

Intro to vRealize Log Insight Content Packs

May 30, 2019

vmware®

© 2019 VMware Inc. All rights reserved.



Content

- **What are the components of Content Packs?**
- **High level Best practices overview**
- **Extracted fields**
- **Alerts**
- **Dashboards**
- **Instructions for installation**
- **Publishing to VSX marketplace**
- **Typical issues with content packs**
- **Useful links**

Content pack – general overview

Content packs are read-only plug-ins to vRealize™ Log Insight™ that provide pre-defined knowledge about specific types of events such as log messages. A content pack should answer questions like, “Is the product/application healthy?” In addition, a content pack should create a greater understanding of how a product/application/device works, how to troubleshoot the main problems in it, how pro-actively monitor the possible issues.

A content pack contains:

- Queries
- Extracted fields
- Dashboards
- Alerts
- Agent Groups (only for Content Packs whose logs can be collected via Log Insight Agent)

Also solution should provide sufficient information about

- Setup Instructions
- Upgrade (if applicable)

Content pack – Best practices


Export Content Pack

Select items to export:

<input checked="" type="checkbox"/>	Dashboards
<input checked="" type="checkbox"/>	General - Overview
<input checked="" type="checkbox"/>	General - Problems
<input checked="" type="checkbox"/>	vRA - Appliance
<input checked="" type="checkbox"/>	vRA - App Authoring
<input checked="" type="checkbox"/>	vRA - Catalog Requests
<input checked="" type="checkbox"/>	vRA - Composition Service
<input checked="" type="checkbox"/>	vRA - Event Broker
<input checked="" type="checkbox"/>	vRA - Authentication
<input checked="" type="checkbox"/>	vRA - IaaS
<input checked="" type="checkbox"/>	vRA - NSX
<input checked="" type="checkbox"/>	vRA - Telemetry
<input checked="" type="checkbox"/>	Alerts
<input checked="" type="checkbox"/>	*** CRITICAL *** vRA IaaS Services St... A vRA IaaS service has become unav...
<input checked="" type="checkbox"/>	*** CRITICAL *** vRA license has expi... Notification when one of the vRA co...
<input checked="" type="checkbox"/>	*** CRITICAL *** vRA disk is full Windows host(s) have disk that is at c...

Select All | Select None Shift-click to select multiple items

Enter information:

Name  BROWSE...

Version

Author

Website

Namespace

Description [Edit](#)

Setup Instructions [Edit](#)

Upgrade Instructions [Edit](#)

Best practices suggest for any content pack to have:

- Three or more dashboards (dashboard groups)
- Three or more queries (chart/table widgets) per dashboard (nine or more in total)
- Five or more alerts
- Twenty or more extracted fields OR similar fields delivered via Log Insight Agent parsers (LI Agent is more efficient from performance perspective if syslog format forwarding is not mandated by product/device configuration)

When bundling Content Pack the fields showed in Export Content Pack screenshot are advised to be provided

Content Pack versioning is not associated with product/device version. Instead, it can be pointed on the Name field

Advised content pack versioning format is MAJOR.MINOR, while some of solution can also have REVISION field

- MAJOR - major changes to the content pack, for example one or more new dashboards. Dashboards/Alerts or previous configuration retirement is a sign of major version increase to be mandated
- MINOR – minor bud fixes, changed a widget type, added couple of widgets
- REVISION – typically used by content pack authors when preparing a version before publishing. It is suggested to send new revision number when implemented feedback from VSX review process.

Field Extraction

Any part of a log message that might be applicable to a query or aggregation can be dynamically extracted from the log by providing a regular expression. Extracted Fields are a type of regular expression query and are especially useful for complex pattern matching, so a user does not need to know, remember, or learn complicated regular expressions. However, if the regex definition of the field is not optimized for performance it can considerably slow down query performance.

Name Convincing

Extracted field name should match to the following pattern: <product or content pack prefix>_<descriptor_what_is_extracting>.

Example: *ms_win_security_audit_failed_account_name*

The screenshot displays the VMware Log Insight interface. At the top, there are navigation tabs for 'vm Log Insight', 'Dashboards', and 'Interactive Analytics'. Below this, a time range is set to '2019-05-30 18:13:27 to 18:18:29 (5 minutes 2 seconds)'. A bar chart titled 'Count of events over time' shows event counts across various time intervals. Below the chart, there are controls for the chart type ('Count of events'), a plus sign, a dropdown for 'over time', and buttons for 'Apply' and 'Reset'. A dialog box titled 'Add Filter:' is open, showing options: 'Contains 'context='''', 'Does not contain 'context='''', and 'Extract field'. Below the dialog, there are tabs for '+ ADD FILTER', 'Events', 'Field Table', 'Event Types', and 'Event Trends'. At the bottom, a log entry is visible: '2019-05-30 18:18:27.000 [UTC:2019-05-30 14:18:27 Local:2019-05-30 14:18:27] [Info]: [sub-thread-Id="56" context="" token=""] Processing ping report, report queue depth is 0'. The log entry includes a table of fields: source, component, context, event_type, filepath, hostname, product, token, vmw_vra Jaas_loglevel, and priority.

