vRealize Log Insight Evaluation Guide

VMWARE TECHNICAL MARKETING 2018

Table of Contents

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Introduction

This document outlines the process to evaluate VMware vRealize Log Insight. This document provides details on product installation and configuration; then guides you through using Log Insight.

The evaluation includes two easy-to-follow sections:

- Installation and Setup
- How to Use Log Insight

For more details and information, please use the following references:

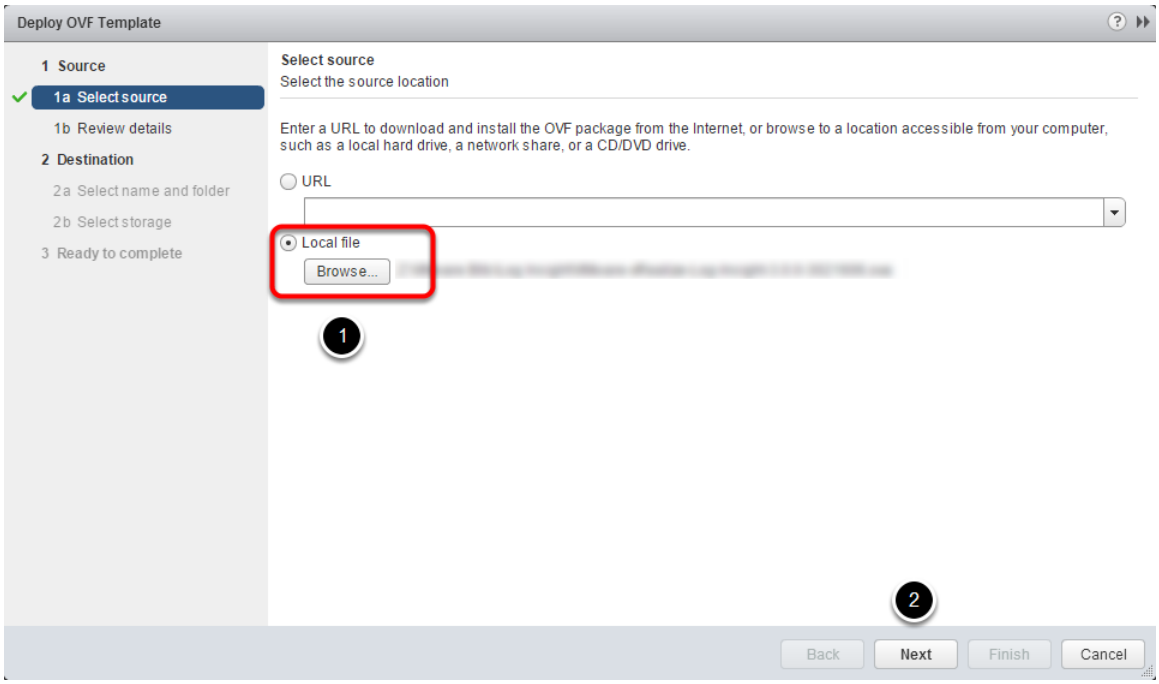
- The Appendix of this document contains sections that will help you during the evaluation.
- YouTube Log Insight Playlist Contains videos that will help you better understand vRealize Log Insight
- vRealize Log Insight Product page

Evaluation Installation and Setup

Follow standard deployment methods for an OVF/OVA in the vSphere client of your choice. For specifics on deploying vRealize Log Insight, follow the steps below and reference the following video:

Log Insight Installation and Configuration Video

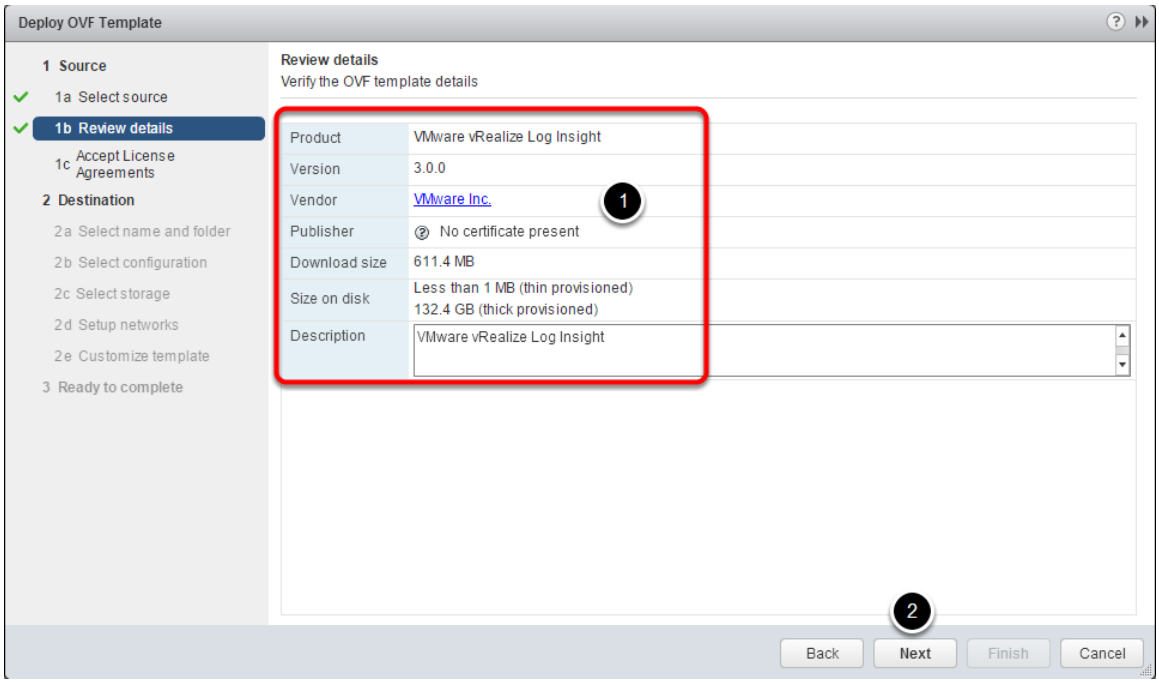
Installing the OVA



1. Browse to the **vRealize Log Insight Appliance OVA.**

2. Click **Next**.

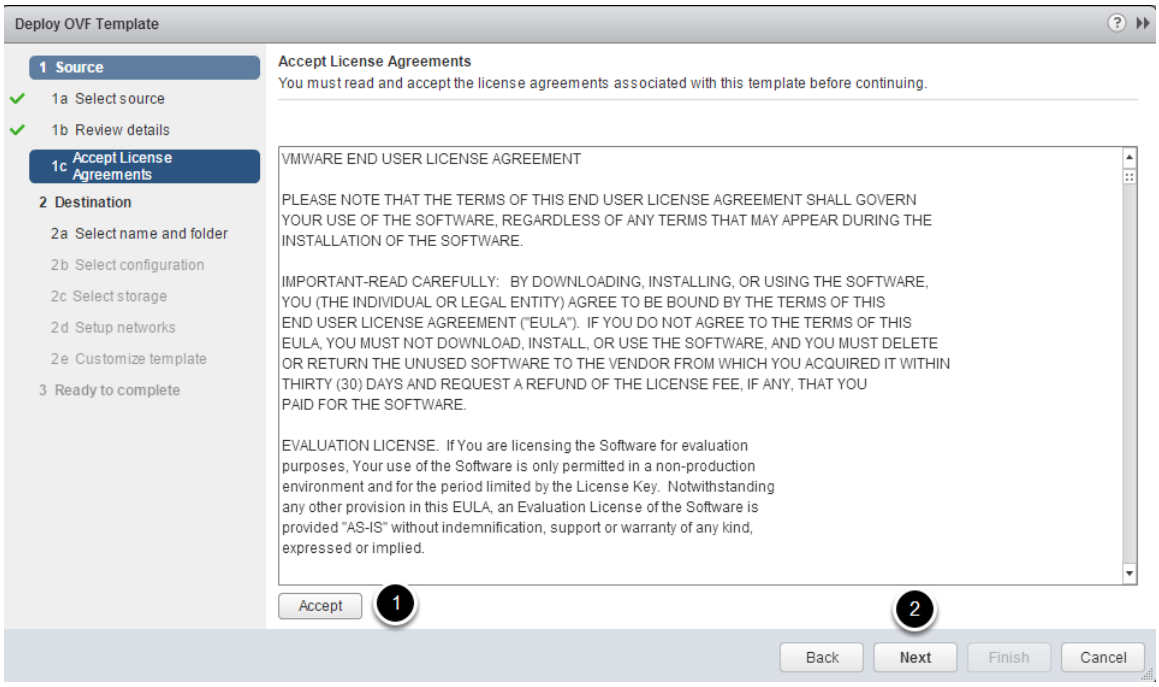
OVA Review details



1. Verify the OVF template details.
2. Click **Next.**

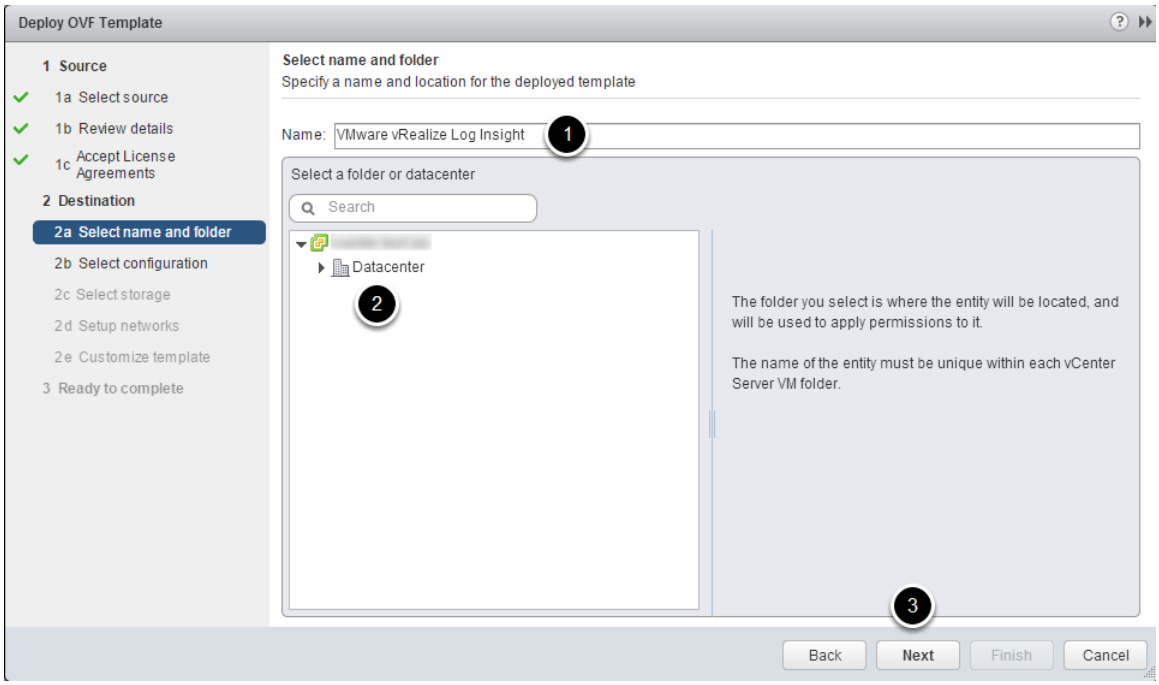
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

OVA Accept EULA



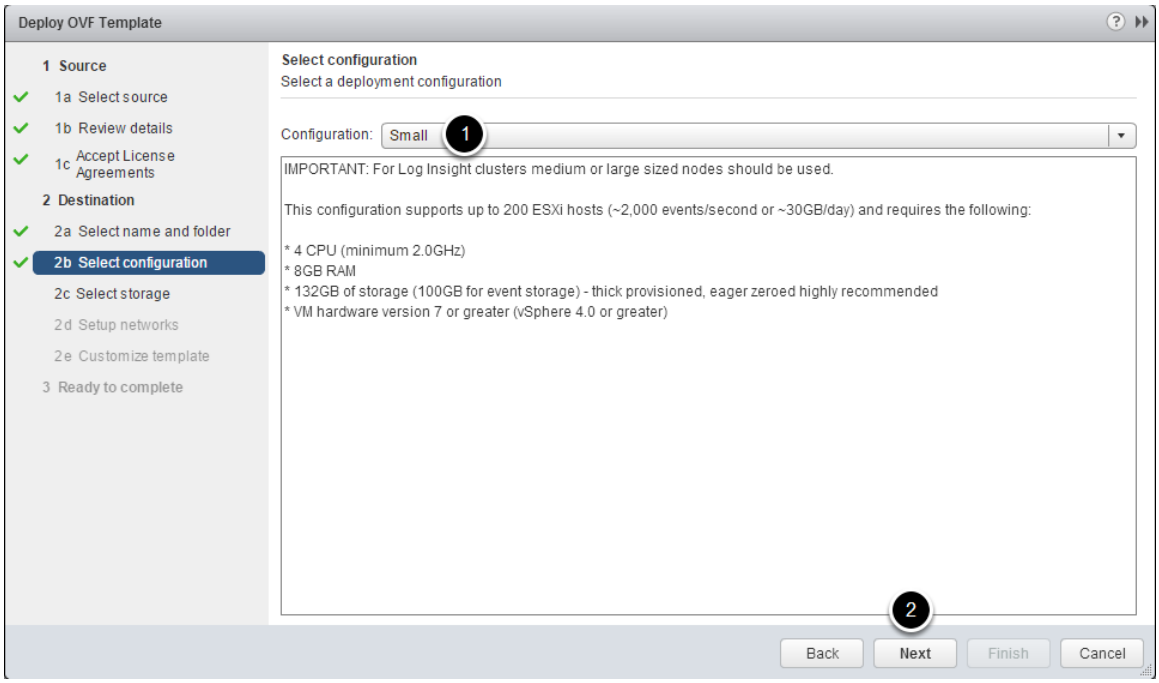
1. Click **Accept**.
2. Click **Next**.

Choose a Name and Destination



1. Name the Log Insight VM.
2. Select a **datacenter** or **target folder**.
3. Click **Next**.

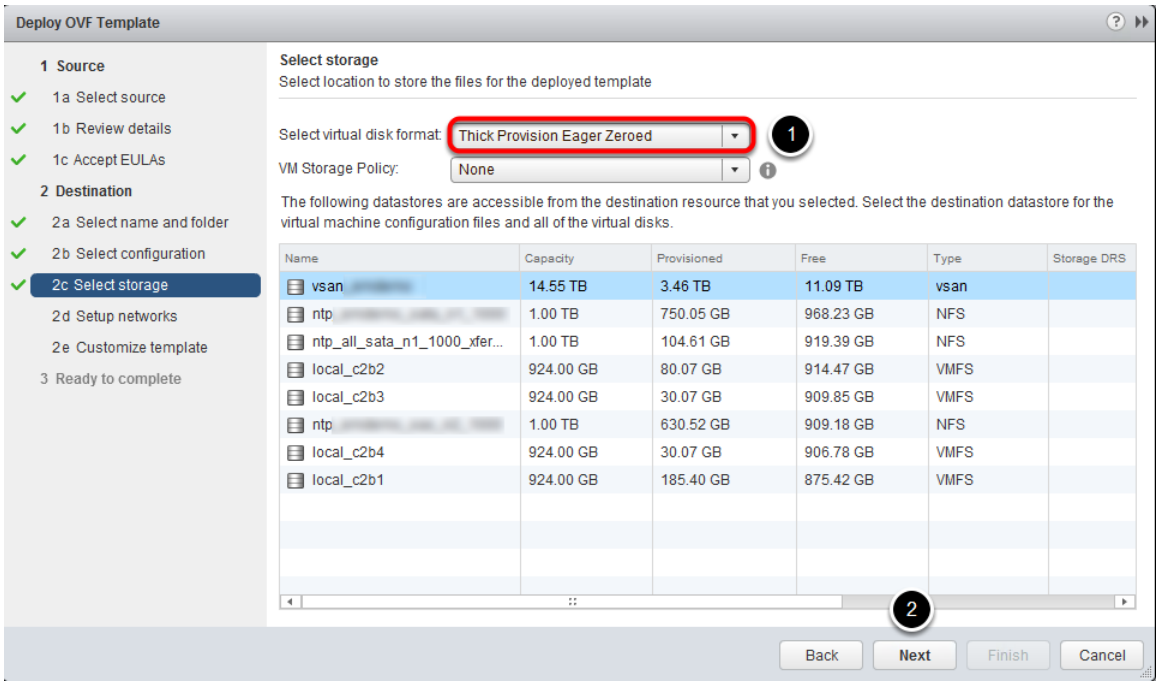
Sizing



1. Pick a **configuration size.** Typically **small** is used for an evaluation. For more information on sizing please consult the Log Insight documentation: Sizing guidance.

2. Click **Next**.

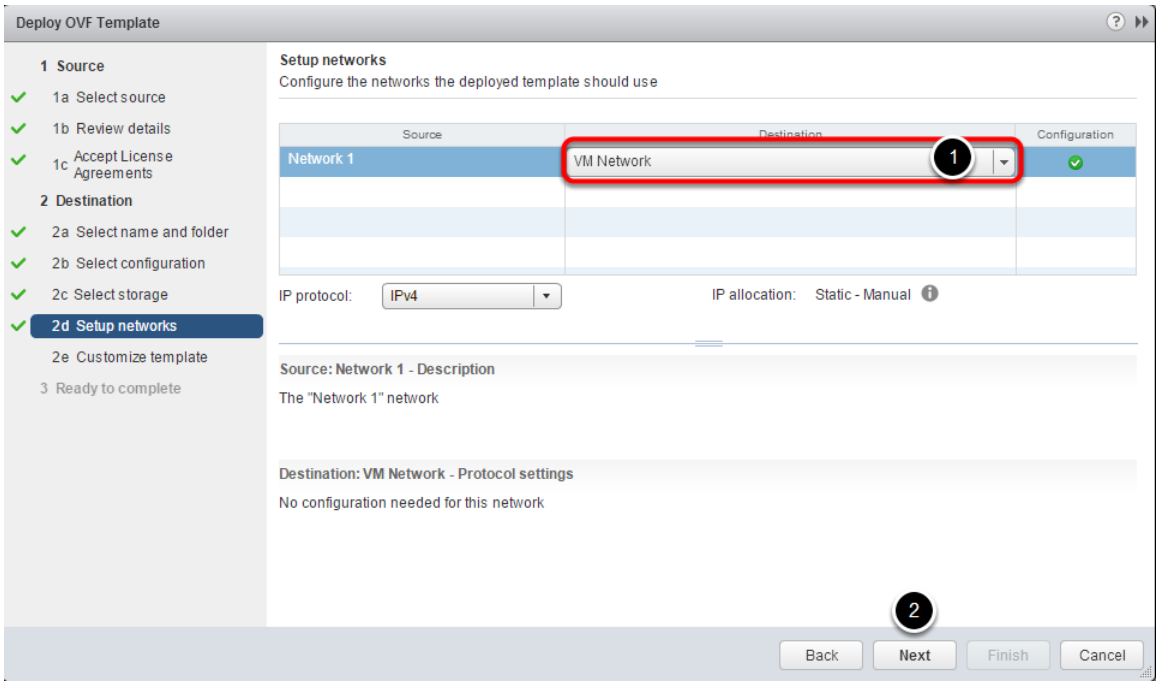
Choose the Target Storage



1. Choose **target storage** for the VM. Deploy the vRealize Log Insight virtual appliance with thick provisioned eager zeroed disks whenever possible for better performance and operation of the virtual appliance.

2. Click **Next**.

Select Network



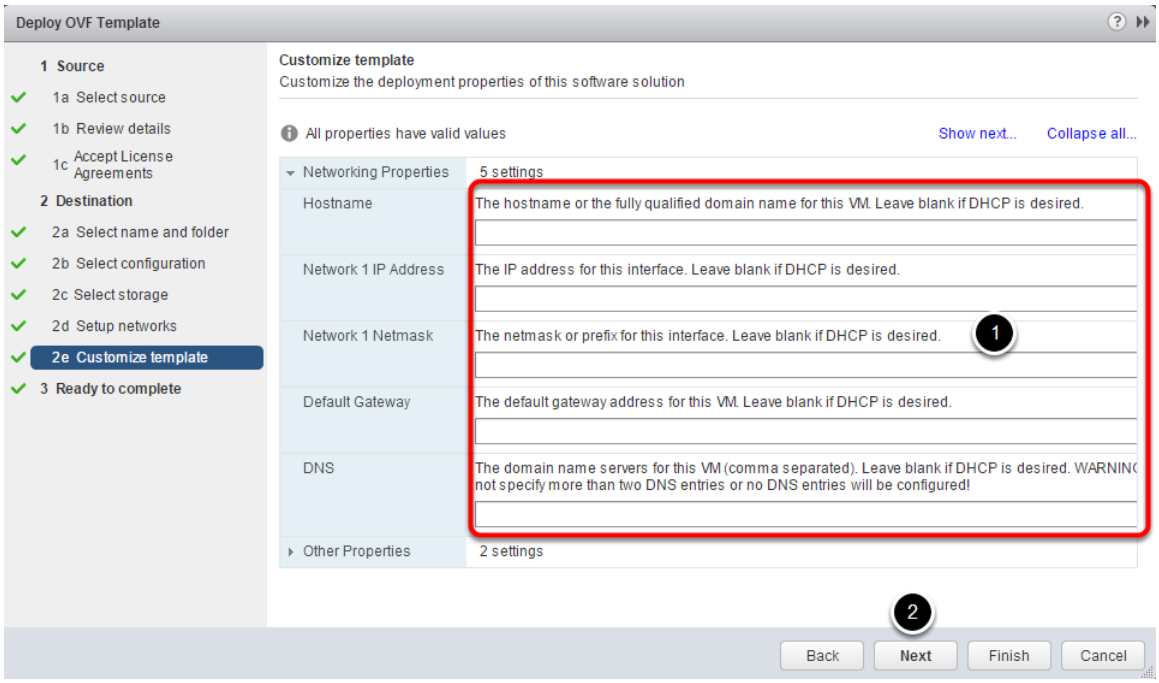
1. Select a **network** which provides access to DNS and NTP services as well as Active Directory and DHCP if required. Additionally the network should allow access to endpoints that will be used for log ingestion

2. Click **Next**.

(**Note:** if a cluster installation is planned, all cluster nodes must be installed

on the same Layer 2 network.)

Configure Network Settings

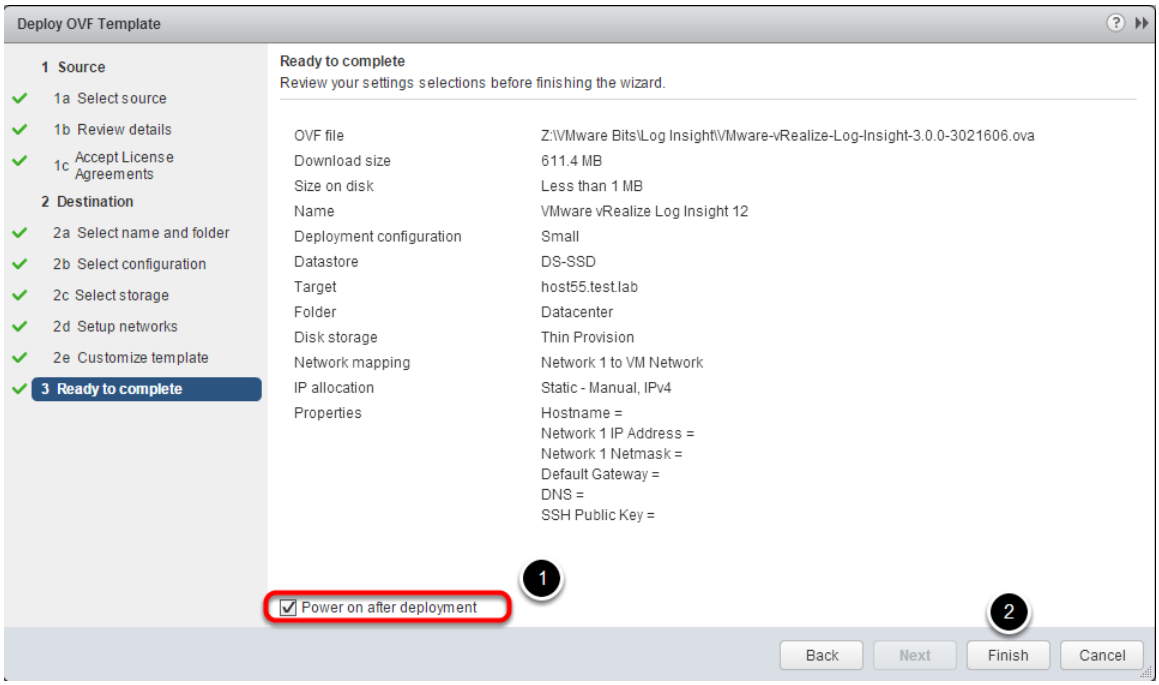


1. Configure the appropriate **network setting** for the VM. Leave the fields blank for DHCP assignment.

2. Click **Next**.

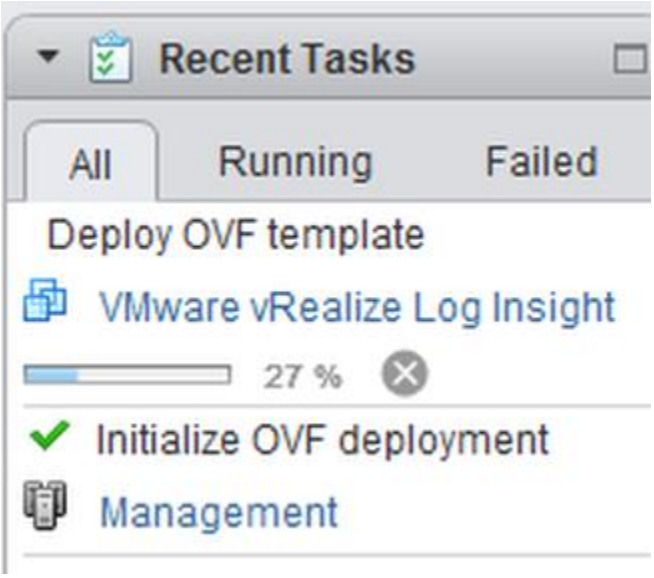
(**Note:** It is highly recommended to use an FQDN entry for the vRealize Log Insight virtual machine.)

Confirm the Installation Settings



1. **Optionally** choose Power on after deployment.
2. Click **Finish**.

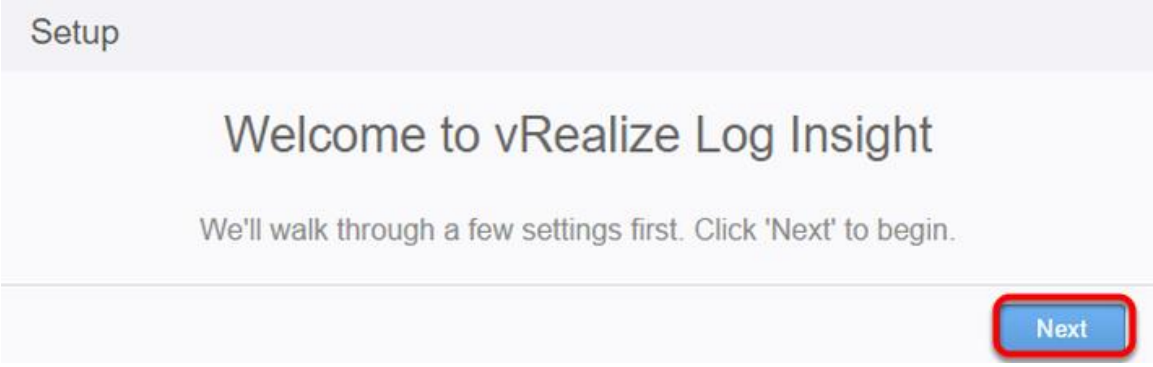
VM Deployment



Wait for the VM to deploy and start.

Once the vRealize Log Insight VM is running, you can point a browser at the appliance IP address or FQDN, and move to the configuration wizard.

Initial Log Insight Configuration Wizard

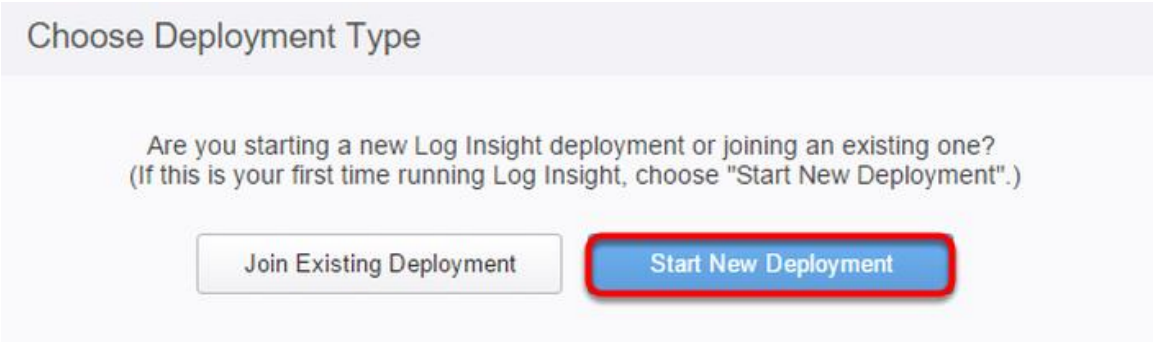


After entering the Log Insight VM's IP address or FQDN, the configuration wizard will appear.

