

# vRealize Log Insight 8.4 Release Notes

## What's in the Release Notes

The notes cover the following topics:

- [About vRealize Log Insight](#)
- [What's New](#)
- [Compatibility](#)
- [Limitations](#)
- [Upgrading from a Previous Release](#)
- [Internationalization Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

## About vRealize Log Insight

vRealize Log Insight delivers the best real-time and archived log management, especially for VMware environment. Machine learning-based intelligent grouping and high performance search enables faster troubleshooting across physical, virtual, and cloud environments. vRealize Log Insight 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 vRealize Log Insight product documentation at <https://docs.vmware.com/en/vRealize-Log-Insight/index.html>.

## What's New

Here are some of the key highlights of vRealize Log Insight 8.4 that will help you leverage log data more quickly, accurately, and powerfully than ever before:

- **Log Sources:** You can now configure Fluentd to collect logs from various sources such as Docker, Kubernetes, Tanzu Kubernetes Grid, and OpenShift, and forward them to vRealize Log Insight. Fluentd is an open source log processor and forwarder, which lets you collect log data from different sources and enrich them with filters. It is the preferred choice for containerized environments such as Kubernetes. You can find the configuration for the Fluentd log sources within the vRealize Log Insight user interface.
- **Log Masking:** Your log data contains information that might be considered sensitive. Specific log messages may include user names, email addresses, URL parameters, and other information that you do not want to disclose. Log masking lets you mask any information by modifying the configuration that handles information you consider to be sensitive.
- **Log Dropping:** Sometimes, your infrastructure may generate a volume of log events that is too large or has significant fluctuations. In this situation, you may need to choose which logs to send to a log management solution, and which logs to drop. Log dropping lets you drop certain logs by modifying the appropriate configuration.
- **Custom Webhooks:** The vRealize Log Insight webhook connection is now available to send notification alerts to Slack and PagerDuty. You can also send notifications to custom webhooks by defining an appropriate payload.
- **Archiving based on Partitions:** Data archiving preserves old logs that might otherwise be removed from vRealize Log Insight virtual appliance due to storage constraints. vRealize Log Insight can store archives for data partitions in NFS mounts.
- **Alert Management:** With the upgraded alert management, you can see the entire list of alerts within the context of your organization in one environment. Alerts are now organization-centric as opposed to being user-centric, which provides more flexibility to control organization alerts. The permissions for managing queries

based alerts have been updated. Users now require Interactive Analytics permission to view alerts, and E Shared Content permission to create and manage alerts.

- **Simplified Sizing with a New Sizing Calculator:** Correctly sizing the vRealize Log Insight cluster is essential to achieve optimal performance when searching for and analyzing logs, and to ensure that a cluster has the required resources. The sizing calculator determines the required node size based on the types of servers, devices logging, the expected ingestion rate, and log retention requirements.
- **NSX Data Center editions:** vRealize Log Insight is now included with the following new NSX Data Center editions. For more information, see the [VMware NSX Data Center datasheet](#).
  - NSX Firewall
  - NSX Firewall with Advanced Threat Prevention
- **Content pack updates:** The following content packs have been updated.
  - VMware NSX-v 4.2.1 (Updates related to fields extraction)
  - VMware NSX-t v4.0.1 (Addition of new dashboard support "Unified Security Flow Logs" )
  - VMware vRA 8.3+ (Support vRA 8.3+ product line)
  - Microsoft IIS v3.4 (Improvement in "Setup Instruction" section to describe how to extract custom from logs.)
  - VMware Horizon v4.0.1
  - vSphere 8.4
  - vRops v4.2
  - vSAN (Support vSAN 70u2)
  - Additional content packs validated:
    - NPE Servers v1.1.1
    - Mongo DB v2.4
    - Solarwinds v1.1
    - Oracle DB v1.1
    - NPE Nimble v1.1

## Compatibility

vRealize Log Insight 8.4 supports the following VMware products and versions:

- vRealize Log Insight can pull events, tasks, and alarms data from VMware vCenter Server 6.0 or later. In mode, vRealize Log Insight can be integrated with VMware vCenter Server 6.0 U1 or later.
- You can integrate vRealize Log Insight 8.4 with vRealize Operations Manager version 8.0.1 or later.

## Browser Support

vRealize Log Insight 8.4 supports the following browser versions. More recent browser versions also work with vRealize Log Insight, but have not been validated.

