Lenovo XClarity Integrator Content Pack for VMware vRealize Log Insight
User Guide

Version 2.0.0

Note

Before using this information and the product it supports, read the information in Appendix A "Notices" on page 25.

First Edition (June 2021)

Contents

About this publication

The document provides a brief walkthrough of the installation and configuration of the Lenovo XClarity Integrator Content Pack for VMware vRealize Log Insight (hereafter called Content Pack for vRLI). In a nutshell, this document describes how to install and configure the plugin.

Conventions and acronyms

Conventions

Convention	Description
Bold	Indicates text on a window, besides the window title, it includes menus, menu options, buttons, fields, and labels. Example: Click **OK**.
Italic	Indicates a variable, which is a placeholder for the actual text provided by the user or system. Example: copy <*source-file*> <*target-file*> **Note:** Angled brackets (< >) are also used to indicate variables.
DIALOG BOX/ CODE	Indicates text displayed in the dialog box or if you have entered. For example: `# PAIRDISPLAY -G ORADB`
Note	These notices provide important tips, guidance, and advice.

Acronyms

LXCA	Lenovo XClarity Administrator
LXCO	Lenovo XClarity Orchestrator
PFA	Predicted failure alerts
vRLI	VMware vRealize Log Insight
vSAN	Virtual storage area network
XCC	Lenovo XClarity Controller

Chapter 1. Content Pack for vRLI introduction

Content packs are read-only plug-ins to vRealize™ Log Insight™ (vRLI) that provide pre-defined knowledge about specific types of events such as log messages. In addition, a content pack creates a greater understanding of how a product, application, device works and troubleshoots the main problems, and pro-actively monitors the possible issues.

A content pack contains:
- Queries
- Extracted fields
- Dashboards
- Alerts
- Agent Groups (only for content packs whose logs are collected via Log Insight Agent)

Content Pack for vRLI overview

This content pack provides analysis of events from the LXCA, LXCO, and the resources managed by LXCA. These insights can help systems administrators find potential problems in their environment.
- Monitoring of hardware events in a LXCA and LXCO-managed environment
  - Quickly identify trends based on hardware events received, including hardware failures, power/thermal thresholds that have been exceeded, and PFAs (predicted failure alerts). These events are also categorized by source, type of hardware surfacing the events, and whether service is required. This information can help identify issues in your data centers, so you can react before more serious issues occur.
  - Listing the common issues helps in understanding the hardware health status, systems that would need attention as they are going out of warranty, systems that are power on or off, have certificate issues, etc.
  - Listing the resource events helps in understanding the memory, CPU, and IO event count, etc.
- Auditing for security changes occurring within the LXCA.
  - Security events surfaced by LXCA can help identify if unauthorized personnel is trying to access your computing resources. This might include events showing that new users have been added/deleted, what IP addresses users are using to access the LXCA, the time and dates when they are accessing resources and any changes to the security settings of the LXCA (or user IDs on the LXCA).
  - Visual representations can show changes in these activities, which could identify if an attack is occurring.
  - The Security Logins help to list the unsuccessful authentications to LXCA and managed resources, grouped by the address of the user. The pie chart lists user IDs that have successfully logged in to LXCA. It further helps to list the number of changes done to the account security settings over time.
- Auditing for the provisioning of LXCA-managed resources, including:
  - Firmware updates
  - Configuration pattern deployment
  - Bare-metal OS deployments
- LXCA specializes in helping system administrators make desired changes on their computing resources. This includes updating the firmware of LXCA-managed resources, deploying configuration changes to groups of systems, and deploying operating systems to bare-metal systems. This can help identify how much change is occurring to the configuration of servers, and if the changes have been authorized.
- The Content Pack for vRLI utilizes the interactive analysis vRLI feature & displays the Predictive Analytics dashboard to leverage the LXCO alerts listing. The alerts are predefined alerts, user-defined custom alerts, and so on.
- Facilitates extending vSAN support to Content Pack for vRLI. It supports adding graphs for correlating Lenovo HW events for disk or storage with vSAN events disk or storage, and so on.

Prerequisites

Before you import the Content Pack for vRLI, verify that you have configured your environment according to the requirements in this section.

Supported server models

The following Lenovo ThinkAgile VX servers and ThinkSystem servers are supported.

System	Server models	
ThinkAgile VX Series appliances	• ThinkAgile VX1320 Certified (7Z58) • ThinkAgile VX 1U Certified (7Y93) • ThinkAgile VX 2U Certified (7Y94) • ThinkAgile VX 2U4N Certified (7Y92) • VX2320 (7Y13, 7Y93) • VX3320 (7Y13, 7Y93) • VX3520-G (7Y14, 7Y94) • VX3720 (7Y12, 7Y92)	• VX3720-N (7Y93) • VX5520 (7Y14, 7Y94) • VX7320 (7Y94) • VX7520 (7Y14) • VX7520-N (7Y14) • VX7520 (7Y94) • VX7820 (7Z12, 7Z13, 7Z14) • VX-SR665 (7D43)
ThinkSystem servers	• SD530 (7X21) • SD630 V2 (7D1K) • SD650 (7X58) • SD650 V2 (7D1M) • SD650-N V2 (7D1N) • SE350 (7D1X, 7D27, 7Z46) • SR150 (7Y54) • SR158 (7Y55) • SR258 (7Y53) • SR250 (7Y51, 7Y52, 7Y72, 7Y73) • SR530 (7X07, 7X08) • SR550 (7X03, 7X04) • SR570 (7Y02, 7Y03) • SR590 (7X98, 7X99) • SR630 (7X01,7X02) • SR630 V2 (7Z70, 7Z71) • SR635 (7Y98, 7Y99) • SR645 (7D2X, 7D2Y) • SR650 (7X05, 7X06) • SR650 (7D4K)	• SR650 V2 (7Z72, 7Z73) • SR655 (7Y00, 7Z01) • SR665 (7D2V, 7D2W) • SR670 (7Y36, 7Y37, 7Y38) • SR670 V2 (7Z22, 7Z23) • SR850 (7X18, 7X19) • SR850 V2 (7D31, 7D32, 7D33) • SR850P (7D2H) • SR850P (7D2F, 7D2G) • SR860 (7X69, 7X70) • SR860 V2 (7Z59, 7Z60 ,7D42) • SR950 (7X11, 7X12) • SR950(7X13) • ST250 (7Y45, 7Y46) • ST258 (7Y47) • ST550 (7X09, 7X10) • ST550 (7X09, 7X10) • ST558 (7Y15, 7Y16) • ST650 V2 (7Z74, 7Z75)

Software requirements

Component	Supported version
VMware vCenter Server	6.7 & 7.0
LXCA	3.1.0 and 3.2.0
LXCO	1.4.0
vRLI	8.2 and 8.3
Supported web browsers	Chrome (89.0 and above) and Firefox (83.0 and above)

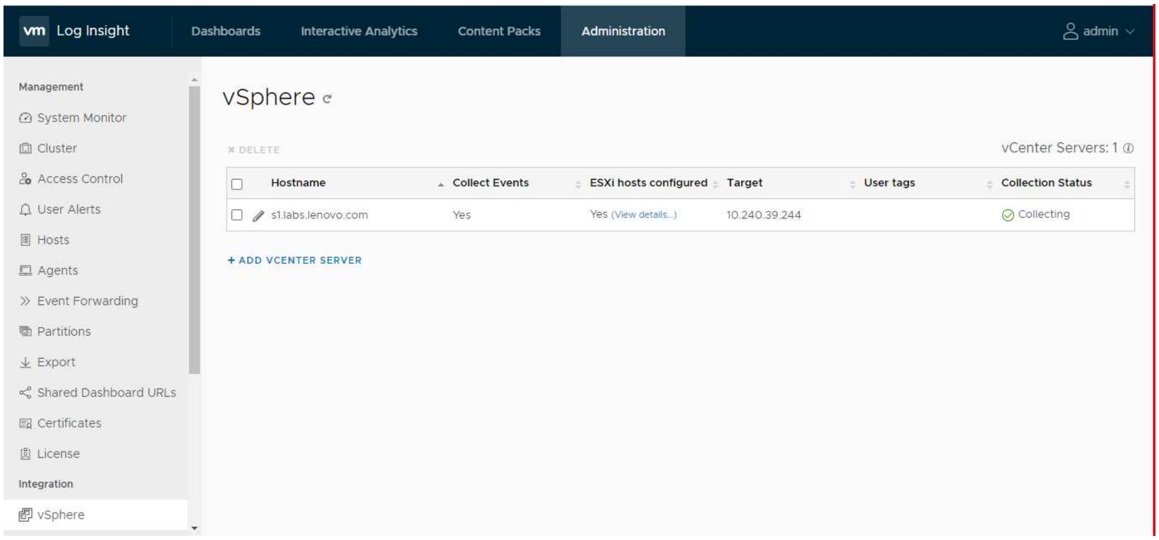
Adding a vCenter server

You need to add the vCenter server that is utilized by the vSAN dashboards.

Procedure

To add a vCenter server, complete the following steps.

1. Log in to VMware Log Insight.
2. Navigate to the **Administration** tab.
3. In the left pane, click **vSphere**.

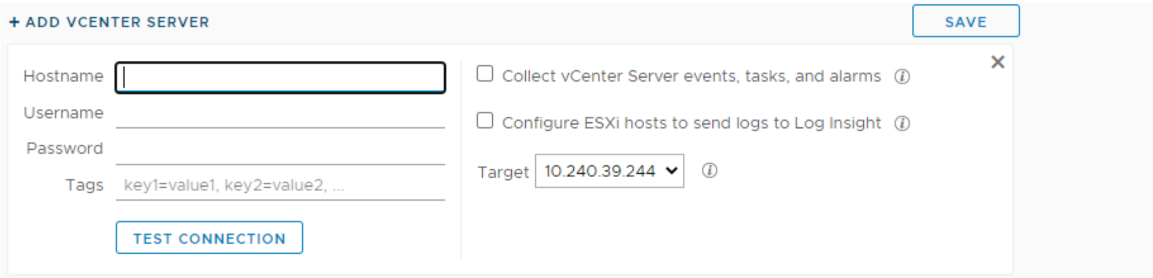


vSphere

vCenter Servers: 1

Hostname	Collect Events	ESXi hosts configured	Target	User tags	Collection Status
s1.labs.lenovo.com	Yes	Yes (View details...)	10.240.39.244		Collecting

4. To add a vCenter server, click **ADD VCENTER SERVER**.



Hostname
Username
Password
Tags key1=value1, key2=value2, ...

□ Collect vCenter Server events, tasks, and alarms

□ Configure ESXi hosts to send logs to Log Insight

Target 10.240.39.244

5. Enter the vCenter hostname, vCenter username and password you want to add. To test the server you are adding, click **TEST CONNECTION**.
6. Click **SAVE** to add the vCenter server.

Chapter 2. Installing and configuring the Content Pack for vRLI

This chapter describes the following topics:

- "Downloading the Content Pack for vRLI" on page 5
- "Importing a content pack" on page 5
- "Configuring LXCA to forward logs to vRLI" on page 6
- "Configuring LXCO to forward logs to vRLI" on page 9

Downloading the Content Pack for vRLI

Download the VLCP file for VMware vRealize Log Insight for Lenovo XClarity from the marketplace. Save the VLCP file to a folder on your local system and ensure the following:

- vRLI 8.2 or 8.3 is installed and configured.
- You have the VLCP file.
- The prerequisites are met. For details, see "Prerequisites" on page 2.

Importing a content pack

You can import content packs to exchange user-defined information with other instances of vRealize Log Insight. You can import only Content Pack (VLCP) files.

Before you begin

- If you want to use it, install the content pack in the import method, verify that you are logged in to the vRealize Log Insight web user interface as a user with the Edit Admin permission. The URL format is <https://log-insight-host>, where *log-insight-host* is the IP address or hostname of the vRealize Log Insight virtual appliance.
- If you want to use Import into My Content, you can log in to the vRealize Log Insight web user interface with the level of permission.