Click **Next** to continue.

(**Note:** These steps assume the Log Insight OVA has already been deployed and the VM has started.)

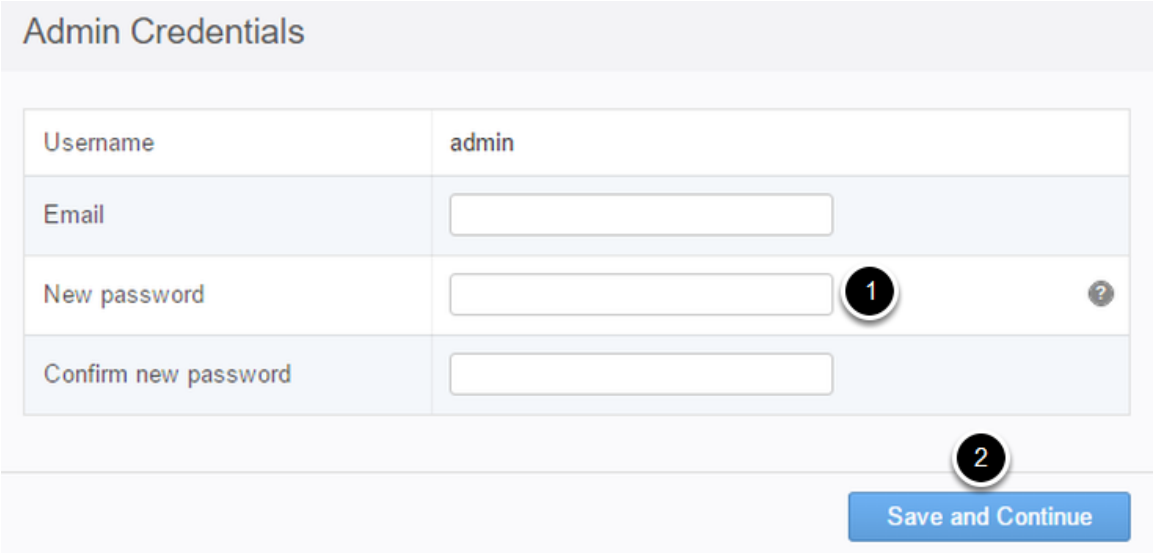
Choose Deployment Type



Choose **Start New Deployment.**

(**Note:** Log Insight supports up to a 12 node cluster installation. For this evaluation we are focusing on installing a single node. Installation of additional cluster nodes is covered in the appendix of this evaluation guide**.)**

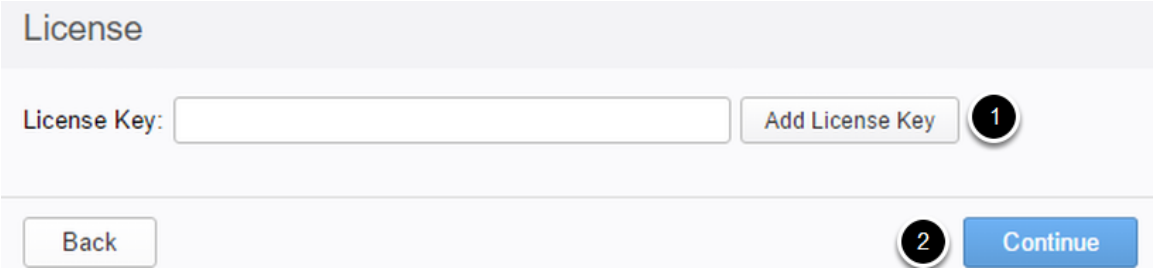
Admin Credentials



1. Enter the **email address and password** for the admin account.

2. Click **Save and Continue.**

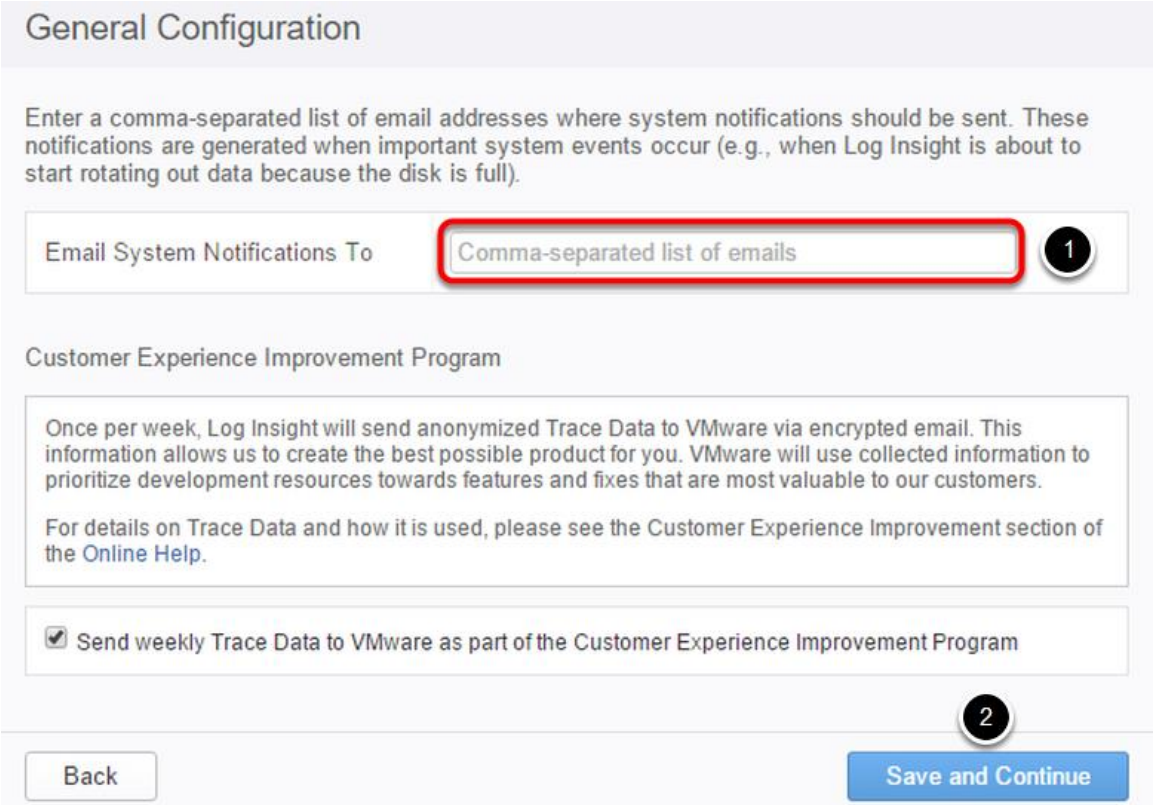
License Key



1. Add the **evaluation license key** that was obtained from MyVMware.com. Click **Add Licence Key**.

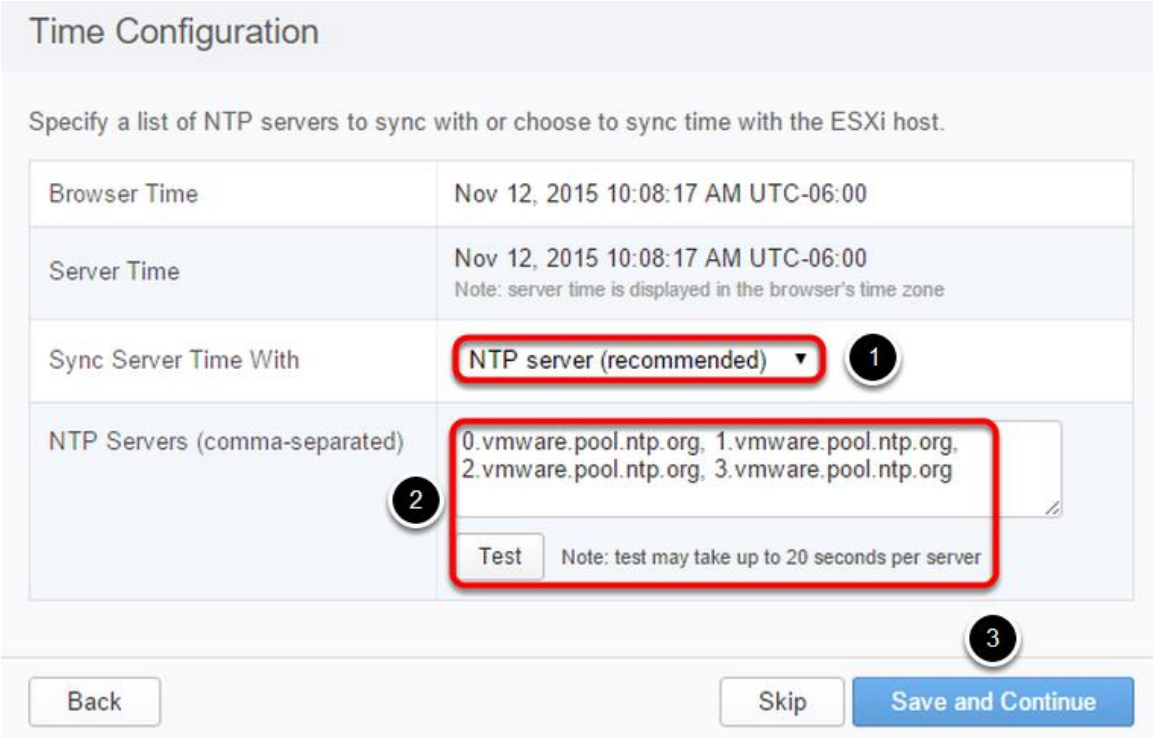
2. Click **Continue**

System Notifications



1. Enter an **email address** where **system notifications** will be sent.
2. Select **Save and Continue**.

Configure NTP

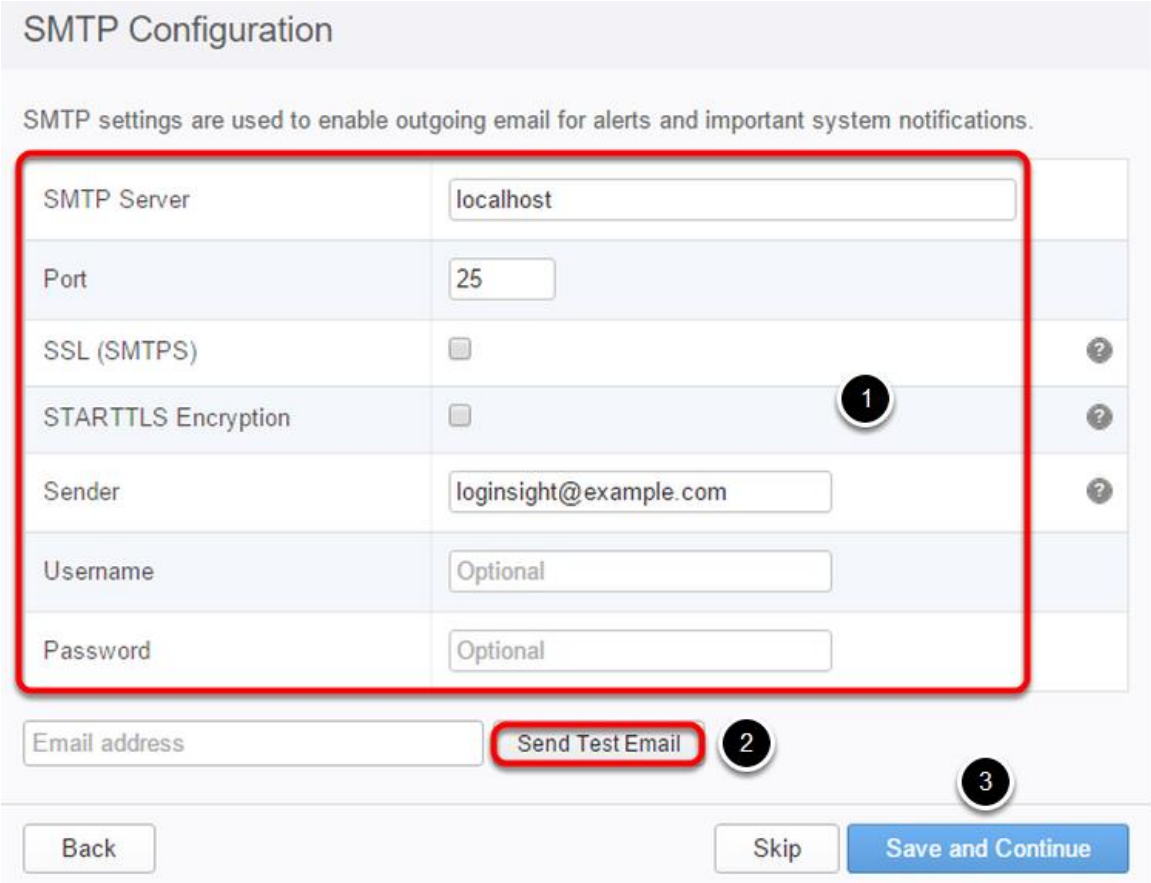


1. Using the **default NTP server** option to synchronize time within vRealize Log Insight is **highly recommended**. If an external NTP server is not accessible due to firewall settings, you can use an internal NTP server from your organization or **optionally an ESXi Host**.

2. You may leave the default NTP servers or choose your own. Use commas to separate multiple NTP servers. Click **Test** to verify the listed NTP servers.

3. Click **Save and Continue**.

Configure SMTP

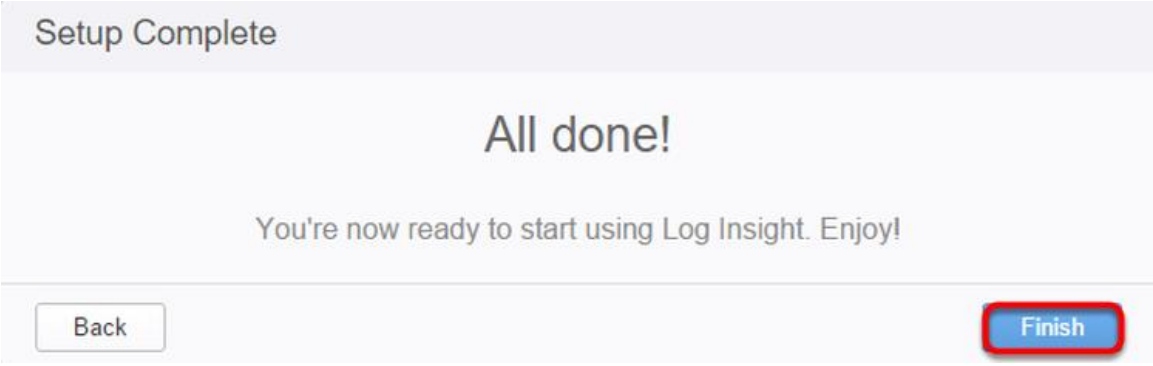


1. Enter SMTP server information to enable outgoing email for alerts and system notifications.

2. Click **Send Test Email** to validate the SMTP server settings and credentials.

3. Click **Save and Continue**.

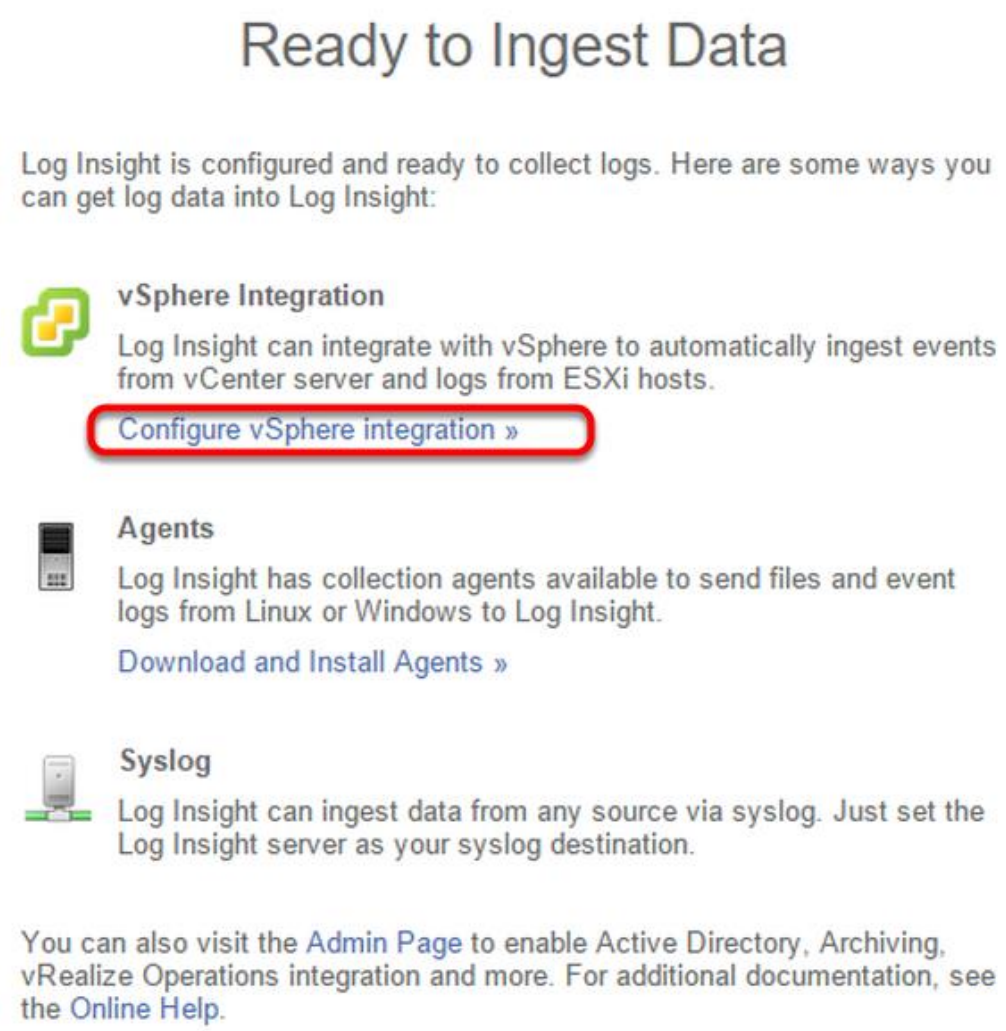
Complete Initial Configuration



Click **Finish**.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

vSphere Integration

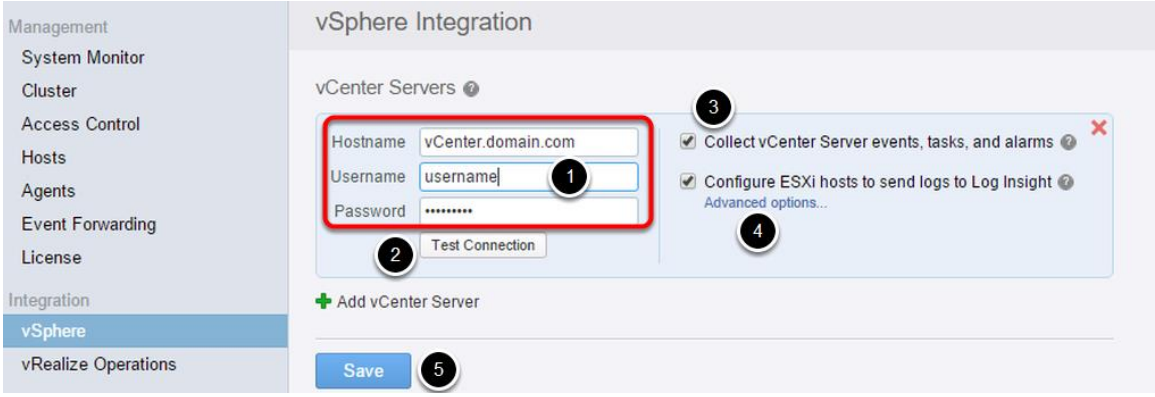


To ingest data from vSphere, you must configure Log Insight to collect data from vCenter Server(s) and configure ESXi Hosts to forward Syslog. When using this integration, Log Insight collects structured data in the form of events, tasks, and alarms from vCenter and unstructured log data from ESXi Hosts.

For this step, you will need the FQDN or IP of all the vCenter Servers to be used for the evaluation.

Click **Configure vSphere Integration**.

Configure Integration



You can integrate additional vCenter Servers with associated ESXi Hosts by clicking **Add vCenter Server**

1. Enter the **Hostname** of the vCenter server where Log Insight will collect events, tasks, and alarms.

The user account must have at a minimum, **System.View privileges in vCenter and the ability to change syslog settings within ESXi**.

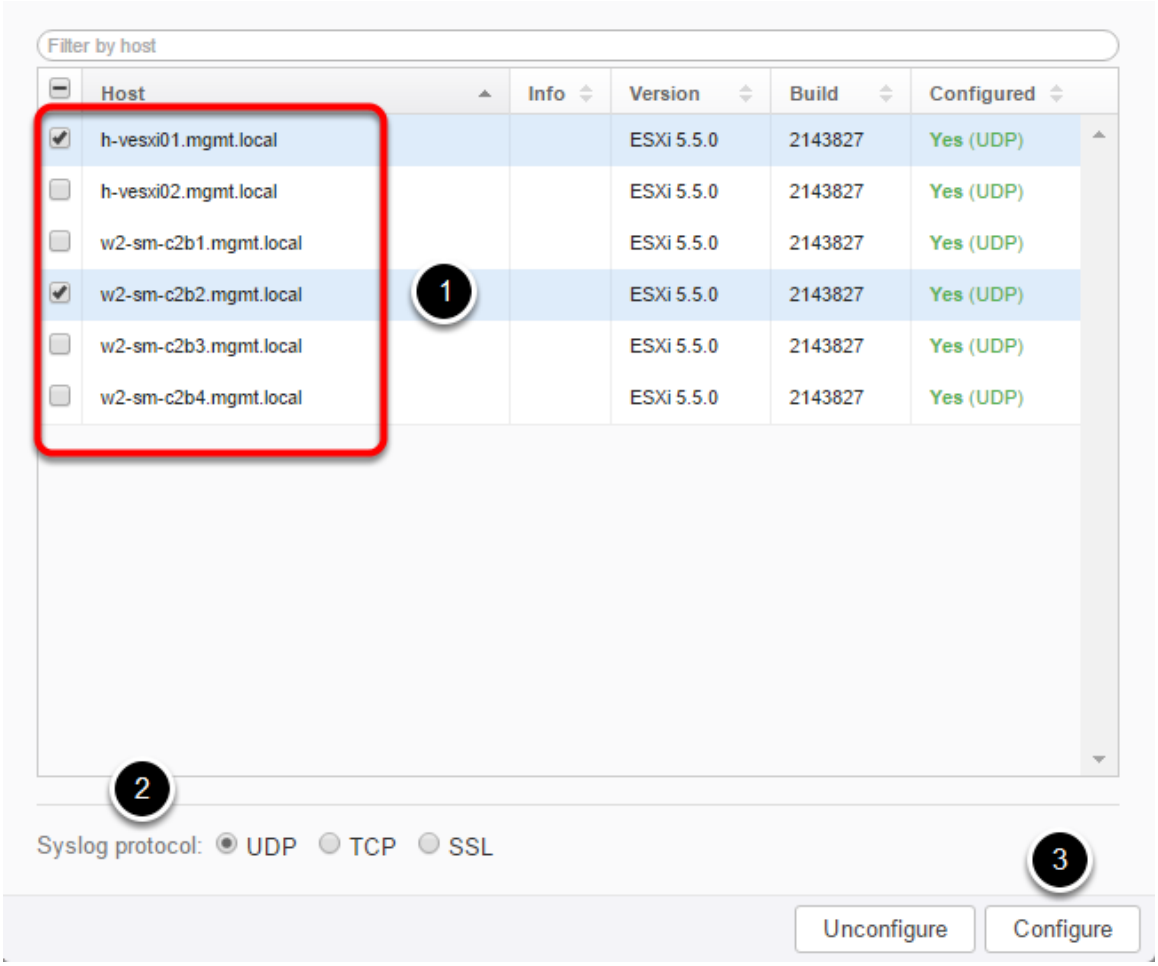
2. Click Test Connection to validate new connection.

3. Verify the checkboxes for **Collect vCenter Server events, tasks, and alarms and Configure ESXi hosts to send logs to Log Insight are checked**.

4. **(<u>Optional</u>)** The typical process configures all associated ESXi Hosts to forward logs to Log Insight. Alternatively you can configure (or unconfigure) specific ESXi Hosts instead of every Host. To configure individual hosts, click **Advanced options** and **move to the next step <u>before</u> clicking Save on #5**.

5. Click Save

Choose Specific ESXi Hosts



Advanced options show the associated ESXi Hosts for the configured vCenter.

1. Select the ESXi Hosts to configure for this evaluation

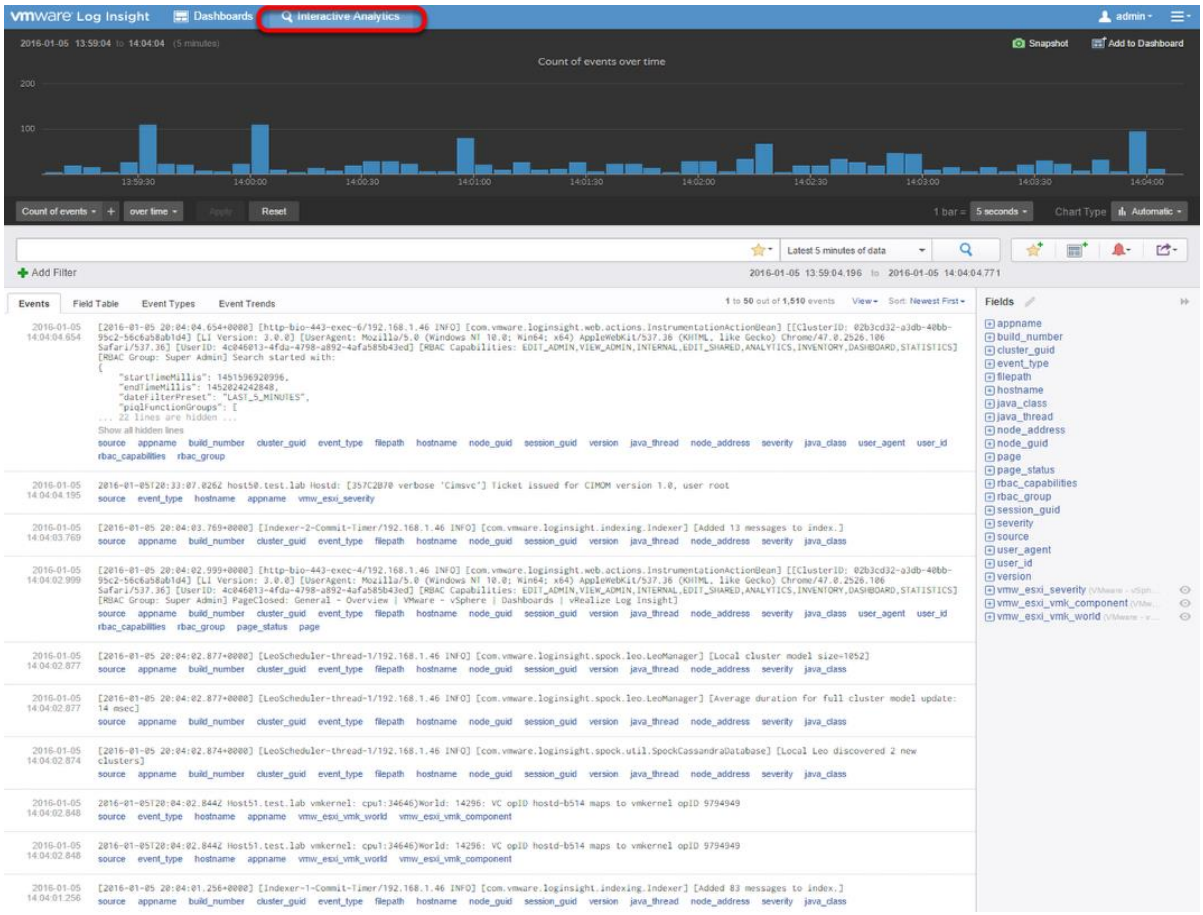
2. Choose a Syslog protocol option

3. Select **Configure.**

(**Note:** To reset the syslog configuration on a Host to the previous configuration, select **Unconfigure**.)

You will need to click Save on the vSphere Integration screen to complete the integration. This was covered on #5 of the previous step.

vSphere Integration Complete

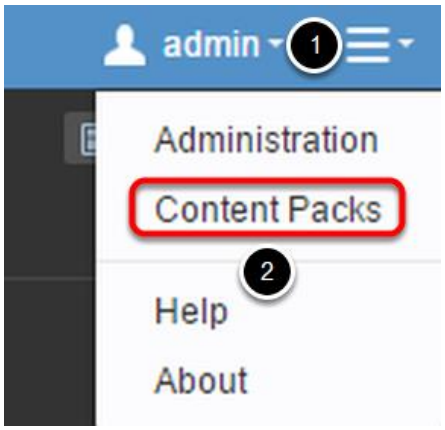


With vSphere integration complete, log events will be ingested from vCenter and ESXi Hosts.

