aria Operations for Logs, set the communication protocol and port, add Windows event channels, and configure flat file log collection. The file is located in the `%ProgramData%\VMware\Log Insight Agent` directory.

You can configure the VMware Aria Operations for Logs Linux Agent after you install it.

You can configure multiple VMware Aria Operations for Logs agents.

You can forward logs collected by an agent to up to three destinations. A destination can include VMware Aria Operations for Logs servers or forwarder, or third-party log management solutions.

You can override the default values of the agent configuration file with common parameter values that apply for each agent configuration section for Windows or Linux agents.

Agent-side log parsers extract structured data from raw logs before delivering to the VMware Aria Operations for Logs server. Using log parsers, VMware Aria Operations for Logs can analyze logs, extract information from them, and show those results on the server. Log parsers can be configured for both Windows and Linux VMware Aria Operations for Logs Agents.

Centralized Configuration of VMware Aria Operations for Logs Agents

You can configure multiple VMware Aria Operations for Logs agents.

Each VMware Aria Operations for Logs agent has a local configuration and a server-side configuration. The local configuration is stored in the `liagent.ini` file on the virtual or physical machine where the VMware Aria Operations for Logs agent is installed. The server-side configuration is accessible and editable, for example, from **Management** > **Agents** in the web user interface. The configuration of each VMware Aria Operations for Logs agent is made up of sections and keys. Keys have configurable values.

VMware Aria Operations for Logs agents periodically poll the VMware Aria Operations for Logs server and receive the server-side configuration. The server-side configuration and the local configuration are merged and the result is the effective configuration. Each VMware Aria Operations for Logs agent uses the effective configuration as its operating configuration. Configurations merge section by section and key by key. The values in the server-side configuration override the values in the local configuration. The merging rules are the following:

- If a section is present only in the local configuration or only in the server-side configuration, this section and all its content become a part of the effective configuration.
- If a section is present in both the local and server-side configuration, the keys in the section are merged according to the following rules:
  - If a key is present only in the local configuration or only in the server-side configuration, the key and its value become a part of this section in the effective configuration.
  - If a key is present in both the local configuration and the server-side configuration, the key becomes a part of this section in the effective configuration, and the value in the server-side configuration is used.

As a VMware Aria Operations for Logs administrator or a user with edit access for agents, you can apply a centralized configuration to all VMware Aria Operations for Logs agents. For example, you can navigate to **Management > Agents**, enter the configuration settings in the **Agent Configuration** box, and click **Save Configuration for All Agents**. The configuration is applied to all the configurable active agents during the next poll cycle.

As an administrator, you can also use specific filters in agent groups, such as by OS, agent version, hostname, or IP ranges, and apply the configuration to specific VMware Aria Operations for Logs agents. For information about agent groups, see *Working with Agent Groups*.

> **NOTE**
>
> - You can apply a centralized configuration only to VMware Aria Operations for Logs agents that use the cfapi protocol.
> - A VMware Aria Operations for Logs agent is not configurable in either of the following scenarios:
>   - The current VMware Aria Operations for Logs server is not a primary destination. For information about configuring multiple destinations, see Specify an Agent's Target .
>   - The parameter `central_config = no` is used in the agent configuration. For information about the default agent configuration for Windows, see Default Configuration of the VMware Aria Operations for Logs Windows Agent.

Related Links

Configure the VMware Aria Operations for Logs Windows Agent on page 73
You can configure the VMware Aria Operations for Logs Windows Agent after you install it. Edit the `liagent.ini` file to configureVMware Aria Operations for Logs Windows Agent to send logs to a VMware Aria Operations for Logs, set the communication protocol and port, add Windows event channels, and configure flat file log collection. The file is located in the `%ProgramData%\VMware\Log Insight Agent` directory.

Configure the VMware Aria Operations for Logs Linux Agent on page 84
You can configure the VMware Aria Operations for Logs Linux Agent after you install it.

Filtering Log Events from VMware Aria Operations for Logs Agents on page 93
You can provide the information that an agent sends to a destination with the filter option in the `[server|<dest_id>]` section of your local `liagent.ini` file.

Forwarding Logs from a VMware Aria Operations for Logs Agent on page 97
You can forward logs collected by an agent to up to three destinations. A destination can include VMware Aria Operations for Logs servers or forwarder, or third-party log management solutions.

Using Common Values for Agent Configuration on page 104
You can override the default values of the agent configuration file with common parameter values that apply for each agent configuration section for Windows or Linux agents.

Agent-side log parsers extract structured data from raw logs before delivering to the VMware Aria Operations for Logs server. Using log parsers, VMware Aria Operations for Logs can analyze logs, extract information from them, and show those results on the server. Log parsers can be configured for both Windows and Linux VMware Aria Operations for Logs Agents.

An Example of Configuration Merging

An example of merging local and server-side configuration of the VMware Aria Operations for Logs Windows Agent.

<u>Local Configuration</u>

You can have the following local configuration of the VMware Aria Operations for Logs Windows Agent.

```
[server]
proto=cfapi
hostname=HOST
port=9000

[winlog|Application]
channel=Application

[winlog|Security]
channel=Security

[winlog|System]
channel=System

[filelog|ApacheAccessLogs]
enabled=yes
directory=C:\Program Files (x86)\Apache Software Foundation\Apache2.2\logs
include=*.log
exclude=*_old.log
event_marker=^(\d{1,3}\.){3}\d{1,3} - -
```

<u>Server-Side Configuration</u>

You can use the **Management** > **Agents** page of the Web user interface to apply centralized configuration to all agents. For example, you can exclude and add collection channels, and change the default reconnect setting.

```
[server]
reconnect=20

[winlog|Security]
channel=Security
enabled=no

[winlog|Microsoft-Windows-DeviceSetupManagerOperational]
channel=Microsoft-Windows-DeviceSetupManager/Operational
```

<u>**Effective Configuration**</u>

The effective configuration is a result of the merging of the local and the server-side configurations. The VMware Aria Operations for Logs Windows Agent is configured to :

- reconnect to the VMware Aria Operations for Logs server every 20 minutes
- continue to collect Application and System event channels
- stop collecting Security event channel
- start to collect Microsoft-Windows-DeviceSetupManager/Operational event channel
- continue to collect ApacheAccessLogs

```
[server]
proto=cfapi
hostname=HOST
port=9000
reconnect=20

[winlog|Application]
channel=Application

[winlog|Security]
channel=Security
enabled=no

[winlog|System]
channel=System

[winlog|Microsoft-Windows-DeviceSetupManagerOperational]
channel=Microsoft-Windows-DeviceSetupManager/Operational

[filelog|ApacheAccessLogs]
enabled=yes
directory=C:\Program Files (x86)\Apache Software Foundation\Apache2.2\logs
include=*.log
exclude=*_old.log
event_marker=^(\d{1,3}\.){3}\d{1,3} - -
```

Forwarding Logs from a VMware Aria Operations for Logs Agent

You can forward logs collected by an agent to up to three destinations. A destination can include VMware Aria Operations for Logs servers or forwarder, or third-party log management solutions.

For example, you might want to send audit or system logs to a server for your security team, application logs to a dev ops team server, and metrics logs to an IT management system. You use filters to specify which information goes to a destination. You can forward logs from a single VMware Aria Operations for Logs agent to up to three destinations.

Agent configuration is done through the `[server|<dest_id>]` section of your local `liagent.ini` file. Use the cfapi protocol with VMware Aria Operations for Logs servers or forwarders and syslog with other targets or destinations.

When you specify more than one destination for an agent, the first destination uses the default `loginsight` location. You must specify location information for other destinations.

The next example shows a portion of an liagent.ini file that specifies two destinations. The default server name `loginsight` is implicit for the first destination by default and is not specified. The second `[server|<dest_id>]` section specifies a destination.

```
; The first (default) destination receives all collected events.
[server]
ssl=yes


; The second destination receives just syslog events through the plain syslog protocol.
[server|syslog-audit]
hostname=third_party_audit_management.eng.vmware.com
proto=syslog
ssl=no
```

For information about creating filters for agents, see Filtering Log Events from VMware Aria Operations for Logs Agents.

Related Links

Configure the VMware Aria Operations for Logs Windows Agent on page 73

You can configure the VMware Aria Operations for Logs Windows Agent after you install it. Edit the `liagent.ini` file to configureVMware Aria Operations for Logs Windows Agent to send logs to a VMware Aria Operations for Logs, set the communication protocol and port, add Windows event channels, and configure flat file log collection. The file is located in the `%ProgramData%\VMware\Log Insight Agent` directory.

Configure the VMware Aria Operations for Logs Linux Agent on page 84

You can configure the VMware Aria Operations for Logs Linux Agent after you install it.

Filtering Log Events from VMware Aria Operations for Logs Agents on page 93

You can provide the information that an agent sends to a destination with the filter option in the `[server|<dest_id>]` section of your local `liagent.ini` file.

Centralized Configuration of VMware Aria Operations for Logs Agents on page 94

You can configure multiple VMware Aria Operations for Logs agents.

Using Common Values for Agent Configuration on page 104

You can override the default values of the agent configuration file with common parameter values that apply for each agent configuration section for Windows or Linux agents.

Parsing Logs on page 105

Agent-side log parsers extract structured data from raw logs before delivering to the VMware Aria Operations for Logs server. Using log parsers, VMware Aria Operations for Logs can analyze logs, extract information from them, and show those results on the server. Log parsers can be configured for both Windows and Linux VMware Aria Operations for Logs Agents.

Set Target VMware Aria Operations for Logs Server

You can set or change the target VMware Aria Operations for Logs server for a VMware Aria Operations for Logs agent running on Windows. You can send log events to up to three destinations and filter output per destination.

- Log in to the Windows machine on which you installed the VMware Aria Operations for Logs Windows agent and start the Services manager to verify that the VMware Aria Operations for Logsagent service is installed.
- If you have a VMware Aria Operations for Logs cluster with an enabled Integrated Load Balancer, see Enable Integrated Load Balancer for custom SSL certificate-specific requirements.

The default destination can be configured through the `[server]` section of the `liagent.ini` file. The default destination is always present and by default the hostname is set to `loginsight`. To add more target destinations, create a `[server|<dest_id>]` section for each target. You must specify a unique hostname as the destination ID for each additional connection. You can use the same options for additional destinations as for the default `[server]` section. Do

not configure additional destinations for auto-upgrade or use them for agent configuration. You can specify two additional destinations.

By default, the agent sends all collected logs to all destinations. You can filter logs to send different logs to different destinations with the `file` option. For more information, see Filtering Log Events.

1. Navigate to the program data directory of the VMware Aria Operations for Logs Windows agent.
   `%ProgramData%\VMware\Log Insight Agent`

2. Open the `liagent.ini` file in any text editor.

3. Modify the following parameters and set the values for your environment.

Parameter	Description
`proto`	Protocol that the agent uses to send log events to the server. The possible values are `cfapi` and `syslog`. The default is cfapi.
`hostname`	IP address or host name of the VMware Aria Operations for Logs virtual appliance. You can specify an IPv4 or IPv6 address. An IPv6 address can be specified with or without square brackets. For example: `hostname = 2001:cdba::3257:9652` or `hostname = [2001:cdba::3257:9652]` If the host supports both IPv4 and IPv6 stacks and a domain name is specified as the hostname, then the agent chooses the IP stack based on the IP address that the name resolver returns. If the resolver returns both IPv4 and IPv6 addresses, then the agent tries to connect sequentially to both addresses in the given order.
`max_disk_buffer`	The maximum disk space in MB that the VMware Aria Operations for Logs Windows Agent can use to buffer log events collected for this particular server. The option overrides the `[storage].max_disk_buffer` value for this server. The default value is 150 MB and you can set the buffer size to between 50 through 8000 MB.
`port`	Communication port that the agent uses to send log events to the or third party server. By default the agent uses the appropriate port based on the options that are set for SSL and the protocol. See default port values provided in the list below. You need to specify the port option only if it's different from these defaults. • cfapi with SSL activated: 9543 • cfapi with SSL deactivated: 9000 • syslog with SSL activated: 6514 • syslog with SSL deactivated: 514
`ssl`	Enables or deactivates SSL. The default value is yes. When `ssl` is set to yes, the port is set as 9543, unless you specify otherwise.
`reconnect`	The time in minutes to force re-connection to the server. The default value is 30.

Parameter	Description
`filter`	Specifies the information an agent sends to a destination. This option takes three arguments: `{collector_type; collector_filter; event_filter}`

```
[server]
hostname=LOGINSIGHT
; Hostname or IP address of your Log Insight server / cluster load balancer. Default:
;hostname=LOGINSIGHT

; Protocol can be cfapi (Log Insight REST API), syslog. Default:
;proto=cfapi

; Log Insight server port to connect to. Default ports for protocols (all TCP):
; syslog: 514; syslog with ssl: 6514; cfapi: 9000; cfapi with ssl: 9543. Default:
;port=9543

; SSL usage. Default:
;ssl=yes
```

4. Save and close the `liagent.ini` file.

The following configuration example sets a target VMware Aria Operations for Logs server that uses a trusted certificate authority.

```
[server]
proto=cfapi
hostname=LOGINSIGHT
port=9543
ssl=yes;
ssl_ca_path=/etc/pki/tls/certs/ca.pem
```

The following example shows a multi-destination configuration that includes filtering messages per destination.

```
; The first (default) destination receives all collected events.
[server]
hostname=prod1.licf.vmware.com

; The second destination receives just syslog events through the plain syslog protocol.
[server|syslog-audit]
hostname=third_party_audit_management.eng.vmware.com
proto=syslog
ssl=no
filter={filelog; syslog; }


; The third destination receives vRealize Operations events if they have the level field equal to
 "error" or "warning"
; and they are collected by sections whose name begins with "vrops-"

[server|licf-prod1]
hostname=vrops-errors.licf.vmware.com
filter={; vrops-.*; level == "error" || level == "warning"}

; Collecting syslog messages.
```

```
[filelog|syslog]
directory=/var/log
include=messages


; various vROPs logs. Note that all section names begin with a "vrops-" prefix, which is used in
 third destination filter.
[filelog|vrops-ANALYTICS-analytics]
directory=/data/vcops/log
include=analytics*.log*
exclude=analytics*-gc.log*
parser=auto


[filelog|vrops-COLLECTOR-collector]
directory=/data/vcops/log
include=collector.log*
event_marker=^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}
parser=auto


[filelog|vrops-COLLECTOR-collector_wrapper]
directory=/data/vcops/log
include=collector-wrapper.log*
event_marker=^\d{4}-\d{2}-\d{2} [\s]\d{2}:\d{2}:\d{2}\.\d{3}
parser=auto
```

You can configure additional SSL options for the VMware Aria Operations for Logs agent. See Configure SSL Connection Between the Server and the VMware Aria Operations for Logs Agents.

Specify an Agent's Target

You can specify up to three destinations for the VMware Aria Operations for Logs Linux agent to send log events to.

- Log in as **root** or use `sudo` to run console commands.
- Log in to the Linux machine on which you installed the VMware Aria Operations for Logs Linux agent, open a console and run `pgrep liagent` to verify that the VMware Aria Operations for Logs Linux agent is installed and running.
- If you have a VMware Aria Operations for Logs cluster with an activated Integrated Load Balancer, see Activate Integrated Load Balancer for custom SSL certificate-specific requirements.

Multiple destination connections are defined through the `[server|<dest_id>]` section of the `li-agent.ini` file where *<dest_id>* is a unique per-configuration connection id. You can use the same options for additional destinations as for the default `[server]` section. However, do not configure additional destinations for auto-upgrade or use them for agent configuration. You can specify two additional destinations.

The first target you define can use the default server value `loginsight` . When you define additional targets, you must specify a hostname in the `[server]` sections for subsequent targets. Without filtering, the agent sends all collected logs to all destinations. This is the default. However, you can filter logs to send different logs to different destinations.

1. Open the `/var/lib/loginsight-agent/liagent.ini` file in any text editor.

2. Modify the following parameters and set the values for your environment.

Parameter	Description
proto	Protocol that the agent uses to send log events to the server. The possible values are `cfapi` and `syslog` .
	The default is cfapi.

Parameter	Description

`hostname`	IP address or host name of the VMware Aria Operations for Logs virtual appliance.
	
	You can specify an IPv4 or IPv6 address. An IPv6 address can be specified with or without square brackets. For example:
	`hostname = 2001:cdba::3257:9652`
	`or`
	`hostname = [2001:cdba::3257:9652]`
	If the host supports both IPv4 and IPv6 stacks and a domain name is specified as the hostname, then the agent uses the IP stack depending on the IP address that is returned by the name resolver. If the resolver returns both IPv4 and IPv6 addresses, then the agent tries to connect sequentially to both addresses in the given order.

`max_disk_buffer`	The maximum disk space in MB that the VMware Aria Operations for Logs Linux Agent can use to buffer log events collected for this particular server. The option overrides the `[storage].max_disk_buffer` value for this server. The default value is 150 MB and you can set the buffer size to between 50 through 8000 MB.
`port`	Communication port that the agent uses to send log events to the or third party server. By default the agent uses the appropriate port based on the options that are set for SSL and the protocol. See default port values provided in the list below. You need to specify the port option only if it's different from these defaults. • cfapi with SSL activated: 9543 • cfapi with SSL deactivated: 9000 • syslog with SSL activated: 6514 • syslog with SSL deactivated: 514
`ssl`	Enables or deactivates SSL. The default value is yes. When `ssl` is set to yes, if you do not set a value for the port, the port is automatically picked up as 9543.
`reconnect`	The time in minutes to force reconnection to the server. The default value is 30.

```
[server]
hostname=LOGINSIGHT
; Hostname or IP address of your Log Insight server / cluster load balancer. Default:
;hostname=LOGINSIGHT

; Protocol can be cfapi (Log Insight REST API), syslog. Default:
;proto=cfapi

; Log Insight server port to connect to. Default ports for protocols (all TCP):
; syslog: 514; syslog with ssl: 6514; cfapi: 9000; cfapi with ssl: 9543. Default:
;port=9543

; SSL usage. Default:
;ssl=yes
```

3. Save and close the `liagent.ini` file.

The following configuration example sets a target VMware Aria Operations for Logs server that uses a trusted certificate authority.

```
[server]
proto=cfapi
hostname=LOGINSIGHT
port=9543
ssl=yes;
ssl_ca_path=/etc/pki/tls/certs/ca.pem
```

The following example shows a multi-destination configuration.

- The first (default) destination receives all collected log events.

```
[server]
hostname=prod1.licf.vmware.com
```

- The second destination receives just syslog events through the plain syslog protocol.

```
[server|syslog-audit]
hostname=third_party_audit_management.eng.vmware.com
proto=syslog
ssl=no
filter= {filelog; syslog; }
```

- The third destination receives VMware Aria Operations log events if they have the level field equal to "error" or "warning" and they are collected by sections whose name begins with "vrops-"

```
[server|licf-prod1]
hostname=vrops-errors.licf.vmware.com
filter= {; vrops-.*; level == "error" || level == "warning"}

;Collecting syslog messages.
[filelog|syslog]
directory=/var/log
include=messages

;various vRops logs. Note that all section names begin with "vrops-" prefix, which is used in third
 destination filter.
[filelog|vrops-ANALYTICS-analytics]
directory=/data/vcops/log
include=analytics*.log*
exclude=analytics*-gc.log*
parser=auto
[filelog|vrops-COLLECTOR-collector]
directory=/data/vcops/log
include=collector.log*
event_marker=^\d
{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}
parser=auto

[filelog|vrops-COLLECTOR-collector_wrapper]
directory=/data/vcops/log
include=collector-wrapper.log*
event_marker=^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\.\d{3}
parser=auto
```

You can configure additional SSL options for the VMware Aria Operations for Logs Linux agent. See Configure SSL
Connection Between the Server and the VMware Aria Operations for Logs Agents.

Using Common Values for Agent Configuration

You can override the default values of the agent configuration file with common parameter values that apply for each
agent configuration section for Windows or Linux agents.

<u>**Common Options**</u>

Options specified in the `[common|global]` section of the `liagent.ini` configuration file are propagated to all
sections, options specified in the `[common|filelog]` section are propagated to all and only filelog sections, and
`[common|winlog]` options are propagated to all and only winlog sections.

You can define the following parameters in common sections: `tags, include, exclude, event_marker,`
`charset, exclude_fields` , and `parser` as shown in the following example. The example is for a Windows agent:

```
[common|global]


tags = {"log_source_vm":"win-2008r2-64"}
exclude_fields = test_tag;some_other_tag
parser = auto

[common|filelog]
tags = {"collector_type":"filelog"}
exclude = *.trc

[filelog|channel_1]
directory = C:\app\log
include = *.log


...
```

This example specifies the following behavior:

- All logs from filelog sections have both `log_source_vm` and `collector_type` tags with their corresponding values.
- `test_tag` and `some_other_tag` tags are excluded from all logs sent.
- `auto` parser is applied to all collected logs.
- By default, all filelog collectors exclude *.trc files from monitoring.

Options in `[common|global]` are also applied to all winlog sections.

<u>**Merge and Override Criteria**</u>

If options are defined in more than one section, their values are merged or overridden and the section with a smaller
scope has a higher priority when merging/overriding. That is, a value from `[common|global]` is merged with or
overridden by a value from `[common|filelog]`] which in turn is combined with or overridden by a value from
`[filelog|sample_section]` .

Merge and override behavior conform to the following rules:

- Options whose values represent a list of values (tags, include, exclude and exclude_fields) are merged with values of
  that option from a section with a higher priority. And in case of tags, values of tags from sections with a higher priority
  override the value of that same tag from a section with a lower priority, as described previously.
- The value of options that can have single value (event_marker, charset and parser) are overridden by values of that
  option from sections with higher priority.

This means that the value of charset=UTF-8 from [filelog|sample_section] overrides the global value of charset= UTF-16LE from [common|global].

So, for example, if you have `tags={"app":"global-test"}` in [common|filelog] and `tags={"app":"local-test","section":"flg_test_section"}` in `[filelog|flg_test_section]`, the value of the "app" tag from the `[filelog|flg_test_section]` section overrides the value from `[common|filelog]`. All logs collected through this filelog section will have an additional "app" tag with "local-test" value and "section" tag with "flg_test_section" value. For winlog sections, the chain of priority is the same, with any `[winlog|...]` section having the highest priority and `[common|global]` having the lowest priority.

When invalid values are specified in common sections, generally they are skipped and not merged with values from prior and corresponding filelog/winlog sections. In the case of invalid values in tags or `exclude_fields` options, the agent extracts as much valid data as possible and skips the rest of the file once invalid data is encountered. All anomalies are reported in the agent log file. Consult the log file if unexpected behavior is encountered and fix all errors reported by the agent.

If the agent detects an invalid value for an option in a filelog or winlog section, then it does not merge option values from that section with option values from common sections and does not enable that section. All errors are reported in an agent log file. Consult the log file if unexpected behavior is encountered and fix all reported errors by agent.

Related Links

Configure the VMware Aria Operations for Logs Windows Agent on page 73
You can configure the VMware Aria Operations for Logs Windows Agent after you install it. Edit the `liagent.ini` file to configureVMware Aria Operations for Logs Windows Agent to send logs to a VMware Aria Operations for Logs, set the communication protocol and port, add Windows event channels, and configure flat file log collection. The file is located in the `%ProgramData%\VMware\Log Insight Agent` directory.

Configure the VMware Aria Operations for Logs Linux Agent on page 84
You can configure the VMware Aria Operations for Logs Linux Agent after you install it.

Filtering Log Events from VMware Aria Operations for Logs Agents on page 93
You can provide the information that an agent sends to a destination with the filter option in the `[server|<dest_id>]` section of your local `liagent.ini` file.

Centralized Configuration of VMware Aria Operations for Logs Agents on page 94
You can configure multiple VMware Aria Operations for Logs agents.

Forwarding Logs from a VMware Aria Operations for Logs Agent on page 97
You can forward logs collected by an agent to up to three destinations. A destination can include VMware Aria Operations for Logs servers or forwarder, or third-party log management solutions.

Parsing Logs on page 105
Agent-side log parsers extract structured data from raw logs before delivering to the VMware Aria Operations for Logs server. Using log parsers, VMware Aria Operations for Logs can analyze logs, extract information from them, and show those results on the server. Log parsers can be configured for both Windows and Linux VMware Aria Operations for Logs Agents.

Parsing Logs

Agent-side log parsers extract structured data from raw logs before delivering to the VMware Aria Operations for Logs server. Using log parsers, VMware Aria Operations for Logs can analyze logs, extract information from them, and show those results on the server. Log parsers can be configured for both Windows and Linux VMware Aria Operations for Logs Agents.

If the syslog protocol is used, fields extracted by parsers are part of STRUCTURED-DATA according to RFC5424.

Related Links

You can configure the VMware Aria Operations for Logs Windows Agent after you install it. Edit the `liagent.ini` file to configureVMware Aria Operations for Logs Windows Agent to send logs to a VMware Aria Operations for Logs, set the communication protocol and port, add Windows event channels, and configure flat file log collection. The file is located in the `%ProgramData%\VMware\Log Insight Agent` directory.

You can configure the VMware Aria Operations for Logs Linux Agent after you install it.

You can provide the information that an agent sends to a destination with the filter option in the `[server|<dest_id>]` section of your local `liagent.ini` file.

You can configure multiple VMware Aria Operations for Logs agents.

You can forward logs collected by an agent to up to three destinations. A destination can include VMware Aria Operations for Logs servers or forwarder, or third-party log management solutions.

You can override the default values of the agent configuration file with common parameter values that apply for each agent configuration section for Windows or Linux agents.

Configure Log Parsers

You can configure parsers for both `FileLog` and `WinLog` collectors.

For the VMware Aria Operations for Logs Linux Agent:

- Log in as root or use `sudo` to run console commands.
- Log in to the Linux machine on which you installed the VMware Aria Operations for Logs Linux Agent, open a console and run `pgrep liagent` to verify that the Linux Agent is installed and running.

For the VMware Aria Operations for Logs Windows Agent:

- Log in to the Windows machine on which you installed the VMware Aria Operations for Logs Windows Agent and start the Services manager to verify that the VMware Aria Operations for Logst service is installed.

1. Navigate to the folder containing the `liagent.ini` file.

Operating System	Path
Linux	/var/lib/loginsight-agent/
Windows	%ProgramData%\VMware\Log Insight Agent

2. Open the `liagent.ini` file in any text editor.

3. To configure a specific parser, define a parser section. `[parser|myparser]`

   Where `myparser` is an arbitrary name of the parser which can be referred from log sources. Parser section should refer to any built in (or any other defined) parser and configure that parser's mandatory options and non-required options if needed.

   For example, `base_parser=csv` shows that `myparser` parser is derived from built-in parser `csv`. It expects that input logs consist of two fields which are separated with a semicolon.

   ```
   [parser|myparser]

   base_parser=csv
   ```

```
fields=field_name1,field_name2

delimiter=";"
```

4. After defining `myparser`, refer to it from log sources `winlog` or `filelog`.

    ```
    [filelog|some_csv_logs]

    directory=D:\Logs

    include=*.txt;*.txt.*

    parser=myparser
    ```

    The logs collected from `some_csv_logs` sources, for example from the `D:\Logs` directory, are parsed by `myparser` and extracted events appear on the server as `field_name1` and `field_name2` respectively.

    > **NOTE**
    > The static logs in the `D:\Logs` directory are not get pulled into VMware Aria Operations for Logs by the agent. However, new files that are created in the `D:\Logs` directory are available in VMware Aria Operations for Logs.

5. Save and close the `liagent.ini` file.

Common Options for Parsers

You can configure common options for all parsers that produce named fields.

Reserved Words for Field Names

Field names are restricted. The following names are reserved and cannot be used as field names.

*   `event_type`
*   `hostname`
*   `source`
*   `text`

Common Parser Options

Options in the following table can be used with all supported parsers.

Option	Description
`base_parser`	The name of the base parser that this custom parser extends. It can be a built-in parser name or another customer parser name. This configuration key is mandatory.
`field_decoder`	Nested parsers specified as a JSON strings. Keys are the names of the field to apply the nested parser to and the value is the name of the parser to use for that field. Each nested parser is applied to the appropriate field decoded by the base parser. Field decoders are useful when the value of a field is a complex value, for example, a timestamp. The `field_decoder` option also supports more comlpex JSON objects as arguments that allow you to use conditions for specific field values that are checked before the nested parser is applied. **NOTE** For more information on usage and conditional configurations, see Conditional Configurations for the field_decoder option section below.
`field_rename`	Renames extracted fields. Use a JSON string where keys are the original names of the fields and values are the new desired names of the fields. The `field_decoder` option is always applied before `field_rename`. The order of these options in the INI file is not important. For clarity, specify `field_decoder` first.
`next_parser`	Name of the next parser to run. Allows multiple parsers to run sequentially on the same input. **NOTE** Parsers process all consequent parsers defined by the `next_parser` keyword and may replace a field value already extracted by a previous parser.
`exclude_fields`	A list of semicolon separated field names to remove from the event before it is delivered to the server. Field names are removed before event filtering is performed so that the field that you excluding during parsing cannot be used in the filter condition.
`debug`	Yes or No option that enables debugging of a particular parser. With debugging enabled, the parser performs detailed logging of input it receives, the operation it performed and the result it produced. The option applies per-section, that is, only to the parser defined by the particular section. The default value for debug is `debug=no` for parsers.

Conditional configurations for the `field_decoder` option

For logs with the same common format but signficant differences related to specific field values, logs with `info` and `error`severities for example, you can use the conditional nested parser to reduce the application of unnecessary parsers to the corresponding fields of already parsed logs.

For example, using these logs:

```
2019-03-29T11:00:54.858Z
        host-FQDN Hostd: error hostd[2099230]
        [Originator@6876 sub=Default opID=1983bdbe-c1-800f user=admin.user] AdapterServer
 caught
```

```
        exception: SSLExceptionE(SSL Exception: error:140000DB:SSL routines:SSL
routines:short read:
        The connection was closed by the remote end during handshake.)
```
```
2019-03-29T11:00:55.477Z
        host-FQDN Hostd: info hostd[6D620B70]
        ['commonhost' opID=5759adcc-cf] [transportConnector] -- FINISH task-internal-5726666
--  -- Completed connection restart --
```

You can use the following configuration to parse them:

```
[parser|clf_parser]
base_parser=clf
format=%t %{generator_host}i %i: %{log_severity}i %i[%{thread_id}i]%M
field_decoder={"log_message" : {"log_severity" : {"error" : "error_parser", "info" : "info_parser"}}}
exclude_fields=log_message
```

```
[parser|info_parser]
base_parser=clf
format=[%{common_info}i] [%{process}i] %M
field_rename={"log_message" : "info_log_content"}
```

```
[parser|error_parser]
base_parser=clf
format=[%{common_info}i] %{exception_handler}i %i:%{exception_type}i:%i:%{error_id}i:%i:%i:%i: %M
field_rename={"log_message" : "exception_content"}
```

This configuration produces the following results:

```
timestamp=2019-03-29T11:00:54.858000
generator_host="host-FQDN"
log_severity="error"
thread_id="2099230"
common_info=Originator@6876 sub=Default opID=1983bdbe-c1-800f user=admin.user
exception_handler="AdapterServer"
exception_type="SSLExceptionE(SSL Exception"
error_id="140000DB"
exception_content="The connection was closed by the remote end during handshake.)"
```

Additioanlly the following fields are parsed for the `info` log:

```
timestamp=2019-03-29T11:00:55.477000
generator_host="host-FQDN"
log_severity="info"
thread_id="6D620B70"
log_message="['commonhost' opID=5759adcc-cf] [transportConnector] -- FINISH task-
internal-5726666 --  -- Completed connection restart --"
common_info="'commonhost' opID=5759adcc-cf"
process="transportConnector"
info_log_content="-- FINISH task-internal-5726666 --  -- Completed connection restart --"
```

Comma-Separated Value Log Parsers

You can configure Comma-Separated Value (CSV) parsers for both `FileLog` and `WinLog` collectors.

The available options for the `csv` parser are `fields` and `delimiter` .

Comma-Separated Value Parser Options

Note the following information about the structure of the `csv` parser.

Option	Description

`fields`	The `fields` option specifies the names of the fields that exist in the log. The total number of the listed field names must be equal to the total number of comma-separated fields in the logs.
	The `fields` option is mandatory for the CSV parser. If it is not specified, nothing is parsed. Double quotes surrounding the field value are optional, depending on the field content.
	Field names must be separated by commas, for example
	  `fields = field_name1, field_name2, field_name3, field_name4`
	This definition assumes that the names `field_name1`, `field_name2`, `field_name3` and `field_name4` are assigned sequentially to the extracted fields.
	If some fields must be omitted by the CSV parser, their names can be omitted from the list. For example,
	  `fields = field_name1, , field_name3, field_name4`
	In this case, the parser extracts only the first, third and fourth fields from the event and subsequently assigns the names `field_name1`, `field_name3` and `field_name4` to them.
	If the fields option does not specify a complete list of the fields in your logs, the parser returns an empty list. For example, if the log file contains `field1`, `field2`, `field3`, `field4`, and `field5`, but only `fields=field1,field2,field3` is specified, the parser returns an empty fields list.
	You cannot use `fields=*` for a CSV parser, because the parser returns an empty fields list. A complete list of fields must be specified, unless you need certain fields omitted as already described.

`delimiter`	The `delimiter` option specifies the delimiter for the parser to use. By default, the `csv` parser uses a comma as a delimiter; however, you can change the delimiter to a semicolon, a space, or other special character. The defined delimiter must be enclosed in double quotes. For example, `delimiter=","` and `delimiter=";"`. The `csv` parser supports any set of characters as delimiters that are enclosed in quotes, for example "||" or "asd". The field values' separators in the logs should exactly match the pattern defined by the delimiter parameter, otherwise the parser will fail. Special characters such as a space or a tab can be defined for as a delimiter for the `csv` parser as long as the escape character precedes the special character for (\", \s, \t). For example, `delimiter="\s"` or `delimiter=" "`. The `delimiter` option is optional.

CSV Log Parser Configuration

To parse logs collected from either `winlog` or `filelog` sources, use the following configuration.

```
[filelog|some_csv_logs]
directory=D:\Logs
include=*.txt;*.txt.*
parser=myparser

[parser|myparser]
base_parser = csv
fields = timestamp,field_name1, field_name2, field_name3
delimiter = ";"
field_decoder={"timestamp": "tsp_parser"}
[parser|tsp_parser]
; timestamp is a built-in parser
base_parser=timestamp
; "format" is an option of timestamp parser
format=%Y-%m-%d %H:%M:%S
```

With this configuration, logs collected from `some_csv_logs` source (for example, from the `directory=D:\Logs` directory) are parsed by `myparser`. If the collected logs contain three values that are separated by a semicolon, the parsed events sequentially receive the `field_name1`, `field_name2` and `field_name3` names.

To parse the following CSV log:

```
"United States","USA","North America","High income: OECD","Fiscal year end: September 30; reporting
 period for national accounts data: CY."
```

Define the CSV parser configuration:

```
[parser|csv_log_parser]
base_parser=csv
fields=country_name, country_code, region, income_group, special_notes
```

The CSV parser returns the following fields:

```
country_name=United States
country_code=USA
region=North America
income_group=High income: OECD
special_notes=Fiscal year end: September 30; reporting period for national accounts data: CY.
```

Common Log Format (Apache) Log Parser

You can configure the Common Log Format (CLF) Apache parser for both `FileLog` and `WinLog` collectors.

Common Log Format (Apache) Parser

The default CLF parser defines the following order and names of fields.

```
host ident authuser datetime request statuscode bytes
```

Parser name: `clf`

The CLF parser-specific option is `format` .

format Option

The `format` option specifies the format with which Apache logs are generated. The option is not mandatory.

If no format is specified, the following default common log format is used.

```
%h %l %u %t \"%r\" %s %b
```

The CLF parser format string does not accept regex expressions. For example, specify a space instead of the expression \s+.

To parse other log formats, specify that format in the agent's configuration. Parsed fields appear on the server side with the following names.

> **NOTE**
> In the cases in which a variable is required, if `{VARNAME}` is not provided in the configuration, the fields are ignored.

Fields	Value
`'%a':`	"remote_ip"
`'%A':`	"local_ip"
`'%B', '%b':`	"response_size"
`'%C':`	Depends on the name of variable specified in the format

Fields	Value
`'%c':`	Depends on the name of variable specified in the format
`'%D':`	"request_time_mcs"
`'%E':`	"error_status"
`'%e':`	Depends on the name of variable specified in the format
`'%F', '%f':`	"file_name"
`'%h':`	"remote_host"
`'%H':`	"request_protocol"
`'%i':`	Depends on the name of variable specified in the format
`'%k':`	"keepalive_request_count"
`'%l':`	"remote_log_name"
`'%L'`	"request_log_id"
`'%M':`	"log_message" (parser stops parsing the input log after reaching this specifier)
`'%m':`	"request_method"
`'%n':`	depends on the name of variable specified in the format
`'%o':`	depends on the name of variable specified in the format
`'%p':`	"server_port" Additional formats can be used with this specifier: %{format}p. Supported formats are "canonical", "local", or "remote". When the "canonical" format is used, the field name remains as "server_port". When the "local" format is used, the field name will be "local_server_port", and when the "remote" format is used, the field name will be "remote_server_port".
`'%P':`	"process_id" Additional formats can be used with this specifier: %{format}P. Supported formats are "pid", "tid", and "hextid". If "pid" is used as a format, the field name will be "process_id". While "tid" and "hextid" formats generate fields with the name "thread_id"
`'%q':`	"query_string"
`'%r':`	"request"
`'%R':`	"response_handler"
`'%s':`	"status_code", which generates the final status of the request.

Fields	Value
'%t':	"timestamp", which works as event timestamp on ingestion, and engages the timestamp parser. To override timestamp auto detection, date and time format can be specified in curly braces: %{%Y-%m-%d %H:%M:%S}t, see Timestamp Parser for more details.
	The timestamp format for the CLF parser can start with "begin:" or "end:" prefixes. If the format starts with begin: (default), the time is taken at the beginning of the request processing. If it starts with end: , it is the time when the log entry gets written, close to the end of the request processing. For example, such formats such as the following are supported by CLF parser: %h %l %u [%{begin:%d/%b/%Y %T}t.%{msec_frac}t] \"%r\" %>s %b
	The following format tokens are also supported for the CLF parer's timestamp format specifier:

sec
> number of seconds since the Epoch. This is equivalent to Timestamp parser's %s specifier.

msec
> number of milliseconds since the Epoch

usec
> number of microseconds since the Epoch

msec_frac
> millisecond fraction (is equivalent to Timestamp parser's %f specifier)

musec
> microsecond fraction (is equivalent to Timestamp parser's %f specifier)

To parse logs where timestamp is represented with format tokens, the following formats can be used in the configuration:

```
format=%h %l %u %{sec}t \"%r\" %s %b
format=%h %l %u %{msec}t \"%r\" %s %b
format=%h %l %u %{usec}t \"%r\" %s %b
```

These tokens cannot be combined with each other or Timestamp parser formatting in the same format string. You can use multiple %{format}t tokens instead. For example, to use Timestamp which includes milliseconds, except of using Timestamp parser's %f specifier, the following combined timestamp can be used: %{%d/%b/%Y %T}t.%{msec_frac}t .

Fields	Value
'%T':	"request_time_sec"
'%u':	"remote_auth_user"
'%U':	"requested_url"
'%v':	"server_name"
'%V':	"self_referential_server_name"
'%X':	"connection_status", which depends on the name of variable specified in the format
'%x':	Depends on the name of variable specified in the format
'%I':	"received_bytes"
'%O':	"sent_bytes"
'%S':	"transferred_size"

For example, to parse logs collected from either winlog or filelog sources with the CLF parser, specify the following configuration:

```
[filelog|clflogs]
directory=D:\Logs
include=*.txt
parser=myclf

[parser|myclf]
debug=yes ;Note: use this option only while debugging and set it to 'no' when used in production.
```

```
base_parser=clf
format=%h %l %u %b %t \"%r\" %s
```

Using this configuration, logs that are collected from the `clflogs` source, for example from the `directory=D:\Logs` directory, are parsed by `myclf`. The `myclf` parser only parses those logs that were generated with the format described in the configuration.

The default value for debug is `debug=no` for parsers.

Parsing Logs that were Generated Using CLF

To parse logs that were generated using CLF, you must define the corresponding format in the configuration. For example,

```
format=%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User_Agent}i\"
```

Fields that are not empty that use the specifiers `%{Referer}i` and `%{User_Agent}i` appear on the VMware Aria Operations for Logs server with the names `referer` and `user_agent` respectively.

Integrating the Timestamp Parser with the CLF Parser

You can parse Apache logs with a custom time format.

Access logs that have a custom time format as follows.

```
format = %h %l %u %{%a, %d %b %Y %H:%M:%S}t \"%r\" %>s %b
```

If a custom time is not specified, the CLF parser attempts to deduce the time format automatically by running the automatic timestamp parser, otherwise the custom time format is used.

The supported custom time formats that are supported for error logs are:

Custom Time Format	Description	Configuration Format
`%{u}t`	Current time including micro-seconds	`format=[%{u}t] [%l] [pid %P] [client %a] %M`
`%{cu}t`	Current time in compact ISO 8601 format, including micro-seconds	`format=[%{cu}t] [%l] [pid %P] [client %a] %M`

For a full list of supported timestamp specifiers, see timestamp parser.

Apache Default Access Logs Configuration for Windows

Apache Default Error Logs Configuration for Windows

This example shows how you can format Apache v2.4 access log configurations for Windows.

```
;ACCESS LOG
;127.0.0.1 - - [13/May/2015:14:44:05 +0400] "GET /xampp/navi.php HTTP/1.1" 200 4023 "http://local-
host/xampp/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0"
;format=%h %l %u %{%d/%b/%Y:%H:%M:%S %z}t \"%r\" %>s %b \"%{Referer}i\" \"%{User_agent}i\"

; Section to collect Apache ACCESS logs
[filelog|clflogs-access]
    directory=C:\xampp\apache\logs
    include=acc*
    parser=clfparser_apache_access
    enabled=yes

;Parser to parse Apache ACCESS logs
```

```
[parser|clfparser_apache_access]
    debug=yes
    base_parser=clf
    format=%h %l %u %{%d/%b/%Y:%H:%M:%S %z}t \"%r\" %>s %b \"%{Referer}i\" \"%{User_agent}i\"
```

Define the access log format:

1. Configure Apache for the access log format (httpd.conf):

```
LogFormat "%h %l %u %{%d-%b-%Y:%H:%M:%S}t \"%r\" %a %A %e %k %l %L %m %n %T %v %V %>s %b
\"%{Referer}i\" \"%{User_Agent}i\"" combined
```

2. Define the CLF parser configuration:

```
;ACCESS LOG
;127.0.0.1 unknown - 21-May-2015:13:59:35 "GET /xampp/navi.php HTTP/1.1" 127.0.0.1 127.0.0.1 - 0
 unknown - GET - 1 localhost localhost 200 4023 "http://localhost/xampp/" "-"
[filelog|clflogs-access]
    directory=C:\xampp\apache\logs
    include=acc*;_myAcc*
    parser=clfparser_apache_access
    enabled=yes
; Parser to parse Apache ACCESS logs
[parser|clfparser_apache_access]
    debug=yes
    base_parser=clf
    format=%h %l %u %{%d-%b-%Y:%H:%M:%S}t \"%r\" %a %A %e %k %l %L %m %n %T %v %V %>s %b \"%{Refer-
er}i\" \"%{User_Agent}i\"
```

The CLF parser returns the following:

```
remote_host=127.0.0.1
timestamp=2015-05-13T10:44:05
request=GET /xampp/navi.php HTTP/1.1
status_code=200
response_size=4023
referer=http://localhost/xampp/
user_agent=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0
```

This example shows how you can format Apache v2.4 error log configurations for Windows.

```
;ERROR LOG
;[Wed May 13 14:37:17.042371 2015] [mpm_winnt:notice] [pid 4488:tid 272] AH00354: Child: Starting
 150 worker threads.
;[Wed May 13 14:37:27.042371 2015] [mpm_winnt:notice] [pid 5288] AH00418: Parent: Created child
 process 3480
;format=[%{%a %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P:tid %{thread_id}i] %E: %M
;format=[%{%a %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P] %E: %M

; Section to collect Apache ERROR logs
[filelog|clflogs-error]
    directory=C:\xampp\apache\logs
    include=err*
    parser=clfparser_apache_error
    enabled=yes

;Parser to parse Apache ERROR logs
[parser|clfparser_apache_error]
    debug=yes
```

```
    base_parser=clf
    format=[%{%a %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P:tid %{thread_id}i] %E: %M
    next_parser=clfparser_apache_error2
```

```
;Parser to parse Apache ERROR logs
[parser|clfparser_apache_error2]
    debug=yes
    base_parser=clf
    format=[%{%a %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P] %E: %M
```

> **NOTE**
> The provided names correspond to the combined log format. Apache error logs are also
> described using the above formatting keys, not the Apache error log format.

Define the error log format:

1. Configure Apache for the error log format (httpd.conf):

   ```
   LogFormat "%h %l %u %{%d-%b-%Y:%H:%M:%S}t \"%r\" %a %A %e %k %l %L %m %n %T %v
   %V %>s %b \"%{Referer}i\" \"%{User_Agent}i\"" combined
   ```

2. Define the CLF parser configuration:

   ```
   ;Parser to parse Apache ERROR logs
   [parser|clfparser_apache_error]
       debug=yes
       base_parser=clf
       format=[%{%a %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P] %E: %M
       next_parser=clfparser_apache_error2
   ```

   ```
   ;Parser to parse Apache ERROR logs
   [parser|clfparser_apache_error2]
       debug=yes
       base_parser=clf
       format=[%{%a %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P:tid
    %{thread_id}i] %E: %M
   ```

Log entry:

```
[Wed May 13 14:37:17.042371 2015] [mpm_winnt:notice] [pid 4488:tid 272] AH00354:
 Child: Starting 150 worker threads.
```

The CLF parser returns the following fields for the log entry (If using a parser in a +0400
timezone):

```
timestamp=2015-05-13T10:37:17.042371
request_method=mpm_winnt
severity=notice
process_id=4488
thread_id=272
error_status=AH00354
log_message=Child: Starting 150 worker threads.
```

Log entry:

```
[Wed May 13 14:37:27.042371 2015] [mpm_winnt:notice] [pid 5288] AH00418: Parent:
 Created child process 3480
```

The CLF parser returns the following fields for the log entry (If using a parser in a +0400
timezone):

```
timestamp=2015-05-13T10:37:27.042371
request_method=mpm_winnt
severity=notice
process_id=5288
error_status=AH00418
log_message=Parent: Created child process 3480
```

Key/Value Pair Parser

You can configure the Key/Value Pair (KVP) parser for both `FileLog` and `WinLog` collectors.

Key/Value Pair (KVP) Parser

The `kvp` parser finds and extracts all `key=value` matches from an arbitrary log message text. The following example shows the `kvp` parser format.

```
[parser|kvp_parser]
base_parser=kvp
fields=*
```

For example, the key-value log can be in the following format: `scope=local; abstract=false; lazyInit=false; autowireMode=0; dependencyCheck=0;`

With the `kvp` parser, you must specify the fields from which the values are to be extracted. For example, if the definition `fields=name,lastname,country` exists in the configuration, only the values with the specified keys are parsed and sent to the server.

Both the key and the value can be optionally surrounded by double quotes " " to define white space or other special characters.

When double quotes are used for the key or value, the backslash character " \ " can be used as the escape character. Any character following the backslash character is defined literally, including a double quote character or a backslash character. For example: " \\ "

Note the following considerations.

- If the key in a key/value pair is not followed by an equals sign and a `VALUE` is not provided, the option is skipped, as with free text.
- The key cannot be empty, the value can be empty.
- An equals sign that is not followed by a value is treated as free text and is skipped.
- A value can be a string of characters that are surrounded by double quote characters, or it can be empty. Use a backslash for escaping special characters that are part of the value.

KVP Parser Options

Note the following information about the structure of the `kvp` parser.

Option	Description
`fields`	The information that you want to extract described as units of data. For example, `fields=name,lastname,country`. If specific field names are defined by the `fields` option, then each invalid char in a field name extracted from a log is replaced with an underscore. For example, if the `fields` option looks for fields "x-A" and "a*(X+Y)", then the parser extracts these fields from logs and renames them to "x_a" and "a__x_y" fields respectively. This makes it possible to extract fields with any chars in the name. If the `fields` option is specified as "*", which means the `kvp` parser recognizes field/value pairs automatically, then the parser looks for fields that have only "alphanumeric+underscore" chars (supported by LI server). All other invalid chars are dropped instead of being converted to underscores. This prevents the parser from extracting unnecessary information into static fields.
`delimiter`	Optional. Default delimiters are the space character, tab, newline characters, comma, and semicolon characters. If delimiters are not specified in the configuration, the `kvp` parser uses default delimiters for parsing. To change the default delimiters to specific delimiters, you must define them between double quotes. For example: `delimiter = "#^|"` . This definition means that each of the characters that are enclosed in the double quotes is used as a delimiter. For the `kvp` parser, any character can be considered as delimiter. You can include the default delimiters with other delimiters in the definition. For example, the `delimiter = "#^|\t\r\n\s"` statement includes the tab, newline characters, and the space as delimiters. If these characters are used, they must be preceded by the escape character. For example, to define the space character as a delimiter, enter the escape character " \" before the space character when defining it as a delimiter, for example, `delimiter ="\s"` .
`field_decoder`	Nested parsers are specified as a JSON string in which the keys are the names of the field to apply to the nested parser, and the value is the name of the parser to use for that field. Each nested parser is applied to the appropriate field, as decoded by the base parser. Field decoders are useful when the value of a key-value pair is a complex value such as a timestamp or a comma-separated list.
`debug =`	Optional. The `debug =` value can be `yes` or `no` . The default value for debug is `debug=no` for parsers. When the option is set to `yes` , you can view detailed logs of the parser ingestion in `liagent_<date>.log`.

Additional Keys Value Options

Key	Definition
`KVP_MESSAGE = *(MESSAGE_ENTRY [WSPR])`	A list of message entries separated by optional white space
`MESSAGE_ENTRY = KVP / FREE_TEXT`	An entry is a key/value pair or just a free text
`KVP = KEY ["=" VALUE]`	Key/value pair. If KEY is not followed by an equal sign and VALUE, it is skipped like free text.
`KEY = BARE_KEY / QUOTED_KEY`	
`FREE_TEXT = "="`	A free standing equal sign is considered a free text and is skipped.

Key	Definition
`BARE_KEY = *1BARE_KEY_CHAR`	At least one character
`BARE_KEY_CHAR = %0x00-08 / %0x10-19 / %0x21-3C / %3E-%FF`	Any character excluding equal sign, space, or TAB
`QUOTED_KEY = 0x22 *1(QUOTED_STRING_CHAR / "\" CHAR) 0x22`	At least one character surrounded by double quote characters. The backslash is used as an escape character.
`QUOTED_STRING_CHAR = %0x00-21 / %0x23-FF`	Any character excluding double quote
`VALUE = BARE_VALUE / QUOTED_VALUE`	
`BARE_VALUE = *BARE_VALUE_CHAR`	Zero or more characters
`BARE_VALUE_CHAR = %0x00-08 / %0x10-19 / %0x21-FF`	Any character excluding space or TAB
`QUOTED_VALUE = 0x22 *(QUOTED_STRING_CHAR / "\" CHAR) 0x22`	A string of characters surrounded by double quote characters. This can be empty. The backslash is used as an escape character.

KVP Parser Configuration Examples

You can use `fields=*` to parse all fields, if necessary.

```
[parser|simple_kvp]
base_parser =kvp
fields=*
```

This example shows how to specify the field decoder.

```
[parser|mykvp]
debug=no
base_parser=kvp
delimiter="#^|"
fields=*
;OR fields=scope,abstract,lazyInit,autowireMode,dependencyCheck
field_decoder={"field1":"field1_parser1"}

[parser|field1_parser1]
base_parser=clf
format=[%{value1}i]]
field_decoder={"value1":"field_parser2"}
```

To parse the following KVP log:

```
Configuring transport... proto = cfapi server_hostname = LOCALHOST ssl = no port = 9000 reconnect = 30
```

Define the KVP parser configuration:
```
[parser|kvp_log_parser]
base_parser=kvp
fields=*
```
The KVP parser returns the following fields:

```
proto=cfapi
server_hostname=LOCALHOST
ssl=no
port=9000
reconnect=30
```

NOTE

In input logs, when an assignment operator (=) is preceded by a randomly generated key, it is a best practice not to use the KVP parser with the * option, because it generates many random fields, which might lead to UI and query performance issues. Instead, you can use the parser by specifying the fields that need to be parsed.

Simple and Complex KVP Parser Examples

Simple KVP Parser Example

```
[filelog|MyLog]
directory=C:\<folder_name>\Parser_logs
include=*.log
parser=my_KVP_parser

[parser|my_KVP_parser]
base_parser=kvp
fields=*
```

Complex KVP Parser Example

```
[filelog|MyLog]
directory=C:\<folder_name>\Parser_logs
include=*.log
parser=my_KVP_parser

[parser|my_KVP_parser]
base_parser=kvp
fields=*
field_decoder={"field1":" field1_parser1"}

[parser| field1_parser1]
base_parser=clf
format=[%{value1}i]]
field_decoder={"value1":" field1_parser2"}
```

Timestamp Parser

The `timestamp` parser does not produce fields but instead transforms its input from a string to an internal timestamp format displayed in milliseconds from the UNIX epoch start, January 1, 1970 (midnight UTC/GMT).

The only supported configuration option is `format` . For example, `format=%Y-%m-%d %H:%M:%S` .

Unlike the CLF parser, the `timestamp` parser can parse time when there are no delimiters between time specifiers, for example `%A%B%d%H%M%S%Y%z` .

Format specifiers that are used by the `timestamp` parser are:

```
'%a':    Abbreviated weekday name, for example: Thu
'%A':    Full weekday name, for example: Thursday
'%b':    Abbreviated month name, for example: Aug
'%B':    Full month name, for example: August
'%d':    Day of the month, for example: 23. strftime() expects zero-padded (01-31) digits
```

```
             for this specifier but Log Insight agents can parse space-padded and non-padded
             day numbers, too.
 '%e':      Day of the month, for example: 13. strftime() expects space-padded ( 1-31) digits
             for this specifier but Log Insight agents can parse zero-padded and non-padded
             day numbers too.
 '%f':      Fractional seconds of time, for example: .036 'f' specifier assumes that '.' or ','
             character should exist before fractional seconds and there is no need to mention
             that character in the format. If none of these characters precedes fractional seconds,
             timestamp wouldn't be parsed.
 '%H':      Hour in 24h format (00-23), for example: 14. Zero-padded, space-padded, and non-padded hours
             are supported.
 '%I':      Hour in 12h format (01-12), for example: 02. Zero-padded, space-padded and non-padded hours
             are supported.
 '%m':      Month as a decimal number (01-12), for example: 08. Zero-padded, space-padded
             and non-padded month numbers are supported.
 '%M':      Minute (00-59), for example: 55
 '%p':      AM or PM designation, for example: PM
 '%S':      Second (00-61), for example: 02
 '%s':      Total number of seconds from the UNIX epoch start, for example 1457940799
             (represents '2016-03-14T07:33:19' timestamp)
 '%Y':      Year, for example: 2001
 '%z':      ISO 8601 offset from UTC in timezone (1 minute=1, 1 hour=100)., for example: +100
```

Additional specifiers are accepted by the timestamp parser, but their values are ignored and do not affect the parsed time.

```
 '%C':      Year divided by 100 and truncated to integer (00-99), for example: 20
 '%g':      Week-based year, last two digits (00-99), for example, 01
 '%G':      Week-based year, for example, 2001
 '%j':      Day of the year (001-366), for example: 235
 '%u':      ISO 8601 weekday as number with Monday as 1 (1-7), for example: 4
 '%U':      Week number with the first Sunday as the first day of week one (00-53), for example: 33
 '%V':      ISO 8601 week number (00-53), for example: 34
 '%w':      Weekday as a decimal number with Sunday as 0 (0-6), for example: 4
 '%W':      Week number with the first Monday as the first day of week one (00-53), for example: 34
 '%y':      Year, last two digits (00-99), for example: 01
```

If a `format` parameter is not defined, the `Timestamp` parser parses the timestamps using the default formats.

