

vRealize Log Insight 8.3 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 environments. 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 structured and 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 8.3 that will help you leverage log data more quickly, accurately, and powerfully than ever before:

- **Support for Federal Information Processing Standard (FIPS) 140-2:** FIPS 140-2 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. To learn more about support for FIPS 140-2 in VMware products, see <https://www.vmware.com/security/certifications/fips.html>. vRealize Log Insight can now activate FIPS mode for vRealize Log Insight during deployment or after upgrade, from the Admin console.

Note: Once activated, FIPS mode cannot be disabled.

- **You can configure the legal consent (DoD) displayed to users during login.**
- **Support for key-based SSH authentication,** which is an alternative mechanism, and a more secure and automatable option as compared to the username and password authentication.
- **Install automation with Log Insight Agent download without authentication:** This feature provides an improved automation experience with a direct download of Log Insight Agent to a target system from the Admin console.
- **Support of cross-domain group-based authentication for vIDM users:** In a multi-domain environment with a trust established among domains, user login is simplified for vIDM users that are part of a different domain.
- **Time format standardization for log forwarding:** You can customize an event date format to a standard format. This feature provides flexibility during syslog type forwarding, especially in scenarios such as a timestamp in an ingested log.
- **Inter-node data communication over SSL:** The communication across the nodes in a cluster (port 5977-16520:16580) through Apache Thrift is enhanced to optionally secure the connection with SSL. For more information, see <https://kb.vmware.com/s/article/82299>.

Compatibility

vRealize Log Insight 8.3 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 8.3 with vRealize Operations Manager version 8.0.1 or later.

Browser Support

vRealize Log Insight 8.3 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 8.3 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 8.3 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 syslog protocol does not have a hostname, vRealize Log Insight uses the source as the hostname. This may 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) for the new configuration to become effective. However, changes in the routing filter, enabled status, 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 output 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 can 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 IP address 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 8.3 from 8.2.

Important Upgrade Notes

- To upgrade to vRealize Log Insight 8.3, you must be running vRealize Log Insight 8.2.
- When performing a manual upgrade, you must upgrade workers one at a time. Upgrading more than one workers at the same time causes an upgrade failure. When you upgrade the primary node to vRealize Log Insight 8.3, 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.
- The sshd customized service configuration (/etc/ssh/sshd_config) resets to its default when you upgrade vRealize Log Insight appliance. As a workaround, save the /etc/ssh/sshd_config configuration before upgrading and then reconfigure manually after upgrade.
- Photon OS has strict rules for the number of simultaneous ssh connection. 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

Internationalization Support

vRealize Log Insight 8.3 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 file names.
- 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 20 minutes.

hour.

- **vRealize Log Insight cannot authenticate users and groups from a second trusted Active Directory 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, the collection will not happen.

Workaround: To start directory monitoring, restart the service or update agent configuration with the license 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 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 in 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 8.0 or earlier, 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.c:101
```

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 email is sent successfully.

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.

- **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.

- **Syslog forwarding over UDP stumbles over extremely long messages**
Syslog forwarding over UDP stumbles over extremely long log messages. These log messages are the ones that exceed the maximum UDP datagram size in length.

Workaround: Change the protocol from UDP to TCP.

- **The vSphere Kubernetes event collection configuration is reset when any vSphere integration is saved**
After manually disabling a vSphere Kubernetes event collection, the corresponding configuration value is reset to default (true) when any vSphere integration is saved.

Workaround: Change the flag value to false from the internal config after every change in the vSphere configuration.