Click the **Interactive Analytics button** to verify log messages are available.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

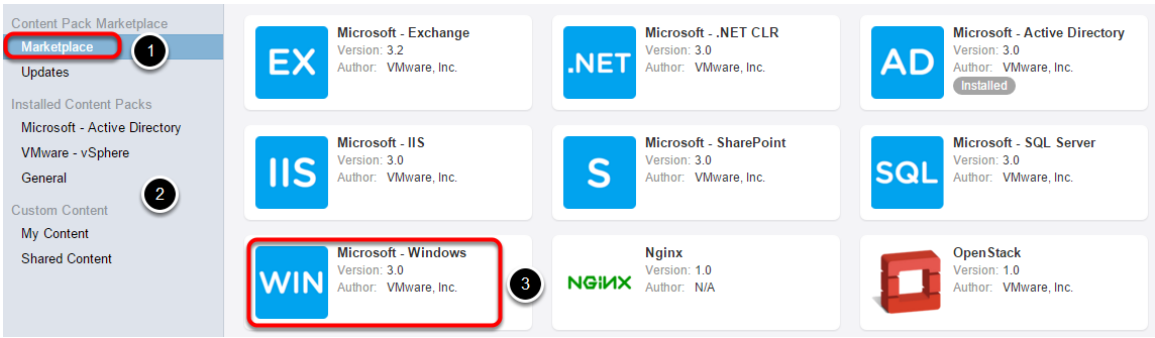
Navigate to Content Packs



1. On the upper right portion of the Log Insight interface, click the **three bars**.

2. Click Content Packs

Add Windows Content Pack



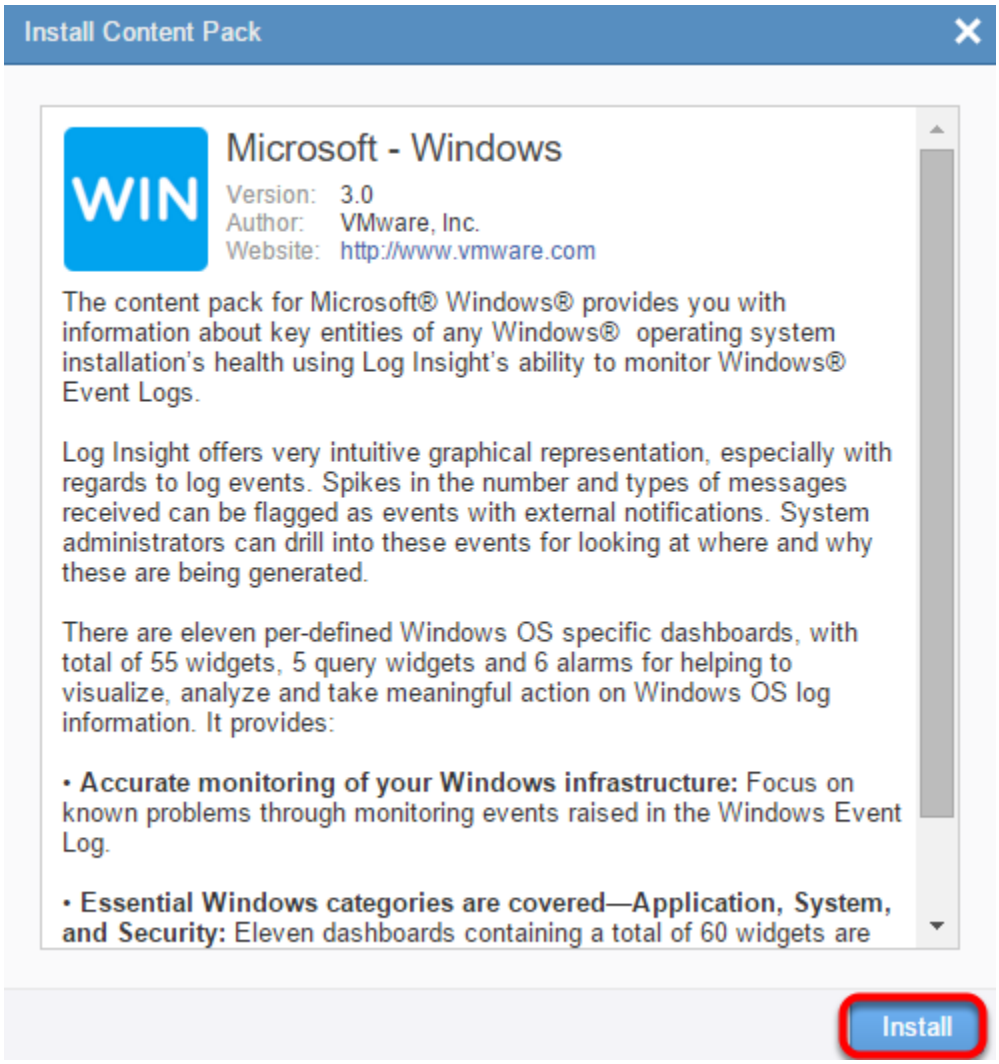
The Content Pack Marketplace is where you can access content packs for VMware and non-VMware products. Content Packs include domain specific queries, alerts, dashboards, field extractions and agent group templates for their associated products. A content pack is not required to ingest logs from a specific product. Essentially the content pack makes it easier and faster to find critical log data by highlighting and alerting you to common issues that are present in the ingested log data. As a result, troubleshooting and root cause analysis efforts take significantly less time.

1. Click Marketplace

2. Previously installed Content Packs are listed below the Marketplace as well any custom Content Packs that have been created by a Log Insight user.

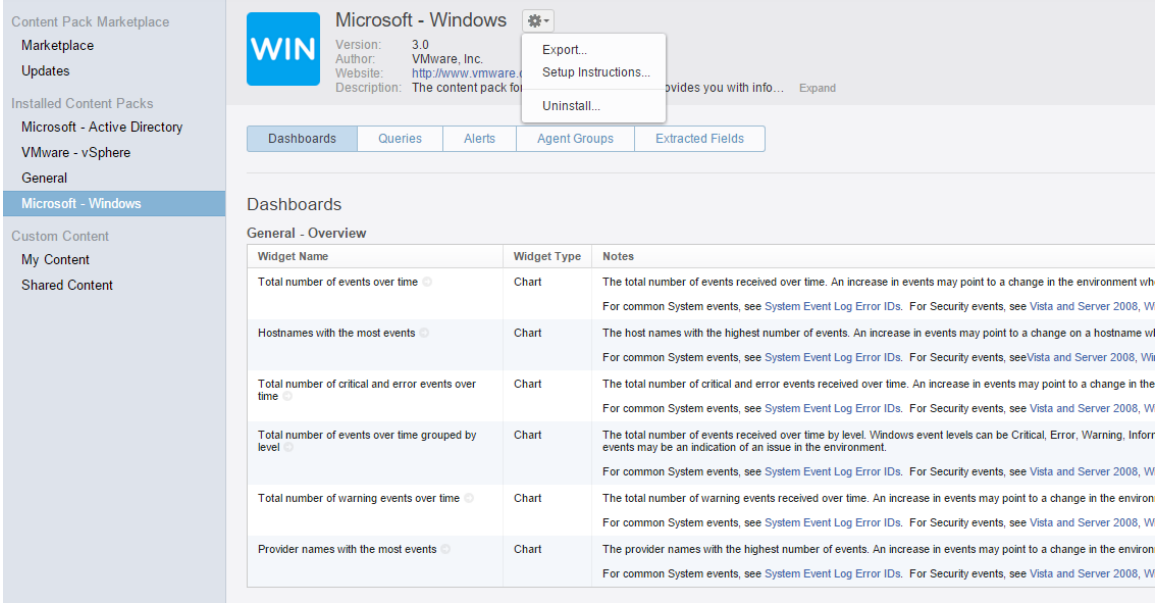
3. Click the **Microsoft - Windows Content Pack**.

Install the Windows Content Pack



Click **Install** then Click **OK**.

Content Pack Post-Install



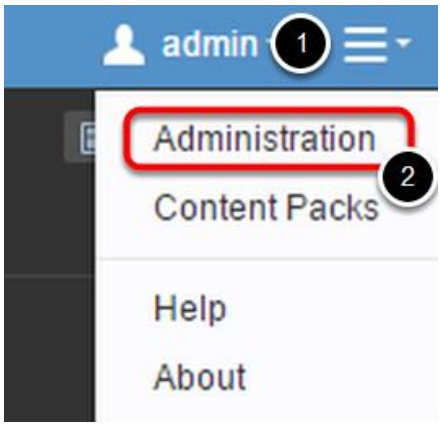
Once a Content Pack is installed you can examine the available options.

1. Click the gear to Export, view Setup Instructions, or Uninstall

2. Click the tabs to view the Dashboards, Queries, Alerts, Agent Groups, and Extracted Fields which are provided with the Content Pack

(**Note:** Extracted fields are keywords that are added to the index. These fields make searching and finding specific log events faster and more efficient. Each field is based on product specific naming within logs, product configurations, and common errors or events.)

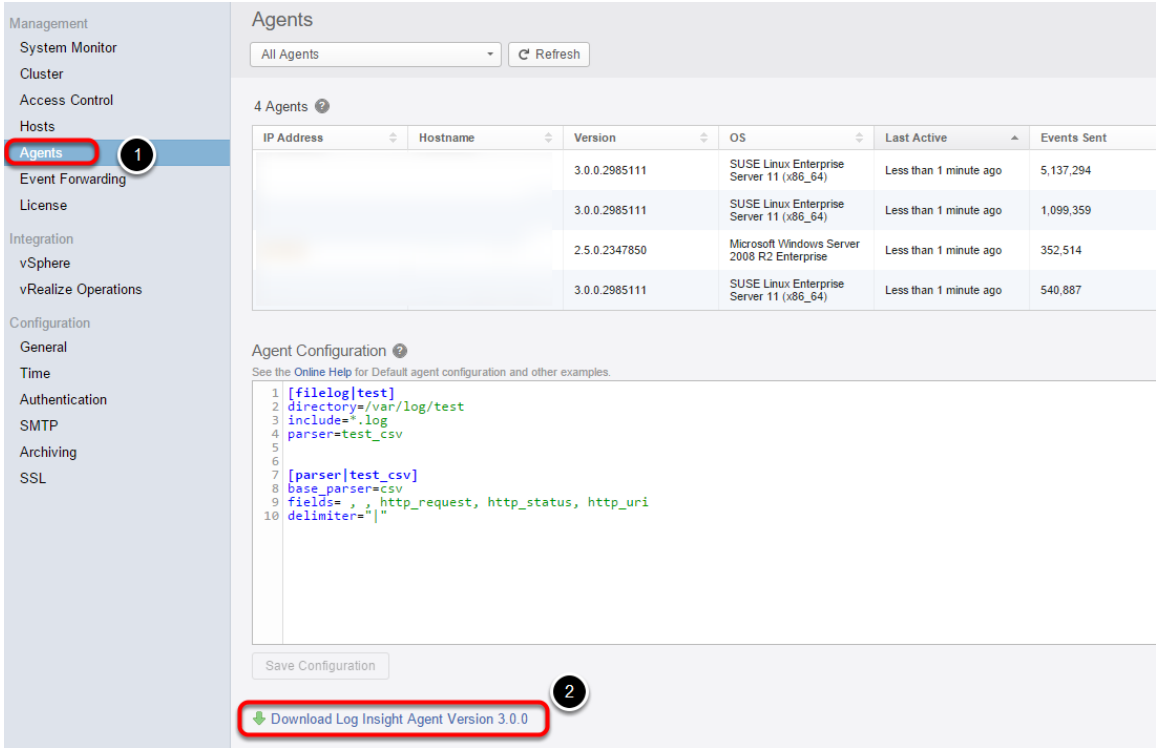
Installing and Configuring the Log Insight Agent



1. On the upper right portion of the Log Insight interface, click the **three bars**.

2. Select **Administration**.

Agents Installation



1. Within the Administration interface, **select Agents**. The Agents section shows configured agent information and status.

2. Click **Download Log Insight Agent Version**…

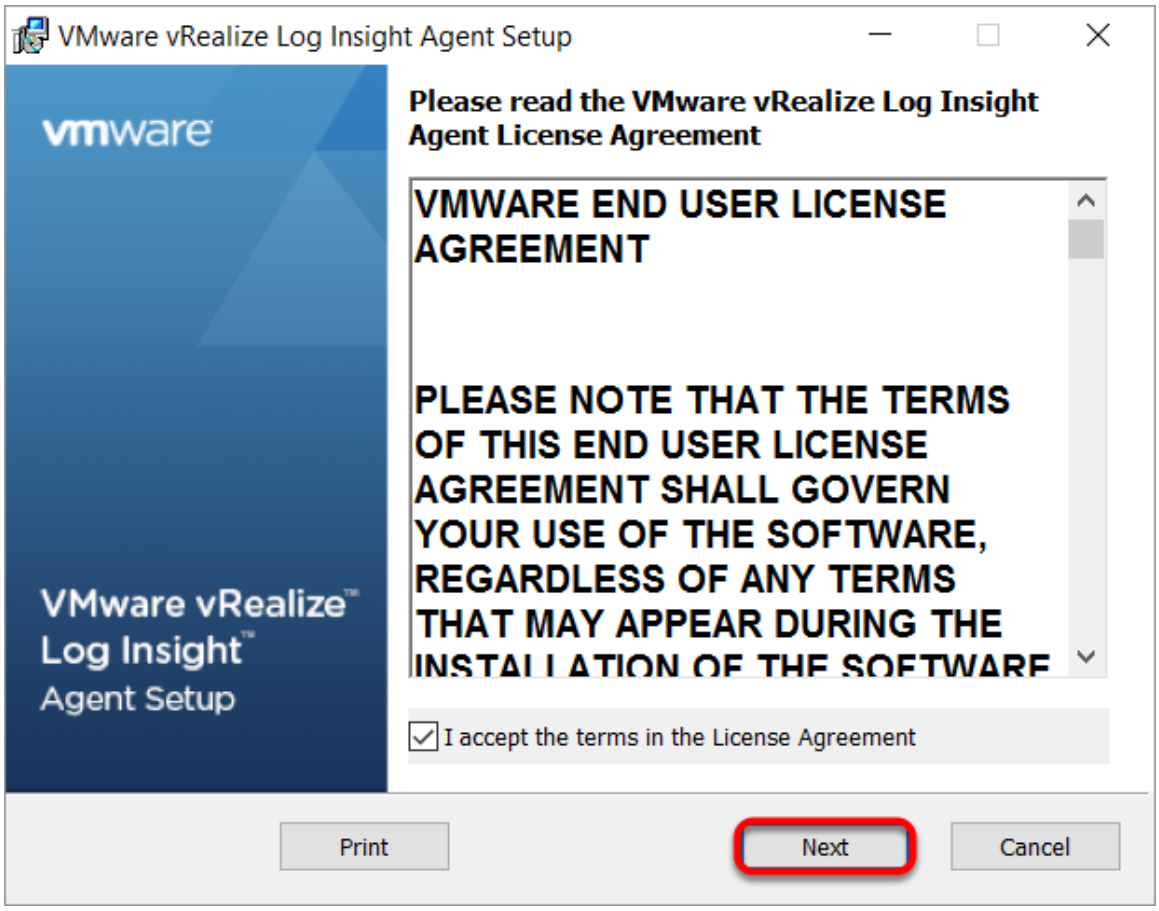
Choose the Agent OS

Windows and Linux agents are available for use. For this evaluation guide, we will choose the Windows agent MSI file.

Select **Windows MSI (32-bit/64-bit)**

Once selected, the agent binaries will download to your local Operating System.

Accept the EULA

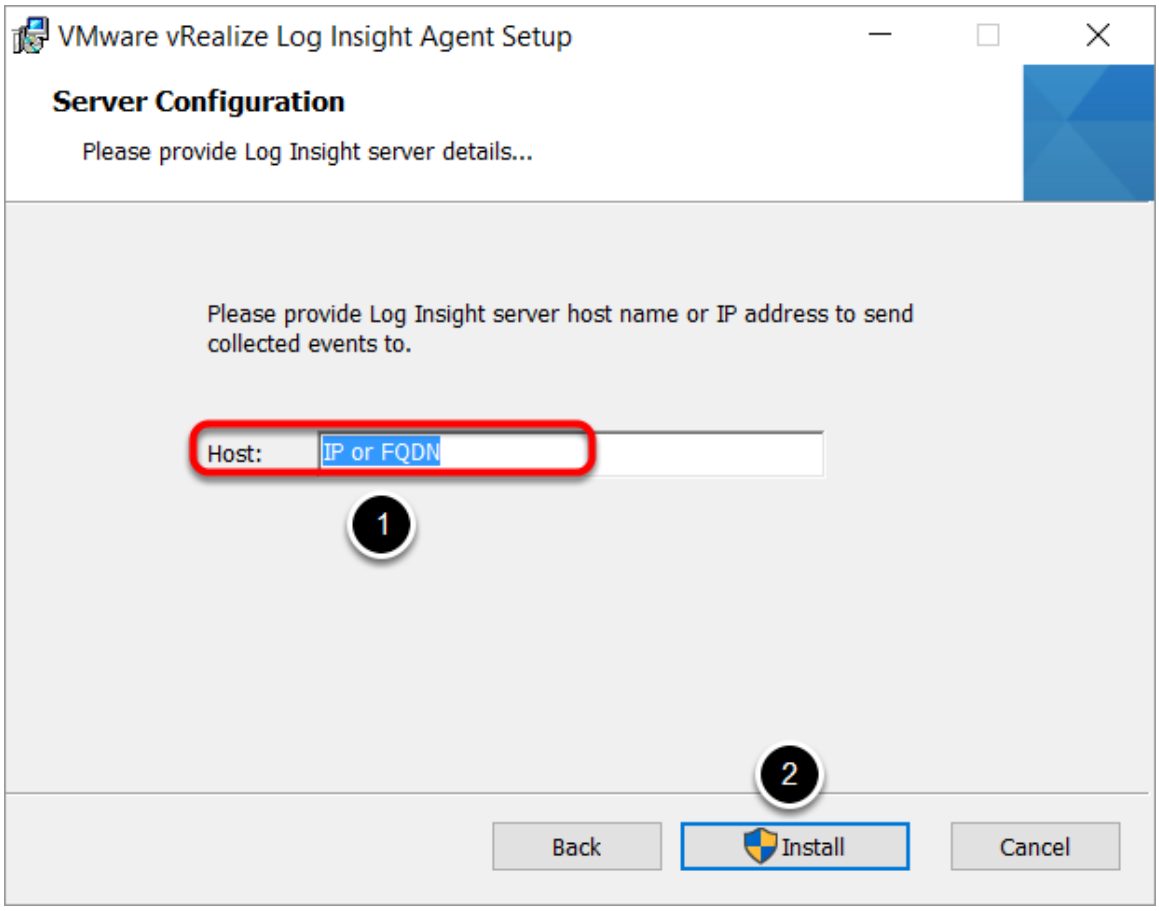


Launch the agent installation on one or more client and server machines that have been chosen for the evaluation.

The initial setup screen is the End User License Agreement. Check the box to accept the EULA and **click Next**.

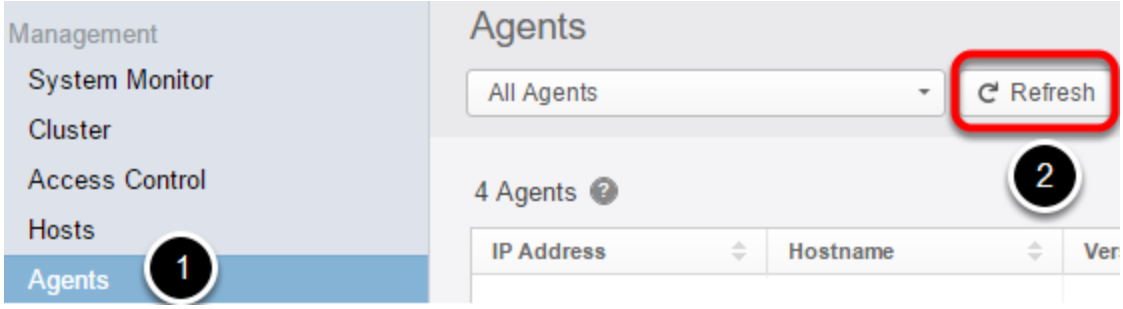
(Note: The agent files can be mass deployed using common enterprise software distribution products.)

Configure Log Event Destination



1. Enter the **IP or FQDN of your Log Insight server**.
2. Click **Install**.

Finish Agent Installation

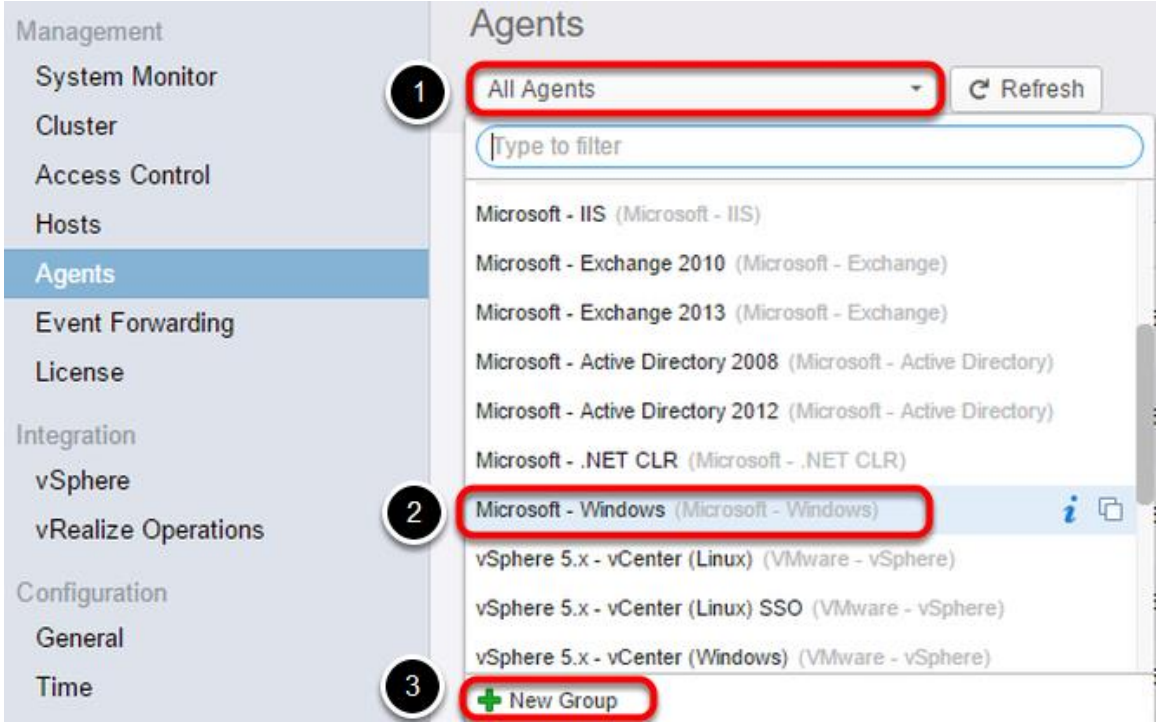


Once the install is complete, Click **Finish**.

1. Click Agents (if necessary). Your new agents should be visible a few minutes after installation.

2. Click **Refresh** if you are not seeing new agents listed.

Create a New Group

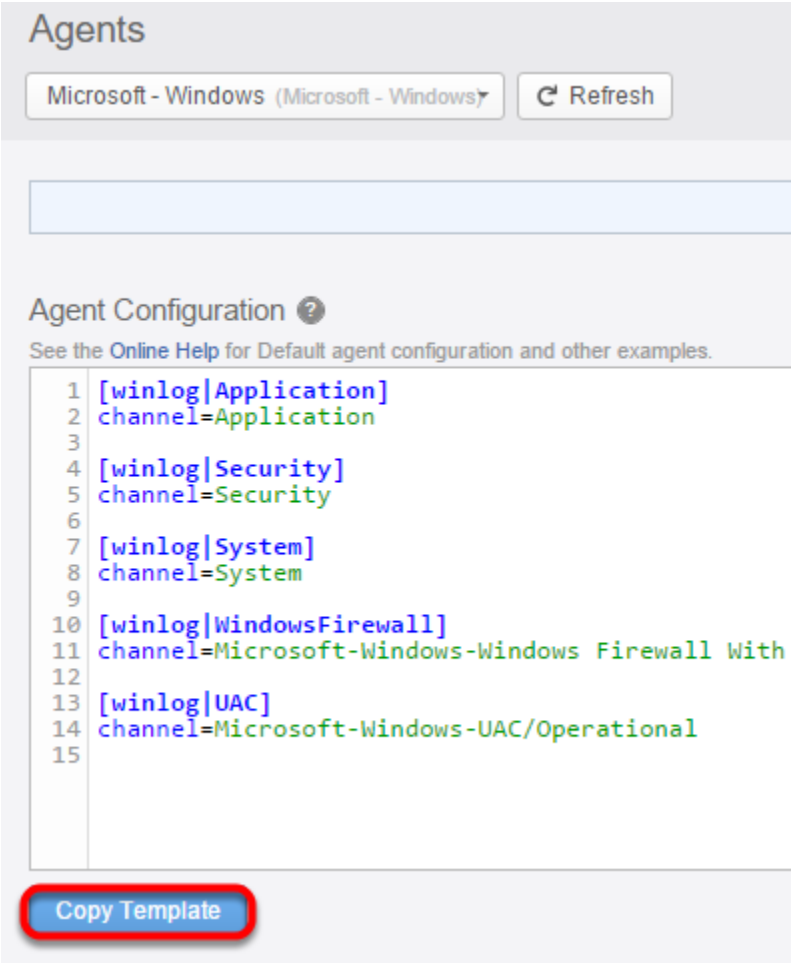


Groups allow you to configure one or many agents centrally from the Log Insight server. The group configuration is added to the liagent-effective.ini file on the client machine in the agent directory. Group agent configurations

typically add a specific log file path and file extension or in the case of Windows, the event log and associated event channel. Changes can be made locally on the client. However, if a difference is encountered between server and client-side settings, the server-side configurations settings will replace the local client configuration settings.

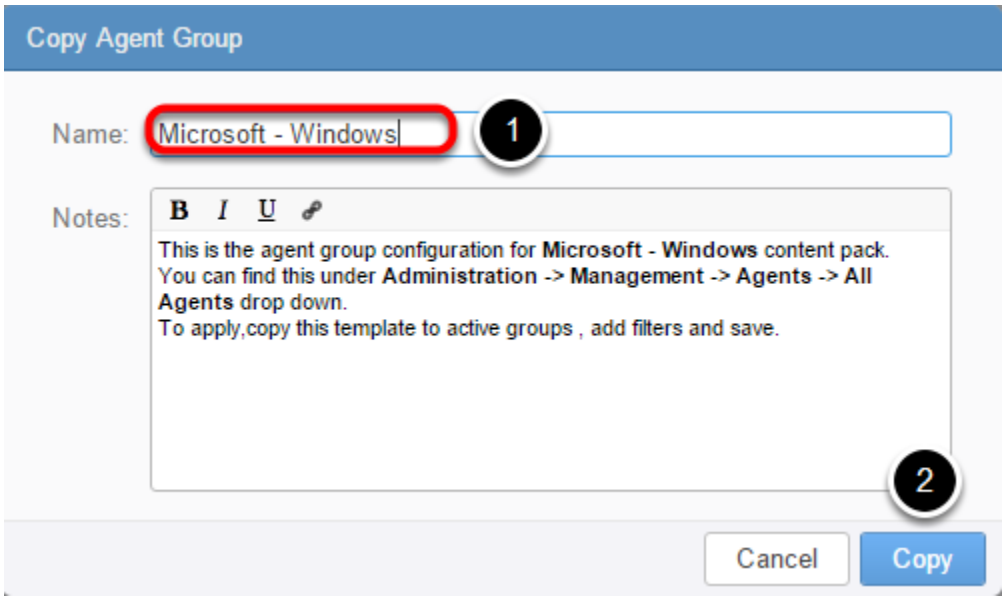
1. Select the **All Agents dropdown**.
2. Scroll down and select **Microsoft - Windows**.
3. Click **New Group**

Copy the Group Template



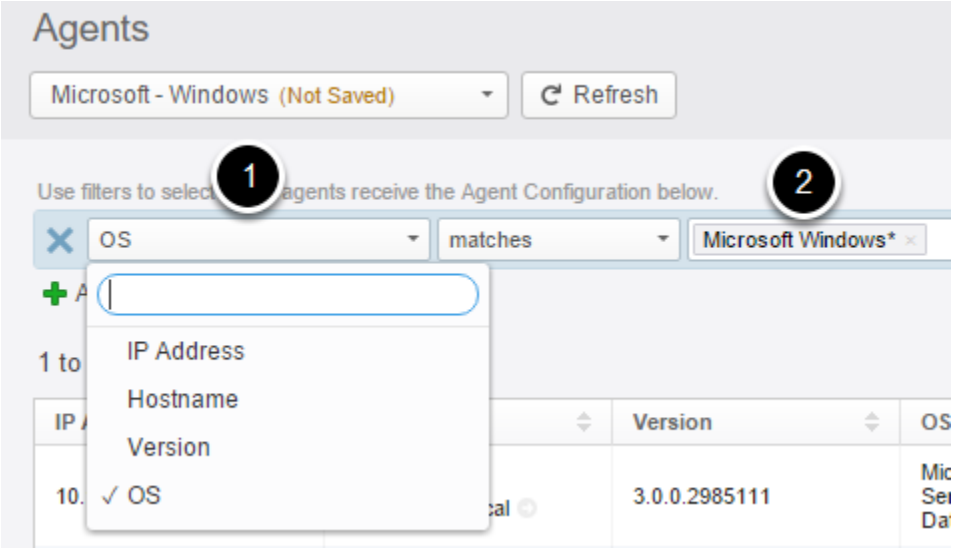
Click **Copy Template**.