Automatic Timestamp Parser

The automatic timestamp parser is called when no format is defined for the timestamp parser or the parser can be called directly without a timestamp parser definition by using `timestamp` in the `field_decoder`. For example:

```
[parser|mycsv]
base_parser=csv
debug=yes
fields=timestamp,action,source_id,dest
field_decoder={"timestamp": "timestamp"}
```

A Timestamp Parser with the Default Configuration

This example shows a `timestamp` parser with a default configuration.

```
[parser|tsp_parser]
base_parser=timestamp
debug=no
format=%Y-%m-%d %H:%M:%S%f
```

To integrate a `timestamp` parser with other parsers, for example the CSV parser, specify the following configuration.

```
[parser|mycsv]
base_parser=csv
fields=timestamp,action,source_id,dest
field_decoder={"timestamp": "tsp_parser"}
```

When this configuration is defined, `mycsv` parser extracts the fields with the names that are specified in the configuration, and runs `tsp_parser` on the content of the `timestamp` field. If `tsp_parser` retrieves a valid timestamp, the server uses that timestamp for the log message.

Automatic Log Parser

The automatic parser automatically detects the timestamp within the first 200 characters of a line. The format of auto-detected time stamps are the same as for the `timestamp` parser.

The automatic parser does not have any options. In addition to the automatic detection of the timestamp, the Key/Value parser runs on the log entry and automatically detects any existing key/value pairs in the logs and extracts the fields accordingly. For example,

```
[filelog|some_logs]
directory=/var/log
include=*
parser=auto
```

As with other parsers, you can define a separate action for the automatic parser.

```
[filelog|kvplogs]
directory=C:\temp_logs\csv-itbm
include=*.txt
parser=myauto
[parser|myauto]

base_parser=auto
debug=yes
```

If you have `debug` enabled for the automatic parser, additional information about parsing is printed. For example, information about on which log the automatic parser was run, and which fields ere extracted from the log.

The default value for debug is `debug=no` for parsers.

> **NOTE**
> In input logs, when an assignment operator (=) is preceded by a randomly generated key, it is a best practice not to use the automatic parser, because it generates many random fields, which might lead to UI and query performance issues. Instead, you can use the KVP parser by specifying the fields that need to be parsed.

Syslog Parser

The syslog parser supports the message_decoder and extract_sd options and automatically detects two formats: RFC-6587, RFC-5424, and RFC-3164.

Configuring the message_decoder Option

All common options and the `message_decoder` option are available for the syslog parser. By default, only the `timestamp` and `appname` fields are extracted. Enable the message_decoder option by setting configuration values in your liagent.ini file to be similar to the following example:

```
[filelog|data_logs]
directory=D:\Logs
include=*.txt
parser=mysyslog


[parser|mysyslog]
base_parser=syslog
message_decoder=syslog_message_decoder
debug=yes


[parser|syslog_message_decoder]
base_parser=kvp
fields=*
```

Parsing with the message_decoder Option

The following example shows a sample event and the fields that are added to the event by a syslog parser configured to use the message_decoder option:

- Sample event:
  ```
  2015-09-09 13:38:31.619407 +0400 smith01 john: Fri Dec 5 08:58:26 2014 [pid 26123] [jsmith.net]
   status_code=FAIL oper_
  ation=LOGIN: Client "176.31.17.46"
  ```
- Returned by a syslog parser to which the message_decoder option is applied to run a KVP parser:
  ```
  timestamp=2015-09-09T09:38:31.619407 appname=john status_code=FAIL operation=LOGIN:
  ```

Configuring the extract_sd Option for Parsing Structured Data

To parse structured data, enable the extract_sd option by setting configuration values in your `liagent.ini` file to be similar to the following example:

```
[filelog|simple_logs]
directory=/var/log
include=*.txt
parser=syslog_parser


[parser|syslog_parser]
base_parser=syslog
extract_sd=yes
```

Parsing with the extract_sd Option

The following example shows a sample event and the fields that are added to the event by a syslog parser configured to use the extract_sd option:

- The sample event: `<165>1 2017-01-24T09:17:15.719Z localhost evntslog - ID47 [exampleSDID@32473 iut="3" eventSource="Application" eventID="1011"] [examplePriority@32473 class="high"] Found entity IPSet, display name dummy ip set 1411`
- The following fields are added to the event by the syslog parser:
  ```
  timestamp=2017-01-24T09:17:15.719000
  pri_facility=20
  pri_severity=5
  procid="-"
  msgid="ID47"
  iut="3"
  ```

```
eventsource="Application"
eventid="1011"
class="high"
appname="evntslog"
```

Fields Extracted By the Parser

The parser automatically extracts the following fields from an event:

RFC Classification	pri_facility	pri_severity	timestamp	appname	procid	msgid
Non-RFC			X	X		
RFC-3164	X	X	X	X		
RFC-5424	X	X	X	X	X	X

Syslog Parser Options

The following table describes available syslog options.

Option	Description
message_decoder	Defines an additional parser, which is used to parse the message body of an event. It can be a built-in parser, such as 'auto' or any custom-defined parser.
extract_sd	Parses structured data. Only yes or no values are supported for the extract_sd option. The option is deactivated by default. When the extract_sd option is enabled, it simply extracts all key-value pairs from the structured data.

Parsing for the RFC-5424 Standard

The following examples show two events parsed by a syslog instance configured shows the configuration used for the collector, a sample event, and the fields that the syslog parser adds to the event.

- Configuration:
  ```
  [filelog|simple_logs]
  directory=/var/log
  include=*.txt
  parser=syslog
  ```

- An event generated in the monitored file:
  ```
  <165>1 2017-01-24T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
  [junos@2636.1.1.1.2.18 username=\"regress\"] User 'regress' exiting
  configuration mode - Juniper format
  ```

- Fields that are added to the event by the syslog parser:
  ```
  The following fields will be added to the event by Syslog parser:
  timestamp=2017-01-24T09:17:15.719000
  pri_facility = 20
  pri_severity = 5
  procid = 3046
  msgid = UI_DBASE_LOGOUT_EVENT
  appname = mgd
  ```

Parsing for the RFC-3164 Standard

The following example shows the configuration used for the collector, a sample RFC-3164 event, and the fields that syslog adds to the event.

- Configuration:
  ```
  [filelog|simple_logs]
  directory=/var/log
  include=*.txt
  parser=syslog
  ```

- An RFC-3164 event generated in the monitored file:
  ```
  <13>2017-01-24T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT User 'regress' exiting con-
  figuration mode - Juniper format
  ```

- Fields that are added to the event by the syslog parser:

  ```
  timestamp=2017-01-24T09:17:15.719000
  pri_facility=1
  pri_severity=5
  appname="mgd"
  ```

Labeled Tab-separated Values Parser

The Labeled Tab-separated Values (LTSV) format is a variant of Tab-separated Values (TSV).

Each record in a LTSV file is represented as a single line. Each field is separated by <TAB> and has a label and a value. The label and the value are separated by : . With the LTSV format, you can parse each line by splitting the line with <TAB> (the same as the TSV format) and extend any fields with unique labels in no particular order. For more information about the LTSV definition and format, see http://ltsv.org/.

LTSV Parser Configuration

Sample LTSV Log

The LTSV parser does not require specific configuration options. To use the LTSV parser, specify the built-in ltsv parser name in the configuration.
```
[parser|myltsv]
base_parser=ltsv
```
An LTSV file must be a byte sequence that matches the LTSV production in the ABNF format.
```
ltsv = *(record NL) [record]
record = [field *(TAB field)]
field = label ":" field-value
label = 1*lbyte
field-value = *fbyte

TAB = %x09
NL = [%x0D] %x0A
lbyte = %x30-39 / %x41-5A / %x61-7A / "_" / "." / "-" ;; [0-9A-Za-z_.-]
fbyte = %x01-08 / %x0B / %x0C / %x0E-FF

host:127.0.0.1<TAB>ident:-<TAB>user:frank<TAB>time:[10/Oct/2000:13:55:36 -0700]<TAB>req:GET /
apache_pb.gif HTTP/1.0<TAB>status:200<TAB>size:2326<TAB>referer:http://www.example.com/start.htm-
l<TAB>ua:Mozilla/4.08 [en] (Win98; I ;Nav)
```
With the sample LTSV configuration, the log's parsing should return the following fields:
```
host=127.0.0.1
ident=-
```

```
user=frank
time=[10/Oct/2000:13:55:36 -0700]
req=GET /apache_pb.gif HTTP/1.0
status=200
size=2326
referer=http://www.example.com/start.html
ua=Mozilla/4.08 [en] (Win98; I ;Nav)
```

Debug Configuration

Additional debugging is also available for the LTSV parser. By default, LTSV debugging is deactivated. To turn on LTSV debugging, enter `debug=yes` .

```
[parser|myltsv]
base_parser=ltsv
debug=yes
```

When debugging is turned on, the LTSV parser extracts values of all valid labels from the log. The LTSV parser requires that label names consist only of alpha-numeric characters, the underscore ('_"), dot ('.') and dash ('-') characters. If at least one invalid label name exists in the log, its parsing will fail. Even if the label name is valid, the agent will check the field name. If invalid names exist, the label name should be corrected to a valid field name.

Configuring the LTSV Parser from the `filelog` Section

You can also configure the LTSV parser from the `filelog` section directly.

```
[filelog|simple_logs]
directory=/var/log
include=*
parser=ltsv
```

Regex Parser

The `regex` parser enables the use of some regular expressions for collected data.

agents use the C++ Boost library regex, which is in Perl syntax. The `regex` parser can be defined by specifying a regular expression pattern that contains named capture groups. For example: `(?<field_1>\d{4})[-](?<field_2>\d{4}) [-](?<field_3>\d{4})[-](?<field_4>\d{4})`

The names specified in the groups (for example: `field_1`, `field_2`, `field_3`, and `field_4`) become names of the corresponding extracted fields. Names have the following requirements:

- Names specified in the regular expression pattern must be valid field names for .
- The names can contain only alphanumeric characters and the underscore " _ " character.
- The name cannot start with a digital character.

If invalid names are provided, configuration fails.

Regex Parser Options

The only required option for the `regex` parser is the `format` option.

The `debug` option can be used when additional debugging information is needed.

Configuration

To create a `regex` parser, use `regex` as a `base_parser` and provide the `format` option.

Regex Configuration Examples

Parsing Apache Logs Example

The following example can be used to analyze `1234-5678-9123-4567`:

```
[parser|regex_parser]
base_parser=regex
format=(?<tag1>\d{4})[-](?<tag2>\d{4})[-](?<tag3>\d{4})[-](?<tag4>\d{4})
[filelog|some_info]
directory=D:\Logs
include=*.txt
parser=regex_parser
```

The results show:

```
tag1=1234
tag2=5678
tag3=9123
tag4=4567
```

To parse Apache logs with the `regex` parser, provide the specific `regex` format for Apache logs:

```
[parser|regex_parser]
base_parser=regex
format=(?<remote_host>.*) (?<remote_log_name>.*) (?<remote_auth_user>.*) \[(?<log_timestamp>.*)\]
 "(?<request>.*)" (?<status_code>.*) (?<response_size>.*)
```

The results show:

```
127.0.0.1 - admin [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
remote_host=127.0.0.1
remote_log_name=-
remote_auth_user=admin
log_timestamp=10/Oct/2000:13:55:36 -0700
request=GET /apache_pb.gif HTTP/1.0
status_code=200
response_size=2326
```

The following code shows another example of parsing Apache logs.

```
[parser|regex_parser]
base_parser=regex
format=(?<remote_host>.* (?<remote_log_name>.*)) (?<remote_auth_user>.*) \[(?<log_timestamp>.*)\]
 "(?<request>.* (?<resource>.*) (?<protocol>.*))" (?<status_code>.*) (?<response_size>.*)
127.0.0.1 unknown - [17/Nov/2015:15:17:54 +0400] \"GET /index.php HTTP/1.1\" 200 4868
remote_host=127.0.0.1 unknown
remote_log_name=unknown
remote_auth_user=-
log_timestamp=17/Nov/2015:15:17:54 +0400
request=GET /index.php HTTP/1.1
resource=/index.php
protocol=HTTP/1.1
status_code=200
response_size=4868
```

Performance Considerations

The `regex` parser consumes more resources than other parsers, such as the `CLF` parser. If you can parse logs with other parsers, consider using those parsers instead of the `regex` parser to achieve better performance.

If a parser is not provided and you use the `regex` parser, define formats as clear as possible. The following example shows a configuration that provides better performance results. This example specifies fields that have digital values.

```
(?<remote_host>\d+.\d+.\d+.\d+) (?<remote_log_name>.*) (?<remote_auth_user>.*) \[(?<log_timestamp>.*)\] "(?
<request>.*)" (?<status_code>\d+) (?<response_size>\d+)
```

JSON Parser

You can customize the JSON parser configuration to selectively parse the JSON log.

You can configure comma-separate value (CSV) parsers for both `FileLog` and `WinLog` collectors. Only valid JSON logs are parsed with the VMware Aria Operations for Logs JSON parser. Invalid JSON log parsers return empty results.

The default JSON parser configuration extracts all fields from the JSON log by the VMware Aria Operations for Logs agent. When the JSON log represents itself as a complex JSON object, which can contain JSON objects as well, the parser uses an underscore (_) characcter to concatenate names of nested and higher tiered JSON objects. This produces an informative field name for the corresponding elements. If the JSON log also contains an array, the member element names contain the array name followed by the element's index in the array.

The JSON parser also provides a specific option, known as `fields`.

JSON Parser 'fields' Option

You can use the `fields` option to specify which fields are parsed in the configuration. The purpose of this option is to enable selective parsing of the JSON log.

> **NOTE**
> For selective parsing, you must specify the path to the desired JSON element. JSON objects from different tiers must be separated with a dot (.) character.

The following list provides example configurations that enable you to selective parse the JSON log as desired.

- To parse more than one element from the JSON log, the desired elements must be listed as parameters for the `fields` option and separated by commas. See example below:
  ```
  {"operation" : {"timestamp" :
       "2018-11-22T15:28:58.094000", "thread_id" : "0x05673", "initiator" : "connector",
       "log_severity" : "info", "log_message" : "Requested connection to the server."},
       "operation_result" : "success"}
  ```

- To parse only the most inner JSON objects, such as `timestamp`, `log_severity`, and `log_message` see the example below. This example configuration produces the following field results: operation_timestamp ="2018-11-22T15:28:58.094000" and operation_log_severity ="info"
  ```
  [parser|json_parser]
  base_parser=json
  fields=operation.timestamp,operation.log_severity, operation.log_message
  ```

- To parse the entire JSON object, include the path to the object followed by an asterisk (*) character.
  ```
  {"product_name" : "LI Agent",
       "operation" : {"timestamp" : "2018-11-22T15:28:58.094000", "thread_id" :
       "0x05673", "initiator" : "connector", "log_severity" : "info", "log_message" :
       "Requested connection to the server."}, "operation_result" :
     "success"}
  ```

- To parse only the `operation` object, use the following configuration:
  ```
  [parser|json_parser]
  base_parser=json
  fields=operation.*
  ```

- If the JSON log contains an array and you want to parse only specific elements of the array, use the array's element index in the configuration, as seen in this example configuration:

```
    {
        "Records": [{
            "object":{
                "key": "/events/mykey",
                "size": 502,
                "eTag": "091820398091823",
                "sequencer": "1123123"
            }
        },
        {
            "object":{
                "key": "/events/user_key",
                "size": 128,
                "eTag": "09182039000001",
                "sequencer": "1123231"
            }
        },
        {
            "object":{
                "key": "/events/admin_key",
                "size": 1024,
                "eTag": "09182039547241",
                "sequencer": "1123213"
            }
        }
    ]
}
```

- To only parse the `key` and `size` elements from the same log, use the following configuration to produce the following fields:

records0_object_key="/events/mykey"

records0_object_size=502

records2_object_key="/events/admin_key"

records2_object_size=1024

```
[parser|json_parser]
base_parser=json
fields = Records0.object.key Records0.object.size, Records2.object.key, Records2.object.size
```

- To parse the `key` field for all array elements, use the following configuration:

```
[parser|json_parser]
base_parser=json
fields=Records.#.object.key
```

- To parse all fields, use the fields option with an asterisk (*) character. This configuraiton is equivalent to the default JSON parser configuration.

```
[parser|json_parser]
base_parser=json
fields=*
```

Uninstalling VMware Aria Operations for Logs Agents

Should you need to uninstall a VMware Aria Operations for Logs agent, follow the instructions that are appropriate to the agent package that you installed.

Uninstall the VMware Aria Operations for Logs Windows Agent

You can uninstall the VMware Aria Operations for Logs Windows Agent from the Programs and Feature screen of the Windows Control Panel.

Log in to the Windows machine on which you installed the VMware Aria Operations for Logs Windows agent and start the services manager to verify that the VMware Aria Operations for Logs agent service is installed.

1. Go to **Control Panel** > **Programs and Features**.
2. Select the VMware Aria Operations for Logs Windows Agent and click **Uninstall**.

The uninstaller stops the VMware Aria Operations for Logs Windows Agent service and removes its files from the system.

Uninstall the VMware Aria Operations for Logs Linux Agent RPM package

You can uninstall the VMware Aria Operations for Logs Linux Agent RPM package.

*   Log in as **root** or use `sudo` to run console commands.
*   Log in to the Linux machine on which you installed the VMware Aria Operations for Logs Linux Agent, open a terminal console and run `pgrep liagent` to verify that the VMware VMware Aria Operations for Logs Linux Agent is installed and running.

Run the following command replacing *VERSION* and *BUILD_NUMBER* with the version and build number of the installed agent.

```
rpm -e VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER
```

The uninstaller stops the VMware Aria Operations for Logs Linux Agent daemon and removes all its files except its own logs from the system.

Uninstall the VMware Aria Operations for Logs Linux Agent DEB package

You can uninstall the VMware Aria Operations for Logs Linux Agent DEB package.

*   Log in as **root** or use `sudo` to run console commands.
*   Log in to the Linux machine on which you installed the VMware Aria Operations for Logs Linux Agent, open a terminal console and run `pgrep liagent` to verify that the VMware VMware Aria Operations for Logs Linux Agent is installed and running.

Run the following command

```
dpkg -P vmware-log-insight-agent
```

The uninstaller stops the VMware Aria Operations for Logs Linux Agent daemon and removes all its files except its own logs from the system.

Uninstall the VMware Aria Operations for Logs Linux Agent bin Package

You can uninstall the VMware Aria Operations for Logs Linux Agent .bin package with a VMware Aria Operations for Logs script.

*   Log in as **root** or use `sudo` to run console commands.
*   Log in to the Linux machine on which you installed the VMware Aria Operations for Logs Linux Agent, open a terminal console and run `pgrep liagent` to verify that the VMware Aria Operations for Logs Linux Agent is installed and running.

1. At the shell prompt, enter the following command to start the script.

```
loginsight-agent-uninstall
```

2. You can verify that the uninstall completed successfully by checking that the returned error code from the following command is 0.
    echo $?

Manually Uninstall the VMware Aria Operations for Logs Linux Agent bin package

You can manually uninstall the VMware Aria Operations for Logs Linux Agent .bin package if you choose not to use the uninstall script.

*   Log in as **root** or use `sudo` to run console commands.
*   Log in to the Linux machine on which you installed the VMware Aria Operations for Logs Linux Agent, open a terminal console and run `pgrep liagent` to verify that the VMware Aria Operations for Logs Linux Agent is installed and running.

1. Stop the VMware Aria Operations for Logs Linux Agent daemon by running the following command
    `sudo service liagentd stop` or `sudo /sbin/service liagentd stop` for older Linux distributions.

2. Manually remove the VMware Aria Operations for Logs Linux Agent files

    *   `/usr/lib/loginsight-agent` - Daemon binary and license files directory.
    *   `/usr/bin/loginsight-agent-support` - Used to generate the support bundle for the VMware Aria Operations for Logs Linux Agent.
    *   `/var/lib/loginsight-agent` - Configuration files and database storage directory.
    *   `/var/log/loginsight-agent` - Log directory for the VMware Aria Operations for Logs Linux Agent.
    *   `/var/run/liagent/liagent.pid` - VMware Aria Operations for Logs Linux Agent PID file. If it is not deleted automatically, remove the file manually.
    *   `/etc/init.d/liagentd` - Script directory for the VMware Aria Operations for Logs Linux Agent daemon.
    *   `/usr/lib/systemd/system/liagentd.service`

Troubleshooting VMware Aria Operations for Logs Agents

Known troubleshooting information can help you diagnose and correct problems related to the operation of the VMware Aria Operations for Logs agents.

Create a Support Bundle for the VMware Aria Operations for Logs Windows Agent

If the VMware Aria Operations for Logs Windows Agent does not operate as expected because of a problem, you can send a copy of the log and configuration files to VMware Support Services.

1. Log in to the target machine where you installed the VMware Aria Operations for Logs Windows Agent.

2. Click the Windows **Start** button and then click **VMware** > **Log Insight Agent - Collect support Bundle**.

3. Optional: If the shortcut is not available, navigate to the installation directory of the VMware Aria Operations for Logs Windows Agent and double-click `loginsight-agent-support.exe`.

    > **NOTE**
    > The default installation directory is `C:\Program Files (x86)\VMware\Log Insight Agent`

The bundle is generated and saved as a `.zip` file in `My Documents`.

Forward the support bundle to VMware Support Services as requested.

Create a Support Bundle for the VMware Aria Operations for Logs Linux Agent

If the VMware Aria Operations for Logs Linux Agent does not operate as expected because of a problem, you can send a copy of the log and configuration files to VMware Support Services.

1. Log in to the target machine where you installed the VMware Aria Operations for Logs Linux Agent.

2. Run the following command.
   ```
   /usr/lib/loginsight-agent/bin/loginsight-agent-support
   ```

The bundle is generated and saved as a `.zip` file in the current directory.

Forward the support bundle to VMware Support Services as requested.

Define Log Details Level in the VMware Aria Operations for Logs Agents

You can edit the configuration file of the VMware Aria Operations for Logs Agent to change the logging level.

For the VMware Aria Operations for Logs Linux Agent:

- Log in as **root** or use `sudo` to run console commands.
- Log in to the Linux machine on which you installed the VMware Aria Operations for Logs Linux Agent, open a console and run `pgrep liagent` to verify that the VMware Aria Operations for Logs Linux Agent is installed and running.

For the VMware Aria Operations for Logs Windows Agent:

- Log in to the Windows machine on which you installed the VMware Aria Operations for Logs Windows agent and start the services manager to verify that the VMware Aria Operations for Logs agent service is installed.

1. Navigate to the folder containing the `liagent.ini` file.

Operating system	Path
Linux	`/var/lib/loginsight-agent/`
Windows	`%ProgramData%\VMware\Log Insight Agent`

2. Open the `liagent.ini` file in any text editor.

3. Change the log debug level in the `[logging]` section of the `liagent.ini` file.

> **NOTE**
> The higher the debug level, the higher the impact it has on the VMware Aria Operations for Logs Agent. The default and recommended value is 0. Debug level 1 provides more information and is recommended for troubleshooting of most issues. Debug level 2 provides detailed information. Use levels 1 and 2 only when requested by VMware Support.

```
[logging]
; The level of debug messages to enable: 0..2
debug_level=1
```

4. Save and close the `liagent.ini` file.

The log debug level is changed.

Management UI Does Not Show VMware Aria Operations for Logs Agents

Information about the VMware Aria Operations for Logs Agents instances does not appear on the Agents page of the Management UI.

After you install the VMware Aria Operations for Logs Agents you do not see the VMware Aria Operations for Logs Agents in the Agents page of the Management UI.

The most common causes are network connectivity problems or incorrect configuration of the VMware Aria Operations for Logs Agents in the `liagent.ini` file.

- Verify that the Windows or Linux system that the VMware Aria Operations for Logs Agents are installed on has connectivity to the VMware Aria Operations for Logs server.
- Verify that the VMware Aria Operations for Logs Agents use the cfapi protocol.

    When using the syslog protocol the UI does not show VMware Aria Operations for Logs Windows Agents.
- View the contents of the VMware Aria Operations for Logs Agents log files located in the following directories .

    - Windows - `%ProgramData%\VMware\Log Insight Agent\log`
    - Linux - `/var/log/loginsight-agent/`

    Look for log messages that contain the phrases `Config transport error: Couldn't resolve host name` and `Resolver failed. No such host is known.`
- Verify that the `liagent.ini` contains the correct configuration for the target VMware Aria Operations for Logs server. See Set Target Log Insight Server of the Log Insight Windows Agent and Set Target Log Insight Server of the Log Insight Linux Agent.

VMware Aria Operations for Logs Agents Do Not Send Logs

An incorrect configuration can prevent the VMware Aria Operations for Logs agents from forwarding logs to the VMware Aria Operations for Logs server. If a flat file collection channel is not configured correctly, you may see messages such as "Invalid settings were obtained for channel 'CHANNEL_NAME'. Channel 'CHANNEL_NAME' will stay dormant until properly configured."

The VMware Aria Operations for Logs agents instances appears on the **Management** > **Agents** page but no logs appear in the Explore Logs page from the VMware Aria Operations for Logs agents host names. The flat file collection channel is not configured correctly.

Incorrect configuration can prevent the VMware Aria Operations for Logs agents from forwarding logs to the VMware Aria Operations for Logs server.

- Define a valid collection channel. Verify whether or not the flat file collection channel is configured correctly. See Configuring VMware Aria Operations for Logs Agents.
- For the VMware Aria Operations for Logs Windows agent, try the following.

    - If Windows channels are enabled, view the contents of the VMware Aria Operations for Logs Windows agent log files located at `%ProgramData%\VMware\Log Insight Agent\log`. Look for log messages related to channel configuration that contain the phrases `Subscribed to channel CHANNEL_NAME`. Typically-used channels are `Application`, `System`, and `Security`.
    - If a channel is not configured correctly, you might see log messages similar to `Could not subscribe to channel CHANNEL_NAME events. Error Code: 15007. The specified channel could not be found. Check channel configuration.` You might see an error code number other than 15007.
    - If a flat file collection channel is not configured correctly, you might see messages like `Invalid settings were obtained for channel 'CHANNEL_NAME'. Channel 'CHANNEL_NAME' will stay dormant until properly configured`
- For both VMware Aria Operations for Logs Windows agent and VMware Aria Operations for Logs Linux agent, try the following.

    - If no flat file collection channel is configured, you might see messages similar to `Cannot find section 'filelog' in the configuration. The flat file log collector will stay dormant until properly configured`

        The contents of the VMware Aria Operations for Logs agents log files are located in the following directories.

        - Windows - `%ProgramData%\VMware\Log Insight Agent\log`
        - Linux - `/var/log/loginsight-agent/`

Add an Outbound Exception Rule for the VMware Aria Operations for Logs Windows Agent

Define an exception rule for unblocking the VMware Aria Operations for Logs Windows Agent in the Windows firewall.

- Verify that you have a **Super Admin** account or an account with **Super Admin** permissions.

The procedure applies to Windows Server 2008 R2 and later, and to Windows 7 and later.

1. Select **Start** > **Run**.

2. Type `wf.msc` and click **OK**.

3. Right-click **Outbound rules** in the left pane and click **New Rule**.

4. Select **Custom** and follow the wizard to set the following options.

Option	Description
Program	`liwinsvc.exe`
Service	LogInsightAgentService
Protocol and Ports	TCP 9000 for cfapi and 514 for syslog

5. On the Specify the profiles for which this rule applies page, select the appropriate network type.

   - Domain
   - Public
   - Private

     NOTE
     You can select all network types to make sure that the exception rule is active regardless of the network type.

Go to the VMware Aria Operations for Logs Windows Agent log directory `%ProgramData%\VMware\Log Insight Agent\log` and open the latest log file. If recent events contain the messages `Config transport error: Couldn't resolve host name` and `Resolver failed. No such host is known`, restart the VMware Aria Operations for Logs Windows Agent service and the Windows machine.

   NOTE
   The VMware Aria Operations for Logs Windows Agent service can take up to 5 minutes to reconnect to the server.

Allow Outbound Connections from theVMware Aria Operations for Logs Windows Agent in a Windows Firewall

Configure Windows firewall settings to allow outbound connections of the VMware Aria Operations for Logs Windows Agent to the VMware Aria Operations for Logs server.

- Verify that you have a **Super Admin** account or an account with **Super Admin** permissions.

After you install and start the VMware Aria Operations for Logs Windows Agent service, the Windows domain or local firewall may restrict the connectivity to the target VMware Aria Operations for Logs server.

The procedure applies to Windows Server 2008 R2 and later, and to Windows 7 and later.

1. Select **Start** > **Run**.

2. Type `wf.msc` and click **OK**.

3. In the Actions pane click **Properties**.

4. On the **Domain Profile** tab, select **Allow(default)** from the **Outbound connections** drop-down menu.

   If the computer is not connected to a domain, you can select **Private Profile** or **Public Profile**, depending on the network type the computer is connected to.

5. Click **OK**.

Define an unblocking exception rule for the VMware Aria Operations for Logs Windows Agent in the Windows firewall. See .Add an Outbound Exception Rule for the VMware Aria Operations for Logs Windows Agent

Mass Deployment of the VMware Aria Operations for Logs Windows Agent is Not Successful

The mass deployment of the VMware Aria Operations for Logs Windows Agent is not successful on target machines.

After performing a mass deployment on Windows domain machines by using Group Policy Objects, the VMware Aria Operations for Logs Windows Agent fails to install as a local service.

Group policy settings might prevent the VMware Aria Operations for Logs Windows Agent from being installed correctly.

1. Edit the Group Policy Object (GPO) settings and redeploy the VMware Aria Operations for Logs Windows Agent agent.
   a) Right-click the GPO, click **Edit** and navigate to **Computer Configuration** > **Policies** > **Administrative Templates** > **System** > **Logon.**
   b) Enable the **Always wait for the network at computer startup and logon** policy.
   c) Navigate to **Computer Configuration** > **Policies** > **Administrative Templates** > **System** > **Group Policy**.
   d) Enable the **Startup policy processing wait time**, and set **Amount of time to wait (in seconds)** to 120.

2. Run the `gpupdate /force /boot` command on target machines.

VMware Aria Operations for Logs Agents Reject Self-Signed Certificates

The VMware Aria Operations for Logs Agents reject self-signed certificate.

A VMware Aria Operations for Logs agent rejects self-signed certificate and cannot establish a connection with the server.

> **NOTE**
> If you experience connection problems with the agent, you can generate detailed logs to check by changing the debug level for the agent to 1. For more information, see Define Log Details Level in the VMware Aria Operations for Logs Agents.

The messages you see in the agent log have specific causes.

Message	Cause
`Rejecting peer self-signed certificate. Public key doesn't match previously stored certificate's key.`	• This might happen when theVMware Aria Operations for Logs certificate is replaced. • This might happen if the HA-enabled in-cluster environment is configured with different self-signed certificates on VMware Aria Operations for Logs nodes.
`Rejecting peer self-signed certificate. Have a previously received certificate which is signed by trusted CA.`	There is a CA-signed certificate stored on the agent side.

Verify whether your target host name is a trusted VMware Aria Operations for Logs instance, and then manually delete the previous certificate from VMware Aria Operations for Logs Agent `cert` directory.

- For VMware Aria Operations for Logs Windows Agent, go to `C:\ProgramData\VMware\Log Insight Agent \cert`.
- For VMware Aria Operations for Logs Linux Agent, go to `/var/lib/loginsight-agent/cert`.

> **NOTE**
> Some platforms might use nonstandard paths for storing trusted certificates. The VMware Aria Operations for Logs Agents have an option to configure the path to trusted certificates store by setting the `ssl_ca_path=<fullpath>` configuration parameter. Replace `<fullpath>` with the path to the trusted root certificates bundle file. See Configure the SSL Parameters.

VMware Aria Operations for Logs Server Rejects the Connection for Non-Encrypted Traffic

The VMware Aria Operations for Logs Server rejects the connection with the VMware Aria Operations for Logs Agents when you try to send non-encrypted traffic.

When you attempt to use `cfapi` to send non-encrypted traffic, the VMware Aria Operations for Logs Server rejects your connection. One of the following error messages appears in the agent log: `403 Forbidden` or `403 Only SSL connections are allowed`.

VMware Aria Operations for Logs is configured to accept only SSL connections, but the VMware Aria Operations for Logs Agents are configured to use a non-SSL connection.

1. Configure your VMware Aria Operations for Logs Server to accept a non-SSL connection.
   a) Expand the main menu and navigate to **Configuration > SSL**.
   b) Under the API Server SSL header, deselect **Require SSL Connection**.
   c) Click **Save**.

2. Configure the VMware Aria Operations for Logs agent to send data through an SSL `Cfapi` protocol connection.
   a) Navigate to the folder containing the `liagent.ini` file.

Operating system	Path
Linux	`/var/lib/loginsight-agent/`
Windows	`%ProgramData%\VMware\Log Insight Agent`

   b) Open the `liagent.ini` file in any text editor.
   c) Change the value of the `ssl` key in the [server] section of the `liagent.ini` file to yes and the protocol to `cfapi`.
   ```
   proto=cfapi
   ```

```
ssl=yes
```

d) Save and close the `liagent.ini` file.

Developer Resources for VMware Aria Operations for Logs (8.14)

VMware Aria Operations for Logs Developer Resources

VMware Aria Operations for Logs Developer Resources provides information about the VMware Aria Operations for Logs API.

This information is intended for anyone who wants to use the VMware Aria Operations for Logs Ingestion API. You must be familiar with REST concepts and with the JSON serialization format.

The VMware Aria Operations for Logs REST API

The REST API provides programmatic access to VMware Aria Operations for Logs and the data it collects.

You can use the API to insert events into the VMware Aria Operations for Logs datastore, to query for events, to change product configuration and for product authentication with VMware Workspace ONE Access and authorization. You can also use the API to install or upgrade VMware Aria Operations for Logs.

To access the VMware Aria Operations for Logs API reference, go to this page: http://<*Operations_for_Logs_host*>/rest-api.

The documentation for the events query interface is available at the internal site http://<*perations_for_Logs_host*>/internal/rest-api#events_query.

> **NOTE**
> The events query interface is a Tech Preview API. The internal site contains documentation for Tech Preview APIs and features.

Using VMware Aria Operations for Logs (8.14)

Using VMware Aria Operations for Logs

Using VMware Aria Operations for Logs provides information about procedures for filtering and searching log messages, performing analysis and visualizing search results, working with alert queries, and dynamic field extraction from log messages based on customized queries.

This information is intended for anyone assigned the **User** role or a role that has the relevant permissions associated with the user tasks. For more information about roles and their permissions, see *Administering VMware Aria Operations for Logs*.

Overview of VMware Aria Operations for Logs Features

VMware Aria Operations for Logs provides scalable log aggregation and indexing for the vCloud Suite, including all editions of VMware vSphere, with near real-time search and analytics capabilities.

VMware Aria Operations for Logs collects, imports, and analyzes logs to provide answers to problems related to systems, services, and applications, and derive important insights.

High-Performance Ingestion

VMware Aria Operations for Logs can process any type of log-generated or machine-generated data. It supports high throughput rates and low latency and accepts data through syslog and the Ingestion API.

Scalability

VMware Aria Operations for Logs can scale out by using multiple virtual appliance instances, which enables linear scaling of the ingestion throughput, increases query performance, and allows for ingestion high availability. In cluster mode, VMware Aria Operations for Logs provides primary and worker nodes. Both primary and worker nodes are responsible for a subset of data. Primary nodes and query nodes can query all subsets of data and aggregate the results.

Near Real-Time Search

The data ingested by VMware Aria Operations for Logs is available for search within seconds. Also, historical data can be searched from the same interface with the same low latency.

VMware Aria Operations for Logs supports complete keyword queries. Keywords are defined as any alphanumeric, hyphen, or underscore characters. In addition to the complete keyword queries, VMware Aria Operations for Logs supports glob queries (for example, `erro?` or `vm*`) and field-based filtering (for example, hostname does NOT match test*, IP contains "10.64"). Furthermore, log message fields that contain numeric values can be used to define selection filters (for example, CPU>80, 10<threads<100, and so on).

Search results are presented as individual events. Each event comes from a single source, but search results might come from multiple sources. You can use VMware Aria Operations for Logs to correlate the data on one or multiple dimensions (for example, time and request identifiers) providing a coherent view across the stack. This way, root cause analysis becomes much easier.

Windows and Linux Agents

VMware Aria Operations for Logs includes agents that collect events and files on Linux and Windows machines.

Intelligent Grouping

VMware Aria Operations for Logs uses a new machine learning technology. Intelligent Grouping scans incoming unstructured data and groups messages together by problem type to give you the ability to rapidly understand issues that may span your physical, virtual, and hybrid cloud environments.

Aggregation

Fields that are extracted from log data can be used for aggregation. This functionality is similar to the functionality that GROUP-BY queries provide in a relational database or pivot-tables in Microsoft Excel. The difference is that there is no need for extract, transform, and load (ETL) processes and VMware Aria Operations for Logs scales to any size of data.

You can generate aggregate views of the data and identify specific events or errors without accessing multiple systems and applications . For example, while viewing an important system metric such as the number of errors per minute, you can drill down to a specific time-range of events and examine the errors that occurred in the environment.

Runtime Field Extraction

Raw log data is not always easy to understand, and you might need to process some data to identify the fields that are important for searching and aggregation. VMware Aria Operations for Logs provides runtime field extraction to address this problem. You can dynamically extract any field from the data by providing a regular expression. The extracted fields can be used for selection, projection, and aggregation, similar to how the fields that are extracted at the parse time are used.

> **NOTE**
> An extracted field name can contain different characters. However, the field name for an ingested event must begin only with a letter or an underscore character and contain only letters, digits, or the underscore character.

Dashboards

You can create dashboards of useful metrics that you want to monitor closely. Any query can be turned into a dashboard widget and summarized for any range in time. You can choose the performance of your system for the last five minutes, hour, or day. You can view a breakdown of errors by hour and observe the trends in log events.

Security Considerations

IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of VMware Aria Operations for Logs must read the security topics in *Administering VMware Aria Operations for Logs*.

These topics provide concise references to the security features of VMware Aria Operations for Logs. Topics include the product external interfaces, ports, authentication mechanisms, and options for configuration and management of security features.

Overview of the VMware Aria Operations for Logs Web User Interface

When you log in to the VMware Aria Operations for Logs Web user interface, the functionality that you can access depends on the roles assigned to your user account. The permissions associated with the roles determine whether you can view or edit specific information.

For information about roles and their corresponding permissions, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*

The Dashboards Page

The **Dashboards** page contains custom dashboards and content pack dashboards. In the **Dashboards** page, you can view graphs of log events in your environment, or create your custom sets of widgets to access the information that matters most to you.

You can access the **Dashboards** page if your user account is associated with a role that has the **Dashboards** permission. You can view or edit all or some dashboard features, depending on the sub-categories and corresponding access levels selected for the permission.

The Explore Logs Page

In the **Explore Logs** page, you can search and filter log events, and create queries to extract events based on timestamp, text, source, and fields in log events. VMware Aria Operations for Logs presents charts of the query results. You can save these charts to look them up later in the **Dashboards** page.

You can access the **Explore Logs** page if your user account is associated with a role that has the **Explore Logs** permission. You can view or edit all or some features of Explore Logs, depending on the sub-categories and corresponding access levels selected for the permission.

The Log Sources Section

Under the **Log Sources** section, you can find pages with instructions for configuring various log sources such as Fluentd, Docker, Kubernetes, and so on.

You can access the **Log Sources** section if your user account is associated with a role that has the view permission for **Management > Agents**.

The Alerts Section

Under the **Alerts** section, you can search for, view, and manage the alerts in your organization.

You can access the **Alerts** section if your user account is associated with a role that has the **Alerts** permission. With view access, you can search for and view all the alerts in your organization. With edit or full access, you can also manage alerts.

The Content Packs Page

In the **Content Packs** page, you can access content packs, which contain dashboards, extracted fields, saved queries, and alerts that are related to a specific product or set of logs.

You can access the **Content Packs** page if your user account is associated with a role that has the **Content Packs** permission. With view access, you can search for and view all the content packs in your organization. With edit or full access, you can also import or create content packs.

The Integration Section

Under the **Integration** section, you can configure VMware Aria Operations for Logs to connect to VMware products such as vSphere, VMware Aria Operations, NSX Identity Firewall, and VMware Aria Operations for Logs (SaaS).

You can access the **Integration** section if your user account is associated with a role that has the **Integrations** permission. You can view or edit all or some integration configurations, depending on the products and corresponding access levels selected for the permission.

The Log Management Page

In the **Log Management** page, you can configure log filtering, log masking, log forwarding, and cloud forwarding. You can also create index partitions for log retention and archiving.

You can access the **Log Management** page if your user account is associated with a role that has the **Log Management** permission. You can view or edit all or some configurations, depending on the sub-categories and corresponding access levels selected for the permission.

<u>**The VMware Aria Operations for Logs (SaaS) Page**</u>

In the VMware Aria Operations for Logs (SaaS) page, you can subscribe to VMware Aria Operations for Logs (SaaS) to avail log management as a service. You can view the setup instructions to:

- Forward logs from VMware Aria Operations for Logs to VMware Aria Operations for Logs (SaaS).
- Retain your logs for a longer period and retrieve them when required, by archiving them in S3 buckets.
- Ingest logs from multiple log sources that VMware Aria Operations for Logs (SaaS) supports.
- Use KB insights to view common errors and their solutions. KB insights use machine learning to detect anomalies in the ingested logs, and provide recommendations to resolve the issues by using the knowledge base created by the VMware community.

All users can access the VMware Aria Operations for Logs (SaaS) page.

<u>**The Management Section**</u>

Under the **Management** section, you can monitor VMware Aria Operations for Logs, manage clusters, configure hosts, agents, and access control for user accounts, and manage event export tasks, shared dashboard URLs, certificates, and your license.

You can access the **Management** section if your user account is associated with a role that has the **Management** permission. You can view or edit all or some features, depending on the sub-categories and corresponding access levels selected for the permission.

<u>**The Configuration Section**</u>

Under the **Configuration** section, you can update the general and time settings. You can also configure SSL, authentication, and an outgoing SMTP server for email notifications.

You can access the **Configuration** section if your user account is associated with a role that has the **Configuration** permission. You can view or edit all or some features, depending on the sub-categories and corresponding access levels selected for the permission.

Searching and Filtering Log Events

You can search and filter log events in the **Explore Logs** page.

To find only events that contain the specified keywords, enter any complete keywords, globs, or phrases in the search text box and click **Search**.

You can specify the time range on either the **Dashboards** or **Explore Logs** pages in the web user interface. Time ranges are inclusive when filtering.

You can search for log events that match certain values of specific fields. Using quoted text in the main search field matches exact phrases. Entering space in the main search field is a logical AND operator. Search uses only full tokens. For example, searching for "err" does not find "error" as a match.

> **NOTE**
> The field name for an ingested event must begin only with a letter or an underscore character and contain only letters, digits, or the underscore character.

You can enter the field search criteria, or filters, by using the drop-down menus and the text box above the list of log events.

Within a single-row filter, you can use comma-separated values to list OR filters. For example, select **hostnamecontains** and type `127.0.0.1, 127.0.0.2`. The search returns events with the host name 127.0.0.1 or 127.0.0.2.

> **NOTE**
> The **text contains** filter treats each comma-separated value as a complete keyword.

Queries with fields using the internal query language syntax names, for example, `from` or `in`, are not able to be processed and should not be used.

You can combine multiple field filters by creating a filter row for each field. You can toggle the operator that is applied to multiple-row filters .

- To apply the AND operator, select **all**.
- To apply the OR operator, select **any**.

> **NOTE**
> Regardless of the toggle value, the operator for comma-separated values within a single filter row is OR, except when you use the **_index** field. For the **_index** field, the operator is AND.

You can use globs in search terms. For example, `vm*` or `vmw?re`.

- For 0 or more characters, use *.
- For one character, use ?.

> **NOTE**
> Globs cannot be used as the first character of a search term. For example, you can use 192.168.0.*, but you cannot use *.168.0.0 in your filtering queries.

Event Types Grouping

VMware Aria Operations for Logs summarizes a large number of individual events into a smaller number of broad event types. VMware Aria Operations for Logs uses machine learning to group similar events together, with each group showing the approximate number of events in the group. Grouping events helps identify the most communicative events and the most quiet ones, both of which are critical for troubleshooting.

The **Event Types** tab in the Explore Logs page, under the search bar, provides an aggregated view of the events for the given time range of the query. An event in a group is selected as the representative event. You can click the **Expand** link under each representative event to view the events in the group.

As a result of grouping events, an Event Type is assigned to each event. An appropriate *event_type* field is created, which you can further use in regular queries.

VMware Aria Operations for Logs does not document the exact mechanism for grouping events. It tries to automatically detect groups of similar events based on the number of common parts that the events have. For example, let us consider the following events:

- `[2019-05-20 06:41:24.291+0000] ["SearchWorker-thread-12999"/10.113.164.150 INFO] [com.company.product.analytics.distributed.LogSearchWorkerService] [Worker fully completed query (token=5f6e5e1faf93e4ce) in 11 msec]`
- `[2019-05-20 06:41:24.284+0000] ["SearchWorker-thread-11961"/10.113.164.167 INFO] [com.company.product.analytics.distributed.SearchWorkerService] [Worker fully completed query (token=3b247b2ba6057c47) in 24 msec]`

These events have eight common parts - timestamp, thread name, host IP, logging level, class name, message text, token number, and duration.

Now, let us consider the following events:

- `[2019-05-20 06:41:24.291+0000] ["LogSearchWorker-thread-12999"/10.113.164.150 INFO] [com.vmware.loginsight.analytics.distributed.LogSearchWorkerService] [Worker finished search (wait=59500 token=5f6e5e1faf93e4ce) in 12 msec]`
- `[2019-05-20 06:41:20.136+0000] ["AliasStudentStudyPool-thread-1"/192.168.110.24 INFO] [com.vmware.loginsight.analytics.alias.AliasStudent] [looking for alias due to rule DatastoreFromVmFileSystem]`

These events only have three common parts - timestamp, host IP, and logging level.

In addition to grouping events together, VMware Aria Operations for Logs identifies useful fields in each event of the group, known as smart fields. Each smart field appears within the representative event as a hyperlink with a drop-down menu icon next to it. You can click the icon to view a histogram for the values of the field or to define an extracted field based on the smart field.

Related Links

Event types widgets provide access to event type groups, which are created through machine learning to group similar events together.

Information in Log Events

VMware Aria Operations for Logs collects and analyzes all types of machine-generated log data, including application logs, network traces, configuration files, messages, performance data and system state dumps.

You can connect VMware Aria Operations for Logs to everything in your environment, including operating systems, applications, storage, firewalls, network devices for enterprise-wide visibility using log analytics.

When VMware Aria Operations for Logs is configured and ready to collect logs, there are several ways you can ingest log data including:

- vSphere Integration — VMware Aria Operations for Logs can integrate with vSphere to automatically ingest events from a vCenter server and logs from ESXi hosts.
- VMware Aria Operations Integration — VMware Aria Operations for Logs can integrate with VMware Aria Operations to enable various alerts to send notification events in VMware Aria Operations and e-mails to administrators.
- Agents — VMware Aria Operations for Logs has collection agents available to send files and event logs from Linux or Windows to VMware Aria Operations for Logs
- Syslog — VMware Aria Operations for Logs can ingest data from any source via syslog. Just set the VMware Aria Operations for Logs server as your syslog destination.
- CFAPI — Events are sent in their original format to VMware Aria Operations for Logs using cfapi. Events sent over cfapi do not have to follow the guidelines of a syslog event and are not modified to comply with the syslog RFC.

Each event contains the following information.

Type	Description
Timestamp	The time when the event occurred
Source	Where the event originated. This could be the originator of the syslog messages such as an ESXi host or a forwarder such as a syslog aggregation.
Text	The raw text of the event.
Fields	A name-value pair extracted from the event. Fields are delivered to the server as static fields only when an agent uses the CFAPI protocol.

NOTE

VMware Aria Operations for Logs is not responsible for the content of the log messages from other VMware products. If you have a question about the log contents, contact the product team that generated the log message.

Filter Log Events by Time Range

You can filter log events to view only the events for a certain period.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering*

VMware Aria Operations for Logs. The URL format of the web user interface is https://`operations_for_logs-host`, where `operations_for_logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

You can specify the time range on either the **Dashboards** or **Explore Logs** pages in the web user interface. Time ranges are inclusive when filtering.

1. From the drop-down menu on the left of the **Search** button, select one of the predefined periods.

2. Optional: To set the initial and final point of the time range, select **Custom time range**.

Search for Log Events that Contain a Complete Keyword

You can search for log events that contain a complete keyword. Keywords contain alpha-numeric, hyphen, and underscore characters.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://`operations_for_logs-host`, where `operations_for_logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and click **Explore Logs**.

2. In the search text box, type the complete keyword that you want to search for in the log events, and click the **Search** button.

Log events that contain the specified complete keyword appear in the list.

The string that you searched for is highlighted in yellow.

You can save the current query to load it at a later stage.

Search Log Events by Field Operations

You can use the list of existing fields to search log events with specific values for a field.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://`operations_for_logs-host`,

where `operations_for_logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

> **IMPORTANT**
> VMware Aria Operations for Logs indexes complete alphanumeric, hyphen, and underscore characters.

1. Expand the main menu and click **Explore Logs**.

2. Click **Add Filter**.

3. In the filter row under the search text box, use the first drop-down menu to select any field defined within VMware Aria Operations for Logs.

   For example, **hostname**, **text**, **_index**, and so on. If you select the **_index** field, you can query logs from an existing index partition, which lists a specific subset of events based on the partition filter and renders quick results.

   The list contains all defined fields that are available statically, in content packs, and in custom content.

   Fields are sorted by name, except for the **text** and **_index** fields. Because **text** is a special field that refers to the message text, **text** appears at the top of the list, and is selected by default. Because **_index** is also a special field that refers to index partitions, **_index** appears after the **text** field in the list.

   > **NOTE**
   > Numeric fields contain additional operators that string fields do not: **=**, **>**, **<**, **>=**, **<=**. These operators perform numeric comparisons and using them yields different results than using string operators. For example, the filter **response_time=**`02` will match an event that contains a **response_time** field with a value 2. The filter **response_timecontains**`02` will not have the same match.

4. In the filter row under the search text box, use the second drop-down menu to select the operation to apply to the field selected in the first drop-down menu.

   For example:

   - Select **is** or **is not**. These filters match the full name. Using **is** for the **_index** field matches all the events stored in the specified index partition. Using **is not** for the **_index** field matches all the events that are not stored in the specified index partition.
   - Select **contains**. The **contains** filter matches full tokens: searching for "err" will not find "error" as a match. Using **contains** for the **_index** field matches glob patterns in all existing index partitions.

5. In the text box to the right of the filter drop-down menu, type the value that you want to use as a filter.

   You can list multiple values separated by comma. The operator between these values is `OR` .

   > **NOTE**
   > The text box is not available if you select the **exists** operator in the second drop-down menu.

6. Optional: To add more filters, click **Add Filter**.

> **NOTE**
> You can add only one filter using the **_index** field. However, after adding a field with the **_index** field, you can add more filters using other fields.

A toggle button appears above the filter rows.

7. Optional: For multiple filter rows, select the operator between filters.

Option	Description
all	Select to apply the AND operation between filter rows
any	Select to apply the OR operation between filter rows

default, **all** is selected.

> **NOTE**
> The **_index** field is considered a supplemental field. When you include this field in a filter, the filter is combined with filters containing other fields using the AND operator. However, you can select the OR operator to combine filters with non-**_index** fields.

8. Click the **Search** button.

Search for a Group of Hosts that Have a Common String in Their Names

Assume that you have several hosts that have a host with the following name: w1-stvc-205-prod3, and another host that is called w1-stvc-206-prod5. To find all logs for both hosts, create the following query.

1. Leave the search text box empty.
2. Define the filter.
   a. Select **hostname** from the field drop-down menu.
   b. Select **starts with** from the operator drop-down menu.
   c. Type `w1-stvc` in the value text box.
   Alternatively, you can use the **contains** operator, but then you must use a glob in the search value. In this example, you must type `w1-stvc-*` in the value text box.
3. Click the **Search** button.

You can save the current query to load it at a later stage.

Exclude Content Pack Field Extraction from Log Events Search

You can exclude content pack fields from extraction when searching log events to increase the query's performance.

Verify that you are logged into the VMware Aria Operations for Logs web user interface. The URL format is https://<operations_for_logs-host> , where operations_for_logs-host is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

> **IMPORTANT**
> Only exclude content packs that are not required to be extracted as part of the specific search.

1. Expand the main menu and click **Explore Logs**.

2. Click **Content Packs** to open the drop-down menu.
   a) Select **All** to select all content packs for the log search.
   b) Select only the content packs you want to include in the log search results.

3. Click **Search**.

> **NOTE**
> If the extracted field participates in the query filter and its content pack is excluded from the search, then the extracted field is used to create the query results. However, the extracted field does not appear in the search results.

Only selected content pack fields are extracted during the log events search.

You can save this search query for future use.

Search for Events that Occurred Before, After, or Around an Event

You can search the list of log events for events that occurred before, after, and around an event in the list.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

If you want to know more about the status of your environment before and after an event, you can check the surrounding events.

1. In the **Explore Logs** page, locate the event in the list.

2. At the left of the event row, click ⚙ and select **Set Time Range From This Event**.

3. In the Set Time Range From Event dialog box, use the drop-down menus to select the period and direction of the time range.
   You can select from a list of predefined periods from 1 second to 10 minutes.

4. Click **Set Range**.

The events that surround the selected event appear in the list.

> **NOTE**
> This operation clears all search parameters and filters that you have specified previously.

View Event in Context

You can view the context of a log event and browse the log events that arrived before and after it.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*,

where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

If you want to know more about the status of your environment before and after an event, you can check the surrounding events.

1. In the **Explore Logs** page, locate the event in the list.

2. At the left of the event row, click ⚙ and select **View Event In Context**.

3. Optional: Scroll up or down to the edge of the window to load more events.

4. Optional: Click the purple timestamp to scroll back to the highlighted message.

5. Optional: To add filters, click **Add filter** at the top, or click a field inside the highlighted event.

6. Optional: Add or remove specific event types by pointing to an event and clicking ⚙.

Analyze Event Trends

You can analyze log events for trends and anomalies.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and click **Explore Logs**.

2. Construct and run your query by using the search text box and applying filters.

3. In the Set Time Range From Event dialog box, use the drop-down menus to select the period and direction of the time range.

4. Click the **Event Trends** tab.

   VMware Aria Operations for Logs compares your query to the same time period immediately before and displays the results.

Clear All Filtering Rules

You can clear filtering and search results to view the list of all log events.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

After you perform a search on the events list, the search results remain on the screen until you clear all queries.

1. In the **Explore Logs** page, remove all filters.

2. If text appears in the search text box, delete it.

3. Click the **Search** button.

Examples of Search Queries

You can use these examples when building your queries in the **Explore Logs** page of VMware Aria Operations for Logs.

Query for all heartbeat events reported by the ESX/ESXi hostd process yesterday between 9-10am

> **IMPORTANT**
> VMware Aria Operations for Logs indexes complete alphanumeric, hyphen, and underscore characters.