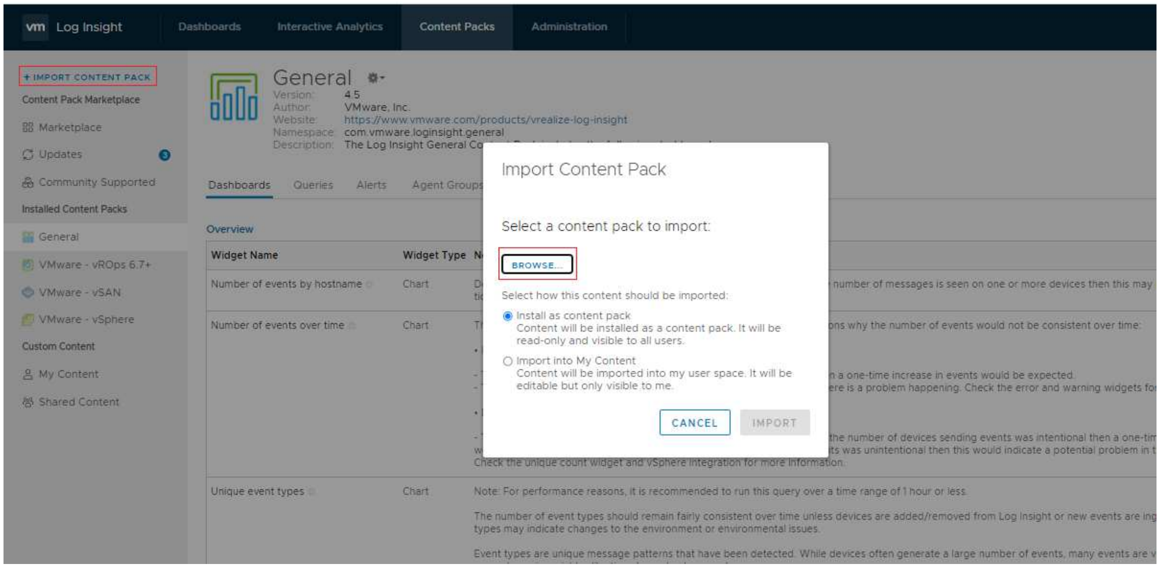
Procedure

To import a content pack, complete the following steps.

1. Navigate to the **Content Packs** tab.
2. In the upper left corner, click **IMPORT CONTENT PACK**.
3. Select the import method.

Menu item	Description
Install as content pack	The content is imported as a read-only content pack that is visible to all users of the vRealize Log Insight instance. **Note:** Content pack dashboards are read-only. You cannot delete or rename them. However, you can clone content pack dashboards to your custom dashboard. You can clone whole dashboards or individual widgets.
Import into My Content	The content is imported as custom content to your userspace and is visible only to you. You can edit the imported content without having to clone it. **Note:** Content pack metadata, such as name, author, icon, and so on, are not displayed in this mode. Once imported into My Content, the content pack cannot be uninstalled as a pack. If you want to remove a content pack from My Content, you have to individually remove each of its elements, such as dashboards, queries, alerts, and fields.

4. Users can import content packs only in their own user spaces.



General

Version: 4.5
Author: VMware, Inc.
Website: https://www.vmware.com/products/vrealize-log-insight
Namespace: com.vmware.loginsight.general
Description: The Log Insight General Co

Import Content Pack

Select a content pack to import:

BROWSE...

Select how this content should be imported:

● Install as content pack
Content will be installed as a content pack. It will be read-only and visible to all users.

○ Import into My Content
Content will be imported into my user space. It will be editable but only visible to me.

CANCEL IMPORT

number of messages is seen on one or more devices then this may

ons why the number of events would not be consistent over time:

n a one-time increase in events would be expected.

ere is a problem happening. Check the error and warning widgets fo

the number of devices sending events was intentional then a one-tim

ts was unintentional then this would indicate a potential problem in t

Check the unique count widget and vSphere integration for more information.

Note: For performance reasons, it is recommended to run this query over a time range of 1 hour or less.

The number of event types should remain fairly consistent over time unless devices are added/removed from Log Insight or new events are ing types may indicate changes to the environment or environmental issues.

Event types are unique message patterns that have been detected. While devices often generate a large number of events, many events are v

5. Browse for the content pack that you want to import, and click **Open**.
6. Click **IMPORT**.
7. (Optional) If you selected to import the content pack as custom content, a dialog box appears and you are prompted to select what content to import. Select the content items and click **IMPORT** again.
8. (Optional) Some content packs require additional setup steps. Instructions for these steps appear after the import is finished. Complete these steps before you use the content pack.

The imported content pack is ready to use and appears in the Content Packs or the Custom Content list to the left.

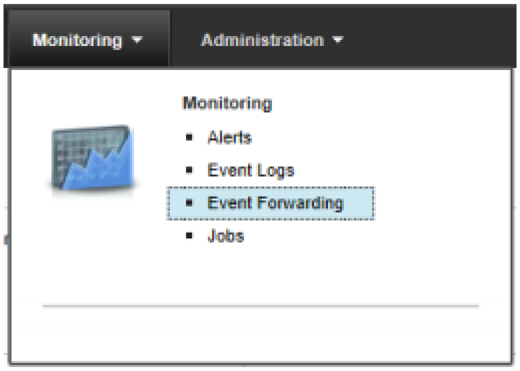
Configuring LXCA to forward logs to vRLI

To forward events from the LXCA to VMware vRealize Log Insight, the Syslog forwarding capability of the LXCA must be configured.

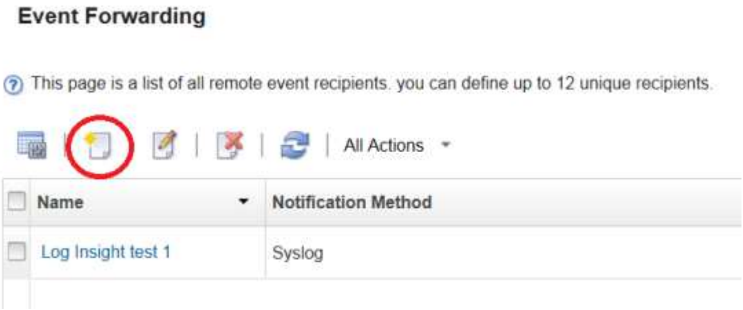
Procedure

To configure LXCA, complete the following steps.

1. After signing in to the LXCA, hover to **Monitoring** on the banner near the top of the screen. Click **Event Forwarding**.



2. From the **Event Forwarding** panel, click the **New** icon.

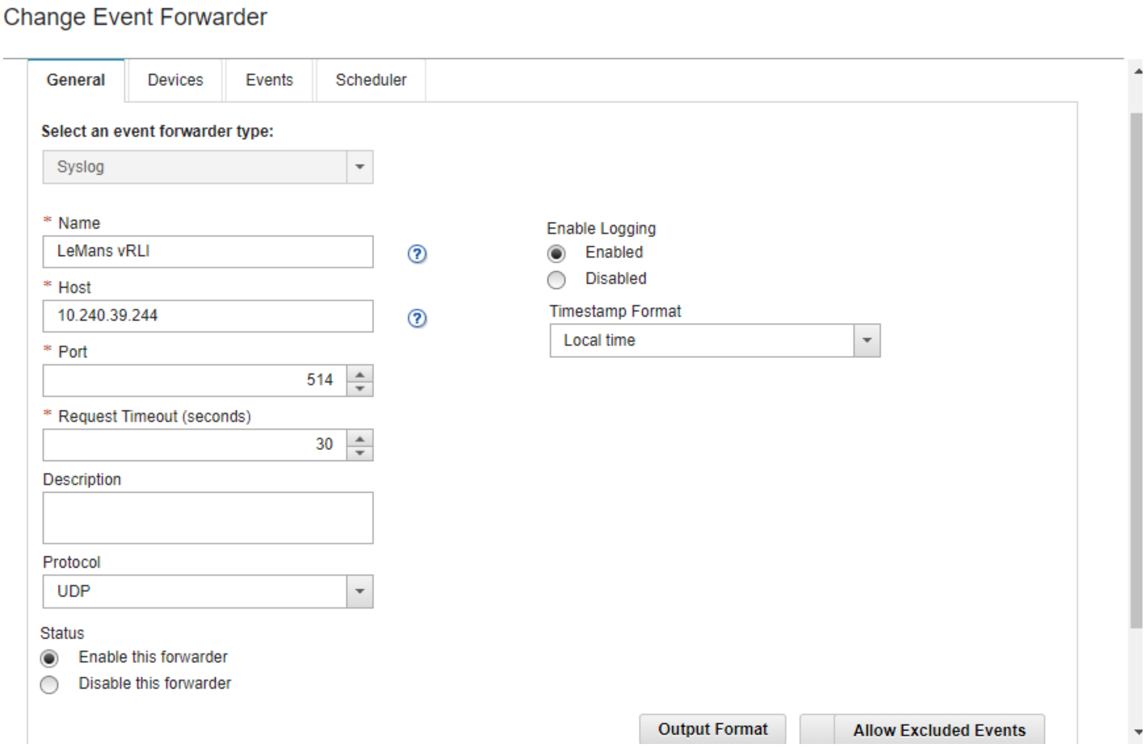


Event Forwarding

This page is a list of all remote event recipients. you can define up to 12 unique recipients.

Name	Notification Method
Log Insight test 1	Syslog

3. Select **Syslog** as the event recipient type, and fill in the appropriate information in the dialog, including the TCP/IP address of the VMware Log Insight server. Click **Next**.



Change Event Forwarder

Select an event forwarder type: Syslog

* Name: LeMans vRLI

* Host: 10.240.39.244

* Port: 514

* Request Timeout (seconds): 30

Description:

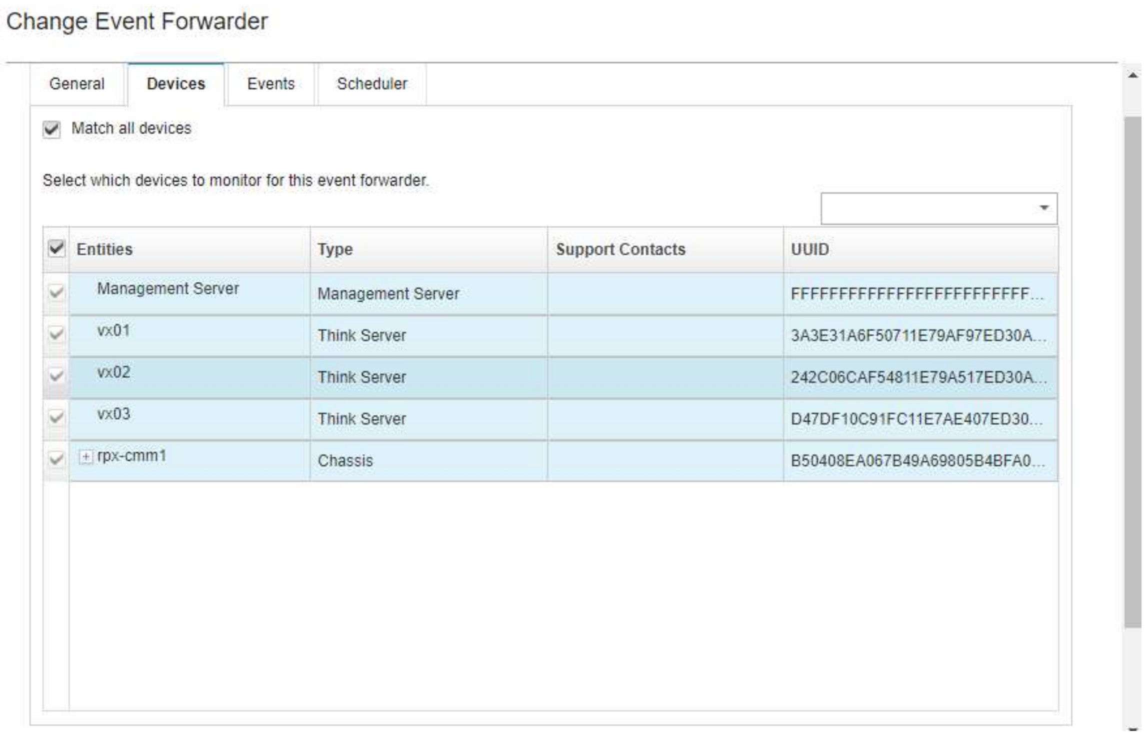
Protocol: UDP

Status
- ● Enable this forwarder
- ○ Disable this forwarder

Enable Logging
- ● Enabled
- ○ Disabled

Timestamp Format: Local time

4. Select the LXCA-managed Devices (and potentially the LXCA management server itself) to forward events from:



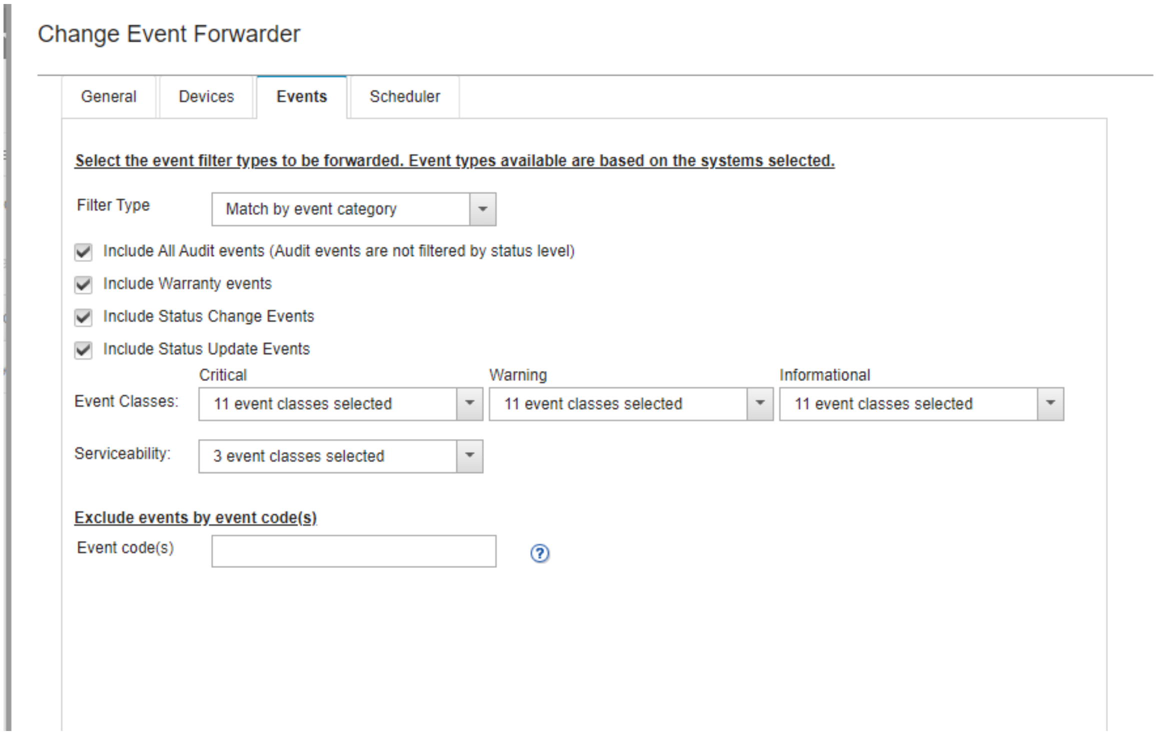
Change Event Forwarder

☑ Match all devices

Select which devices to monitor for this event forwarder.

☑	Entities	Type	Support Contacts	UUID
✓	Management Server	Management Server		FFFFFFFFFFFFFFFFFFFFFFFF...
✓	vx01	Think Server		3A3E31A6F50711E79AF97ED30A...
✓	vx02	Think Server		242C06CAF54811E79A517ED30A...
✓	vx03	Think Server		D47DF10C91FC11E7AE407ED30...
✓	+ rpx-cmm1	Chassis		B50408EA067B49A69805B4BFA0...

5. Select which event types you want to forward as VMware vRealize Log Insight. Then click **Create**. From this point, the selected event types will be forwarded to the VMware vRealize Log Insight server.



Change Event Forwarder

Select the event filter types to be forwarded. Event types available are based on the systems selected.

Filter Type: Match by event category

☑ Include All Audit events (Audit events are not filtered by status level)

☑ Include Warranty events

☑ Include Status Change Events

☑ Include Status Update Events

	Critical	Warning	Informational
Event Classes:	11 event classes selected	11 event classes selected	11 event classes selected
Serviceability:	3 event classes selected		

Exclude events by event code(s)

Event code(s):

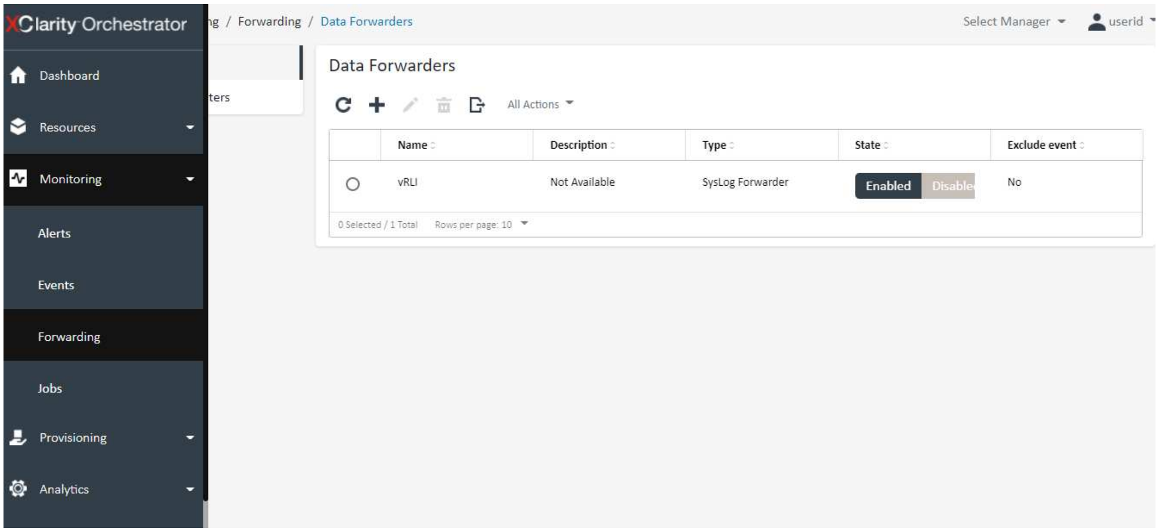
Configuring LXCO to forward logs to vRLI

To forward events from the LXCO to VMware vRealize Log Insight, the Syslog forwarding capability of the LXCO must be configured.

Procedure

To configure LXCO for log forwarding, complete the following steps.

1. After signing in to the LXCO, on the left pane, click **Monitoring** > **Forwarding > Data Forwarders**. The **Data Forwarders** screen is displayed.

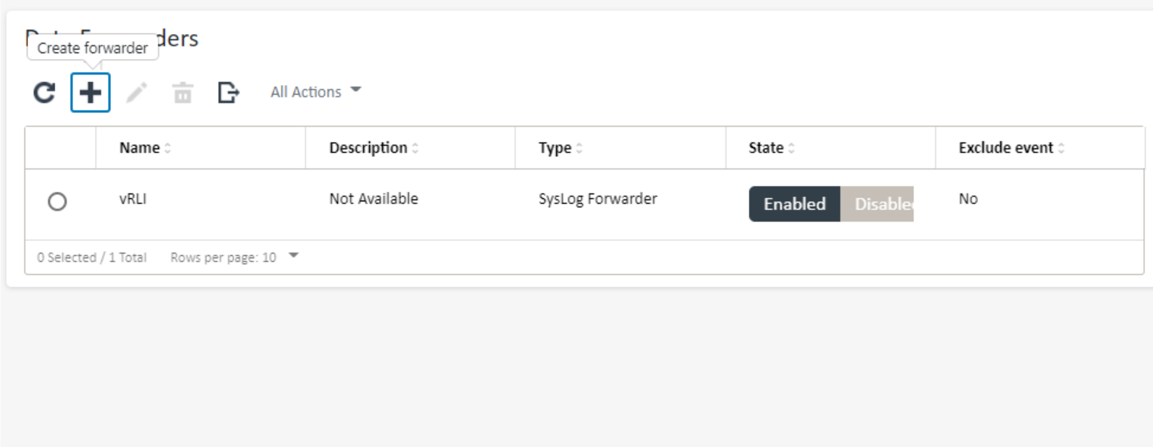


Data Forwarders

	Name	Description	Type	State	Exclude event
○	vRLI	Not Available	SysLog Forwarder	Enabled Disable	No

0 Selected / 1 Total   Rows per page: 10

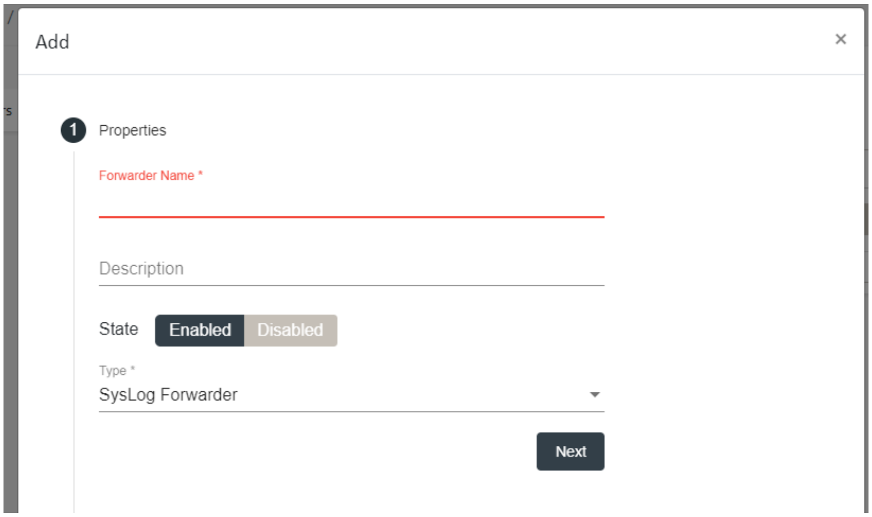
2. On the **Data Forwarders** page, click the **+** icon to configure the orchestrator by creating a forwarder. The **Add** wizard is displayed.



	Name	Description	Type	State	Exclude event
○	vRLI	Not Available	SysLog Forwarder	Enabled Disable	No

0 Selected / 1 Total   Rows per page: 10

3. In the **Properties** section, enter the forwarder name, description, and select **SysLog Forwarder** as the event recipient type, and click **Next**.


Add

1 Properties

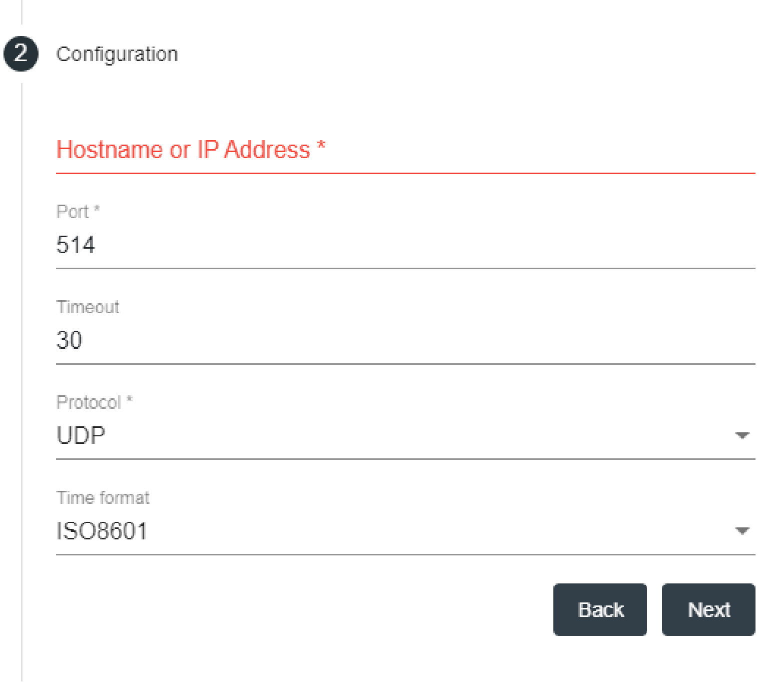
Forwarder Name *

Description

State Enabled Disabled

Type *
SysLog Forwarder

4. In the **Configuration** section, enter the TCP/IP address of the VMware Log Insight server and click **Next**.


2 Configuration

Hostname or IP Address *

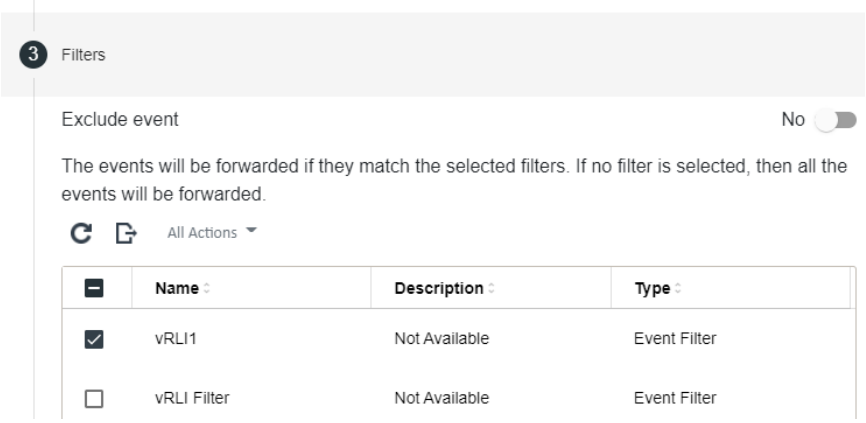
Port *
514

Timeout
30

Protocol *
UDP

Time format
ISO8601

5. Exclude the events you do not want to consider for forwarding by selecting the respective checkbox and the radio button.