Name the Group



1. Name the **Group**
2. Click **Copy**

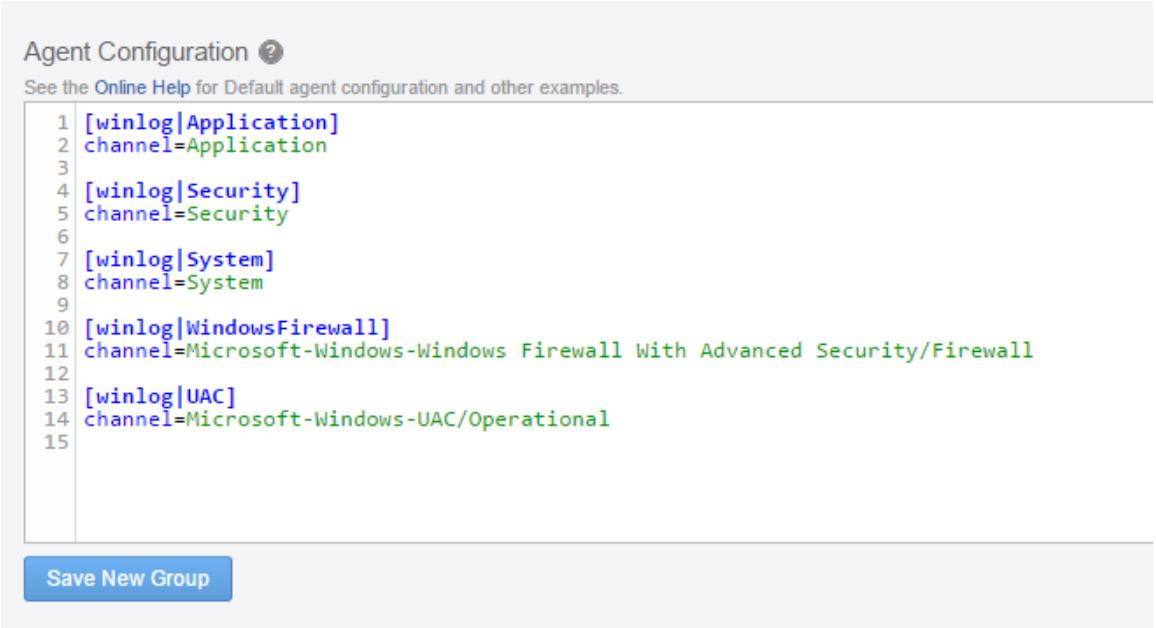
Create the Group Filter



1. Click the filter field drop down and select **OS**.
2. Type **Microsoft Windows***

This will result in a filter rule which matches any agent running on a client OS starting with Microsoft Windows.

Save the Group



Click **Save New Group**.

The agent will now collect events from the Application, Security, System, Windows Firewall, and UAC channels on the Windows operating system.

How to Use Log Insight

Log Insight User Interface

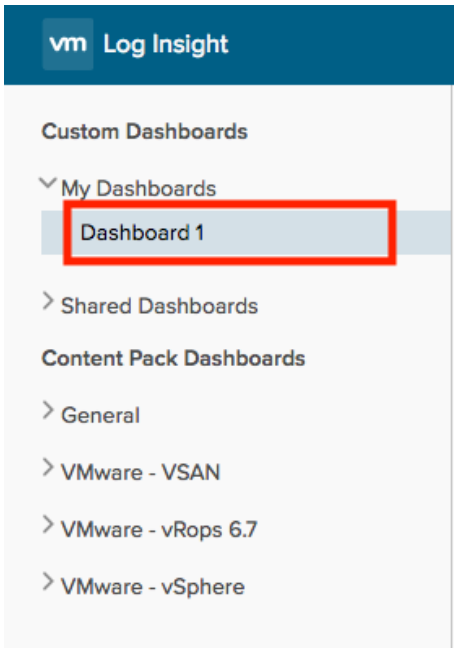
There are two primary interfaces for log monitoring and analysis in Log Insight.

- Dashboards: Dashboards are visual representations of the log data ingested by Log Insight. Dashboards are included with Content Packs or can be created and shared. Each dashboard has one or more widgets. Widgets are based upon pre-built or user created queries and include charts to visualize the log data. Query list widgets can also be created to quickly run a list of queries to determine if there are results in the log data.

- Interactive Analytics: This view allows you to examine log messages, identify problem areas, and perform root cause analysis.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

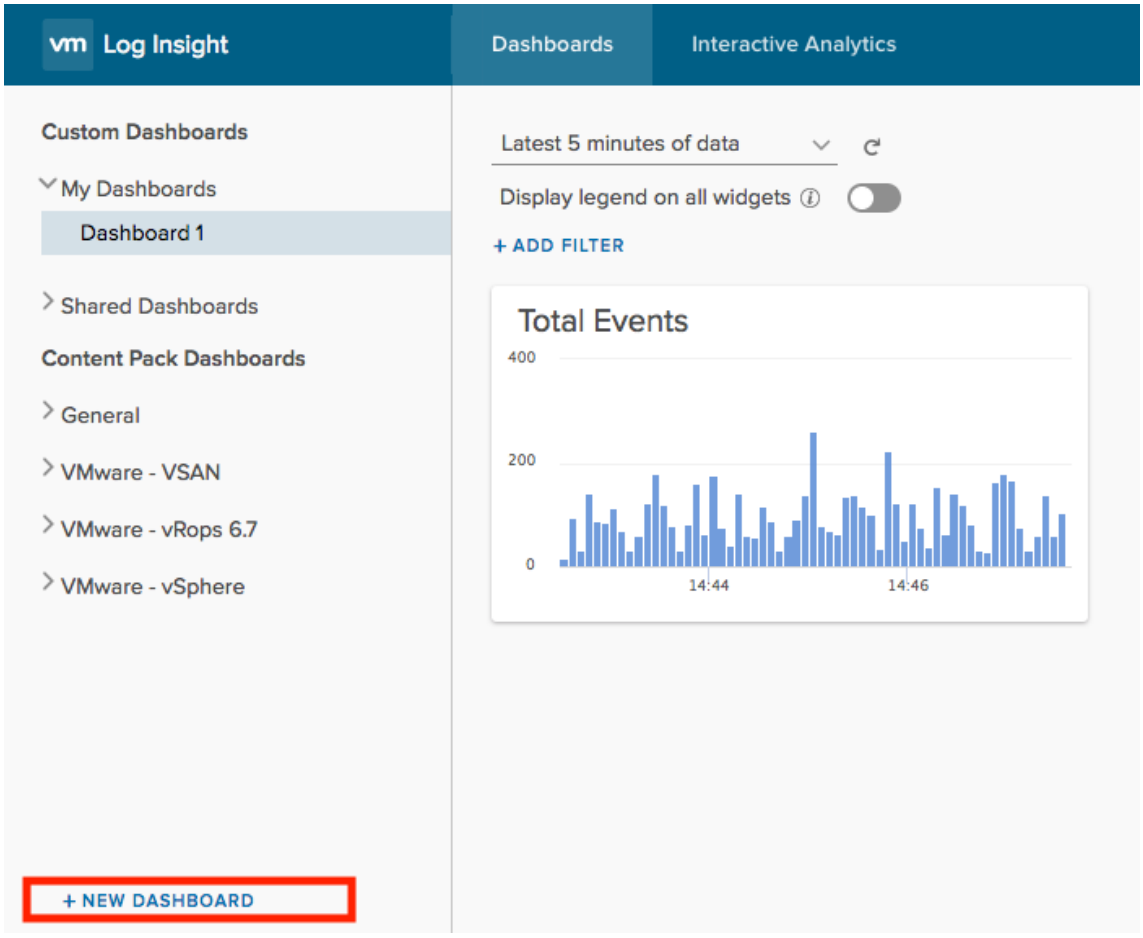
Dashboards



The view in the example shows the vSphere, General Content, vSAN, vROPs Content Packs, all of which are pre-installed within Log Insight. Each dashboard included in a Content Pack shows a different set of charts highlighting information and problem areas within the log data ingested from the source.

1. Click **My Dashboards**.
2. The Select **Dashboard 1**.

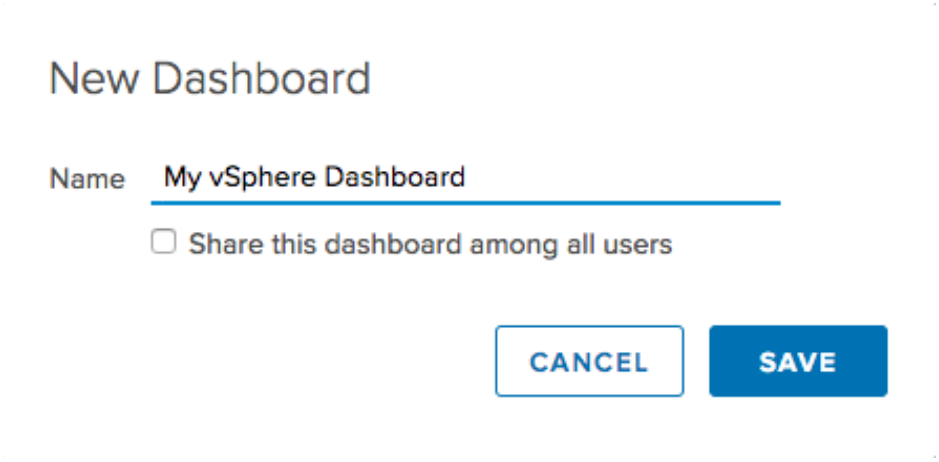
My Dashboards



My Dashboards includes dashboards that have been created by cloning existing dashboards or created from within Interactive Analytics. In this example, the dashboard includes widgets created from queries in Interactive Analytics and cloned from the vSphere Content Pack.

Click **New Dashboard**.

New Dashboard

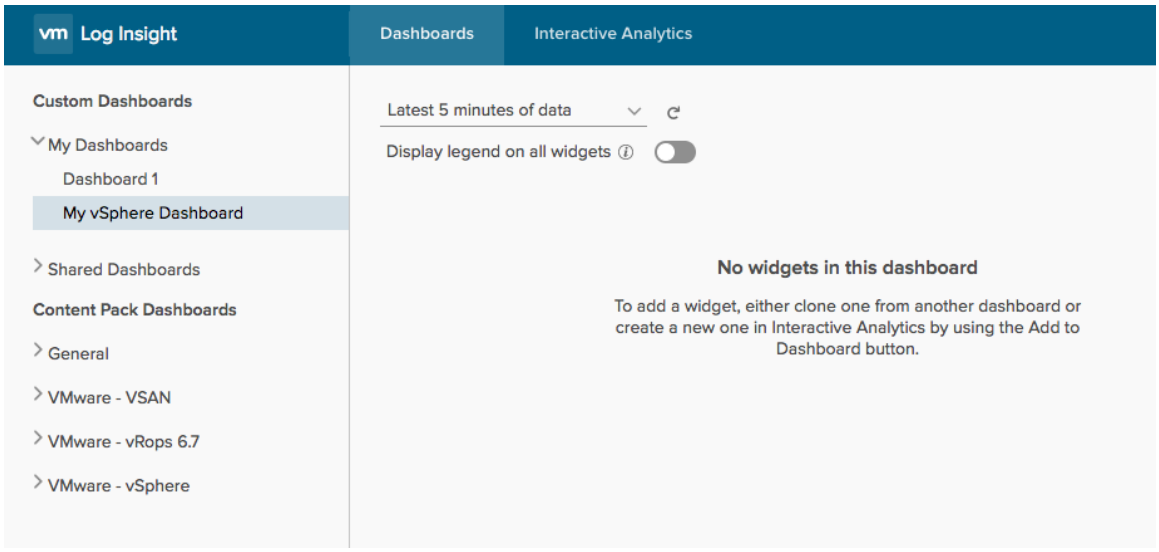


1. Name the dashboard.

2. Click Save

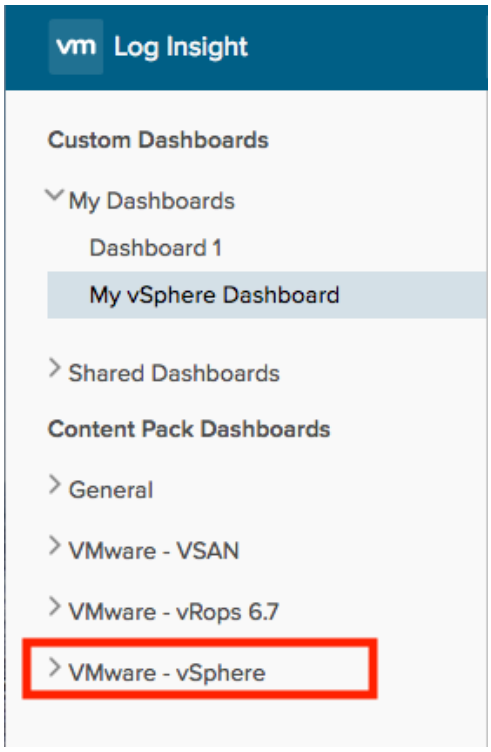
(**Note:** You can also share this dashboard, if you are a Log Insight administrator, by selecting the **Share this dashboard among all users** checkbox.

View the New Dashboard



The new dashboard is blank. Widgets will be added as we move through the evaluation.

Select the vSphere Content Pack



1. Select the **VMware - vSphere Content Pack Dashboard**.

The vSphere Content Pack

- VMware - vSphere
  - General - Overview
  - General - Problems
  - General - Performance
  - General - Licensing
  - General - Inventory
  - Security - Auditing
  - Security - Authentication
  - vCenter Server - Overview
  - vCenter Server - Events
  - vCenter Server - Tasks
  - vCenter Server - Alarms
  - vCenter Server - Reconfigurations
  - vCenter Server - Performance
  - vSphere - Overview
  - vSphere - DRS
  - vSphere - HA
  - vSphere - vMotion
  - vSphere - Network
  - vSphere - Replication
  - Storage - Overview
  - Storage - SCSI Latency / Errors
  - Storage - SCSI Sense Codes
  - Storage - VSAN / VVOL
  - Storage - NFS
  - Virtual Machine - Overview
  - Virtual Machine - Snapshots

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

The vSphere Content Pack includes different dashboards that provide details on log data pertaining to different types of events. The dashboards focus on high level overview information through specific events such as DRS/HA, vMotion, Security, and Performance. The Content Pack aggregates and displays correlated log data from across a vSphere environment. This capability allows you to quickly view where trouble areas are in the environment then view the logs to find possible correlations, establish root cause, and resolve the problem.

vSphere Content Pack dashboard summary:

General - Overview - All vSphere events. vSphere warning and error events.

General - Problems - ESXi events, vSphere events by type, hardware events, alarms, DRS and HA events

General - Performance - vCenter performance issues SOAP and Database, VMotion performance, vSphere performance events SCSI latency, VMFS reservations, VM tasks.

General - Security - Failed login attempts to vCenter and ESX, vCenter and ESX authentication events, service enabled events, ESX shell commands

General - Auditing - Audit events by type, ESX firewall changes, Snapshot events, VM events

General - Licensing - vCenter and ESX power on events, vMotion events, Hosts, datacenters, clusters

General - Inventory - Number of vCenter servers, datacenters, clusters, Hosts, datastores, portgroups, VMs, VMs created and deleted

vCenter Server - Events - vCenter events and error events over time, VM events by user, and vCenter system events.

vCenter Server - Tasks - vCenter tasks over time, by type, by user, by VM. ESX tasks.

vCenter Server - Alarms - vCenter server alarms over time, by type, by alarm source.

vCenter Server - Application - VPXD events. SSO events, vSphere client events, CPU utilization by vCenter Server, number of session by username and IP.

vSphere - Overview - VMKwarning events, DRS events, VMkernel events, VMWare HA events, vFlash Read Cache events.

vSphere - ESXi - VOB events, VMkernel events, esxupdate events, ESX events by appname and severity, VMODL events.

vSphere - DRS/HA - DRS executed VMotion events, DRS imbalance by cluster and vCenter, HA failovers, HA heartbeat problems.

vSphere - vMotion - VMotion events, VMotion bandwidth average.

vSphere - Network/Firewall - ESX network events, DVS events, NSX events.

Storage - Overview - VMFS reservation times, storage queries, VMFS heartbeat events.

Storage - SCSI Latency/Errors - Average SCSI latency, SCSI errors by device, hostname, path.

Storage - SCSI Sense Codes - Host-side, device-side, and plugin-side error codes, errors by device and sense data.

Storage - VSAN/VVOL - VSAN events over time, VVOL events over time.

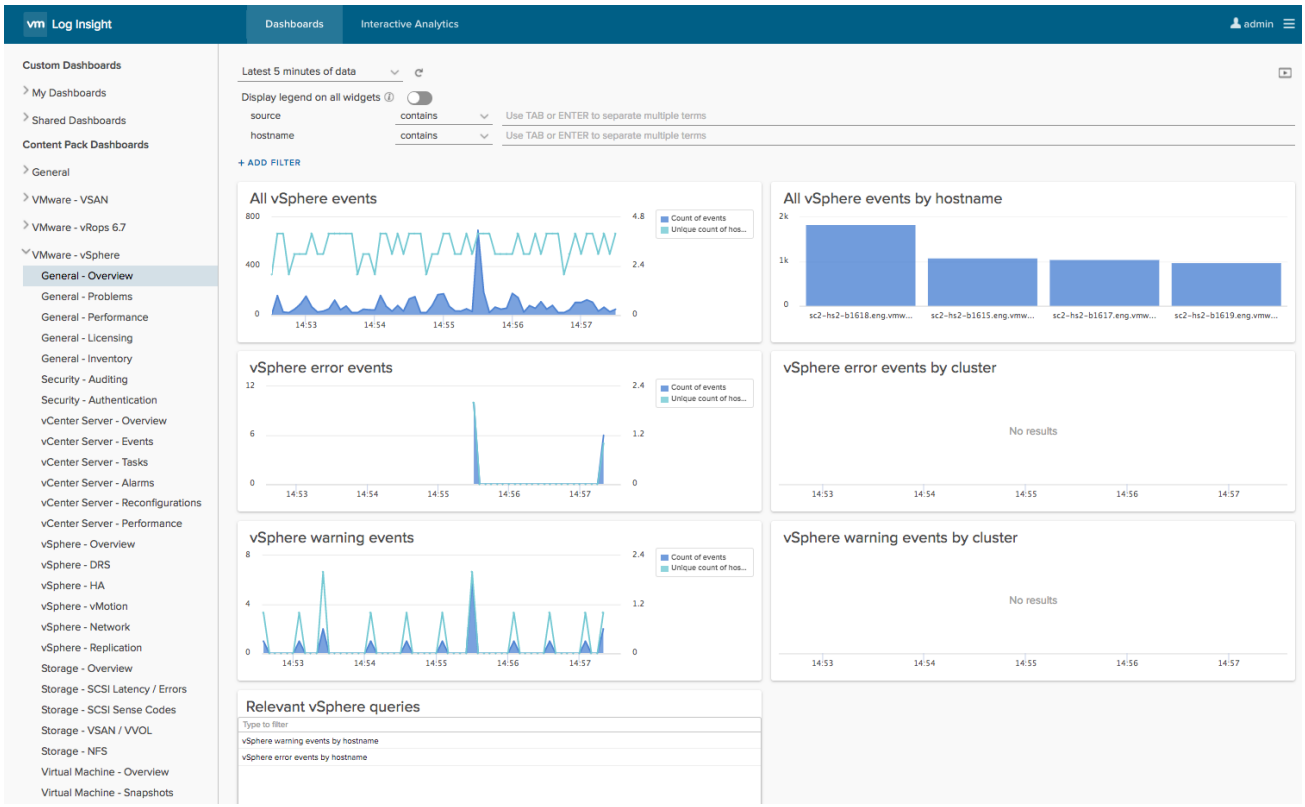
Storage - NFS - NFS events over time, problem events by NFS server, by status, by datastore.

Virtual Machine - Overview - VM events by name, by VM, by type. VM state events.

Virtual Machine - Snapshots - Snapshot errors by event type, by VM and operation.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

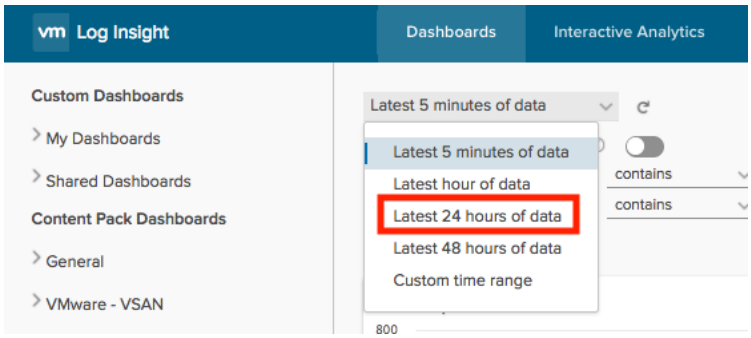
vSphere Content Pack Dashboards



Select the General - Overview Dashboard.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

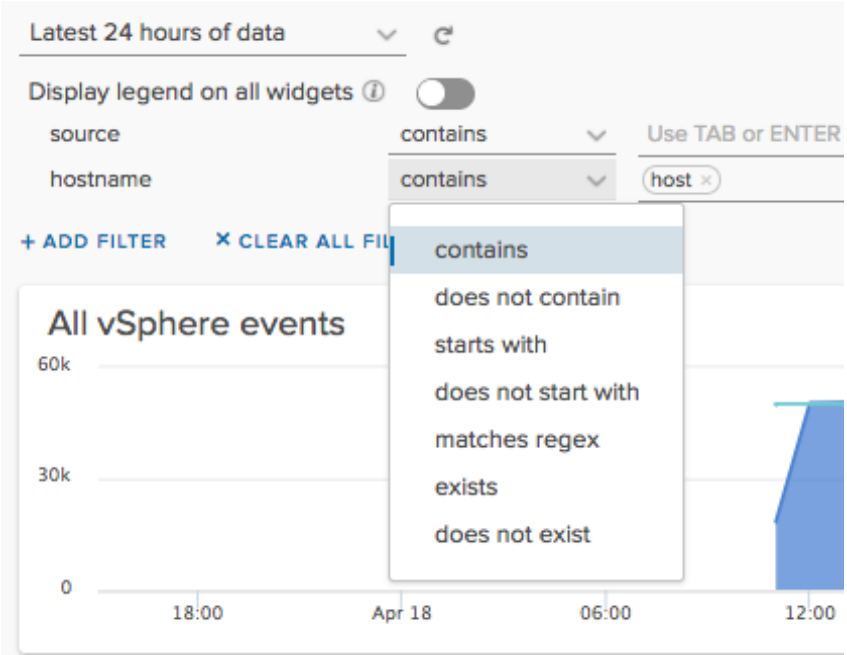
Dashboard Time Range



Dashboard data is partly displayed based on the selected time range. You can select a predefined time range or a **Custom time range**. To use a **Custom time range**, specify a time and date or use **normal language** such as **last 48 hours, last week, or last month**. Only log data with time stamps that are within the time range will be displayed on the dashboards.

1. Click the dropdown menu then choose **Latest 24 hours of data**.

Dashboard Filter



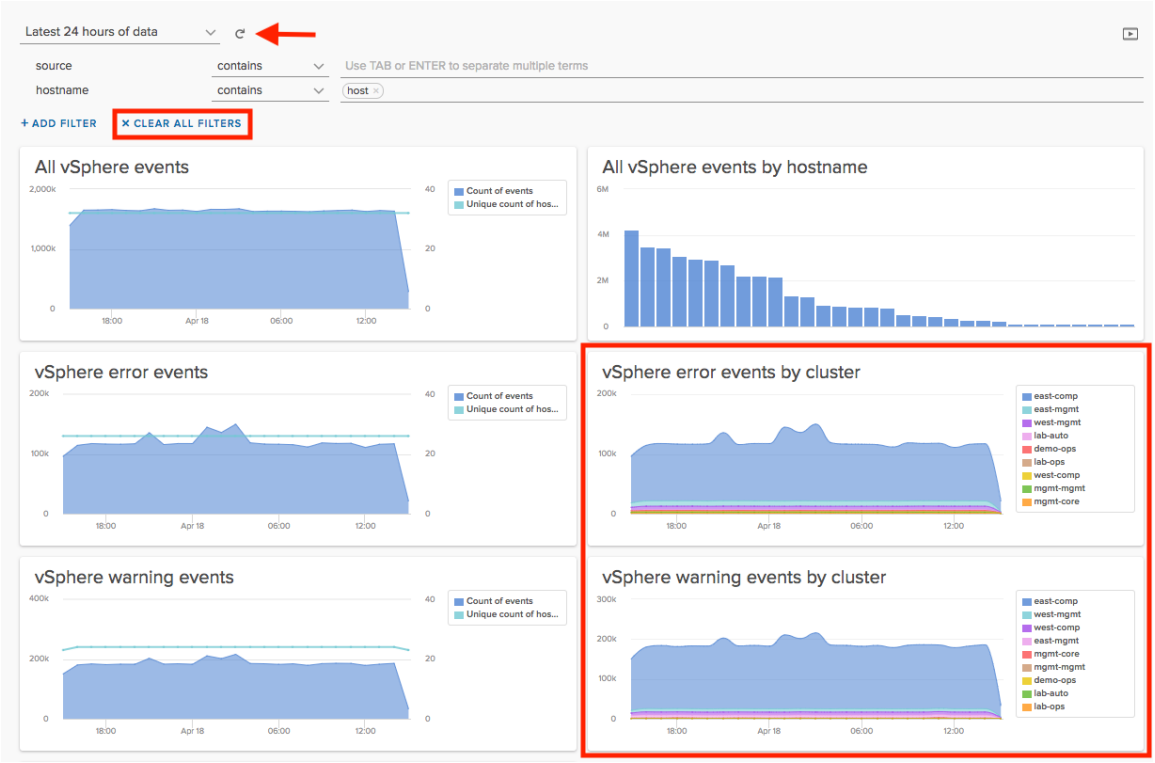
Log Insight allows you to filter the presented view with Dashboard Filters. The default fields are source and hostname. You can create a filter based on any field that has been added by a content pack or manually extracted. In the example, we have listed the name of an ESXi Host within the hostname field. Once the filter is added, the dashboard only shows data from that Host and any related information.

1. To create a filter for a specific Host, **enter the name of an ESXi Host that is forwarding logs to Log Insight, from the evaluation environment, within the hostname field**. Log Insight will autocomplete the field based on matches from the log data.

2. Select the dropdown to choose from a number of operators and change how the filter matches data. The default operator is **contains.**

3. Click **Update** after you have created the desired filter.

Filtered Dashboard Data



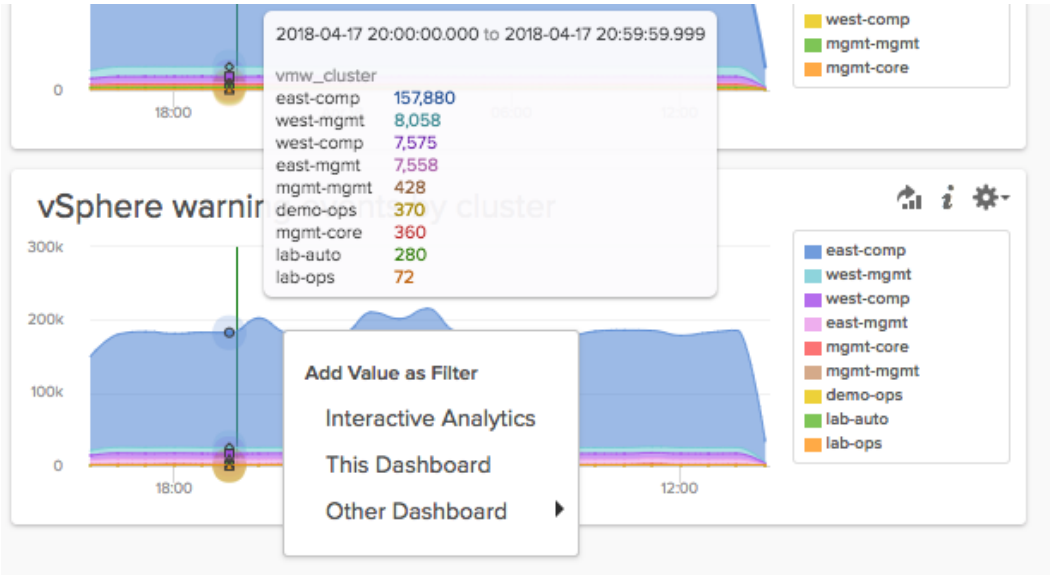
The widget data now only shows visualized log data which contains the word Host in the hostname field.

1. Notice that related parent cluster information is also presented. Log Insight presents log data for related objects where relevant in Dashboards or Interactive Analytics. The ability to show related objects can also be controlled via filters and aggregation functions within Dashboards and Interactive Analytics.

2. Click **Clear All Filters**.

3. Click **Update**.

Widget Options



Choose a widget you would like to add to the newly created My vSphere Dashboard. For this example we have chosen the vSphere error events by cluster widget. This widget groups error events by cluster objects.

1. Hovering over the chart you can see a window appears with further information about the data in the chart. In this case a color-coded reference to the number of error events over a week period for each cluster. The legend on the right shows the cluster and associated color.