To query for all heartbeat events reported by the ESX/ESXi hostd process:

1. In the search text box, type `heartbeat*`.
2. Define a filter.
   a. Select **appname** from the first drop-down menu.
   b. Select **contains** from the second drop-down menu.
   c. Type `hostd` in the value text box.
3. Define the time range.
   a. In the **Time Range** drop-down menu select **Custom**.
   b. In the first text box, enter yesterday's date and 9am.
   c. In the second text box, enter yesterday's date and 10am.
4. Click the **Search** button.

Search for a Group of Hosts that Have a Common String in Their Names

Assume that you have several hosts that have a host with the following name: w1-stvc-205-prod3, and another host that is called w1-stvc-206-prod5. To find all logs for both hosts, create the following query.

1. Leave the search text box empty.
2. Define the filter.
   a. Select **hostname** from the field drop-down menu.
   b. Select **starts with** from the operator drop-down menu.
   c. Type `w1-stvc` in the value text box.
   Alternatively, you can use the **contains** operator, but then you must use a glob in the search value. In this example, you must type `w1-stvc-*` in the value text box.
3. Click the **Search** button.

Query for all errors reported by vCenter Server tasks, events, and alarms

To query for all errors reported by vCenter Server tasks, events, and alarms:

1. In the search text box, type `error`.
2. Define a filter.
   a. Select **vc_event_type** from the first drop-down menu.
   b. Select the **exists** operator from the second drop-down menu.
3. Click the **Search** button.

Query for SCSI latency over one second as reported by ESX/ESXi

To query for SCSI latency over one second as reported by ESX/ESXi:

1. In the search text box, type `scsi latency "performance has"`.
2. Define a filter.
   a. Select **vmw_vob_component** from the first drop-down menu.
   b. Select the **contains** operator from the second drop-down menu.
   c. Type `scsiCorrelator` in the text box.
3. Define a second filter.
   a. Select **vmw_latency_in_micros** from the first drop-down menu.
   b. Select the **>** operator from the second drop-down menu.
   c. Type `1000000` in the text box.

4. Click the **Search** button.

Query for events in an index partition

To query for events in an index partition:

1. Leave the search text box empty.
2. Define the following filter.
   a. Select **_index** from the first drop-down menu.
   b. Select the **is** operator from the second drop-down menu.
   c. Enter the partition name in the text box. You can use one of the autocomplete suggestions.
3. Click the **Search** button.

Examples of Regular Expressions

You can type regular expressions in text boxes for field values to extract fields from log events.

The expressions you type must use the Java regular expressions syntax.

Table 4: Characters operators

Regular Expression	Description
\	Escapes a special character
\b	Word boundary
\B	Not a word boundary
\d	One digit
\D	One non-digit
\n	New line
\r	Return character
\s	One space
\S	Any character except white space
\t	Tab
\w	One alphanumeric or underscore character
\W	One non alphanumeric or underscore character

For example, if you have the string `1234-5678` and apply the following regular expressions

Regular Expression	Result
\d	1
\d+	1234
\w+	1234
\S	1234-5678

Table 5: Quantifiers operators

Regular Expression	Description
.	Any character except new line
*	Zero or more characters as long as possible
?	Zero or one character OR as short as possible
+	One or more
{<n>}	Exactly <n> times
{<n>,<m>}	<n> to <m> times

For example, if you have the string `aaaaa` and apply the following regular expressions

Regular Expression	Result
.	a
*	aaaaa
.*?	aaaaa
.{1}	a
.{1,2}	aa

Table 6: Combinations operators

Regular Expression	Description
.*	Anything
.*?	Anything as short as possible before

For example, if you have the string `a b 3 hi d hi` and apply the following regular expressions

Regular Expression	Result
a.* hi	b 3 hi d
a .*? hi	b 3

Table 7: Logic operators

Regular Expression	Description
^	Beginning of a line OR not if in brackets
$	End of a line
()	Encapsulation
[]	One character in brackets
|	OR
-	Range
\A	Beginning of a string

Regular Expression	Description
\Z	End of a string

For example, if you apply the following regular expressions

Regular Expression	Result
(hello)?	Either contains hello OR does not contain hello
(a|b|c)	a OR b OR c
[a-cp]	a OR b OR c OR p
world$	Ends with world followed by nothing else

Table 8: Lookahead operators

Regular Expression	Description
?=	Positive lookahead (contains)
?!=	Negative lookahead (does not contain)

For example, if you apply the following regular expressions

Regular Expression	Result
is (?=\w+)\w{2} primary	is FT primary? false
opid=(?!WFU-1fecf8f9)\S+	WFU-3c9bb994

Table 9: Additional Examples of Regular Expressions

Regular Expression	Description
[xyz]	x, y, or z
(info|warn|error)	info, warn, or error
[a-z]	A lowercase letter
[^a-z]	Not a lowercase letter
[a-z]+	One or more lowercase letters
[a-z]*	Zero or more lowercase letters
[a-z]?	Zero or one lowercase letter
[a-z] {3}	Exactly three lowercase letters
[\d]	A digit
\d+$	One or more digits followed by end of message
[0-5]	A number from 0 to 5
\w	A word character (letter, digit, or underscore)
\s	White space
\S	Any character except white space
[a-zA-Z0-9]+	One or more alphanumeric characters

Regular Expression	Description
([a-z] {2,} [0-9] {3,5})	Two or more letters followed by three to five numbers

Using the Explore Logs Chart to Analyze Logs

The chart at the top of the **Explore Logs** page lets you perform visual analysis on the results of your query.

Charts represent graphical snapshots of log search queries. You can use the drop-down menus under the chart to change the chart type.

You can use the first drop-down menu to the left to control the aggregation level of the chart. The **Count** function is selected by default.

Chart Types

You can select different chart types to change the way data is visualized in the Explore Logs page.

Different chart types require different aggregation functions, the use of time series, and group-by fields. Chart displays are limited to the 2,000 most recent results.

Chart Type	Aggregation Function	Time Series Requirement	Group-by Field Requirement
Column	Any	Time series	N/A
Line	Any	Time series	N/A
Area	Any	Time series	N/A
Bar	Any	Non-time series	At least one field
Pie	Count or Unique Count	Non-time series	At least one field
Bubble	Any	Non-time series	Two fields
Gauge	Count	Non-time series	N/A
Scalar	Count	Non-time series	N/A
Table	Any	Any	N/A

Multi-function Charts

You can use multi-function charts to compare variables that are not the same scale.

With multi-function charts, you can assign a y-axis for each series or an x-axis if you want to compare data sets of different categories. Each axis can be placed to the right or left of the chart. You can swap the functions to swap the y-axis on which they are plotted from right to left.

For example, you can chart the count of events grouped by channel and level in addition to the average of tasks grouped by channel and level.

Aggregation Function

VMware Aria Operations for Logs provides several aggregation functions.

Type	Field	Description
Count	Events only	Creates a chart of the number of events for a specific query.
Unique count	Any field	Creates a chart of the number of unique values for a field.
Minimum	Numeric fields only	Creates a chart of the minimum value for a field.
Maximum	Numeric fields only	Creates a chart of the maximum value for a field.
Average	Numeric fields only	Creates a chart of the average value for a field.
Std dev	Numeric fields only	Creates a chart of the standard deviation for a field's values.
Sum	Numeric fields only	Creates a chart of the sum of values for a field.
Variance	Numeric fields only	Creates a chart of the variance for the values of a field.

You can modify the way you view the query results.

View	Description
To group query results by specific field values	Use the second drop-down menu under the chart to group query results by specific field values rather than or in addition to time series.
To view the number of events for a field	For example, the number of events per host, deselect the **Time series** check box and select the check box for that field.
To view a stacked bar chart for a field with groupings over time	Select both the **Time series** check box and the field check box.

Examples of Aggregation Functions

An area chart displaying the average upgrade duration over time:
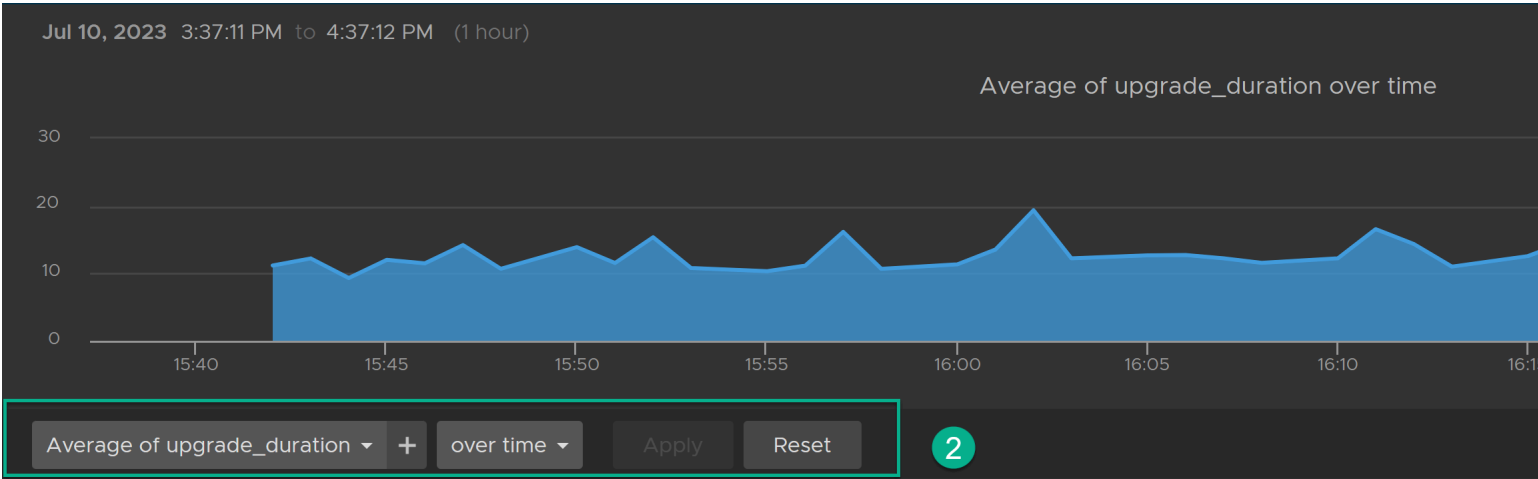
A column chart displaying the sum of gigabytes used over time:

A column chart displaying the count of events grouped by severity:

Jul 10, 2023 3:39:45 PM to 3:44:45 PM (5 minutes)

Count of events grouped by vmw_esxi_severity

20k

10k

0

info   error   verbose

Count of events ▾ + grouped by vmw_esxi_severity ▾   Apply   Reset

⭐▾   Custom time r

Jul 10, 2023 , 15:39:45.83
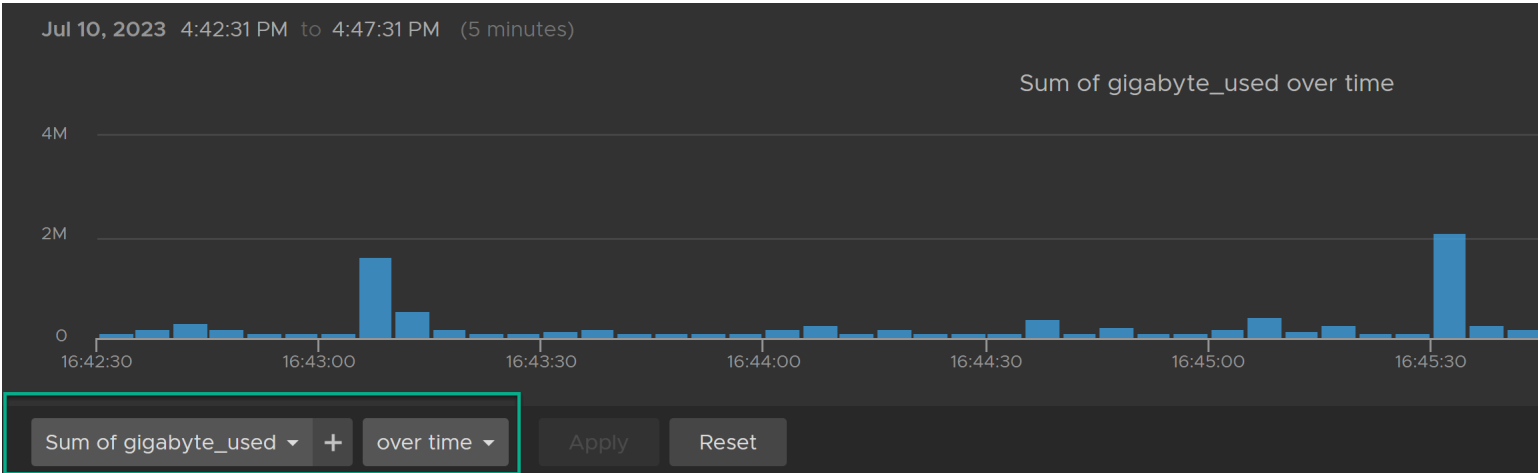
+ ADD FILTER

CONTENT PACKS ⌄   (Extract all fields)

Events	Field Table	Event Types	Event Trends

1 to 50 out of 50+ events

⚙▾   Jul 10, 2023
     15:44:45.817

source   event_type   facility   priority   hostname   appname   vmw_vsan_severity

Working with Charts

You can change how charts look in the **Explore Logs** page, add charts to your custom dashboards, and manage dashboard charts.

Task	Procedure
Change the time range of a chart	In the **Explore Logs** page, use the drop-down menu to the left of the **Search** button to switch the period displayed in the chart.
Change the granularity of a chart	In the **Explore Logs** page, use the buttons at the upper right to switch between different time ranges for each point represented on the chart. The available ranges depend on the time range specified for the query.

Task	Procedure
Load a dashboard chart in the **Explore Logs** page	In the **Dashboards** page, locate the chart and click the **Open in Explore Logs page** icon. The time range is set to the current time range of the dashboard. You can modify the time range if needed.
Save a chart to your custom dashboard	1. In the upper-right corner of the **Explore Logs** page, click **Add to Dashboard**. Alternatively, from the menu to the right of the **Search** button, select **Add Current Query to Dashboard**. 2. Type a name, select the destination dashboard from the drop-down menu, select the widget type, add information about the widget, and click **Add**.
Save a query as a chart to your custom dashboard	1. Click **Add Current Query to Dashboard** next to the **Search** button. 2. Type a name, select the destination dashboard from the drop-down menu, make sure the widget type is set to **Chart**, add information about the widget, and click **Add**.
Save a query as a field table to your custom dashboard	1. Click **Add Current Query to Dashboard** next to the **Search** button. 2. Type a name, select the destination dashboard from the drop-down menu, make sure the widget type is set to **Field Table**, add information about the widget, and click **Add**.
Delete a widget from your custom dashboard	1. In the **Dashboards** page, select the custom dashboard that contains the widget that you want to delete. 2. In the upper right corner of the widget, click the **Other Actions** icon ⚙, and select **Delete**. 3. In the Delete Widget dialog box, click **Delete** to confirm.

Change the Type of the Explore Logs Chart

You can change the aggregation and grouping of query results displayed in the chart to graphically analyse log events.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

The number of drop-down menus that you see under the chart depends on the selected aggregation function.

1. Use the drop-down menus under the Explore Logs chart to change the aggregation function and grouping type.

   - To view the number of events over time, select the **Time series** button.
   - To view only event values, select the **Non-time series** button and select at least one field.

2. Click **Update**.

   Aggregation and Grouping in the Explore Logs Chart

   The following table contains examples to illustrate aggregation and grouping in VMware Aria Operations for Logs charts.

Table 10: Example Aggregation and Grouping in the Explore Logs Chart

Selection in the First Drop-Down Menu	Selection in the Second Drop-Down Menu	Time series selection	Text Displayed on the Screen	Result
Count	Time series	Time series	**Count** of events **over time**	The chart displays a bar chart with the number of events for the current query over time.
Average	vmw_op_latency (VMware - vSphere)	Time series	**Average** of **vmw_op_latency (VMware - vSphere) over time**	The chart displays a line chart with average value of operations latency over time.
Count	vmw_esx_problem **NOTE** Thevmw_esx_problem field does not appear by default. You must extract the vmw_esx_problem field and save the query so that vmw_esx_problem appears in the drop-down menu.	Non-time series	**Count** of events **grouped by vmw_esx_problem**	The chart displays a bar chart of the number of events for containing the vmw_esx_problem field.
Count	Time series, **vmw_esx_p roblem**	Time series	**Count** of events **over time grouped by vmw_esx_problem**	The chart displays a stacked bar chart grouped by vmw_esx_problem over time.

Dynamic Field Extraction

In a large environment with numerous log events, you cannot always locate the data fields that are important to you.

VMware Aria Operations for Logs provides runtime field extraction to address this problem. You can extract any field dynamically from the data by providing a regular expression. See Examples of Regular Expressions.

> **NOTE**
> Generic queries might be slow. For example, if you attempt to extract a field by using the `\(\d+\)` expression, the query returns all log events that contain numbers in parentheses. Verify that your queries contain as much textual context as possible. For example, a better field extraction query is `Event for vm\(\d+\)`.

You can use the extracted fields to search and filter the list of log events, or to aggregate events in the Explore Logs chart.

> **NOTE**
> An extracted field name can contain different characters. However, the field name for an ingested event must begin only with a letter or an underscore character and contain only letters, digits, or the underscore character.

Extract Fields by Using One-Click Extract

Instead of typing context values for extracting fields dynamically, you can use the one-click extract function.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

The one-click extract populates all context values that correspond to the field that you select in a log event.

> **NOTE**
> The one-click extract option is available only in Events tab.

1. Expand the main menu and click **Explore Logs**.

2. In the list of log events, highlight the text that represents the field that you want to extract.

    An action menu appears above the set of field names present in that event.

3. Click **Extract Field**.

    The pre and post context values in the Fields pane are populated automatically with the context needed to extract the highlighted field.

4. Optional: Modify the Extracted value regular expression in the Fields pane.

5. Optional: Modify the Pre and post context regular expressions in the Fields pane.

6. Optional: Click ✚**Add additional context** to add more keywords and filters.

    You can add one or more keywords and use a single static field as a filter.

7. If you are an administrator or a user with edit access for the **Explore Logs** > **Extracted Fields** permission, select which users can access the field from the drop down menu.

Option	Description
All users	All users will see the field in their events and in the filter drop-down menu.
Me only	Only the creator of the field will see the field in their events and filter drop down menu.

8. Optional: At the top of the Fields pane, click *i* and then **Edit** to add notes to this field. Add notes in the **Edit Notes** window and click **OK**.

9. Click **Save**.

You can use the extracted field to search and filter the list of log events, or to aggregate events in the Explore Logs chart.

You can modify saved field definitions or delete them if you no longer need them.

Modify an Extracted Field

You can modify the definitions of extracted fields.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*,

where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

VMware Aria Operations for Logs creates copies of the fields that you use when you create charts, queries, or alerts. If you modify a field definition, all charts, queries, and alerts that use the modified field are updated to reflect the new definition.

Administrators and users with edit access for the **Explore Logs** > **Extracted Fields** permission can modify their own content and their shared content. Other users can modify only their own content.

Content pack fields are read-only.

1. Expand the main menu and click **Explore Logs**.

2. At the top of the Fields pane, click **Manage extracted fields** and select an extracted field from the list.

3. Modify the values and click **Update**.

   A dialog box displays a list of content that will be affected by the updated field. If the field is shared between multiple users, the dialog box also displays a list of affected users.

4. Optional: At the top of the Fields pane, click *i* and then **Edit** to add notes to this field. Add notes in the **Edit Notes** window and click **OK**.

5. Click **Update** to confirm your changes.

VMware Aria Operations for Logs updates all queries, alerts, and charts that use the field that you modified.

Duplicate an Extracted Field

You can duplicate an extracted field.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

You use the Duplicate option when you want to extract more than one field from an event and both fields appear in a similar context. After you extract a field and save it, open the extracted field definition and use the Duplicate option. The duplicated field has the exact same definition as the original extracted field. You can modify the definition of the duplicated field to match another value in the event that interests you.

Normal users can duplicate only their own content. Administrator users can modify their own content and their shared content.

1. Expand the main menu and click **Explore Logs**.

2. At the top of the Fields pane, click **Manage extracted fields** and select an extracted field from the list.

3. Click **Duplicate** to create a copy of the field.

4. Optional: Modify the Extracted value regular expression in the Fields pane.

5. Optional: Modify the Pre and post context regular expressions in the Fields pane.

6. Optional: Click **Add additional context** to add more keywords and filters.

   You can add one or more keywords and use a single static field as a filter.

7. If you are an administrator or a user with edit access for the **Explore Logs** > **Extracted Fields** permission, select which users can access the field from the drop down menu.

Option	Description
All users	All users will see the field in their events and in the filter drop-down menu.
Me only	Only the creator of the field will see the field in their events and filter drop down menu.

8. Click **Save**.

You can use the extracted field to search and filter the list of log events, or to aggregate events in the Explore Logs chart.

You can modify saved field definitions or delete them if you no longer need them.

Delete an Extracted Field

You can delete extracted fields that are no longer needed.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://`operations_for_logs-host`, where `operations_for_logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

VMware Aria Operations for Logs creates copies of the fields that you use when you create widgets, queries, or alerts. If you delete a field that is used in widgets, queries, or alerts, VMware Aria Operations for Logs creates a temporary copy of the deleted field for each widget, query, or alert that uses that field.

You can delete only fields that have the **Edit this field** icon next to their names. Administrators and users with edit access for the **Explore Logs** > **Extracted Fields** permission can delete their own content and their shared content. Other users can delete only their own content.

Content pack fields are read-only.

1. Expand the main menu and click **Explore Logs**.

2. At the top of the Fields pane, click **Manage extracted fields** and hover over an extracted field from the list.

3. Click .

   A dialog box displays a list of content that uses the field that you want to delete. If you are an administrator user, and the field is shared by multiple users, the dialog box also displays a list of affected users.

4. Click **Delete** to confirm.

If a deleted field is used in existing queries, VMware Aria Operations for Logs creates a temporary copy of the field and displays it when you load a query that uses the deleted field.

If you export content that contains temporary fields, VMware Aria Operations for Logs creates the fields in the exported content pack to avoid temporary fields.

Managing Search Queries

You can export query results, share your queries with other users, and can save, delete, rename, and load existing queries. You can take snapshots of queries and save them to dashboards.

Save a Query in VMware Aria Operations for Logs

You can save your current query and time range in VMware Aria Operations for Logs to view it later. Saved queries can only be loaded from the **Explore Logs** page.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. In the **Explore Logs** page, perform the query that you want to save.

2. Click , select **Add current query to favorites** icon .

3. Type a name and click **Save**.

> **NOTE**
> Saved queries include a fixed time range and are not updated. By saving a query, you take a snapshot of log messages available within the time range at the moment when you save.

The query is added to the Favorite queries list.

All users, including administrators, have an individual list of saved queries.

Rename a Query in VMware Aria Operations for Logs

You can change the name of a query that you saved in VMware Aria Operations for Logs.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and click **Explore Logs**.

2. Click the Favorite queries icon

3. Point to the query that you want to rename, and click the **Edit this saved query** icon .

4. Type a new name and click **Save**.

Load a Query in VMware Aria Operations for Logs

You can load queries from content packs or queries that you saved to view them in the **Explore Logs** page.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

Saved queries are separate from dashboard items. They do not appear on any custom dashboard. If you want to view a saved query, you have to load it.

All users, including administrators, have an individual list of saved queries.

1. Expand the main menu and click **Explore Logs**.

2. Click the Favorite queries icon ⭐

3. In the Favorite Queries list, click the query that you want to view in the **Explore Logs** page.

   The query is loaded in the **Explore Logs** page. The time range of the query is displayed above the list of events.

You can add the query to a dashboard, change the granularity of the chart, or apply additional filtering to the query results.

Delete a Query from VMware Aria Operations for Logs

You can delete saved queries from VMware Aria Operations for Logs.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://`operations_for_logs-host`, where `operations_for_logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and click **Explore Logs**.

2. From the drop-down menu on the right of the **Search** button, select **Load Query**.

3. Click the Favorite queries icon ⭐

4. In the Favorite Queries list, click ❌ next to the query you want to delete.

5. Click **Delete** to confirm.

Share the Current Query

You can send your peers a link to the current query.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://`operations_for_logs-host`, where `operations_for_logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. In the **Explore Logs** page, perform the query that you want to share.

2. Click 🔗 and select **Share Query**.

   VMware Aria Operations for Logs creates and displays a shortened URL for the query. The URL is kept for 93 days after its last use before being deleted.

3. Copy the URL and send it to the person that you want to share with.

Export the Current Query

You can export the results of a log query to share them with other systems, or forward them to your support contact.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://`operations_for_logs-host`,

where `operations_for_logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. In the **Explore Logs** page, perform the query that you want to export.

2. Click and select **Export Event Results**.

3. If your log query has 20,000 results or less, select the format to save the query in and click **Export**.

Menu Item	Description
Raw Events	Select to save the results in TXT format.
JSON	Select to save the results in JSON format.
CSV	Select to save the results in CSV format.

4. If your log query has more than 20,000 results, create a task to export the results to an NFS storage path:
   a) Select the format to save the query in, as described in the previous step.
   b) Enter a name for the export task.
   c) Enter the location for the NFS share to which you want to export the results.
   d) To receive an email notification when the export is done, use the toggle button to activate the notification and enter an email address to which the notification is sent. You can send a test email to verify the notification.
   e) Click **Export**.

The export task takes some time to finish, depending on the volume of the log query results. If there are multiple export tasks, new tasks are added to a queue and the nodes pick up the tasks from the queue. In the **Management** > **Export** page, you can track the progress of the export tasks. If a task is queued, you can see the position of the task in the queue. You can perform the following actions on an ongoing or queued task:

- Click the stop icon to end the export task.
- Click the pencil icon to activate or deactivate the email notification on the export completion, or modify the email address to which the notification is sent.

Administrators and users with the **Explore Logs** > **Export** permission can see all the tasks, whereas other users can see only their tasks. When an export task is finished, you can access the NFS share to open the file that contains the results.

Take a Snapshot of a Query

You can take a snapshot of your current query and time range in VMware Aria Operations for Logs for quick viewing or to save to a dashboard. Snapshots can be taken from the Explore Logs page.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://`operations_for_logs-host`, where `operations_for_logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

A snapshot saves the log messages available within the time range at the moment when you take the snapshot. After you take a snapshot, click it to return to the query when you took the snapshot. If you want to save one or more snapshots, add them to an existing dashboard or create a new dashboard.

1. In the **Explore Logs** page, perform the query that you want to save as a snapshot.

2. Click the Snapshot icon.
   The snapshot appears at the bottom of the screen.

3. Optional: Change the query and take additional snapshots.
   The snapshots appear at the bottom of the screen.

4. Optional: At the bottom of the screen, click ⚙ and select **Save All to Dashboard**.

   a) Select an existing dashboard or create a new dashboard.

   b) Click **Add.**

   The snapshot is added to the selected or new dashboard.

5. Optional: Click the "X" on a snapshot to delete the snapshot.

6. Optional: Click ⚙ and select **Delete All** to delete snapshots.

Troubleshooting Query Results

A warning icon next to a dashboard widget or in the Explore Logs page indicates that query results might be incomplete.

One cause is a timeout during dynamic field extraction as the query is run. A timeout can occur when becomes overloaded processing many log events, many queries, or complex content. Timeouts can result in a small portion of collected logs being ignored. A warning icon and detailed warning message inform you about these timeouts.

> **NOTE**
> Results for queries affected by timeouts are not fixed and can vary, depending on the load at the moment and the quantity of logs that are being processed for the query.

To resolve the problem, try the following actions.

- Ensure sizing is correct for the ingestion load. For more information about sizing, see
   a. Navigate to **Management > System Monitor** tab to check the ingestion load.
      > **NOTE**
      > To troubleshoot query results, you must be an administrator or a user with edit access for the **Management** > **System Monitor** permission.
   b. Go to the **Active Queries** tab of the **System Monitor** page to check the number of active queries and how long it took to run them.
   c. Make sure that is sized correctly for the current ingestion rate.
- Revise your query. In some cases, queries that have long processing times and the potential to time out contain a group-by clause, cover a significant number of logs, or return a relatively large number of results.

   Instead of a query whose result is a single value, substitute a query that produces time series results. This type of query is not affected by log volume during query processing.

Working with Dashboards

Dashboards in VMware Aria Operations for Logs are collections of chart, field table, query list, event types, and event trends widgets.

Custom Dashboards

Custom dashboards are created by users of the current instance of VMware Aria Operations for Logs. Custom dashboards are organized in two categories, My Dashboards and Shared Dashboards. Shared dashboards are visible to all users of the VMware Aria Operations for Logs instance.

My Dashboards are user-specific.

> **NOTE**
> - Administrators and dashboard users can modify the dashboards in the My Dashboards section, and the dashboards that they created in the Shared Dashboards section.
> - Users with the relevant **Dashboards** permissions can view or edit dashboards in the My Dashboards or Shared Dashboards section, based on the selected access levels.

Content Pack Dashboards

Content pack dashboards are imported with content packs and are visible to all users of the VMware Aria Operations for Logs instance.

> **NOTE**
> Content pack dashboards are read-only. You cannot delete or rename them. However, if you are an administrator, a dashboard user, or a user with view access to the **Dashboards** > **Content Pack Dashboards** permission, you can clone content pack dashboards to your custom dashboard. You can clone whole dashboards or individual widgets.

To view the dashboards that are available in your instance of VMware Aria Operations for Logs, expand the main menu and click **Dashboards**. The left pane that appears lists all dashboards you have access to, grouped by Custom Dashboards and Content Pack Dashboards. Click **>** next to each subgroup to display associated dashboards. You can open one dashboard group at a time by clicking **>** next to the group name. Click **>** next to another group name to open a new group and close the previous one. Only one group at a time can be open.

To view the contents of a dashboard, click the dashboard name in the list on the left.

Managing Dashboards

You can add, modify, and delete dashboards in your Custom Dashboards space.

Content Pack dashboards, pre-built dashboards that you download, cannot be modified, but you can clone these dashboards to your Custom Dashboards space and modify the clones.

> **IMPORTANT**
> VMware Aria Operations for Logs does not perform checks for duplicate names of the dashboards, queries, and alerts that you save or clone. The display name is not a unique identifier when VMware Aria Operations for Logs saves queries. Therefore, you can save multiple charts, alerts, and dashboards with the same name. To make data more easily retrievable, do not duplicate names when you save charts, alerts, or dashboards.

Working with Custom Dashboards

The following table lists the product capabilities you can use to create or modify a custom dashboard.

Task	Procedure
Create a custom dashboard.	In the **Dashboards** page, select **My Dashboards** in the left pane, and click **New Dashboard** at the top of the pane. If you are an administrator, a dashboard user, or a user with edit access for the **Dashboards** > **Shared Dashboards** permission, you can select **Share this dashboard among all users** to share your dashboard with other users.
Edit the name of a custom dashboard.	In the **Dashboards** page, point to the dashboard name in the left pane, click the menu icon , and select **Rename**. Enter a new name and click **Save.**

Task	Procedure
Delete a custom dashboard.	In the **Dashboards** page, point to the dashboard name, click the menu icon ⚙ and select **Delete**. In the confirmation dialog box, select **Delete**.
Clone a dashboard from a content pack to your custom dashboard.	1. In the **Dashboards** page, select a content pack in the left pane and point to the dashboard that you want to clone. 2. Click the menu icon ⚙ and select **Clone** from the drop-down menu. 3. Enter a name and click **Save**. If you are an administrator, a dashboard user, or a user with edit access for the **Dashboards** > **Shared Dashboards** permission, you can select whether to share your dashboard with other users.
Add a chart widget to a dashboard.	1. In the upper-right corner of the **Explore Logs** page, click **Add to Dashboard**. Alternatively, from the menu to the right of the **Search** button, select **Add Current Query to Dashboard**. 2. Type a name, select the destination dashboard from the drop-down menu, select the widget type, add information about the widget, and click **Add**. To modify the chart type, in the upper right corner of the widget, click the **Other Actions** icon. ⚙, and select **Edit Chart Type**.
Add a query list widget to the dashboard.	See Add a Query List Widget to the Dashboard.
Add a query to a query list widget in a dashboard.	See Add a Query to a Query List Widget in a Dashboard.
Add a query to a field table widget in a dashboard.	See Add a Field Table Widget to a Dashboard
Add an event types widget to a dashboard.	Add an Event Types Widget to a Dashboard
Add an event trends widget to a dashboard.	Add an Event Trends Widget to a Dashboard
Rename a widget.	1. In the **Dashboards** page, in the left pane, select the custom dashboard that contains the widget that you want to rename. 2. Click the title of the widget, modify the text, and press Enter.

Task	Procedure
Display time-synchronized data for all widgets.	By default, you can display a legend label for a given data point in a widget by hovering your pointer over that point. You can also display legend labels for all widgets for the same moment in time by enabling the setting for **Display legend for all widgets**, which is applied to all dashboards. The setting is cookie-based and persists across browser sessions. 1. In the **Dashboards** page, select a dashboard in the left pane. 2. In the upper left corner of the dashboard, set the toggle for **Display legend on all widgets** to be active.
Clone a widget.	1. In the **Dashboards** page, in the left pane, select the custom dashboard that contains the widget that you want to clone. 2. In the upper right corner of the widget, click the **Other Actions** icon. 🔅, and select **Clone**. 3. In the Clone to Dashboard dialog box, enter the widget details and click **Clone**.
Move a widget to another dashboard.	1. In the **Dashboards** page, in the left pane, select the custom dashboard that contains the widget that you want to move. 2. In the upper right corner of the widget, click the **Other Actions** icon. 🔅, and select **Move to Dashboard**. 3. In the Move to Dashboard dialog box, in the **Dashboard** drop-down menu, select the dashboard to which you want to move the widget.
Modify a widget.	1. In the **Dashboards** page, in the left pane, select the custom dashboard that contains the widget that you want to modify. 2. In the upper right corner of the widget, click the **Other Actions** icon. 🔅, and select **Edit**. 3. In the Edit Widget dialog box, modify the widget details and click **Save**.
Modify a query list, field table, event types, or event trends widget in Explore Logs.	1. In the **Dashboards** page, in the left pane, select the custom dashboard that contains the widget that you want to modify in Explore Logs. 2. In the upper right corner of the widget, click the **Other Actions** icon. 🔅, and select **Edit in Explore Logs page**. 3. In the **Explore Logs** page, modify the query details and click **Save**.
Delete a widget from a dashboard.	1. In the **Dashboards** page, in the left pane, select the custom dashboard that contains the widget that you want to delete. 2. In the upper right corner of the widget, click the **Other Actions** icon. 🔅, and select **Delete**. 3. In the Delete Widget dialog box, click **Delete** to confirm.
Troubleshoot a widget that displays the warning symbol.	See Troubleshooting Query Results.
Provide unauthenticated access to a custom or content pack dashboard for a certain period.	See Provide Unauthenticated Access to a Dashboard.

Add a Query List Widget to the Dashboard

You can save lists of search queries to your custom dashboards by creating query list widgets.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. In the **Explore Logs** page, run the query that you want to add to the dashboard.

2. Click the **Add current query to dashboard** icon .

3. Optional: In the **Name** text box, modify the widget name.

4. From the **Dashboard** drop-down menu, select the dashboard to which you want to add the query.

5. From the **Widget Type** drop-down menu, select **Query List**.

6. From the **Query List** drop-down menu, select **New Query List**, type a name for the list, and click **Save**.

7. Under **Notes**, enter additional information for the widget.

8. Click **Add**.

The query list widget appears on the dashboard that you specified.

You can add queries to the query list widget that you created. See Add a Query to a Query List Widget in a Dashboard.

Add a Query to a Query List Widget in a Dashboard

Query list widgets provide quick access to one or more saved queries from the dashboard.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

You can modify your custom query list widgets to add new queries.

1. In the **Explore Logs** page, run the query that you want to add to the query list widget.

2. Click the **Add current query to dashboard** icon .

3. From the **Dashboard** drop-down menu, select the dashboard that contains the query list widget.

4. Optional: In the **Name** text box, modify the widget name.

5. From the **Widget Type** drop-down menu, select **Query List**.

6. From the **Query List** drop-down menu, select the name of the widget to which you want to add the query, and click **Save**.

7. Under **Notes**, enter additional information for the widget.

8. Click **Add**.

VMware Aria Operations for Logs adds the query to the widget that you selected.

> **NOTE**
> Query list widgets use message queries. If you use the same message query in a chart widget and choose a group-by field that does not exist in any of the messages, the chart will display no results.

Add a Field Table Widget to a Dashboard

Field table widgets provide quick access to one or more saved fields from the dashboard.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. In the **Explore Logs** page, run the query that you want to add to the field table widget.

2. Click the **Add current query to dashboard** icon .

3. Optional: In the **Name** text box, modify the widget name.

4. From the **Dashboard** drop-down menu, select the dashboard to which you want to add the field table.

5. From the **Widget Type** drop-down menu, select **Field Table**.

6. Select the fields you want to include in the field table.

7. Under **Notes**, enter additional information for the widget.

8. Click **Add**.

The field table widget appears on the dashboard that you specified.

Add an Event Types Widget to a Dashboard

Event types widgets provide access to event type groups, which are created through machine learning to group similar events together.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. In the **Explore Logs** page, run the query that you want to add to the widget.

2. Click the **Add current query to dashboard** icon .

3. Optional: In the **Name** text box, modify the widget name.

4. From the **Dashboard** drop-down menu, select the dashboard to which you want to add the widget.

5. From the **Widget Type** drop-down menu, select **Event Types**.

6. Under **Notes**, enter additional information for the widget.

7. Click **Add**.

The widget appears on the dashboard that you specified.

Related Links

VMware Aria Operations for Logs summarizes a large number of individual events into a smaller number of broad event types. VMware Aria Operations for Logs uses machine learning to group similar events together, with each group showing the approximate number of events in the group. Grouping events helps identify the most communicative events and the most quiet ones, both of which are critical for troubleshooting.

Add an Event Trends Widget to a Dashboard

Event trends widgets provide access to information about event trends, which analyze trends in a specified time period.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://`operations_for_logs-host`, where `operations_for_logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. In the **Explore Logs** page, run the query that you want to add to the widget.

2. Click the **Add current query to dashboard** icon ▦⁺.

3. Optional: In the **Name** text box, modify the widget name.

4. From the **Dashboard** drop-down menu, select the dashboard to which you want to add the widget.

5. From the **Widget Type** drop-down menu, select **Event Trends**.

6. Under **Notes**, enter additional information for the widget.

7. Click **Add**.

The widget appears on the dashboard that you specified.

Filter Using Field Values from Charts

You can use a field value in a chart as filter on the dashboard that contains the chart, on a different dashboard that uses the field, and in Explore Logs.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://`operations_for_logs-host`, where `operations_for_logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

If you see a problem with a field value in a chart, you can quickly use the field value as an input and jump to another dashboard that uses that field. If no other dashboard uses this field, you can use the field value as a filter on the same dashboard or run it in Explore Logs.

1. From the **Dashboard** drop-down menu, select the dashboard that contains a chart widget.

2. In the chart widget, hover over the chart data and view field values that appear as tooltips.

3. Click the field value that you want to use as a filter.

   The **Add Value as Filter** menu appears.

4. Select where you want to use the field value as a filter.

Option	Action
Explore Logs	The Explore Logs page opens and displays the results of the chart query. The field value you selected in Step 3 is used as a filter.
This Dashboard	The field value you selected in Step 3 is used as a filter on the same dashboard.
Other Dashboard	The field value you selected in Step 3 is used as a filter on another dashboard that contains the field.

Provide Unauthenticated Access to a Dashboard

You can share a dashboard for a certain period by generating a URL with an expiry date. When other users access the URL, they can see a read-only view of the dashboard without logging in to VMware Aria Operations for Logs. If you apply filters to the dashboard, users see the filtered content.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a user associated with the User role, or a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

You can provide unauthenticated access to a custom dashboard or a content pack dashboard.

1. In the **Dashboards** page, select a dashboard.

2. Optionally, add one or more filters to refine the dashboard content.

3. Click the **Share** icon in the upper-right corner.

4. In the pop-up window, you can modify the dashboard name as seen by the users who access the generated URL.

5. Enter an expiry date for the generated URL. If you do not enter a date, the URL is active for seven days.

6. Click **Generate**.

7. Copy the URL that is generated and share it with other users.

   When you close the pop-up window after generating the URL, you can find it in **Management > Shared Dashboard URLs**. In this page, you can also edit or delete a shared dashboard URL.

Working with Content Packs

Content packs contain dashboards, extracted fields, saved queries, and alerts that are related to a specific product or set of logs.

VMware Aria Operations for Logs comes installed with General, vSphere, VMware vSAN, and VMware Aria Operations content packs. You can install community supported content packs from the VMware Sample Exchange and other content packs from the Content Pack Marketplace. You can also create and export your own content packs for individual or team use.

Using Content Packs

Content packs contain dashboards, extracted fields, saved queries, and alerts that are related to a specific product or set of logs.

To view the content packs that are loaded on your system, navigate to the **Content Packs** page in the VMware Aria Operations for Logs user interface.

To view the contents of a content pack, click the content pack in the list on the left.

Content Packs

The Content Packs category contains imported sets of dashboards, extracted fields, queries, and alerts. The General and VMware - vSphere content packs are imported by default.

> **NOTE**
> Content pack dashboards are read-only. You cannot delete or rename them. However, if you are an administrator, a dashboard user, or a user with view access to the **Dashboards** > **Content Pack Dashboards** permission, you can clone content pack dashboards to your custom dashboard. You can clone whole dashboards or individual widgets.

<u>Custom Content</u>

The Custom Content category contains dashboards, extracted fields, and queries created in the current instance of VMware Aria Operations for Logs. The My Content section contains the custom content of the user that is logged in. The Shared Content section contains content that is shared among all users of VMware Aria Operations for Logs.

> **NOTE**
> - You can share and manage content if you are a Super Admin user, or a user with edit or full access to content packs.
> - You cannot uninstall content from the Custom Content section. If you want to remove saved information from the Custom Content section, you have to delete individual elements, such as dashboards, queries, alerts, and fields.

Install a Content Pack from the Content Pack Marketplace

You can install content packs from the Content Pack Marketplace without leaving the VMware Aria Operations for Logs UI.

- Verify that the web browser you use to access the VMware Aria Operations for Logs user interface is connected to the internet.
- Verify that you are logged into the VMware Aria Operations for Logs web user interface as a Super Admin user, or a user associated with a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

If the web browser that you use to access the VMware Aria Operations for Logs user interface is not connected to the internet, you can download and install content packs separately as described in Import a Content Pack.

1. Expand the main menu and click **Content Packs**.
2. Click **Marketplace** under **Content Pack Marketplace** on the left.
3. Click the content pack you want to install.
4. Select the check box to agree to the terms of any license agreement.
5. Click **Install**.

When the installation is finished, the content pack appears on the Installed Content Packs list on the left.

Update an Installed Content Pack from the Content Pack Marketplace

You can update the content packs that are already installed from the Content Pack Marketplace without leaving VMware Aria Operations for Logs.

Verify that you are logged into the VMware Aria Operations for Logs web user interface as a Super Admin user, or a user associated with a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

> **NOTE**
> When alerts from content packs are enabled, the alerts are copied to a user's profile. Users can modify the copy's description or conditions. Beginning with alert definitions instantiated in 4.0, updating a content pack, and by extension its alert definitions, updates or removes the copies to match the improved content pack. If you want

to preserve any user modifications, export them as a content pack before applying the update and import the changes back into the user profile after the update.

1. Expand the main menu and click **Content Packs**.

2. From the menu on the left, select **Updates** to see a list of content packs for which updates are available.

   - To update a single content pack, click its icon to open an informational window. Click **Update** to begin the import. Depending on the content pack, after the import is finished you might see further instructions. If these appear, follow the configuration steps to successfully finish the upgrade.
   - To silently update all content packs with pending updates, click **Update All**. Read the instructions in the informational pop-up window and click **Update** to proceed. After the upgrade, click each content pack to see if there are further steps to finish the import. If you have exported a content pack to preserve user modifications, import it back into the user profile.

The updated content pack appears in the Installed Content Packs list on the left.

Download a Community Supported Content Pack

Community supported content packs are provided by the VMware community and are subject to the VMware Community Terms of Use. You can download these content packs from the VMware Sample Exchange and import them into VMware Aria Operations for Logs.

Verify that you are logged into the VMware Aria Operations for Logs web user interface as a Super Admin user, or a user associated with a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and click **Content Packs**.

2. Click **Community Supported** under **Content Pack Marketplace** on the left.

3. In the **Log Insight Community supported content packs** page, click the link to view the community content packs in the VMware Sample Exchange.

4. In the VMware Sample Exchange, click the content pack you want to install.

5. Click **Download** and save the Content Pack (VLCP) file.

Import the VLCP file into VMware Aria Operations for Logs. For more information, see Import a Content Pack.

You can check for community supported content pack updates in the VMware Sample Exchange and install the latest version by following the steps in this task. Once you import the content pack, the installed version overrides the existing version.

Import a Content Pack

You can import content packs to exchange user-defined information with other instances of VMware Aria Operations for Logs.

- If you want to use **Install as content pack** as the import method, verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user with full or edit access to content packs. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- If you want to use **Import into My Content**, you can log in to the VMware Aria Operations for Logs web user interface with any level of permission.

You can import only Content Pack (VLCP) files.

You can download content packs from the VMware Solutions Exchange at https://marketplace.vmware.com. You can also download community supported content packs from the VMware Sample Exchange at https://code.vmware.com.

If you are accessing the VMware Aria Operations for Logs user interface from a web browser that is connected to the internet, you can install or update content packs from within VMware Aria Operations for Logs. See Install a Content Pack from the Content Pack Marketplace.

NOTE

When you update a content pack that has alerts activated, the update overwrites any modifications you have made to alert descriptions or conditions.

Modifications are kept in your user profile. To preserve these modifications, export them as a content pack before the update, and import them into the user profile after the update.

1. Expand the main menu and click **Content Packs**.

2. In the upper left corner, click **Import Content Pack**.

3. Select the import method.

Menu Item	Description
Install as content pack	The content is imported as a read-only content pack that is visible to all users of the VMware Aria Operations for Logs instance. **NOTE** Content pack dashboards are read-only. You cannot delete or rename them. However, if you are an administrator, a dashboard user, or a user with view access to the **Dashboards** > **Content Pack Dashboards** permission, you can clone content pack dashboards to your custom dashboard. You can clone whole dashboards or individual widgets.
Import into My Content	The content is imported as custom content to your user space, and is visible only to you. You can edit the imported content without having to clone it. **NOTE** Content pack metadata, such as name, author, icon, and so on, are not displayed in this mode. Once imported in My Content, the content pack cannot be uninstalled as a pack. If you want to remove a content pack from My Content, you have to individually remove each of its elements, such as dashboards, queries, alerts, and fields.

Non-admin users can import content packs only in their own user spaces.

4. Browse for the content pack that you want to import, and click **Open**.

5. Click **Import**.

6. Optional: If you selected to import the content pack as custom content, a dialog box appears and you are prompted to select what content to import. Select the content items and click **Import** again.

7. Optional: Some content packs require additional setup steps. Instructions for these steps appear after the import is finished. Complete these steps before you use the content pack.

The imported content pack is ready to use and appears in the Content Packs or the Custom Content list to the left.

NOTE
Imported alerts are deactivated by default.

Export a Content Pack

You can export your custom dashboards, saved queries, alerts, and extracted fields as a content pack, to share content between VMware Aria Operations for Logs instances or with VMware Aria Operations for Logs users on the community.

Content packs are saved as VMware Aria Operations for Logs Content Pack (VLCP) files.

All fields used in queries, charts, and alerts that you export are included in the exported content pack. If the custom dashboards, saved queries, and alerts contain the **_index** field in their filters, the filters are excluded from the export content.

If you export content that contains temporary fields, VMware Aria Operations for Logs creates these fields within the content pack during the export.

1. Expand the main menu and click **Content Packs**.

2. Click the content pack that you want to export and select **Export** from the drop-down menu ⚙ next to the name of the content pack.

3. Optional: Select the content that you want to include in the content pack.

    NOTE
    You cannot deselect fields that are used in dashboards, queries, or alerts selected for export.

4. In the text boxes to the right, enter the metadata for your content pack.

Option	Description
Name	The name is displayed when you import the pack into a VMware Aria Operations for Logs instance. The content pack filename is derived from the **Name** text box. The format is of the form `Vendor - Product`. For example, VMware - vSphere.
Version	If you plan to upgrade this content pack, type a version. VMware Aria Operations for Logs displays the version when you try to install a content pack that is already on the Content Packs list.
Namespace	The namespace is a unique identifier for the content pack. Use reverse DNS naming, for example `com.companyname.contentpackname`.
Author	Optionally, you can type your name or the name of your company.
Website	Optionally, you can provide a link to the website that is associated with the content pack. All users that can view the content pack can see the website link as well.
Description	Optionally, you can provide information about the contents and purpose of the pack.
Icon	Optionally, you can browse for an icon to be displayed next to the content pack name. **NOTE** The icon file format must be PNG or JPG, and is scaled to 144 by 144 pixels in size.

NOTE
This data is visible only if you import the content pack by using the **Install as content pack** option. You cannot view this information if you choose to import the content pack as custom content.

5. Click **Export**, browse to the location where you want to save the file, and click **Save**.

The exported VLCP file is downloaded to the selected location.

View Details About Content Pack Elements

You can open the queries that build up dashboards, or open the definitions of fields, queries, and alerts, directly from the Content Packs view.

You might want to use the definitions of content pack elements as templates for your custom definitions.

1. Expand the main menu and click **Content Packs**.

2. Select the content pack that contains the element that you want to review.

3. Click the button that corresponds to the element type you want to review.

   For example, click **Alerts** to view all alerts that the content pack contains.

4. In the list of elements, click the name of the element that you want to review.

The **Explore Logs** page opens and displays the query that corresponds to the selected element.
You can modify the query or definition of the content pack element and save it to your custom content.

Uninstall a Content Pack

You can uninstall content packs. Uninstalling contact packs removes custom dashboards, saved queries, alerts, and extracted fields.

Verify that you are logged into the VMware Aria Operations for Logs web user interface as a Super Admin user, or a user associated with a role that has the relevant permissions. For more information, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*. The URL format of the web user interface is https://*operations_for_logs-host*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

Content packs are saved as vCenter VMware Aria Operations for Logs Content Pack (VLCP) files.

Uninstalling a content pack makes it permanently unavailable for all users. Make a backup by exporting the content pack as a VLCP file first. See Export a Content Pack.

1. Expand the main menu and click **Content Packs**.

2. Click the content pack that you want to uninstall and select **Uninstall** from the drop-down menu ⚙ next to the name of the content pack.

3. Click **Uninstall**.

The content pack is removed from the Installed Content Packs list.

Extract Selected Content Pack Fields for Queries

When you run queries that use extracted fields, you can specify which content packs to run the query against.

By default, all content pack fields are extracted after running a query. However, some of the content packs might not be relevant to the desired information, and as a result their extracted fields creates inefficiency and overhead during query processing.

To run the query more efficiently and to reduce the content pack fields' extraction timeouts, you can select only the content packs that contain the fields of interest for extraction. To specify the content packs, select them in the Content Packs drop-down menu in the Explore Logs page.

Creating Content Packs

Any Log Insight user can create a content pack for private or public use.

Content packs are immutable or read-only plug-ins to VMware Aria Operations for Logs, that provide predefined knowledge about specific types of events, such as log messages. The goal of a content pack is to provide knowledge about a specific set of events in a format that is easily understandable by administrators, engineers, monitoring teams, and executives.

Content packs give information about the health status of a product or application. In addition, a content pack helps you understand how a product or an application works.

You can save the information from a content pack by using either the Dashboards or Explore Logs pages in VMware Aria Operations for Logs. The information in a content pack includes:

- Queries - A content pack usually contains at least three queries and three chart widgets for each dashboard, which means more than nine queries in total.
- Fields - Fields can be used in multiple ways for aggregations and filters. For example, functions and groupings can be applied to fields, and operations can also be performed against fields. A field should include as many keywords as possible to improve performance.
- Aggregations
- Alerts - A content pack contains at least five alerts.
- Dashboards - A content pack contains at least three dashboards.
- Dashboard filters - See Searching and Filtering Log Events.
- Visualizations - See Using the Explore Logs Chart to Analyze Logs.
- Agent groups - VMware Aria Operations for Logs agents that are used as logs collection mechanize.

By default, VMware Aria Operations for Logs ships with the VMware - vSphere, VMware - VMware Aria Operations, VMware vSAN, and General content packs. You can import additional content packs if needed.

Content Pack Terms

The content pack creation workflow is based on several concepts and terms. You should get familiar with them in order to create and maintain content packs effectively.

Instance

Only administrators or users with edit or full access to the **Content Packs** permission can import a content pack file as a content pack. If a content pack is imported as a content pack, it cannot be edited.

All users can import a content pack file into a user space. If you import a content pack file into a user space, the operation selectively imports the objects under My Content. When you import a content pack into a user space, you can edit the content packs in a VMware Aria Operations for Logs instance. If you want to publish or modify a content pack you need an exported content pack.

User

Content packs are created in part from the content saved under Custom Dashboards, also known as user space, or more specifically either My Dashboards or Shared Dashboards on the Dashboards page. While objects from a custom dashboard can be selectively exported, it is recommended that every individual content pack be authored by a separate user entity inVMware Aria Operations for Logs to ensure a clean user space per content pack.

For information about creating users in VMware Aria Operations for Logs, see Managing VMware Aria Operations for Logs User Accounts.

For information about creating users in VMware Aria Operations for Logs, see the *VMware Aria Operations for Logs Administration Guide*.

Use a separate content pack author user in VMware Aria Operations for Logs for every content pack you create.

Events

It is essential to collect relevant events before attempting to create a content pack to ensure that a content pack covers all relevant events for a product or an application. One common way to collect relevant events is to ask quality assurance and support teams as these teams usually have access to, and knowledge about common events.

Attempts to generate events while you create a content pack are time consuming and results in missing important events. If QA and support teams are unable to supply events, you may simulate events and use them instead if product or application events are known and documented.

Once you collect the appropriate logs, they must be ingested into VMware Aria Operations for Logs.

Authors

The authors of a content pack need to have the following qualifications:

- Experience using VMware Aria Operations for Logs.
- Real world operating knowledge of the product or application.
- Understanding and ability to generate optimized regular expressions.
- Experience debugging multiple problems with product or application using logs.
- Support background, with exposure to a myriad of problems.
- System administrator background with previous syslog experience.

Workflow

The recommended approach for content pack creation is to start on the Explore Logs page and begin querying for specific types of events such as error or warning. Look at the results of the queries and analyze and extract potential field candidates as appropriate. With some understanding of the types of events and useful pieces of information available in the events, construct and save relevant queries as appropriate. For queries that highlight an issue that needs a quick action, create and save alerts. As you save queries, remove them from the results list using a filter to show other events that may be potential candidates for new saved queries. Once you save all relevant queries, organize and display them in a logical manner on the Dashboards page.

Queries

Queries in VMware Aria Operations for Logs can retrieve and summarize events.

You can create and save queries from the Interactive Analysis page. A query consists of one or more of the following:

Keywords
    Complete, or full-text, alphanumeric, hyphen, and/or underscore matches.
Globs
    Complete, or full-text, alphanumeric, hyphen, and/or underscore matches.
Regular expressions
    Sophisticated string pattern matching based on Java regular expressions.
Field operations
    Keyword, regular expression, and pattern matches applied to extracted fields.
Aggregations
    Functions that are applied to one or more subgroups of the results.

VMware Aria Operations for Logs supports the following types of queries:

- Message. A query made up of keywords, regular expressions and/or field operations.
- Regular expression or field. A query made up of keywords and/or regular expressions.
- Aggregation. A query made up of a function, one or more groupings, and any number of fields.