Alerts

New Alert

Name

Description: Optional. This description is included in the notification message when the alert is fired.

[Edit](#)

Recommendation: Optional. This recommendation is included in the notification message when the alert is fired.

[Edit](#)

Notify:

Email Email address(es) separated by commas

Webhook URLs separated by spaces

Send to vRealize Operations Manager [Configure vRealize Operations Manager integration »](#)

[SEND TEST ALERT](#)

Raise an alert:

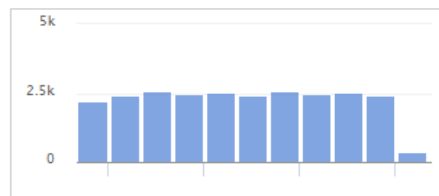
On any match

When an event is seen for the first time in the last Hours

When matches are found in the last Minutes

Modify the chart to enable group-by and/or aggregation-based alerts.

The query will run every 5 minutes and will only alert once for the defined threshold above.



Count of events over time

[CANCEL](#)

[SAVE](#)

Alerts provide a way to trigger a reaction when a certain type of event is seen. Alerts are based on queries performed in **Interactive Analytics** page. By default, vRealize Log Insight supports three different types of alerts trigger mechanism:

- Email
- notification to vRealize Operations Manager
- Webhook

Alerts can only be saved in user space and as such, all content pack alerts are disabled by default. If an enabled alert is created and then exported as part of a content pack, the alert is disabled in the content pack. This means that email, webhook and/or vRealize Operations Manager settings are not contained and cannot be added to a content pack.

Thresholds: if enabled, a content pack alert does not unintentionally spam a user. When considering a threshold, there are two things to keep in mind:

- How frequently to trigger the alert: vRealize Log Insight comes with pre-defined trigger frequencies. Important: Alerts only trigger once for a specific threshold window.
- How often to check if an alert state has occurred: An alert is triggered by a query. Alerts, such as queries, are not real-time in the current version. For each threshold window, a pre-determined query frequency has been allocated. Changing the threshold changes the query time.
- Alert can also be raised every time a new event type is seen but this can be noisy. For alerts defined in a content pack, the “On any match” threshold should not be used.

Thresholds should intuitively reflect criticality of the Alert condition, but it is again advised to mark the Criticality of the Alert on the Alert **Name**.

Description and **Recommendation** fields are highly recommended to reflect what action items should be done by a person who received the Alert notification.

vmware®

Dashboards/widgets

There are two different types of dashboard widgets in VRealize Log Insight:

- Chart: contains a visual representation of events with a link to a saved query.
- Query: contains title links to saved queries.

A chart can either be represented as a bar or line chart (or bubble, pie & area chart) and can be displayed in a stacked fashion.

The screenshot displays a dashboard with a left-hand navigation menu and a main content area. The navigation menu includes sections for 'Custom Dashboards', 'My Dashboards', 'Shared Dashboards', and 'Content Pack Dashboards', with sub-items for 'General', 'VMware - VSAN', and 'VMware - vRA 7.3+'. The main content area features a filter section at the top with a date range of 'Latest 48 hours of data' and a legend toggle. Below the filters are four widgets: 1) 'vRA tenant events by tenant name' (pie chart), 2) 'vRA non-info events by message type' (pie chart), 3) 'Count of errors by Cafe component' (pie chart), and 4) 'Counts of vRA error events by sub component' (table). The table data is as follows:

component	Count
server	195
cafe:component-registry	49
cafe:software-service	31

Below this table is another widget: 'vRA warning events by sub component' (table):

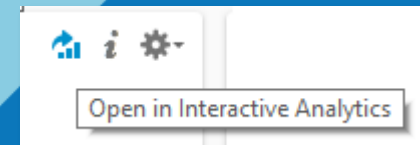
component	Count
cafe:identity	5661
vidm	802
cafe:composition-service	504

The bottom right widget is 'Relevant Queries', which lists several saved queries such as 'vRA error events by error code' and 'vRA non-info tenant events by tenant name'.