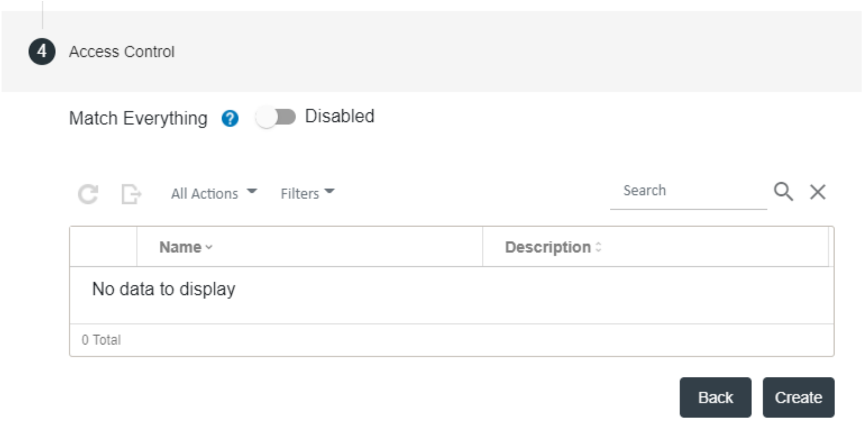


Exclude event — No

The events will be forwarded if they match the selected filters. If no filter is selected, then all the events will be forwarded.

☐	Name	Description	Type
☑	vRLI1	Not Available	Event Filter
☐	vRLI Filter	Not Available	Event Filter

6. In the **Access Control** section, select the required matching criteria and click **Create**. The data forwarder is created.



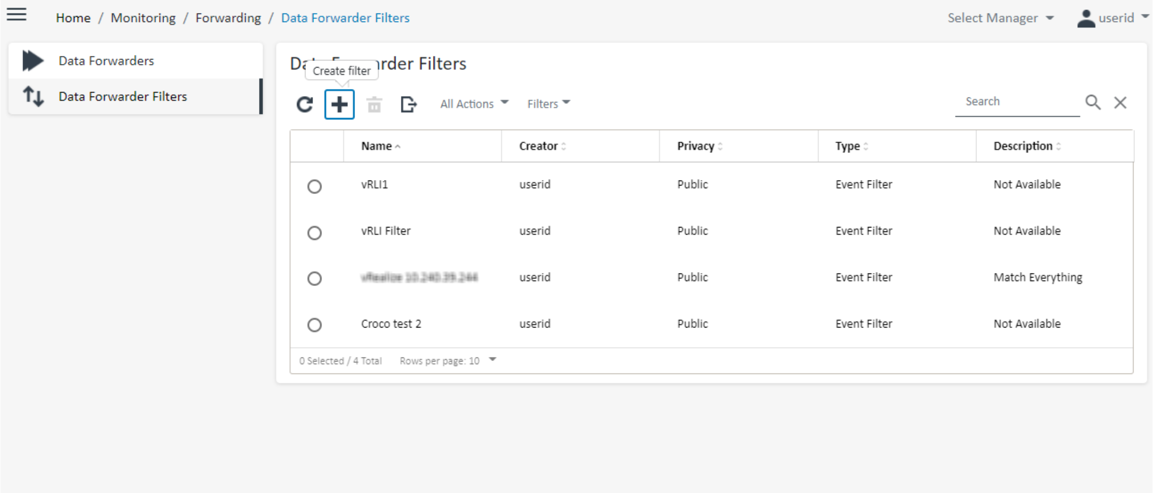
Match Everything — Disabled

	Name	Description

No data to display

0 Total

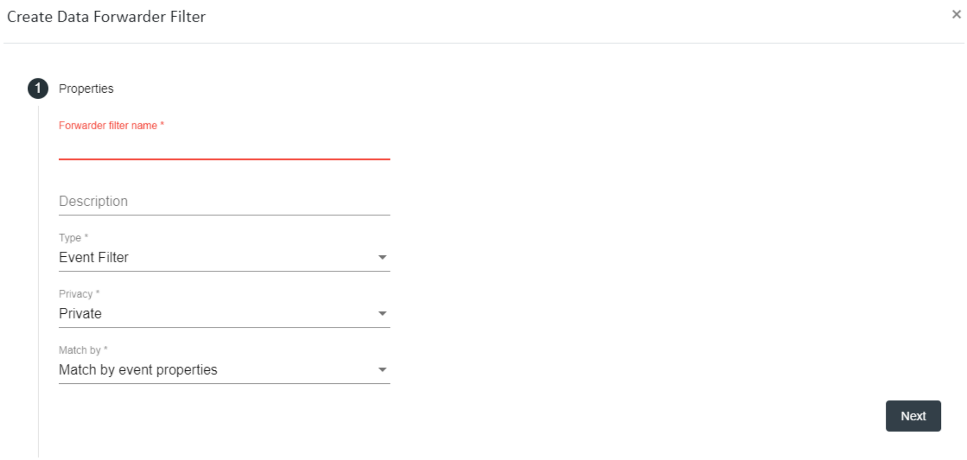
7. To create a data filter, navigate to **Data Forwarder Filters** and click the **Create Filter** icon.



	Name	Creator	Privacy	Type	Description
○	vRLI1	userid	Public	Event Filter	Not Available
○	vRLI Filter	userid	Public	Event Filter	Not Available
○	[redacted]	userid	Public	Event Filter	Match Everything
○	Croco test 2	userid	Public	Event Filter	Not Available

0 Selected / 4 Total Rows per page: 10

8. Add an appropriate data filter name, description, and click **Next**.



Create Data Forwarder Filter

1 Properties

Forwarder filter name *

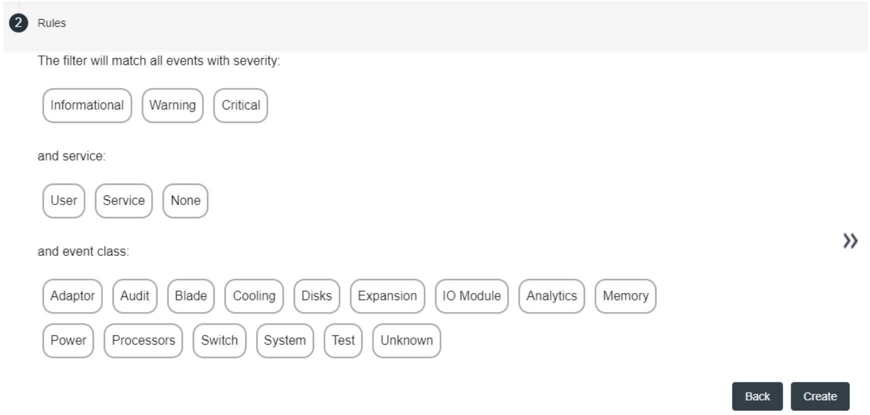
Description

Type *
Event Filter

Privacy *
Private

Match by *
Match by event properties

9. Select the rules as required and click **Create**.



2 Rules

The filter will match all events with severity:

Informational Warning Critical

and service:

User Service None

and event class:

Adaptor Audit Blade Cooling Disks Expansion IO Module Analytics Memory Power Processors Switch System Test Unknown

Chapter 3. Content Pack for vRLI specifications

After importing and configuring the Content Pack for vRLI, you can view the following:

- "Dashboards" on page 13
- "Viewing interactive analytics and alerts" on page 20
- "Fields" on page 21
- "Logs" on page 23

Dashboards

Dashboards provide a graphic representation of the status and relationships of selected objects. The standard dashboards are delivered as templates.

The Lenovo XClarity vRLI dashboards provide an overview of the predictive analytics, events, and common issues of LXCA resources. The dashboards enable you to view, monitor, and troubleshoot resources.

The following dashboards are supported in this content pack:

- Overview Dashboard
- Security - Logins Dashboard
- Security - Changes Dashboard
- Provisioning Dashboard
- Power and Thermal Dashboard
- Events Recommending Service
- Resource Events
- Common Issues
- Predictive Analytics Dashboard
- Lenovo HW and vSAN Events
- Security Login

Before you begin

From the vRLI main menu, select **Dashboards > All Dashboards**. The available dashboards are listed here.

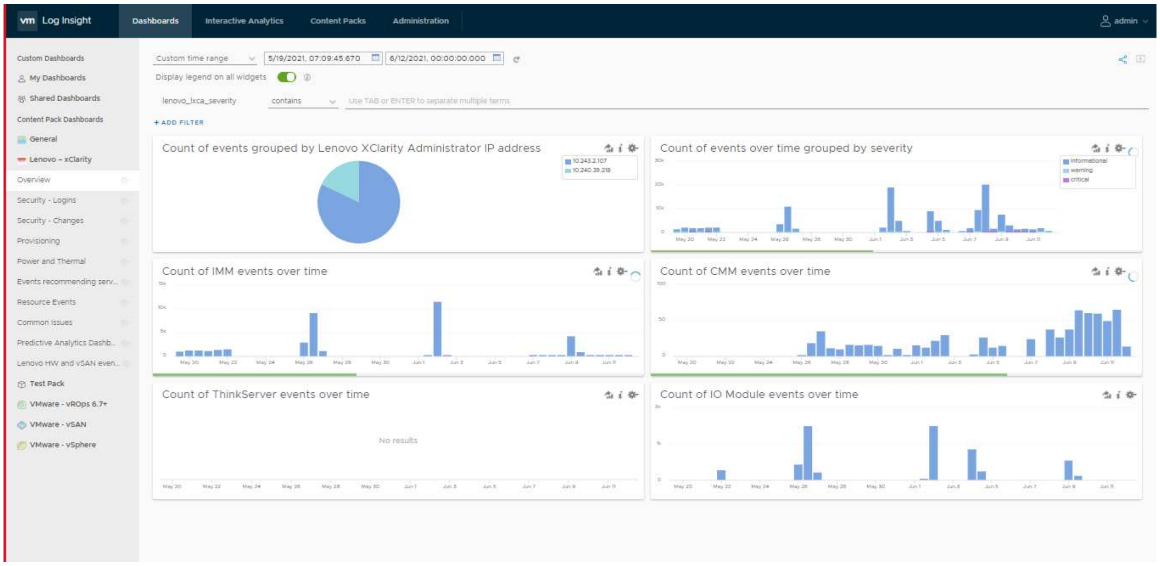
Once the required dashboards are selected, it is listed in the navigation panel on the left.

Procedure

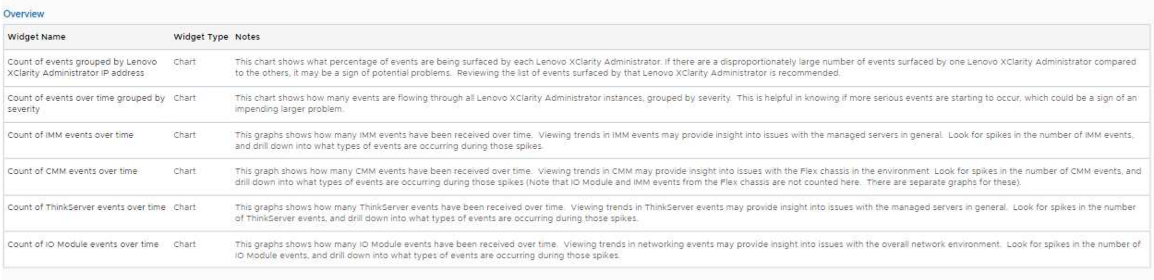
1. Log in to the vRLI UI using admin credentials.
2. Click **Dashboards**.
3. From the **All Dashboards** list, select the required dashboard.