You can define custom alerts inVMware Aria Operations for Logs and trigger them from scheduled queries of any type.

Best Practices for Creating Message Queries

Basic concepts for creating message queries.

You can enter message queries by using the Search bar, or by entering filters.

Use the search bar to refine the results for events in a VMware Aria Operations for Logs instance. While you can use a filter instead of the search bar, it is often easier to understand a query that leverages the search bar over an equivalent filter. The best practice is to use the search bar instead of an equivalent filter when possible.

A filter allows you to create queries by using a regular expression, a field, logical OR operation, or a combination of search bar and filter queries.

When you create queries by using the search bar and filters, the following best practices apply:

- Ensure queries are not environment specific. Public content packs need to be generic to any environment and as such need not to rely on environment specific information. Examples of environment specific information include source, hostname, and potentially facility if the facility uses `local*`.
- When constructing a query, use keywords when possible, when keywords are not sufficient use globs, and when globs are not sufficient use regular expressions. Keyword queries are the least resource intensive type of query. Globs are a simplified version of regular expression and are the next least resource intensive type of query. Regular expressions are the most expensive type of query.
- Provide as many keywords as possible when using regular expressions or fields. If a regular expression includes a logical OR, for example `this|that`, do not include keywords. VMware Aria Operations for Logs is optimized to perform keyword queries prior to regular expressions to minimize regular expression overhead.

Field Queries

Fields are a powerful way to add structure to unstructured events and allow the manipulation of both the textual and visual representation of data.

Fields are one of the most important items in a content pack as they can be used in different ways including aggregations and filters. Aggregations allow you to apply functions and groupings to fields. Filters allow you to perform operations over fields.

You must extract any part of a log message that might be applicable to a query or aggregation. Fields are a type of regular expression query and are useful for complex pattern matching so you do not need to know, remember, or learn complicated regular expressions.

Field Context Value	Definition
Regex before value	Include as many keywords as possible. If this field is empty or only contains special characters, then the Regex after value must include keywords.
Regex after value	Include as many keywords as possible. If this field is empty or only contains special characters, then the Regex before value must include keywords.

Field Context Value	Definition
Name	Only use alphanumeric characters. Ensure all characters are lower case and use underscores instead of spaces as this makes fields easier to view. Keep in mind that names for content pack fields and user fields can be the same, though content pack fields will have a namespace in parenthesis to the right of the field name. Prefix content pack fields with an abbreviation, for example vmw_, to avoid confusion.
Keyword Search Terms	One or more keywords, separated by space, that appear within events containing the field.
Filter	A static field, operator, and a potential value that appears within events containing the field. It is common to use this in conjunction with the VMware Aria Operations for Logs agent and tags for events that do not contain keywords.
Information ("i" button)	Used to provide information about the field including what it means, what potential values could be returned, and possibly a user-friendly mapping of values to human-understandable information.

Best Practices

In addition to the various components that make up a field, several best practices apply.

- Only create fields for regular expression patterns. If a field can be queried using keyword queries, or will only ever return a single value, then use keyword queries instead of a pre-defined field. If a field will only return two values then consider constructing individual queries instead of extracting a field. Fields are meant to add structure to unstructured data as well as provide a way to query over specific parts of an event.
- Only create fields for regular expression patterns that return a fraction of the total events. Fields that will match most events and/or return a very large number of results are not a good candidate for field extraction. The regular expression will need to be applied to a large quantity of events resulting in a resource intensive operation. If possible add additional keywords to reduce the number of results returned and optimize the query.
- If a field contains keywords within regular expression syntax, then add such keywords as a filter without regular expression syntax. For example, if the value or the context of a field contains keywords within regular expression syntax such as `this|that`, then add the keywords as a text filter to optimize the query like `text contains this, that`.
- Use of the additional context with one or more keywords is recommended over complex regular expressions in the before or after context.
- Add additional context to all extracted fields in order to optimize query performance.

Temporary Fields

A temporary field is a field that exists as part of a query, but is not saved globally within a VMware Aria Operations for Logs instance or as part of an installed content pack.

VMware Aria Operations for Logs reduces the chances of creating a temporary field by automatically updating the query that relies on a field being modified.

> **NOTE**
> If you delete a field that a saved query relies on, the saved query contains a temporary field.

You can see temporary fields when you run a saved query in the Interactive Analysis page and a field used in the saved query contains the namespace Temporary to the right of the field name.

Queries to contain one or more fields. For saved queries in VMware Aria Operations for Logs the field definition used when a query is saved will be modified if the field is modified. Field modifications include

- Changing the field value
- Changing the regex before value and the regex after field value
- Changing the name of the field
- Deleting the field

When you export a content pack VMware Aria Operations for Logs converts all temporary fields to content pack fields. If you see a temporary field in a content pack, you might be looking at a content pack from a previous product version that is exported with temporary fields, or the content pack is manually edited.

If a temporary field exists with the same name as an existing extracted field, the temporary field displays ending in {n}. For example, if you have a field called `product_test_field`, product_test_field {2} might also be visible during export. If you see this behavior, a temporary field exists. To address the issue, choose the **Select None** option at the bottom of the export dialog box and select each dashboard and/or alert until the extract field(s) with the {n} ending are checked. Go to those dashboards and/or alerts and edit each query. When you find a query using the extracted field, change the filter or aggregation to use the field without the {n} ending, run the query, and save the query. After you complete these steps for all queries using a field ending in {n}, the field no longer displays during export.

Aggregation Queries

VMware Aria Operations for Logs lets you manipulate the visual representation of events by using aggregation queries.

Aggregation queries consist of the following two attributes:

- Functions
- Groupings

An aggregation query requires one function and at least one grouping. Groupings are an important part of the content packs. Functions and groupings impact the way charts are displayed.

Chart displays are limited to the 2,000 most recent results.

Bar Charts

By default, the overview chart in the Interactive Analysis page of VMware Aria Operations for Logs displays a count of events over time. If you use the count function in conjunction with the time series grouping, VMware Aria Operations for Logs creates a bar chart.

If you use the count function in conjunction with a single field grouping instead of time series, VMware Aria Operations for Logs creates bar charts with quantities listed from greatest to least.

Line Charts

All functions, except the count function, are mathematical. They require a field, against which you apply the equation. When performing a mathematical function on a field and grouping by time series, VMware Aria Operations for Logs creates a line chart.

Stacked Charts

By default, the overview chart on the Explore Logs page of VMware Aria Operations for Logs is a count of events over time. If you add one field to the time series grouping, then VMware Aria Operations for Logs creates a stacked chart.

If you use grouping by time series, plus a field, and you use any function except count, VMware Aria Operations for Logs creates stacked line chart. Stacked charts are powerful when attempting to find anomalies for an object.

You must decide which type of stacked chart to use, based on the number of object that the aggregation query might return. Displaying more objects require more resources, that are needed to parse and display information. In addition, the number of colors is fixed, and distinguishing between objects might become challenging, depending on the number of returned objects. In general the following best practices apply

- If the number of returned objects in each bar is less than ten, then you might want to use stacked charts.
- If the number of returned objects in each bar is or could be between ten and twenty, then stacked charts could be good. You must consider the way to visually represent the chart in a content pack.
- If the number of returned objects in each bar is or could be greater than twenty, then stacked charts are discouraged.

Multi-Colored Charts

If you create a grouping by using more than one field and time series, then VMware Aria Operations for Logs creates a multi-colored chart. The chart consists of two colors that interchange. Each interchange represents a new time range. Multi-colored charts can be hard to interpret so consider the value of such a chart before including it in a content pack.

When you make a grouping by multiple fields, consider using non-time series. Removing time series makes the bar chart easier to understand.

If multiple fields are important in a given time range, then you can create multiple charts for each field individually over the time range. You can then display the charts in the same column of a dashboard group in a content pack.

Other Charts

Several other chart types are available, including pie, bubble, and table charts. To use these charts, a specific query type is required. If the option for these charts are available, then you already have the correct query. If the option for these charts is not available, hover over the chart name you want to use. A pop-up message describes the type of query required for the chart type.

Message Queries

When constructing an aggregation query, the message query should only return results relevant to the aggregation query. This makes analyzing easier and ensures that only results only show relevant fields. To ensure the message query returns the same results as the aggregation query, you must add filters using the $exists$ operator for each field that is used in the aggregation query.

Changing Chart Type

If you want to change the chart type of a widget on a dashboard, click the gear icon on the widget and select **Edit Chart Type**. If you want to change a widget type, save a new widget and delete the old widget.

Alerts

Alerts provide a way to trigger a reaction when a certain type of event occurs.

VMware Aria Operations for Logs supports three types of alerts.

- Email
- Webhook
- VMware Aria Operations

You can save alerts only in a user space. By default all content pack alerts are deactivated. If you create an activated alert and export it as a part of a content pack, the alert will be deactivated in the content pack.

Content packs do not contain email and VMware Aria Operations settings. And you cannot add these settings to a content pack.

Thresholds

Thresholds set a limit to the number of triggered alerts.

It is important to understand how thresholds work to ensure that, if enabled, a content pack alert does not unintentionally spam a user. When considering the usage of a threshold, there are two questions you must keep in mind

- How frequently to trigger the alert? Log Insight comes with pre-defined frequencies. Alerts will only trigger once for a given threshold window.
- How often to check if an alert state has occurred? An alert is triggered by a query. Alerts, like queries, are not real-time in the current version. For each threshold window, a pre-determined query frequency is allocated. Changing the threshold changes the query time.

Groupings

When you create an email alert it is important to group by a field that identifies the source of the alert.

The email that the alert sends contains a table of results for a particular aggregation query. You can see the visual representation of the query on the Explore Logs page.

Without a unique identifier to group by you will not know if the result is relevant for one or multiple systems in your environment. You should group by hostname field and not by source field. You can also add any field that uniquely identifies where the event comes from.

Dashboards Best Practices

Dashboards are part of the content packs. There are some best practices that apply when creating dashboards.

When creating dashboards, the following best practices apply

- Content packs usually contain a minimum of three dashboards. The best practice is to start with an overview dashboards to provide high-level information about the events for a particular product or application. In addition to the overview dashboards, dashboards should be created based on logical groupings of events. The logical groupings are product-specific or application-specific, but some common approaches are performance, faults, and auditing. It is also common to create dashboards for a component, like disk and controller. With the component approach, it is important to note that it is only effective if queries can be constructed to return results from specific components. If this is not possible, then the logical approach is recommended.
- When you name dashboards, make the title generic and avoid adding product-specific or application- specific names unless being used in a component specific fashion. For example, in the VMware - vSphere content pack, there is a dashboard groups called ESX/ESXi instead of VMware ESX/ESXi.
- Dashboards must contain a minimum of three dashboard widgets and a maximum of six dashboard widgets. With any less than three dashboard widgets the amount of knowledge that can be attained by dashboards is minimal. In addition, having a lot of dashboards with only a limited amount of dashboard widgets requires a user to switch between different pages and does not provide information in a coherent way.

    Conversely, any more than six dashboard widgets for dashboards can have negative impact. You might get too much information that might be confusing. Too many widgets require intense usage of your system resources, as each widget is a query that must be run against the system.

    When you include more than six dashboard widgets in dashboards, you must separate the information and create multiple dashboards. If a dashboard widget is applicable to one or more dashboards, create the widget in each applicable dashboards.

Dashboard Filters

Dashboard filters can be used to drill down to specific events. The filters function similar to the filters on the Explore Logs page and leverage fields to drill down. Every dashboard should have at least one dashboard filter, typically with the hostname field, but up to five fields can be added to each dashboard.

The field added should be used by the majority of widgets on a given dashboard so that if the dashboard filter is used, most of the widgets return results. Examples of dashboard filters could include a severity field, a user field, or even a component field.

> **NOTE**
> The field and the operator used by the dashboard filter will be saved in an exported content pack. Any value used by a dashboard filter will not be saved during export as the value is likely to be specific to an environment and not generic to all environments.

Dashboard Widgets

Dashboard widgets help you visualize information.

There are several types of widgets in VMware Aria Operations for Logs that you can add to a dashboard. These include:

- A Chart widget that contains a visual representation of events with a link to a saved query.
- A Query List widget that contains title links to saved queries.
- A Field table widget that contains events where each field represents a column.
- A simplified Event Types table widget that contains similar events combined in single groups.
- A simplified Event Trends table widget that shows a list of event types found in the query, sorted by number of occurrences. This is a quick way to see what sorts of events are happening very frequently in a query.

Chart

A dashboard chart widget contains a visual representation of events. You can represent a chart as a bar or line chart and either can be displayed as a stack.

There are several ways to represent charts:

- Charts can contain a lot of information. Avoid having more than two chart widgets in a single row. In some rare cases, three chart widgets can be used effectively, but more than three is strongly discouraged. When determining whether chart widgets are readable or not, be sure to use the minimum resolution supported by VMware Aria Operations for Logs, which is 1024 x 768 pixels.
- If any row except the last row has a single chart widget, then make that widget full-width
- When naming a chart widget, use a descriptive title and avoid cryptic field names. For example, an extracted field is called `vmw_error_message`. Instead of calling a chart Count of `vmw_error_message`, call it Count of error messages
- You can save similar charts and stack them in the same column of a dashboard group for visual comparison. For example:
  - Average X of events over time + Maximum X of events over time. Given the different functions used, the Y-axis of the charts might have a different scale.
  - Count of events over time grouped by X + Count of events over time grouped by Y.

Query List

A dashboard query list widget contains one or more links to pre-defined queries.

You can use Query list widgets for the following reasons

- When a chart widget does not provide significant value, but the underlying query does.
- To save complex queries such as those using regular expressions.
- To use different aggregations on the same underlying query within a dashboard group.

Field Table

A Field Table that contains events where each field represents a column.

A dashboard field table widget contains the latest events for the given query in a table format where each field represents a column.

You can use a field table widget for the following reasons.

- To see the latest events for the given query. This can be useful for change management or for security reasons.
- To see only the fields you care about for a given query. This can be useful to limit event output.

Content Pack Import Errors

When you import a content pack, you might get some warnings or error messages.

Upgrade

You might get an upgrade message. It means that another content pack is installed in the system that has the same namespace. In this case you can either upgrade, and replace the existing content pack, or cancel the upgrade process and keep the existing content pack.

Invalid Format

You might get a message stating the format is invalid. This means that the VLCP file is manually edited and contains syntax errors. The syntax errors must be fixed before you import the content pack.

Newer Version

This type of message implies that the content pack is created and is supported only oin a newer version of Log Insight. On product versions, later than Log Insight 1.5 seeing this type of message means that the VLCP file is manually edited.

Unrecognized Version

When the VLCP file is manually edited and contains syntax errors you might see this type of message. You must fix the syntax errors before you attempt to import the content pack.

> **NOTE**
> You should not edit VLCP files manually. As a result, it is hard to locate and fix syntax errors.

Requirements for Publishing Content Packs

When you create and want to publish a content pack, make sure that the content packs meet the basic publishing requirements.

You must check both the content pack requirements and the publishing requirements.

Content Pack Requirements

Content packs must meet some requirements for the content, quality, and standards.

The content requirements include:

- Minimum of three dashboards
- Minimum of one, ideally three, and up to five dashboard filters per dashboard
- Minimum of three dashboard widgets per dashboards
- Maximum of six dashboard widgets per dashboards
- Maximum of three dashboard widgets per row
- Minimum of five alerts
- Minimum of 20 extracted fields

The quality requirements for a content pack are the following:

Alerts

        Use meaningful time periods for alerts.

Dashboard groups

- Consider starting with an overview dashboard group.
- Create dashboard groups based on message types (for example, overview or performance), and not on component types (for example, compute, network, or storage).
- Duplicate the same dashboard widget in multiple dashboards groups if the dashboard widget is applicable in each dashboard group.
- Target at least three dashboard groups in a content pack.
- You cannot reorder dashboard groups and dashboard widgets, except with user content.
- When naming dashboard groups, make the title generic and avoid adding product-specific or application-specific names, unless they are used in a component-specific manner.

Dashboard widgets

- Do not put more than three dashboard widgets in the same row.
- When displaying similar information in different formats, ensure that each format brings value.
- Stack-related dashboards together for easier viewing.
- Give the dashboard widgets descriptive names. Do not use field names in widget titles.
- Ensure that each dashboard widget contains information or links about what the chart shows and why it is important. The notes should answer questions such as, "Why is the widget important?" and "Where can additional information be found?".

Queries

- Every query has at least one full-text keyword and ideally three or more keywords.
- Queries are not based on environment-specific attributes such as source, hostname, or facility.
- Use regular expressions in queries only if keywords and globs are not sufficient. When using regular expressions, provide as many keywords as possible.
- Make queries as specific as possible. Content pack queries should only match events applicable to the product or application for which the content pack was designed.

Field extraction

- Use additional context filters on fields to improve field performance in queries.
- Minimize the number of regular expressions that are used, whenever possible.
- Verify that a regular expression value matches every applicable log message.
- Provide as much pre and post keyword context as possible.
- Every field has at least one full-text keyword and ideally three or more keywords.
- Fields are specific to a product or application and do not return results for other product or application logs.
- Whenever possible, use agents for log collection. Use agents for the parsing of fields instead of field extraction after ingestion.

Field naming

- Use the following naming standard: `Prefix_Field_Name`. The prefix should be applicable to the content pack.
- Use all lowercase letters.
- Use keywords in the additional context of the field to improve the field performance in queries.

Filters

- When using filters, do not use the match "any" operator unless one or more keywords are defined in the search bar. "any" means that each filter is a separate query. For example, when three filters are used with the "any" operator in a query, the query is treated as three queries. More queries lead to slower results. You can think of "any" as "or" and "all" as the "and" operator.
- When using the text filter with multiple different values, ensure that one or more keywords are defined in the search bar.

Content pack information

- When exporting a content pack, use the naming format *Company – Product* v*Version*. Ideally, the content pack name must be fewer than 30 characters to prevent word wrapping.
- When exporting with a namespace, use the namespace format *Ext.Domain.Product*.
- When exporting a content pack, export with a detailed description of the product that the content pack addresses and how the content pack helps monitor the product.
- Add information to the Setup Instructions section of a content pack. These instructions help the end user set up and use the content pack.
- Add information in the Upgrade Instructions section of a content pack. These instructions help the end user understand and use all the features in the upgraded version of the content pack.
- Provide detailed information about the tested versions of the product or device for which the content pack is designed.
- By default, it is assumed that content packs are backward compatible for all supported versions of the product or device, and new versions of the content pack will not interrupt with the previous configurations after a content pack update from the Marketplace. If not, ensure that you deliver a separate content pack.
- When separating a content pack, ensure that the content packs have different namespaces and there is no possibility to upgrade from the old to the new content pack. Also, support the use of old and new solutions in parallel, without confusing users with incorrect data or extra alerting. Add exceptions to the Release Notes and Known Issues sections for both content packs.
- Give the content pack a version number in the format *Major.Minor.Revision*. The major version is for multiple changes in the content pack, for example one or more new dashboards. The minor version is for a small change, such as a bug fix, a widget type change, or the addition of one or two widgets. The revision is optional and can be used by content pack authors when preparing a new version to send to VMware with the revision set, but might be skipped after publishing the finalized version. Use only two-digit version numbers for content packs.

Agent groups

VMware Aria Operations for Logs supports both syslog forwarded configurations and its own agents for delivering logs. Content packs designed to be used with agent and agent groups templates include suggested configurations. See the instructions of each content pack for more information.

Publishing Requirements

Before you publish a content pack, check if it meets the publishing requirements. Use the content pack publisher on the Developer Center for content pack recommendations and to upload a version for review to VMware. https://developercenter.vmware.com/web/loginsight

Publishing Requirement	Description
Content Pack file format	A `VLCP` file.
Events	The appropriate events necessary to validate the content pack.
Overview	A one to two paragraph overview of the content pack.
Highlights	Three highlights, demonstrating the value of the content pack.
Description	A two to three paragraph description of the content pack and its value.
Tech Specs	Describe the minimum system requirements including Product versions and configuration and VMware Aria Operations for Logs version and configuration. In addition, provide all directions require to configure the product to log to VMware Aria Operations for Logs and populate the content pack.
Screenshots	Three or more screenshots showing the content pack with real data.
Video (Optional)	Example of how the content pack brings value.

Publishing Requirement	Description
White Paper (Optional)	How to configure the product or application to forwards logs to VMware Aria Operations for Logs.

Submit Content Pack

Submit the content pack you created on VMware Solutions Exchange.

- Verify that your content pack meets the Requirements for Publishing Content Packs.
- If you do not have an account on http://solutionexchange.vmware.com, click the **Register** and select **Partner**. Fill out the Partner Registration Request form and submit. You will receive a notification email if your login request is approved.

1. Go to http://solutionexchange.vmware.com and click **Log In Now** in the top right corner of the page.

2. Enter your username and password and click **Log In Now**.

3. Click the **Administration** and choose **Manage Solutions** to add or edit a solution.

4. Click **Add Solution** and fill out the required information.

   Use the **Save Draft** button frequently to make sure that you do not lose any of your work.

5. Click **Submit for Approval**.

   Your solution is sent to the VMware Solution Exchange Alliance Team for review and approval.

You will receive an email regarding the approval status of your solution.

For more information about completing a solution listing click the **Partner Corner** link at the top of the page. If you do not find the information you need, contact VSXAlliance@vmware.com with any questions.

Datastore to Device ID Aliases for vSphere Datastores

maps predefined vSphere datastore names to device IDs. Because of this mapping, you can use datastore names that are aliases for device IDs in queries. The query finds messages with the datastore name or the device ID for which it is aliased. must receive both the key (datastore name) and its value (datastore ID) in messages before the alias can be enabled.

Aliases are defined in the VMware-vSphere content pack. Aliases can be static or dynamic.

Static Aliases

Static aliases are configured by using the following fields:

Field	Description
`aliasFields`	The static mapping of a `value` to a `key` for a given `searchField`.
`name`	The name of the alias field.
`searchField`	The name of the field for which an alias is desired.
`value`	The value of the `searchField` to match.
`key`	The alias to display with events that contain the `searchField`.

Field	Description
definition	A static alias is defined as:

```
"aliasFields":[{
    "name":"vmw_esxi_scsi_host_status",
    "searchField":"vmw_esxi_scsi_host_status_label",
    "aliases":[{
        "key":"OK",           "value":"0x0"},{
        "key":"NO_CONNECT",   "value":"0x1"},{
        "key":"BUS_BUSY",     "value":"0x2"},{
        "key":"TIME_OUT",     "value":"0x3"},{
        "key":"BAD_TARGET",   "value":"0x4"},{
        "key":"ABORT",        "value":"0x5"},{
        "key":"PARITY",       "value":"0x6"},{
        "key":"ERROR",        "value":"0x7"},{
        "key":"RESET",        "value":"0x8"},{
        "key":"BAD_INTR",     "value":"0x9"},{
        "key":"PASSTHROUGH",  "value":"0xa"},{
        "key":"SOFT_ERROR",   "value":"0xb"
    }]
},{
    "name":"vmw_esxi_scsi_device_status",
    "searchField":"vmw_esxi_scsi_device_status_la-
bel",
    "aliases":[{
        "key":"GOOD",                 "val-
ue":"0x0"},{
        "key":"CHECK CONDITION",      "val-
ue":"0x2"},{
        "key":"CONDITION MET",        "val-
ue":"0x4"},{
        "key":"BUSY",                 "val-
ue":"0x8"},{
        "key":"RESERVATION CONFLICT", "val-
ue":"0x18"},{
        "key":"TASK SET FULL",        "val-
ue":"0x28"},{
        "key":"ACA ACTIVE",           "val-
ue":"0x30"},{
        "key":"TASK ABORTED",         "value":"0x40"
    }]
},{
    "name":"vmw_esxi_scsi_sense_code",
    "searchField":"vmw_esxi_scsi_sense_label",
    "aliases":[{
        "key":"NO SENSE",         "value":"0x0"},{
        "key":"RECOVERED ERROR",  "value":"0x1"},{
        "key":"NOT READY",        "value":"0x2"},{
        "key":"MEDIUM ERROR",     "value":"0x3"},{
        "key":"HARDWARE ERROR",   "value":"0x4"},{
        "key":"ILLEGAL REQUEST",  "value":"0x5"},{
        "key":"UNIT ATTENTION",   "value":"0x6"},{
        "key":"DATA PROTECT",     "value":"0x7"},{
        "key":"BLANK CHECK",      "value":"0x8"},{
        "key":"VENDOR SPECIFIC",  "value":"0x9"},{
        "key":"COPY ABORTED",     "value":"0xA"},{
        "key":"ABORTED COMMAND",  "value":"0xB"},{
        "key":"VOLUME OVERFLOW",  "value":"0xD"},{
        "key":"MISCOMPARE",       "value":"0xE"
    }]
```

Dynamic Aliases

Dynamic aliases are configured by using the following fields:

Field	Description
aliasRules	The dynamic mapping of a *valueField* to a *keyField* for *associatedFields*.
name	A unique name to identify the alias (internal only).
keyField	The field for which a dynamic alias should be mapped against.
valueField	A second field in the same event as the *keyField* that provides the alias value.
aliasFieldName	The name of the alias field to be shown next to the events that contain the *keyField*.
associatedFields	The field or fields for which the *aliasFieldName* should appear.

Field	Description

definition	A dynamic alias is defined as:
	
	``
	"aliasRules":[{
	    "name":"DatastoreFromVmFileSystem",
	    "filter":"hostd VmFileSystem Label headExtent
	 naa*",
	    "keyField":"vmw_esxi_device_id",
	    "valueField":"vmw_esxi_vmfs_label",
	    "aliasFieldName":"vmw_esxi_vmfs_name",
	    "associatedFields":[
	        "vmw_esxi_device_id"
	    ]
	},{
	    "name":"DatastoreFromScsiCorrelator",
	    "filter":"scsiCorrelator storage Datastores
	 naa*",
	    "keyField":"vmw_esxi_device_id",
	    "valueField":"vmw_esxi_datastore",
	    "aliasFieldName":"vmw_esxi_datastore_name",
	    "associatedFields":[
	        "vmw_esxi_device_id"
	    ]
	}],
	``
	
	For the dynamic alias fields to function, requires specific messages to be logged to build the aliases.
	
	• For the *vmw_esxi_vmfs_name* field to work correctly, must first receive a log message similar to:
	
	``
	016-10-22T00:50:00.042Z host001.corp.local Hostd:
	 info hostd[5179FB70] [Originator@6876 sub=Libs]
	VmFileSystem: uuid:57925c06-0a8a627e-9f0b-
	b82a72d50b06, Label:datastore001,logicalDe-
	vice:57925c05-63b188db-37da-b82a72d50b06, headEx-
	tent:naa.6b083fe0c212bd001f22e05d07099022:1
	``
	
	The query used to match this event is `hostd VmFileSystem Label headExtent naa*`. For every unique *vmw_esxi_device_id* field value found, maps the value of the *vmw_esxi_vmfs_label* field to the *vmw_esxi_vmfs_name* field. In this example, the *vmw_esxi_device_id* field is "naa.6b083fe0c212bd001f22e05d07099022" and the *vmw_esxi_vmfs_label* field is "datastore001". After this event is logged, running a query with a filter in which the *vmw_esxi_vmfs_name* field contains a datastore name returns log messages that contain "naa.6b083fe0c212bd001f22e05d07099022".
	
	• For the *vmw_esxi_datastore_name* field to work correctly, must first receive a log message similar to:
	
	``
	2016-11-24T03:56:47.738Z host002.corp.local vobd:
	  [scsiCorrelator] 4851129307827us: [esx.clear.s-
	torage.redundancy.restored]
	Path redundancy to storage device
	 naa.6006016006502a004b1c42e756fbe411 (Data-
	stores: "datastore002") restored. Path vmh-
	ba39:C0:T1:L2 is active again.
	``
	
	The query used to match this event is `scsiCorrelator storage Datastores naa*`. For every unique value found in the *vmw_esxi_device_id* field, maps the value of the *vmw_esxi_datastore* field to the *vmw_esxi_datastore_name* field. In this example, the *vmw_esxi_device_id* field is "naa.6006016006502a004b1c42e756fbe411" and the *vmw_esxi_datastore* field is "datastore002". After this event is logged, running a query with a filter in

<u>**Requirements for Aliases**</u>

To use aliases, ensure that:

- You are using 4.0 or later.
- You are using the VMware - vSphere content pack 4.0 or later. includes this content pack.
- ESXi is configured to send logs to .
- There is a minimum gap of five minutes after the first event that contains both the key and value goes through the ingestion pipeline.

<u>**Restrictions for Aliases**</u>

The following restrictions apply to the use of aliases:

- You cannot use aliases with mathematical functions, for example, avg, min, max, and so on.
- You cannot use aliases with the "exists" and "does not exist" operators.
- Aliases are not forwarded as a part of log forwarding.
- Up to 100,000 aliases can be learned per node, after which they are rotated out in a FIFO manner.

Configuring Log Sources

Log sources generate log data that VMware Aria Operations for Logs can ingest and analyze. You can find the information for configuring a log source under the **Log Sources** section.

Agents such as VMware Aria Operations for Logs Agents and Fluentd support data collection from the log sources.

- A VMware Aria Operations for Logs agent collects log events from log files and forwards the logs to a VMware Aria Operations for Logs server using cfapi or syslog protocols, or to any third-party syslog destination.
- Fluentd is an open source data collector integrated with VMware Aria Operations for Logs, which lets you unify the data collection and consumption for a better understanding of the data. You can collect logs from log sources such as Docker and Kubernetes through Fluentd.

  The configuration for these log sources uses the Fluentd output plug-in fluent-plugin-vmware-loginsight. For more information, see https://github.com/vmware/fluent-plugin-vmware-loginsight. This plug-in parses logs based on the log source configuration and forwards logs to VMware Aria Operations for Logs. You can configure cfapi or syslog protocols using the plug-in. For information about the plug-in configuration, see https://github.com/vmware/fluent-plugin-vmware-loginsight/blob/master/README.md.

For information about configuring an agent, navigate to **Log Sources > Agents** and click the agent.

To view the installation instructions for a log source, navigate to **Log Sources > Containers** and click the log source.

> **NOTE**
> Oracle Cloud VMware Solution (OCVS) lets you create and manage VMware-enabled SDDCs in Oracle Cloud Infrastructure, hence providing infrastructure as a service. OCVS uses the scale and flexibility of the public cloud, while providing a private cloud-like operating environment. VMware Aria Operations for Logs can be used to monitor ESXi hosts deployed to the OCVS infrastructure.

Alerts in VMware Aria Operations for Logs

VMware Aria Operations for Logs provides built-in system alerts for critical issues. You can also configure VMware Aria Operations for Logs to run specific queries at scheduled intervals.

System Alerts

System alerts contain information about activities related to VMware Aria Operations for Logs's health, such as when the disk space is almost exhausted and old log files are about to be deleted. For information about managing the notifications for these alerts, see Managing System Notifications.

To view the list of system alerts and information about their status and frequency, expand the main menu and navigate to the **Alerts > System Alerts**. You can activate or deactivate system alerts.

User-Defined Alerts

You can define alerts in VMware Aria Operations for Logs and send email or webhook notifications, or trigger notification events in VMware Aria Operations if the number of events that match the query exceeds the thresholds that you have set.

To view the list of user-defined alerts and information about their status, owner, origin, and so on, navigate to **Alerts > Alerts Definition**.

> **NOTE**
>
> - If your user account is assigned a role with view access to alerts, you can view all the alerts in your organization . However, you can manage only your own alerts.
> - If your user account is assigned a role with edit or full access to alerts:
>   - You can activate or deactivate all the system alerts in your organization.
>   - You can create, modify, and remove all the user-defined alerts in your organization. For example, a user with a Super Admin role can manage the alerts of other users.
>
> For information about roles, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*

Content Pack Alerts

Content packs can contain alert queries. The vSphere content pack that is included in VMware Aria Operations for Logs by default contains several predefined alert queries. They can trigger alerts if an ESXi host stops sending syslog data, if VMware Aria Operations for Logs can no longer collect events, tasks, and alarms data from a vCenter Server, or when an alarm status changes to red. You can use these alert queries as templates to create alerts that are specific to your environment.

All content pack alerts are deactivated by default.

Enabling the **ESX/ESXi stopped logging** alert is a good practice, because certain versions of ESXi hosts might stop sending syslog data when you restart VMware Aria Operations for Logs. This alert monitors for the vCenter Server event `esx.problem.vmsyslogd.remote.failure` to detect whether there is an ESXi host that has stopped sending syslog feeds. For details about syslog problems and solutions, see VMware ESXi 5.x host stops sending syslogs to remote server (2003127).

You can add the following filter to the alert query and save it as a new alert to detect only ESXi hosts that stop sending feeds to your instance of VMware Aria Operations for Logs: **vc_remote_host (VMware - vSphere)contains** `log-insight-hostname`.

If your user account is assigned a role with full access for content packs and alerts, you can activate a content pack alert and modify its notifications. However, you cannot update or remove the content pack alert.

Define an Alert

You can define an alert in VMware Aria Operations for Logs and send email or webhook notifications, or trigger notification events in VMware Aria Operations if the number of events that match the alert query exceeds the thresholds that you have set.

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface, for which the URL format is https://*operations_for_logs-host*. Here, *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Verify that your user account is associated with a role that has the relevant permissions for alerts.

  If your user account is assigned a role with view access to alerts (for example, the User role), you can view and manage all the alerts in your organization.

  If your user account is assigned a role with edit or full access to alerts (for example, the Super Admin role):

  - You can activate or deactivate all the system alerts in your organization.
  - You can create, modify, and remove all the user-defined alerts in your organization.

  For information about roles, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*.

1. Expand the main menu and navigate to **Alerts > Alerts Definition**.

2. Click **Create New**.

   > **TIP**
   > Alternatively you can navigate to the **Explore Logs** page and create an alert based on a query. Enter a query, and next to the **Search** button, click 🔔 and select **Create Alert from Query**.

3. Enter a name for the alert.

   You can customize the alert name by including a field in the format `${ field name}` . For example, you can enter the alert name as `Alert for ${hostname} VPXA Logs`. Assuming that there are two host names and you have set up email notifications for the alert, the email subject looks like this:

   ```
   Alert for "hostname loginsight-01.eng.vmware.com and 1 more" VPXA Logs
   ```

   You can use other static fields in the description, such as *event_type*, *source*, *filepath*, and so on. You can also use extracted fields.

   > **NOTE**
   > - You can add only one static or extracted field to the alert name.
   > - If you use an extracted field in the alert name, it must be a part of the alert query. If the alert has a "Group by" condition, the extracted field must also be a part of the "Group by" condition.
   > - If you are sending notifications to VMware Aria Operations, one notification event is sent for each field. For example, if your alert name contains `${hostname}` and there are five host names, five notification events are sent - one for each host name.

4. Enter a short meaningful description of the event that triggers the alert.

   You can customize the alert description by including one or more fields in the format `${ field name}` . For example, you can enter the alert description as `VPXA logs were generated for ${hostname}`. Assuming that there are two host names and you have set up email notifications for the alert, the email lists some sample logs and then displays the following information:

   ```
   Additional notes for this alert:
   VPXA logs were generated for
   hostname
   loginsight-01.eng.vmware.com
   ```

```
loginsight-02.eng.vmware.com
```

You can use other static fields in the description, such as *event_type*, *source*, *filepath*, and so on. You can also use extracted fields.

> **NOTE**
> - You can use only one static or extracted field in the alert description.
> - If you use an extracted field in the alert name, it must be a part of the alert query. If the alert has a "Group by" condition, the extracted field must also be a part of the "Group by" condition.

5. Enter the query on which the alert is based.

6. Enter the trigger condition for the alert. You can select a time period and group the query results by static or extracted fields.

Trigger Condition	Description
On every match **NOTE** You can set this trigger condition when you select **Real Time** in the time period drop-down menu.	The alert query runs automatically every minute. A notification is triggered when at least one event within the last minute matches the query.
Total count of events	A notification is triggered when more or less than X matching events occur within the time period that you select from the drop-drown menu. If this type of alert is triggered, it is snoozed for the duration of its time period to prevent duplicate alerts from being raised for the same set of events. If you want to activate an alert while it is snoozing, you can deactivate and then re-activate it.
Unique count of a field	A notification is triggered when the unique count of field F is more or less than X, within the time period that you select from the drop-drown menu.
Aggregation operation on a field	A notification is triggered when the aggregation operation A applied on the field F is more or less than X, within the time period that you select from the drop-drown menu.

You can configure the alert to send notifications based on the trigger condition.

- To send email notifications, enter comma-separated recipient email addresses.
  Ensure that SMTP is configured to activate email notifications. For more information, Configure the SMTP Server.
- For information about sending webhook notifications, see Add an Alert to Send Webhook Notifications.
- For information about sending notifications to VMware Aria Operations, see Add an Alert to Send Notifications to VMware Aria Operations.

7. Optional: Enter a recommendation for the alert, which is included in the notification message when the alert is sent.

8. Optional: To send a test alert notification, click **Send Test Alert**.

9. Click **Save**.

Your alert definition appears in the Alerts Definition page.
You can activate, deactivate, or modify the alert.
Related Links

You can configure alerts in VMware Aria Operations for Logs to send webhook notifications to a remote web server when specific data appears in the logs. Webhooks provide event notifications over HTTP POST/PUT.

You can configure alerts in VMware Aria Operations for Logs to send notification events to VMware Aria Operations when specific VMware Aria Operations for Logs alert queries return results beyond a given threshold.

You can view system and user-defined alerts and check whether their notifications are activated. You can activate or deactivate multiple system and user-defined alerts, and set up email and webhook notifications for multiple user-defined alerts. You can also view the history of user-defined alerts.

You can change the trigger conditions for an alert, activate or deactivate alert notifications, or change the alert notification method (email, webhook, or send to VMware Aria Operations).

Add an Alert to Send Webhook Notifications

You can configure alerts in VMware Aria Operations for Logs to send webhook notifications to a remote web server when specific data appears in the logs. Webhooks provide event notifications over HTTP POST/PUT.

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface, for which the URL format is https://*operations_for_logs-host*. Here, *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Verify that your user account is associated with a role that has the relevant permissions for alerts.
  If your user account is assigned a role with view access to alerts (for example, the User role), you can view and manage all the alerts in your organization.
  If your user account is assigned a role with edit or full access to alerts (for example, the Super Admin role):

  - You can activate or deactivate all the system alerts in your organization.
  - You can create, modify, and remove all the user-defined alerts in your organization.

  For information about roles, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*.

Also, verify that a web server has been configured to receive webhook notifications. For more information, see Configure a Webhook.

The content of the webhook notification contains a maximum of up to 200 events that meet the alert query criteria. In aggregated queries, the content contains up to a maximum of 200 groups that meet the alert criteria. The content contains the total number of events and groups and a link to the **Explore Logs** page. This page displays all the events or groups of events.

> **NOTE**
> The server might report a success or failure. VMware Aria Operations for Logs retries on failure. VMware Aria Operations for Logs treats all HTTP/2xx status code responses as successful. All other responses, including timeouts or refused connections, are considered failed and retried later.

1. Expand the main menu and navigate to **Alerts > Alerts Definition**.

2. Click **Create New**.

   > **TIP**
   > Alternatively you can navigate to the **Explore Logs** page and create an alert based on a query. Enter a query, and next to the **Search** button, click 🔔 and select **Create Alert from Query**.

3. Enter the alert name, description, and trigger condition as described in Define an Alert.
   The alert name and description are included in the notification that VMware Aria Operations for Logs sends.

4. From the **Select Webhook** drop-down menu, select a webhook.

5. Click **Save**.

You can activate, deactivate, or modify the alert.

Related Links

You can define an alert in VMware Aria Operations for Logs and send email or webhook notifications, or trigger notification events in VMware Aria Operations if the number of events that match the alert query exceeds the thresholds that you have set.

You can configure alerts in VMware Aria Operations for Logs to send notification events to VMware Aria Operations when specific VMware Aria Operations for Logs alert queries return results beyond a given threshold.

You can view system and user-defined alerts and check whether their notifications are activated. You can activate or deactivate multiple system and user-defined alerts, and set up email and webhook notifications for multiple user-defined alerts. You can also view the history of user-defined alerts.

You can change the trigger conditions for an alert, activate or deactivate alert notifications, or change the alert notification method (email, webhook, or send to VMware Aria Operations).

Add an Alert to Send Notifications to VMware Aria Operations

You can configure alerts in VMware Aria Operations for Logs to send notification events to VMware Aria Operations when specific VMware Aria Operations for Logs alert queries return results beyond a given threshold.

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface, for which the URL format is https://*operations_for_logs-host*. Here, *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Verify that your user account is associated with a role that has the relevant permissions for alerts.
  If your user account is assigned a role with view access to alerts (for example, the User role), you can view and manage all the alerts in your organization.
  If your user account is assigned a role with edit or full access to alerts (for example, the Super Admin role):

  - You can activate or deactivate all the system alerts in your organization.
  - You can create, modify, and remove all the user-defined alerts in your organization.

  For information about roles, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*.

Also, verify that the connection between VMware Aria Operations for Logs and VMware Aria Operations is configured to activate alert integration. See Configure Log Insight to Send Notification Events to VMware Aria Operations.

Notification events that VMware Aria Operations for Logs generates are associated with resources in VMware Aria Operations. You can read more about resources in the *VMware Aria Operations Getting Started Guide (Custom UI)*.

> **NOTE**
> Several minutes are required for notification events to appear in the VMware Aria Operations user interface.

1. Expand the main menu and navigate to **Alerts > Alerts Definition**.

2. Click **Create New**.

   > **TIP**
   > Alternatively you can navigate to the **Explore Logs** page and create an alert based on a query. Enter a query, and next to the **Search** button, click 🔔 and select **Create Alert from Query**.

3. Enter the alert name, description, and trigger condition as described in Define an Alert.
   The alert name and description are included in the notification event that VMware Aria Operations for Logs sends.

4. Select **Send to** VMware Aria Operations.

5. From the **Fallback Object** drop-down menu, select a fallback object.

   When integrated with VMware Aria Operations, alerts are sent as notifications to the virtual machines, ESXi hosts, or vCenter Server objects that caused the alert. Alerts raised by other entities are sent to the selected fallback object.

6. Optional: From the **Criticality** drop-down menu, select the criticality level for the notification events that appear in the VMware Aria Operations custom user interface.

7. Optional: To cancel the alert in VMware Aria Operations if it is not triggered within a certain period, select the **Auto Cancel** check box and enter the cancellation period.

8. Click **Save**.

When the alert query returns results that match the alert criteria, a notification event is sent to VMware Aria Operations. Alert queries run on a predefined schedule and are triggered only once for a given threshold time range.

The locations of the notification events depend on the VMware Aria Operations user interface that you use. See VMware Aria Operations for Logs Notification Events in VMware Aria Operations.

Configure a Notification Alert to VMware Aria Operations

Assume that in VMware Aria Operations, you have a virtual machine resource named `vm-abc`. You have configured VMware Aria Operations for Logs to pull events from the vCenter Server system where the virtual machine `vm-abc` runs. You want to receive a notification in VMware Aria Operations each time the `vm-abc` virtual machine is powered off. Here is how to configure VMware Aria Operations for Logs to send these notification events to VMware Aria Operations.

1. In the search text box in the **Explore Logs** page, enter `Power Off virtual machine.`
2. Click **Add a Filter**, select **vc_vm_name**.
3. Click **Search**.

   If the `vm-abc` virtual machine has been powered off during the selected time range, the search returns all instances that occurred.
4. From the drop-down menu on the right of the **Search** button, select **Create Alert from Query**.
5. Enter a name and description for the alert.
6. Under Trigger Conditions, select **Real Time** from the time period drop-down menu.
7. Select **Send to vROps**.
8. From the **Fallback Object** drop-down menu, select **vm-abc**.
9. Modify the criticality level that is displayed in the VMware Aria Operations custom user interface.
10. Select an auto-cancel setting and cancellation period.
11. Click **Save**.

VMware Aria Operations for Logs polls the vCenter Server system at five-minute intervals. If the query returns a new power off virtual machine task from the virtual machine `vm-abc`, VMware Aria Operations for Logs sends a notification event that is associated with the `vm-abc` resource in VMware Aria Operations.

You can activate, deactivate, or modify the alert.

Related Links

Define an Alert on page 197

You can define an alert in VMware Aria Operations for Logs and send email or webhook notifications, or trigger notification events in VMware Aria Operations if the number of events that match the alert query exceeds the thresholds that you have set.

Add an Alert to Send Webhook Notifications on page 199

You can configure alerts in VMware Aria Operations for Logs to send webhook notifications to a remote web server when specific data appears in the logs. Webhooks provide event notifications over HTTP POST/PUT.

View and Manage Alerts on page 202

You can view system and user-defined alerts and check whether their notifications are activated. You can activate or deactivate multiple system and user-defined alerts, and set up email and webhook notifications for multiple user-defined alerts. You can also view the history of user-defined alerts.

You can change the trigger conditions for an alert, activate or deactivate alert notifications, or change the alert notification method (email, webhook, or send to VMware Aria Operations).

View and Manage Alerts

You can view system and user-defined alerts and check whether their notifications are activated. You can activate or deactivate multiple system and user-defined alerts, and set up email and webhook notifications for multiple user-defined alerts. You can also view the history of user-defined alerts.

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface, for which the URL format is https://*operations_for_logs-host*. Here, *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Verify that your user account is associated with a role that has the relevant permissions for alerts.

  If your user account is assigned a role with view access to alerts (for example, the User role), you can view and manage all the alerts in your organization.

  If your user account is assigned a role with edit or full access to alerts (for example, the Super Admin role):

  - You can activate or deactivate all the system alerts in your organization.
  - You can create, modify, and remove all the user-defined alerts in your organization.

  For information about roles, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*.

- To view system alerts, navigate to **Alerts > System Alerts**.

  You see a list of system alerts with information about their status and frequency. You can activate or deactivate individual alerts by using the toggle button against each alert. To activate or deactivate multiple alerts, select the alerts and then select **Actions > Enable** or **Actions > Disable**.

  > **TIP**
  > To select all the alerts, click the check box in the header.

- To view user-defined alerts, navigate to **Alerts > Alerts Definition**.

  You see a list of user-defined alerts with information about their status, owner, origin, and target. For content pack alerts, the content pack name is listed in the **Origin** column. You can perform the following tasks:

  - Search for alerts by using the text search.
  - Filter alerts by origin or alert type and click **Apply**.

    When you filter alerts by origin, you can select user-defined, general alerts, or alerts for specific content packs.

    When you filter alerts by alert type, you can select real-time alerts, which are alerts based on every match. You can also select count-based alerts, which are alerts based on the total count of events, unique count of a field, or aggregation operation on a field.
  - Sort alerts by alert details, status, owner, and so on.
  - Add or remove columns to control the alert information displayed. Click the **Show or hide columns** icon in the lower left corner and select or clear columns according to your requirement.

    > **TIP**
    >
    > - The value in the **Owner** column is the name of the user who defines the alert. For content pack alerts, this value is blank or **System**.
    >   For alerts created in VMware Aria Operations for Logs 8.4 or earlier, the value in the **Owner** column is a user assigned to the **Super Admin** role.
    > - The value in the **Last Hit** column remains **never** until the first hit occurs.
- Activate or deactivate individual alerts by using the toggle button against each alert.

- Activate or deactivate multiple alerts by following these steps.
    - To activate multiple alerts, select the alerts and then select **Actions > Enable**. In the **Enable Alerts** dialog box, you can set up email or webhook notifications for the selected alerts and click **Enable**.
      To send email notifications, in the **Emails** text box, enter comma-separated recipient email addresses.

        > **NOTE**
        > Ensure that SMTP is configured to activate email notifications. For more information, see Configure the SMTP Server for Log Insight.

      To send webhook notifications, from the **Webhook** drop-down menu, select webhooks.
    - To deactivate multiple alerts, select the alerts and then select **Actions > Disable**.

        > **TIP**
        > To select all the alerts, click the check box in the header.
- View the history of an alert. To view the history of an alert, click the three dots icon against the alert and click **History**.
  In the **Alert History** dialog box, you can see the alert instances associated with the alert, along with the date and time for each alert instance. You can expand each alert instance for additional information and click the link icon to view the instance in the **Explore Logs** page.
- View the log results for the query associated with an alert. Click the alert and then click **Run Query** to open the query in Explore Logs.
- Modify an alert.
- Remove one or more alerts. To remove an alert, click the three dots icon against the alert and click **Delete**. To remove multiple alerts, select the alerts and then select **Actions > Delete**.
- To view content pack alerts, navigate to the **Content Packs** page. On the left pane, click a content pack and then click the **Alerts** tab.

If your user account is assigned a role with full access for content packs and alerts, you can activate a content pack alert and modify its notifications on the Alerts page. However, you cannot update or remove the content pack alert.

Activate an Alert from the VMware - vSphere Content Pack

The VMware vSphere content pack contains several predefined alert queries, including the **ESXi: Stopped logging** alert. Enabling the **ESXi: Stopped logging** alert is a good practice, because certain versions of ESXi hosts might stop sending syslog data when you restart VMware Aria Operations for Logs. This alert monitors for the vCenter Server event `esx.problem.vmsyslogd.remote.failure` to detect if there is an ESXi host that has stopped sending syslog feeds.

1. Navigate to **Alerts > Alerts Definition**.
2. Search for the VMware - vSphere content pack alert ***** CRITICAL *** ESXi: Stopped logging** and click the alert name.
3. Click the **Edit** icon in the upper-right corner.
4. Activate email notifications, webhook notifications, or VMware Aria Operations notification events.
5. Click **Enable**.

To detect only ESXi hosts that stop sending feeds to your instance of VMware Aria Operations for Logs, you can add the following filter to the alert query: **vc_remote_host (VMware - vSphere)contains**`<operations_for_logs-hostname>`, and save the new query to your alerts. For details about syslog problems and solutions, see the Knowledge Base article VMware ESXi 5.x host stops sending syslogs to the remote server (2003127) at https://kb.vmware.com/kb/2003127.

Related Links

You can define an alert in VMware Aria Operations for Logs and send email or webhook notifications, or trigger notification events in VMware Aria Operations if the number of events that match the alert query exceeds the thresholds that you have set.

You can configure alerts in VMware Aria Operations for Logs to send webhook notifications to a remote web server when specific data appears in the logs. Webhooks provide event notifications over HTTP POST/PUT.

You can configure alerts in VMware Aria Operations for Logs to send notification events to VMware Aria Operations when specific VMware Aria Operations for Logs alert queries return results beyond a given threshold.

You can change the trigger conditions for an alert, activate or deactivate alert notifications, or change the alert notification method (email, webhook, or send to VMware Aria Operations).

Modify an Alert

You can change the trigger conditions for an alert, activate or deactivate alert notifications, or change the alert notification method (email, webhook, or send to VMware Aria Operations).

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface, for which the URL format is https://*operations_for_logs-host*. Here, *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Verify that your user account is associated with a role that has the relevant permissions for alerts.
  If your user account is assigned a role with view access to alerts (for example, the User role), you can view and manage all the alerts in your organization.
  If your user account is assigned a role with edit or full access to alerts (for example, the Super Admin role):

  - You can activate or deactivate all the system alerts in your organization.
  - You can create, modify, and remove all the user-defined alerts in your organization.

  For information about roles, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*.

Also, verify the following for email, webhook, and VMware Aria Operations notifications:

- Verify that SMTP is configured to activate email notifications. See Configure the SMTP Server for VMware Aria Operations for Logs.
- If you are using webhooks, verify that a web server has been configured to receive webhook notifications. See Configure a Webhook.
- Verify that the connection between VMware Aria Operations for Logs and VMware Aria Operations is configured to activate alert integration. See Configure VMware Aria Operations for Logs to Send Notification Events to VMware Aria Operations.

  NOTE

  If your user account is assigned a role with full access for content packs and alerts, you can activate a content pack alert and modify its notifications. However, you cannot update or remove the content pack alert.

1. Expand the main menu and navigate to **Alerts > Alerts Definition**.

2. Locate the alert that you want to modify. You can search for the alert by entering keywords in the search text box or by using the sort or filter functionalities.

3. Click the three dots icon against the alert and click **Edit**.

4. Modify the alert as required.

   NOTE
   If you clear all the notification options, the alert is deactivated.

5. Click **Save**.

Related Links

You can define an alert in VMware Aria Operations for Logs and send email or webhook notifications, or trigger notification events in VMware Aria Operations if the number of events that match the alert query exceeds the thresholds that you have set.

You can configure alerts in VMware Aria Operations for Logs to send webhook notifications to a remote web server when specific data appears in the logs. Webhooks provide event notifications over HTTP POST/PUT.

You can configure alerts in VMware Aria Operations for Logs to send notification events to VMware Aria Operations when specific VMware Aria Operations for Logs alert queries return results beyond a given threshold.

You can view system and user-defined alerts and check whether their notifications are activated. You can activate or deactivate multiple system and user-defined alerts, and set up email and webhook notifications for multiple user-defined alerts. You can also view the history of user-defined alerts.

Schedule a Report

You can schedule a report to analyze the data in dashboard widgets.

Verify that your user account is associated with a role that has **Edit** permissions for **Dashboards > Scheduled Reports**. For information about roles, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*.

1. Expand the main menu and navigate to **Reports**.

2. Click **Schedule Report**.

> **TIP**
> Alternatively you can open a dashboard from the **Dashboards** page and click the **Schedule Report** icon in the upper-right corner of the page.

3. Enter a name for the report.

4. From the **Dashboard Select** drop-down menu, select the dashboard for which you want to schedule the report.

5. From the **Dashboard Duration** drop-down menu, select a period of 5 minutes, 10 minutes, 30 minutes, 1 hour, or a custom period.

   This period determines the duration within which the dashboard data is used to generate the report, till the **Schedule Time**.

   For example, if you select a **Dashboard Duration** of 10 minutes and a **Schedule Time** of 08:30, the report is scheduled based on the dashboard data from 08:20 to 08:30.

6. In the **Schedule Time**, select the date, time, and recurrence to schedule the report.

   You can set the frequency of the report to a single day of a week or month, or a range of days. The following report is sent to recipients on the 1st and 30th of every third month starting from the set date. As the report is scheduled from

the 07th of July, the recipients will receive the first report on the 30th of July, followed by 1st and 30th of October, and so on.

7. Under **Notify**, enter comma-separated recipient email addresses to send email notifications for the report.

   For all enabled report configurations, the reports are generated and sent to corresponding recipients based on the provided schedule and for the specified dashboard.

   > **NOTE**
   >
   > Ensure that SMTP is configured to enable email notifications. For more information, see Configure the SMTP Server for Log Insight.

8. Optional: To send a test report notification, click **Send Test Report**.

9. Click **Save**.

Your report appears in the **Reports** page.

The actual report is sent to the recipients based on the schedule as a PDF attachment. For example, let us consider a report schedule with a dashboard duration of 10 minutes and a schedule configured for every 5 days with a start time of 15:30. The report is sent every 5 days at 15:30 as a PDF attachment. The attachment contains information for the specified dashboard within the selected dashboard duration, which is from 15:20 to 15:30.

> **NOTE**
>
> Field table, Event types, and Event trends widgets are not supported in scheduled reports. When the report is generated for a dashboard containing unsupported widgets, the report displays Widget type not supported in the PDF file.

You can enable, deactivate, or modify the report. See View and Manage Reports.

View and Manage Reports

You can view reports, activate or deactivate one or multiple reports, set up email notifications for reports, and modify reports.

Verify that your user account is associated with a role that has the relevant permissions for reports. For information about roles, see Create and Modify Roles in *Administering VMware Aria Operations for Logs*.

To view or modify reports, expand the main menu and click **Reports**. In the **Reports** page, you see a list of reports with information about their status, email recipients, and so on. For reports related to content pack dashboards, the content pack name is listed in the **Content Packs** column. You can perform the following tasks:

* Search for reports by using the text search.
* Filter reports by content type or stage and click **Apply**.