Creation of Dashboards/widgets performed from Interactive Analytics page



Modification of widgets performed from widget's



Instructions for installation

VMware - vRA 7.3+ Setup Instructions



vRealize Automation (vRA) is made up of multiple components and as such multiple configurations and multiple content packs are required in order to harness the power of all the logs generated. In addition to installing and configuring the vRA content pack, the following content packs should also be installed and configured:

- vRealize Orchestrator
- NSX (optional)

The vRA content pack requires the use of the Log Insight agent on both the vRA virtual appliance (Linux) as well as all IaaS devices (Windows). The Log Insight agent comes preinstalled on the vRA virtual appliance version 7.0.1 and newer, but must be manually installed on all other devices. The agent must be configured to send events to Log Insight, use the cfapi protocol (default), and leverage the included agent group configuration.

To apply the agent group configuration:

- Go to the Administration > Agents page (requires Super Admin privileges)
- Select the All Agents drop-down at the top of the window and select the Copy Template button to the right of the appropriate vRealize Automation agent groups
- Add the desired filters to restrict which agent receive the configuration (i.e. Linux vs Windows hosts)
- For IaaS Windows hosts, adjust the configurations per your install paths and vRA

OK

Setup instructions for the content pack should give sufficient details about what user needs to do to receive the logs from the product/device. Setup Instructions should clearly outline the exact steps required in product/device and vRealize Log Insight (if necessary) for content pack full functional state.

In rare situations if additional configurations are required for specific widget functionality (e.g. statistics, telemetry which is not always enabled by default) it can be exceptionally added to widget description

Setup Instructions should contains detailed steps e.g. how to configure “**Remote Syslog Server**” on the device. Some of the partners also providing additional configuration guide with delated screenshots and basic troubleshooting tips.

Publishing

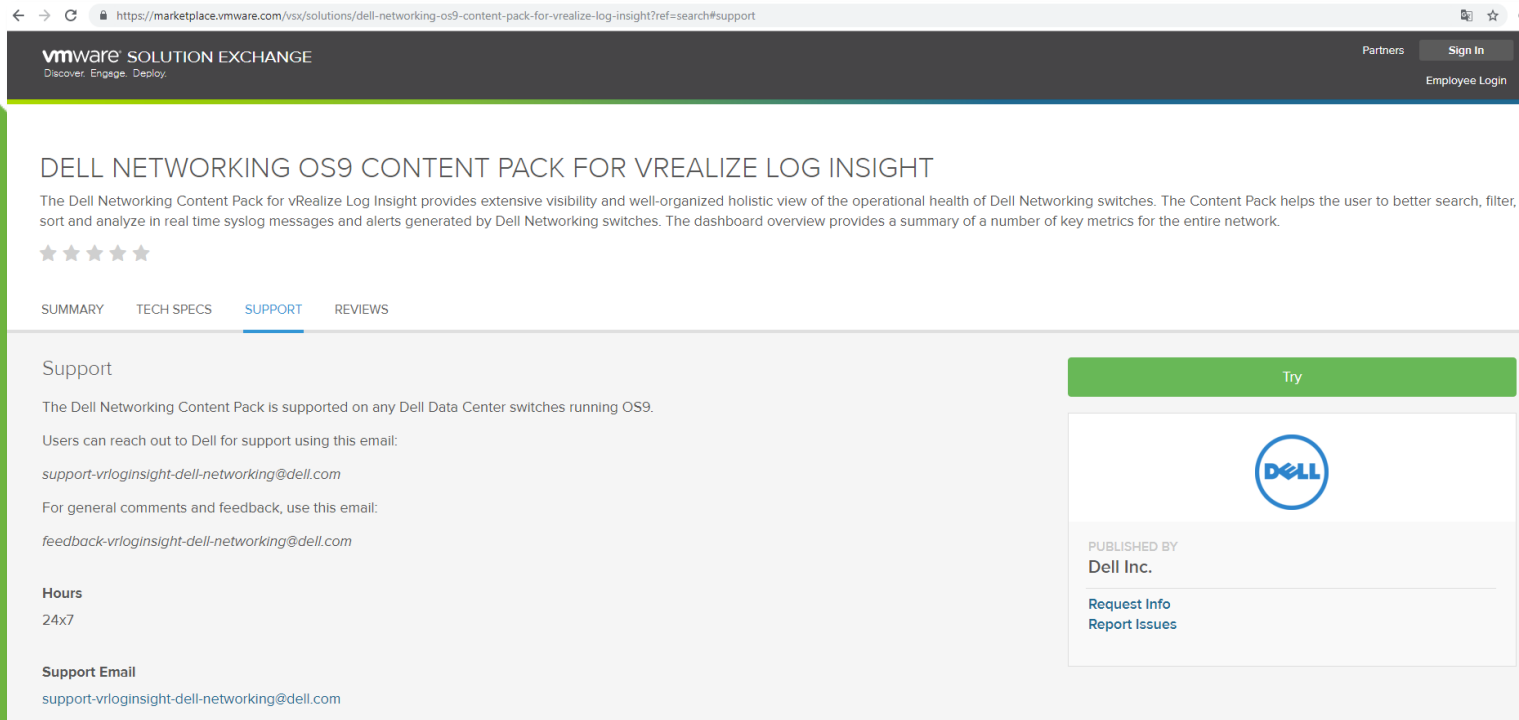
The screenshot shows the VMware Solution Exchange interface. At the top, the VMware logo and 'SOLUTION EXCHANGE' are visible, along with the tagline 'Discover. Engage. Deploy.'. Below this, there are navigation tabs for 'SOLUTIONS' and 'PRODUCTS'. The 'SOLUTIONS' tab is active, and a search bar contains the text 'juniper'. The search results are displayed under the heading 'SEARCH RESULTS (1)'. A list of vRealize Log Insight versions is shown at the top of the results: vRealize Log Insight 1.5.x, 2.0.x, 1.0.x, 4.8.x, 3.3.x, 3.0.x, 4.7.x, 4.6.x, and 4.0.x. Below this, a search result card for 'JUNIPER' is displayed. The card title is 'Juniper Content Pack for VMware vRealize Log Insight'. It includes the following details: 'Version: 1.x', 'By: Juniper Networks', and 'Updated: Jan-2016'. A green plus icon with '+100' is also visible. On the left side of the 'PRODUCTS' tab, a list of product categories is shown with checkboxes: vSphere (769), vRealize Automation - Advanced (208), Horizon (with View) (193), Horizon Clients (193), vRealize Log Insight (75) (checked), and a '+ See More' option.