Overview Dashboard

Provides a consolidated listing for all messages coming from LXCA servers (including events from LXCA-managed resources).



The following table lists the widget names and their details:

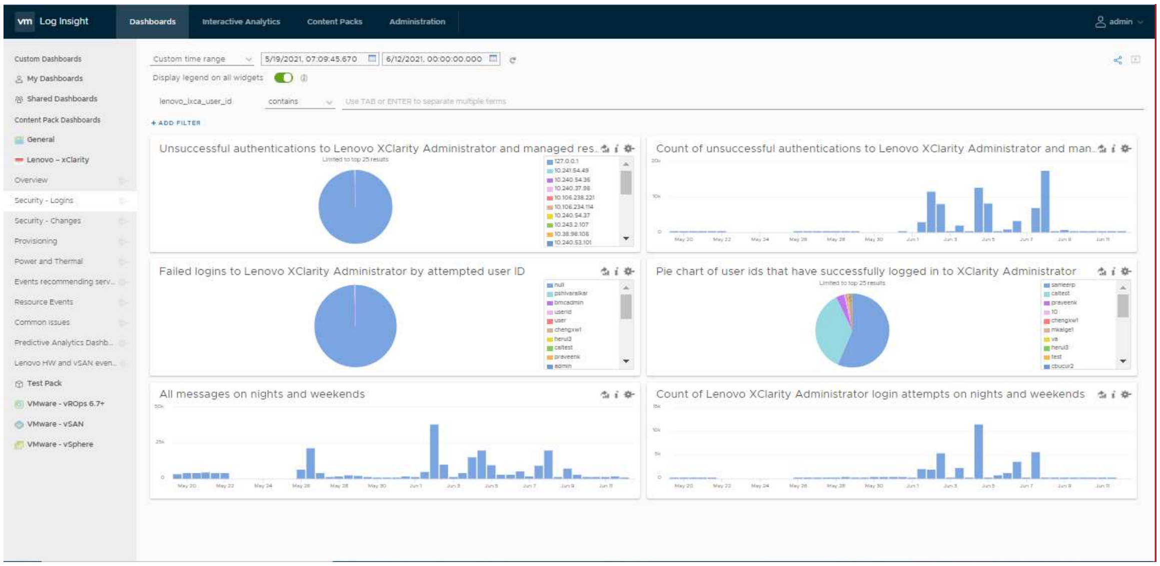


Overview

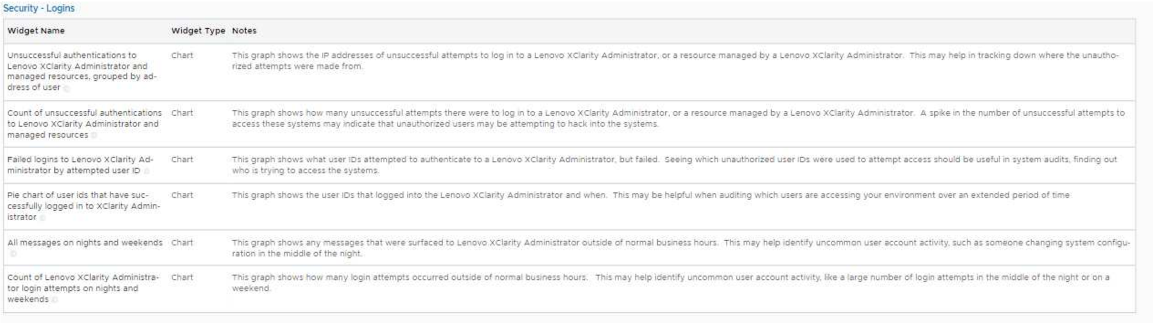
Widget Name	Widget Type	Notes
Count of events grouped by Lenovo XClarity Administrator IP address	Chart	This chart shows what percentage of events are being surfaced by each Lenovo XClarity Administrator. If there are a disproportionately large number of events surfaced by one Lenovo XClarity Administrator compared to the others, it may be a sign of potential problems. Reviewing the list of events surfaced by that Lenovo XClarity Administrator is recommended.
Count of events over time grouped by severity	Chart	This chart shows how many events are flowing through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem.
Count of IMM events over time	Chart	This graphs shows how many IMM events have been received over time. Viewing trends in IMM events may provide insight into issues with the managed servers in general. Look for spikes in the number of IMM events, and drill down into what types of events are occurring during those spikes.
Count of CMM events over time	Chart	This graph shows how many CMM events have been received over time. Viewing trends in CMM may provide insight into issues with the Flex chassis in the environment Look for spikes in the number of CMM events, and drill down into what types of events are occurring during those spikes (Note that IO Module and IMM events from the Flex chassis are not counted here. There are separate graphs for these).
Count of ThinkServer events over time	Chart	This graphs shows how many ThinkServer events have been received over time. Viewing trends in ThinkServer events may provide insight into issues with the managed servers in general. Look for spikes in the number of ThinkServer events, and drill down into what types of events are occurring during those spikes.
Count of IO Module events over time	Chart	This graphs shows how many IO Module events have been received over time. Viewing trends in networking events may provide insight into issues with the overall network environment. Look for spikes in the number of IO Module events, and drill down into what types of events are occurring during those spikes.

Security - Logins Dashboard

Provides statistics on any security-related events, such as user logins or failures.



The following table lists the widget names and their details:

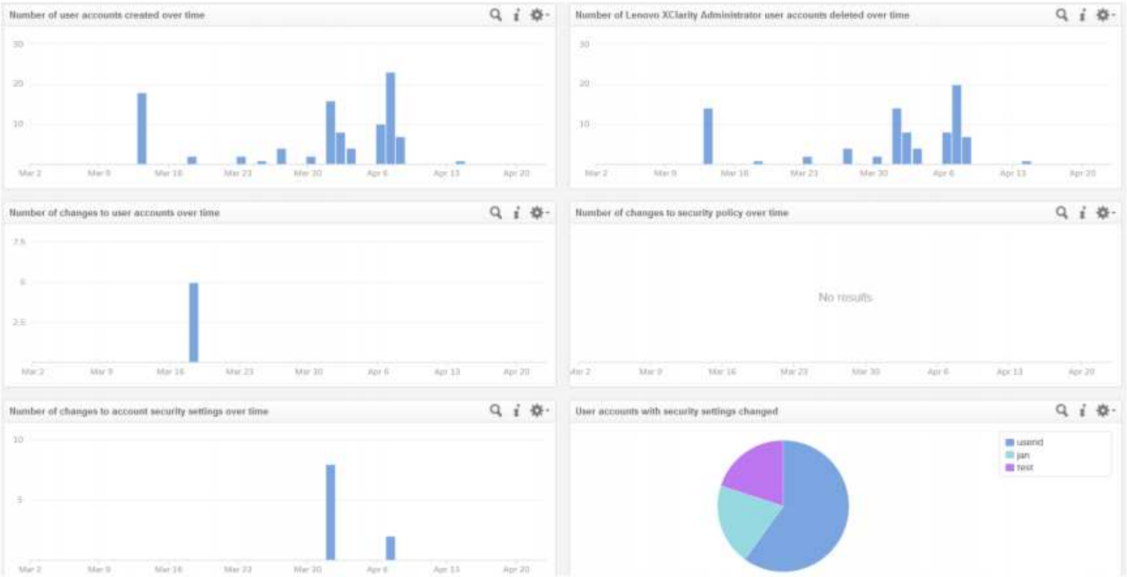


Security - Logins

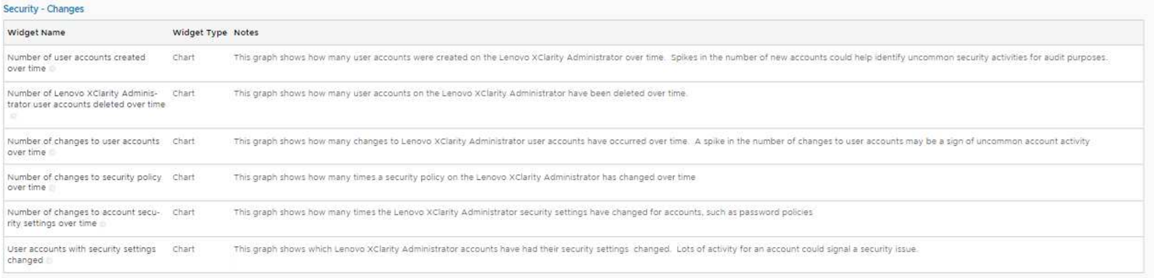
Widget Name	Widget Type	Notes
Unsuccessful authentications to Lenovo XClarity Administrator and managed resources, grouped by address of user	Chart	This graph shows the IP addresses of unsuccessful attempts to log in to a Lenovo XClarity Administrator, or a resource managed by a Lenovo XClarity Administrator. This may help in tracking down where the unauthorized attempts were made from.
Count of unsuccessful authentications to Lenovo XClarity Administrator and managed resources	Chart	This graph shows how many unsuccessful attempts there were to log in to a Lenovo XClarity Administrator, or a resource managed by a Lenovo XClarity Administrator. A spike in the number of unsuccessful attempts to access these systems may indicate that unauthorized users may be attempting to hack into the systems.
Failed logins to Lenovo XClarity Administrator by attempted user ID	Chart	This graph shows what user IDs attempted to authenticate to a Lenovo XClarity Administrator, but failed. Seeing which unauthorized user IDs were used to attempt access should be useful in system audits, finding out who is trying to access the systems.
Pie chart of user ids that have successfully logged in to XClarity Administrator	Chart	This graph shows the user IDs that logged into the Lenovo XClarity Administrator and when. This may be helpful when auditing which users are accessing your environment over an extended period of time
All messages on nights and weekends	Chart	This graph shows any messages that were surfaced to Lenovo XClarity Administrator outside of normal business hours. This may help identify uncommon user account activity, such as someone changing system configuration in the middle of the night.
Count of Lenovo XClarity Administrator login attempts on nights and weekends	Chart	This graph shows how many login attempts occurred outside of normal business hours. This may help identify uncommon user account activity, like a large number of login attempts in the middle of the night or on a weekend.

Security - Changes Dashboard

Shows any security changes made to the LXCA, such as security policy changes, or changes for individual LXCA users.


Number of user accounts created over time
30
20
10
Mar 2
Mar 9
Mar 16
Mar 23
Mar 30
Apr 6
Apr 13
Apr 20
Number of Lenovo XClarity Administrator user accounts deleted over time
30
20
10
Mar 2
Mar 9
Mar 16
Mar 23
Mar 30
Apr 6
Apr 13
Apr 20
Number of changes to user accounts over time
7.5
5
2.5
Mar 2
Mar 9
Mar 16
Mar 23
Mar 30
Apr 6
Apr 13
Apr 20
Number of changes to security policy over time
No results
Mar 2
Mar 9
Mar 16
Mar 23
Mar 30
Apr 6
Apr 13
Apr 20
Number of changes to account security settings over time
10
5
Mar 2
Mar 9
Mar 16
Mar 23
Mar 30
Apr 6
Apr 13
Apr 20
User accounts with security settings changed
usernd
jan
test

The following table lists the widget names and their details:

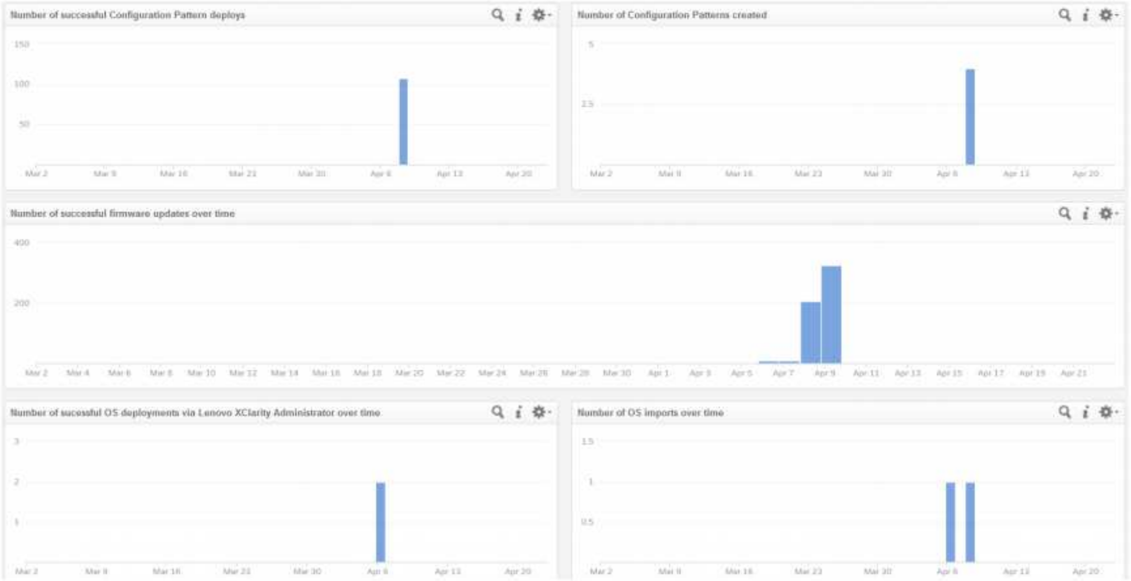


Security - Changes

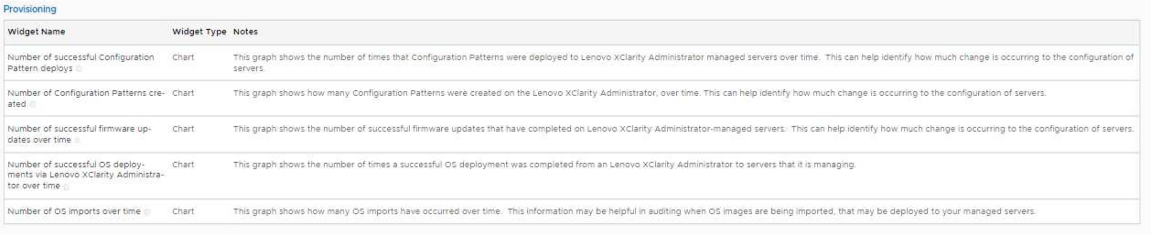
Widget Name	Widget Type	Notes
Number of user accounts created over time	Chart	This graph shows how many user accounts were created on the Lenovo XClarity Administrator over time. Spikes in the number of new accounts could help identify uncommon security activities for audit purposes.
Number of Lenovo XClarity Administrator user accounts deleted over time	Chart	This graph shows how many user accounts on the Lenovo XClarity Administrator have been deleted over time.
Number of changes to user accounts over time	Chart	This graph shows how many changes to Lenovo XClarity Administrator user accounts have occurred over time. A spike in the number of changes to user accounts may be a sign of uncommon account activity
Number of changes to security policy over time	Chart	This graph shows how many times a security policy on the Lenovo XClarity Administrator has changed over time
Number of changes to account security settings over time	Chart	This graph shows how many times the Lenovo XClarity Administrator security settings have changed for accounts, such as password policies
User accounts with security settings changed	Chart	This graph shows which Lenovo XClarity Administrator accounts have had their security settings changed. Lots of activity for an account could signal a security issue.

Provisioning Dashboard

Shows events related to the provisioning of managed resources. LXCA can provision changes to managed resources, including updating firmware, pushing configuration changes, and deploying operating system images.



The following table lists the widget names and their details:

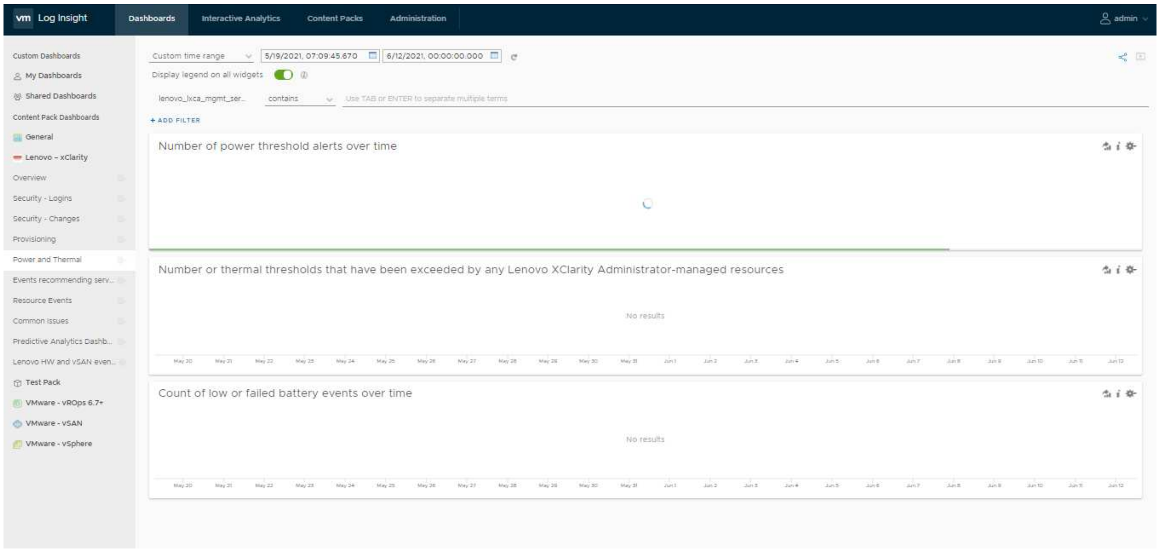


Provisioning

Widget Name	Widget Type	Notes
Number of successful Configuration Pattern deploys	Chart	This graph shows the number of times that Configuration Patterns were deployed to Lenovo XClarity Administrator managed servers over time. This can help identify how much change is occurring to the configuration of servers.
Number of Configuration Patterns created	Chart	This graph shows how many Configuration Patterns were created on the Lenovo XClarity Administrator, over time. This can help identify how much change is occurring to the configuration of servers.
Number of successful firmware updates over time	Chart	This graph shows the number of successful firmware updates that have completed on Lenovo XClarity Administrator-managed servers. This can help identify how much change is occurring to the configuration of servers.
Number of successful OS deployments via Lenovo XClarity Administrator over time	Chart	This graph shows the number of times a successful OS deployment was completed from an Lenovo XClarity Administrator to servers that it is managing.
Number of OS imports over time	Chart	This graph shows how many OS imports have occurred over time. This information may be helpful in auditing when OS images are being imported, that may be deployed to your managed servers.

Power and Thermal Dashboard

Graphically depicts power/thermal thresholds. Any time power or thermal threshold is exceeded, the events associated with that situation are reflected in the graphs.



Custom time range 5/19/2021, 07:09:45.670 6/12/2021, 00:00:00.000

Display legend on all widgets

lenovo_lxca_mgmt_ser... contains Use TAB or ENTER to separate multiple terms

Number of power threshold alerts over time

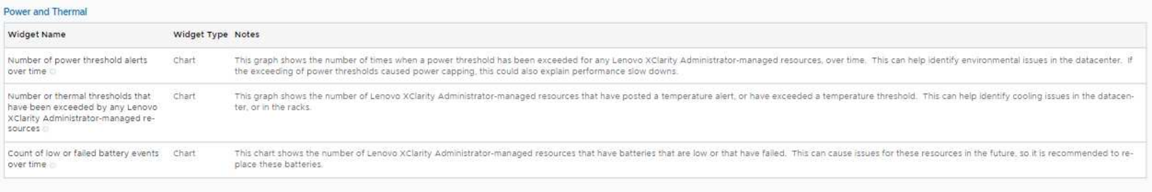
Number or thermal thresholds that have been exceeded by any Lenovo XClarity Administrator-managed resources

No results

Count of low or failed battery events over time

No results

The following table lists the widget names and their details:

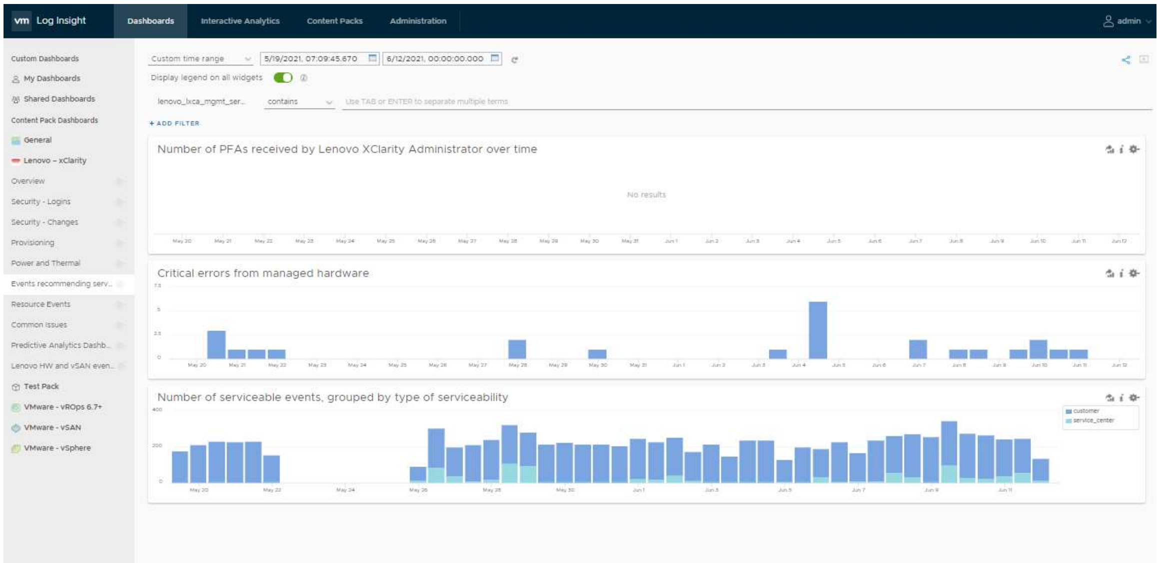


Power and Thermal

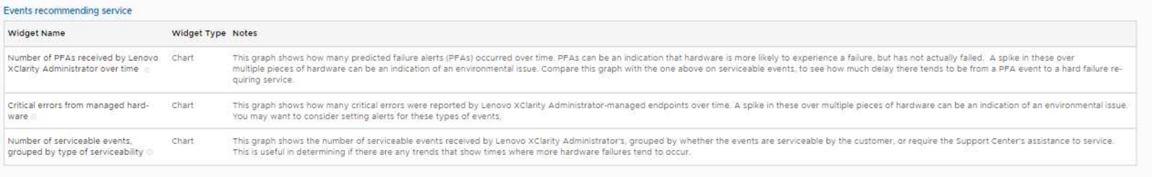
Widget Name	Widget Type	Notes
Number of power threshold alerts over time	Chart	This graph shows the number of times when a power threshold has been exceeded for any Lenovo XClarity Administrator-managed resources, over time. This can help identify environmental issues in the datacenter. If the exceeding of power thresholds caused power capping, this could also explain performance slow downs.
Number or thermal thresholds that have been exceeded by any Lenovo XClarity Administrator-managed resources	Chart	This graph shows the number of Lenovo XClarity Administrator-managed resources that have posted a temperature alert, or have exceeded a temperature threshold. This can help identify cooling issues in the datacenter, or in the racks.
Count of low or failed battery events over time	Chart	This chart shows the number of Lenovo XClarity Administrator-managed resources that have batteries that are low or that have failed. This can cause issues for these resources in the future, so it is recommended to replace these batteries.

Events Recommending Service Dashboard

Displays events for resources that require attention by the System Administrator or the Support Center (or events predicting that these types of failures are imminent).