  When you filter reports by content type, you can select user dashboards, shared dashboards, or dashboards for specific content packs.

When you filter reports by stage, you can select activated or deactivated reports.

- Sort reports by report details, status, dashboard, and so on.
- Activate or deactivate individual reports by using the toggle button against each report.
- Activate or deactivate multiple reports by following these steps.

  - To activate multiple reports, select the reports and then select **Actions > Enable**. In the **Enable Reports** dialog box, you can set up email notifications for the selected reports and click **Enable**.
    To send email notifications, in the **Emails** text box, enter comma-separated recipient email addresses.

      > **NOTE**
      > Ensure that SMTP is configured to activate email notifications. For more information, see Configure the SMTP Server for Log Insight.
  - To deactivate multiple reports, select the reports and then select **Actions > Disable**.

      > **TIP**
      > To select all the reports, click the check box in the header.
- Modify a report. Click the report name and then click the **Edit** icon in the upper-right corner.
- Remove one or more reports. To remove a report, click the three dots icon against the report and click **Delete**. To remove multiple reports, select the reports and then select **Actions > Delete**.

Viewing Usage Reports

Usage reports show the volume of log data ingested and stored in VMware Aria Operations for Logs.

You can view usage reports when you expand the main menu and click **Management** > **Usage Reports**.

Ingestion & Storage

This tab displays details about the amount of log data streamed into the system, the log volume in storage, and the log volume in archive for the last 7-30 days. You can select the period for which the data is displayed. You must select a minimum period of seven days. You can select up to a maximum period of 30 days.

Summary

This section displays the following information:

Information	Description
Ingestion Volume	The volume of logs ingested within the selected period.
Storage Volume	The volume of logs stored in VMware Aria Operations for Logs within the selected period.
Archived Volume	The volume of logs archived within the selected period.

Ingestion & Storage

This chart displays the volume of logs ingested daily within the selected period. You can view the volume of ingested logs and stored logs.

Storage by partitions

This chart displays the volume of all partitions that contain data.

To download a report of the ingestion and storage within the selected period in CSV format, click **Download CSV** in the upper-right corner of the tab.

Subscribing to VMware Aria Operations for Logs (SaaS)

You can subscribe to VMware Aria Operations for Logs (SaaS) to achieve flexible log consumption and visibility across the data center, the edge, and any cloud.

To subscribe to VMware Aria Operations for Logs (SaaS), go to the **Integrations** > **Operations for Logs (SaaS)** page and click **Request Free Trial**. For more information, see the following topics in *Getting Started with VMware Aria Operations for Logs (SaaS)*:

- Getting Started Checklist for VMware Aria Operations for Logs (SaaS)
- VMware Aria Operations for Logs (SaaS) Subscriptions and Billing

Configuring Non-Indexed Partitions

To view the instructions for configuring non-indexed partitions in VMware Aria Operations for Logs (SaaS), click **Setup Instructions** under **Simplify Log Archival using Non-Index Partitions**.

You can archive logs in non-indexed partitions for up to seven years at a minimal cost. For more information, see Log Partitions in *Using VMware Aria Operations for Logs (SaaS)*.

Configuring Log Sources

To view the information about configuring log sources in VMware Aria Operations for Logs (SaaS), click **Learn More** under **Flexible Consumption with Expanded Support for Log Sources**.

Log sources such as agents, applications, and application development platforms generate logs. Installing log sources lets VMware Aria Operations for Logs (SaaS) ingest and analyze logs from these sources, and provides a single point of visibility across your infrastructure, public clouds, and other third-party application logs. VMware Aria Operations for Logs (SaaS) supports logs across AWS, Azure, and GCP services.

Configuring KB Insights

To view the instructions for viewing KB insights in VMware Aria Operations for Logs (SaaS), click **Setup Instructions** under **Actionable Insights from your Logs with AI/ML Capabilities**.

VMware Aria Operations for Logs (SaaS) uses a combination of processes and machine learning methods to provide insights into logs with errors and exceptions, and suggests solutions for these problems. The suggested solutions utilize the documentation created by various internal and external experts when they solved similar problems in the past. For more information, see Viewing Insights and Solutions in *Using VMware VMware Aria Operations for Logs (SaaS)*.

Administering VMware Aria Operations for Logs (8.14)

Administering VMware Aria Operations for Logs

Administering VMware Aria Operations for Logs provides information about the administration of VMware Aria Operations for Logs, including how to manage user accounts and how to configure integration with other VMware products. It also includes information about managing product security and upgrading your deployment.

The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations. Administrators are users associated with the **Super Admin** role, clones of the **Super Admin** role, or roles that have permissions for the relevant administrative tasks. These roles are defined in the **Management** > **Access Control** page, on the **Roles** tab.

Upgrading VMware Aria Operations for Logs

You can upgrade your current VMware Aria Operations for Logs environment to a later version by following the correct upgrade path.

To download the PAK files for VMware Aria Operations for Logs, go to the Download VMware Aria Operations for Logs page.

> **NOTE**
>
> You must upgrade VMware Aria Operations for Logs from the FQDN of the primary node. You cannot upgrade VMware Aria Operations for Logs using the Integrated Load Balancer IP address.

During the upgrade process, the primary node is upgraded first, and restarted. Each of the cluster nodes is upgraded sequentially. You can see the status of the rolling upgrade on the **Management** > **Cluster** page.

If the integrated load balancer is configured, its IPs are migrated among the cluster nodes so cluster services, including UI, API, and ingestion of incoming events, remain available throughout the rolling upgrade. Low-level details are written to the file `/storage/core/loginsight/var/upgrade.log` on each individual node. A system notification is sent when the upgrade finishes successfully.

After a successful upgrade, all nodes are placed in the connected state and are in the online mode even if they were in maintenance mode before the upgrade.

VMware Aria Operations for Logs Upgrade Path

VMware Aria Operations for Logs supports incremental software upgrades. The upgrade path to follow depends on which version of VMware Aria Operations for Logs is installed and the version you are upgrading to.

You can upgrade VMware Aria Operations for Logs by following the upgrade path:

Table 11: Upgrade path

Version	Upgrade Path
8.14	Upgrade from VMware Aria Operations for Logs version 8.12.x.
8.12	Upgrade from VMware Aria Operations for Logs version 8.10.x.
8.10	Upgrade from VMware Aria Operations for Logs version 8.8.x.
8.8	Upgrade from VMware Aria Operations for Logsversion 8.6.x.
8.6	Upgrade from VMware Aria Operations for Logsversion 8.4.

Version	Upgrade Path
8.4	Upgrade from VMware Aria Operations for Logs version 8.3 or 8.2.
8.1	Upgrade from VMware Aria Operations for Logs version 4.8 or 8.0. For more information, see: • Upgrading to VMware Aria Operations for Logs version 8.1 • Upgrading to VMware Aria Operations for Logs version 8.0
Other versions	Follow the incremental path.

You must upgrade the versions incrementally. For example:

- To upgrade from version 8.10 to 8.14, you must first upgrade VMware Aria Operations for Logs to version 8.12 and then upgrade to version 8.14.
- To upgrade from version 8.8.x to 8.12, you must first upgrade to version 8.10.x and then upgrade to version 8.12.

For supported upgrade paths, see the VMware Product Interoperability Matrix.

Upgrade to the Latest Version of VMware Aria Operations for Logs

You can upgrade to the latest version of VMware Aria Operations for Logs by following incremental software upgrades.

- Verify that you are upgrading to the correct version of VMware Aria Operations for Logs. For more information about the upgrade process, see Upgrading VMware Aria Operations for Logs.
- Create a snapshot or backup copy of the VMware Aria Operations for Logs virtual appliance.
- Obtain a copy of the VMware Aria Operations for Logs upgrade bundle `.pak` file for the release you are upgrading to.
- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Make a note of any nodes you are upgrading that are in the **Maintenance** mode. When the upgrade is finished, you must move them from the state **Connected** to the state **Maintenance**.

To upgrade a cluster to the latest version, you must follow the upgrade path in VMware Aria Operations for Logs Upgrade Path.

1. Expand the main menu and navigate to **Management** > **Cluster**.

2. Click **Upgrade from PAK** to upload the `.pak` file.

3. Accept the new EULA to complete the upgrade procedure.

4. Activate or deactivate VMware's Customer Experience Improvement Program (CEIP) for VMware Aria Operations for Logs.

   - If CEIP was activated in the earlier release of VMware Aria Operations for Logs, no action is required during the upgrade. CEIP remains activated after the upgrade completes.
   - If you had deactivated CEIP for the earlier release, the CEIP check box is activated by default when the upgrade completes. Deselect the check box to not participate in CEIP.

     Click **OK**.

After the primary node upgrade process is complete, you can view the remaining upgrade process, which is automatic.

Check for the email sent to the Admin to confirm the upgrade completed successfully.

After the upgrade completes, all nodes are in the online mode even if they were in maintenance mode before the upgrade. Move these nodes back to the maintenance mode as needed.

Managing VMware Aria Operations for Logs User Accounts

You can create user accounts and roles to provide users with access to the VMware Aria Operations for Logs web interface.

You can create and edit user accounts if you are a user associated with the Super Admin role or a role that has the **Access control** permission with **Edit** access level. However, you can change your own email and account password without having this permission.

User Management Overview

You can use a combination of user logins, role-based access control, and data sets to manage VMware Aria Operations for Logs users. Role-based access control lets you manage users and the tasks that they can perform.

> **NOTE**
> You can create and edit user accounts if you are a user associated with the Super Admin role or a role that has the **Access control** permission with **Edit** access level.

Roles are sets of permissions required to perform particular tasks. VMware Aria Operations for Logs has a set of predefined roles. Additionally, you can create custom roles as part of defining security policies, and grant the roles to users. To change the permissions and tasks associated with a custom role, you can update the role settings. The updated settings take effect for all users associated with the role.

- To allow a user to perform a task, you grant the role to the user.
- To prevent a user from performing a task, you revoke the role from the user.

Managing roles for each user is based on their user login account. You can assign multiple roles to a user, in which case the role permissions are merged.

Users who cannot view or access certain objects or cannot perform certain operations were not assigned the roles with the permissions to do so.

Role-Based Access Control

Role-based access control lets you restrict log access for specific users, and control tasks that these users can perform after they log in. You can associate or revoke roles with or from user login accounts. A user can see all the dashboards that they have access to, but the data in the dashboards and in Explore Logs is filtered based on the data sets that the user role has access to.

> **NOTE**
> You can create and edit user accounts if you are a user associated with the Super Admin role or a role that has the **Access control** permission with **Edit** access level.

Users
> You can control the access and actions of each user by granting or revoking roles to or from the login account of the user.

Permissions
> Permissions and access levels are associated with roles, and control the allowed actions in VMware Aria Operations for Logs. Permissions apply to particular administrative or user tasks in VMware Aria Operations for Logs. The predefined roles in VMware Aria Operations for Logs have a fixed set of permissions. You can modify these permissions for all predefined roles except the Super Admin role. Additionally, you can also create custom roles and assign permissions with access levels according to your requirement. For example, you can grant the **Management** permission with **Full Access** to allow a user to view and modify the VMware Aria Operations for Logs administrative settings in the **Management** section.

Data Sets
> Data sets consist of a set of filters. You can use data sets to provide users with access to specific content by associating a data set with a role.
> > **NOTE**
> > You can associate data sets with all predefined roles except the Super Admin role.

Roles

Roles are collections of permissions and data sets that can be associated with users. Roles provide a convenient way to package all the permissions required to perform a task. One user can be assigned multiple roles.

VMware Aria Operations for Logs has a set of predefined roles. You can modify all predefined roles except the Super Admin role. You can also create custom roles and modify the associated permissions and data sets according to your requirement.

Using Filtering to Manage User Accounts

You can search for a user or set of users by specifying a search filter.

To use filtering for user accounts, navigate to **Management > Access Control** and select the **Users** tab.

The search text box contains the phrase `Filter by username`.

The search function filters results as you type, returning user names that contain the input pattern. For example, if you have user names `John_Smith`, `John_Doe`, and `Helen_Jonson`, when you type the letter `J`, search returns all user names that include that letter, for this example `John_Smith`, `John_Doe`, and `Helen_Jonson`. When you continue to type letters, search results are narrowed to match the exact pattern. For this example, when you type `John_`, search returns `John_Smith` and `John_Doe`.

You can sort the table by fields such as domain, authentication, roles, email, or UPN. In addition, you can perform a bulk action, such as deleting multiple users, on the search result.

Create a User Account

You can create user accounts to provide access to the VMware Aria Operations for Logs web user interface.

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a a role that has the **Access control** permission with **Edit** access level. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Verify that you have configured or Active Directory support if you are creating user accounts that use either of these types of authentication. See Activate User Authentication Through and Activate User Authentication Through Active Directory.

1. Expand the main menu and navigate to **Management > Access Control**.

2. Click **Users**.

3. Click **New User**.

4. Do either of the following:

   - If you are using the default, built-in authentication, enter a user name and an email address.
   - If you are using Active Directory or authentication, enter the domain to which the user belongs, a user name, and optionally, the email address for the user name account.

5. From the **Roles** list on the right, select one or more predefined or custom user roles.

Option	Description
Dashboard User	**Dashboard** users can only use the **Dashboards** page of VMware Aria Operations for Logs.
Super Admin	**Super Admin** users can access all the functionalities of VMware Aria Operations for Logs, can administer VMware Aria Operations for Logs, and can manage the accounts of all other users.
User	Users can access all the functionalities of VMware Aria Operations for Logs. Users can view log events, run queries

Option	Description
	to search and filter logs, import content packs into their own user space, view alerts, and manage their own user accounts to change a password or email address. Users do not have access to the administration options and cannot share content with other users, create or modify alerts, modify the accounts of other users, and or install a content pack from the Marketplace. However, they can import a content pack into their own user space which is visible only to them.
View Only Admin	**View Only Admin** users can view Admin information, have full user access, and can edit shared content.
Custom Role	A user with a **custom role** can view or modify information based on the permissions associated with the role.

To view the permissions associated with a predefined or custom role, in the **Access Control** page, click the **Roles** tab and then click **Show Permissions** against the role.

6. Click **Save**.

- For built-in authentication, the information is saved locally. An email is sent to the user's email address with a link to finish the registration. The user can click the link and enter a password for their account. Before the user registers their account, the account status is pending. After registration, the account status is active.

NOTE
A user must register their account within 24 hours of receiving the registration email. If they fail to do so, their account status remains pending, and they have to request the Super Admin user to unlock their account. For more information, see Unlock a User Account.

- For authentication with , VMware Aria Operations for Logs verifies whether the user's domain is linked to a group. If the domain does not belong to a group, VMware Aria Operations for Logs verifies whether the domain has established trust with a domain associated with a group. If cross-domain trust has been established, the user can log in to VMware Aria Operations for Logs, and the corresponding user account is added to the user table in **Access Control** > **Users**.

Unlock a User Account

If a user account is in pending status because of the failure to register within 24 hours or if the account is in locked status, a Super Admin user can unlock the account.
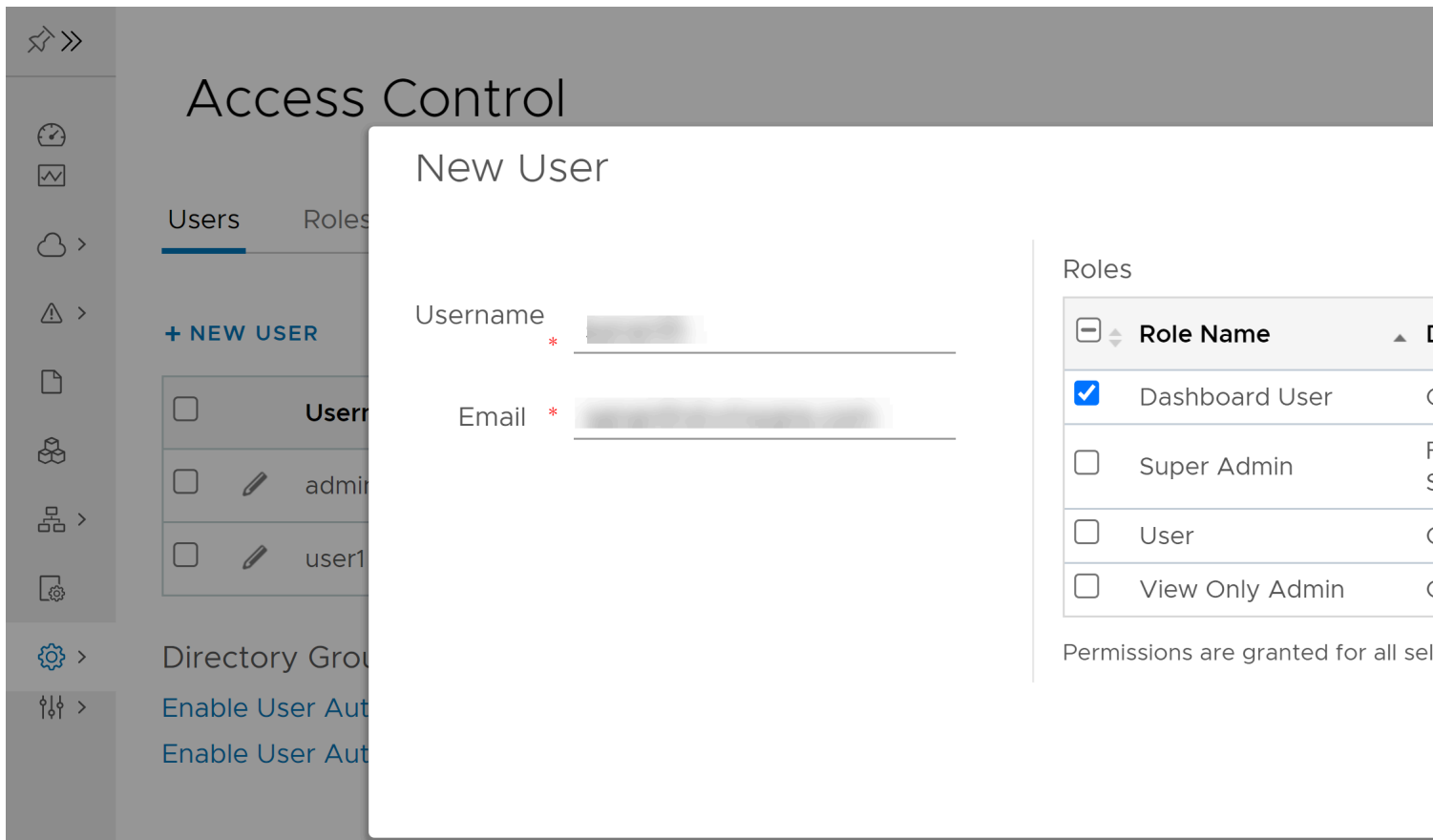
Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a a role that has the **Access control** permission with **Edit** access level. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

User accounts are locked in either of the following situations:

- The user enters the wrong password three consecutive times in a 15 minute period.
- The user has not logged in to VMware Aria Operations for Logs for 35 days. This lock condition is valid only if the password policy restriction is activated.
- The user has not changed their password for 60 days. This lock condition is valid only if the password policy restriction is activated.

For information about enabling the password policy restriction, see Configure STIG Compliance for VMware Aria Operations for Logs.

NOTE
This procedure unlocks accounts that use the default, built-in authentication only, and not accounts that use or Active Directory authentication.

1. Expand the main menu and navigate to **Management > Access Control**.

2. Click **Users**.

3. Optional: For the locked user account, point to the red lock icon in the **Status** column to know why the account is locked.

4. Click the pencil icon against the user name of the account.

5. Select the **Reset Password** check box if it is not selected already.

6. Click **Save**.

An email is sent to the user's email address with a link to reset their password. The user can click the link and enter a new password for their account.

NOTE
A user must unlock their account within 24 hours of receiving the email. If they fail to do so, they have to request the Super Admin user to unlock their account again.

Configure to Use Active Directory Groups for VMware Aria Operations for Logs

You can use Active Directory groups with VMware Aria Operations for Logs through single sign-on authentication. Your site must be configured for authentication that is enabled for Active Directory support, and server synchronization must be in place.

- Verify that you have configured the UPN attribute (userPrincipalName) attribute. It can be configured through the administrator interface at **Identity & Access Management** > **User Attributes**.
- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a a role that has the **Access control** permission with **Edit** access level. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Verify that you configured support in VMware Aria Operations for Logs. See Activate User Authentication Through

You must also import group information to VMware Aria Operations for Logs.

A user inherits roles that are assigned to any group the user belongs to in addition to the roles that are assigned to the individual user. For example, you can assign Group A to the role of **View Only Admin** and assign a user to the role of **User**. The same user can also be assigned to Group A. When the user logs in, they inherit the group role with privileges for both the **View Only Admin** and **User** roles.

The group is not a local group, but an Active Directory group that is synchronized with .

1. Expand the main menu and navigate to **Management > Access Control**.

2. Click **Users**.

3. Scroll to the Directory Groups table and click **New Group**.

4. Select **VMware Identity Manager** from the **Type** drop-down menu.

   The default domain name that you specified when you configured support appears in the **Domain** text box.

5. Change the domain name to the Active Directory name for the group.

6. Enter the name of the group that you want to add.

7. From the **Roles** list on the right, select one or more predefined or custom user roles.

Option	Description
Dashboard User	**Dashboard** users can only use the **Dashboards** page of VMware Aria Operations for Logs.
Super Admin	**Super Admin** users can access all the functionalities of VMware Aria Operations for Logs, can administer VMware Aria Operations for Logs, and can manage the accounts of all other users.
User	Users can access all the functionalities of VMware Aria Operations for Logs. Users can view log events, run queries to search and filter logs, import content packs into their own user space, view alerts, and manage their own user accounts to change a password or email address. Users do not have access to the administration options and cannot share content with other users, create or modify alerts, modify the accounts of other users, and or install a content pack from the Marketplace. However, they can import a content pack into their own user space which is visible only to them.
View Only Admin	**View Only Admin** users can view Admin information, have full user access, and can edit shared content.

Option	Description
Custom Role	A user with a **custom role** can view or modify information based on the permissions associated with the role.

To view the permissions associated with a predefined or custom role, in the **Access Control** page, click the **Roles** tab and then click **Show Permissions** against the role.

8. Click **Save**.

For authentication, VMware Aria Operations for Logs verifies whether the user's domain is linked to a group. If the domain does not belong to a group, VMware Aria Operations for Logs verifies whether the domain has established trust with a domain associated with a group. If cross-domain trust has been established, the user can log in to VMware Aria Operations for Logs, and the corresponding user account is added to the user table in **Access Control** > **Users**.

Users that belong to the group that you added can use their account to log in to VMware Aria Operations for Logs and have the same level of permissions as the group to which they belong.

Import an Active Directory Group to VMware Aria Operations for Logs

Instead of adding individual domain users, you can add domain groups to allow users to log in to VMware Aria Operations for Logs.

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a a role that has the **Access control** permission with **Edit** access level. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Verify that you configured AD support. See Activate User Authentication Through Active Directory

When you activate the AD support in VMware Aria Operations for Logs, you configure a domain name and provide a binding user that belongs to the domain. VMware Aria Operations for Logs uses the binding user to verify the connection to the AD domain, and to verify the existence of AD users and groups.

The Active Directory groups that you add to VMware Aria Operations for Logs must either belong to the domain of the binding user, or to a domain that is trusted by the domain of the binding user.

An Active Directory user inherits roles that are assigned to any group the user belongs to, in addition to the roles that are assigned to the individual user. For example, you can assign GroupA to the role of **View Only Admin** and assign the user Bob to the role of **User**. Bob can also be assigned to GroupA. When Bob logs in, he inherits the group role and has privileges for both the **View Only Admin** and **User** roles.

1. Expand the main menu and navigate to **Management > Access Control**.

2. Click **Users**.

3. Under Directory Groups, click **New Group**.

4. Click Active Directory in the **Type** drop-down menu.

   The default domain name that you specified when you configured Active Directory support appears in the **Domain** text box. If you are adding groups from the default domain, do not modify the domain name.

5. Optional: If you want to add a group from a domain that trusts the default domain, type the name of the trusting domain in the **Domain** text box.

6. Enter the name of the group that you want to add.

7. From the **Roles** list on the right, select one or more predefined or custom user roles.

Option	Description
Dashboard User	**Dashboard** users can only use the **Dashboards** page of VMware Aria Operations for Logs.

Option	Description
Super Admin	**Super Admin** users can access all the functionalities of VMware Aria Operations for Logs, can administer VMware Aria Operations for Logs, and can manage the accounts of all other users.
User	Users can access all the functionalities of VMware Aria Operations for Logs. Users can view log events, run queries to search and filter logs, import content packs into their own user space, view alerts, and manage their own user accounts to change a password or email address. Users do not have access to the administration options and cannot share content with other users, create or modify alerts, modify the accounts of other users, and or install a content pack from the Marketplace. However, they can import a content pack into their own user space which is visible only to them.
View Only Admin	**View Only Admin** users can view Admin information, have full user access, and can edit shared content.
Custom Role	A user with a **custom role** can view or modify information based on the permissions associated with the role.

To view the permissions associated with a predefined or custom role, in the **Access Control** page, click the **Roles** tab and then click **Show Permissions** against the role.

8. Click **Save**.

VMware Aria Operations for Logs verifies whether the AD group exists in the domain that you specified or in a trusting domain. If the group cannot be found, a dialog box informs you that VMware Aria Operations for Logs cannot verify that group. You can save the group without verification or cancel to correct the group name.

Users that belong to the Active Directory group that you added can use their domain account to log in to VMware Aria Operations for Logs and have the same level of permissions as the group to which they belong.

Define a Data Set

You can define a data set to provide users access to specific content.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a a role that has the **Access control** permission with **Edit** access level. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and navigate to **Management > Access Control**.

2. Click **Data Sets**.

3. Click **New Data Set**.

4. Enter a name and description for the data set.

5. Click **Add Filter**.

> **TIP**
> The **This data set restricts other data sets** check box determines how a data set should behave when combined with other data sets. For example, you have two data sets:

Data set 1:
```
hostname contains "host"
appname contains "app"
```

Data set 2:

```
severity contains "error"
```

If both of these data sets are added to a role, the resulting combined data set would be:

```
(hostname contains "host" AND appname contains "app") OR (severity contains "error")
```

However, if you select the **This data set restricts other data sets** check box for data set 2, the combined data set would be:

```
(hostname contains "host" AND appname contains "app") AND (severity contains "error")
```

6. Use the first drop-down menu to select a field defined within VMware Aria Operations for Logs to filter on.

   For example, **hostname**.

   The list contains static fields only and excludes fields that are extracted, user shared, and fields created through event_type filters.

   > **NOTE**
   > Numeric fields contain the additional operators **=**, **>**, **<**, **>=**, and **<=**, which string fields do not. These operators perform numeric comparisons. Using them yields different results than using string operators. For example, the filter **response_time=**`02` matches an event that contains a **response_time** field with a value 2. The filter **response_timecontains**`02` does not have the same match.

7. Use the second drop-down menu to select the operation to apply to the field selected in the first drop-down menu.

   For example, select **contains**. The **contains** filter matches full tokens: searching for the string `err` does not result in `error` as a match.

8. In the filter box to the right of the filter drop-down menu, enter the value that you want to use as a filter.

   You can use multiple values. The operator between these values is OR. If you are using the **_index** field in one of the filters, the operator is AND.

   > **NOTE**
   > The box is not available if you select the **exists** operator in the second drop-down menu.

9. Optional: To add more filters, click **Add Filter**.

10. Optional: To verify that the filter behavior is what you want, click **Run in Explore Logs page**, which opens an Explore Logs window with data that matches your filters.

11. Click **Save**.

Associate a data set with a user role. See Create and Modify Roles.

Create and Modify Roles

You can create or modify roles to allow users to perform certain tasks and access specific content.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a a role that has the **Access control** permission with **Edit** access level. The URL format of the web

user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

> **NOTE**
> You can edit all predefined roles except the Super Admin role. You can clone the Super Admin role and then modify the cloned role.

1. Expand the main menu and navigate to **Management > Access Control**.

2. Click **Roles**.

3. Click **New Role** or the pencil icon to edit an existing role.

4. Modify the **Name** and **Description** text boxes.

5. Select one or more permissions and their corresponding access levels from the **Permissions** list. Permissions have main categories and sub-categories within each main category.

   The following access levels are available:

   Full Access

   > Provides view and edit access to all the sub-categories for a permission. For example, if you select the **Full Access** check box against the **Management** permission, the users associated with the role can view and edit clusters, hosts, agents, and the rest of the sub-categories in the **Management** section.

   No Access

   > Does not provide view or edit access to the corresponding sub-category in a permission.

   View

   > Provides view access to the corresponding sub-category in a permission.

   Edit

   > Provides view and edit access to the corresponding sub-category in a permission.

   > **NOTE**
   > Some permissions do not have all access levels due to absence of use cases. For example, you do not have the **Edit** access level for content pack dashboards. Similarly, you do not have the **No Access** access level for extracted fields in the **Explore Logs** page.

   The following permissions are available:

Permission	Description
Management	Can view or modify information corresponding to the selected sub-categories, in the **Management** section: • System monitor • Cluster • Access control • Hosts • Agents • Certificates • Licenses
Configuration	Can view or configure information corresponding to the selected sub-categories, in the **Configuration** section: • General Configuration • Authentication Configuration • Time Configuration • SMTP Configuration • SSL Configuration • Proxy Configuration

Permission	Description
Log Management	Can view or manage information corresponding to the selected sub-categories, in the **Log Management** page: • Log Masking • Log Filtering • Log Forwarding • Index Partitions
Integrations	Can view or configure the integration of VMware Aria Operations for Logs with the products corresponding to the selected sub-categories, in the **Integration** section: • vSphere Integration • VMware Aria Operations Integration • NSX Identity Firewall Integration • Operations for Logs(SaaS) Integration
Content Packs	Can view or manage content packs in the **Content Packs** page.
Alerts	Can view, create, or modify alerts in the **Alerts** page or perform alert-related activities from the **Explore Logs** page.
Explore Logs	Can view or modify information corresponding to the selected sub-categories in the **Explore Logs** page: • Explore Logs • Extracted Fields • Export
Dashboards	Can view or modify information corresponding to the selected sub-categories in the **Dashboards** page: • User Dashboards • Shared Dashboards • Content Pack Dashboards • Shared Dashboard URLs • Scheduled Reports

6. Optional: From the **Data Sets** list, select a data set to associate with the user role.

7. Click **Save**.

The role appears in the **Roles** tab of the **Access Control** page, with information such as name, description, data sets, and so on.

• To view the user accounts associated with any role, click **Show Users** against the role.
• To view the permissions associated with any role, click **Show Permissions** against the role.

You can associate a user account or group with the role. For more information, see:

• Create a User Account
• Configure to Use Active Directory Groups for VMware Aria Operations for Logs
• Import an Active Directory Group to VMware Aria Operations for Logs

Delete a User Account or Group

You can delete user accounts or groups from the VMware Aria Operations for Logs user interface.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a a role that has the **Access control** permission with **Edit** access level. The URL format of the web

user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

User accounts and groups are listed in separate tables on the Access Control page. You can use a search filter to find specific user accounts. When you delete a group, all users that belong to the group lose the privileges given to them by the group.

1. Expand the main menu and navigate to **Management > Access Control**.

2. Click **Users**.

3. Select the check box beside the user name or group that you want to delete.

4. To remove the account or group, click **X DELETE** at the top of the User Account or Groups table.

Configuring Authentication

You can use several authentication methods with your deployment.

Authentication methods include local authentication, authentication, and Active Directory authentication. You can use more than one method in the same deployment and users then select the type of authentication to use at login.

The download page for includes a download link for the appropriate version of . includes the following features.

• Directory integration to authenticate users against existing directories such as Active Directory or LDAP.
• Single Sign-On integration with other VMware products that also support Single Sign-On capability.
• Single Sign-On with several third-party identity providers such as ADFS, Ping Federate, and others.
• Two-factor authentication through integration with third-party software such as RSA SecurID, Entrust, and others. Two-factor authentication with VMware Verify is included.

For more information, see the documentation.

Local authentication is a component of . To use it, you create a local user and password that is stored on the server. A product administrator must activate and Active Directory.

Activate User Authentication Through

When activated, authentication can be used with VMware Aria Operations for Logs.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

With authentication, users can use a single sign-on for all VMware products that use the same .

Active Directory users can also authenticate through when the Active Directory and servers are synchronized. See documentation for more information about synchronization.

Integration with can be done only with local users. Active Directory users who are assigned a tenant admin role in are not eligible for integration with .

1. Expand the main menu and navigate to **Configuration > Authentication**.

2. Select **Enable Single Sign-On**.

3. In the **Host** text box, enter a host identifier for the instance to use for authenticating users .

   For example, `company-name.vmwareworkspaceone.com`.

4. In the **API Port** text box, specify the port to use to connect to the instance. The default is 443.

5. Optionally, enter the tenant. The tenant is required only if the tenant mode is configured as tenant-in-path in .

6. Specify user credentials in the **Username** and **Password** text boxes.

   This information is used only once during configuration for creating a client onand is not stored locally in . The user must have permission to run API commands against the tenant.

7. Click **Test Connection** to verify that the connection works.

8. If the instance provides an untrusted SSL certificate, a dialog box appears with the details of the certificate. Click **Accept** to add the certificate to the truststores of all the nodes in the VMware Aria Operations for Logs cluster.

   If you click **Cancel**, the certificate is not added to the truststores and the connection with the instance fails. You must accept the certificate for a successful connection.

9. In the **Redirect URL Host** drop-down menu, select the Hostname or IP to be used in Redirect URL for registering on .

   If at least one virtual IP is defined for the Integrated Load Balancer, redirects to the VIP selected. If the Integrated Load Balancer is not configured, the primary node's IP address is used instead.

10. Select whether to allow log in support for Active Directory users through .

    You can use this option for Active Directory users when is synchronized with that Active Directory instance.

11. Click **Save**.

    If you did not test the connection and the instance provides an untrusted certificate, follow the instructions in step 9.

Activate User Authentication Through Active Directory

You can authenticate users through Active Directory to simplify the log in process by letting users use a common password for multiple purposes.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

Child domain access is not supported through Active Directory. This type of access is supported through VMware Workspace ONE Access only.

1. Expand the main menu and navigate to **Configuration > Authentication**.

2. Select **Enable Active Directory support**.

3. In the **Default Domain** text box, type a domain name.

   For example, `company-name.com`.

   > **NOTE**
   > You cannot list multiple domains in the default domain text box. If the default domain that you specify is trusted by other domains, VMware Aria Operations for Logs uses the default domain and the binding user to verify Active Directory users and groups in the trusting domains. Child-domain access with Active Directory is unsupported.
   >
   > If you switch to a different domain that already includes users and groups, the authentication fails for the existing users and groups, and data saved by the existing users is lost.

4. If you have geo-located or security-restricted domain controllers, manually specify the domain controllers closest to this VMware Aria Operations for Logs instance.

   > **NOTE**
   > Load-balanced Active Directory authorization servers are not supported.

5. Enter the credentials of a binding user that belongs to the default domain.

   VMware Aria Operations for Logs uses the default domain and the binding user to verify AD users and groups in the default domain, and in domains that trust the default domain.

6. Specify values for the connection type.

   This connection is used for Active Directory authentication.

7. Click **Test Connection** to verify that the connection works.

8. If the Active Directory server provides an untrusted SSL certificate, a dialog box appears with the details of the certificate. Click **Accept** to add the certificate to the truststores of all the nodes in the VMware Aria Operations for Logs cluster.

   If you click **Cancel**, the certificate is not added to the truststores and the connection with the Active Directory server fails. You must accept the certificate for a successful connection.

9. Click **Save**.

   If you did not test the connection and the Active Directory server provides an untrusted certificate, follow the instructions in step 9.

Give permissions to Active Directory users and groups to access the current instance of VMware Aria Operations for Logs.

Configure the Protocol to Use for Active Directory

You can configure the protocol to use when connecting to Active Directory. By default, when VMware Aria Operations for Logs connects to Active Directory, it first tries SSL LDAP, and then non-SSL LDAP if necessary.

- Verify that you have the root user credentials to log in to the virtual appliance.
- To enable SSH connections, verify that TCP port 22 is open.

If you want to limit the Active Directory communication to one particular protocol, or want to change the order of protocols that are tried, you must apply additional configurations in the VMware Aria Operations for Logs virtual appliance.

1. Establish an SSH connection to the virtual appliance and log in as the root user.

2. Navigate to the following location: `/storage/core/loginsight/config`

3. Locate the latest configuration file where [number] is the largest: `/storage/core/loginsight/config/loginsight-config.xml#`*`[number]`*

4. Copy the latest configuration file: `/storage/core/loginsight/config/loginsight-config.xml#`*`[number]`*

5. Increase the [number] and save to the following location: `/storage/core/loginsight/config/loginsight-config.xml#[number + 1]`

6. Open the file for editing.

7. In the `Authentication` section, add the line that corresponds to the configuration that you want to apply:

Option	Description
`<ad-protocols value="LDAP" />`	For specifically using LDAP without SSL
`<ad-protocols value="LDAPS" />`	For specifically using LDAP with SSL only
`<ad-protocols value="LDAP,LDAPS" />`	For specifically using LDAP first and then using LDAP with SSL.
`<ad-protocols value="LDAPS,LDAP" />`	For specifically using LDAPS first and then using LDAP without SSL

When you do not select a protocol, VMware Aria Operations for Logs attempts to use LDAP first, and then uses LDAP with SSL.

8. Save and close the file.

9. Run the `service loginsight restart` command.

Configuring VMware Aria Operations for Logs

You can configure and customize VMware Aria Operations for Logs to change default settings, network settings, and modify storage resources. You can also configure system notifications.

VMware Aria Operations for Logs Configuration Limits

When you configure VMware Aria Operations for Logs, you must stay at or below the supported maximums.

Table 12: VMware Aria Operations for Logs Configuration Maximums

Item	Maximum
Node Configuration	
CPU	16 vCPUs
Memory	32 GB
Storage device (vmdk)	2 TB - 512 bytes
Total addressable storage	4 TB (+ OS drive) A maximum of 4 TB addressable log storage on Virtual Machine Disks (VMDKs) with a maximum size of 2 TB each. You can have two 2 TB VMDKs or four 1 TB VMDKs, and so on. When you reach the maximum, you must scale outward with a larger cluster size instead of adding more disks to existing VMs.
Syslog connections	750
Cluster Configuration	
Nodes	18 (Primary + 17 Workers)
Virtual IP addresses	60
Ingestion per Node	
Events per second	15,000 eps
Syslog message length	10 KB (text field)
Ingestion API HTTP POST request	16 KB (text field); 4 MB per HTTP Post request
Integrations	
VMware Aria Operations	1
vSphere vCenter Server	15 per node
Cloud Channel	1
Active Directory domains	1
Email servers	1
DNS servers	2
NTP servers	4
Forwarders	10
Index Partition Configuration	
Index partitions	10

Add a Log Filter Configuration

You can add a configuration to drop logs that match the filter criteria you provide.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

Dropping logs lets you view only the logs that you require, which is cost-effective, saves storage, and improves performance.

> **NOTE**
>
> - A log filter configuration is applied only to the logs that are ingested after you create and activate the configuration.
> - A log filter configuration is applied only to logs with static fields in the filter criteria.

1. Expand the main menu, click **Log Management** and then click **Log Filtering**.

2. Click ➕**New Configuration**.

3. Enter a unique name for the log filter configuration.

4. Select fields and constraints to define the logs that you want to drop. If you do not select a filter, all the logs are dropped. To see the results of your filter, click **Run in Explore Logs page**.

Operator	Description
Matches	Finds strings that match the string and wildcard specification, where * means zero or more characters and ? means zero or any single character. Prefix and postfix globbing is supported. For example, `*test*` matches strings such as `test123` or `my-test-run`.
does not match	Excludes strings that match the string and wildcard specification, where * means zero or more characters and ? means zero or any single character. Prefix and postfix globbing is supported. For example, `test*` excludes `test123`, but not `mytest123`. `?test*` excludes `test123` and `xtest123`, but not `mytest123`.
starts with	Finds strings that start with the specified character string. For example, `test` finds `test123` or `test`, but not `my-test123`.
does not start with	Excludes strings that start with the specified character string. For example, `test` filters out `test123`, but not my-test123.

5. The log filter configuration is activated by default. To deactivate the configuration, click the **Enabled** toggle button.

6. To activate log forwarding for the logs that match the filter criteria, click the **Allow Forwarding** toggle button.

   When you click the toggle button and save this configuration, the logs matching the filter criteria are no longer ingested into the current VMware Aria Operations for Logs instance. Instead, they are sent to the log forwarding or cloud forwarding destination that has the same filter criteria as your log filter configuration.

   You can configure a log forwarding destination in **Log Management > Log Forwarding** and a cloud forwarding destination in **Log Management > Cloud Forwarding**.

7. Click **Save**.

The log filter configuration appears in the **Log Filtering** tab with information about the drop filter and whether it is activated. You can activate or deactivate the configuration by clicking the **Enabled** toggle button.

Add a Log Mask Configuration

You can add a configuration to mask sensitive information in all logs or logs that match the filter criteria you provide.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

> **NOTE**
> - A log mask configuration is applied only to the logs that are ingested after you create and activate the configuration.
> - A log mask configuration is applied only to logs in which the *FieldName* field and the filter criteria have static fields.

1. Expand the main menu, click **Log Management** and then click **Log Masking**.

2. Click ➕**New Configuration**.

3. Enter a unique name for the log mask configuration.

4. In the **Field Name** drop-down menu, select the field that you want to mask in the logs.

5. In the **Selector** text box, enter the regex selector for the field value, which indicates the part of the field that you want to mask.

   You must express this value as a capture group in the regex. Capture groups are identified with enclosed parentheses `()`. You can have multiple capture groups inside a selector. To mask all the content for a specified field, you can set the selector as `(.*)`.

6. In the **Mask Value** text box, enter a value to replace the masked content of the specified fields, the default value for which is an empty string.

7. Click ➕**Add Filter** to define the logs for which you want to mask information. If you do not add a filter, all the logs are masked. To see the results of your filter, click **Run in Explore Logs page**.

Operator	Description
Matches	Finds strings that match the string and wildcard specification, where * means zero or more characters and ? means zero or any single character. Prefix and postfix globbing is supported. For example, `*test*` matches strings such as `test123` or `my-test-run`.
does not match	Excludes strings that match the string and wildcard specification, where * means zero or more characters and ? means zero or any single character. Prefix and postfix globbing is supported. For example, `test*` excludes `test123`, but not `mytest123`. `?test*` excludes `test123` and `xtest123`, but not `mytest123`.
starts with	Finds strings that start with the specified character string. For example, `test` finds `test123` or `test`, but not `my-test123`.

Operator	Description
does not start with	Excludes strings that start with the specified character string.
	For example, `test` filters out `test123`, but not my-test123.

8. The log mask configuration is activated by default. To deactivate the configuration, click the **Enabled** toggle button.

9. Click **Save**.

The log mask configuration appears in the **Log Masking** tab with information about whether it is activated, the logs to which it is applied, and so on. You can activate or deactivate the configuration by clicking the **Enabled** toggle button.

Configuring Virtual Appliance Settings

You can modify virtual appliance settings, including storage capacity and memory or CPU capacity.

Configure the Root SSH Password for the VMware Aria Operations for Logs Virtual Appliance

You can configure the root SSH password from the VMware Remote Console or when you deploy the VMware Aria Operations for Logs virtual appliance.

Verify that the VMware Aria Operations for Logs virtual appliance is deployed and running.

By default, the SSH connection to the VMware Aria Operations for Logs virtual appliance is activated. To SSH to the virtual instance, you must configure the root password.

As a best practice, you must also set the root SSH password when you deploy theVMware Aria Operations for Logs .ova file. For more information, see Deploy the VMware Aria Operations for Logs Virtual Appliance.

To activate SSH and set the root password from the VMware Remote Console, perform the following steps:

1. In the vSphere Client inventory, click the VMware Aria Operations for Logs virtual appliance, and open the **Console** tab.

2. Go to a command line by following the key combination specified on the splash screen.

3. In the console, type `root`, and press `Enter` . Leave the password empty and press `Enter` again.
   The following message is displayed in the console: `Password change requested. Choose a new password.`

4. Leave the old password empty and press `Enter` .

5. Type a new password for the root user, press `Enter` , type the new password again for the root user, and press `Enter` again.
   The password must consist of at least eight characters, and must include at least one upper case letter, one lower case letter, one digit, and one special character. You cannot repeat the same character more than four times.

The following message is displayed: `Password changed.`

You can use the root password to establish SSH connections to the VMware Aria Operations for Logs virtual appliance.

To troubleshoot issues in configuring the root SSH password, see the KB articles:

- https://kb.vmware.com/s/article/53649
- https://kb.vmware.com/s/article/90831

Change the Network Settings of the VMware Aria Operations for Logs Virtual Appliance

You can change the network settings of the VMware Aria Operations for Logs virtual appliance by following the steps described in https://kb.vmware.com/s/article/87992 and https://kb.vmware.com/s/article/91258.

> **NOTE**
> In a multi-node cluster, you must perform operations such as shutting down, adding storage, and restarting, on one node at a time.

Increase the Storage Capacity of the VMware Aria Operations for Logs Virtual Appliance

You can increase the storage resources allocated to VMware Aria Operations for Logs as your needs grow.

- Log in to the vSphere Client as a user who has privileges to modify the hardware of virtual machines in the environment.
- Shut down the VMware Aria Operations for Logs virtual appliance safely. See Power off the VMware Aria Operations for Logs Virtual Appliance

To increase the storage space of a VMware Aria Operations for Logs virtual appliance, you must add a new virtual disk to the virtual appliance. This is the only supported option.

Instead of adding numerous smaller disks, It is recommended that you add fewer large disks of up to 4 TB (+ OS drive) total addressable storage. The total can be a combination of two 2-TB disks, or four 1-TB disks, and so on. To learn more, see VMware Aria Operations for Logs Configuration Limits.

> **NOTE**
>
> - You must add the same amount of storage to each node in a VMware Aria Operations for Logs cluster.
> - In a multi-node cluster, you must perform operations such as shutting down, adding storage, and restarting, on one node at a time.

You can add storage to nodes in any order. However, it is recommended that the internal load balancing (ILB) node must be the last node to receive additional storage.

1. In the vSphere Client inventory, right-click the VMware Aria Operations for Logs virtual machine and select **Edit Settings**.

2. On the **Hardware** tab, click **Add**.

3. Select **Hard Disk** and click **Next**.

4. Select **Create a new virtual disk** and click **Next**.

    a) Type the disk capacity.

    VMware Aria Operations for Logs supports virtual hard disks of up to 2 TB. If you need more capacity, add more than one virtual hard disk.

    b) Select a disk format.

Option	Description
Thick Provision Lazy Zeroed	Creates a virtual disk in the default thick format. The space required for the virtual disk is allocated when the virtual disk is created. The data residing on the physical device is not erased during creation, but is zeroed out on demand later, after first write from the virtual appliance.
Thick Provision Eager Zeroed	Creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. The space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data residing on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks. Create thick provisioned eager zeroed disks whenever possible for better performance and operation of the VMware Aria Operations for Logs virtual appliance.
Thin Provision	Creates a disk in thin format. Use this format to save storage space.

    c) Required: To select a datastore, browse for the datastore location and click **Next**.

5. Accept the default virtual device node and click **Next**.

6. Review the information and click **Finish**.

7. Click **OK** to save your changes and close the dialog box.

When you power on the VMware Aria Operations for Logs virtual appliance, the virtual machine discovers the new virtual disk and automatically adds it to the default data volume. Completely power off the virtual machine first. For information about powering on virtual appliances, see https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html.

⚠️ **CAUTION**
After you add a disk to the virtual appliance, you cannot remove it safely. Removing disks from the VMware Aria Operations for Logs virtual appliance may result in complete data loss.

Add Memory and CPU to the VMware Aria Operations for Logs Virtual Appliance

You can change the amount of memory and CPUs allocated to a VMware Aria Operations for Logs virtual appliance after deployment.

- Log in to the vSphere Client as a user who has privileges to modify the hardware of virtual machines in the environment.
- Shut down the VMware Aria Operations for Logs virtual appliance safely. See Power off the VMware Aria Operations for Logs Virtual Appliance

You might need to adjust resource allocation if, for example, the number of events in your environment increases.

> **NOTE**
> In a multi-node cluster, you must perform operations such as shutting down, adding storage, and restarting, on one node at a time.

1. In the vSphere Client inventory, right-click the VMware Aria Operations for Logs virtual machine and select **Edit Settings**.

2. On the **Hardware** tab, click **Add**.

3. Adjust the amount of CPU and memory as needed.

4. Review the information and click **Finish**.

5. Click **OK** to save your changes and close the dialog box.

When you power on the VMware Aria Operations for Logs virtual appliance, the virtual machine begins to utilize the new resources.

Assign a License to VMware Aria Operations for Logs

You can use VMware Aria Operations for Logs only with a valid license key.

- Obtain a valid license key from My VMware™.
- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

You obtain an evaluation license when you download VMware Aria Operations for Logs from the VMware website. This license is valid for 60 days. When the evaluation license expires, you must assign a permanent license to continue using VMware Aria Operations for Logs.

The VMware Aria Operations for Logs Operating System Instance (OSI) license model defines an OSI as a single installation of an operating system on a non-virtualized physical server or virtual machine. For VMware Aria Operations for Logs, an OSI can also be a single system identified by an IP address such as virtualized physical servers, storage arrays, or network devices that can generate log messages.

When a host, server or other source stops sending logs to VMware Aria Operations for Logs, the OSI count on the License page is unchanged during the retention period. The retention period is based on license use calculated as the average of the OSI count over the last three months.

You use the Management section of the VMware Aria Operations for Logs web user interface to check the VMware Aria Operations for Logs licensing status and manage your licenses.

As part of solution interoperability, VMware NSX users on Standard, Advanced, or Enterprise editions can license VMware Aria Operations for Logs with their NSX license key. For more information, consult VMware NSX documentation.

1. Expand the main menu and navigate to **Management > License**.

2. In the **License Key** text box, enter your license key and click **Set Key**. If you have a VMware NSX license key, enter it here.

3. Verify that the license status is Active, and the license type and expiry day are correct.

Log Storage Policy

The VMware Aria Operations for Logs virtual appliance uses a minimum of 100 GB of storage for incoming logs.

When the volume of logs imported into VMware Aria Operations for Logs reaches the storage limit, old log messages are automatically and periodically retired on a first-come-first-retired basis. You can increase the storage limit by adding more storage to the VMware Aria Operations for Logs virtual appliance. See Increase the Storage Capacity of the VMware Aria Operations for Logs Virtual Appliance.

To preserve old messages, you can enable the archiving feature of VMware Aria Operations for Logs. See Data Archiving.

Data stored by VMware Aria Operations for Logs is immutable. After a log has been imported, it cannot be removed until it is automatically retired.

Managing System Notifications

VMware Aria Operations for Logs provides built-in system notifications about activity related to VMware Aria Operations for Logs health, such as when disk space is almost exhausted and old log files are about to be deleted.

System notifications inform you of critical issues that require immediate attention, provide you with warnings that might require a response, and inform you of normal system activity. System notifications are suspended during upgrade, but in effect at all other times.

To view system notifications, expand the main menu and navigate to **Alerts > System Alerts**. With appropriate permissions, you can activate or deactivate the notifications. For more information, see View and Manage Alerts in *Using VMware Aria Operations for Logs*.

You can specify where system notifications are sent by navigating to **Configuration > General**. System notifications concerning VMware Aria Operations for Logs can also be sent to third-party applications.

VMware Aria Operations for Logs System Notifications

VMware Aria Operations for Logs provides you with two sets of notifications about system health, general notifications, applicable for all product configurations, and notifications related to clusters for cluster-based deployments.

To view system notifications, expand the main menu and navigate to **Alerts > System Alerts**. With appropriate permissions, you can activate or deactivate the notifications. For more information, see View and Manage Alerts in *Using VMware Aria Operations for Logs*.

> **NOTE**
> In this topic, an admin user refers to a user associated with the **Super Admin** role, or a role that has the relevant permissions, as described in Create and Modify Roles.

The following tables list and describe system notifications for VMware Aria Operations for Logs.

General System Notifications

VMware Aria Operations for Logs issues notifications about conditions that might require administrative intervention, including archival failure or alert scheduling delays.

Notification Name	Description
Oldest data will be unsearchable soon	VMware Aria Operations for Logs is expected to start decommissioning old data from the virtual appliance storage based on the expected size of searchable data, storage space, and the current ingestion rate. Data that has been rotated out is archived if you have configured archiving, or deleted if you have not. To address this, add storage or adjust the retention notification threshold. For more information, see Configure VMware Aria Operations for Logs to Send Health Notifications. The notification is sent after each restart of the VMware Aria Operations for Logs service.
Repository retention time	A retention period is the length of time data is retained on the local disk of your VMware Aria Operations for Logs instance. A retention period is determined by the amount of data the system can hold and the current ingestion rate. For example, if you are receiving 10 GB/day of data (after indexing) and you have 300 GB of space, then your retention rate is 30 days. When your storage limit is reached, old data is removed to make way for newly ingested data. This notification tells you when the amount of searchable data that VMware Aria Operations for Logs can store at the current ingestion rates exceeds the storage space that is available on the virtual appliance. You might run out of storage before the time period set with the **Retention Notification Threshold**. Add storage or adjust the retention notification threshold.

Dropped events	VMware Aria Operations for Logs failed to ingest all incoming log messages.
	
	• If a TCP Message drops, as tracked by VMware Aria Operations for Logs server, a system notification is sent as follows:
	  — Once a day
	  — Each time the VMware Aria Operations for Logs service is restarted, manually or automatically
	• The email contains the number of messages dropped since last notification email was sent and total message drops since the last restart of VMware Aria Operations for Logs.
	    NOTE
	    The time in the sent line is controlled by the email client, and is in the local time zone, while the email body displays the UTC time.

Corrupt index buckets	Part of the on-disk index is corrupt. A corrupt index usually indicates serious issues with the underlying storage system. The corrupt part of the index is excluded from serving queries. A corrupt index affects the ingestion of new data. VMware Aria Operations for Logs checks the integrity of the index upon service start-up. If corruption is detected, VMware Aria Operations for Logs sends a system notification as follows: • Once a day • Each time the VMware Aria Operations for Logs service is restarted, manually or automatically
Out of disk	VMware Aria Operations for Logs is running out of allocated disk space. VMware Aria Operations for Logs has most probably run into a storage-related issue.

Notification Name	Description
Archive space will be full	The disk space on the NFS server used for archiving VMware Aria Operations for Logs data will be used up soon. If the amount of archived data that the NFS server can hold at the current ingestion rate is less than seven days, a system notification is sent. For example, if you are archiving with a disk consumption rate of 708.9 MB per day of data and you have 2000 MB space, you have about three days of capacity, which is less than the threshold. In this case, you will receive a notification that you are below this capacity.
Total disk space change	The total size of the partition for the VMware Aria Operations for Logs data storage has decreased. This notification usually signals a serious issue in the underlying storage system. When VMware Aria Operations for Logs detects the condition, it sends this notification as follows: • Immediately • Once a day
Pending archivings	VMware Aria Operations for Logs cannot archive data as expected. The notification usually indicates problems with the NFS storage that you configured for data archiving.
Allocated log record storage volume reached 75 percent of the maximum log record storage capacity	VMware Aria Operations for Logs is configured to ensure STIG compliance, and the allocated log record storage volume reaches 75 percent of the maximum log record storage capacity of the repository. **NOTE** This notification is sent per node.
License is about to expire	The license for VMware Aria Operations for Logs is about to expire.
License is expired	The license for VMware Aria Operations for Logs has expired.
SSL certificate is about to expire	The SSL certificate for the VMware Aria Operations for Logs cluster will expire in 30 days.
Unable to connect to AD server	VMware Aria Operations for Logs is unable to connect to the configured Active Directory server.
Cannot take over High Availability IP address [IP Address] as it is already held by another machine	The VMware Aria Operations for Logs cluster was unable to take over the configured IP Address for the Integrated Load Balancer (ILB). The most common reason for this notification is that another host within the same network holds the IP address, and therefore the IP address is not available to be taken over by the cluster. You can resolve this conflict by either releasing the IP address from the host that currently holds it, or configuring VMware Aria Operations for Logs Integrated Load Balancer with a Static IP address that is available in the network. When changing the ILB IP address, you must reconfigure all clients to send logs to the new IP address, or to a FQDN/URL that resolves to this IP address. You must also unconfigure and reconfigure every vCenter Server integrated with VMware Aria Operations for Logs from the vSphere integration page.