After a content pack has been created by partners in the vRealize Log Insight Partner Program, the content pack has to be reviewed and approved by the vRealize Log Insight Content Pack team via DCPN, post approval it can be published to the in-product vRealize Log Insight marketplace and on the VMware Solution Exchange.

The requirements for content pack publishing are as follows:

- Must be a partner in the Log Insight Partner Program.
- Content pack: a tested VLCP file ready for publishing.
- Logs: Appropriate log bundle that is necessary to validate content pack by Log Insight team, especially from performance perspective.
- Documentation: Information about how to configure the product/application to forward logs to vRealize Log Insight. Some release notes and upgrade instructions if it is an update to a published content pack.
- versions of the product/device which was tested with the provided solution
- support information
- screenshots from the solution reflecting the power of the dashboards widgets
- (Optional) Demo/Story: Example of how the content pack brings value (for example, YouTube video).

Support cases



vmware SOLUTION EXCHANGE
Discover. Engage. Deploy.

Partners Sign In
Employee Login

DELL NETWORKING OS9 CONTENT PACK FOR VREALIZE LOG INSIGHT

The Dell Networking Content Pack for vRealize Log Insight provides extensive visibility and well-organized holistic view of the operational health of Dell Networking switches. The Content Pack helps the user to better search, filter, sort and analyze in real time syslog messages and alerts generated by Dell Networking switches. The dashboard overview provides a summary of a number of key metrics for the entire network.

★★★★★

SUMMARY TECH SPECS **SUPPORT** REVIEWS

Support

The Dell Networking Content Pack is supported on any Dell Data Center switches running OS9.


Users can reach out to Dell for support using this email:
support-vrloginsight-dell-networking@dell.com

For general comments and feedback, use this email:
feedback-vrloginsight-dell-networking@dell.com

Hours
24x7

Support Email
support-vrloginsight-dell-networking@dell.com

Try



PUBLISHED BY
Dell Inc.

[Request Info](#)
[Report Issues](#)

Typical customer issues with Content Packs which are not related to Log Insight functionality:

- misconfigured environment
- log format changes
- log expected to be generated but it doesn't (configuration steps are not enough clear or not sufficient)
- All other cases are covered by vRealize Log Insight Content Pack team

Useful links

For any clarifications about vRealize Log Insight Content Packs functionality, contact li-cp@vmware.com

- Good source of documentation about publishing process, creation of Content Packs:
 - <https://code.vmware.com/web/loginsight>
- Best practices guideline:
 - [Creating content packs in vRLI](#)
- Joining the vRealize Log Insight Partner Program
 - <https://code.vmware.com/programs/management/vrealize-loginsight>