- Mozilla Firefox 72.0 and above
- Google Chrome 78.0 and above
- Safari 11.1 and above
- Internet Explorer 11.0 and above

**Note:** Internet Explorer Document mode must be used in **Standards Mode**. Other modes are not supported. Compatibility View browser mode is not supported.

The minimum supported browser resolution is 1280 by 800 pixels.

**Important:** Cookies must be enabled in your browser.

## vRealize Log Insight Windows Agent Support

The vRealize Log Insight 8.4 Windows agent supports the following versions:

- Windows 7, Windows 8, Windows 8.1, and Windows 10

- Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019

## vRealize Log Insight Linux Agent Support

The vRealize Log Insight Linux agent supports the following distributions and versions:

- RHEL 5, RHEL 6, RHEL 7, and RHEL 8
- SUSE Enterprise Linux (SLES 11 SP3) and SLES 12 SP1
- Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04
- VMware Photon, version 1 revision 2, version 2, and version 3

## Limitations

vRealize Log Insight 8.4 has the following limitations:

### General

- vRealize Log Insight does not handle non-printable ASCII characters correctly.
- vRealize Log Insight does not support printing. However, you can use the Print options of your browser. Printed results might vary depending on the browser that you use. We recommend Internet Explorer or Firefox for printing portions of the vRealize Log Insight 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 both as 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, vRealize Log Insight uses the source as the hostname. This might result in the device being listed more than once because vRealize Log Insight cannot determine if the two formats point to the same device.
- Adding a new data 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, or retention period for existing data partitions apply immediately (restarting the cluster is not required).
- Once activated, FIPS mode cannot be disabled.

## vRealize Log Insight Windows and Linux Agents

- Non-ASCII characters in hostname and source fields are not delivered correctly when vRealize Log Insight Windows and Linux agents are running in syslog mode.

### vRealize Log Insight Windows Agent

- The vRealize Log Insight 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 vRealize Log Insight 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 Service, add the following line to the corresponding section of the vRealize Log Insight Windows agent configuration file: `=C:\Windows\Sysnative\dhcp.`

### vRealize Log Insight Linux Agent

- Due to an operating system limitation, the vRealize Log Insight Linux agent does not detect network outages when configured to send events over syslog.
- The vRealize Log Insight Linux agent does not support non-English (UTF-8) symbols in field or tag names.

- The vRealize Log Insight Linux agent collects hidden files and directories by default. To prevent this, you 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 vRealize Log Insight agent might not correctly recognize event boundaries in such log files.

## vRealize Log Insight Integrations

Launch in context, both from vRealize Log Insight and vRealize Operations, does not work for a virtual machine if the IP address of the virtual machine is not visible to the vRealize Operations instance and is not shown by the **VM Summary** tab 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 in vCenter displays the IP address of the virtual machine.

## Upgrading from a Previous Version of vRealize Log Insight

Keep in mind the following considerations when upgrading to this version of vRealize Log Insight.

### Upgrade Path

You can upgrade to vRealize Log Insight 8.4 from 8.3 or 8.2.

### Important Upgrade Notes

- To upgrade to vRealize Log Insight 8.4, you must be running vRealize Log Insight 8.3 or 8.2.
- 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 vRealize Log Insight 8.4 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.
- vRealize Log Insight does not support two-node clusters. Add a third vRealize Log Insight 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 vRealize Log Insight 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 to resolve 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.

## Internationalization Support

vRealize Log Insight 8.4 includes the following localization features.

- The vRealize Log Insight server web user interface is localized to Japanese, French, Spanish, German, Simplified Chinese, Traditional Chinese, and Korean.
- The vRealize Log Insight server web user interface supports Unicode data, including machine learning feedback.
- vRealize Log Insight agents work on non-English native Windows.

### Limitations

- The agent installer and content pack are not localized. Parts of the vRealize Log Insight server Web user interface might still show non-localized strings and have layout issues.
- vRealize Log Insight is interoperable with localized versions of vCenter Server and vRealize Operations Manager. However, Content Packs depend on matching non-localized log messages. vCenter Server events are retrieved in its default locale, which should be set to en\_US. For more information, see <http://kb.vmware.com/kb/2121646>.
- Integration with Active Directory, vSphere, and vRealize Operations Manager for user names with non-ASCII characters is not supported.
- Localization of event logs is not supported. Event logs support UTF-8 and UTF-16 character encoding only.