Notification Name	Description
High Availability IP address [IP Address] is unavailable due to too many node failures	The IP Address configured for the Integrated Load Balancer (ILB) is unavailable. Clients trying to send logs to a VMware Aria Operations for Logs cluster through the ILB IP address or a FQDN/URL that resolves to this IP address will see it as unavailable. The most common reason for this notification is that most of the nodes in the VMware Aria Operations for Logs cluster are unhealthy, unavailable, or unreachable from the primary node. Another common reason is that NTP time synchronization has not been activated, or the configured NTP servers have a significant time drift between each other. You can confirm that the problem is still ongoing by trying to ping (if allowed) the IP address to verify that it is not reachable. You can resolve this problem by ensuring that most of your cluster nodes are healthy and reachable, and enabling NTP time synchronization to accurate NTP servers.
Too many migrations of High Availability IP address [your IP Address] between VMware Aria Operations for Logs nodes	The IP address configured for the Integrated Load Balancer (ILB) has migrated too many times within the last 10 minutes. Under normal operation, the IP address rarely moves between VMware Aria Operations for Logs cluster nodes. However, the IP address might move if the current owner node is restarted or put in maintenance. The other reason can be the lack of time synchronization between VMware Aria Operations for Logs cluster nodes, which is essential for proper cluster functioning. For the latter, you can fix the problem by enabling NTP time synchronization to accurate NTP servers.
SSL certificate error	A syslog source has initiated a connection to VMware Aria Operations for Logs over SSL but ended the connection abruptly. This notification might indicate that the syslog source was unable to confirm the validity of the SSL certificate. In order for VMware Aria Operations for Logs to accept syslog messages over SSL, a certificate that is validated by the client is required and the clocks of the systems must be synchronized. There might be a problem with the SSL Certificate or with the Network Time Service. You can validate that the SSL Certificate is trusted by your syslog source, reconfigure the source not to use SSL, or reinstall the SSL Certificate. See Configure the VMware Aria Operations for Logs Agent SSL Parameters and Install a Custom SSL Certificate.
vCenter collection failed	VMware Aria Operations for Logs is unable to collect VMware vCenter events, tasks, and alarms. To look for the exact error that caused the collection failure and to see if collection is working currently, look in the `/var/log/vmware/loginsight/plugins/vsphere/li-vsphere.log` file.
vCenter Kubernetes Service event collection failed	VMware Aria Operations for Logs is unable to collect VMware vCenter Kubernetes System events, tasks, and alarms. To look for the exact error that caused the collection failure and to see if collection is working currently, look in the `/var/log/vmware/loginsight/plugins/vsphere/li-vsphere.log` file.

Notification Name	Description
Event forwarder events dropped	A forwarder drops events because of connection or overload problems. Example: ``` Operations for Logs Admin Alert: Event Forwarder Events Dropped This alert is about your Operations for Logs installation on https://<your_url> Event Forwarder Events Dropped triggered at 2016-08-02T18:41:06.972Z Operations for Logs just dropped 670 events for forwarder target 'Test', reason: Pending queue is full. ```
Alert queries behind schedule	VMware Aria Operations for Logs was unable to run a user-defined alert at its configured time. The reason for the delay might be because of one or more inefficient user-defined alerts or because the system is not properly sized for the ingestion and query load.
Auto deactivated alert	If a user-defined alert has run at least 10 times and its average run time is more than one hour, the alert is considered inefficient and is deactivated to prevent impacting other user-defined alerts.
Inefficient alert query	If a user-defined alert takes more than one hour to finish, then the alert is deemed to be inefficient.
New user created or user logged in for the first time	VMware Aria Operations for Logs is configured to ensure STIG compliance, and a new user is created or an Active Directory or user logs in for the first time.

System Notifications for Clusters

VMware Aria Operations for Logs sends notifications about cluster topology changes, including the addition of new cluster members or transient node communication problems.

Sent by	Notification Name	Description
Primary node	Approval needed for new worker node	A worker node is sending a request to join a cluster. An Admin user must approve or reject the request.
Primary node	New worker node approved	An Admin user approved a membership request from a worker node to join a VMware Aria Operations for Logs cluster.
Primary node	New worker node denied	An Admin user rejected a membership request from a worker node to join a VMware Aria Operations for Logs cluster. If the request was denied by mistake, an Admin user can place the request again from the worker and then approve it at the primary node.
Primary node	Maximum supported nodes exceeded due to worker node	The number of worker nodes in the VMware Aria Operations for Logs cluster has exceeded the maximum supported count due to a new worker node.

Sent by	Notification Name	Description
Primary node	Allowed nodes exceeded, new worker node denied	An user attempted to add more nodes to the cluster than the maximum allowed node count and the node has been denied.
Primary node	Worker node disconnected	A previously connected worker node disconnected from the VMware Aria Operations for Logs cluster.
Primary node	Worker node reconnected	A worker node reconnected to the VMware Aria Operations for Logs cluster.
Primary node	Worker node revoked by	An Admin user revoked a worker node membership and the node is no longer a part of the VMware Aria Operations for Logs cluster.
Primary node	Unknown worker node rejected	The VMware Aria Operations for Logs primary node rejected a request by a worker node because the worker node is unknown to the primary. If the worker is a valid node and it should be added to the cluster, log in to the worker node, remove its token file and user configuration at `/storage/core/loginsight/config/`, and run `restart loginsight service` on the worker node.
Primary node	Worker node has entered into maintenance mode	A worker node entered into maintenance mode and an Admin user has to remove the worker node from maintenance mode before it can receive configuration changes and serve queries.
Primary node	Worker node has returned to service	A worker node exited maintenance mode and returned to service.
Worker node	Primary failed or disconnected from worker node	The worker node that sends the notification is unable to contact the VMware Aria Operations for Logs primary node. This notification might indicate that the primary node failed, and might need to be restarted. If the primary node failed, the cluster cannot be configured and queries cannot be submitted until it is back online. Worker nodes continue to ingest messages. **NOTE** You might receive many such notifications because many workers might detect the primary node failure independently and raise notifications.
Worker node	Primary connected to worker node	The worker node that sends the notification is reconnected to the VMware Aria Operations for Logs primary node.

Configuring Destinations for VMware Aria Operations for Logs System Notifications

You can configure the action that VMware Aria Operations for Logs takes when a system notification is triggered.

VMware Aria Operations for Logs generates system notifications when an important system event occurs, for example when the disk space is almost exhausted and VMware Aria Operations for Logs must begin deleting or archiving old log files.

Super Admin users and users with the relevant permissions can configure VMware Aria Operations for Logs to send email notifications about these events. The From address of system notification emails is configured on the SMTP configuration page, in the **Sender** text box. See Configure the SMTP Server for VMware Aria Operations for Logs.

You can also send notifications to third-party applications. See Configure a Webhook.

Configure VMware Aria Operations for Logs to Send Health Notifications

You can configure VMware Aria Operations for Logs to send notifications related to its own health.

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Verify that the SMTP server is configured for VMware Aria Operations for Logs. For more information, see Configure the SMTP Server for VMware Aria Operations for Logs.

If an email message cannot be delivered, you are notified of the error on the Web interface.

1. Expand the main menu and navigate to **Configuration** > **General**.

2. Under the Alerts header, set the system notifications.
   a) In the **Email System Notifications To** text box, type the email addresses to be notified.
      Use commas to separate multiple email addresses.
   b) Select the **Retention notification threshold** check box and set the threshold that triggers the notifications.
      A notification is sent when the amount of data the system can hold is insufficient for the time period specified. This value is calculated based on the current ingestion rate.

3. Click **Save**.

4. Click **Restart Operations for Logs** to apply your changes.

Configure VMware Aria Operations for Logs System Notifications for Third-Party Products

You can configure VMware Aria Operations for Logs to send notifications related to its own health to third-party applications.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL

format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

VMware Aria Operations for Logs generates these notifications when an important system event occurs, for example when the disk space is almost exhausted and VMware Aria Operations for Logs must start deleting old log files.

1. Expand the main menu and navigate to **Configuration** > **General**.

2. Under the Alerts header, set the system notifications.
   a) In the **Send HTTP Post System Notifications To** text box, type the URLs to be notified.
   b) Optional: Confirm that the **Send a notification when capacity drops below** check box and associated threshold are configured correctly for your environment.

3. Click **Save**.

Configure a webhook to send notifications to your third-party application. For more information, see Configure a Webhook.

Webhook Format for a System Notification
The format of a VMware Aria Operations for Logs webhook depends on the type of query from which it is created. System notifications, user alert message queries, and alerts generated from aggregate user queries each have a different webhook format.

> **NOTE**
> To configure VMware Aria Operations for Logs to send system notifications, you must be a user associated with the Super Admin role, or a role with the relevant permissions. For more information, see Create and Modify Roles.

Webhook Format for System Notifications

The following example shows the VMware Aria Operations for Logs webhook format for system notifications.

```
{
   "AlertName":" Admin Alert: Worker node has returned to service  (Host = 127.0.0.2)",
   "messages":[
      {
         "text":"This notification was generated from Operations for Logs node (Host = 127.0.0.2,

Node Identifier = a31cad22-65c2-4131-8e6c-27790892a1f9).
A worker node has returned to service after having been in maintenance mode.
The Operations for Logs primary node reports that worker node has finished maintenance
and exited maintenance mode. The node will resume receiving configuration changes and
serving queries. The node is also now ready to start receiving incoming log messages."

         "timestamp":1458665320514,"fields":[]
      }
   ]
}
```

Add a VMware Aria Operations for Logs Log Forwarding Destination

You can configure a VMware Aria Operations for Logs server to forward incoming log events to a syslog or Ingestion API target.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://`operations-for-logs-host`, where `operations-for-logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

Verify that the destination can handle the number of logs that are forwarded. If the destination cluster is much smaller than the forwarding instance, some logs might be dropped.

Use log forwarding to send filtered or tagged logs to one or more remote destinations such as VMware Aria Operations for Logs or syslog or both. Log forwarding can be used to support existing logging tools such as SIEM and to consolidate logging over different networks such as DMZ or WAN.

Log forwarders can be standalone or clustered, but a log forwarder is a separate instance from the remote destination. Instances configured for log forwarding also store logs locally and can be used to query data.

The operators you use to create filters on the Log Forwarding page are different from the filters used on the Explore Logs page. See Using Log Management Filters in Explore Logs for more information about using the **Run in Explore Logs page** menu item to preview the results of your log filter.

1. Expand the main menu, click **Log Management** and then click **Log Forwarding**.

2. Click ➕**New Destination** and provide the following information.

Option	Description
Name	A unique name for the new destination.
Host	The IP address or fully qualified domain name. ⚠️ **CAUTION** A forwarding loop is a configuration in which a VMware Aria Operations for Logs cluster forwards logs to itself, or to another cluster, which then forwards the logs back to the original cluster. Such a loop might create an indefinite number of copies of each forwarded log. The VMware Aria Operations for Logs Web interface does not permit you to configure a log to be forwarded to itself. But VMware Aria Operations for Logs is not able to prevent an indirect forwarding loop, such as VMware Aria Operations for Logs cluster A forwarding to cluster B, and B forwarding the same logs back to A. When creating forwarding destinations, take care not to create indirect forwarding loops.
Protocol	Ingestion API, Syslog, or RAW. The default value is Ingestion API. When logs are forwarded using **Ingestion API**, the log's original source is preserved in the source field. When logs are forwarded using **Syslog**, the log's original source is lost and the receiver can record the message's source as the VMware Aria Operations for Logs forwarder's IP address or hostname. When logs are forwarded using **Raw**, the behavior is similar to syslog, but syslog RFC-compliance is not ensured. RAW forwards a log exactly the way it is received, without a custom syslog header added by VMware Aria Operations for Logs. The

Option	Description
	RAW protocol is useful for third-party destinations, because they expect syslog events in their original form.
	If you select the **Adjust PRI/VERSION** check box, VMware Aria Operations for Logs will automatically add the `PRI` and `VERSION` headers to the log if the headers are missing.
	NOTE - If you are upgrading from the previous versions of VMware Aria Operations for Logs, the **Adjust PRI/VERSION** check box is deselected by default. Make sure to manually select this option after the upgrade. - The source field might have different values depending on the protocol selected on the Log Forwarder: - For the ingestion API, the source is the initial sender's (the log originator) IP address. - For syslog and RAW, the source is the Log Forwarder's VMware Aria Operations for Logs instance IP address.
Use SSL	You can optionally secure the connection with SSL for the ingestion API or syslog. If the SSL certificate provided by the forwarding destination is untrusted, you can accept the certificate when you test or save this configuration.
Tags	You can optionally add tag pairs with predefined values. Tags permit you to more easily query logs. You can add multiple comma-separated tags.
Forward Complementary tags	You can select whether to forward complementary tags for syslog. Complementary tags are tags added by the cluster itself, such as 'vc_username' or 'vc_vmname.' and can be forwarded with the tags coming directly from sources. Complementary tags are always forwarded when Ingestion API is used.
Transport	Select a transport protocol for syslog. You can select UDP or TCP.

3. To control which logs are forwarded, click ➕**Add Filter**.

Select fields and constraints to define the desired logs. Only static fields are available for use as filters. If you do not select a filter, all logs are forwarded. You can see the results of the filter you are building by clicking **Run in Explore Logs page**.

Operator	Description
Matches	Finds strings that match the string and wildcard specification, where * means zero or more characters and ? means zero or any single character. Prefix and postfix globbing is supported. For example, `*test*` matches strings such as `test123` or `my-test-run`.
does not match	Excludes strings that match the string and wildcard specification, where * means zero or more characters and ? means zero or any single character. Prefix and postfix globbing is supported.

Operator	Description
	For example, `test*` excludes `test123`, but not `mytest123`. `?test*` excludes `test123` and `xtest123`, but not `mytest123`.
starts with	Finds strings that start with the specified character string. For example, `test` finds `test123` or `test`, but not `my-test123`.
does not start with	Excludes strings that start with the specified character string. For example, `test` filters out `test123`, but not my-test123.

For example, to see the successful logins from vCenter Server users over the past 24 hours:

4. Optional: To modify the following log forwarding information, click **Show Advanced Settings**.

Option	Description
Port	The port to which logs are sent on the remote destination. The default value is set based on the protocol. Do not change unless the remote destination listens on a different port.
Worker Count	The number of simultaneous outgoing connections to use. Set a higher worker count for a higher network latency to the forwarded destination and for a greater number of forwarded logs per second. The default value is 8.

5. To verify your configuration, click **Test**.

6. If the forwarding destination provides an untrusted SSL certificate, a dialog box appears with the details of the certificate. Click **Accept** to add the certificate to the truststores of all the nodes in the VMware Aria Operations for Logs cluster.

   If you click **Cancel**, the certificate is not added to the truststores and the connection with the forwarding destination fails. You must accept the certificate for a successful connection.

7. Click **Save**.

   If you did not test the configuration and the destination provides an untrusted certificate, follow the instructions in step 7.

You can edit or clone a log forwarding destination. If you edit the destination to change a log forwarder name, all statistics are reset.

Using Log Management Filters in Explore Logs

Operators used in log management filters and operators used in filters in Explore Logs do not have a one-to-one correspondence by name. However, you can select operators that produce similar results for both formats.

This difference is important when you use the **Run in Explore Logs page** menu item from the following tabs in the **Log Management** page:

- **Log Masking**
- **Log Filtering**
- **Log Forwarding**
- **Cloud Forwarding**
- **Index Partitions**

For example, if you have a log management filter of **matches** `*foo*` and select the menu item **Run in Explore Logs page**, the Explore Logs query equates the log management filter to **match regexp** `^.*foo.*$`, which might not match all the same log events.

Another example is **matches** `foo`, which when run on Explore Logs is treated as **contains** `foo`. Because the Explore Logs function also searches keyword queries, **contains** `foo` is likely to match more events than **matches** `foo`.

You can change the operators used by Explore Logs to address these differences.

- Change the **contains** operator to **matches regex**.
- Change occurrences of `*` from log management filters to **.*** and prefix filter terms with **.***. For example, change the event filter expression **matches** `*foo*` to **matches regex** `.*foo.*` for Explore Logs.
- For the **does not match** operator from event filters, you can use the **matches regex** operator with a regex look ahead value. For example, **does not match** `*foo*` is equivalent to **matches regex** .*(?!foo).*

Configure Log Forwarding to VMware Aria Operations for Logs (SaaS)

Add a cloud forwarder to forward logs from a VMware Aria Operations for Logs server to VMware Aria Operations for Logs (SaaS) without using a Cloud Proxy.

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://`operations-for-logs-host`, where `operations-for-logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Verify that you have integrated your VMware Aria Operations for Logs server with a VMware Aria Operations for Logs (SaaS) service. See Integrate VMware Aria Operations for Logs with VMware Aria Operations for Logs (SaaS) for more information.

Use cloud forwarding to send filtered or tagged events to VMware Aria Operations for Logs (SaaS). Cloud forwarding lets you consolidate logging over different networks and eventually concentrate data in VMware Aria Operations for Logs (SaaS).

1. Expand the main menu, click **Log Management**, and then click **Cloud Forwarding**.

2. Click **New Forwarder** and provide the following information.

Option	Description
Name	A unique name for the cloud forwarder.
	NOTE
	Once you assign a name for the forwarder, you cannot modify the name.
Cloud channel	Select the cloud channel you created on the **VMware Aria Operations for Logs (SaaS)** page.
Tags	Optionally, add tag pairs with predefined values. Tags let you query logs easily. You can add multiple comma-separated tags.
Filter	Control which logs are forwarded to VMware Aria Operations for Logs (SaaS).
	Select static fields and constraints to define the desired logs. If you do not select a filter, all logs are forwarded. You can see the results of the filter you are building by clicking **Run in Explore Logs page**.
	For information about using filters in a cloud forwarder, see Using Log Management Filters in Explore Logs.

3. Optional: To modify additional cloud forwarding information, click **Show Advanced Settings**.

Option	Description
Worker Count	The number of simultaneous outgoing connections to use. Set a higher worker count for a higher network latency to VMware Aria Operations for Logs (SaaS) and for a greater number of forwarded logs per second. The default value is 16.

4. Click **Save**.

The relevant logs are forwarded to the VMware Aria Operations for Logs (SaaS) service. You can query these logs in the **Explore Logs** page of the service.

Synchronize the Time on the VMware Aria Operations for Logs Virtual Appliance

You must synchronize the time on the VMware Aria Operations for Logs virtual appliance with an NTP server or with the ESX/ESXi host on which you deployed the virtual appliance.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

Time is critical to the core functionality of VMware Aria Operations for Logs.

By default, VMware Aria Operations for Logs synchronizes time with a pre-defined list of public NTP servers. If public NTP servers are not accessible due to a firewall, you can use the internal NTP server of your company. If no NTP servers are available, you can sync time with the ESX/ESXi host where you have deployed the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and navigate to **Configuration > Time**.

2. From the **Sync time with** drop-down menu, select the time source.

Option	Description
NTP server	Synchronizes the time on the VMware Aria Operations for Logs virtual appliance with one of the listed NTP servers.
ESX/ESXi host	Synchronizes the time on the VMware Aria Operations for Logs virtual appliance with the ESX/ESXi host on which you have deployed the virtual appliance.

3. Optional: If you selected NTP server synchronization, list the NTP server addresses, and click **Test**.

   NOTE
   Testing the connection to NTP servers might take up to 20 seconds per server.

4. Click **Save**.

Configure the SMTP Server for VMware Aria Operations for Logs

You can configure an SMTP to allow VMware Aria Operations for Logs to send email notifications.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

System notifications are generated when VMware Aria Operations for Logs detects an important system event, for example when the storage capacity on the virtual appliance reaches the thresholds that you set.

1. Expand the main menu and navigate to **Configuration > SMTP**.

2. Enter the SMTP server address and port number.

3. If the SMTP server uses an encrypted connection, select the encryption protocol.

4. In the **Sender** text box, type an email address to use when sending system notifications.

   The **Sender** address appears as the From address in system notification emails. It need not be a real address, and can be something that represents the specific instance of VMware Aria Operations for Logs. For example, operationsforlogs@example.com.

5. Type a user name and password to authenticate with the SMTP server when sending system notifications.

6. Type a destination email and click **Send Test Email** to verify the connection.

7. If the SMTP server provides an untrusted SSL certificate, a dialog box appears with the details of the certificate. Click **Accept** to add the certificate to the truststores of all the nodes in the VMware Aria Operations for Logs cluster.

   If you click **Cancel**, the certificate is not added to the truststores and the connection with the SMTP server fails. You must accept the certificate for a successful connection.

8. Click **Save**.

   If you did not test the connection and the SMTP server provides an untrusted certificate, follow the instructions in step 7.

Configure an HTTP Proxy

If your VMware Aria Operations for Logs appliance is restricted to the public network or the intranet, you can configure an HTTP proxy to let VMware Aria Operations for Logs send webhook notifications to endpoints such as Slack, PagerDuty, VMware Aria Automation Orchestrator, or a custom endpoint, which can be accessed through an isolated network.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and navigate to **Configuration > Proxy**.

2. Click **ADD NEW HTTP PROXY**.

3. In the **Name** text box, enter a unique name for your proxy.

4. In the **Host/IP** text box, enter the FQDN or IP address of your proxy server.

5. In the **Proxy Port** text box, enter the port of your proxy server.

6. In the **Username** and Password text boxes, enter the username and password for authentication with your proxy server while sending webhook notifications.

7. To verify that the connection with your proxy works, click **Test**.

8. Click **Save**.

You can use this HTTP proxy when you configure a webhook to send alert notifications. For more information, see Configure a Webhook.

> **NOTE**
> The cache settings on the proxy determines the validation frequency of the username and password.

Configure a Webhook

You can configure a webhook to send alert notifications to a remote web server. Webhooks provide notifications over HTTP POST/PUT.

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information.

The URL format of the web user interface is https://`operations-for-logs-host`, where `operations-for-logs-host` is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

- If you are creating a webhook with a VMware Aria Automation Orchestrator endpoint, ensure that you have created a workflow in VMware Aria Automation Orchestrator. For more information, see Create Workflows in the VMware Aria Automation Orchestrator Client.

1. Expand the main menu and navigate to **Configuration > Webhooks**.

2. Click **New Webhook**.

3. In the **Name** text box, enter a name for the webhook.

4. Enter the following information.

Option	Description
Endpoint	Select the endpoint type to which you want to send the notification: - Slack - Pager Duty - Orchestrator - Custom Depending on the endpoint type you select, the user interface provides additional input options. The user interface also populates the webhook payload with a predefined template, which you can customize according to your requirement.
Log Payload	Select whether you want to send a webhook notification for each result matching the corresponding alert query or a single webhook notification for all matching results. - To send a single webhook notification for all matching results, select **Log Stream**. - To send a webhook notification for each matching result, select **Individual Logs**.
Webhook URL	Enter the URL for the remote web server where you want to post the webhook notifications. The URL format changes based on your endpoint selection. The sample format is provided in the text box. **NOTE** In the VMware Aria Automation Orchestrator endpoint URL, you must include the ID of the corresponding workflow created in VMware Aria Automation Orchestrator. After entering the URL, click **Test Alert** to verify the connection. You can enter multiple webhook URLs separated by a blank space.
Web Proxy	If you have configured one or more HTTP proxies, select a proxy from the drop-down menu. VMware Aria Operations for Logs sends webhook notifications to the endpoint through the selected proxy.
Integration Key	If you select **Pager Duty** as the endpoint type, enter an integration key for webhook requests.

Option	Description

Advanced Settings	If you select **Orchestrator** or **Custom** as the endpoint type, you must provide more information.
	
	For the **Orchestrator** endpoint type, you can:
	
	• Enter the name and value of the **Custom Header** to authorize VMware Aria Automation Orchestrator requests. Some of the authorization options are:
	
	  • Basic authentication - retain the default value `Authorization` in the first text box. In the second text box, enter a value in the format `Basic` *`Base64_encoded_string_for_username_and_passwo`*
	  • Bearer token authentication - Retain the default value `Authorization` in the first text box. In the second text box, enter a value in the format `Bearer` *`bearer_token`*.
	
	• Select the content type. The default value for **Content Type** is **JSON**. You can change it to **XML** if required. The webhook payload is generated according to the selected content type.
	
	For the **Custom** endpoint type, you can:
	
	• Select an **Action** such as POST and PUT. The default action is POST.
	• Select the **Add Basic Authentication** check box and enter the user name and password to authenticate the credentials with the server.
	• Add headers to the request under **Custom Headers** to provide additional information, if any.

Webhook Payload	This area is auto-populated based on your selection in the **Endpoint Type** drop-down menu. You can customize the payload, which is the template of the body sent as a part of the POST/PUT webhook notification request. The body can be in XML or JSON format.
	
	The parameters in the payload are replaced with the actual values while sending the webhook notification. For example the parameter *`$(AlertName)`* is replaced with the name of the alert.
	
	    NOTE
	    For the **Orchestrator** endpoint type, the parameters should match the input or output parameters in the corresponding workflow created in VMware Aria Automation Orchestrator.

Parameters	Use the list of parameters to construct or modify the webhook payload: • `AlertName` • `AlertNameString` • `AlertType` • `AlertTypeString` • `SearchPeriod` • `SearchPeriodString` • `HitOperator` • `HitOperatorString` • `messages`

Option	Description

	• `messagesString`
	• `HasMoreResults`
	• `HasMoreResultsString`
	• `Url`
	• `UrlString`
	• `EditUrl`
	• `EditUrlString`
	• `Info`
	• `InfoString`
	• `Recommendation`
	• `RecommendationString`
	• `NumHits`
	• `NumHitsString`
	• `TriggeredAt`
	• `TriggeredAtString`
	• `SourceInfo`
	• `SourceInfoString`
	
	    NOTE
	    Except `messagesString`, all the other string parameter types have the same content.

5. Click **Save**.

    The webhook is created. You can click the **Available Actions** icon before to the webhook name to view, edit, or delete the webhook.

Configure an alert to send webhook notifications to the selected endpoint. For more information, see Add an Alert to Send Webhook Notifications.

After configuring the alert, you can view the webhook notifications in the endpoint. For example, in VMware Aria Automation Orchestrator, the webhook notifications are listed as workflow runs. In each workflow run, you can see the values for the payload parameters in the variables section.

Install a Custom SSL Certificate

By default, VMware Aria Operations for Logs installs a self-signed SSL certificate on the virtual appliance.

- Verify that your custom SSL certificate meets the following requirements.
    - The certificate allows the `SSL Client` key usage extension.
    - The CommonName contains a wildcard or exact match for the primary node or FQDN of the virtual IP address. Optionally, all other IP addresses and FQDNs are listed as subjectAltName.
    - The certificate file contains both a valid private key and a valid certificate chain.
    - The private key is generated by the RSA or the DSA algorithm.
    - The private key is not encrypted by a pass phrase.
    - If the certificate is signed by a chain of other certificates, all other certificates are included in the certificate file that you plan to import.
    - The private key and all the certificates that are included in the certificate file are PEM-encoded. VMware Aria Operations for Logs does not support DER-encoded certificates and private keys.
    - The private key and all the certificates that are included in the certificate file are in the PEM format. VMware Aria Operations for Logs does not support certificates in the PFX, PKCS12, PKCS7, or other formats.
- Verify that you concatenate the entire body of each certificate into a single text file in the following order.
    a. The Private Key - *your_domain_name*.key
    b. The Primary Certificate - *your_domain_name*.crt

    c. The Intermediate Certificate - *DigiCertCA*.crt

    d. The Root Certificate - *TrustedRoot*.crt

- Verify that you include the beginning and ending tags of each certificate in the following format.

```
-----BEGIN PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

The self-signed certificate generates security warnings when you connect to the VMware Aria Operations for Logs web user interface. If you do not want to use a self-signed security certificate, you can install a custom SSL certificate. The only feature requiring a custom SSL certificate is Log Forwarding through SSL. If you have a Cluster setup with ILB enabled, see Activate the Integrated Load Balancer for the specific requirements of a custom SSL certificate.

> **NOTE**
> The VMware Aria Operations for Logs Web user interface and the ingestion protocol `cfapi` use the same certificate for authentication.

Generate a Self-Signed Certificate

You can generate a self-signed certificate for Windows or Linux by using the OpenSSL tool.

- Download the appropriate installer for OpenSSL from https://www.openssl.org/community/binaries.html. Use the downloaded OpenSSL installer to install it on Windows.
- Edit the `openssl.cfg` file to add additional required parameters. Make sure the `[req]` section has the `req_extensions` parameter defined.

```
[req]
        .
        .
        req_extensions=v3_req #
```

- Add an appropriate Subject Alternative Name entry for the hostname or IP address of your server, for example *server-01.operationsforlogs.domain*. You cannot specify a pattern for the hostname.

```
[v3_req]
        .
        .
        subjectAltName=DNS:server-01.operationsforlogs.domain
```

```
#subjectAltName=IP:10.27.74.215
```

1. Create a folder to save your certificate files, for example `C:\Certs\OperationsforLogs`.

2. Open a command prompt and run the following command.

   ```
   C:\Certs\OperationsforLogs>openssl req -x509 -nodes -newkey 2048 -keyout server.key -out server.crt -days
   3650
   ```

   OpenSSL prompts you to supply certificate properties, including country, organization, and so on.

3. Enter the exact IP address or hostname of your VMware Aria Operations for Logs server, or the VMware Aria Operations for Logs cluster address if load balancing is enabled.

   This property is the only one for which it is mandatory to specify a value.

Two files are created, `server.key` and `server.crt`.

- `server.key` is a new PEM-encoded private key.
- `server.crt` is a new PEM-encoded certificate signed by `server.key`.

Generate a Certificate Signing Request

Generate a certificate-signing request by using the OpenSSL tool for Windows.

- Install the OpenSSL tool. See http://www.openssl.org for information about obtaining the OpenSSL tool.
- Edit the `openssl.cfg` file to add additional required parameters. Make sure the `[req]` section has the `req_extensions` parameter defined.

   ```
   [req]
           .
           .
   req_extensions=v3_req #
   ```

- Add an appropriate Subject Alternative Name entry for the hostname or IP address of your server, for example *server-01.operationsforlogs.domain*. You cannot specify a pattern for the hostname.

   ```
   [v3_req]
           .
           .
   subjectAltName=DNS:server-01.operationsforlogs.domain
   #subjectAltName=IP:10.27.74.215
   ```

1. Create a folder to save your certificate files, for example `C:\Certs\OperationsforLogs`.

2. Open a Command Prompt and run the following command to generate your private key.

   ```
   C:\Certs\OperationsforLogs>openssl genrsa -out server.key 2048
   ```

3. Create a certificate signing request by running the following command.

   ```
   C:\Certs\OperationsforLogs>openssl req -new -key server.key -out server.csr
   ```

   > **NOTE**
   > This command runs interactively and asks you a number of questions. Your certificate authority will cross check your answers. Your answers must match the legal documents regarding the registration of your company.

4. Follow the onscreen instructions and enter the information that will be incorporated into your certificate request.

   > **IMPORTANT**
   > In the Common Name field, enter the hostname or IP address of your server, for example `mail.your.domain`. If you want to include all subdomains, enter `*your.domain`.

Your certificate signing request file `server.csr` is generated and saved.

Request a Signature from a Certificate Authority

Send your certificate signing request to a Certificate Authority of your choice and request a signature.

Submit your `server.csr` file to a Certificate Authority.

> **NOTE**
> Request that the Certificate Authority encode your file in the PEM format.

The Certificate Authority processes your request and sends you back a `server.crt` file encoded in the PEM format.

Concatenate Certificate Files

Combine your key and certificate files into a PEM file.

1. Create a new `server.pem` file and open it in a text editor.

2. Copy the contents of your `server.key` file and paste it in `server.pem` using the following format.

   ```
   -----BEGIN RSA PRIVATE KEY-----
   (Your Private Key: server.key)
   -----END RSA PRIVATE KEY-----
   ```

3. Copy the contents of the `server.crt` file you received from a certificate authority and paste it in `server.pem` using the following format.

   ```
   -----BEGIN CERTIFICATE-----
     (Your Primary SSL certificate: server.crt)
   -----END CERTIFICATE-----
   ```

4. If the Certificate Authorities provided you with an intermediate or chained certificate, append the intermediate or chained certificates to the end of the public certificate file in the following format.

   ```
   -----BEGIN RSA PRIVATE KEY-----
   (Your Private Key: server.key)
   -----END RSA PRIVATE KEY-----
   -----BEGIN CERTIFICATE-----
   (Your Primary SSL certificate: server.crt)
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   (Your Intermediate certificate: DigiCertCA.crt)
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   (Your Root certificate: TrustedRoot.crt)
   -----END CERTIFICATE-----
   ```

5. Save your `server.pem` file.

Upload Signed Certificate

You can upload a signed SSL certificate.

1. Expand the main menu and navigate to **Configuration > SSL**.

2. Browse to your custom SSL certificate and click **Open**.

3. Click **Save**.

4. Restart VMware Aria Operations for Logs.

After VMware Aria Operations for Logs restarts, verify that syslog feeds from ESXi continue to arrive in VMware Aria Operations for Logs.

Configure SSL Connection Between the VMware Aria Operations for Logs Server and the VMware Aria Operations for Logs Agents

SSL function allows you to provide SSL only connections between the VMware Aria Operations for Logs Agents and the VMware Aria Operations for Logs Server through the secure flow of Ingestion API. You can also configure various SSL parameters of the VMware Aria Operations for Logs Agents.

Agents communicate over TLSv.1.2. SSLv.3/TLSv.1.0 is deactivated to meet security guidelines.

Main SSL Functions

Understanding of the main SSL functions can help you configure the VMware Aria Operations for Logs Agents properly.

The VMware Aria Operations for Logs Agent stores certificates and uses them to verify the identity of the server during all but the first connection to a particular server. If the server identity cannot be confirmed, the VMware Aria Operations for Logs Agent rejects connection with server and writes an appropriate error message to the log. Certificates received by the Agent are stored in `cert` folder.

- For Windows go to `C:\ProgramData\VMware\Log Insight Agent\cert`.
- For Linux go to `/var/lib/loginsight-agent/cert`.

When the VMware Aria Operations for Logs Agent establishes secure connection with the VMware Aria Operations for Logs Server, the Agent checks the certificate received from the VMware Aria Operations for Logs Server for validity. The VMware Aria Operations for Logs Agent uses system-trusted root certificates.

- The VMware Aria Operations for Logs Linux Agent loads trusted certificates from `/etc/pki/tls/certs/ca-bundle.crt` or `/etc/ssl/certs/ca-certificates.crt`.
- The VMware Aria Operations for Logs Windows Agent uses system root certificates.

If the VMware Aria Operations for Logs Agent has a locally stored self-signed certificate and receives a different valid self-signed certificate with the same public key, then the agent accepts the new certificate. This can happen when a self-signed certificate is regenerated using the same private key but with different details like new expiration date. Otherwise, connection is rejected.

If the VMware Aria Operations for Logs Agent has a locally stored self-signed certificate and receives valid CA-signed certificate, the VMware Aria Operations for Logs Agent silently replaces new accepted certificate.

If the VMware Aria Operations for Logs Agent receives self-signed certificate after having a CA-signed certificate, the VMware Aria Operations for Logs Agent rejects it. The VMware Aria Operations for Logs Agent accepts self-signed certificate received from VMware Aria Operations for Logs Server only when it connects to the server for the first time.

If the VMware Aria Operations for Logs Agent has a locally stored CA-signed certificate and receives a valid certificate signed by another trusted CA, the Agent rejects it. You can modify the configuration options of the VMware Aria Operations for Logs Agent to accept the new certificate. See Configure the VMware Aria Operations for Logs Agent SSL Parameters.

Agents communicate over TLSv.1.2. SSLv.3/TLSv.1.0 is deactivated to meet security guidelines.

Enforce SSL-Only Connections

You can use the VMware Aria Operations for Logs Web user interface to configure the VMware Aria Operations for Logs Agents and the Ingestion API to allow only SSL connections to the server.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

The VMware Aria Operations for Logs API is normally reachable through HTTP on port 9000 and through HTTPS on port 9543. Both ports can be used by the VMware Aria Operations for Logs Agent or custom API clients. All authenticated requests require SSL, but unauthenticated requests, includingVMware Aria Operations for Logs agent ingestion traffic, can be performed with either. You can force all API request to use SSL connections. The option does not restrict syslog port 514 traffic or affect the VMware Aria Operations for Logs user interface, for which HTTP port 80 requests continue redirecting to HTTPS port 443.

1. Expand the main menu and navigate to **Configuration > SSL**.

2. Under the API Server SSL, select **Require SSL Connection**.

3. Click **Save**.

VMware Aria Operations for Logs API allows only SSL connections to the server. Non-SSL connections are refused.

Configure the VMware Aria Operations for Logs Agent SSL Parameters

You can edit the VMware Aria Operations for Logs agent configuration file to change the SSL configuration, add a path to the trusted root certificates, and say whether the agent accepts certificates.

For the VMware Aria Operations for Logs Linux agent:

- Log in as **root** or use `sudo` to run console commands.
- Log in to the Linux machine on which you installed the VMware Aria Operations for Logs Linux agent, open a console and run `pgrep liagent` to verify that the VMware Aria Operations for Logs Linux agent is installed and running.

For the VMware Aria Operations for Logs Windows agent:

- Log in to the Windows machine on which you installed the VMware Aria Operations for Logs Windows agent and start the services manager to verify that the VMware Aria Operations for Logs agent service is installed.

This procedure applies to the VMware Aria Operations for Logs agents for Windows and Linux.

1. Navigate to the folder containing the `liagent.ini` file.

Operating system	Path
Linux	`/var/lib/loginsight-agent/`
Windows	`%ProgramData%\VMware\Log Insight Agent`

2. Open the `liagent.ini` file in any text editor.

3. Add the following keys to the `[server]` section of the `liagent.ini` file.

Key	Description
`ssl_ca_path`	Overrides the default storage path for root Certificate Authority-signed certificates, which are used to verify connection peer certificates. When you provide a path for `ssl_ca_path`, you override the defaults for both Linux and Windows agents. You can use a file where multiple certificates in PEM format are concatenated or a directory that contains certificates are in PEM format and have names of the form `hash.0`. (See the -hash option of the x509 utility.) **Linux**: If no value is specified, the agent uses the value assigned to the LI_AGENT_SSL_CA_PATH environment variable. If that value is not present, the agent attempts to load trusted certificates from the `/etc/pki/tls/certs/ca-bundle.crt` file or from the `/etc/ssl/certs/ca-certificates.crt` file. **Windows**: If no value is specified, the agent uses the value specified by the LI_AGENT_SSL_CA_PATH environment variable. If that value is not present, the VMware Aria Operations for Logs Windows agent loads certificates from the Windows root certificate store.
`ssl_accept_any`	Defines whether any certificates are accepted by the VMware Aria Operations for Logs agent. The possible values are `yes`, `1`, `no`, or `0`. When the value is set to yes or 1, the agent accepts any certificate from the server and establish secure connection for sending data. The default value is no.
`ssl_accept_any_trusted`	The possible values are yes, 1, no, or 0. If the VMware Aria Operations for Logs agent has a locally stored trusted Certificate Authority-signed certificate and receives a different valid certificate signed by a different trusted Certificate Authority, it checks the configuration option. If the value is set to yes or 1, the agent accepts the new valid certificate. If the value is set to no or 0, it rejects the certificate and ends the connection. The default value is no.
`ssl_cn`	The `Common Name` of the self-signed certificate. The default value is `VMware vCenter Log Insight`. You can define a custom `Common Name` to be checked against the certificate `Common Name` field. The VMware Aria Operations for Logs agent compares the `Common Name` field of the received certificate to the host name specified for the `hostname` key in the `[server]` section. If they do not match, the agent checks the `Common Name` text box against the `ssl_cn` key in the `liagent.ini` file. If the values match, the VMware Aria Operations for Logs agent accepts the certificate.

NOTE
These keys are ignored if SSL is deactivated.

4. Save and close the `liagent.ini` file.

Configuration

The following is an example of the SSL configuration for CA-signed certificates.

```
proto=cfapi
port=9543
ssl=yes
ssl_ca_path=/var/lib/loginsight-agent/cert
ssl_accept_any=no
ssl_accept_any_trusted=yes
ssl_cn=LOGINSIGHT
```

The following is an example of the SSL configuration for accepting any type of certificates, including self-signed.

```
proto=cfapi
port=9543
ssl=yes
ssl_accept_any=yes
```

Add, View, and Remove SSL Certificates

You can add new certificates and view the accepted SSL certificates. You can also remove certificates that you do not require anymore.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and navigate to **Management > Certificates**.

2. Do either of the following:

   - To display information about a certificate, click the information icon to the right of the thumbprint of the certificate.
   - To add a trusted certificate, click **Add New Certificate**, enter an alias name for the certificate and upload the certificate in `.pem` format.
   - To remove certificates, select the certificates and click **Delete**. Optionally, you can click the delete icon to the right of the thumbprint of each certificate.

        TIP
        You can sort and filter the certificates by using the options provided.

Change the Default Timeout Period for VMware Aria Operations for Logs Web Sessions

By default, to keep your environment secure, VMware Aria Operations for Logs Web sessions expire in 30 minutes. You can increase or decrease the timeout duration.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL

format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

> **NOTE**
> The change in the timeout period is applicable only for newly created sessions.

1. Expand the main menu and navigate to **Configuration** > **General**.

2. In the Browser Session pane, specify a timeout value in minutes.

   The value -1 deactivates session timeouts.

3. Click **Save**.

Retention and Archiving

You can retain log data in index partitions by defining different retention periods for different types of logs. For example, you can define a short retention period for logs with sensitive information. You can also archive the log data in a partition for an extended period of time. If you enable archiving for an index partition, the data in the partition is moved to an NFS mount after its retention period.

Configure an Index Partition

You can retain log data in a partition with a filter and a retention period. Index partitions let you define different retention periods for different types of logs. For example, logs with sensitive information might require a short retention period, such as five days. You can also archive the data in an index partition to an NFS mount, to retain the logs for an extended period.

- If you want to activate archiving for an index partition, verify that you have access to an NFS partition that meets the following requirements.
  - The NFS partition must allow reading and writing operations for guest accounts.
  - The mount must not require authentication.
  - The NFS server must support NFS v3 or v4.
  - If using a Windows NFS server, allow unmapped user UNIX access (by UID/GID).

  For more information about archiving, see Data Archiving.
- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

The log data that matches the filter criteria for an index partition is stored in the partition for the specified retention period. If you activate archiving, the data is moved to an NFS storage at the ingestion time. Logs that do not match the filter criteria in any of the defined index partitions are stored in the default partition. This partition is always activated and stores data for an unlimited amount of time. You can modify the retention period and activate archiving for the default partition.

NOTE

You can have a maximum of 10 index partitions.

1. Expand the main menu, click **Log Management** and then click **Index Partitions**.

2. Optional: To view details for the default partition such as the retention period and archival location, click the edit icon against the partition titled **Default** . To modify the details for the partition, click the edit icon and follow steps 7 through 9.

3. To create a partition, click **New Partition** and follow steps 5 through 9.

4. In the **Partition Name** text box, enter a name for the index partition.

5. Add one or more filters to refine the logs that you want to store in the index partition. Optionally, click **Run in Explore Logs page** to preview the filtered log results.

6. In the **Retention Period** text box, enter the number of days for which you want to retain logs in the index partition. Retain the default value `0` for an unlimited retention period.

7. Enter the location to store archived data.

    a) Click the **Archive Location** toggle button to archive the log data in the partition.

    b) In the text box, enter the NFS location where you want to store the archived data, in the format `nfs://servername:<port-number>/exportname`.

    The port number defaults to 2049.

New Partition (requires cluster restart)

Partition Name	evn_li_logs
Routing Filter	✕ text ⌄	matches ⌄	evn-li-vc-1 ✕
	+ ADD FILTER ✕ CLEAR ALL FILTERS	Run in Explore Logs page
Retention Period	0	days ⓘ
⬤ Archive Location	nfs://1692.168.3.1:2049/li_logs	TEST	ⓘ

CANCEL   SAV

    c) Click **Test** to verify the connection with the NFS storage.

8. Click **Save**.

    NOTE

    - The index partition is activated by default. To deactivate it, use the toggle button against the partition on the **Index Partitions** tab.
    - Creating, modifying, and deleting index partitions requires you to restart VMware Aria Operations for Logs on all the cluster nodes.
      After VMware Aria Operations for Logs restarts, verify that syslog feeds from ESXi continue to arrive in VMware Aria Operations for Logs.

The index partition is listed in the **Index Partitions** tab with information about whether the partition is activated, the filter criteria, retention period, storage used, and time of ingesting the first log. You can view or modify the partition details by clicking the edit icon against the partition name.

Data Archiving

Data archiving preserves old logs that might otherwise be removed from an index partition after the retention period. VMware Aria Operations for Logs can store archived data to NFS mounts.

> **NOTE**
>
> - Data archiving happens during log ingestion, as described in Key Aspects of the Event Life Cycle in *Getting Started with VMware Aria Operations for Logs*.
> - VMware Aria Operations for Logs does not manage the NFS mount used for archiving purposes. If system notifications are enabled, VMware Aria Operations for Logs sends an email when the NFS mount is about to run out of space or is unavailable.
> - Archived log events are no longer searchable. If you want to search archived logs, you must import them into a VMware Aria Operations for Logs instance. For information about importing archived log files, see Import a VMware Aria Operations for Logs Archive.
> - Do not mount NFS permanently or change the `/etc/fstab` file. VMware Aria Operations for Logs itself performs NFS mounting for you.

For information about enabling archiving in an index partition, see Configure an Index Partition.

Import a VMware Aria Operations for Logs Archive

Data archiving preserves old logs that might otherwise be removed from an index partition after the retention period. See Data Archiving. You can use the command line to import logs that have been archived in VMware Aria Operations for Logs.

- Verify that you have the root user credentials to log in to the VMware Aria Operations for Logs virtual appliance.
- Verify that you have access to the NFS server where VMware Aria Operations for Logs logs are archived.
- Verify that the VMware Aria Operations for Logs virtual appliance has enough disk space to accommodate the imported log files.
  The minimum free space in the `/storage/core` partition on the virtual appliance must equal approximately 10 times the size of the archived log that you want to import.

  > **NOTE**
  > Although VMware Aria Operations for Logs can handle historic data and real-time data simultaneously, you are advised to deploy a separate instance of VMware Aria Operations for Logs to process imported log files.

1. Establish an SSH connection to the VMware Aria Operations for Logs vApp and log in as the root user.

2. Mount the shared folder on the NFS server where the archived data resides.

3. To import a directory of archived VMware Aria Operations for Logs logs, run the following command.

   `/usr/lib/loginsight/application/bin/loginsight repository import` *Path-To-Archived-Log-Data-Folder*.

   > **NOTE**
   >
   > - To avoid the modification of the timestamp of the directory to be imported, ensure that this command is executed from a directory other than the one you want to import. Running the command from the directory you want to import results in the creation of a `JavaClient.log` file and an update of the directory's modification timestamp.
   > - Importing archived data might take a long time, depending on the size of the imported folder.

4. Close the SSH connection.

You can search, filter, and analyze the imported log events.

Format of the VMware Aria Operations for Logs Archive Files

VMware Aria Operations for Logs archives data in a specific format.

VMware Aria Operations for Logs stores archive files on an NFS server and organizes them in hierarchical directories based on archiving time. For example,

`/backup/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49/data.blob`

where `/backup` is the NFS location, `2014/08/07/16` is the archiving time, `bd234b2d-df98-44ae-991a-e0562f10a49` is the bucket ID of the bucket that stores the log files, and `data.blob` is the archived data for the bucket.

The archive data `data.blob` is a compressed file that uses VMware Aria Operations for Logs internal encoding. It contains the original content for all of the messages stored in the bucket, together with the static fields such as timestamp, hostname, source, and appname.

You can import archived data to VMware Aria Operations for Logs, export archive data to a raw text file, and extract message content from archive data. See Export a Log Insight Archive to a Raw Text File or JSON and Import a VMware Aria Operations for Logs Archive.

Export a VMware Aria Operations for Logs Archive to a Raw Text File or JSON

You can use the command line to export a VMware Aria Operations for Logs archive to a regular raw text file or in JSON format.

- Verify that you have the root user credentials to log in to the VMware Aria Operations for Logs virtual appliance.
- Verify that the VMware Aria Operations for Logs virtual appliance has enough disk space to accommodate the exported files.

    NOTE
    This is an advanced procedure. Command syntax and output formats might change in later releases of VMware Aria Operations for Logs without backward compatibility.

1. Establish an SSH connection to the VMware Aria Operations for Logs vApp and log in as the root user.

2. Create an archive directory on the VMware Aria Operations for Logs vApp.

    ```
    mkdir /archive
    ```

3. Mount the shared folder on the NFS server where the archived data resides by running the following command.

    ```
    mount -t nfs
    archive-fileshare:archive directory path /archive
    ```

4. Check the available storage space on the VMware Aria Operations for Logs vApp.

    ```
    df -h
    ```

5. Export a VMware Aria Operations for Logs archive to a raw text file.

```
        /usr/lib/loginsight/application/sbin/repo-exporter -d archive-file-directory out-
   put-file
```

For example,
```
/usr/lib/loginsight/application/sbin/repo-exporter -d /archive/2014/08/07/16/bd234b2d-
df98-44ae-991a-e0562f10a49 /tmp/output.txt
```

6. Export a VMware Aria Operations for Logs archive message content in JSON format.

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d archive-file-directory output-file.
```

For example,
```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d /archive/2014/08/07/16/bd234b2d-df98-44ae-991a-
e0562f10a49 /tmp/output.json
```

7. Close the SSH connection.

Restart the VMware Aria Operations for Logs Service

You can restart VMware Aria Operations for Logs by using the Cluster page in the Web user interface.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

> ⚠️ **CAUTION**
> Restarting VMware Aria Operations for Logs closes all active user sessions. Users of the VMware Aria Operations for Logs instance will be forced to log in again.

1. Expand the main menu and navigate to **Management** > **Cluster**.

2. Select a cluster node.

3. Click **Restart Primary** and click **Restart**.

After VMware Aria Operations for Logs restarts, verify that syslog feeds from ESXi continue to arrive in VMware Aria Operations for Logs.

Power off the VMware Aria Operations for Logs Virtual Appliance

To avoid data loss when powering off a VMware Aria Operations for Logs primary or worker node, you must power off the node by following a strict sequence of steps.

- If you plan to connect to the VMware Aria Operations for Logs virtual appliance by using SSH, verify that TCP port 22 is open.
- Verify that you have the root user credentials to log in to the VMware Aria Operations for Logs virtual appliance.

You must power off the VMware Aria Operations for Logs virtual appliance before modifying the virtual hardware of the appliance.

You can power off the VMware Aria Operations for Logs virtual appliance by using the **Power** > **Shut Down Guest** menu option in the vSphere Client. You can also use the virtual appliance console or establish an SSH connection to the VMware Aria Operations for Logs virtual appliance and run a command.

1. Establish an SSH connection to the VMware Aria Operations for Logs vApp and log in as the root user.

2. To power off the VMware Aria Operations for Logs virtual appliance, run `shutdown -h now`.

You can safely modify the virtual hardware of the VMware Aria Operations for Logs virtual appliance.

Download a VMware Aria Operations for Logs Support Bundle

If VMware Aria Operations for Logs does not operate as expected because of a problem, you can send a copy of the log and configuration files to VMware Support Services in the form of a support bundle.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

Downloading a cluster-wide support bundle is necessary only if requested by VMware Support Services. You can create the bundle either statically, which uses disk space on the node, or by streaming, which uses no disk space on the node and stores the bundle on your initiating machine by default.

The storage location for the support bundle depends on the option that you use to get the support bundle:

Option	Support Bundle Location
API - POST appliance/vm-support-bundle	This is a streaming version with no local file.
API - POST appliance/support-bundle	`/tmp/ui-support/`
Web user interface - Static support bundle	`/tmp/ui-support/`
Web user interface - Streaming support bundle	This is a streaming version with no local file.
Command line - scripts/loginsight-support	The bundle is generated in the current directory.

1. Expand the main menu and navigate to **Management > Cluster**.

2. Under the Support header, click **Download Support Bundle**.

   The VMware Aria Operations for Logs system collects the diagnostic information and sends the data to your browser in a compressed tarball.

3. Choose the method to create the bundle.

   - Select **Static support bundle** to create a bundle locally. Creation of the bundle consumes disk space on the node.
   - Select **Streaming support bundle** to start streaming the support bundle immediately. This method uses no disk space on the node.

4. Click **Continue**.

5. In the File Download dialog box, click **Save**.

6. Select a location to which you want to save the tarball archive and click **Save**.

You can review the contents of log files for error messages. When you resolve or close issues, delete the outdated support bundle to save disk space.

Activate or Deactivate VMware Customer Experience Improvement Program (CEIP)

After deploying VMware Aria Operations for Logs, by default, your account is activated to take part in the VMware Customer Experience Improvement Program (CEIP). However, you can opt out of the CEIP program.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL

format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

If you deactivate CEIP, VMware may not be able to gain proactive insights about product issues that you might be facing or effectively prioritize essential feature enhancements of the product.

After installation or upgrade of VMware Aria Operations for Logs, you can deactivate the CEIP program by following these steps.

1. Expand the main menu and navigate to **Configuration** > **General**.

2. Expand **Advanced Settings**.

3. Deactivate the **Customer Experience Improvement Program (CEIP)**option.

   Activating CEIP sends data to VMware. VMware Aria Operations for Logs uses a third-party tool called Pendo to collect analytics cookies. Pendo collects data based on your interaction with the user interface by tracking where you click, to help VMware understand how VMware Aria Operations for Logs is used. The analytics data is used to improve the VMware services and design them better. For more information, see the Privacy Notice.

4. Click **Save**.

Configure STIG Compliance for VMware Aria Operations for Logs

You can configure VMware Aria Operations for Logs to ensure STIG (Security Technical Implementation Guide) compliance for better security. This configuration includes the DoD (Department of Defense) consent agreement and additional password policy restrictions.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

When you activate STIG compliance, VMware Aria Operations for Logs sends system notifications when:

- A new user is created or an Active Directory or user logs in for the first time.
- The allocated log record storage volume reaches 75 percent of the maximum log record storage capacity of the repository. This notification is sent per node.

For more information, see VMware Aria Operations for Logs System Notifications.

1. Expand the main menu and navigate to **Configuration** > **General**.

2. In the Security Technical Implementation Guide pane, perform the relevant actions:

   - Click the **DoD Consent Agreement** toggle button to display the mandatory DoD consent agreement when a user logs in to VMware Aria Operations for Logs. Select a login message type - a simple message on the login page, a login page with a check box to accept the consent before logging in, or a consent dialog box with a button to accept the DoD consent agreement. Add a consent title and description.

     When the DoD consent agreement is activated, users can see the selected login message type when they log in.

   - Click the **Password Policy Restriction** toggle button to activate further password restrictions for user accounts and additional rules to lock the accounts.

     If the password policy restriction is activated, the following additional rules are applied to passwords:

     - A password must contain at least 15 characters.
     - A user can change their password only once in 24 hours.
     - When a user changes their password, they cannot use the last five passwords.
     - When a user changes their password, at least eight characters of the new password must be different from the old password.