2. Click anywhere within the chart data to open the **Add Value as Filter** menu. You can add a filter based on where you have clicked on the chart. For example, if we click on the green portion of the chart in this example, and select **This Dashboard**, the filter **vmw_cluster contains east-comp** will be added to the dashboard filter above. Additionally you can click **Interactive Analytics** to open into that interface with query and filter information added for you. Finally, widgets can link to other widgets. Clicking Other Dashboard, also known as **dashboard linking**, brings up a list of dashboards to further refine how a set of logs are viewed.

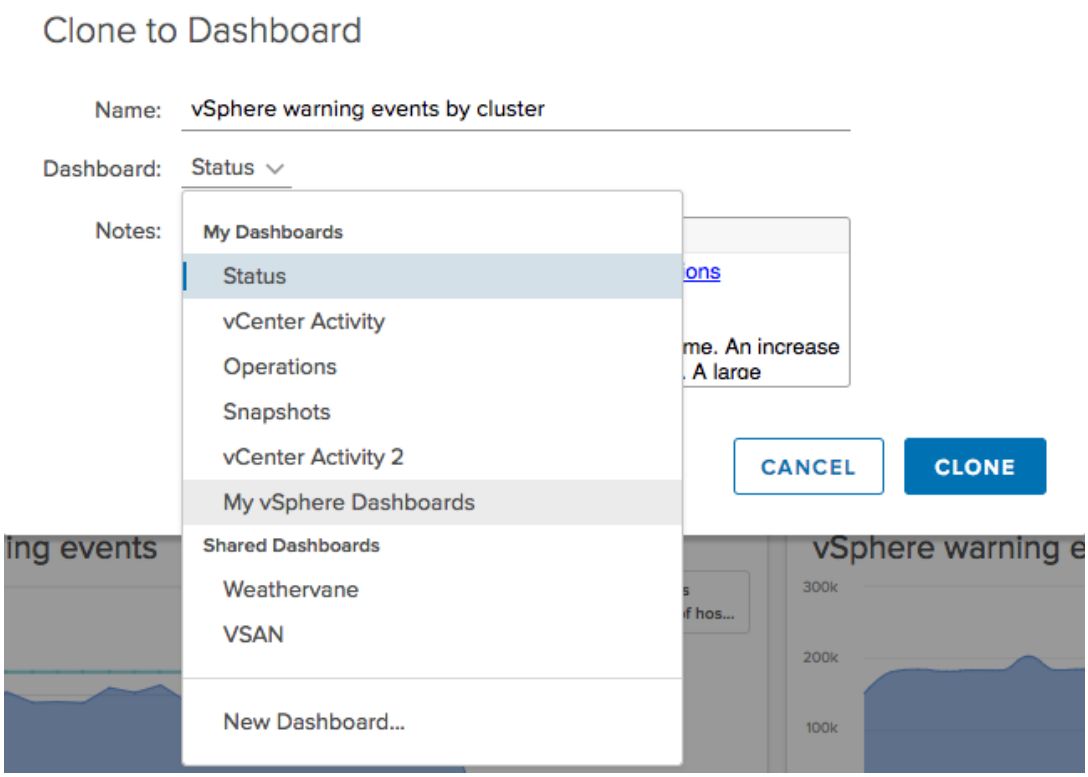
A good example of **dashboard linking** is the **All vSphere events by hostname widget in the vSphere Content Pack General - Overview dashboard**. Selecting Other Dashboard on that widget will bring up a list of dashboards containing specific info or problem areas in the Content Pack for a selected Host.

3. Hover over the magnifying glass with your mouse. Selecting this icon transitions to Interactive Analytics with widget query and filters added for you. This option differs from the **Add Value as Filter** menu by using the overall widget query.

4. Click the ***i*** *to learn about a widget, including important configuration information and how to interpret the widget data.*

*5. Click the **Gear** and select **Clone**.*

Clone a Widget



1. Name your widget or use the default name.

2. Choose the **dashboard you previously created** - in this example **My vSphere Dashboards**.

The widget's original notes will be added to the cloned widget. You can also add your own notes, including links to external websites. Adding notes helps other Log Insight users understand the context or intended purpose of the widget data.

3. Click **Clone**.

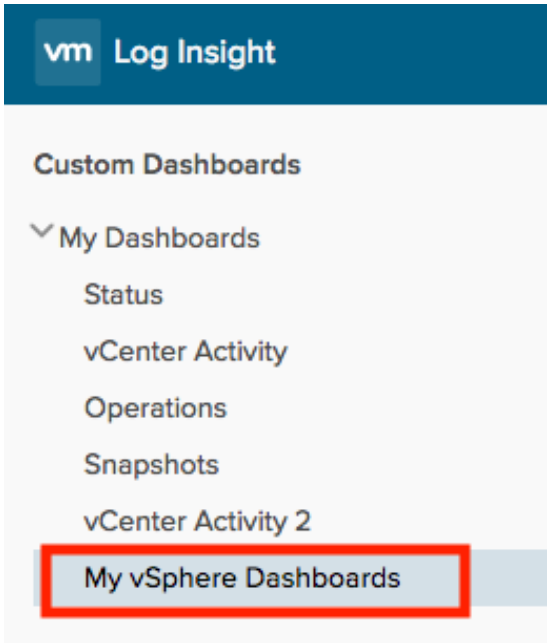
4. Choose **two additional widgets** and clone them to your My vSphere Dashboard

To clone an entire dashboard, hover your mouse cursor over the dashboard name on the left side of the interface, a gear will appear. Click the gear and select **Clone**. **The entire dashboard will be cloned to My Dashboards as a new dashboard**.

(**Note:** You cannot modify Content Pack Dashboards or widgets unless they are cloned to a user created dashboard in My Dashboards.)

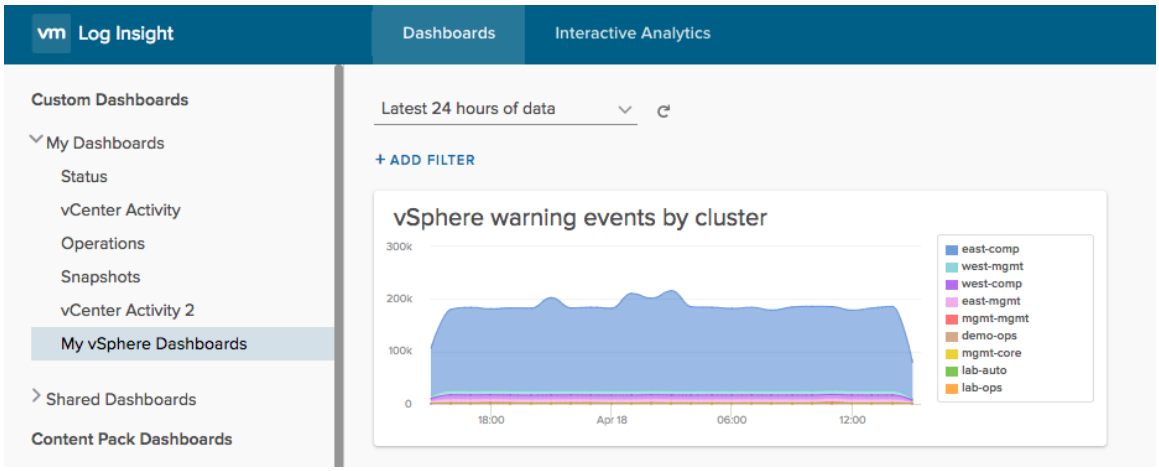
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Navigate to My Dashboards



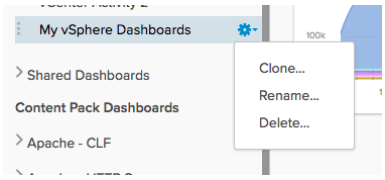
1. Select the **Custom Dashboards**
2. Click **My Dashboards**

View and Modify a Dashboard

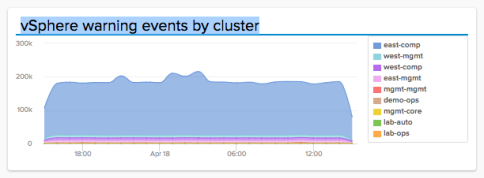


Notice your dashboard now contains a widget.

1. We have the **option to Clone, rename and delete the dashboard**.

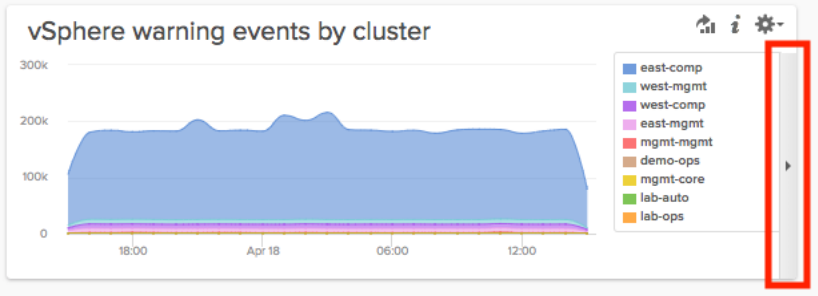
   a. 

2. To rename a widget, click the name and begin typing a new name.

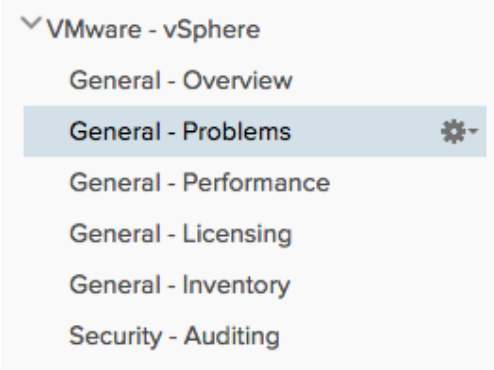
   a. 

3. Move the widget by **hovering the mouse cursor over the widget top bar**, to the right of the name, **click and hold the mouse button on the bar and drag the widget to the desired location**. **Release the mouse button when the widget move is complete**.

4. To expand a widget, and use the entire space, **hover the mouse cursor over the right-side of the widget and click the arrow**. The widget will expand to fill the empty space.

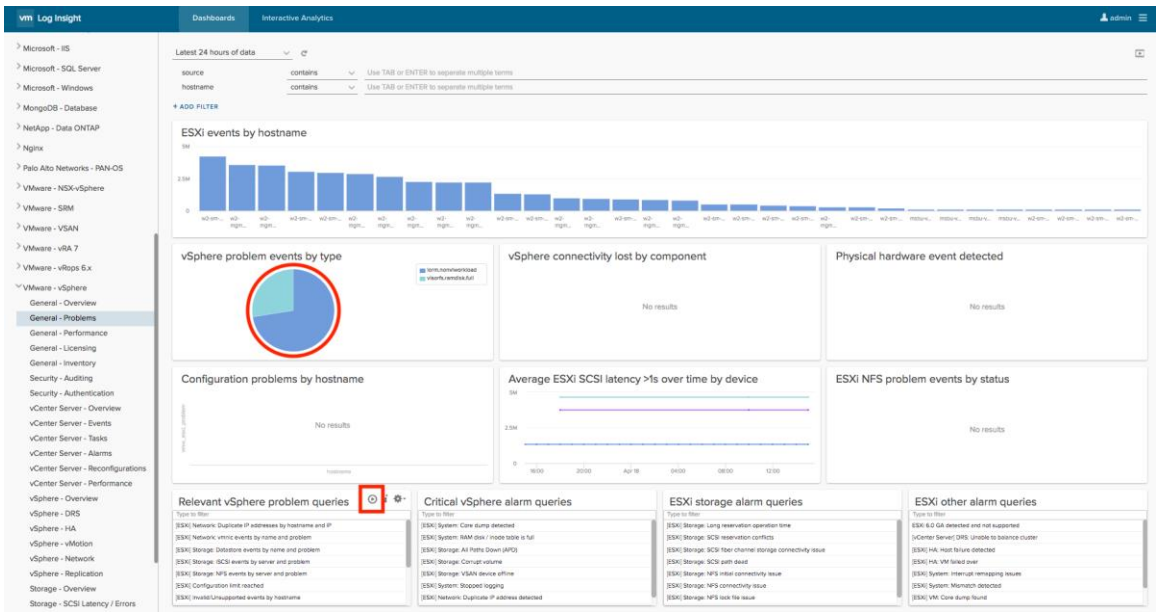
a. 

Problems Dashboard



Select the vSphere Content Pack **General - Problems** dashboard.

vSphere Problem Dashboard



1. Hover your mouse over any of the charts in the dashboard to view the different types of data that are highlighted.

2. Click one of the colors on the legend. Notice that color is now removed from the chart. Each color indicates a different problem event.

3. The run all queries button provides the ability to run a series of queries against the log data. This is known as a query list widget. Typically these queries are used to find problems within the log data. Choose a widget and click the green run button.

(**Note:** You may need to scroll down and try other widgets or increase your time range to find problems.)

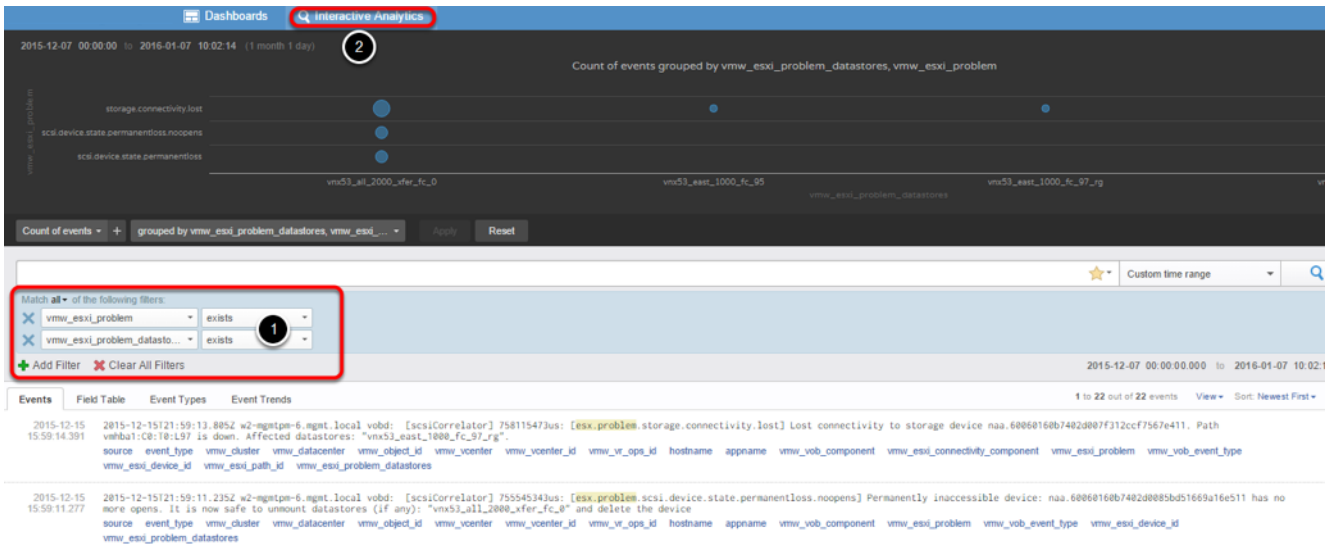
Problem Queries

The query list may run for several minutes depending on the size of your environment and time range. If issues are found in the log data, **Has Results** will be listed.

1. Hover over **Has Results** an **i** will appear. Click the **i** to view notes and a description of the issue the query has found. Once you are done, click **Has Results**.

(**Note:** if you were unable to find any results, click Interactive Analytics on the top bar. In the next step, you will not see the query filter information in the example. Skip #2.)

Datastore Events in Interactive Analytics

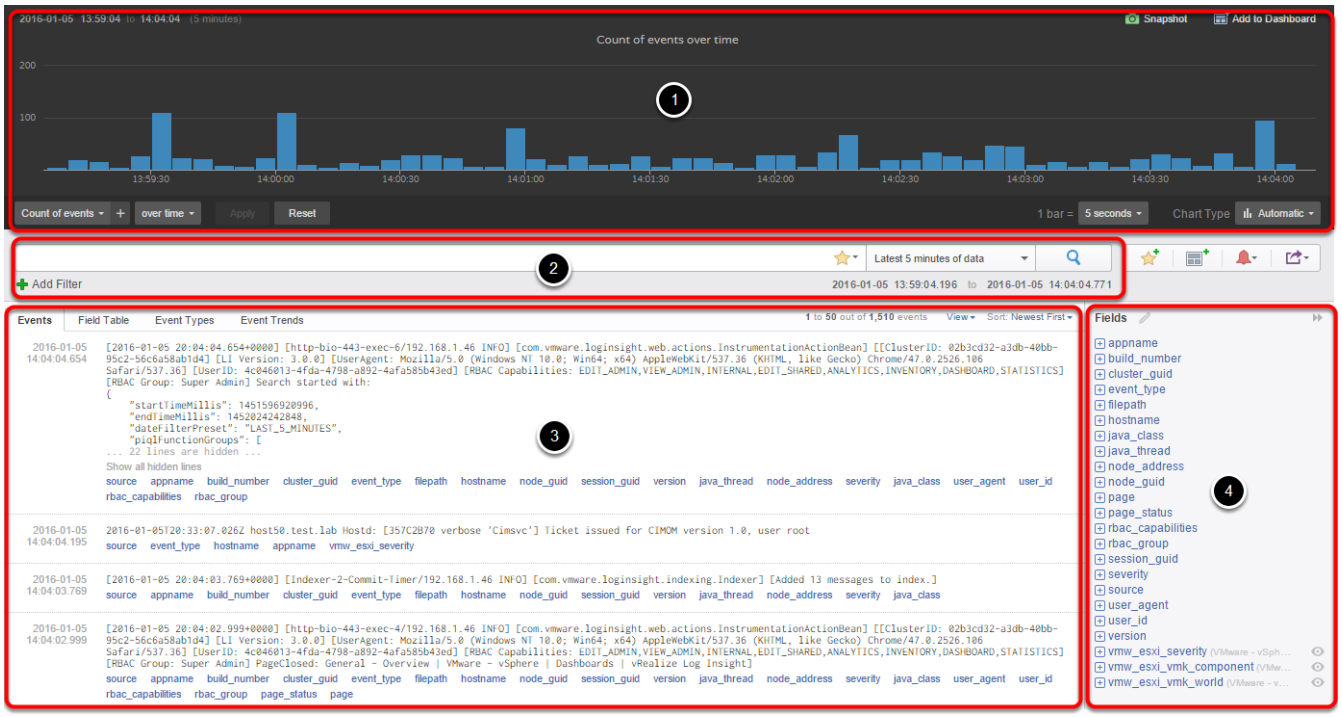


1. We are transitioned to Interactive Analytics with the query filter information and time range already configured.

2. Click the **Interactive Analytics button** at the top of the interface. This will reset the overview chart and query to default.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Interactive Analytics



1. The top of the interactive analytics page displays a visual representation of log data called the overview chart. The overview chart visualizations are based on the chart type, query, and chosen aggregation functions.

2. The search box and query builder help users quickly filter and locate relevant log information. In the previous step we saw that if a user transitions from a widget in the dashboard view, query criteria is automatically entered.

3. The bottom view shows individual log events.

4. Shows fields that are present in the log messages for the specified time range. Fields are regular expressions that are applied to the text of a message. Log Insight extracts a subset of the log data so we can treat that data like a column in a database. This allows unstructured log data to be queried in a similar way to how a database would be queried. The fields pane shows fields which are currently displayed in Events. Fields can be static that are added to the index or manually extracted. These fields could be data extracted or added via agent parsers, Content Pack fields, syslog fields, or manually extracted fields. When you click a field, a mini-chart is

displayed in the field pane. Clicking anywhere within the mini-chart loads it into the overview chart at the top and adds a filter specific to that field.

Events

Ingested log events are displayed within Interactive Analytics. By default all log events are presented when no filters are added.

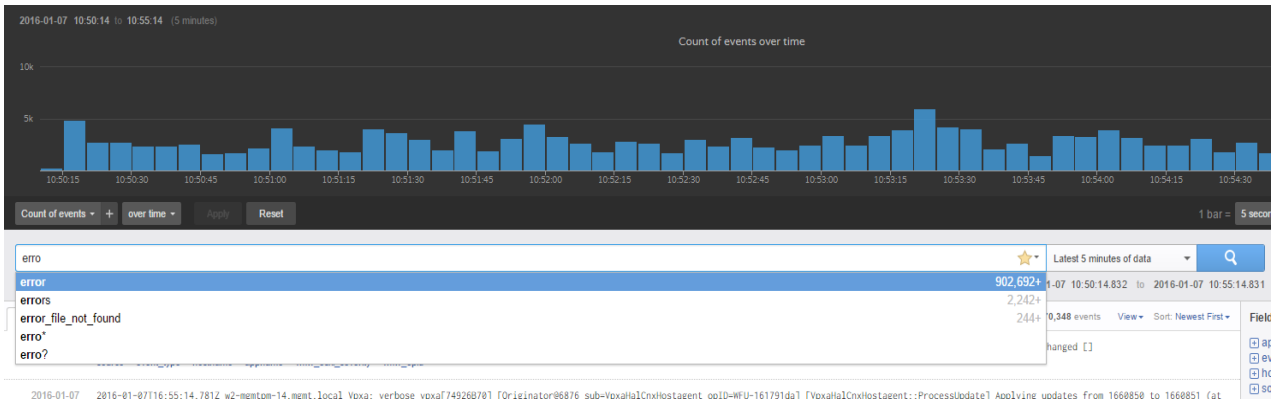
1. Each log message is timestamped on arrival to the Log Insight server.

2. Log messages have associated fields to make queries faster and more efficient. Hostname and appname are examples of Syslog RFC compliant fields.

3. Fields are also added by Content Packs and product integrations. vmw_datacenter, vmw_object_id, and vmw_vcenter are all examples of fields added by VMware integrations. You can create queries based on these fields to help find specific log messages.

(**Note:** Hover your mouse cursor over the fields shown in blue to learn more information about that field. For example, hovering over certain fields will provide further details such as parent or child relationships for a hostname.

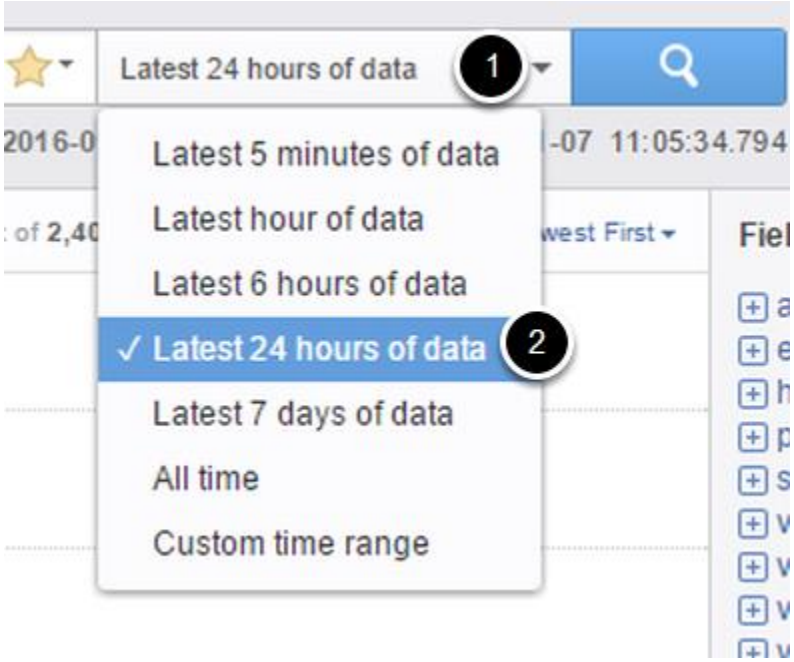
Build a Query



Log Insight allows you to use plain English words when searching for log messages. You can also build queries using regular expression.

Type **error** in the search box. Notice Log Insight will present an autocomplete list based on what you have typed.

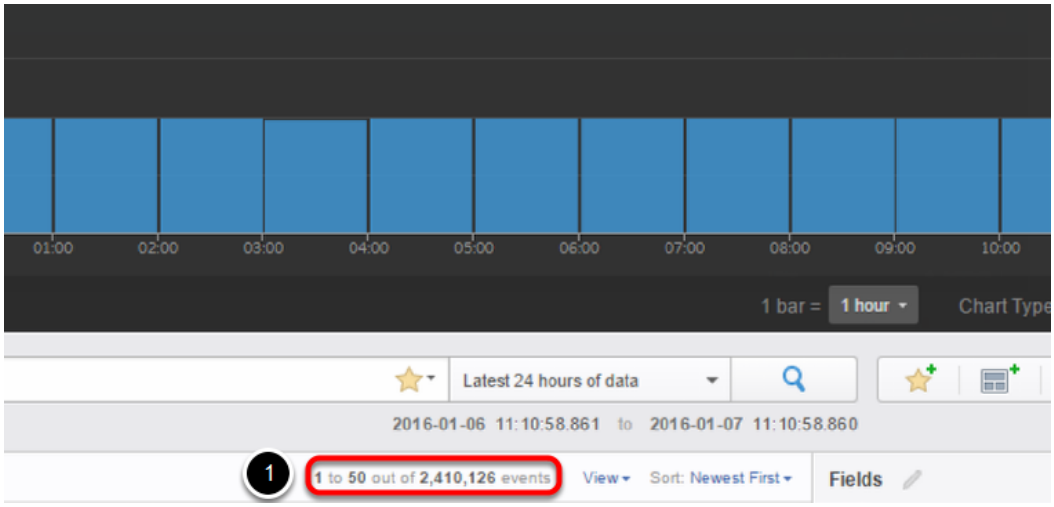
Choose a Time Range



1. Click the time range drop down menu
2. Select the **Latest 24 hours of data**.

(**Note:** The time range menu in Interactive Analytics serves the same function as what was shown in the dashboards portion of this guide. Only log events with time stamps that are within the time range will be displayed. The timezone of the client web browser determines the log messages that are visible.)

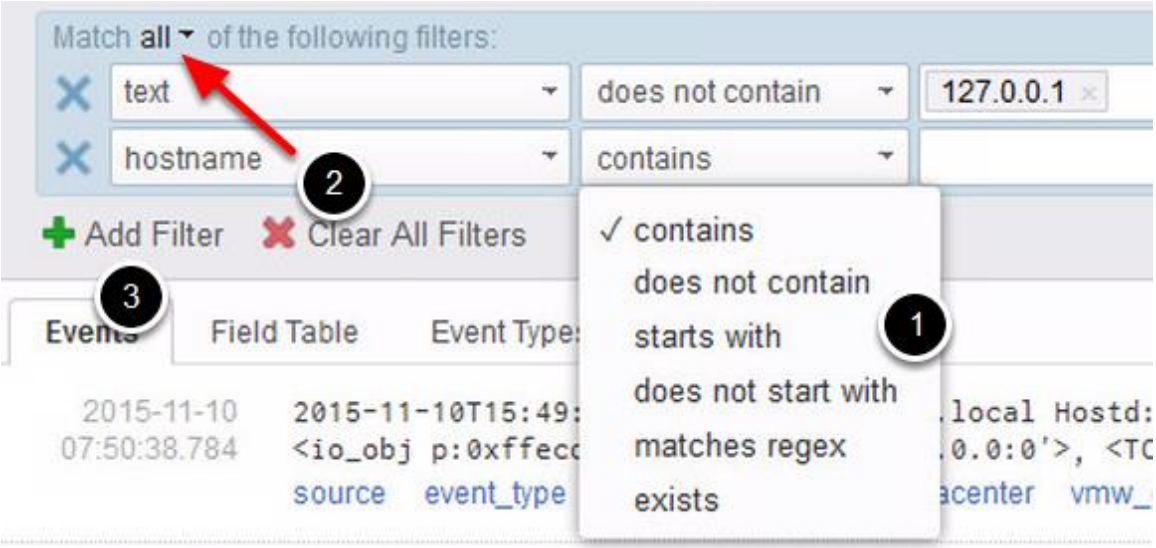
Number of Events



The event list will update showing the last 24 hours of log messages. The word error will be highlighted in each event message to indicate a match. Only log messages including the word **error** will be displayed.

1. The number of pages and events is shown. The word error occurs in many log messages, which is the primary reason we chose the word. Log Insight has found over 2.4 million log events with the word error over the past 24 hours. Log Insight uses numerous methods to help you decrease the number of log events that are displayed. We will cover those methods in the following steps.

