

vRealize Log Insight

4.8 Release Notes

Updated Apr 11 2019

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 archive 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 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

vRealize Log Insight Server Features

- Data retention configuration options based on time:
 - Option to configure the data retention period based on your needs from a few days to 12 months
- Better insight into possible user privilege issues on vROps integration page includes:
 - Checking vROps user privileges when testing the vROps connection
 - Displaying descriptive information to the user if the test alert is not received in the vROps side
 - Details on vROps integration UI related to required user privileges via help tips
- Agent configuration UI fields for new agent side features:
 - JSON parser configurations
 - Conditional decoder configurations
- Extracting Selected Content Pack fields for a query
- Users with 'View Only Admin' role now have the possibility to see the list of integrated ESXi hosts
- The minimum key size for the virtual appliance certificate must be 2048 bits or greater
- The OSI usage is now calculated based on usage over a 3 month period

vRealize Log Insight Agent Features



- JSON parser added, the parser will extract all fields from JSON logs in case of a default configuration
- Log Parser can be configured for conditional parsing. Users can specify if a parser should be applied based on the value of a parsed field

Compatibility

vRealize Log Insight 4.8 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.
- You can integrate vRealize Log Insight 4.8 with vRealize Operations Manager version 6.6 or later.

Browser Support

vRealize Log Insight 4.8 supports the following browser versions. More recent browser versions also work with vRealize Log Insight, but have not been validated.

- 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 used in **Standards Mode**. Other modes are not supported. The 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 4.8 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, and Windows Server 2016

vRealize Log Insight Linux Agent Support

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

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

Limitations

vRealize Log Insight 4.8 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. The 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 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, 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.

vRealize Log Insight Windows and Linux Agents

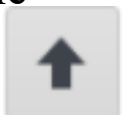
- Non-ASCII characters in hostname and source fields are not delivered correctly when vRealize Log Insight Windows and Linux agents are running in syslog mode.

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 Server, 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 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 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 when the IP address of the virtual machine is not visible to the vRealize 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.

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 4.8 directly from vRealize Log Insight 4.7 or 4.7.1. If you are running an earlier version of vRealize Log Insight, you must first incrementally upgrade your installation to 4.7 or 4.7.1.

Important Upgrade Notes

- To upgrade to vRealize Log Insight 4.8, you must be running vRealize Log Insight 4.7 or 4.7.1.
- When performing a manual upgrade, you must upgrade workers one at a time. Upgrading more than one workers at the same



causes an upgrade failure. When you upgrade the master node to vRealize Log Insight 4.8, a rolling upgrade occurs unless specifically disabled.

- Upgrading must be done from the master 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.
- If the vRealize Log Insight upgrade (.pak file) has a new JRE version, then the user-installed certificates in a vRealize Log Insight setup (such as for event forwarding) become invisible after upgrade.

Internationalization Support

vRealize Log Insight 4.8 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 features.
- 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

The following defects have been fixed as part of this release.

- **The Log Insight launch in context for vROps is not working correctly.**
Log Insight launch in context for vROps does not work correctly for the following reasons:
 - The cleanup of vROps inventory mapping in Log Insight did not remove mapping for previous vROps integrations.
 - The cleanup was triggered unnecessarily after the leader node was changed, which caused the missing launch in context information.
- **Queries now support time-related terms that when entered are automatically translated to the current time.**
When the following terms are entered in a query they are automatically translated to the correct specified time:
 - now
 - today (can also be specified using 't')
 - yesterday
 - tomorrow
 - t - *d, where *d represents the number of days
 - t + *d, where *d represents the number of days
- **On the Interactive analysis page, the date is displayed incorrectly when you click the 'From' date field of the time range filter.**
When the 'From' date is selected from the time range filter, the date is displayed incorrectly.



- **The vSphere content pack can not be installed from the Marketplace.**
The vSphere content pack is too large to be downloaded and installed from the Marketplace.
- **The 'Global' section of the agent configurations is not available under the 'Agent Group' tab for content packs.**
Some content packs require the 'Global' section of the agent group configurations which is not available under the 'Agent Group' tab.

Known Issues

The following known issues are present in this release.

- **Virtual Center (VC) events collection is delayed**
After a restart of the Log Insight service or a Log Insight 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 4-node cluster, the delay would be an hour.

- **Deletion of the vRealize Operations integration fails**
If Log Insight was previously integrated with a VRealize Operations instance but that integration has become unreachable, it isn't possible to force a removal of the integration.

Workaround: Refresh and try removing the integration again.

- **Log Insight cannot authenticate users and groups from a second trusted Active Directory when two-way trust is configured**

When an Active Directory is configured with 2-way trust with another Active Directory, vRealize Log Insight



cannot authenticate users and groups of 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 will not happen

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