If the password policy restriction is activated, a user account is locked if:

- The user has not logged in to VMware Aria Operations for Logs for 35 days.
- The user has not changed their password for 60 days.

> **NOTE**
> Super Admin user accounts are never locked.

3. Click **Save**.

Activate FIPS for VMware Aria Operations for Logs

You can configure VMware Aria Operations for Logs to ensure FIPS (Federal Information Processing Standards) compliance for better security. This set of standards describes document processing, encryption algorithms, and other information technology standards for use within United States' non-military government agencies and by government contractors and vendors who work with the agencies. When you activate FIPS, VMware Aria Operations for Logs uses the FIPS 140-2 standard with Security Level 1, which specifies basic security requirements to protect sensitive or valuable data.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

For information about how different VMware products support FIPS 140-2, see https://www.vmware.com/security/certifications/fips.html.

VMware Aria Operations for Logs uses Apache Thrift for node-to-node communication. Activating FIPS automatically enables Thrift over SSL, which makes this communication more secure. However, you can also enable Thrift over SSL without activating FIPS. For more information, see https://kb.vmware.com/s/article/82299.

1. Expand the main menu and navigate to **Configuration** > **General**.

2. In the FIPS Mode pane, click the **Activate FIPS Mode** toggle button to activate FIPS.

> ⚠️ **CAUTION**
> Once you activate FIPS, you cannot deactivate it.

3. Click **Save**.

When you save the FIPS configuration, all the nodes are rebooted. You have to wait for a few minutes before you can use VMware Aria Operations for Logs again.

Managing VMware Aria Operations for Logs Clusters

You can add, remove, and upgrade the nodes of a VMware Aria Operations for Logs cluster.

> **NOTE**
> VMware Aria Operations for Logs does not support WAN clustering. Current versions of VMware Aria Operations for Logs do not support WAN clustering (also called geo-clustering, high-availability clustering, or remote clustering). All nodes in the cluster should be deployed in the same Layer 2 LAN. In addition, the ports described in Ports and External Interfaces must be opened between nodes for proper communication.

Add a Worker Node to a VMware Aria Operations for Logs Cluster

Deploy a new instance of the VMware Aria Operations for Logs virtual appliance and add it to an existing VMware Aria Operations for Logs primary node.

Deploy the VMware Aria Operations for Logs Virtual Appliance

Download the VMware Aria Operations for Logs virtual appliance. VMware distributes the VMware Aria Operations for Logs virtual appliance as an `.ova` file. Deploy the VMware Aria Operations for Logs virtual appliance by using the vSphere Client.

- Verify that you have a copy of the VMware Aria Operations for Logs virtual appliance `.ova` file.
- Verify that you have permissions to deploy OVF templates to the inventory.
- Verify that your environment has enough resources to accommodate the minimum requirements of the VMware Aria Operations for Logs virtual appliance. See Minimum Requirements.
- Verify that you have read and understand the virtual appliance sizing recommendations. See Sizing the Virtual Appliance.

1. In the vSphere Client, select **File** > **Deploy OVF Template**.

2. Follow the prompts in the **Deploy OVF Template** wizard.

3. On the **Select Configuration** page, select the size of the VMware Aria Operations for Logs virtual appliance based on the size of the environment for which you intend to collect logs.

   Small is the minimum requirement for production environments.

   VMware Aria Operations for Logs provides preset VM (virtual machine) sizes that you can select from to meet the ingestion requirements of your environment. These presets are certified size combinations of compute and disk resources, though you can add extra resources afterward. A small configuration is suitable only for demos.

   > **NOTE**
   > If you select **Large**, you must upgrade the virtual hardware on the VMware Aria Operations for Logs virtual machine after the deployment.

4. On the Select Storage page, select a disk format.

   - **Thick Provision Lazy Zeroed** creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. The data remaining on the physical device is not erased during creation, but is zeroed out on demand later, on first write from the virtual appliance.
   - **Thick Provision Eager Zeroed** creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks.

     > **IMPORTANT**
     > Deploy the VMware Aria Operations for Logs virtual appliance with thick provisioned eager zeroed disks whenever possible for better performance and operation of the virtual appliance.
   - **Thin Provision** creates a disk in thin format. The disk expands as the amount of data saved on it increases. If your storage device does not support thick provisioning disks or you want to conserve unused disk space on the VMware Aria Operations for Logs virtual appliance, deploy the virtual appliance with thin provisioned disks.

     > **NOTE**
     > Shrinking disks on the VMware Aria Operations for Logs virtual appliance is not supported and might result in data corruption or data loss.

5. Optional: On the **Select Networks** page, set the networking parameters for the VMware Aria Operations for Logs virtual appliance. You can select the IPv4 or IPv6 protocol.

   If you do not provide network settings, such as an IP address, DNS servers, and gateway information, VMware Aria Operations for Logs uses DHCP to set those settings.

   > ⚠️ **CAUTION**
   > Do not specify more than two domain name servers. If you specify more than two domain name servers, all configured domain name servers are ignored in the VMware Aria Operations for Logs virtual appliance.

   Use a comma-separated list to specify domain name servers.

6. Optional: On the **Customize template** page, set network properties if you are not using DHCP.

   Under Application, select the **Prefer IPv6 addresses** check box if you want to run the virtual machine in a dual stack network.

   > ⚠️ **CAUTION**
   > Do not select the **Prefer IPv6 addresses** check box if you want to use pure IPv4 even with IPv6 supported in your network. Select the check box only if your network has a dual stack or pure stack support for IPv6.

7. Optional: On the **Customize template** page, select **Other Properties** and set the root password for the VMware Aria Operations for Logs virtual appliance.

   The root password is required for SSH. You can also set this password through the VMware Remote Console.

8. Follow the prompts to complete the deployment.

   For information on deploying virtual appliances, see the *VMware Aria Operations vApps Deployment and Configuration* guide.

   After you power on the virtual appliance, an initialization process begins. The initialization process takes several minutes to complete. At the end of the process, the virtual appliance restarts.

9. Navigate to the **Console** tab and verify the IP address of the VMware Aria Operations for Logs virtual appliance.

IP Address Prefix	Description
https://	The DHCP configuration on the virtual appliance is correct.
http://	The DHCP configuration on the virtual appliance failed. 1. Power off the VMware Aria Operations for Logs virtual appliance. 2. Right-click the virtual appliance and select **Edit Settings**. 3. Set a static IP address for the virtual appliance.

- If you want to configure a standalone VMware Aria Operations for Logs deployment, see Configure New Deployment. The VMware Aria Operations for Logs Web interface is available at https://*operations-for-logs-host*/ where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

Join an Existing Deployment

After you deploy and set up a standalone VMware Aria Operations for Logs node, you can deploy a new VMware Aria Operations for Logs instance and add it to the existing node to form a VMware Aria Operations for Logs cluster.

- In the vSphere Client, note the IP address of the worker VMware Aria Operations for Logs virtual appliance.
- Verify that you have the IP address or host name of the primary VMware Aria Operations for Logs virtual appliance.
- Verify that you have a user account on the primary VMware Aria Operations for Logs virtual appliance with the Super Admin role, a role that has the relevant permissions. See Create and Modify Roles for more information.

- Verify that the versions of the VMware Aria Operations for Logs primary and worker nodes are in sync. Do not add an older version VMware Aria Operations for Logs worker to a newer version VMware Aria Operations for Logs primary node.
- Synchronize the time on the VMware Aria Operations for Logs virtual appliance with an NTP server. For more information, see Synchronize the Time on the Log Insight Virtual Appliance.
- Login to the web user interface of the VMware Aria Operations for Logs primary node and generate a secure token on the **Management** > **Cluster** page.
- For information on supported browser versions, see the Release Notes.

VMware Aria Operations for Logs can scale out by using multiple virtual appliance instances in clusters. Clusters enable linear scaling of ingestion throughput, increase query performance, and allow high-availability ingestion. In cluster mode, VMware Aria Operations for Logs provides primary and worker nodes. Both primary and worker nodes are responsible for a subset of data. Primary nodes can query all subsets of data and aggregate the results. You might require more nodes to support site needs. You can use from three to 18 nodes in a cluster. This means that a fully functional cluster must have a minimum of three healthy nodes. Most nodes in a larger cluster must be healthy. For example, if three nodes of a six-node cluster fail, none of the nodes functions fully until the failing nodes are removed.

1. Use a supported browser to navigate to the web user interface of the VMware Aria Operations for Logs worker.

   The URL format is https://*operations_for_logs-host*/, where *operations_for_logs* is the IP address or host name of the VMware Aria Operations for Logs worker virtual appliance.

   The initial configuration wizard opens.

2. Click **Join Existing Deployment**.

3. Enter the following details and click **Go**.

   1. IP address or host name of the VMware Aria Operations for Logs primary node.
   2. The secure token generated on the **Management** > **Cluster** page.

   If the primary node provides an untrusted SSL certificate, a dialog box appears with the details of the certificate. Click **Accept** to send a request to the VMware Aria Operations for Logs primary node to join the existing deployment.

   If you click **Cancel**, the join request is not sent to the primary node. You must accept the certificate to ensure that the worker node joins the existing deployment.

   The worker node joins the existing deployment and VMware Aria Operations for Logs begins to operate in a cluster.

- Add more worker nodes as needed. The cluster must have a minimum of three nodes.

Remove a Worker Node from a VMware Aria Operations for Logs Cluster

You can remove a worker node that is no longer working correctly from a VMware Aria Operations for Logs cluster. Do not remove worker nodes that are operating correctly from a cluster.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL

format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

> **WARNING**
> Removing a node results in data loss. If a node must be removed, ensure that it has been backed up first. Avoid removing nodes within 30 minutes of adding new nodes.

1. Expand the main menu and navigate to **Management** > **Cluster**.

2. In the Workers table, find the node you want, click the pause icon, and click **Continue**.

   The node is now in maintenance mode.

   > **NOTE**
   > A node in maintenance mode continues to receive logs.

3. Click the cross icon to remove the node.

   VMware Aria Operations for Logs removes the node from the cluster and sends out an email notification.

Working with an Integrated Load Balancer

The VMware Aria Operations for Logs integrated load balancer (ILB) supports VMware Aria Operations for Logs clusters and ensures that incoming ingestion traffic is accepted by VMware Aria Operations for Logs even if some VMware Aria Operations for Logs nodes become unavailable. You can also configure multiple virtual IP addresses.

> **NOTE**
> Starting from version 8.14, VMware Aria Operations for Logs supports VMware NSX Advanced Load Balancer. To learn more, see the Working With VMware NSX Advanced Load Balancer documentation.

It is a best practice to include the Integrated Load Balancer (ILB) in all deployments, including single-node instances. Send queries and ingestion traffic to the ILB so that a cluster can easily be supported in the future if needed. The ILB balances traffic across nodes in a cluster and minimizes administrative overhead.

The ILB ensures that incoming ingestion traffic is accepted by VMware Aria Operations for Logs even if some VMware Aria Operations for Logs nodes become unavailable. The ILB also balances incoming traffic fairly among available VMware Aria Operations for Logs nodes. VMware Aria Operations for Logs clients, using both the web user interface and ingestion (through syslog or the Ingestion API), connect to VMware Aria Operations for Logs through the ILB address.

ILB requires that all VMware Aria Operations for Logs nodes be on the same Layer 2 networks, such as behind the same switch or otherwise able to receive ARP requests from and send ARP requests to each other. The ILB IP address must be set up so that any VMware Aria Operations for Logs node can own it and receive traffic for it. Typically, this means that the ILB IP address is in the same subnet as the physical address of the VMware Aria Operations for Logs nodes. After you configure the ILB IP address, try to ping it from a different network to ensure that it is reachable.

To simplify future changes and upgrades, you can have clients point to an FQDN that resolves to the ILB IP address, instead of pointing directly to the ILB IP address.

About Direct Server Return Configuration

The VMware Aria Operations for Logs load balancer uses a Direct Server Return (DSR) configuration. In DSR, all incoming traffic passes through the VMware Aria Operations for Logs node that is the current load balancer node. Return traffic is sent from VMware Aria Operations for Logs servers directly back to the client without needing to go through the load balancer node.

Multiple Virtual IP Addresses

You can configure up to 60 virtual IP addresses (vIPs) for the Integrated Load Balancer. You can also configure a list of static tags to each vIP so that each log message received from the vIP is annotated with the configured tags.

Activate the Integrated Load Balancer

When you activate the VMware Aria Operations for Logs integrated load balancer (ILB) on a VMware Aria Operations for Logs cluster, you must configure one or more virtual IP addresses.

- Verify that all VMware Aria Operations for Logs nodes and the specified Integrated Load Balancer IP address are on the same network.
- If you are using VMware Aria Operations for Logs with NSX, verify that the **Enable IP Discovery** option is deactivated on the NSX logical switch.
- The VMware Aria Operations for Logs primary and worker nodes must have the same certificates. Otherwise, the VMware Aria Operations for Logs Agents configured to connect through SSL reject the connection. When uploading a CA-signed certificate to VMware Aria Operations for Logs primary and worker nodes, set the Common Name to the ILB FQDN (or IP address) during the certificate generation request. See Generate a Certificate Signing Request .
- You must synchronize the time on the VMware Aria Operations for Logs virtual appliance with an NTP server. See Synchronize the Time on the Log Insight Virtual Appliance.

The Integrated Load Balancer supports one or more virtual IP addresses (vIPs). Each vIP balances incoming ingestion and query traffic among available VMware Aria Operations for Logs nodes. It is a best practice to connect all VMware Aria Operations for Logs clients through a vIP and not directly to a node.

To simplify future changes and upgrades, you can have clients point to an FQDN that resolves to the ILB IP address, instead of pointing directly to the ILB IP address. VMware vSphere, VMware Aria Operations integrations, and alert messages use the FQDN if provided. Otherwise, they use the ILB IP address. VMware Aria Operations for Logs can resolve the FQDN to the given IP address, which means that the FQDN value you provide should match what is defined in DNS.

1. Expand the main menu and navigate to **Management** > **Cluster**.

2. In the Integrated Load Balancer section, select **New Virtual IP Address** and enter the virtual IP (vIP) address to use for integrated load balancing.

3. Optional: To configure multiple virtual IP addresses, click **New Virtual IP Address** and enter the IP address. You can choose to enter the FQDN and tags.

   - Each vIP should be in the same subnet as at least one network interface on each node and the vIP must be available (not used by any other machine).
   - Tags let you add fields with predefined values to events for easier querying. You can add multiple comma-separated tags. All events coming into the system through a vIP are marked with the vIP's tags.
   - You can configure a list of static tags (key=value) for an ILB vIP, so that each log message received from the vIP is annotated with the configured tags.

4. Optional: To activate VMware Aria Operations for Logs users to access the cluster through FQDN, point the clients to the FQDN instead of directly to the configured ILB IP address.

   You might want to have clients point to an FQDN that resolves to an ILB IP address to simplify future changes and upgrades. You can have clients point to the FQDN instead of pointing directly to the ILB IP address.

5. Click **Save**.

   The Integrated Load Balancer is managed by one node in the VMware Aria Operations for Logs cluster, declared the leader for that service. The current leader is denoted by the text (ILB) next to the node.

Query the Results of In-Production Cluster Checks

The in-production cluster check service runs a battery of checks periodically at each node. You can query the latest results of the in-product cluster checks using the CLI.

For example, the service determines if the cluster is running and configured as expected or if there are any issues with integrations to other systems. Additional checks are listed below.

- Is NTP configured in a multi-host deployment?
- Can the Active Directory be reached (if it is currently configured)?
- Can Active Directory authentication occur (if it is currently configured)?
- Can the Active Directory hosts and Kerberos hosts be reached (if Active Directory is currently configured)?
- Is the system running in a non-supported two-host deployment?
- Is there enough space in `/tmp` to perform an upgrade?
- Is there enough space in `/storage/core` to perform an upgrade?
- Is `localhost` correctly placed inside `/etc/hosts`?

1. At the command line, establish an SSH connection to the VMware Aria Operations for Logs virtual appliance and log in as the root user.

2. In the command line, type `/usr/lib/loginsight/application/sbin/query-check-results.sh {username}` and press **Enter**.

   Replace `{username}` with your user name such as `root` .

   > **NOTE**
   > The `query-check-results.sh` script is only available in VMware Aria Operations for Logs version 8.12 and below.

Configuring, Monitoring, and Updating VMware Aria Operations for Logs Agents

You can centrally manage the configuration of multiple VMware Aria Operations for Logs Agents, monitor their status, and activate auto-update.

Centralized Agent Configurations and Agent Groups

Using the VMware Aria Operations for Logs server, you can configure agents from within the application's user interface. Agents poll the VMware Aria Operations for Logs server regularly to determine if new configurations are available.

You can group agents that require the same configuration. For example, you might group all VMware Aria Operations for Logs Windows agents separately from the VMware Aria Operations for Logs Linux agents.

In the **All Agents** menu, existing agent groups from content packs are listed automatically. The agents listed relate to content packs that you have already installed (for example the vSphere content pack), which use agent groups. All user-created agent groups appear under **Content Packs** > **Custom Content**, when you click **My Content** or **Shared Content**.

A user with at least a view-only admin role can export content packs with the agent group templates.

   > **NOTE**
   > - You cannot use the same content pack template more than once.
   > - Content pack groups are read-only.

Only configuration sections beginning with `[winlog]`, `[filelog]`, `[journaldlog]` and `[parser]` are used in content packs. Additional sections are not exported as part of a content pack. Only single-line comments (lines beginning with `;`) under the `[winlog]`, `[filelog]`, and `[parser]` sections, are preserved in a content pack.

NOTE

A single agent can belong to multiple agent groups and inherits all the settings from the centralized agent configuration.

You can create a configuration for the *All Agents* group as described in Create an Agent Group. If an agent is configured from the combination of a centralized agent configuration and another configuration, the agent configuration is a result of merging both the configurations. For more information about merging, see Agent Group Configuration Merging.

NOTE

Use agent groups whenever possible, and avoid using the *All Agents* configuration unless needed.

See *Working with VMware Aria Operations for Logs Agents* for information about configuring agents and merging local and server-side configurations.

Agent Group Configuration Merging

With agent groups, agents can be part of multiple groups and they can belong to the default group *All Agents*—activating centralized configuration.

Merging occurs server-side—and the resulting configuration is merged with the agent-side configuration. The merged configuration is a result of the following rules.

- The individual group configurations have a higher priority and overrides the All Agents group settings.
- The All Agents group configuration overrides the local configuration.
- You cannot configure sections with the same name in different groups except with the All Agents groups. However, the sections in individual groups have a higher priority.

NOTE

To prevent agent loss, the **hostname** and **port** parameters of an agent configuration cannot be changed centrally from the server.

The merged configuration is stored in the agent-side `liagent-effective.ini` file. For windows systems, this file is stored in `%ProgramData%\VMware\Log Insight Agent` and for Linux systems it is stored in `/var/lib/loginsight-agent/`.

Related Links

You can create a group of agents that are configured with the same parameters.

You can edit the name and description of an agent group, change the filters, and edit the configuration.

You can add an agent group that was defined as part of a content pack to your active groups and apply an agent configuration to the group.

You can delete an agent group to remove it from the active groups list.

Create an Agent Group

You can create a group of agents that are configured with the same parameters.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL

format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and navigate to **Management** > **Agents**.

2. On the **Agents** page,expand the **All agents** drop-down menu and select **New Group**.

3. Provide a unique name and a description for the agent group and click **New Group**.

   The agent group appears in the **All Agents** list, but is not saved.

4. Specify one or more filters for the agent group. To create a filter, specify a field name, an operator, and a value.

Agents

Agent_test (Not Saved)   ⌄   ↻

No Agent Information Available

⬇ Download VMware Aria Operations for Logs Agent Version 8.12.0

Use filters to select which agents receive the Agent Configuration below.

✕ IP Address   ⌄   matches   ⌄   Use TAB or ENTER to separate multiple terms

+ ADD FILTER

a) Choose one of the following fields to filter on:

- IP address
- Hostname
- Version

- OS

b) Select an operator from the drop-down menu and specify a value.

Operator	Description
matches	Finds strings that match the specified string and wildcard specification, where * means zero or more characters and ? means any single character. Prefix and postfix globbing is supported. For example, `*test*` matches strings such as `test123` or `my-test-run`.
does not match	Excludes strings that match the specified string and wildcard specification, where * means zero or more characters and ? means any single character. Prefix and postfix globbing is supported. For example, `test*` filters out `test123`, but does not exclude `mytest123`. `%test*` does not filters out `test123`, but does exclude `xtest123`
starts with	Finds strings that start with the specified character string. For example, `test` finds `test123` or `test`, but not `my-test123`.
does not start with	Excludes strings that start with the specified character string. For example, `test` filters out `test123`, but not my-test123.

Multiple filters are treated as `AND` operands, and multiple values of the same filter are treated as `OR` operands. Filters can contain wildcards, such as `*` and `?` . For example, you can select the OS filter `contains` and specify the value `windows` to identify all your Windows agents for configuration.

5. Specify the agent configuration values in the Agent Configuration section and click **Save New Group**.

The agent configuration is applied after the next polling interval.

Related Links

With agent groups, agents can be part of multiple groups and they can belong to the default group *All Agents*—activating centralized configuration.

You can edit the name and description of an agent group, change the filters, and edit the configuration.

You can add an agent group that was defined as part of a content pack to your active groups and apply an agent configuration to the group.

You can delete an agent group to remove it from the active groups list.

Edit an Agent Group

You can edit the name and description of an agent group, change the filters, and edit the configuration.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL

format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and navigate to **Management > Agents**.

2. In the **All Agents** menu, select the name of the appropriate agent group and click the pencil icon to edit it.

3. Make your changes.

Item to Edit	Action
Name or **Description**	Make the necessary changes and click **Save**.
Filters or **Configuration**	Make the necessary changes and click **Save Group**.

Related Links

With agent groups, agents can be part of multiple groups and they can belong to the default group *All Agents*—activating centralized configuration.

You can create a group of agents that are configured with the same parameters.

You can add an agent group that was defined as part of a content pack to your active groups and apply an agent configuration to the group.

You can delete an agent group to remove it from the active groups list.

Add a Content Pack Agent Group as an Agent Group

You can add an agent group that was defined as part of a content pack to your active groups and apply an agent configuration to the group.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and navigate to **Management > Agents**.

2. In the **All Agents** menu, select an agent template for the Available Templates list.

3. Click **Copy Template** to copy the content pack agent group to your active groups.

4. Click **Copy**.

5. Select the required filters and click **Save new group**.

The content pack agent group is added to the active groups and the agents are configured according to the filters that you specified.

Related Links

With agent groups, agents can be part of multiple groups and they can belong to the default group *All Agents*—activating centralized configuration.

You can create a group of agents that are configured with the same parameters.

You can edit the name and description of an agent group, change the filters, and edit the configuration.

You can delete an agent group to remove it from the active groups list.

Delete an Agent Group

You can delete an agent group to remove it from the active groups list.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and navigate to **Management > Agents**.

2. In the **All Agents** menu, select the name of the agent group to delete, by clicking the X icon next to its name.

3. Click **Delete**.

The agent group is removed from the active groups.

Related Links

With agent groups, agents can be part of multiple groups and they can belong to the default group *All Agents*—activating centralized configuration.

You can create a group of agents that are configured with the same parameters.

You can edit the name and description of an agent group, change the filters, and edit the configuration.

You can add an agent group that was defined as part of a content pack to your active groups and apply an agent configuration to the group.

Monitor the Status of the VMware Aria Operations for Logs Agents

You can monitor the status of the VMware Aria Operations for Logs Windows and Linux agents and view current statistics about their operation.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **View Only Admin** user, or a user associated with a role that has the relevant permissions.. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

Only those agents that are configured to send data through CFAPI appear on the Agents page. Agents that are configured to send data through syslog appear on the Hosts page, as with other syslog sources. If protocol changes from CFAPI to syslog, stats are not updated and represented on the Statistics page and Agent status is shown as "disconnected". Data represented there is being sent from LI Agents every 30 sec. VMware Aria Operations for Logs can display information for up to 15,000 agents.

If you change protocol from CFAPI to syslog, statistics cease to be updated and represented on the Agent page anymore and agent status is shown as disconnected. Data represented there is being sent from VMware Aria Operations for Logs agent every thirty seconds.

NOTE

If you change a host IP for a VMware Aria Operations for Logs server in agent configuration, the agent resets page stats to zero.

Expand the main menu and navigate to **Management > Agents**.

Status information for each agent that sends data with CFAPI appears.

You can use the information from the Agents page to monitor the operation of the installed VMware Aria Operations for Logs Windows and Linux agents. Click the agent hostname to go to the Explore Logs page for that host. After setting the hostname parameter from the LI Agent, and if default CFAPI proto is used and points to a VMware Aria Operations for Logs instance, you can monitor the connection by opening the Agents statistics page and verifying that the agent appears in the list of agents. You can use the links under the hostname column to navigate to the VMware Aria Operations for Logs Agents page and check the logs coming from the mentioned Agent.

Activate Agent Auto-Update from the Server

You can activate auto-update for agent groups or all agents from the VMware Aria Operations for Logs server.

- Ensure that agents have an active status are version 4.3 or later.
- Ensure that the client-side agent configuration has `auto_update` set to yes.

Auto-update applies the latest available update to the selected agent group or all agents connected to the server. You can deactivate the auto-update feature for individual servers by editing the agent's `liagent.ini` file.

NOTE

- If `auto-update=yes` is changed to `auto-update=no` in the client, you cannot activate auto-update for the agent in the server.
- If the default configuration in the client is not changed (`auto_update=yes`), the configuration in the server works. So, you can activate auto-update for all agents or agent groups using the relevant option.

For more information, see *Working with VMware Aria Operations for Logs Agents*.

Auto-update is deactivated for the server by default.

1. Expand the main menu and navigate to **Management > Agents**.

2. Do either of the following.

   - To activate auto-update for all agents, in the upper-right corner of the Agents page, click the toggle control for **Enable auto-update for all agents**.
   - To activate auto-update for an agent group, select the agent group in the agent drop-down menu and click the toggle control for **Enable auto-update for selected Agent Group**.

     NOTE
     This toggle control appears only when **Enable auto-update for all agents** is deactivated.

Agents in the selected agent group or all agents connected to this server are updated when an update is present.

Monitoring VMware Aria Operations for Logs

You can monitor the VMware Aria Operations for Logs virtual appliance and the hosts and devices that send log events to VMware Aria Operations for Logs.

Check the Health of the VMware Aria Operations for Logs Virtual Appliance

You can check available resources and active queries on the VMware Aria Operations for Logs virtual appliance, and view current statistics about the operation of VMware Aria Operations for Logs.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and navigate to **Management** > **System Monitor**.

2. If VMware Aria Operations for Logs is running as a cluster, click **Show resources for** and choose the node you want to monitor.

3. Click the buttons on the System Monitor page to view the information that you need.

Option	Description
Resources	View information about the CPU, memory, IOPS (read and write activity), and storage usage on the VMware Aria Operations for Logs virtual appliance.
	The charts on the right represent historical data for the last 24 hours, and are refreshed at five-minute intervals. The charts on the left display information for the last five minutes, and are refreshed every three seconds.
Active Queries	View information about the queries that are currently active in VMware Aria Operations for Logs.
Statistics	View statistics about the log ingest operations and rates.
	To view more detailed statistics, click **Show advanced statistics**.

You can use the information from the System Monitor page to manage resources on the VMware Aria Operations for Logs virtual appliance.

Monitor Hosts That Send Log Events

You can view a list of all hosts and devices that send log events to VMware Aria Operations for Logs and monitor them.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

Entries in host tables expire three months after the last ingested event.

Expand the main menu and navigate to **Management > Hosts**.

> **NOTE**
> If you have configured a vCenter Server to send events and alarms, but have not configured the individual ESXi hosts to send logs, the Hostname column lists both the vCenter Server and the individual ESXi hosts as the source instead of listing just the vCenter Server.

Users with a Super Admin role or relevant privileges can set up a system notification that is sent when hosts have been inactive. For more information, see Configure a System Notification to Report on Inactive Hosts.

Configure a System Notification to Report on Inactive Hosts

VMware Aria Operations for Logs includes a built-in notification that you can use to learn about which hosts have been inactive for a specified period of time.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL

format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

You activate the notification from the Hosts screen and specify a threshold that triggers the notification. You can apply this to all hosts or to smaller list of hosts.

1. Expand the main menu and navigate to **Management > Hosts**.

    NOTE
    If you have configured a vCenter Server to send events and alarms, but have not configured the individual ESXi hosts to send logs, the Hostname column lists both the vCenter Server and the individual ESXi hosts as the source instead of listing just the vCenter Server.

2. Select **Inactive hosts notification** on the **Hosts** page to display a form for configuring when and for which hosts the notification should be sent.

3. Specify how long the host should be inactive before sending a notification.

    Values can range from 10 minutes to the maximum of the host Time to Live (TTL) period, for which the default is three months.

    For example

    ```
    Send alert listing hosts that are inactive for 8hours of last received event.
    ```

4. You control which hosts are monitored for notification with the **Inactive hosts notification acceptlist** setting. When this setting is not selected, notifications are sent for all inactive hosts.

    - To have notifications sent for all inactive hosts, clear the check box.
    - To have notifications sent for only some inactive hosts, select **Inactive hosts notification acceptlist** and specify the host names in a comma-separated list.

5. Click **Save**.

System notifications are sent to the address specified on the **Configuration > SMTP** page when a host is inactive for longer than the specified limit.

Integrating VMware Aria Operations for Logs with VMware Products

VMware Aria Operations for Logs can integrate with other VMware products to use events and log data, and to provide better visibility into events that occur in a virtual environment.

Integration with VMware vSphere

You can set up VMware Aria Operations for Logs to connect to vCenter Server systems at two-minute intervals, and collect events, alarms, and tasks data from these vCenter Server systems. In addition, VMware Aria Operations for Logs can configure ESXi hosts through vCenter Server. See Connect VMware Aria Operations for Logs to a vSphere Environment.

Integration with VMware Aria Operations

You can integrate with on-premises. Integrating with the on-premises version requires additional changes to the configuration. For information about configuring on-premises to integrate with , see the *Getting Started with Aria Operations for Logs Guide*.

VMware Aria Operations for Logs and VMware Aria Operations can be integrated in two independent ways.

Notification Events

You can set up VMware Aria Operations for Logs to send notification events to VMware Aria Operations based on queries that you create. See Configure VMware Aria Operations for Logs to Send Notifications and Metrics to VMware Aria Operations.

Launch in Context

Launch in context is a feature in VMware Aria Operations that lets you launch an external application through URL in a specific context. The context is defined by the active UI element and object selection. Launch in context lets the VMware Aria Operations for Logs adapter add menu items to different views within the custom user interface and the vSphere user interface of VMware Aria Operations. See Activate Launch in Context in VMware Aria Operations for Logs.

> **NOTE**
> Notification events do not depend on the launch in context configuration. You can send notification events from VMware Aria Operations for Logs to VMware Aria Operations even if you do not enable the launch in context feature.

Integration with VMware NSX Identity Firewall

You can set up VMware Aria Operations for Logs to integrate with an NSX Manager instance. Within the NSX Manager scope, you can use NSX Identity Firewall(IDFW) to create identity based firewall rules.

After configuring the integration, add predefined third-party identity providers such as GlobalProtect or ClearPass, or custom identity providers to the configuration. VMware Aria Operations for Logs parses the auth logs from these providers, extracts user ID-to-IP mapping information, and sends the data to NSX Manager. Based on this data, IDFW defines identity based firewall rules and applies the rules to users for access control.

If the environment changes, you can:

- Change, add, or remove vSphere systems from VMware Aria Operations for Logs.
- Change or remove the instance of VMware Aria Operations to which alert notifications are sent.
- Change or remove the NSX Manager instance.
- Change the passwords that are used to connect to vSphere systems, VMware Aria Operations, and NSX Identity Firewall.

Connect VMware Aria Operations for Logs to a vSphere Environment

Before you configure VMware Aria Operations for Logs to collect alarms, events, and tasks data from your vSphere environment, you must connect VMware Aria Operations for Logs to one or more vCenter Server systems.

- For the level of integration that you want to achieve, verify that you have user credentials with enough privileges to perform the necessary configuration on the system and its hosts.

Level of Integration	Required Privileges

Events, tasks, and alarms collection	- **System** > **View**
	     NOTE
	     System > **View** is a system-defined privilege. When you add a custom role and do not assign any privileges to it, the role is created as a Read Only role with three system-defined privileges: **System** > **Anonymous**, **System** > **View**, and **System** > **Read**.

Syslog configuration on hosts	- **Host** > **Configuration** > **Change settings** - **Host** > **Configuration** > **Network configuration** - **Host** > **Configuration** > **Advanced Settings** - **Host** > **Configuration** > **Security profile and firewall**

NOTE
You must configure the permission on the top-level folder within the inventory, and verify that the **Propagate to children** check box is selected.

- Verify that you know the IP address or domain name of the vCenter Server system.
- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

VMware Aria Operations for Logs can collect two types of data from vCenter Server instances and the ESXi hosts that they manage.

- Events, tasks, and alerts are structured data with specific meaning. If configured,VMware Aria Operations for Logs pulls events, tasks, and alerts from the registered vCenter Server instances.
- Logs contain unstructured data that can be analyzed in VMware Aria Operations for Logs. ESXi hosts or vCenter Server Appliance instances can push their logs to VMware Aria Operations for Logs through syslog.

TIP
Tags let you add fields with pre-defined values to events coming from vSphere and configured ESXi hosts for easier querying. Note that comma (,) and equal (=) symbols are not supported in the tag values. The tags configured during vSphere integration can be assigned only to the logs coming from vCenter itself or from the logs coming from vCenter's ESXi hosts.

Tagging is based on the ESXi host configuration through integration.

1. Expand the main menu and navigate to **Integration > vSphere**.

2. Enter the IP address and service account credentials for a vCenter Server, and click **Test Connection**.

3. If the vSphere environment provides an untrusted SSL certificate, a dialog box appears with the details of the certificate. Click **Accept** to add the certificate to the truststores of all the nodes in the VMware Aria Operations for Logs cluster.

    If you click **Cancel**, the certificate is not added to the truststores and the connection with the vSphere environment fails. You must accept the certificate for a successful connection.

4. Optional: To register another vCenter Server, click **Add vCenter Server** and repeat steps 3 through 5.

    NOTE
    Do not register vCenter Server systems with duplicate names or IP addresses. VMware Aria Operations for Logs does not check for duplicate vCenter Server names. You must verify that the list of registered vCenter Server systems does not contain duplicate entries.

5. Click **Save**.

    If you did not test the connection and the vSphere environment provides an untrusted certificate, follow the instructions in step 4.

- Collect events, tasks, and alarms data from the vCenter Server instance that you registered. See Configure VMware Aria Operations for Logs to Pull Events, Tasks, and Alarms from vCenter Server Instance.
- Collect syslog feeds from the ESXi hosts that the vCenter Server manages. See Configure an ESXi Host to Forward Log Events to VMware Aria Operations for Logs.

VMware Aria Operations for Logs as a Syslog Server

VMware Aria Operations for Logs includes a built-in syslog server that is constantly active when the VMware Aria Operations for Logs service is running.

The syslog server listens on ports 514/TCP, 1514/TCP, and 514/UDP, and is ready to ingest log messages that are sent from other hosts. Messages that are ingested by the syslog server become searchable in the VMware Aria Operations for Logs web user interface near real time. The maximum syslog message length that VMware Aria Operations for Logs accepts is 10 KB.

Syslog formats RFC-6587, RFC-5424, and RFC-3164 are supported.

Configure an ESXi Host to Forward Log Events to VMware Aria Operations for Logs

ESXi hosts or vCenter Server Appliance instances generate unstructured log data that can be analyzed in VMware Aria Operations for Logs.

- Verify that the vCenter Server that manages the ESXi host is registered with your VMware Aria Operations for Logs instance. Or, you can register the ESXi host and configure vCenter Server in a single operation.
- Verify that you have user credentials with enough privileges to configure syslog on ESXi hosts.
  - **Host** > **Configuration** > **Advanced settings**
  - **Host** > **Configuration** > **Security profile and firewall**
        NOTE
        You must configure the permission on the top-level folder within the inventory, and verify that the **Propagate to children** check box is selected.

You use the VMware Aria Operations for Logs Integration interface to configure ESXi hosts on a registered vCenter Server to push syslog data to VMware Aria Operations for Logs.

CAUTION
Running parallel configuration tasks might result in incorrect syslog settings on the target ESXi hosts. Verify that no other user is configuring the ESXi hosts that you intend to configure.

A VMware Aria Operations for Logs cluster can use an integrated load balancer to distribute ESXi and vCenter Server Appliance syslog feeds between the individual nodes of the cluster.

For information on filtering syslog messages on ESXi hosts before messages are sent to VMware Aria Operations for Logs, see the *Configure Log Filtering on ESXi Hosts* topic in the Setting Up ESXi section, of the **vSphere Installation and Setup** guide.

For information on configuring syslog feeds from a vCenter Server Appliance, see Configure vCenter Server to Forward Log Events to VMware Aria Operations for Logs.

        NOTE
        VMware Aria Operations for Logs can receive syslog data from ESXi hosts version 5.5 and later.

1. Expand the main menu and navigate to **Integration > vSphere**.

2. In the vCenter Server table, locate the vCenter Server instance that manages the ESXi host from which you want to receive syslog feeds and click **Edit**.

3. Select the **Configure ESXi hosts to send logs to Operations for Logs** check box in the opened edit view.

    By default, VMware Aria Operations for Logs configures all reachable ESXi hosts of version 5.5 and later to send their logs through UDP.

4. Optional: To modify the default configuration values, click **Advanced Options**.

    - To change the protocol for all ESXi hosts, select **Configure all ESXi hosts**, select a protocol, and click **OK**.
    - To set up specific ESXi hosts logging only or to change the protocol for selected ESXi hosts, use the following steps:

    a. Select **Configure specific ESXi hosts**.
    b. Select one or more hosts from the **Filter by host** list.

    c. Select the syslog protocol.

        NOTE
        If you select `SSL` as your syslog protocol, you must manually download the VMware Aria Operations for Logs certificate and add it to the ESXi certificate store for each ESXi host you configure in step 4b.

    d. Click **OK**.

5. Optional: If you are using clusters, open the drop-down menu for the **Target** text box and select the hostname or IP address for the load balancer that distributes syslog feeds.

6. Click **Save**.

The ESXi host configurations are shown in the ESXi hosts configured column of the vCenter Server table. If the hosts are configured, you can click **View details** in the hosts configured column to view detailed information for the configured ESXi hosts.

Modify an ESXi Host Configuration for Forwarding Log Events to VMware Aria Operations for Logs

ESXi hosts or vCenter Server Appliance instances generate unstructured log data that can be analyzed in VMware Aria Operations for Logs.

- Verify that the vCenter Server that manages the ESXi host is registered with your VMware Aria Operations for Logs instance.
- Verify that you have user credentials with enough privileges to configure syslog on ESXi hosts.
    - **Host** > **Configuration** > **Advanced settings**
    - **Host** > **Configuration** > **Security profile and firewall**

        NOTE
        You must configure the permission on the top-level folder within the inventory, and verify that the **Propagate to children** check box is selected.

You use the VMware Aria Operations for Logs Integration interface to configure ESXi hosts on a registered vCenter Server to push syslog data to VMware Aria Operations for Logs.

CAUTION
Running parallel configuration tasks might result in incorrect syslog settings on the target ESXi hosts. Verify that no other user is configuring the ESXi hosts that you intend to configure.

After the initial configuration is set up, you can enable an option to periodically look for and automatically configure both existing and newly added vSphere ESXi hosts that are not configured yet. The currently configured protocol is used to configure the ESXi hosts automatically.

A VMware Aria Operations for Logs cluster can use an integrated load balancer to distribute ESXi and vCenter Server Appliance syslog feeds between the individual nodes of the cluster.

For information on filtering syslog messages on ESXi hosts before configured messages are sent to VMware Aria Operations for Logs, see the *Configure Log Filtering on ESXi Hosts* topic in the Setting Up ESXi section, of the **vSphere Installation and Setup** guide.

For information on configuring syslog feeds from a vCenter Server Appliance, see Configure vCenter Server to Forward Log Events to VMware Aria Operations for Logs.

VMware Aria Operations for Logs can receive syslog data from ESXi hosts version 5.5 and later.

1. Expand the main menu and navigate to **Integration > vSphere**.

2. Select the **Configure ESXi hosts to send logs to Log Insight** check box.

3. Click **Advanced Options**.

4. To change the protocol for selected ESXi hosts, use the following steps:
   a) Select one or more hosts from the **Filter by host** list.
   b) Verify that the current protocol is what you want, or select another protocol.
   c) To enable the automatic configuration of ESXi hosts with the currently configured protocol, select **Automatically configure all ESXi hosts**. When enabled, VMware Aria Operations for Logs periodically looks for and configures both existing and newly added vSphere ESXi hosts that are not configured yet.
   d) Click **Configure** to begin the configuration of the selected hosts. The ESXi dialog box closes.
   e) Click **OK** in the message dialog box.
   f) If you changed the protocol setting, click **Save** in the main window after you close the **ESXi configuration** dialog box.

5. Optional: If you are using clusters, you can specify a load balancer by opening the drop-down menu for the **Target** text box on the **vSphere Integration** page and selecting the hostname or IP address for the load balancer.

VMware Aria Operations for Logs Notification Events in VMware Aria Operations

You can configure VMware Aria Operations for Logs to send notification events to VMware Aria Operations based on the alert queries that you create.

When you configure a notification alert in VMware Aria Operations for Logs, you select a resource in VMware Aria Operations that is associated with the notification events. See Add an Alert Query to Send Notification Events to VMware Aria Operations.

Here are the sections of the VMware Aria Operations UI where notification events appear.

- **Home** > **Recommendations** dashboard > **Top Health Alerts For Descendants** widget.
- Home > **Alerts** tab.
- On all custom dashboards that include widgets with notification events.

For more information on where notification events appear, see the VMware Aria Operations documentation.

Configure vCenter Server to Forward Log Events to VMware Aria Operations for Logs

The vSphere Integration collects task and events from vCenter Server, but not the low-level internal logs from each vCenter Server component. These logs are used by the vSphere Content Pack.

For vCenter Server 6.5 and later releases, the preferred way to use native integration from VMware Aria Operations for Logs and install a VMware Aria Operations for Logs agent on it. Alternatively, the configuration can be done through the vCenter Server Appliance Management Interface.

For more information about how to forward log events from vCenter Server, see the vSphere documentation about redirecting vCenter Server Appliance log files to another machine.

For earlier versions of vSphere, although the vCenter Server Appliance contains a syslog daemon that can be used to route logs, the preferred method is to install a VMware Aria Operations for Logs agent.

For information about installing VMware Aria Operations for Logs agents, see *Working with VMware Aria Operations for Logs Agents*.

The vSphere content pack contains agent groups defining specific log files to collect from vCenter Server installations. The configuration is visible at `https://LogInsightServerFqdnOrIP/contentpack?contentPackId=com.vmware.vsphere`.

For information about working with agent groups, see Centralized Agent Configurations and Agent Groups

For information about vCenter Server log file locations, see `http://kb.vmware.com/kb/1021804` and `http://kb.vmware.com/kb/1021806`.

Connect VMware Aria Operations for Logs to VMware Cloud Gateway

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

To connect to VMware Cloud Gateway and work with cloud packs, you must:

1. Create a custom role with **EDIT_LICENSE** and **VIEW_CLUSTER** privileges.
2. Create a user and assign the custom role to the user.

1. Login to VMware Aria Operations for Logs user interface as an Administrator.

2. Expand the main menu and go to **Management** > **Access Control** > **Roles** tab.

3. Click **New Role** to create a new custom role.

4. Enter a name and description for the role.

   For example,

   Name - CustomRole.

   Description - Can connect to VMware Cloud Gateway.

5. In the **Permissions** table, expand the **Management** section and assign the following permissions to the role.

Permission	Access Level
Cluster	View
License	Edit

6. Click **Save**.

7. On the **Access Control** page, click the **Users** tab to create a new user and assign **CustomRole** to the user.

8. Click **New User**.

9. Enter the user name and email address of the user.

10. In the **Roles** table, deselect **User** and select **CustomRole** as the role for the user.

11. Click **Save**.

The assigned user will receive an email with a link to update the password. After updating the password, the user can connect VMware Aria Operations for Logs to VMware Cloud Gateway.

Configure VMware Aria Operations for Logs to Pull Events, Tasks, and Alarms from vCenter Server Instance

Events, tasks, and alerts are structured data with specific meaning. You can configure VMware Aria Operations for Logs to collect alarms, events, and tasks data from one or more vCenter Server systems.

Verify that you have user credentials with **System** > **View** privileges.

> **NOTE**
> You must configure the permission on the top-level folder within the inventory, and verify that the **Propagate to children** check box is selected.

You use the Integration UI to configure VMware Aria Operations for Logs to connect to vCenter Server systems. The information is pulled from the vCenter Server systems by using the vSphere Web Services API and appears as a vSphere content pack in the VMware Aria Operations for Logs web user interface.

1. Expand the main menu and navigate to **Integration > vSphere**.

2. In the vCenter Server table, locate the vCenter Server instance from which you want to collect data.

3. Select the **Collect vCenter Server events, tasks, and alarms** check box in the opened edit view.

4. Click **Save**.

VMware Aria Operations for Logs connects to the vCenter Server every two minutes and ingests all new information since the last successful poll.

- Analyze vSphere events using the vSphere content pack or custom queries.
- Enable vSphere content pack alerts or custom alerts.

Using VMware Aria Operations with VMware Aria Operations for Logs

Requirements for Integrating With VMware Aria Operations

As part of integrating VMware Aria Operations for Logs with VMware Aria Operations, you must specify credentials for VMware Aria Operations for Logs to authenticate against VMware Aria Operations.

Verify that the integration user account has permissions to manipulate objects in VMware Aria Operations. See Minimum Required Permissions for a Local or Active Directory User Account.

VMware Aria Operations supports both local user accounts and multiple LDAP sources. Both VMware Aria Operations and VMware Workspace ONE Access integrations are configured by a VMware Aria Operations for Logs**Super Admin** user or a user with **Integration** permissions.

If your deployment uses a VMware Workspace ONE Access integration in VMware Aria Operations for Logs, the VMware Workspace ONE Access fallback URL (Redirect URL Host) and the target field on the VMware Aria Operations integration page must have the exact same value.

- To determine the user name for a local user account:
  a) On the VMware Aria Operations web interface, go to **Adminstration** > **Access Control**.
  b) Identify or create the integration user.
  c) Note the value of the **User Name** field. You specify this user name when you configure the integration in the VMware Aria Operations for Logs user interface.
- To determine the user name format for the LDAP user account that must be provided in VMware Aria Operations for Logs, follow these instructions:
  a) On the VMware Aria Operations web interface, go to **Adminstration** > **Access Control**.
  b) Identify or create the integration user. Note the **User Name** and **Source Type** fields. For example, a user named `integration@example.com` from the source type **AD**.
  c) On the VMware Aria Operations for Logs user interface, enter the user name as a combination of the user name and source type - `user@example.com@Source`. For example, `integration@example.com@ad`.

Minimum Required Permissions for a Local or Active Directory User Account

To integrate VMware Aria Operations for Logs with VMware Aria Operations, you must specify credentials for VMware Aria Operations for Logs to authenticate against VMware Aria Operations. To manipulate objects in VMware Aria Operations, a user account must have the required permissions.

If you assign permissions to a user for Launch in Context, the user can also configure alert integration. Use the information in the alert integration table to assign permissions for alert integration only.

Table 13: Alert Integration

Action	Permissions and Objects to Select

Create a custom role with the listed permissions.	1. Administration -> Rest APIs
	   a. All other, Read, Write APIs
	   b. Read access to APIs

Assign the preceding role to the local or Active Directory user (new or existing) and select objects/object hierarchies to assign.	1. Adapter Instance -> vRealizeOpsMgrAPI [Check All] 2. vSphere Hosts and Clusters [Check All] 3. vSphere Networking [Check All] 4. vSphere Storage [Check All]

Table 14: Launch in Context Integration

Action	Permissions and Objects to Select

Create a custom role with the listed permissions.	1. Administration -> Rest APIs
	   a. All other, Read, Write APIs
	   b. Read access to APIs
	   c. Delete resource
	2. Administration -> Configuration -> Manage Resource Relationships
	3. Administration -> Resource Kind Management
	   a. Create
	   b. Edit
	4. Administration -> Resource Management
	   a. Create
	   b. Delete
	   c. Read
	5. Administration -> Access -> Access Control -> Add, Edit, or Delete a Role.
	NOTE
	This permission is required for VMware Aria Operations versions 7.0 and earlier.

Assign the preceding role to the local or Active Directory user (new or existing) and select objects/object hierarchies to assign.	Select **Allow Access to All Objects in the System**.

Configure VMware Aria Operations for Logs to Send Notifications and Metrics to VMware Aria Operations

You can configure VMware Aria Operations for Logs to send alert notifications and metrics to VMware Aria Operations by integrating VMware Aria Operations for Logs with VMware Aria Operations (On-Premises).

- Create an integration user account in VMware Aria Operations with required permissions. For more information, see Requirements for Integrating With VMware Aria Operations.
- Verify that you know the IP address or host name of the target instance.
- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

> **NOTE**
>
> In an environment running a VMware Aria Operations cluster with a configured load balancer, you can use the load balancer IP address if one is available.

Integrating with the On-Premises version requires additional changes to the VMware Aria Operations configuration. For information about configuring VMware Aria Operations On-Premises to integrate with VMware Aria Operations for Logs, see the *Getting Started with Aria Operations for Logs Guide*.

Integrating VMware Aria Operations for Logs alerts with VMware Aria Operations allows you to view all information about your environment in a single user interface.

You can send notification events from multiple VMware Aria Operations for Logs instances to a single VMware Aria Operations instance. You can also activate launch in context for a single VMware Aria Operations for Logs instance per VMware Aria Operations instance.

VMware Aria Operations for Logs uses the VMware Aria Operations REST API to create resources and relationships in VMware Aria Operations for configuring the launch-in-context adapter.

1. Expand the main menu and navigate to **Integration** > **VMware Aria Operations**.

2. Enter the IP address or host name of the primary node or the load balancer if one is configured.

3. Enter the username and password of the user account created in VMware Aria Operations. To learn more, see Requirements for Integrating With VMware Aria Operations.

4. Click **Test**.

   VMware Aria Operations for Logs uses the credentials to push notification events to VMware Aria Operations. Make sure that the configured user has the minimum permissions required for the integration to work. See Minimum Required Permissions for a Local or Active Directory User Account.

5. If VMware Aria Operations provides an untrusted SSL certificate, a dialog box appears with the details of the certificate. Click **Accept** to add the certificate to the truststores of all the nodes in the VMware Aria Operations for Logs cluster.

   If you click **Cancel**, the certificate is not added to the truststores and the connection with VMware Aria Operations fails. You must accept the certificate for a successful connection.

6. Select the relevant check boxes according to your preference:

   - To send alerts to VMware Aria Operations, select **Enable alerts integration**.
   - To allow VMware Aria Operations open VMware Aria Operations for Logs and query for object logs, select **Enable launch in context**. For more information, see Activate Launch in Context in VMware Aria Operations for Logs.
   - To calculate and send metrics to VMware Aria Operations, select **Enable metric calculation**.

7. Click **Save**.

   If you did not test the connection, or if VMware Aria Operations provides an untrusted certificate, follow the instructions in step 5.

Activate Launch in Context in VMware Aria Operations for Logs

You can configure VMware Aria Operations to display menu items related to VMware Aria Operations for Logs and launch VMware Aria Operations for Logs with an object-specific query.

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Verify that you know the IP address or host name of the target instance.
- Verify that you have the required user credentials. See Minimum Required Permissions for a Local or Active Directory User Account.

- Integrate VMware Aria Operations for Logs with VMware Aria Operations, see the VMware Aria Operations Configuration Guide.

    IMPORTANT
    One instance of VMware Aria Operations supports launch in context for only one instance of VMware Aria Operations for Logs. Because VMware Aria Operations for Logs does not check whether other instances are already registered with VMware Aria Operations, you might override the settings of another user.

1. Expand the main menu and navigate to **Integration** > **VMware Aria Operations**.

2. On the **VMware Aria Operations Integration** page, select the **Enable launch in context** check box.

    NOTE
    To enable the launch in context functionality, you must have integrated with VMware Aria Operations using administrator privileges.

3. Click **Save**.

VMware Aria Operations for Logs configures the VMware Aria Operations instance. This operation might take a few minutes.

Items related to VMware Aria Operations for Logs appear in the menus of VMware Aria Operations.

Launch a VMware Aria Operations for Logs query from the VMware Aria Operations instance. See Launch in Context from VMware Aria Operations.

Launch in Context from VMware Aria Operations

When you activate launch in context for VMware Aria Operations for Logs, a VMware Aria Operations for Logs resource is created in VMware Aria Operations.

The resource identifier contains the IP address of the VMware Aria Operations for Logs instance, and is used by VMware Aria Operations to open VMware Aria Operations for Logs.

Launch in Context in VMware Aria Operations

To activate launch in context for an object in VMware Aria Operations, you must have added the VMware Aria Operations for Logs integration on the VMware Aria Operations user interface. To learn more, see the VMware Aria Operations Configuration Guide.

1. On the VMware Aria Operations user interface, navigate to the **Environment** > **Object Browser** page.
2. Choose an object on the object browser and select the **Logs** tab.

3. Click the **Launch Operations for Logs** button.
   For example, the **Launch Operations for Logs** option on the vCenter Server page:

The **Explore Logs** page opens on the VMware Aria Operations for Logs user interface and displays the log events for the selected object.

For example, the log events for the vCenter Server in the VMware Aria Operations for Logs user interface:

NOTE

The time range of the events is limited to one hour before the **Launch Operations for Logs** option is triggered. For example, if the **Launch Operations for Logs** option is triggered at 2:00 PM, the query in VMware Aria Operations for Logs displays all log events that occurred between 1:00 PM and 2:00 PM.

Table 15: Objects in VMware Aria Operations UI and Their Corresponding Actions

Object selected in VMware Aria Operations	Action in VMware Aria Operations	Action in VMware Aria Operations for Logs
vSphere World	Opens VMware Aria Operations for Logs.	VMware Aria Operations for Logs displays the log events for the vSphere World.
vCenter Server	Opens VMware Aria Operations for Logs.	VMware Aria Operations for Logs displays the log events for the vCenter Server.
Data center	Opens VMware Aria Operations for Logs and passes the resource names of all host systems under the selected data center object.	VMware Aria Operations for Logs displays the log events that contain names of hosts within the data center.
Cluster	Opens VMware Aria Operations for Logs and passes the resource names of all host systems under the selected Cluster object.	VMware Aria Operations for Logs displays the log events that contain names of hosts within the cluster.
Host System	Opens VMware Aria Operations for Logs and passes the resource name of the selected Host object.	VMware Aria Operations for Logs displays the log events that contain the name of the selected Host system.
Virtual Machine	Opens VMware Aria Operations for Logs and passes the IP address of the selected virtual machine and the resource name of the related host system.	VMware Aria Operations for Logs displays the log events that contain the IP address of the virtual machine, and the name of the host where the virtual machine resides.

Launch in Context from VMware Aria Operations for Logs Events

The Launch in Context functionality is also available from VMware Aria Operations for Logs events.

If you have added the VMware Aria Operations integration in the VMware Aria Operations for Logs user interface, you can perform a Launch in Context from a VMware Aria Operations for Logs event by selecting the gear icon to the left of the event and selecting the option to view in VMware Aria Operations.

For information about Launch in Context from VMware Aria Operations to VMware Aria Operations for Logs, see Launch in Context from VMware Aria Operations.