Add Filters



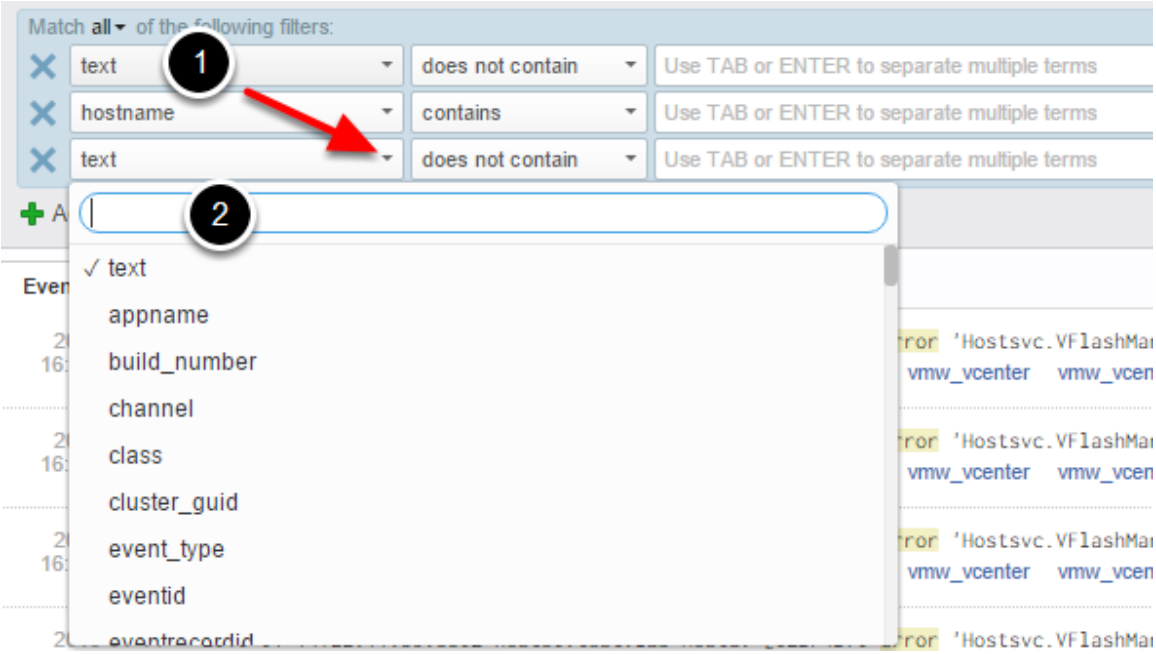
Filters function in the same way as filters with dashboards. Log message results are based on matched values and operators in the filter.

1. Operators control filtering behavior in the same manner as with dashboards. Fields with numeric values, for example latency numbers, include additional operators such as <, >, or =.

2. When two or more filters are created, you are presented with the option to **match all or match any** values in the filters.

3. Click **Add Filter**.

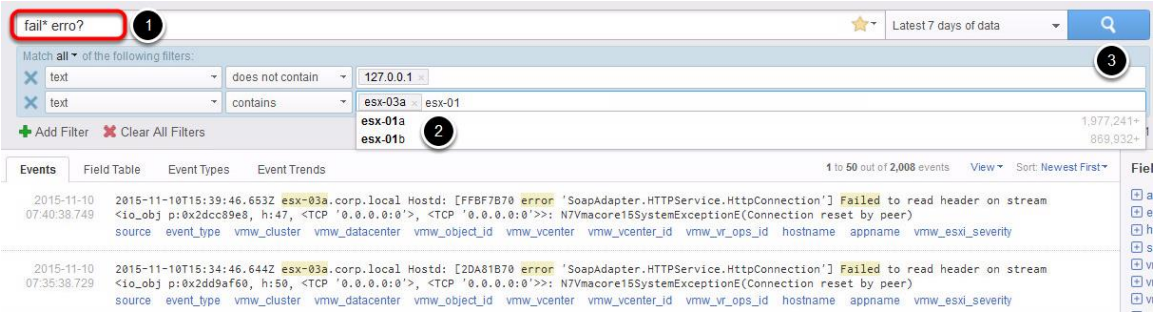
Choosing a Field



1. New filters default to the **text** field. You can choose a new field by selecting the down arrow and scrolling to the desired field.

2. Alternatively you can type the filter into the search box. Log Insight will match results against what you have typed.

Globbing



Log Insight supports using globs in queries.

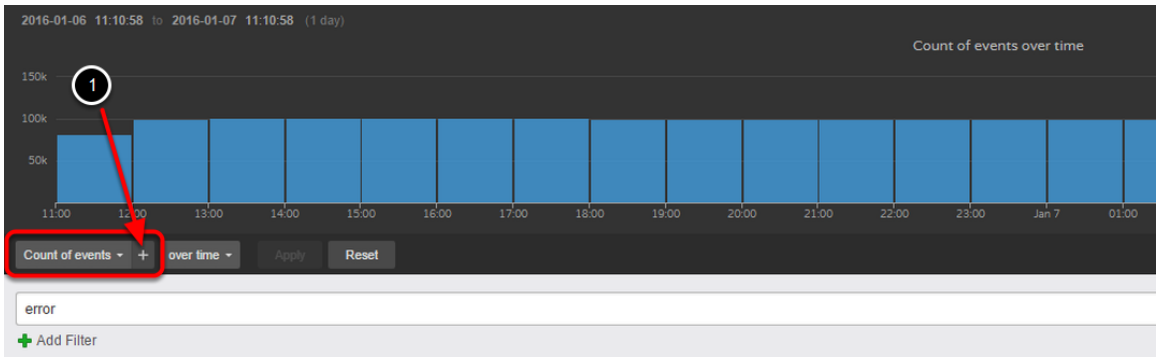
1. The * supports matching multiple characters. The ? only matches one character. In the example, using fail* could return Failed, failure, or failing. Erro? will probably always return the word error.

2. When entering a value, Log Insight will perform a match against what you have typed. Also multiple values for a single filter line will automatically have an OR constraint. The filter above will translate to **text contains esx-03a OR esx-01a** when complete.

3. Try **creating a filter for an ESXi Host in your environment** then click the search button.

(**Note:** Search queries will not work properly if globs are the first character in a word, i.e. *rror. Multiple globs **can** be used such as e*r*.)

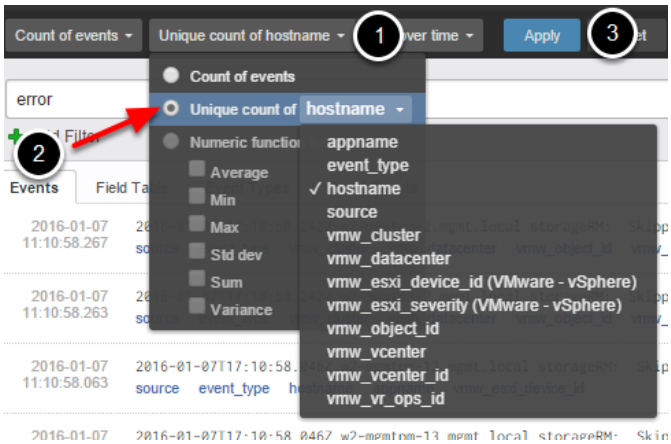
Aggregation Functions



We can also control the data which drives the Overview Chart in Log Insight via aggregation functions. Above the search box, the default aggregation function Count of events over time is presented. Selecting the down arrow will open a drop down menu with additional functions.

1. Click the **+ plus sign**.

Adding a Second Function



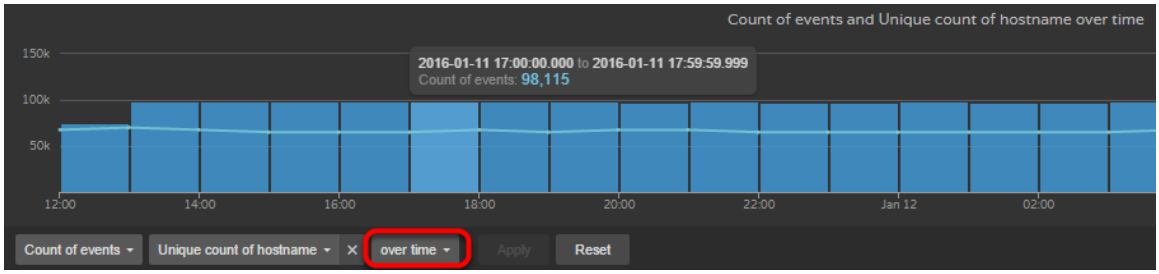
Multiple functions can be added to a chart. This allows you to show a single event in two different ways.

1. Click the down arrow to open the drop down menu.

2. Click the radio button for **Unique count of** and select **hostname**.

3. Click **Apply**.

Multi-function Overview Chart

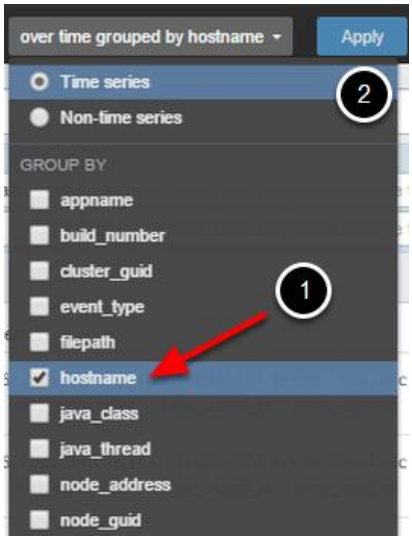


The Overview Chart will update and include the Unique count of hostname in the view as a line.

1. Hover over the column and line. Notice that each will present information. The column will present the count of events for that time frame. The line shows the number of hostnames that had matching error logs during that time frame.

2. Click **over time.**

Overview Chart with Hostname Grouping

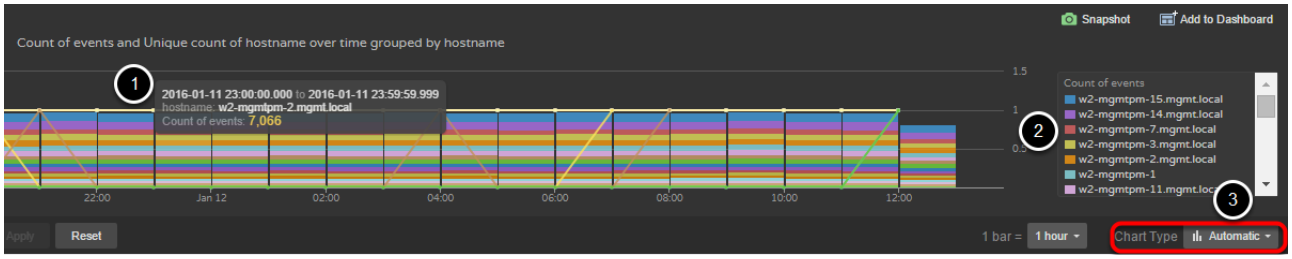


Next we will group the results by hostname.

1. Select the **hostname checkbox**.

2. Click **Apply**.

Overview Chart With Grouped Hostname

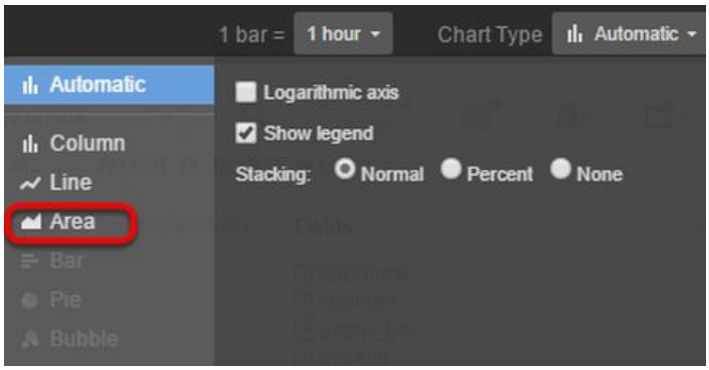


1. Now that events are grouped by hostname, **hover the mouse cursor over the different colors in the columns** on the chart. Information will appear showing the time range and count events for that hostname.

2. The legend on the right shows the color and associated hostname.

3. Click **Chart Type**.

Chart Options

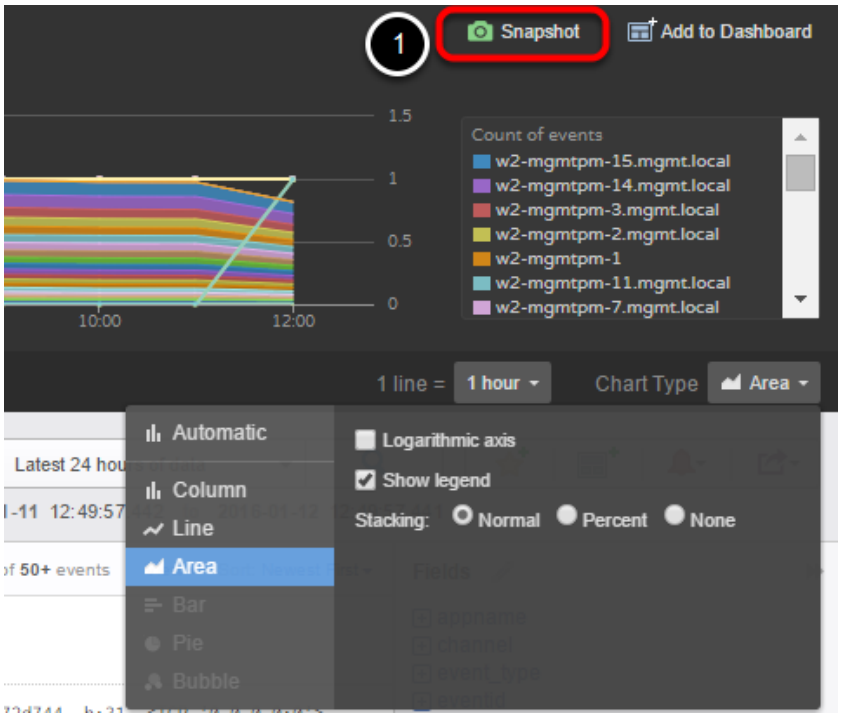


Different charts are also available. By default, Log Insight will automatically select the best chart for the data set. You can manually choose charts to visualize the data in different ways.

1. Choose the **Area chart**.

(**Note:** Some charts like the Bar or Pie chart will be grayed out unless non-time series data is selected. You can change to non-time series data in the group by drop down menu. **Hint** this is where we selected the over time grouped by hostname setting.)

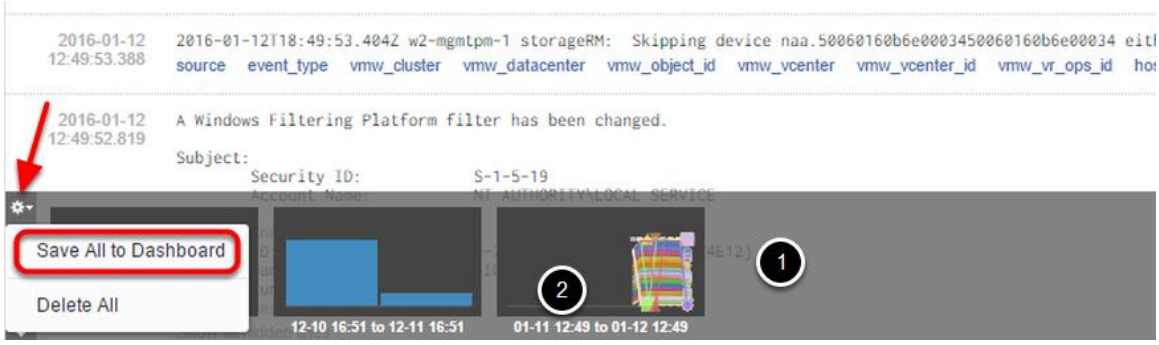
Snapshot the Query



Notice the view changes to an area chart. Experiment with the different charts possibilities before moving forward.

1. Click **Snapshot** once you have finished looking at chart options.

Snapshot Options



As a user is working with a query, they may want to add a field or tweak the query a bit, which could change the visualization. Snapshots allow a user to go back and compare these visualizations side by side. You can take a snapshot of your current query and time range in vRealize Log Insight for quick viewing or to save to a dashboard. Think of snapshots as a visual favorite query. The goal of snapshots is to assist with Root cause analysis and troubleshooting, they are saved between logons, but they are unique to each user account.

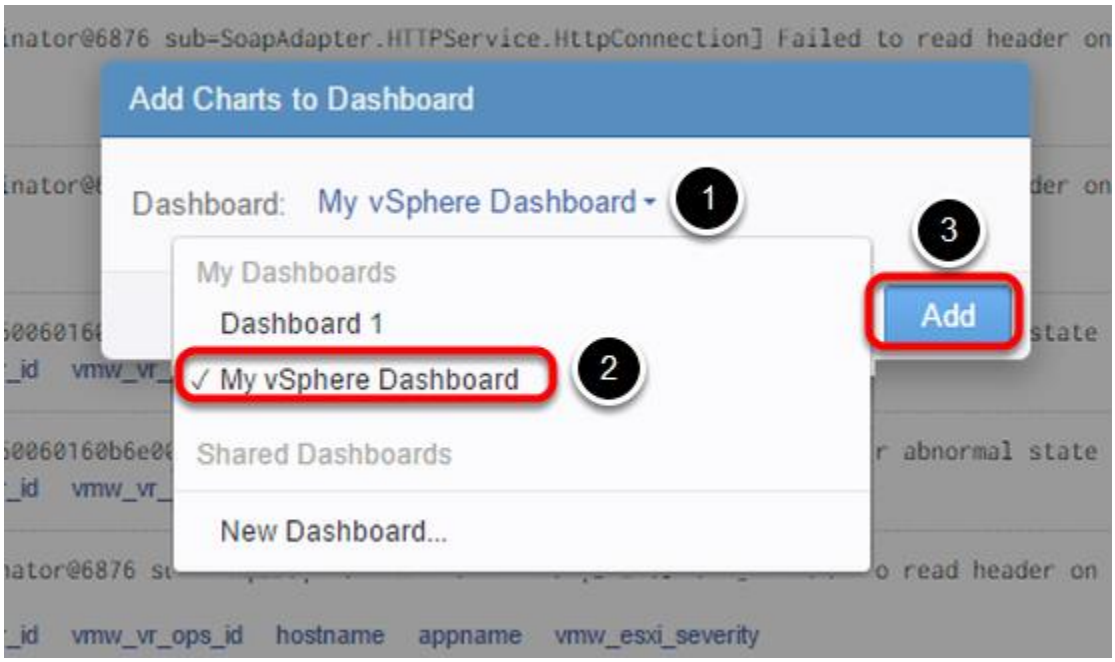
Snapshots appear on the bar at the bottom of Interactive Analytics.

1. Locate your snapshot.

2. Click the **date and time text** along the bottom of your snapshot. Rename the snapshot to something which conveys meaning for the content. For example, you could name the snapshot **Count of Error events grouped by hostname**.

3. Click the gear on the left and select **Save All to Dashboard**.

Add to Dashboard



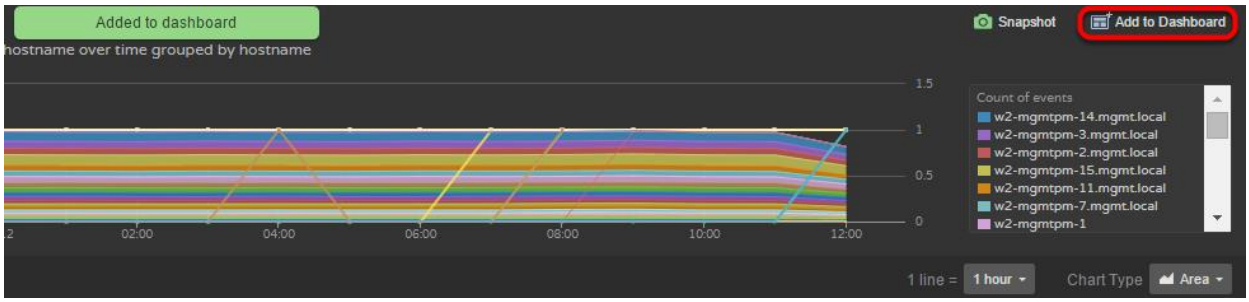
For this step we will add the snapshot to the existing dashboard created earlier.

1. Click the Dashboard drop down.

2. Select **My vSphere Dashboard** (or the name of the dashboard you created.)

3. Click **Add**.

Additional Add to Dashboard Option



Your snapshot has now been added to the dashboard. This functionality allows you to add all current snapshots to an existing or new dashboard.

You can also add the current overview chart to an existing or new dashboard by clicking **Add to Dashboard** on the upper right of Interactive Analytics. This can be accomplished without creating a snapshot.

Events Types

1. Click the **Event Types** tab.

Aggregation Functions and Grouping help to change how much log data we can visualize. As we have seen though, queries will often return thousands to millions of log events in the events list. In these cases, even with filters in place, searching through every log message could present a challenge. Log Insight addresses this issue by intelligently grouping or clustering events into manageable groups. **Event Clustering** is a machine learning technology that groups the related data together. Log Insight detects the types of events, discovers the schema, and automatically understands the structure of each event. We then create **Smart Fields** and pattern match the same event types.

Event clustering allows potentially thousands of events to be grouped and summarized into a smaller set of results within the Event types tab. Event clustering happens at ingestion time to reduce query times and changes to Log Insight data visualizations.

2. In our example, Log Insight has grouped all of the **error** messages into 115 different event types.

3. The most common event types are shown first. The top event type group includes 2.3 million log messages.

4. Click **Expand** to view the log messages included in any group.

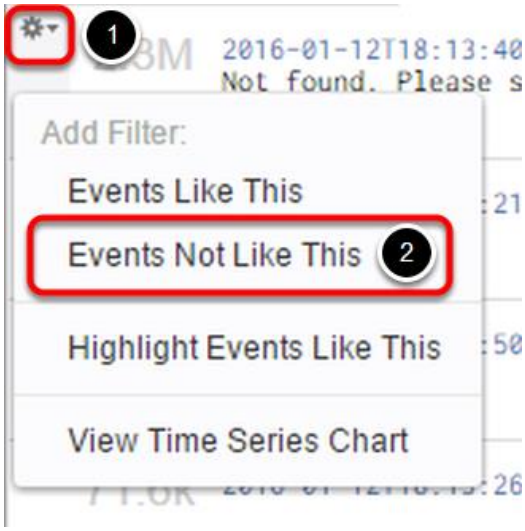
Smart Fields

The group is now expanded. There will be differences in the messages within each log. Although there are differences, intelligent grouping identifies various patterns to differentiate between a constant and a variable within each log message.

1. The variable text, also known as Smart Fields, are shown in blue. In this screenshot, the indicated smart field displays a host, one or more different hosts might be included in this log information and may be different for each log message in the grouping.

2. The text in black represents similar static components of a log message. That portion of a message includes pattern matched log messages, which helps determine how messages will be grouped.

Filter Event Types



1. Hover the mouse cursor over a group and **click the gear that appears** next to a group of event types.

2. Select **Event Not Like This**.

3. Choose another group of event types and select **Events Not Like This** again.

Using this process a Log Insight user can rapidly work through a large number of irrelevant logs to find the important information. This process is also particularly helpful when the user is not sure what to search for in the log data.

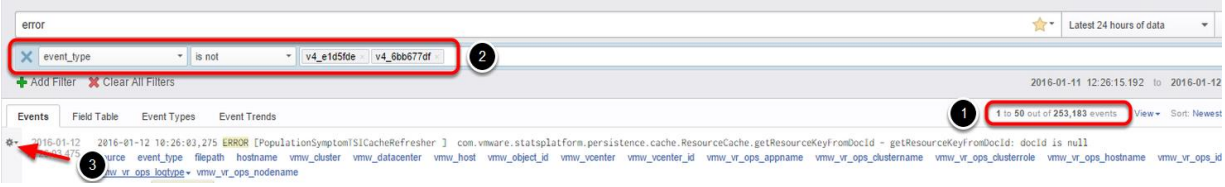
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Event Types Filtered

1. Selecting **Events Not Like This** creates the new filter **event_type is not "event type"**. Had we selected **Events Like This** instead, the filter would have constrained the results only to that event type group

2. Click **Events**.

Events Filtered

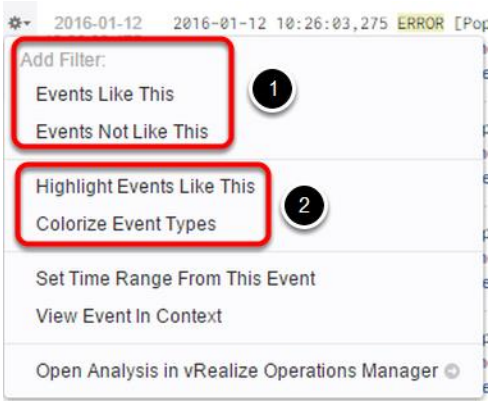


1. Moving back to the Events tab, we quickly see that, with a few simple clicks, most of the log messages are now filtered.

2. The filters have remained in place as we transitioned between tabs.

3. Hover the mouse cursor over a log message and click the **gear** next to a log message. This menu presents further methods to organize log messages.

Highlight and Colorize Events

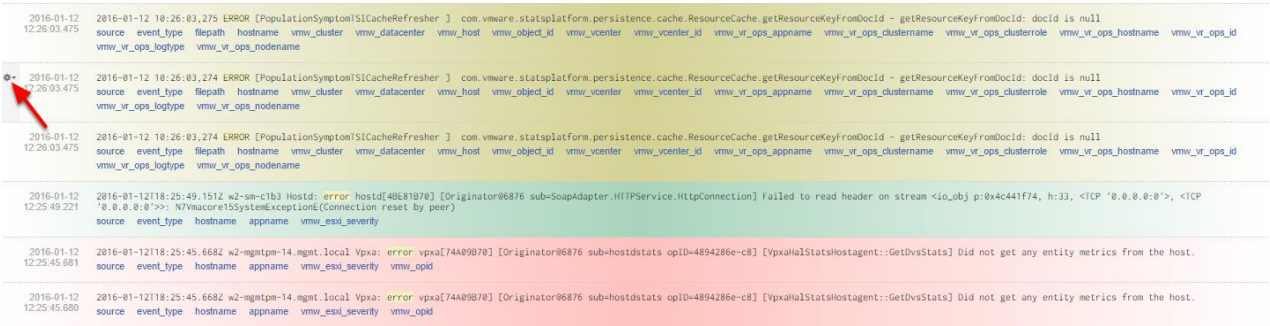


1. Note that you can also add event type filters from the Events Tab as well.

2. In addition to filters we can Highlight and Colorize each event type. **Highlight Events Like This** colorizes a single event type in the list. All events with the same event type will have the same color.

To colorize all messages in the list, click **Colorize Event Types.**

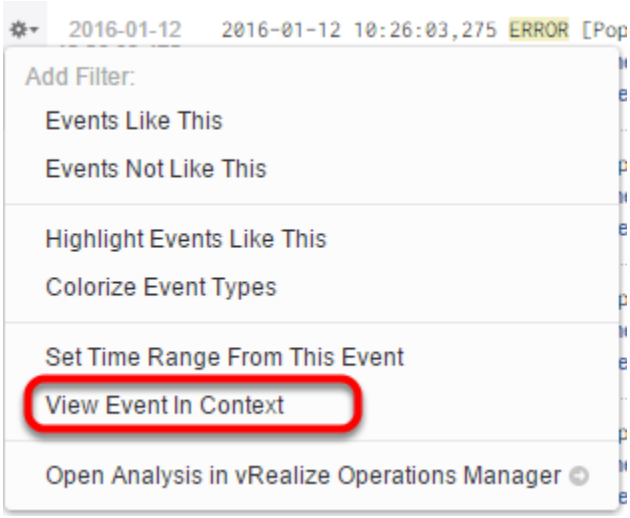
Colorized Events



All events in the list will be colorized according to their event type. This capability allows you to quickly see different event types in context within the message list. You are quickly able to correlate logs in the same time frame to determine if an issue is impacting multiple objects in the environment and where numerous issues might be contributing to a larger problem. Once that information is clear, filters can be added to further refine which log data is relevant to your search and analysis efforts.

Hover the mouse cursor over a log message and click the **Gear** next to any log message.

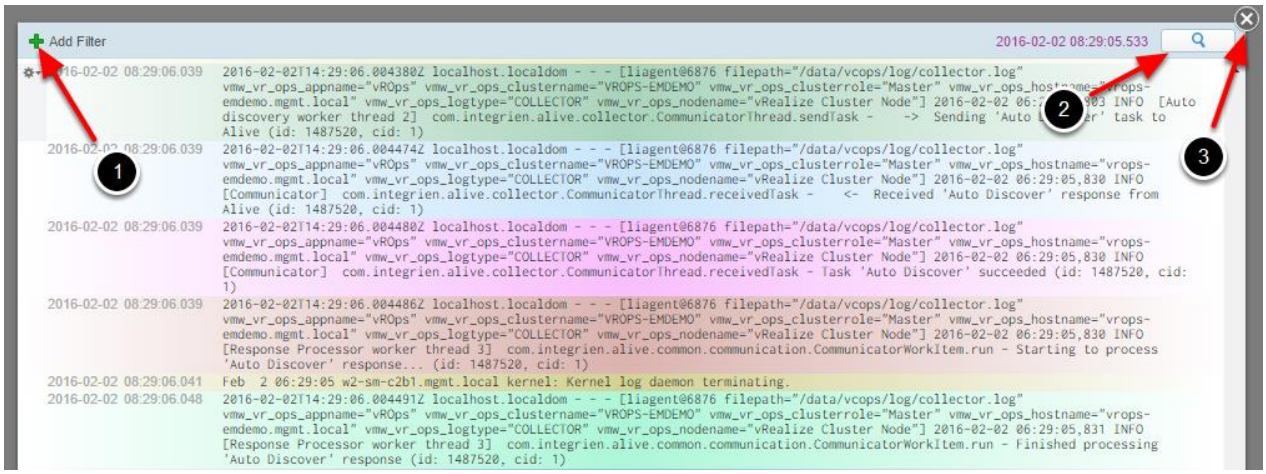
View Event in Context



Log Insight allows you to view log events in real time and in context with other log events. This view can be very helpful if you are attempting to troubleshoot an issue as logs are being ingested.