The following table lists the widget names and their details:

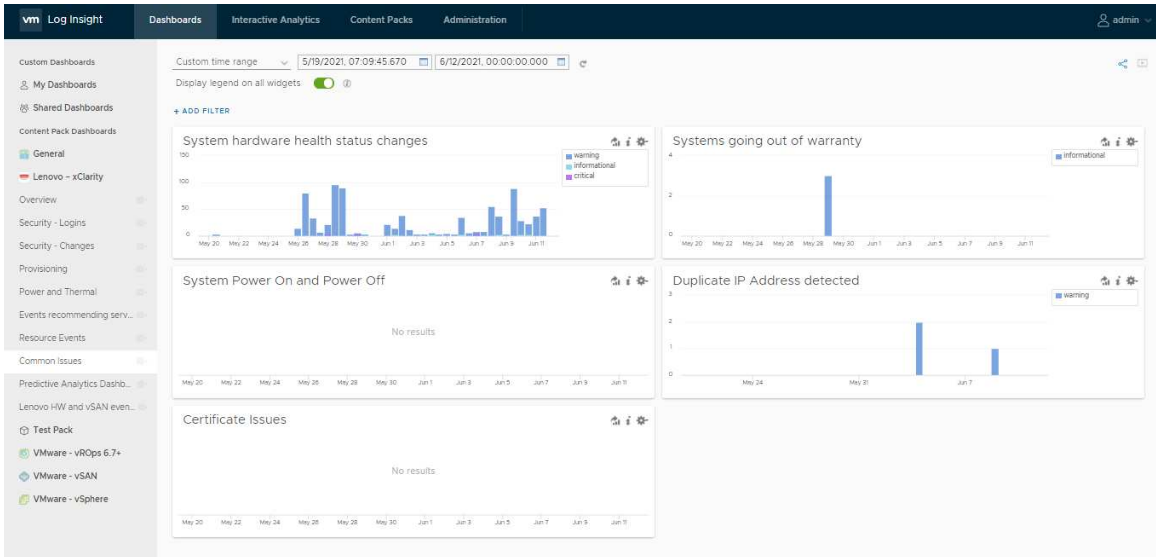


Events recommending service

Widget Name	Widget Type	Notes
Number of PFAs received by Lenovo XClarity Administrator over time	Chart	This graph shows how many predicted failure alerts (PFAs) occurred over time. PFAs can be an indication that hardware is more likely to experience a failure, but has not actually failed. A spike in these over multiple pieces of hardware can be an indication of an environmental issue. Compare this graph with the one above on serviceable events, to see how much delay there tends to be from a PFA event to a hard failure requiring service.
Critical errors from managed hardware	Chart	This graph shows how many critical errors were reported by Lenovo XClarity Administrator-managed endpoints over time. A spike in these over multiple pieces of hardware can be an indication of an environmental issue. You may want to consider setting alerts for these types of events.
Number of serviceable events, grouped by type of serviceability	Chart	This graph shows the number of serviceable events received by Lenovo XClarity Administrator's, grouped by whether the events are serviceable by the customer, or require the Support Center's assistance to service. This is useful in determining if there are any trends that show times where more hardware failures tend to occur.

Common Issues Dashboard

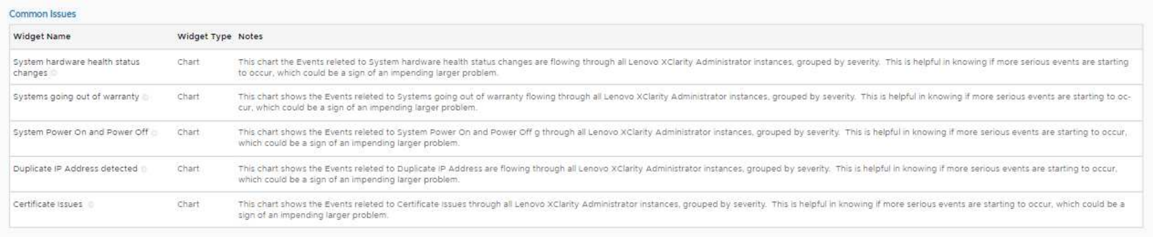
Lists the widgets that help in understanding the hardware health status, systems that would need attention as they are going out of warranty, systems that are power on or off, and has certificate issues.



Custom time range 5/19/2021, 07:09:45.670 6/12/2021, 00:00:00.000

Display legend on all widgets

The following table lists the widget names and their details:

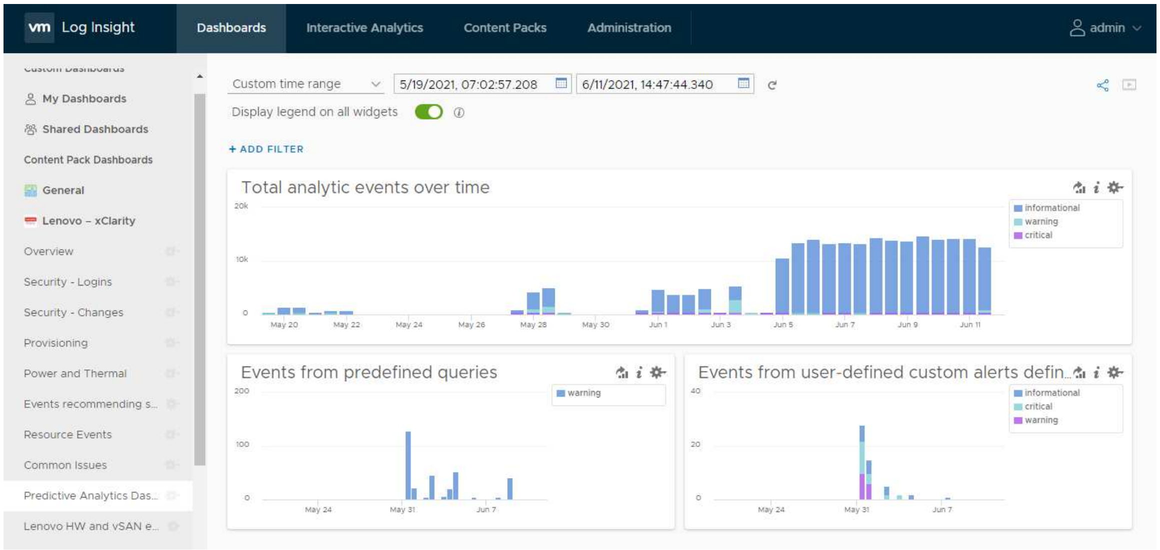


Common Issues

Widget Name	Widget Type	Notes
System hardware health status changes	Chart	This chart the Events releted to System hardware health status changes are flowing through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem.
Systems going out of warranty	Chart	This chart shows the Events releted to Systems going out of warranty flowing through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem.
System Power On and Power Off	Chart	This chart shows the Events releted to System Power On and Power Off g through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem.
Duplicate IP Address detected	Chart	This chart shows the Events releted to Duplicate IP Address are flowing through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem.
Certificate Issues	Chart	This chart shows the Events releted to Certificate Issues through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem.

Predictive Analytics Dashboard

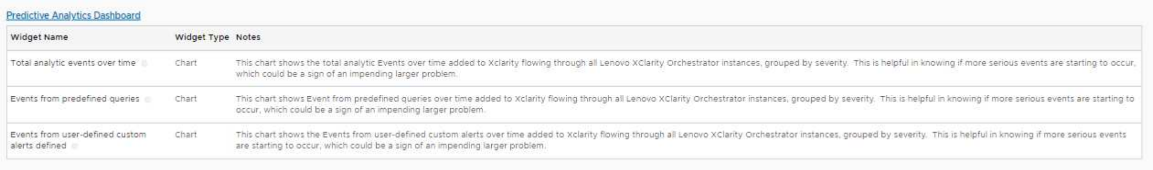
Lists the widgets that help in presenting the event analytics, events that are generated from predefined queries, user-defined alerts, and events that are triggered for known hardware issues.



Custom time range 5/19/2021, 07:02:57.208 6/11/2021, 14:47:44.340

Display legend on all widgets

The following table lists the widget names and their details:

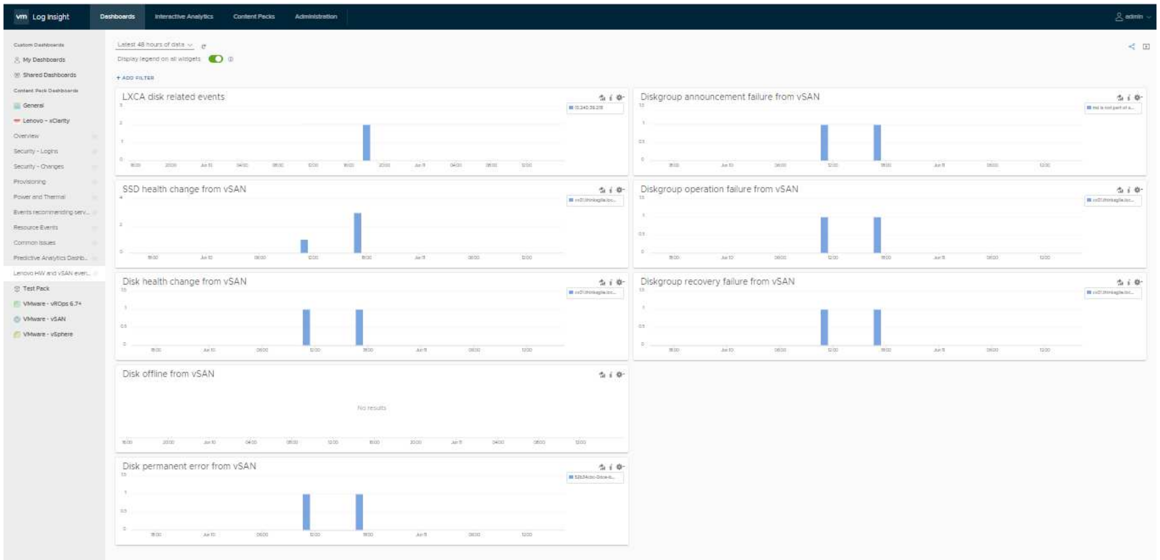


Predictive Analytics Dashboard

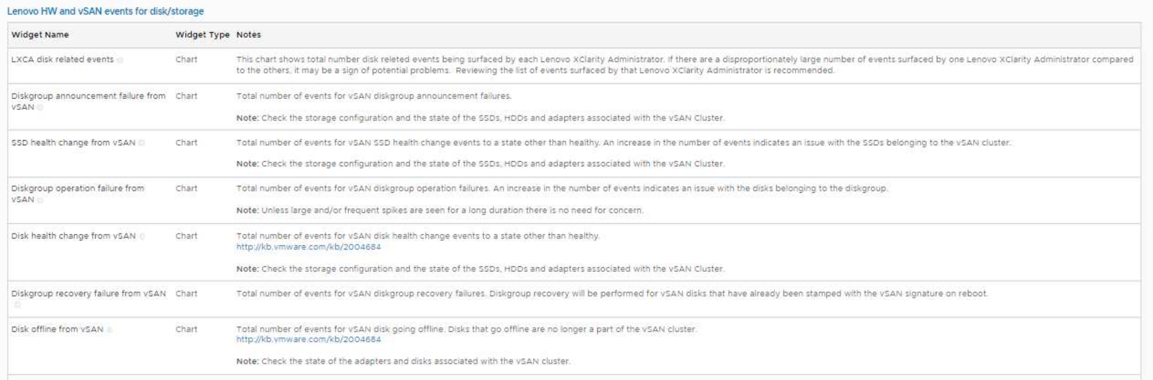
Widget Name	Widget Type	Notes
Total analytic events over time	Chart	This chart shows the total analytic Events over time added to Xclarity flowing through all Lenovo XClarity Orchestrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem.
Events from predefined queries	Chart	This chart shows Event from predefined queries over time added to Xclarity flowing through all Lenovo XClarity Orchestrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem.
Events from user-defined custom alerts defined	Chart	This chart shows the Events from user-defined custom alerts over time added to Xclarity flowing through all Lenovo XClarity Orchestrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem.

Lenovo HW and vSAN events Dashboard

List the widgets that help in understanding the LXCA events and health status of SSD, diskgroup, disks, etc.