1. In VMware Aria Operations for Logs, navigate to the **Explore Logs** page.

2. Locate an event that contains inventory mapping fields and hover over the event.

3. Click the gear icon and select **Open Analysis in VMware Aria Operations** from the drop-down menu.

   A new browser tab opens directing you to the VMware Aria Operations instance integrated with VMware Aria Operations for Logs. Once you authenticate, you are directed to the **Environment** > **Object Browser** section of VMware Aria Operations with the object selected.

   > **NOTE**
   > When multiple VMware Aria Operations for Logs instances are connected to the same VMware Aria Operations instance, only the last VMware Aria Operations for Logs instance integrated with VMware Aria Operations has the Launch in Context feature. This also means that the Launch in Context feature is overridden whenever a VMware Aria Operations for Logs instance is integrated with a VMware Aria Operations instance that was previously integrated with a different VMware Aria Operations for Logs instance.

Deactivate Launch in Context for VMware Aria Operations for Logs in VMware Aria Operations

You can uninstall the VMware Aria Operations for Logs adapter from the VMware Aria Operations instance to remove menu items related to VMware Aria Operations for Logs from the VMware Aria Operations user interface.

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

You use the VMware Aria Operations for Logs UI to deactivate launch in context. If you do not have access to VMware Aria Operations for Logs or if the VMware Aria Operations for Logs instance is deleted before the connection with VMware Aria Operations is deactivated, you can unregister VMware Aria Operations for Logs from the Administration UI of VMware Aria Operations. See the Help in the VMware Aria Operations Administration portal.

⚠️ **CAUTION**
One instance of VMware Aria Operations supports launch in context for only one instance of VMware Aria Operations for Logs. If another instance of VMware Aria Operations for Logs has been registered after you registered the instance that you want to deactivate, the second instance overrides the settings of the first one without notifying you.

1. Expand the main menu and navigate to **Integration** > **VMware Aria Operations**.

2. Deselect the **Enable Launch in Context** check box.

3. Click **Save**.

VMware Aria Operations for Logs configures the VMware Aria Operations instance to remove the VMware Aria Operations for Logs adapter. This operation might take a few minutes.

Add a DNS Search Path and Domain

You can add a DNS search path and domain to improve the VMware Aria Operations inventory matching.

Adding a DNS search path and domain improves matching when a virtual machine label and search domain resolve to the IP address of the host that sends log messages to VMware Aria Operations for Logs. For example, if you have a virtual machine named linux_01 in VMware Aria Operations and the hostname linux_01.company.com resolves to

192.168.10.10, then adding a search domain allows VMware Aria Operations for Logs to recognize and match that resource.

1. Perform a guest shutdown of the VMware Aria Operations for Logs virtual appliance.

2. Once the virtual machine is powered down, select **Edit Settings**.

3. Select the **vApp Options** tab.

4. From **vApp Options** > **Authoring**, click **Properties**.

5. Find the `vami.searchpath.VMware_vCenter_Log_Insight` and `vami.domain.VMware_vCenter_Log_Insight` keys.

    If the keys do not exist, create them.

    For the search path keys, use the following values:

    - **Category** is `Networking Properties`
    - **Label** is `DNS searchpath`
    - **Key class ID** is `vami`
    - **Key instance ID** is `VMware_vCenter_Log_Insight`.
    - **Type** is **Static property**, String and **User configurable**.

    For domain keys, use the same values, substituting `DNS domain` for **Label** and `domain` for **Key ID**.

6. Set the DNS search path and domain. For example, `ny01.acme.local`.

7. Power on the virtual appliance.

After VMware Aria Operations for Logs boots, you can validate the DNS configuration by logging in and viewing the contents of the `/etc/resolv.conf` file. You should see the search and domain options near the end of the file.

Remove the VMware Aria Operations for Logs Adapter

When you activate launch in context on a VMware Aria Operations 6.2 and later instance, VMware Aria Operations for Logs creates an instance of the VMware Aria Operations for Logs adapter on the VMware Aria Operations instance.

- Verify that cURL is installed on your system. Note that this tool is preinstalled in the VMware Aria Operations virtual appliance and the steps can be performed from the appliance using IP address `127.0.0.1`.
- Verify that you know the IP address or host name of the target instance.
- Depending on the VMware Aria Operations license that you own, verify that you have the minimum credentials required to remove the management pack. See Minimum Required Permissions for a Local or Active Directory User Account.

The instance of the adapter remains in the VMware Aria Operations instance when you uninstall VMware Aria Operations for Logs. As a result, the launch in context menu items continue to appear in the actions menus, and point to a VMware Aria Operations for Logs instance that no longer exists.

To deactivate the launch in context functionality in VMware Aria Operations, you must remove the VMware Aria Operations for Logs adapter from the VMware Aria Operations instance.

You can use the command line utility cURL to send REST calls to VMware Aria Operations.

> **NOTE**
> These steps are only required if Launch in Context was activated.

1. In cURL, run the following query on the VMware Aria Operations virtual appliance to find the VMware Aria Operations for Logs adapter.

```
curl -k -u "admin" https://ipaddress/suite-api/api/adapterkinds/LogInsight/resourcekinds/LogInsight-
LogServer/resources
```

Where *admin* is the administrator login name and *ipaddress* is the IP address (or hostname) of the VMware Aria Operations instance. You are prompted to enter the password for the user: *admin*.

From the curl output find the GUID value assigned to the identifier: `<ops:resource creationTime="{TIMESTAMP}" identifier="{GUID}">`. You can use this GUID value in the below command that removes the adapter instance.

2. Run the following command to remove the VMware Aria Operations for Logs adapter.

```
curl -k -u "admin" -X DELETE https://ipaddress/suite-api/api/adapters/{GUID}
```

Where *admin* is the administrator login name and *ipaddress* is the IP address (or hostname) of the VMware Aria Operations instance. You are prompted to enter the password for the user: *admin*.

VMware Aria Operations for Logs launch in context items are removed from the menus in VMware Aria Operations. For more information about launch in context, see the topic *VMware Aria Operations for Logs Launch in Context* of the VMware Aria Operations for Logs in-product help.

VMware Aria Operations Content Pack for VMware Aria Operations for Logs

The VMware Aria Operations content pack for VMware Aria Operations for Logs contains dashboards, extracted fields, saved queries, and alerts that are used to analyze all logs redirected from a VMware Aria Operations instance.

The VMware Aria Operations content pack provides a way to analyze all logs redirected from a VMware Aria Operations instance. The content pack contains dashboards, queries, and alerts to provide diagnostics and troubleshooting capabilities to the VMware Aria Operations administrator. The dashboards are grouped according to the major components of VMware Aria Operations such as Analytics, UI, and Adapters to provide better manageability. You can enable various alerts to send notification events in VMware Aria Operations and emails to administrators.

You can download the VMware Aria Operations content pack from VMware Marketplace.

See Working with Content Packs.

Integrate VMware Aria Operations for Logs with NSX Identity Firewall

Create a configuration to connect VMware Aria Operations for Logs to an NSX Manager instance. Within the NSX Manager scope, you can use NSX Identity Firewall(IDFW) to create identity based firewall rules.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface. The URL format of the web user interface is https://*operations_for_logs*, where *operations_for_logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

1. Expand the main menu and navigate to **Integration > NSX Identity Firewall**.

2. Enter the IP address or host name and admin credentials for the NSX Manager instance, and click **Test**.

> **NOTE**
> You must have the **Enterprise Administrator** role in the NSX Manager instance to perform this step.

3. If the NSX Manager instance provides an untrusted SSL certificate, a dialog box appears with the details of the certificate. Click **Accept** to add the certificate to the truststores of all the nodes in the VMware Aria Operations for Logs cluster.

   If you click **Cancel**, the certificate is not added to the truststores and the connection with the NSX Manager instance fails. You must accept the certificate for a successful connection.

4. Click **Save**.

   If you did not test the connection and the NSX Manager instance provides an untrusted certificate, follow the instructions in step 4.

After configuring the integration, add predefined or custom identity providers to the configuration. For more information, see Add an Identity Provider to an NSX Identity Firewall Integration.

Add an Identity Provider to an NSX Identity Firewall Integration

After configuring the integration of VMware Aria Operations for Logs with NSX Identity Firewall(IDFW), add a predefined third-party identity provider such as GlobalProtect or ClearPass to the configuration. You can also add a custom identity provider.

- Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.
- Verify that you have an IDFW integration configuration in VMware Aria Operations for Logs.

1. Expand the main menu and navigate to **Integration > NSX Identity Firewall**.

2. Under Provider, click **New Provider**.

3. Enter the following information:

Option	Description
Name	A unique name for your identity provider.
Type	The identity provider type. You can select a predefined provider such as GlobalProtect or ClearPass, or a custom provider. If you select a predefined provider, the regex patterns for **Username**, **IP Address**, **Domain**, and **Event Type** are populated based on the provider. You can modify these values. If you select a custom provider, you must enter the regex patterns for **Username**, **IP Address**, and **Domain**.
Username	The regex pattern to identify the user name in the logs from your provider.
IP Address	The regex pattern to identify the IP address in the logs from your provider.
Domain	The regex pattern to identify the domain in the logs from your provider.
Event Type	The regex pattern to identify the event type in the logs from your provider. The event type for custom providers is `Login` and is not mandatory. If you want another value, enter a regex pattern to identify the event type.

Option	Description
Source	One or more source IP addresses or FQDNs. You can separate multiple entries by using commas. VMware Aria Operations for Logs parses the logs only from the sources that you enter for your provider, for optimal performance and security. • To ensure optimal performace, VMware Aria Operations for Logs applies the regex patterns only to the logs from the selected sources. • To ensure security, VMware Aria Operations for Logs sends only valid data from known sources to NSX Manager.

NOTE

- For custom providers that are sending logs through syslog, the regex patterns for the fields are applied to the message, and not the syslog headers.
- regex patterns are case sensitive.
- For regex field definitions, you must use Java-based regex.
- Forwarding logs from a VMware Aria Operations for Logs instance can change the source, which is used for provider configuration. Instead, send logs directly from the identity provider to VMware Aria Operations for Logs.
- Ensure that a provider source is unique within the scope of an NSX IDFW integration configuration.
- Predefined providers are configured for certain versions of the identity providers, which are available in the VMware Aria Operations for Logs user interface. The pre-populated regex pattern might not be accurate for other versions.

4. Click **Save**.

VMware Aria Operations for Logs parses the auth logs from your identity provider, extracts user ID-to-IP mapping information, and sends the data to NSX Manager. Based on this data, IDFW defines identity based firewall rules and applies the rules to users for access control.

regex Parsing for GlobalProtect and ClearPass Logs

- Consider the following log sample from a GlobalProtect provider:
  ```
  Apr 8 14:35:19 PA-500-GW-1-EAT1 1,2021/04/08
  14:35:19,009401010000,USERID,login,2049,2021/04/08
  14:35:19,vsys1,10.20.30.40,vmware\john,UID-
  SJC31,0,1,10800,0,0,agent,,79021111,0x8000000000000000,0,0,0,0,,PA-500-GW-1-
  EAT1,1,,2021/04/08 14:35:28,1,0x80000000,vmware\john
  ```
  The following table shows the mapping between the regex patterns and the values in the log sample, which VMware Aria Operations for Logs sends to NSX Manager.

Option	regex Pattern	Log Value
Username	`\\(\w+)\,`	`john`
IP Address	`\,(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\,`	`10.20.30.40`
Domain	`\,(\w+)\\`	`vmware`
Event Type	`USERID\,(\w+)\,`	`login`

- Consider the following log sample from a ClearPass provider:

```
2021-08-19 13:47:46,797 10.10.100.10 Insight Logs 10000111
1 0 Auth.Username=smith,Auth.Service=SOF6 vrealize SSID
EAP-TLS Service,Auth.NAS-IP-Address=10.02.20.02,Auth.Host-
MAC-Address=111aaaaab10b,Auth.Protocol=RADIUS,Auth.Login-
Status=9002,Auth.Enforcement-Profiles=[Deny Access Profile]
```

The following table shows the mapping between the regex patterns and the values in the log sample, which VMware Aria Operations for Logs sends to NSX Manager.

Option	regex Pattern	Log Value
Username	`Username=(\w+)`	`smith`
IP Address	`Address=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`	`10.02.20.02`
Domain	`SOF6\s+(\w+)`	`vrealize`
Event Type	`Auth.(\w+)-Status=`	`Login`

Integrate VMware Aria Operations for Logs with VMware Aria Operations for Logs (SaaS)

Add a cloud channel to forward logs from a VMware Aria Operations for Logs server to VMware Aria Operations for Logs (SaaS) without using a Cloud Proxy.

Verify that you are logged in to the VMware Aria Operations for Logs web user interface as a **Super Admin** user, or a user associated with a role that has the relevant permissions. See Create and Modify Roles for more information. The URL format of the web user interface is https://*operations-for-logs-host*, where *operations-for-logs-host* is the IP address or host name of the VMware Aria Operations for Logs virtual appliance.

> **NOTE**
> You can add only one VMware Aria Operations for Logs (SaaS) connection in VMware Aria Operations for Logs.

1. Expand the main menu and go to **Integrations** > **Operations for Logs (SaaS)**.

2. On the **VMware Aria Operations for Logs (SaaS)** page, provide the following information:

Option	Description
Cloud Channel Name	A unique name for the cloud channel. **NOTE** Once you assign a name for the channel, you cannot modify the name.
Cloud URL	The API URL that appears in the pop-up window when you generate an API key in VMware Aria Operations for Logs (SaaS). For more information, see Securing Logs with API Keys in *Using VMware Aria Operations for Logs (SaaS)*.
Cloud Key	The API key generated in VMware Aria Operations for Logs (SaaS). **NOTE** • The API key is unique for each connection and must not be used anywhere else. • When you regenerate the API key in VMware Aria Operations for Logs (SaaS), make sure to update it in the **VMware Aria Operations for Logs (SaaS)** page.

3. Click **Save**.

Use your cloud channel to configure a log forwarder to VMware Aria Operations for Logs (SaaS). For more information, see Configure Log Forwarding to VMware Aria Operations for Logs (SaaS).

Security Considerations for VMware Aria Operations for Logs

Use VMware Aria Operations for Logs features to safeguard your environment from attack.

Ports and External Interfaces

VMware Aria Operations for Logs uses specific required services, ports, and external interfaces.

To view information about the ports and protocols of VMware Aria Operations for Logs, see the VMware Ports and Protocols tool.

Communication Ports

VMware Aria Operations for Logs uses the communication ports and protocols listed in the Ports and Protocols tool. The required ports are organized based on whether they are required for sources, for the user interface, between clusters, for external services, or whether a firewall can safely block them. Some ports are used only if you enable the corresponding integration.

> **NOTE**
> VMware Aria Operations for Logs does not support WAN clustering (also called geo-clustering, high-availability clustering, or remote clustering). All nodes in the cluster should be deployed in the same Layer 2 LAN. Also, communication ports must be opened between nodes for proper exchange of information.

VMware Aria Operations for Logs network traffic has several sources.

Admin Workstation
> The machine that an administrator uses to manage the VMware Aria Operations for Logs virtual appliance remotely.

User Workstation
> The machine on which a VMware Aria Operations for Logs user uses a browser to access the Web interface of VMware Aria Operations for Logs.

System sending logs
> The endpoint that sends logs to VMware Aria Operations for Logs for analysis and search. For example, endpoints include ESXi hosts, virtual machines or any system with an IP address.

VMware Aria Operations for Logs Agents
> The agent that resides on a Windows or Linux machine and sends operating system events and logs to VMware Aria Operations for Logs over APIs.

VMware Aria Operations for Logs appliance
> Any VMware Aria Operations for Logs virtual appliance, primary, or worker where the VMware Aria Operations for Logs services reside. The base operating system of the appliance is SUSE 11 SP3.

Ports Required for Sources Sending Data

These ports must be open to network traffic from sources that send data to VMware Aria Operations for Logs, both for connections from outside the cluster and connections load-balanced between cluster nodes.

Ports Required for the User Interface

These ports must be open to network traffic that must use the VMware Aria Operations for Logs user interface, both for connections outside the cluster and connections load-balanced between cluster nodes.

Ports Required Between Cluster Nodes

These ports should only be open on a VMware Aria Operations for Logs primary node for network access from worker nodes for maximum security. These ports are in addition to the ports used for sources and UI traffic that are load-balanced between cluster nodes.

Ports Required for External Services

These ports must be open for outbound network traffic from VMware Aria Operations for Logs cluster nodes to remote services.

VMware Aria Operations for Logs Configuration Files

Some configuration files contain settings that affect VMware Aria Operations for Logs security.

> **NOTE**
> All security-related resources are accessible by the root account. Protecting this account is critical to the security of .

Table 16: Configuration Files

File	Description
`/usr/lib/loginsight/application/etc/loginsight-config-base.xml`	The default system configuration for VMware Aria Operations for Logs.
`/storage/core/loginsight/config/loginsight-config.xml#`*number*	The modified (from the default) system configuration forVMware Aria Operations for Logs.
`/usr/lib/loginsight/application/etc/jaas.conf`	The configuration for active directory integration.
`/usr/lib/loginsight/application/etc/3rd_config/server.xml`	The system configuration for Apache Tomcat server.
`/storage/var/loginsight/apache-tomcat/conf/tomcat-users.xml`	The system configuration for Apache Tomcat server.
`/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/server.xml`	The system configuration for Apache Tomcat server.
`/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/tomcat-users.xml`	User information for Apache Tomcat server.

VMware Aria Operations for Logs Public Key, Certificate, and Keystore

The public key, the certificate, and the keystore of VMware Aria Operations for Logs are located on the VMware Aria Operations for Logs virtual appliance.

NOTE

All security-related resources are accessible by the root account. Protecting this account is critical to the security of .

Description	Location

The keystore for user-facing end points such as APIs and web interfaces.	• Default mode:
	`/usr/lib/loginsight/application/3rd_party` `/apache-tomcat-*/conf/keystore`
	• FIPS mode:
	`/usr/lib/loginsight/application/3rd_party` `/apache-tomcat-*/conf/keystore.bcfks`

The keystore for node to node communication.	Default mode: • `/usr/lib/loginsight/application/etc/trust` `store` • `/usr/lib/loginsight/application/etc/3rd_c` `onfig/keystore` FIPS mode: • `/usr/lib/loginsight/application/etc/trust` `store.bcfks` • `/usr/lib/loginsight/application/etc/3rd_c` `onfig/keystore.bcfks`
The default certificate for VMware Aria Operations for Logs.	`/usr/lib/loginsight/application/etc/certs/de` `fault.pem`
The cluster certificate for VMware Aria Operations for Logs.	`/usr/lib/loginsight/application/etc/certs/cl` `uster.pem`

NOTE

The cluster certificate is generated only when you add a custom certificate to VMware Aria Operations for Logs.

VMware Aria Operations for Logs License and EULA File

The end-user license agreement (EULA) and license file are located on the VMware Aria Operations for Logs virtual appliance.

NOTE

All security-related resources are accessible by the root account. Protecting this account is critical to the security of .

File	Location
License	`/usr/lib/loginsight/application/etc/license/` `loginsight_dev.dlf`
License	`/usr/lib/loginsight/application/etc/license/` `loginsight_cpu.dlf`
License	`/usr/lib/loginsight/application/etc/license/` `loginsight_osi.dlf`
License Key file	`/usr/lib/loginsight/application/etc/license/` `loginsight_license.bak`
End-user license agreement	`/usr/lib/loginsight/application/etc/license/` `release/eula.txt`

Log Files for VMware Aria Operations for Logs

The files that contain system messages are on the VMware Aria Operations for Logs virtual appliance.

The following table lists each file and its purpose.

If you need information on log rotation or log archiving for these files, see Data Archiving and Log Rotation Schemes Supported by VMware Aria Operations for Logs Agents in the *Working with VMware Aria Operations for Logs Agents* guide.

File	Description
`/var/log/vmware/loginsight/alert.log`	Used to track information about user-defined alerts that have been triggered.
`/var/log/vmware/loginsight/apache-tomcat/logs/*.log`	Used to track events from the Apache Tomcat server.
`/var/log/vmware/loginsight/cassandra.log`	Used to track cluster configuration storage and replication in Apache Cassandra.
`/var/log/vmware/loginsight/plugins/vsphere/li-vsphere.log`	Used to trace events related to integration with VMware vSphere Web Client.
`/var/log/vmware/loginsight/loginsight_daemon_stdout.log`	Used for the standard output of VMware Aria Operations for Logs daemon.
`/var/log/vmware/loginsight/phonehome.log`	Used to track information about trace data collection sent to VMware (if enabled).
`/var/log/vmware/loginsight/scheduled_reports.log`	Used to track logs related to scheduled reports generation.
`/var/log/vmware/loginsight/runtime.log`	Used to track all run time information related to VMware Aria Operations for Logs.
`/var/log/firstboot/stratavm.log`	Used to track the events that occur at first boot and configuration of the VMware Aria Operations for Logs virtual appliance.
`/var/log/vmware/loginsight/systemalert.log`	Used to track information about system notifications that VMware Aria Operations for Logs sends. Each alert is listed as a JSON entry.
`/var/log/vmware/loginsight/systemalert_worker.log`	Used to track information about system notifications that a VMware Aria Operations for Logs worker node sends. Each alert is listed as a JSON entry.
`/var/log/vmware/loginsight/ui.log`	Used to track events related to the VMware Aria Operations for Logs user interface.
`/var/log/vmware/loginsight/ui_runtime.log`	Used to track runtime events related to the VMware Aria Operations for Logs user interface.
`/var/log/vmware/loginsight/upgrade.log`	Used to track events that occur during a VMware Aria Operations for Logs upgrade.
`/var/log/vmware/loginsight/usage.log`	Used to track all queries.
`/var/log/vmware/loginsight/vrops_integration.log`	Used to track events related to the VMware Aria Operations integration.
`/var/log/vmware/loginsight/watchdog_log*`	Used to track the run time events of the watch dog process, which is responsible for restarting VMware Aria Operations for Logs if it is shut down for some reason.

File	Description
`/var/log/vmware/loginsight/api_audit.log`	Used to track the API calls to VMware Aria Operations for Logs.
`/var/log/vmware/loginsight/pattern_matcher.log`	Used to track the pattern matching times and timeouts for field extraction.
`/var/log/vmware/loginsight/audit.log`	Used to track how VMware Aria Operations for Logs is used. For more information, see Audit Logs in VMware Aria Operations for Logs.

Log Messages Related to Security

The `ui_runtime.log` file contains user audit log messages in the following format.

- `[2019-05-10 11:28:29.709+0000] ["https-jsse-nio-443-exec-9"/10.153.234.136 DEBUG] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User login success: vIDM: SAM=myusername, Domain=vmware.com, UPN=myusername@vmware.com]`
- `[2019-05-10 11:28:45.812+0000] ["https-jsse-nio-443-exec-3"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User logged out: vIDM: SAM=myusername, Domain=vmware.com, UPN=myusername@vmware.com]`
- `[2019-05-10 11:28:29.709+0000] ["https-jsse-nio-443-exec-9"/10.153.234.136 DEBUG] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User login success: Active Directory User: SAM=myusername, Domain=vmware.com,UPN=myusername@vmware.com]`
- `[2019-05-10 11:28:45.812+0000] ["https-jsse-nio-443-exec-3"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User logged out: Active Directory User: SAM=myusername, Domain=vmware.com,UPN=myusername@vmware.com]`
- `[2019-05-10 11:29:28.330+0000] ["https-jsse-nio-443-exec-6"/10.153.234.136 DEBUG] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User login success: Local User: Name=myusername]`
- `[2019-05-10 11:29:47.078+0000] ["https-jsse-nio-443-exec-10"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User logged out: Local User: Name=myusername]`
- `[2019-05-10 11:29:23.559+0000] ["https-jsse-nio-443-exec-7"/10.153.234.136 WARN] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User login failure: Bad username/password attempt (username: incorrectUser)]`
- `[2019-05-10 11:45:37.795+0000] ["https-jsse-nio-443-exec-7"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: Local User: Name=myusername]`
- `[2019-05-10 11:09:50.493+0000] ["https-jsse-nio-443-exec-6"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: vIDM: SAM=myusername, Domain=vmware.com, UPN=myusername@vmware.com]`
- `[2019-05-10 11:47:05.202+0000] ["https-jsse-nio-443-exec-10"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new group: (directoryType= VIDM, domain=vmware.com, group=vidm_admin)]`
- `[2019-05-10 11:58:11.902+0000] ["https-jsse-nio-443-exec-4"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed groups: [class com.vmware.loginsight.database.dao.RBACADGroupDO<vidm/vmware.com/vidm_admin>]]`

Some logs are available in debug level. For information about enabling the debug level for each node, see Enable Debug Level for User Audit Log Messages.

TIP

If you are an administrator, you can modify the logging level without restarting the VMware Aria Operations for Logs service. Go to http://*<your_Operations_for_Logs_host>*/internal/config, update the value of the logging level for the relevant logs, and click **Save**. For example:

```
<self-logging>
    <logger name="root" level="INFO" />
</self-logging>
```

You can change the logging level to `OFF` , `FATAL` , `ERROR` , `WARN` , `INFO` , `DEBUG` , `TRACE` , or `ALL` .

NOTE

Each node in a VMware Aria Operations for Logs cluster has its own `ui_runtime.log` file. You can examine the log files of the nodes to monitor the cluster.

Activate Debug Level for User Audit Log Messages

You can activate the debug level for user audit log messages to include the log messages in the `ui_runtime.log` file.

Verify that you have the root user credentials to log in to the VMware Aria Operations for Logs virtual appliance.

1. Navigate to the location `/usr/lib/loginsight/application/etc/` and open the configuration file `loginsight-config-base.xml` in any text editor.

2. Add a new logger for `LoginActionBean` with the `DEBUG` login level:

```
<loggers>
    <logger name="com.vmware.loginsight.web" level="${uiLevel}" additivity="false">
      <appenderRef ref="UI_RUNTIME_FILE"/>
</loggers>
```

3. Save and close the `loginsight-config-base.xml` file.

4. Run the `service loginsight restart` command to apply your changes.

    TIP

    You can also activate the debug level for user audit logs without restarting the VMware Aria Operations for Logs service. For more information, see Log Files for VMware Aria Operations for Logs.

Audit Logs in VMware Aria Operations for Logs

Audit logs track how VMware Aria Operations for Logs is used.

The audit log file `audit.log` is located in `/var/log/vmware/loginsight/`. This file logs the following actions:

Category	Logged Actions
User authentication	• Login, logout, and authentication failures.
Access control	• Creating, removing, and modifying users, groups, roles, and datasets.
Configuration	• Creating and removing forwarders, vSphere and VMware Aria Operations integrations, and so on. • Changing configuration values such as session timeout, SSL, SMTP configuration, and so on.
Content packs	• Installing, uninstalling, and upgrading. • Importing and exporting.
Dashboards and widgets	• Creating, removing, and modifying. • Sharing dashboards.
Administration	• Configuring agents and enabling auto-update. • Upgrading clusters. • Adding and removing certificates and licenses.
Alerts	• Creating, removing, and modifying.
Explore logs	• Creating, removing, and modifying snapshots and extracted fields.

VMware Aria Operations for Logs User Accounts

You must set up a system and a root account to administer VMware Aria Operations for Logs.

VMware Aria Operations for Logs Root User

VMware Aria Operations for Logs currently uses the root user account as the service user. No other user is created.

Unless you set the root password property during deployment, the default root password is blank. You must change the root password when you log in to the VMware Aria Operations for Logs console for the first time.

SSH is deactivated until the default root password is set.

The root password must meet the following requirements.

• Must be at least eight characters long
• Must contain at least one uppercase letter, one lowercase letter, one digit, and one special character
• Must not repeat the same character four times

VMware Aria Operations for Logs Admin User

When you start the VMware Aria Operations for Logs virtual appliance for the first time, VMware Aria Operations for Logs creates the admin user account for its Web user interface, which is a user associated with the Super Admin role.

The default password for admin is blank. You must change the admin password in the Web user interface during the initial configuration of VMware Aria Operations for Logs.

Active Directory Support

VMware Aria Operations for Logs supports integration with Active Directory. When configured, VMware Aria Operations for Logs can authenticate or authorize a user against Active Directory.

To learn more, see Enabling User Authentication Through Active Directory.

Privileges Assigned to Default Users

The VMware Aria Operations for Logs service user has root privileges.

The Web user interface admin user has the Super Admin privileges only to the VMware Aria Operations for Logs web user interface.

VMware Aria Operations for Logs Firewall Recommendations

To protect sensitive information gathered by VMware Aria Operations for Logs, place the server or servers on a management network segment protected by a firewall from the rest of your internal network.

Required Ports

The following ports must be open to network traffic from sources that send data to VMware Aria Operations for Logs.

Port	Protocol
514/UDP, 514/TCP	Syslog
1514/TCP, 6514/TCP	Syslog-TLS (SSL)
9000/TCP	VMware Aria Operations for Logs Ingestion API
9543/TCP	VMware Aria Operations for Logs Ingestion API - TLS (SSL)

The following ports must be open to network traffic that must use the VMware Aria Operations for Logs UI.

Port	Protocol
80/TCP	HTTP
443/TCP	HTTPS

The following set of ports should only be open on a VMware Aria Operations for Logs primary node for network access from worker nodes for maximum security.

Port	Protocol
16520:16580/TCP	Thrift RPC
59778/TCP	log4j server
12543/TCP	database server

To view information about the ports and protocols of VMware Aria Operations for Logs, see the VMware Ports and Protocols tool.

Security Updates and Patches

The VMware Aria Operations for Logs virtual appliance uses VMware Photon 3.0 as the guest operating system.

VMware Aria Operations for Logs 8.0 or later comes with a Photon operating system. Photon is more secure than the SLES operating system, which accompanies VMware Aria Operations for Logs 4.8 or earlier.

VMware releases patches to address security issues in maintenance releases. You can download these patches from the VMware Aria Operations for Logs download page.

Before you apply an upgrade or patch to the guest operating system, consider the dependencies. See Ports and External Interfaces .

Backup, Restore, and Disaster Recovery

To guard against expensive data center downtime, follow these best practices for performing VMware Aria Operations for Logs backup, restoration, and disaster recovery operations.

Backup, Restore, and Disaster Recovery Overview

VMware delivers a comprehensive, integrated portfolio of Business Continuity and Disaster Recovery (BCDR) solutions that provide high availability, data protection, and disaster recovery.

Use the backup, restore, and disaster recovery information in this document for VMware Aria Operations for Logs components, including the primary node, worker node, and forwarder.

- For information about primary and worker cluster members, including configuration, log data, and customization, see Backup Nodes and Clusters.
- For information about Linux or Windows agent local configuration, see Backup Linux or Windows Agents.

The information in this document does not apply to the following tools and products. You must obtain information about these tools and products from multiple resources.

- Third-party tools used for backup, restore, and disaster recovery. For more information, see the vendor documentation.
- vSphere Data Protection, Site Recovery Manager, and Veritas NetBackup. For additional information on VMware BCDR solutions, see https://www.vmware.com/solutions/business-continuity-disaster-recovery-draas.html.
- Backup, restore, and disaster recovery capability for products that integrate with .
  - VMware Aria Operations
  - VMware vSphere Web Client server
  - ESXi hosts

Using Static IP Addresses and FQDN

You can use static IP addresses and FQDN to avoid risk during backup, restoration, and disaster recovery operations.

Static IP Addresses for VMware Aria Operations for Logs Cluster Nodes and Load Balancer

When you use static IP addresses for all nodes in a VMware Aria Operations for Logs cluster, you eliminate the need to update the IP addresses of the cluster nodes when the IP addresses change.

VMware Aria Operations for Logs includes all node IP addresses in each cluster node configuration file as described in Knowledge Base article 2123058

All products that integrate with VMware Aria Operations for Logs (ESXi, vSphere, VMware Aria Operations) use the cluster primary node's fully qualified domain name (FQDN) or IP address as the syslog target. Those products might use the FQDN or IP address of the load balancer, if configured, as the syslog target. Static IP addresses reduce the risk of constantly updating the syslog target IP address in multiple locations.

Provide static IP addresses and optional virtual IP addresses for the load balancer. When configuring an integrated load balancer, provide the optional FQDN for the virtual IP address. The FQDN is used when an IP address is not reachable for any reason.

FQDN for VMware Aria Operations for Logs Cluster Nodes and Worker Node

When you use an FQDN for all nodes in the VMware Aria Operations for Logs cluster, you can save time on post-restoration and recovery configuration changes, assuming that the same FQDN can be resolved on the recovery site.

For the primary node (load balancer when used), a fully resolvable FQDN is required. Otherwise, the ESXi hosts fail to feed the syslog messages to VMware Aria Operations for Logs or to any remote target.

For system notifications, VMware Aria Operations for Logs uses FQDN host names, if available, instead of IP addresses.

You can reasonably assume that only the underlying IP addresses change after backup and restoration or disaster recovery operations. Using FQDN eliminates the need to change the syslog target address (primary node FQDN or internal load balancer FQDN) on all the external devices that feed logs to the VMware Aria Operations for Logs cluster.

Verify that join requests from a VMware Aria Operations for Logs worker node use the FQDN of the VMware Aria Operations for Logs primary node.

The primary node host value in the configuration file on each of the nodes is based on the value used by the first worker node sending a join request. Using the FQDN of the primary node for the join request prevents making any manual changes to the primary node host value post-disaster recovery. Otherwise, the worker nodes cannot rejoin the primary node until the primary node host name is updated in the configuration files on all restored cluster nodes.

Planning and Preparation

Before implementing a backup, restoration, or disaster recovery procedure, review the planning and preparation information in this topic.

The following recommendations should be included in a backup, restoration, and disaster recovery plan.

Test Backup Operations

Perform a test run of the backup, restoration, and disaster recovery operations in a test or staging environment before performing these operations on a live production setup.

Perform a full backup of the entire VMware Aria Operations for Logs cluster. Do not rely on automatic procedures to back up individual files and configurations.

Verify Fixes

Verify that fixes are implemented and warnings and errors are addressed before performing backup, restoration, and disaster recovery operations. Backup, restoration, and disaster recovery tools usually provide visual validations and steps to ensure that backup, restoration, and disaster recovery configurations are successfully created.

Scheduling Backups

Depending on the cluster configuration, the first backup operation is usually a full backup. You should allow for an extended period of time for the first backup to complete. Successive backups, which can be incremental or full backups, finish relatively faster compared to the first backup operation.

Additional Documentation and Tools

Verify that you are following the documentation for allocating resources for the VMware Aria Operations for Logs backup, restoration, and disaster recovery tools.

Verify that you are following the tool-specific best practices and recommendations for third-party backup, restoration, and disaster recovery tools.

For virtual machines deployed using VMware products, use additional tools that can provide special features and configurations to support backup, restoration, and disaster recovery.

<u>**Forwarders and Clusters**</u>

For forwarders, apply the backup, restoration, and disaster recovery steps for the main VMware Aria Operations for Logs cluster. See Restore Nodes and Clusters.

Based on the customer requirements, you might have a single or multiple VMware Aria Operations for Logs forwarders. In addition, the forwarders can be installed as a standalone node or as a cluster. For the purpose of backup, restoration, and disaster recovery operations, VMware Aria Operations for Logs forwarders are identical to the primary VMware Aria Operations for Logs cluster nodes and handled the same way.

Backup Nodes and Clusters

It is a best practice to set up scheduled backups or replication for VMware Aria Operations for Logs nodes and clusters.

- Verify that no configuration problems exist on source and target sites before performing the backup or replication operations.
- Verify that cluster resource allocation is not at capacity.

  In configurations with reasonable ingestion and query loads, the memory and swap usage can reach almost 100% capacity during backup and replication operations. Because the memory is near capacity in a live environment, part of the memory spike is due to the VMware Aria Operations for Logs cluster usage. Also, the scheduled backup and replication operations can contribute significantly to the memory spike.

  Sometimes, worker nodes are disconnected momentarily for 1–3 minutes before rejoining primary nodes, possibly because of high memory usage.
- Reduce the memory throttling on VMware Aria Operations for Logs nodes by doing one or both of the following:
  – Allocate additional memory over the VMware Aria Operations for Logs recommended configurations.
  – Schedule the recurring backups during off-peak hours.

1. Enable regular backup or replication of VMware Aria Operations for Logs forwarders by using the same procedures that you use for the VMware Aria Operations for Logs server.

2. Verify that the backup frequency and backup types are appropriately selected based on the available resources and customer-specific requirements.

3. If the resources are not a problem and if it is supported by the tool, enable concurrent cluster node backups to speed up the backup process.

4. Back up all the nodes at the same time.

Monitoring—As the backup is in progress, check any environment or performance problems in the VMware Aria Operations for Logs setup. Most backup, restore, and disaster recovery tools provide monitoring capabilities.

During the backup process, check all the relevant logs in the production system because the user interface might not display all problems.

Backup Linux or Windows Agents

You backup agents by backing up installation and configuration information on the server side. A separate backup of the agent node is not required.

Verify that the agent configuration is on the VMware Aria Operations for Logs server side.

Agents are typically installed on Linux or Windows systems that also used for some other application or service and might be included in existing backup procedures. A full file-level or block-level backup of the machine that includes the entire agent installation and its configuration is sufficient for recovery. Agents support both local and server-provided configuration.

If the agent is configured entirely from the VMware Aria Operations for Logs server, without any local change to the `liagent.ini` configuration file, you can avoid creating a backup of the agent installation at all. Instead, perform a fresh installation of the agent and retrieve the server backup.

If the agent has a custom local configuration, backup the `liagent.ini` file and restore it along with a fresh installation of the agent. If you use the agent nodes for more than installing the agent software and if these nodes need a full backup, follow the same backup procedure as for any other virtual machine.

If the agent configuration is done on the client side (on the agents) and if the agent nodes are used only for VMware Aria Operations for Logs agent software installation, making a backup of the agent configuration file is sufficient.

1. Backup the `liagent.ini` file.

2. Replace the file on the recovered agent or Linux or Windows machine with the backup file.

Restore Nodes and Clusters

Nodes must be restored in a specific order and some restoration scenarios might require manual configuration changes.

- Verify that the restored nodes are in the powered off state.
- Verify that the cluster instances are powered off before restoring the cluster to a new site.
- Verify that no split-brain behavior occurs when the same IP addresses and FQDNs are used on the recovery site.
- Verify that no one is accidentally using a partially working cluster on the primary site.

Depending on the tool used for restoring, you can restore the virtual machines to the same host, a different host on the same data center, or a different host on a target remote data center. See Changing Configurations After Restoration

1. Restore the primary node first before restoring worker nodes.

2. Restore worker nodes in any order.

3. Optional: Restore the forwarders if configured.

   Be sure the VMware Aria Operations for Logs server (the primary node and all the worker nodes in a cluster setup) are restored before restoring the forwarders.

4. Restore any recovered agents.

- When restoring a VMware Aria Operations for Logs cluster, if the same IP addresses are used, verify that all restored node IP addresses and FQDNs are associated with their original counterparts.
  For example, the following scenario fails. In a three-node cluster with nodes A, B, and C, node A is restored with IP address B, node B is restored with IP address C, and node C is restored with the IP address A.
  – If the same IP addresses are used for only a subset of restored nodes, verify that for these nodes, all restored images are associated with their original IP addresses.
- Most backup restoration and disaster recovery tools provide a monitoring view for watching the progress of the restoration operations for failures or warnings. Take appropriate actions on any identified problems.
- If manual configuration changes are required before the site can be fully restored, follow the guidelines in the Changing Configurations After Restoration.
- When a successful restoration is finished, perform a spot check of the cluster that was restored.

Changing Configurations After Restoration

The recovery target and IP customizations applied during the backup configuration determine which manual configuration changes are required. You must apply configuration changes to one or more VMware Aria Operations for Logs nodes before the restored site can become fully functional.

Restore to the Same Host

Recovering a VMware Aria Operations for Logs cluster to the same host is straightforward and can be performed by any tool.

Review important information about Planning and Preparation.

1. Power off the existing cluster before beginning the restoration operation. By default, the same IP addresses and FQDNs are used for the restored cluster nodes.

2. Optional: Provide a new name for the cluster.

   During the restoration process, the original copy of the cluster is overwritten with the restored version unless a new name is provided to the virtual machine.

3. Optional: If possible, verify that all network, IP, and FQDN settings that are used for the production environment are preserved in the restored and recovered site.

After a successful restoration and a sanity check, delete the old copy to conserve resources and to prevent accidental split-brain situations if a user powers on the old copy.

Restore to a Different Host

When you perform a restoration to a different host, you must make configuration changes on the VMware Aria Operations for Logs cluster.

Review important information about Planning and Preparation.

Modifying the configuration files directly from the appliance console is not officially supported in VMware Aria Operations for Logs 3.0 and later releases. See Knowledge Base article 2123058 for information about how to modify these files by using the Web UI interface.

These configuration changes are specific to VMware Aria Operations for Logs builds that can be used with any backup recovery tool.

Recovering to a different host requires manual configuration changes on the VMware Aria Operations for Logs cluster. You can assume that the restored VMware Aria Operations for Logs nodes have different IP addresses and FQDNs than their source counterparts from which a backup was taken.

1. List all new IP addresses and FQDNs that were assigned to each VMware Aria Operations for Logs node.

2. Make the following configuration changes on the primary node by using the steps described in Knowledge Base article 2123058.

   a) In the VMware Aria Operations for Logs config section, look for lines that resemble the following lines.

```
<distributed overwrite-children="true">
  <daemon host="prod-es-vrli1.domain.com" port="16520" token="c4c4c6a7-f85c-4f28-a48f-43aeea27cd0e">
    <service-group name="standalone" />
  </daemon>
  <daemon host="192.168.1.73" port="16520" token="a5c65b52-aff5-43ea-8a6d-38807ebc6167">
    <service-group name="workernode" />
  </daemon>
  <daemon host="192.168.1.74" port="16520" token="a2b57cb5-a6ac-48ee-8e10-17134e1e462e">
    <service-group name="workernode" />
  </daemon>
</distributed>
```

The code shows three nodes. The first node is the primary node, which shows `<service-group name=standalone>`, and the remaining two nodes are worker nodes, which show `<service-group name="workernode">`

b) For the primary node, in the newly recovered environment, verify that the DNS entry that was used in the pre-recovery environment can be reused.

- If the DNS entry can be reused, update only the DNS entry to point to the new IP address of the primary node.
- If the DNS entry cannot be reused, replace the primary node entry with a new DNS name (pointing to the new IP address).
- If the DNS name cannot be assigned, as a last option, update the configuration entry with the new IP address.

c) Update the worker node IP addresses as well to reflect the new IP addresses.

d) In the same configuration file, verify that you have entries that represent NTP, SMTP, and database and appenders sections.

```
<ntp>
  <ntp-servers value="ntp1.domain.com, ntp2.domain.com" />
</ntp>

<smtp>
  <server value="smtp.domain.com" />
  <default-sender value="source.domain.com@domain.com" />
</smtp>

<database>
  <password value="xserttt" />
  <host value="vrli-node1.domain.com" />
  <port value="12543" />
</database>
```

- If the configured NTP server values are no longer valid in the new environment, update these values in the `<ntp>...</ntp>` section.
- If the configured SMTP server values are no longer valid in the new environment, update these values in the `<smtp>...</smtp>` section.
- Optionally, change the `default-sender` value in the SMTP section. The value can be any value but as a good practice, represent the source from where the email is being sent.
- In the `<database>..</database>` section, change the host value to point to the primary node FQDN or IP address.

e) In the same configuration file, update the VMware Aria Operations for Logs ILB configuration section.

```
<load-balancer>
<leadership-lease-renewal-secs value="5" />
<high-availability-enabled value="true" />
<high-availability-ip value="10.158.128.165" />
<high-availability-fqdn value="LB-FQDN.eng.vmware.com" />
<layer4-enabled value="true" />
<ui-balancing-enabled value="true" />
```

```
              </load-balancer>
```

f) Under the `<load-balancer>...</load-balancer>` section, update the `high-availability-ip` value if it is different from the current setting.

g) Ensure that you also update the FQDN of the load balancer.

h) Restart from the Web UI through the **Cluster** subtab on the **Administration** tab. For each node listed, select its host name or IP address to open the details panel and click **Restart Operations for Logs**.

   The configuration changes are automatically applied to all cluster nodes.

i) Wait 2 minutes after the VMware Aria Operations for Logs service starts to allow enough time for the Cassandra service to start before bringing other worker nodes online.

Verify that the restored VMware Aria Operations for Logs nodes have been assigned different IP addresses and FQDNs than their source counterparts from which a backup was taken.

Verify Restorations

You must verify that all restored VMware Aria Operations for Logs clusters are fully functional.

Confirm that the backup and restoration process is finished before verifying node and cluster configurations.

1. Log in to VMware Aria Operations for Logs using the internal load balancer (ILB) IP address or the FQDN (if configured).

2. Expand the main menu and navigate to **Management > Cluster**.

3. Verify the following:

   a) Verify that you can access all individual cluster nodes using the respective IP addresses or FQDNs.

   b) Verify the status of cluster nodes from the cluster page and ensure that the ILB, if configured, is also in an active state.

   c) Verify the vSphere integration. If necessary, reconfigure the integration. Reconfiguration is required when the ILB or the primary node IP address or FQDN is changed post-recovery.

   d) Verify the VMware Aria Operations integration and reconfigure again if needed.

   e) Verify that all content packs and UI features are functioning properly.

   f) Verify that VMware Aria Operations for Logs forwarders and agents are functioning properly, if configured.

4. Verify that other key features of VMware Aria Operations for Logs are functioning as expected.

Make any necessary adjustments to your backup and recovery plan to address any issues that may have been identified during your backup, restoration, and verification operations.

Disaster Recovery

A well-documented and well-tested recovery plan is essential to quickly returning a cluster to a working state.

The choice of replication type is critical when configuring a virtual machine for disaster recovery. Consider the Recovery Point Objective (RPO), the Recovery Time Objective (RTO), and the cost and scalability when deciding on a replication type.

In a disaster recovery scenario, sometimes you cannot restore to the same site if the primary site is fully down. But based on the option you choose, some manual steps are required to fully restore and return the VMware Aria Operations for Logs cluster to a running state.

Unless the VMware Aria Operations for Logs cluster is fully down and inaccessible, verify that the cluster instances are powered off before restoring the cluster to a new site.

During an outage or disaster, recover the VMware Aria Operations for Logs cluster as soon as possible.

Troubleshooting VMware Aria Operations for Logs

You can solve common problems related to VMware Aria Operations for Logs administration before calling VMware Support Services.

VMware Aria Operations for Logs Runs Out of Disk Space

A VMware Aria Operations for Logs primary or worker node might run out of disk space if you are using a small virtual disk, and archiving is not activated.

VMware Aria Operations for Logs runs out of disk space if the rate of incoming logs exceeds 3 percent of the storage space per minute, or when VMware Aria Operations for Logs cannot delete the oldest buckets from the storage.

In normal situations, VMware Aria Operations for Logs never runs out of disk because every minute it checks if the free space is less than 3 percent. If the free space on the VMware Aria Operations for Logs virtual appliance drops below 3 percent, old data buckets are retired.

If archiving is activated, VMware Aria Operations for Logs archives the bucket before marking it as archived and retiring in future. If the free space is filled before the old bucket is archived and retired, VMware Aria Operations for Logs runs out of disk.

Verify whether the data archival location is available and has enough free space. See Data Archiving.

> **NOTE**
> If none of the solutions are applicable, contact customer support.

Import of Archived Data Might Fail

The import of archived data might fail if the VMware Aria Operations for Logs virtual appliance runs out of disk space.

The VMware Aria Operations for Logs repository import utility does not check for available disk space on the VMware Aria Operations for Logs virtual appliance. Therefore, the import of archived logs might fail if the virtual appliance runs out of disk space.

Increase the storage capacity of the VMware Aria Operations for Logs virtual appliance and start the import again. Note, though, that information that was successfully imported before failure will be duplicated.

Use the Virtual Appliance Console to Create a Support Bundle of VMware Aria Operations for Logs

If you cannot access the VMware Aria Operations for Logs Web user interface, you can download the support bundle by using the virtual appliance console or after establishing an SSH connection to the VMware Aria Operations for Logs virtual appliance.

- Verify that you have the root user credentials to log in to the VMware Aria Operations for Logs virtual appliance.
- If you plan to connect to the VMware Aria Operations for Logs virtual appliance by using SSH, verify that TCP port 22 is open.

1. Establish an SSH connection to the VMware Aria Operations for Logs vApp and log in as the root user.

2. To generate the support bundle, run `loginsight-support`.

   To generate a support bundle and include only files that have changed within a certain time period, execute the `loginsight-support` command with the `--days` constraint. For example, `--days=1` will only include files that have changed within 1 day.

The support information is collected and saved in a `*.tar.gz` file that has the following naming convention: `loginsight-support-YYYY-MM-DD_HHMMSS.xxxxx.tar.gz`, where `xxxxx` is the process ID under which the `loginsight-support` process ran.
Forward the support bundle to VMware Support Services as requested.

Reset the Admin User Password

If an admin user forgets the password to the Web user interface, the account becomes unreachable.

If VMware Aria Operations for Logs has only one admin user and the admin user forgets the password, the application cannot be administered. If an admin user is the only user of VMware Aria Operations for Logs, the whole Web user interface becomes inaccessible.

If a user does not remember their current password, VMware Aria Operations for Logs does not provide a user interface for admin users to reset their own passwords.

> **NOTE**
> Admin users who can log in can reset the password of other admin users. Reset the admin user password only when all admin user accounts' passwords are unknown.

1. Establish an SSH connection to the virtual appliance and log in as the root user.

2. Run the script that resets the admin user password:

    ```
    li-reset-admin-passwd.sh
    ```

   The script resets the admin user password, generates a new password, and displays it on the screen.

Reset the Root User Password

If you have forgotten the root user password, or have locked the root user account, you can no longer establish SSH connections to the VMware Aria Operations for Logs virtual appliance.

To reset the root user password and unlock the account, see KB-53649.

Alerts Could Not Be Delivered to VMware Aria Operations

VMware Aria Operations for Logs notifies you if an alert event cannot be sent to VMware Aria Operations. VMware Aria Operations for Logs retries sending the alert every minute until the problem is resolved.

A red sign with an exclamation mark appears in the VMware Aria Operations for Logs toolbar when an alert could not be delivered to VMware Aria Operations.

Connectivity problems prevent VMware Aria OperationsVMware Aria Operations for Logs from sending alert notifications to VMware Aria Operations.

- Click on the red icon to open the list of error messages, and scroll down to view the latest message.

    The red sign disappears from the toolbar when you open the list of error messages, or if the problem is resolved.

- To fix the connectivity problem with VMware Aria Operations, try the following.

    - Verify that the VMware Aria Operations vApp is not shut down.
    - Verify that you can connect to VMware Aria Operations through the **Test Connection** button in the **Integration > VMware Aria Operations** page of the VMware Aria Operations for Logs Web user interface.
    - Verify that you have the correct credentials by logging directly into VMware Aria Operations.
    - Check the logs for messages related to connectivity issues in VMware Aria Operations for Logs and VMware Aria Operations.
    - Verify that no alerts are filtered out in VMware Aria Operations vSphere user interface.

Unable to Log In Using Active Directory Credentials

You cannot log in to the VMware Aria Operations for Logs Web user interface when you use Active Directory credentials.

You cannot log in to VMware Aria Operations for Logs by using your Active Directory domain user credentials, despite that an administrator has added your Active Directory account to VMware Aria Operations for Logs.

The most common causes are expired passwords, incorrect credentials, connectivity problems, or lack of synch between the VMware Aria Operations for Logs virtual appliance and Active Directory clocks.

- Verify that your credentials are valid, your password has not expired, and your Active Directory account is not locked.
- If you have not specified a domain to use with Active Directory authentication, verify that you have an account on the default domain stored in the latest VMware Aria Operations for Logs configuration at `/storage/core/loginsight/config/loginsight-config.xml#[number]` where [number] is the largest.
- Find the latest configuration file: `/storage/core/loginsight/config/loginsight-config.xml#[number]` where `[number]` is the largest.
- Verify VMware Aria Operations for Logs has connectivity to the Active Directory server.
  – Navigate to **Configuration > Authentication**, fill in your user credentials, and click the **Test Connection** button.
  – Check the VMware Aria Operations for Logs `/var/log/vmware/loginsight/runtime.log` for messages related to DNS problems.
- Verify that the VMware Aria Operations for Logs and Active Directory clocks are in synch.
  – Check the VMware Aria Operations for Logs `/var/log/vmware/loginsight/runtime.log` for messages related to clock skew.
  – Use an NTP server to synchronize the VMware Aria Operations for Logs and Active Directory clocks.

SMTP does not work with STARTTLS option activated

When you configure the SMTP server with the STARTTLS option activated, test emails fail. Add your SSL certificate for the SMTP server to the Java truststore to resolve the problem.

- Verify that you have the root user credentials to log in to the VMware Aria Operations for Logs virtual appliance.
- If you plan to connect to the VMware Aria Operations for Logs virtual appliance by using SSH, verify that TCP port 22 is open.

1. Establish an SSH connection to the VMware Aria Operations for Logs vApp and log in as the root user.

2. Copy the SSL certificate for the SMTP server to the VMware Aria Operations for Logs vApp.

3. Run the following command.

```
`/usr/java/jre-vmware/bin/keytool -import -alias certificate_name -file path_to_certificate -keystore /
usr/java/jre-vmware/lib/security/cacerts -storepass store_pass`
```

> **NOTE**
> The outer quotes are inserted by using the back quote symbol that is on the same key as tilde on your keyboard. Do not use single quotes.

4. Replace the password `store_pass` with the default password `changeit`.

5. Run the `service loginsight restart` command.

Navigate to **Configuration** > **SMTP** and use **Send Test Email** to test your settings. See Configure the SMTP Server for VMware Aria Operations for Logs

Upgrade Fails Because the Signature of the .pak file Cannot Be Validated

VMware Aria Operations for Logs upgrade fails because of a corrupted `.pak` file, expired license or insufficient disk space.

Upgrading VMware Aria Operations for Logs fails and you see an error message `Upgrade Failed. Failed to upgrade: Signature of the PAK file cannot be validated.`

The error might occur for the following reasons:

- The uploaded file is not a `.pak` file.
- The uploaded `.pak` file is not complete.
- The license of VMware Aria Operations for Logs has expired.

- The VMware Aria Operations for Logs virtual appliance root file system does not have enough disk space.

- Verify that you are uploading a `.pak` file.
- Verify the md5sum of the `.pak` file against the VMware download site.
- Verify that at least one valid license is configured on VMware Aria Operations for Logs.
- Log in to the VMware Aria Operations for Logs virtual appliance and run `df -h` to check the available disk space.

> **NOTE**
> Do not put files on the VMware Aria Operations for Logs virtual appliance root file system.

Upgrade Fails with an Internal Server Error

VMware Aria Operations for Logs upgrade fails with an Internal Server Error because of a connection problem.

Upgrading VMware Aria Operations for Logs fails and you see an error message `Upgrade Failed. Internal Server Error.`

A connection problem occurred between the client and the server. For example, when you attempt to upgrade from a client that is on a WAN.

Upgrade LI from a client on the same LAN as the server.

Missing vmw_object_id Field in the First Log Message After Integration with VMware Products

After integrating VMware Aria Operations for Logs with VMware products, the first log message does not contain the `vmw_object_id` field.

The first log message that you receive after you integrate VMware Aria Operations for Logs with vCenter Server and VMware Aria Operations does not contain the associated `vmw_object_id` field. The missing field can have an impact on the alert delivery mechanism when a VMware Aria Operations object is specified as an alert target.

> **NOTE**
> Ensure that the vCenter Server is also integrated with VMware Aria Operations.

Wait for two minutes. The next log message that you receive will contain the `vmw_object_id` field.

Documentation Legal Notice