Click **View Event in Context**

View Event in Context - Continued



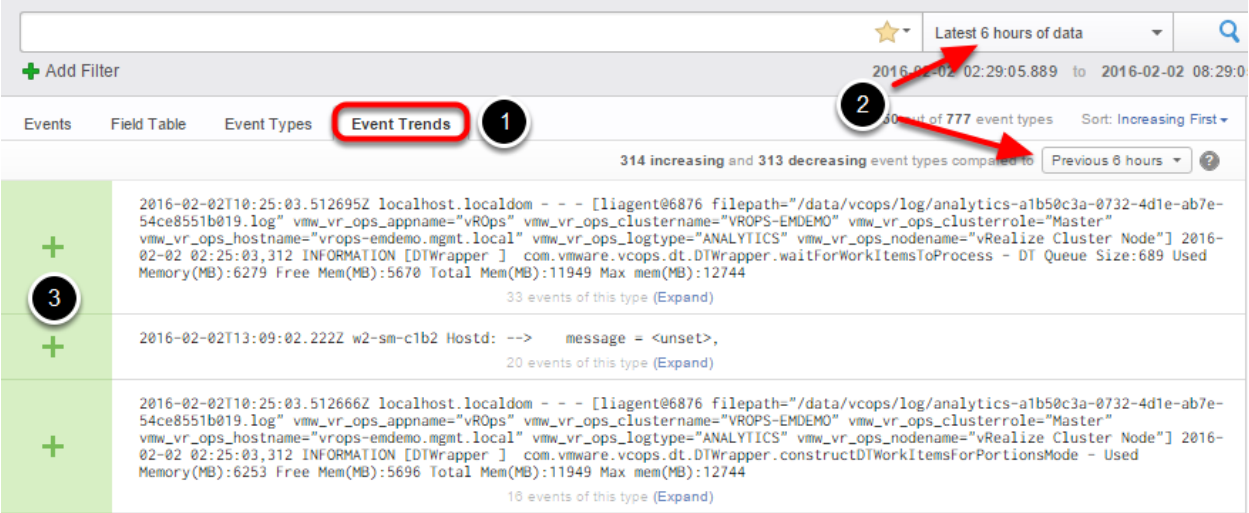
This view provides infinite scroll, simply scroll up or down to view additional log messages. If Highlight or Colorize Event Types was selected, the colorization will persist in this view as well.

1. Filters can be added to constrain visible log messages

2. Searches the log message for filter matches.

3. Scroll through the list of logs and add a filter to get the feel of the interface. Click **X** when you are finished.

Event Trends



1. Click the **Event Trends Tab**.

With Event Trends, you are able to determine if event volumes are changing over time, in other words whether Log Insight is detecting anomalous behavior in the log messages.

2. Log Insight provides a second time range in Event trends. The time range drop down menu controls the previous time frame where event types will be compared. Log Insight then initiates a query to compare events between the two time ranges that have been configured. We determine which events are changing between those time ranges. Log messages are examined to understand the similarity or difference among event types. For example, are we seeing new events types or are there reoccurring event types? Are event types unchanged between the two time ranges?

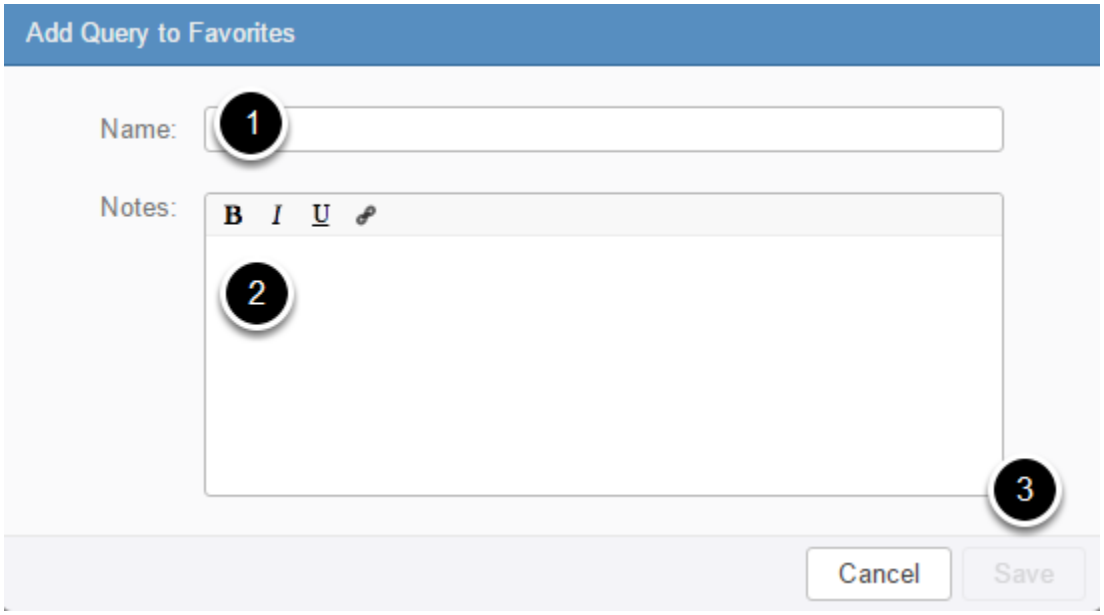
The second time drop down helps correlate events over different time windows. This is a great way to look at specific time windows, for instance looking at the same backup times across different days to view and understand problems or changes which may have occurred during each backup run.

3. **Green, grey, or red badges** indicate how event types are changing. Green indicates an increase in the number of event types, grey means they have remained the same, red tells us they are happening less frequently. An increase in the number of event types might indicate a problem and depending on the issue, might warrant further investigation.

Quick Links

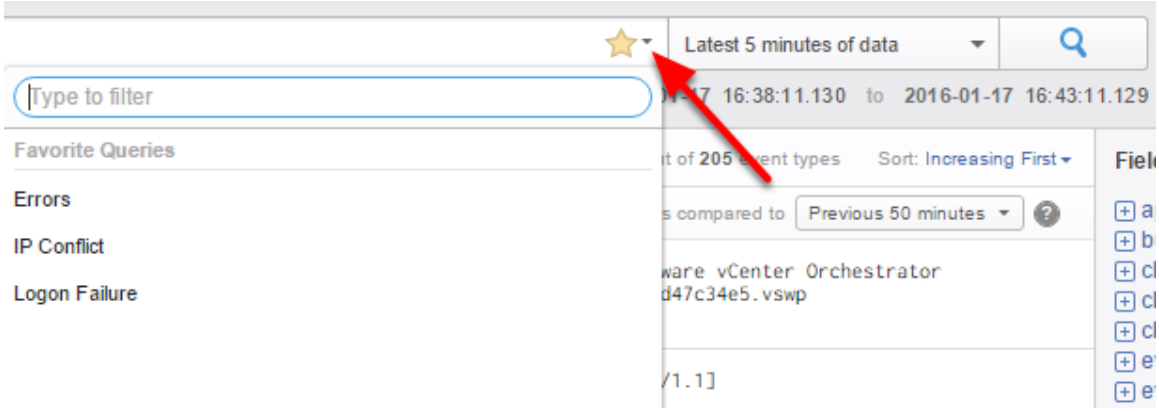
1. Add Current Query to Favorites
2. Add Current Query to Dashboard
3. Create or Manage Alerts
4. Export or Share Current Query

Create Favorite Query



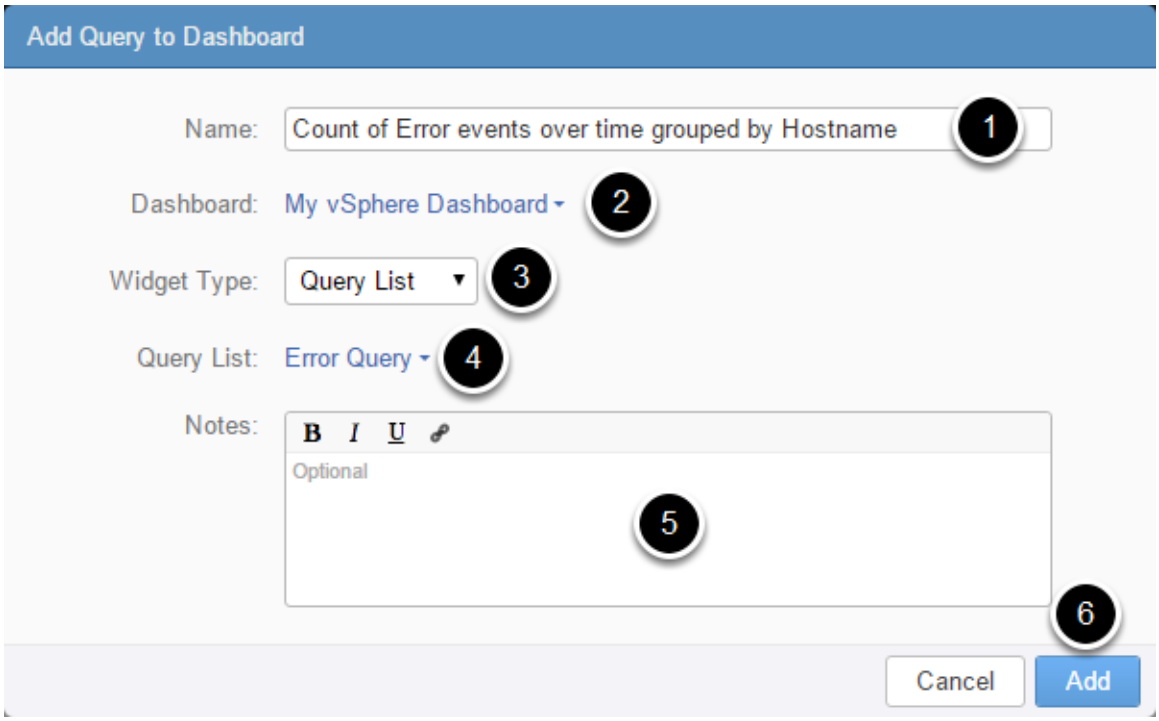
1. Name your query.
2. Add notes for additional information, troubleshooting steps, or Web URLs
3. Click Save when finished.

Favorite Query Location



Click **the favorites button** to view and use favorite queries.

Add Current Query to Dashboard

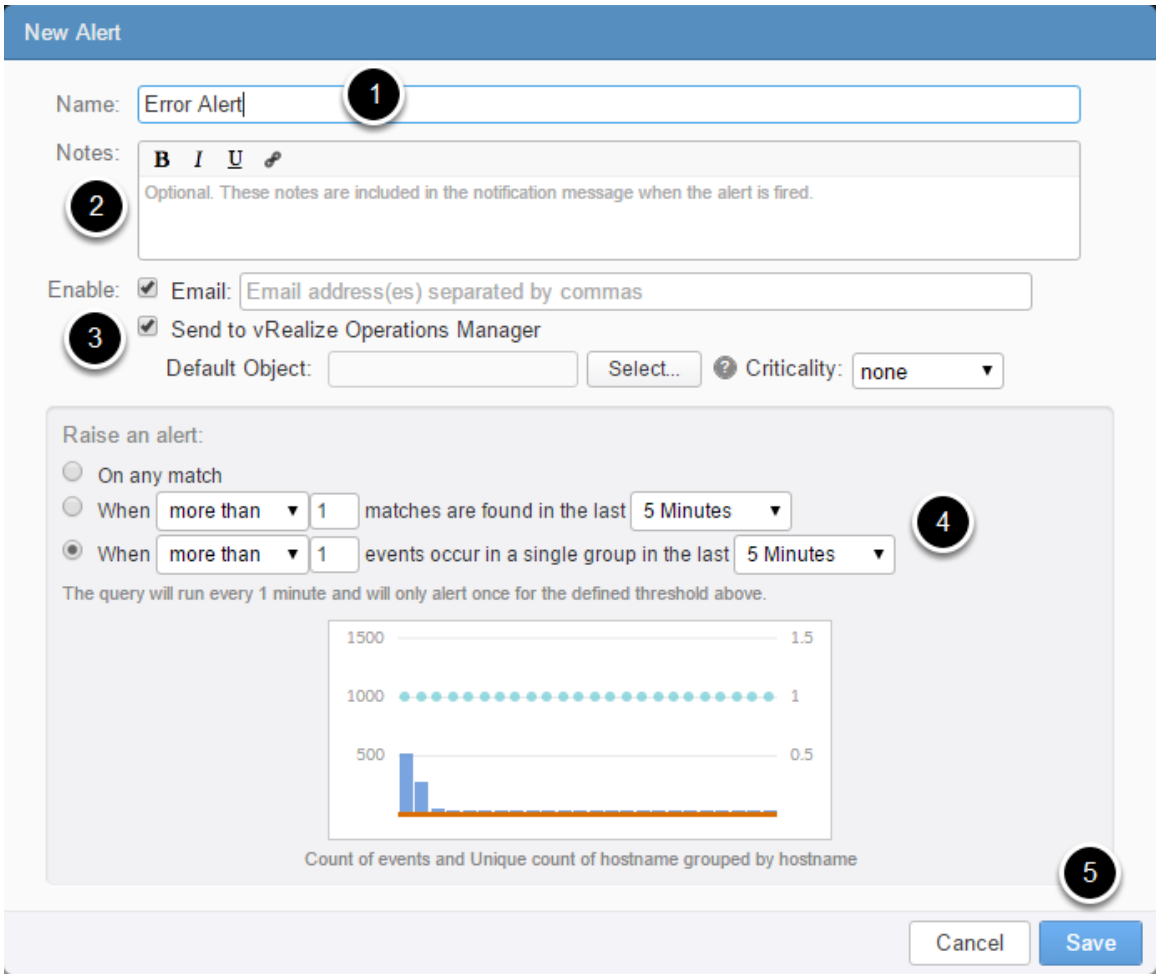


You may also add the current query to a dashboard. The main difference between this option and other options is you can choose the widget type to use with a query. Widget types include, chart, query list, or field table.

Click the Quick Link **Add Current Query to Dashboard**

1. Name your widget.
2. Choose the dashboard you created previously.
3. Click the **Widget Type** drop down and select query list.
4. Name your query - **Error Query**.
5. Notes and Web URL can be added to the widget.
6. Click **Add**.

Create an Alert



Users create alerts from queries or leverage alerts often included with content packs. Notes are useful additions to alerts and allow, for example, context on the alert a knowledge base article or resolution steps for a given issue. Once integration between Log Insight and vRealize Operations Manager is enabled, alerts can be forwarded to vRealize Operations Manager. Alerts are sent to matching objects in the vRealize Operations inventory or the default object, if a match is not found in the log message.

It is important to note that user alerts are separate from system alerts and that admins can only disable all alerts at once not individual user created alerts.

Click the **Create or Manager alerts quick link** and **choose Create Alerts from Query**.

1. Name the alert.

2. Add notes that provide additional detail. The notes will be included in the notification message. Often troubleshooting or resolution steps are included in the notes field.

3. Enable email notifications and/or notifications in vRealize Operations Manager. The vRealize Operations Manager integration must be enabled first. Integration steps are covered in the appendix of this evaluation guide.

4. Choose to Raise an alert at an interval that is appropriate for the issue and your environment. The default settings with the word Error will typically result in a large number of notification messages.

5. Click Save to complete creation of the alert

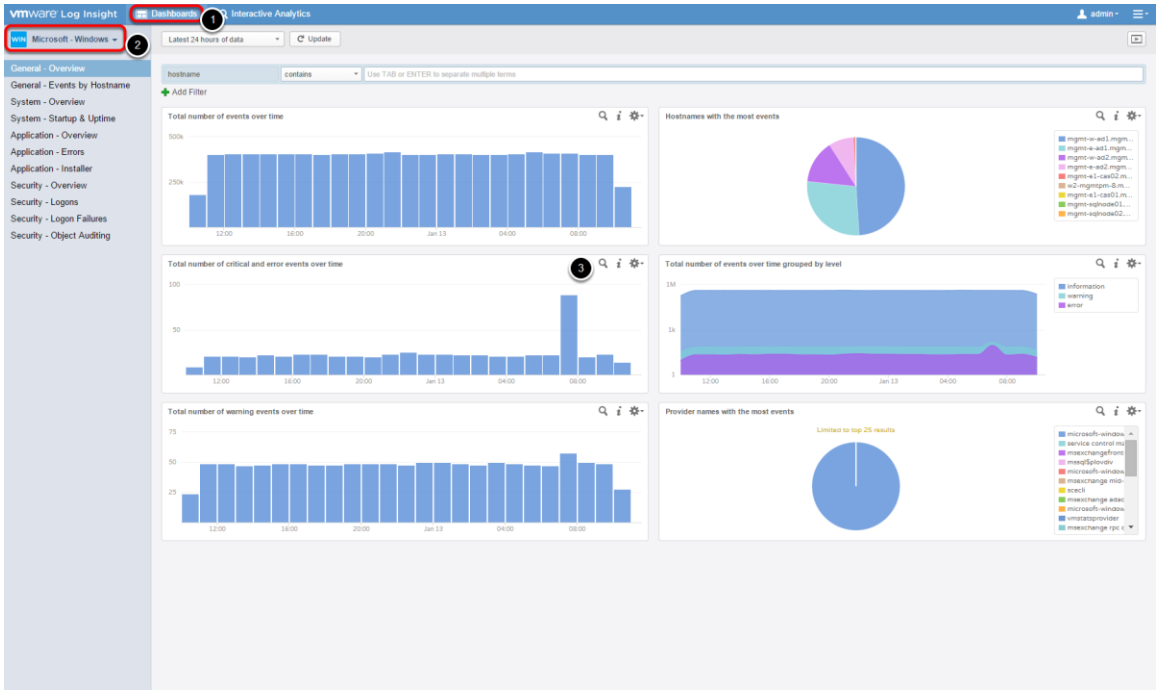
(**Note:** When you click the Create or Manage alerts quick link, you also have the option to manage existing alerts. Alerts that are installed with content packs or previously created user alerts can be modified to suit your needs.)

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Share a Query

Queries can be shared with other Log Insight users. This is particularly useful when a complicated query is created. Click Export or Share a Query. Select Share Query and the a link will be presented that can be shared with other users.

Windows Content Pack



These steps assume the Windows Content Pack and Windows agent was installed after the install and configuration of Log Insight and is not covered in this evaluation guide.

We will navigate back to the Dashboard view and look at the Windows Content Pack Dashboards.

1. Click Dashboards.

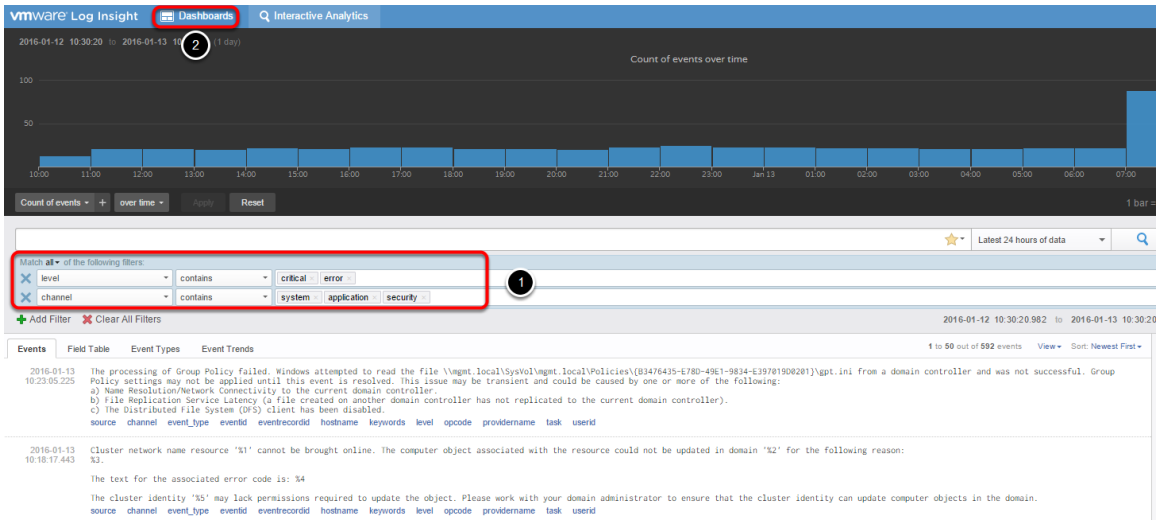
2. Click the Dashboards drop down menu and select the **Microsoft - Windows Content Pack Dashboard**.

Notice the dashboard contains several sections focused on common Windows troubleshooting scenarios. Verify the **General - Overview** dashboard is selected.

3. Examine the widgets in this dashboard. Log events are visualized using different chart options. Click the magnifying glass on the **Total number of critical and error events over time** widget.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

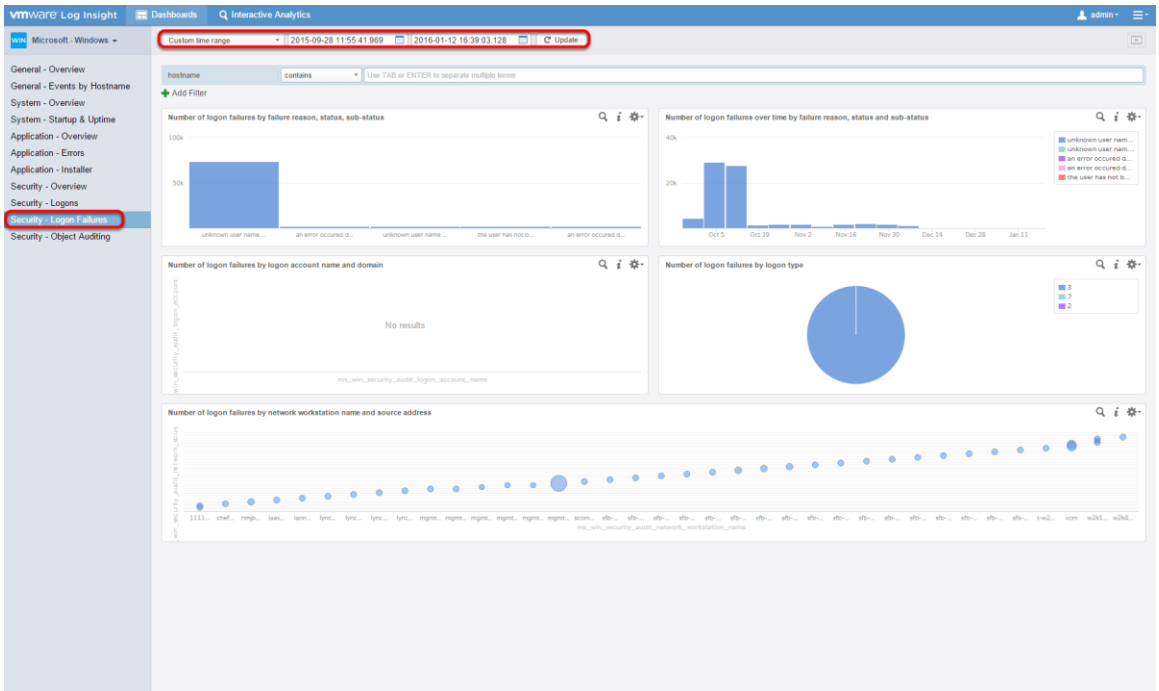
Examine Windows Events in Interactive Analytics



1. Similarly to the vSphere content pack example, we are transitioned to **Interactive Analytics** with the widget's filter information already added. Each field filter pertains to elements of Windows event log channels and issue severity. Browse through the list of log messages to get a feel for the information Log Insight has collected.

2. Click **Dashboards**.

Windows Logon Failures Example



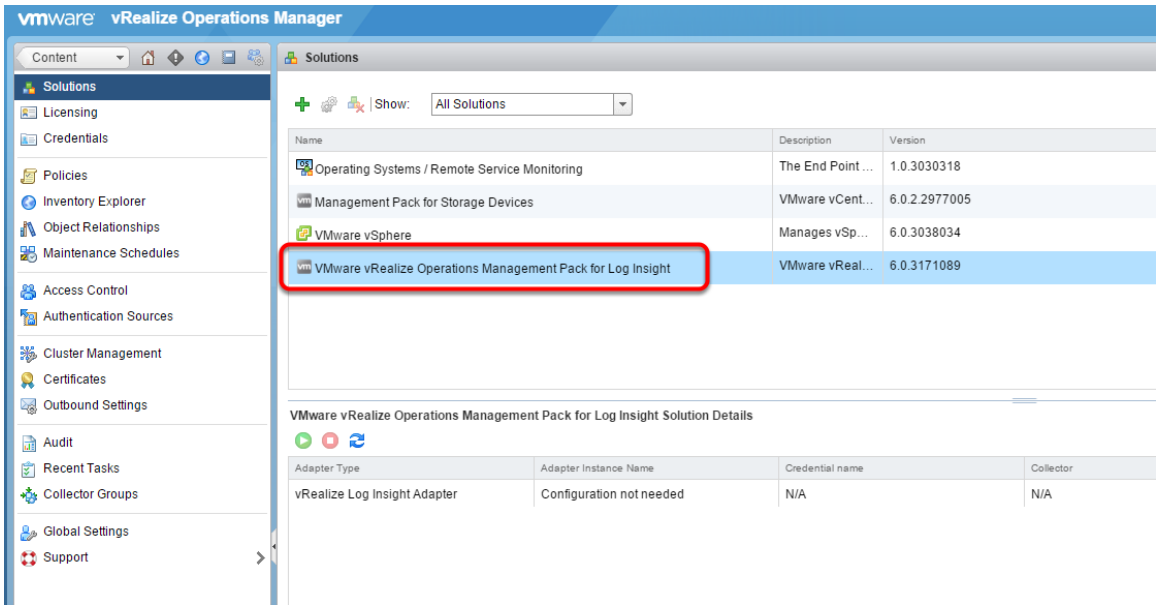
Once you have transitioned back to the **Microsoft - Windows** content pack, click **Security - Logon Failures**.

This dashboard is particularly useful for viewing logon failures within your Windows environment. An **Active Directory** Content Pack is available that offers similar dashboards for logon events.

(**Note:** If you are not finding sufficient log data, in this or other dashboards and queries, remember you can always increase your time range to include additional log messages in the search.)

Appendix

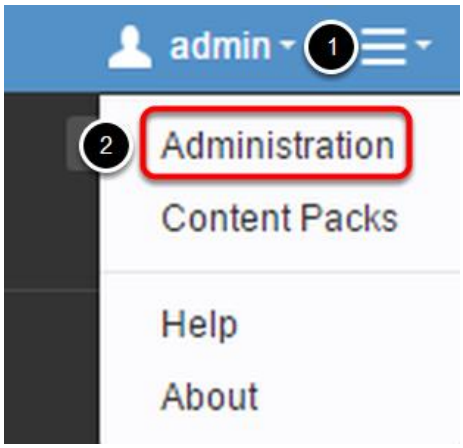
vRealize Operations Integration



[Log Insight Integration with vRealize Operations Manager Overview video]

This portion of the evaluation guide assumes a functioning installation of **vRealize Operations Manager 6.X** is available for the evaluation.

Navigate to Administration

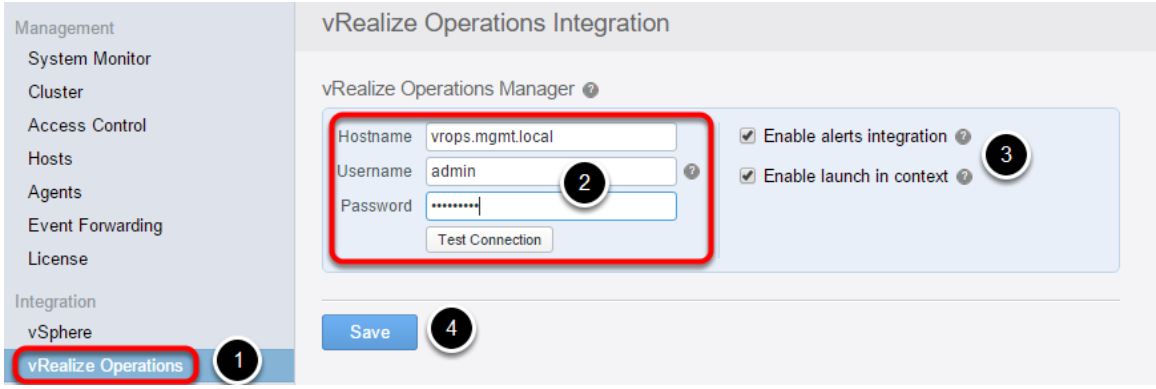


Login to Log Insight if required.

1. On the upper right portion of the Log Insight interface, click the **three bars**.

2. Select **Administration**.

Enable Integration



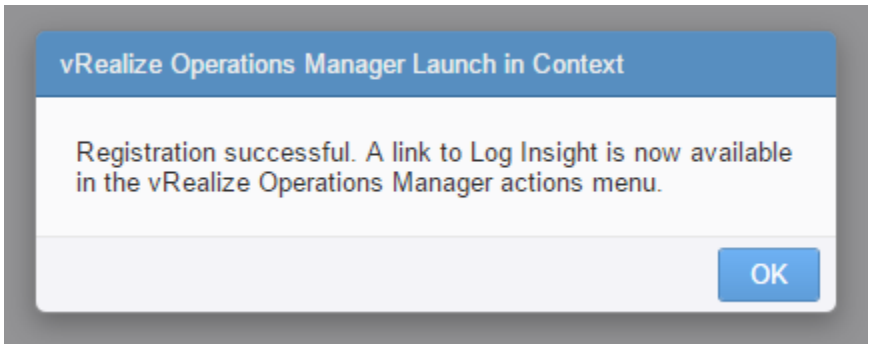
1. Click **vRealize Operations**.