## Resolved Issues

There are no resolved issues in this release.

## Known Issues

The following known issues are present in this release.

- **Virtual Center (VC) events collection is delayed**  
After a restart of the vRealize Log Insight service or a cluster upgrade, Virtual Center (VC) events collection might be delayed if a large number of VC's are integrated.  
  
**Workaround:** Events are automatically restored as collected after a sufficient amount of time. The length of time depends on your environment. For example, for 80 VCs on a cluster with four nodes, the delay would be approximately one hour.
- **vRealize Log Insight cannot authenticate users and groups from a second trusted Active Directory if a two-way trust is configured**  
When an Active Directory is configured with a two-way trust with another Active Directory, vRealize Log Insight cannot authenticate users and groups of the second trusted Active Directory.  
  
**Workaround:** Use vIDM, which is directly integrated with both Active Directories.
- **Collection from some of directories will not take place if they were created before agent start or re-configuration event.**  
If a new directory is being created after re-configuration of the Agent collection of newly created directories, collection will not happen.  
  
**Workaround:** To start directory monitoring, restart the service or update agent configuration with the local configuration file or from the Server Admin Agents page.
- **No automatic upgrade for vRealize Log Insight Agent on Photon OS**  
You cannot perform an automatic upgrade for vRealize Log Insight 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 e-mail services such as Google and Yahoo, because these services might leverage tighter restriction policies for IPv6.  
  
**Workaround:** Use an alternative mail server such as your corporate mail server, or bring up a dedicated mail server.
- **Integrating VMware Identity Manager with vRealize Log Insight through IPv4 changes the redirect URL host to IPv6 address**  
If you select the option to prefer IPv6 addresses when you deploy a vRealize Log Insight virtual appliance, the redirect URL host list is populated by IPv6 node addresses while integrating with VMware Identity Manager.

which does not support IPv6.

**Workaround:** Create a spare IPv4 VIP for the integration of vRealize Log Insight with VMware Identity Manager.

- **Layout issues in Internet Explorer 11.0**

In Internet Explorer 11.0, there are layout issues for the user icon in the header and chart legend list display the **Dashboards** and **Interactive Analytics** tabs.

**Workaround:** See <https://kb.vmware.com/s/article/78592> for the workaround.

- **The REST API call 'POST /api/v1/sessions' fails**

When you join a newly deployed node in vRealize Log Insight 8.2 or 8.3 with an old cluster upgraded from an earlier version, the REST API call 'POST /api/v1/sessions' to the new worker node fails and throws the following error:

```
Error: write EPROTO 1319245176:error:100000f7:SSL routines:OPENSSL_internal:WRONG_VERSION_NUMBER:../third_party/boringssl/src/ssl/tls_record
```

You can find the relevant log in the REST client. Because of this error, you cannot get a session for the new node.

**Workaround:** Restart the vRealize Log Insight service by running the 'service loginsight restart' command on the affected node.

- **Testing a custom SMTP server configured with STARTTLS in FIPS mode throws a certificate error**

While configuring a custom SMTP server with the STARTTLS option in FIPS mode, clicking **Send Test Email** displays a pop-up window to accept the self-signed certificate. When you accept the certificate, the following error is displayed:

```
Unable to find valid certification path to requested target
```

**Workaround:** Restart the vRealize Log Insight service by running the 'service loginsight restart' command on the affected node.

- **vRealize Log Insight sends email notifications using a custom SMTP server without a trusted certificate**

With a custom SMTP server, vRealize Log Insight sends alerts and system notifications through email even when the custom certificate is not accepted.

**Workaround:** None.

- **Upgrade fails for fresh vRealize Log Insight 8.3 setups deployed in FIPS mode**

The upgrade for fresh vRealize Log Insight 8.3 setups fails when deployed with the FIPS mode enabled.

**Workaround:** Enable FIPS mode after the deployment. See <https://kb.vmware.com/s/article/83360>.

- **vRealize Log Insight displays an "Upgrade unconfirmed" message even when the upgrade is successful**

While upgrading to vRealize Log Insight 8.4, a message stating that the upgrade status is unconfirmed may appear. This message does not have an impact on the overall upgrade status, and the upgrade is eventually successful.

**Workaround:** None.

- **The upgrade for dual stack or IPv6 setups fails**

Upgrading dual stack or IPv6 setups to vRealize Log Insight 8.4 fails.

**Workaround:** None.