2. Enter your admin user credentials for vRealize Operations Manager. Click **Test Connection**.

3. Verify that **Enable alerts integration** and **enable launch in context** are selected.

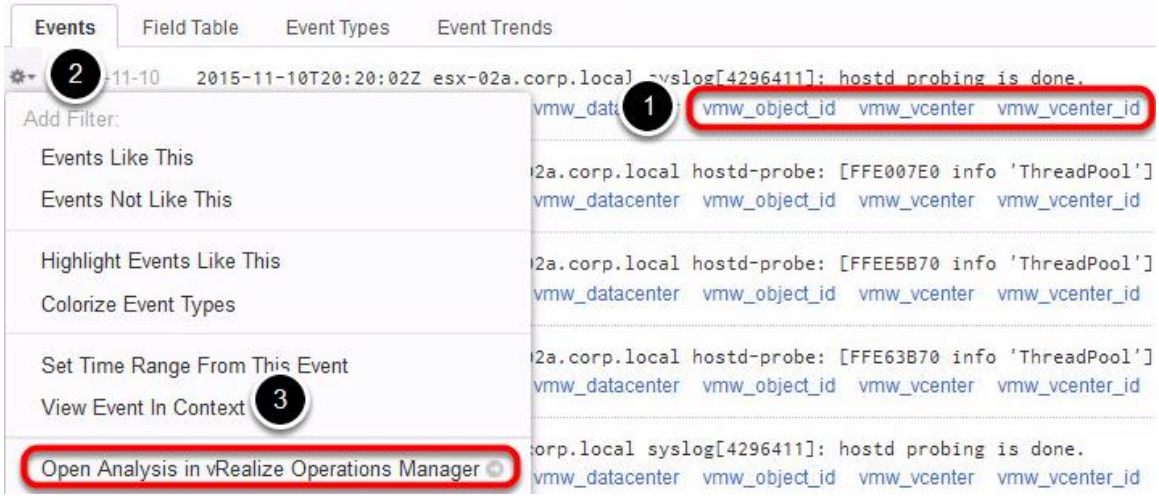
4. Click **Save**.

Registration Successful



Once registration is successful click OK.

Test Launching from Log Insight



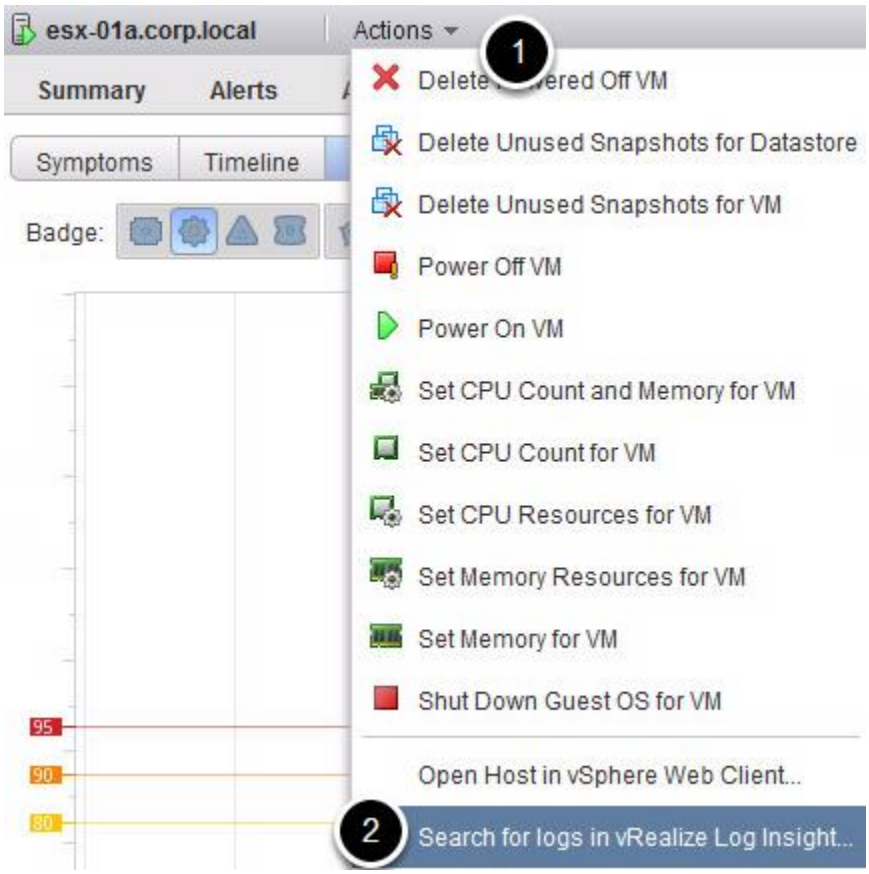
Navigate to Interactive Analytics.

1. Notice new fields have been added for many vSphere related log messages. These fields contain parent object information and often the vRealize Operations ID. This is an example of the integration at work. You now have access to the vRealize Operations inventory data in Log Insight. Logs will be matched to objects in the vRealize Operations inventory.

2. **Choose a log message for a Host or VM** in your environment, hover the mouse cursor over the message. Click the **gear icon** on the left side of the message.

3. Click **Open Analysis in vRealize Operations Manager**. You will be launched into vRealize Operations Manager to the object matched with the log message.

Test Launching from vRealize Operations



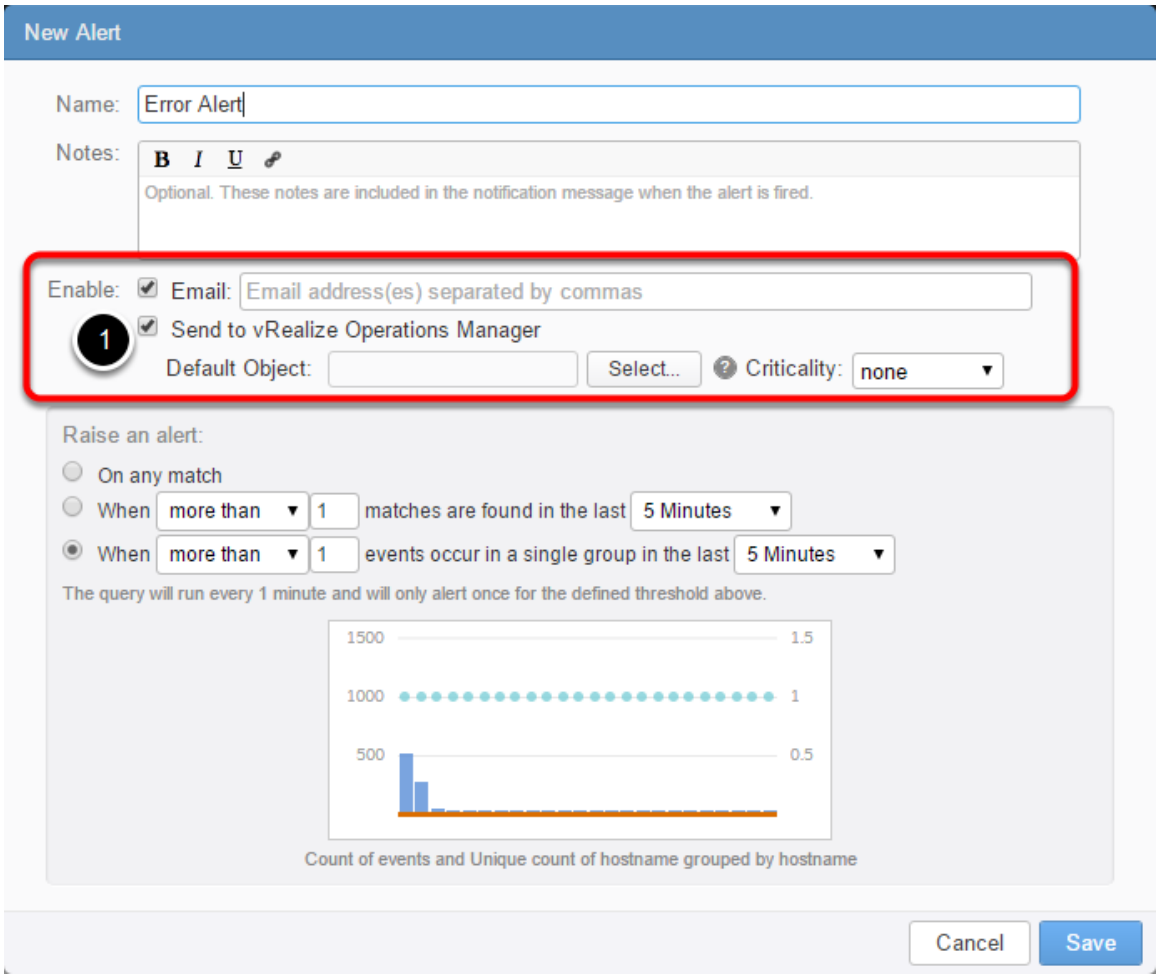
You are also able to launch into Log Insight from vRealize Operations Manager.

1. From vRealize Operations Manager, select a vSphere object, for example a vCenter Server or Host, then click the **Actions menu**.

2. Select **Search for logs in vRealize Log Insight**.

Log Insight will open with a filter added for the object that was selected in vRealize Operations Manager.

Configure an Alert

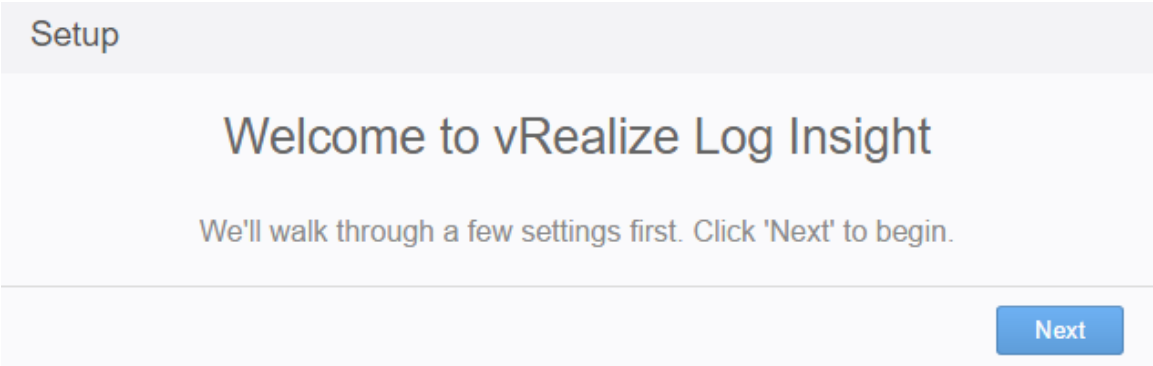


Alerts are covered in the User Interface portion of this evaluation guide. Once vRealize Operations integration is enabled you can send alerts to vRealize Operations Manager. Log Insight will automatically match hostnames in the log message to vRealize Operations Manager objects. This means that alerts will appear in vRealize Operations Manager as notification events with the matched object. If a match is not made, the notification event will be assigned to the default object. Using the default object is required so alerts are sent for objects that do not have a match in the vRealize Operations Manager inventory database.

1. Click **Send to vRealize Operations Manager**.

2. Enter a **Default Object**, a vCenter server or vSphere World object can be used. In a non-match situation, the notification events will appear with the default object in vRealize Operations Manager.

Install Cluster Nodes



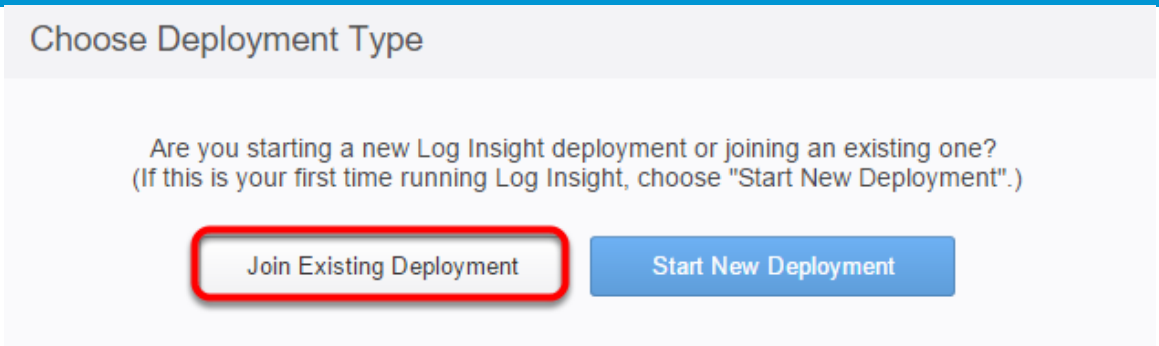
The following steps assume at least one Log Insight cluster node is already installed and running on the same Layer 2 network. **Log Insight supports 1, 3 or more nodes up to 12 in a cluster instance.**

The linked video walks through the cluster installation process: Log Insight Cluster Node Installation and Configuration video

1. **Go through the Log Insight OVA installation steps** then navigate in a supported web browser to the newly installed node **FQDN or IP address** to begin

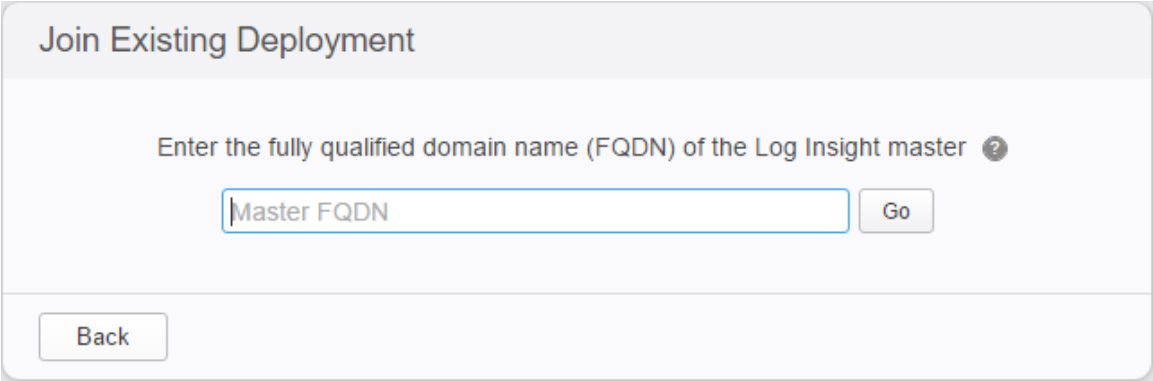
2. Click Next

Choose Deployment Type



Select **Join Existing Deployment**.

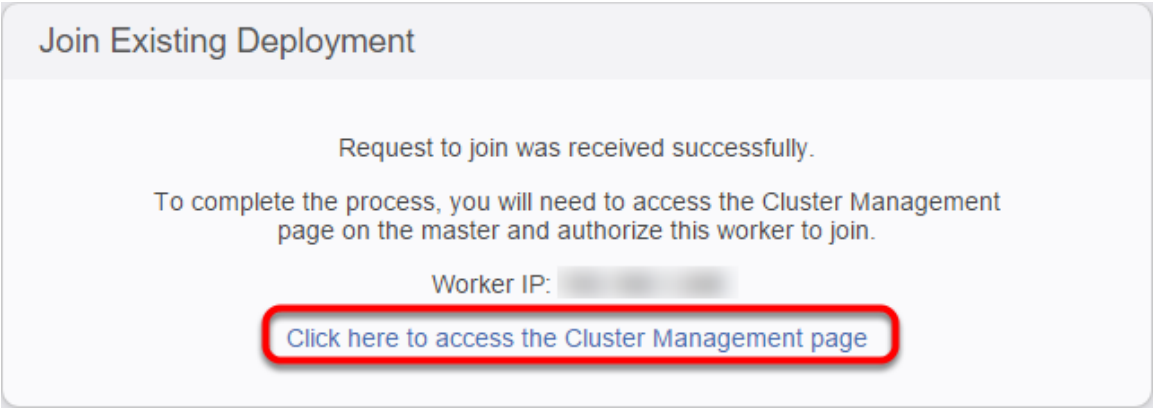
Connect to Log Insight Master



Enter the **FQDN or IP address of the Log Insight Master**. This is typically the initial node in the cluster. You can confirm the Master by navigating to Administration on an existing Log Insight node and selecting Cluster. The Master information will be listed alongside the Node hostname.

Click **Go**.

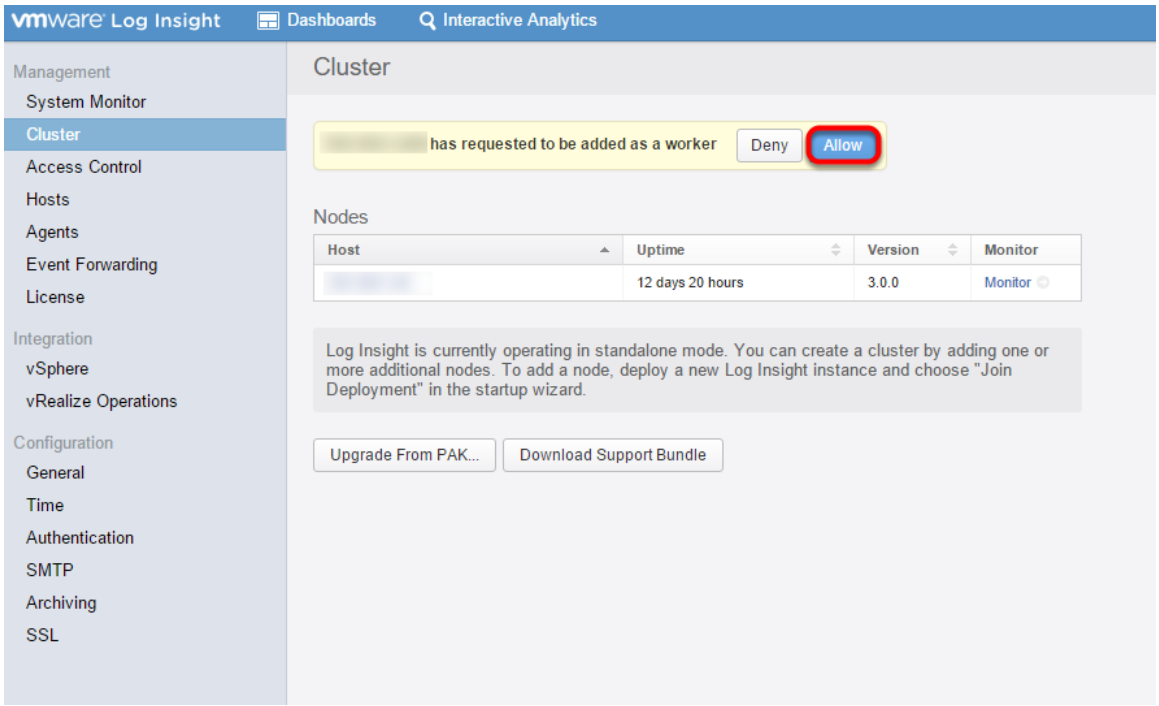
Access the Cluster Management Page



Confirm the Work IP information.

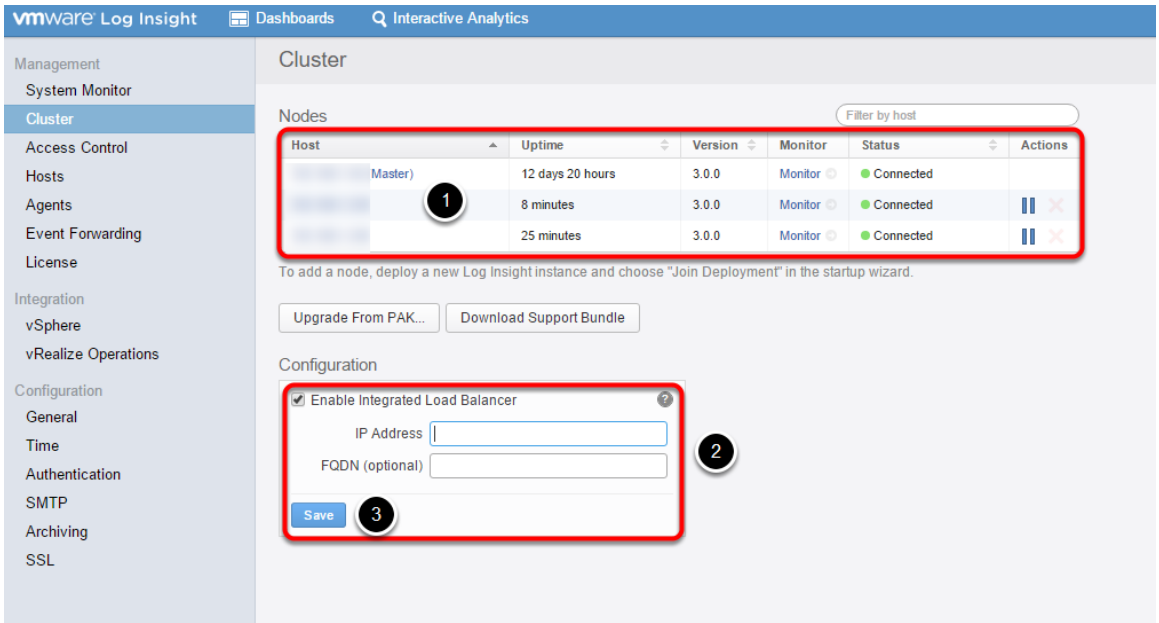
Confirm the Worker IP address. Click the C**lick here to access the Cluster Management page** link.

Worker Node Join Request



Click **Allow**.

Confirm the New Cluster Node and Enable ILB



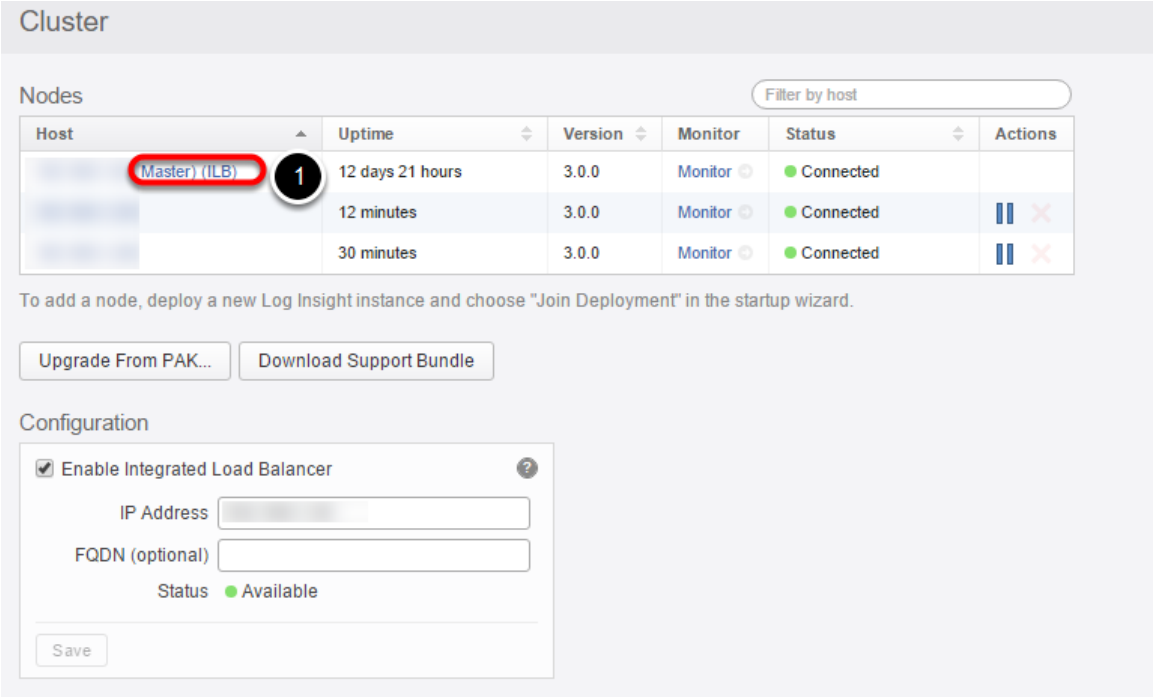
1. Your worker node is now added to the Cluster instance. **A minimum of three cluster nodes is required in a multi-node installation**. Information about each node is presented.

2. The Integrated Load Balancer (ILB) automatically balances ingestion across all nodes in the cluster. To **enable the Integrated Load Balancer**, enter a **unique IP address and optional Full Qualified Domain Name (FQDN)** in their respective fields. Click the **Enable Integrated Load Balancer** checkbox.

3. Click **Save**.

(**Note:** vSphere integration and any log endpoints will need to be reconfigured to use the integrated load balancer virtual IP.)

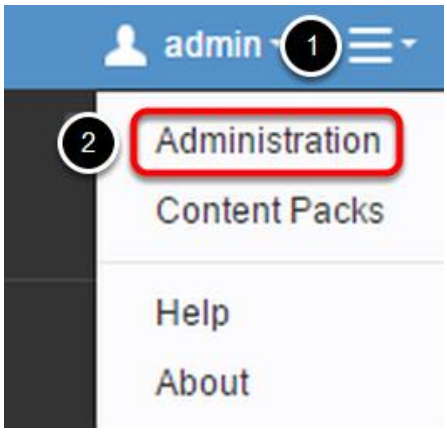
Enable ILB



1. Once the ILB is enabled, the node hosting the load balancer will be listed in the cluster management interface.

(**Note:** ILB placement is determined during an election process. The ILB can run on any node in the cluster.)

Log Insight System Monitor

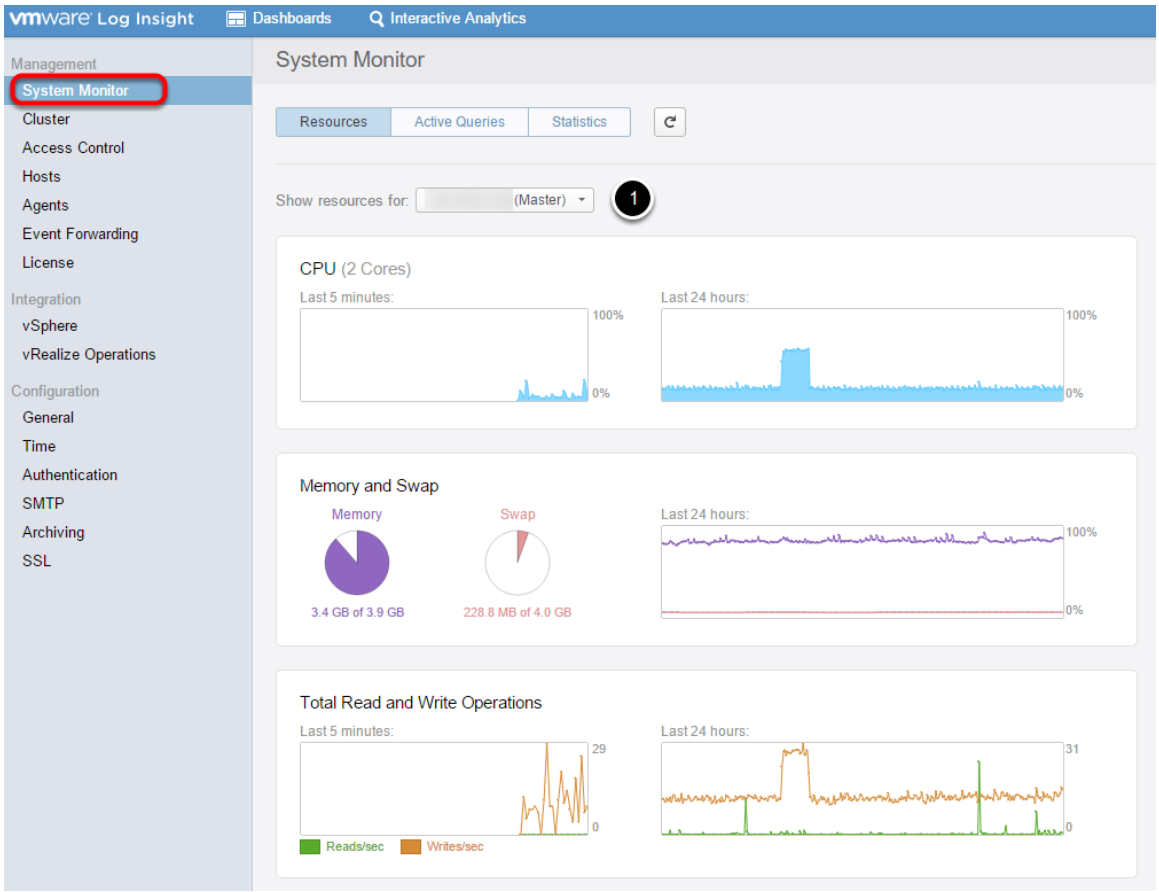


If required:

1. On the upper right portion of the Log Insight interface, click the **three bars**.

2. Select **Administration**.

System Monitor



Click **System Monitor**.

1. System monitor will display information on the selected node. Resource utilization and capacity data helps determine if **resources** are sufficient. Incoming event rates and advanced **statistics** such as query metrics and ingestion queue are also available. **Active queries** show currently running queries including the ability to cancel queries that are too expensive. Admins can configure system notifications or suspend all user alerts when the need arises.