The following table lists the widget names and their details:

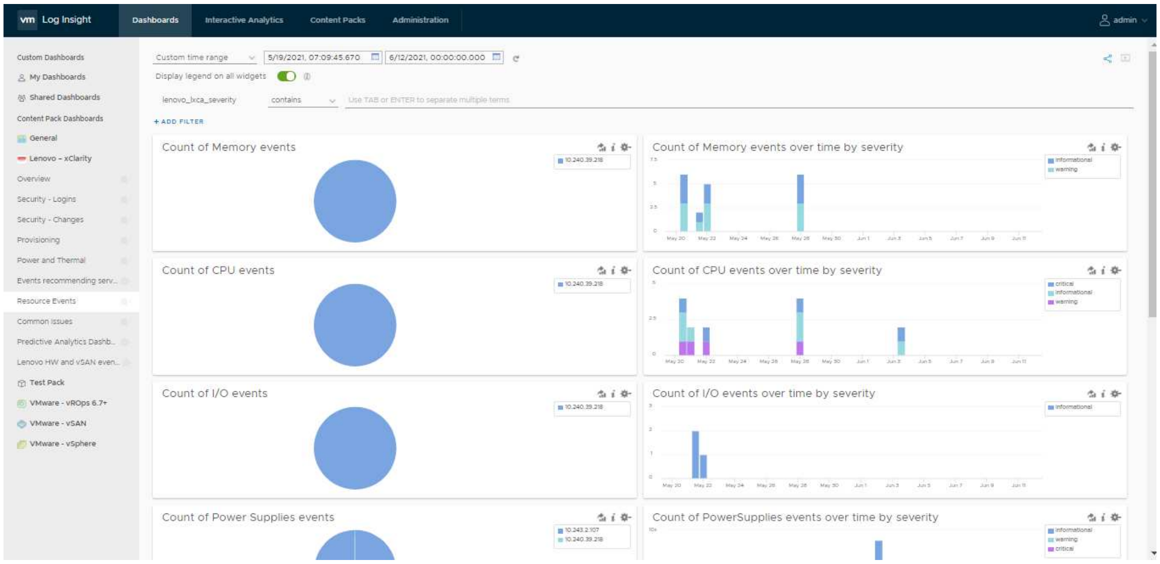


Lenovo HW and vSAN events for disk/storage

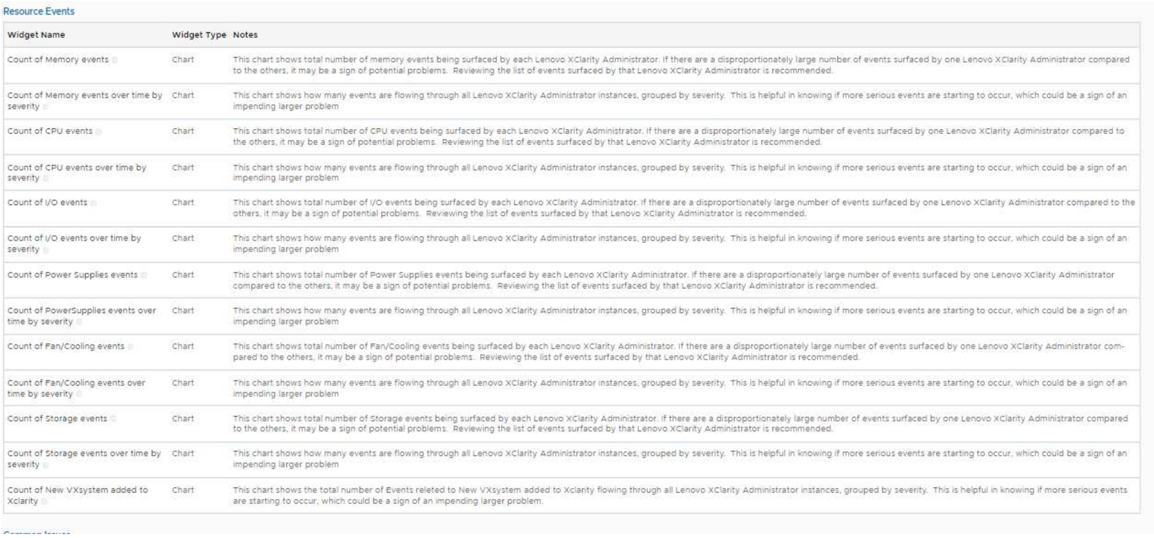
Widget Name	Widget Type	Notes
LXCA disk related events	Chart	This chart shows total number disk releted events being surfaced by each Lenovo XClarity Administrator. If there are a disproportionately large number of events surfaced by one Lenovo XClarity Administrator compared to the others, it may be a sign of potential problems. Reviewing the list of events surfaced by that Lenovo XClarity Administrator is recommended.
Diskgroup announcement failure from vSAN	Chart	Total number of events for vSAN diskgroup announcement failures. **Note:** Check the storage configuration and the state of the SSDs, HDDs and adapters associated with the vSAN Cluster.
SSD health change from vSAN	Chart	Total number of events for vSAN SSD health change events to a state other than healthy. An increase in the number of events indicates an issue with the SSDs belonging to the vSAN cluster. **Note:** Check the storage configuration and the state of the SSDs, HDDs and adapters associated with the vSAN Cluster.
Diskgroup operation failure from vSAN	Chart	Total number of events for vSAN diskgroup operation failures. An increase in the number of events indicates an issue with the disks belonging to the diskgroup. **Note:** Unless large and/or frequent spikes are seen for a long duration there is no need for concern.
Disk health change from vSAN	Chart	Total number of events for vSAN disk health change events to a state other than healthy. http://kb.vmware.com/kb/2004684 **Note:** Check the storage configuration and the state of the SSDs, HDDs and adapters associated with the vSAN Cluster.
Diskgroup recovery failure from vSAN	Chart	Total number of events for vSAN diskgroup recovery failures. Diskgroup recovery will be performed for vSAN disks that have already been stamped with the vSAN signature on reboot.
Disk offline from vSAN	Chart	Total number of events for vSAN disk going offline. Disks that go offline are no longer a part of the vSAN cluster. http://kb.vmware.com/kb/2004684 **Note:** Check the state of the adapters and disks associated with the vSAN cluster.

Resource Events Dashboard

Lists the widgets that help in understanding the memory, CPU, and I.O event count.



The following table lists the widget names and their details:



Resource Events

Widget Name	Widget Type	Notes
Count of Memory events	Chart	This chart shows total number of memory events being surfaced by each Lenovo XClarity Administrator. If there are a disproportionately large number of events surfaced by one Lenovo XClarity Administrator compared to the others, it may be a sign of potential problems. Reviewing the list of events surfaced by that Lenovo XClarity Administrator is recommended.
Count of Memory events over time by severity	Chart	This chart shows how many events are flowing through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem
Count of CPU events	Chart	This chart shows total number of CPU events being surfaced by each Lenovo XClarity Administrator. If there are a disproportionately large number of events surfaced by one Lenovo XClarity Administrator compared to the others, it may be a sign of potential problems. Reviewing the list of events surfaced by that Lenovo XClarity Administrator is recommended.
Count of CPU events over time by severity	Chart	This chart shows how many events are flowing through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem
Count of I/O events	Chart	This chart shows total number of I/O events being surfaced by each Lenovo XClarity Administrator. If there are a disproportionately large number of events surfaced by one Lenovo XClarity Administrator compared to the others, it may be a sign of potential problems. Reviewing the list of events surfaced by that Lenovo XClarity Administrator is recommended.
Count of I/O events over time by severity	Chart	This chart shows how many events are flowing through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem
Count of Power Supplies events	Chart	This chart shows total number of Power Supplies events being surfaced by each Lenovo XClarity Administrator. If there are a disproportionately large number of events surfaced by one Lenovo XClarity Administrator compared to the others, it may be a sign of potential problems. Reviewing the list of events surfaced by that Lenovo XClarity Administrator is recommended.
Count of PowerSupplies events over time by severity	Chart	This chart shows how many events are flowing through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem
Count of Fan/Cooling events	Chart	This chart shows total number of Fan/Cooling events being surfaced by each Lenovo XClarity Administrator. If there are a disproportionately large number of events surfaced by one Lenovo XClarity Administrator compared to the others, it may be a sign of potential problems. Reviewing the list of events surfaced by that Lenovo XClarity Administrator is recommended.
Count of Fan/Cooling events over time by severity	Chart	This chart shows how many events are flowing through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem
Count of Storage events	Chart	This chart shows total number of Storage events being surfaced by each Lenovo XClarity Administrator. If there are a disproportionately large number of events surfaced by one Lenovo XClarity Administrator compared to the others, it may be a sign of potential problems. Reviewing the list of events surfaced by that Lenovo XClarity Administrator is recommended.
Count of Storage events over time by severity	Chart	This chart shows how many events are flowing through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem
Count of New VXsystem added to Xclarity	Chart	This chart shows the total number of Events releted to New VXsystem added to Xclarity flowing through all Lenovo XClarity Administrator instances, grouped by severity. This is helpful in knowing if more serious events are starting to occur, which could be a sign of an impending larger problem.

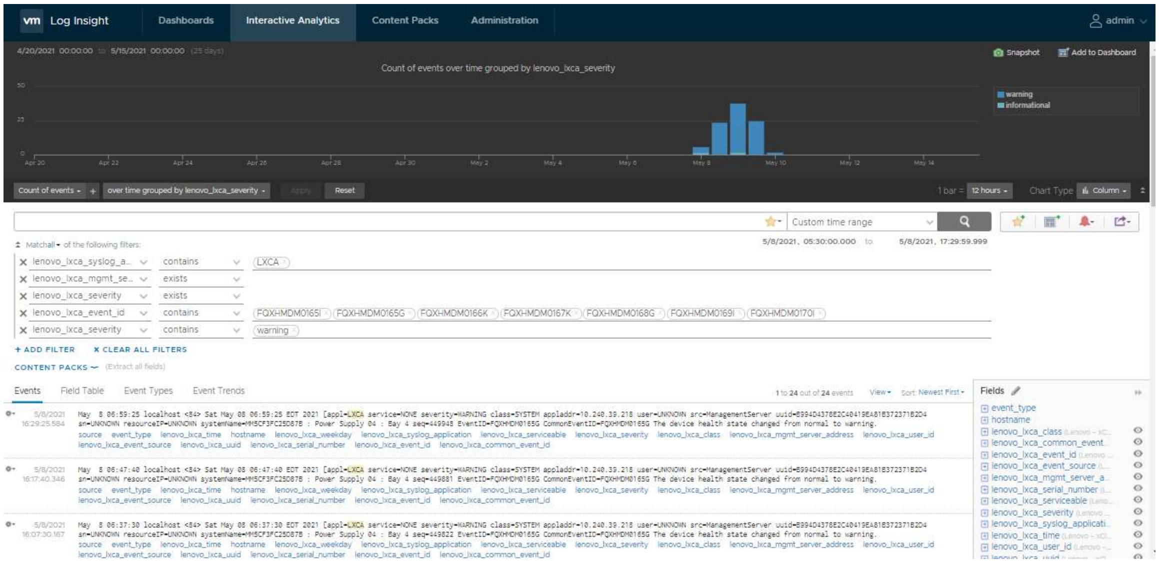
Viewing interactive analytics and alerts

The interactive analytics and alerts help you with information or warning messages. The alerts are triggered based on defined symptoms conditions such that when a metric value matches with a symptom, an alert is triggered. The alerts also include a short description of the alert.

Procedure

To view interactive analytics and alerts, complete the following steps.

1. Log in to vRLI as an admin user.
2. To view alerts, click **Interactive Analytics**. The count of events is displayed in graphical format.

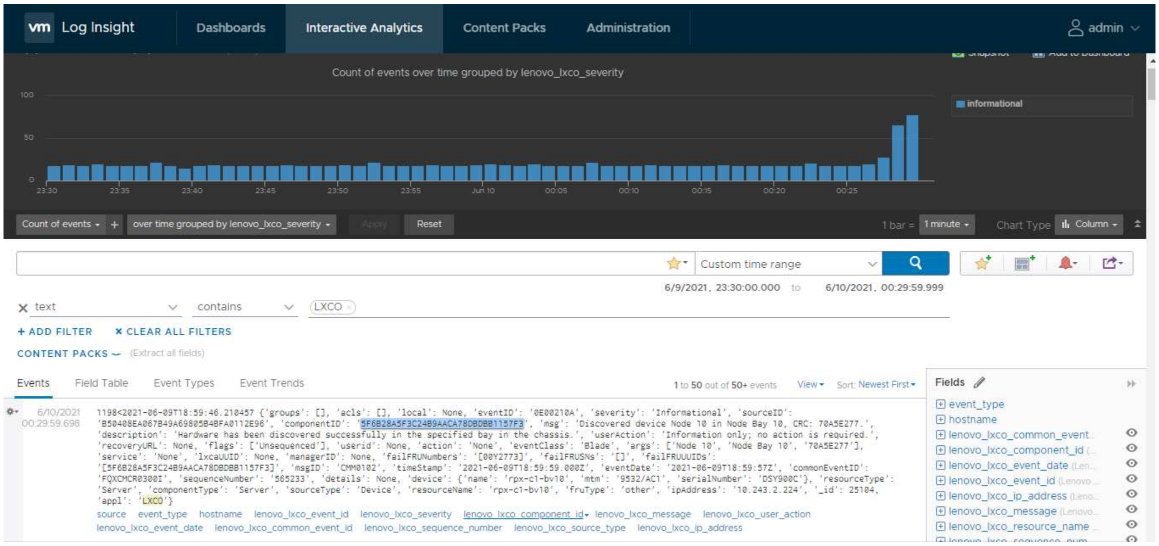

vm Log Insight
Dashboards
Interactive Analytics
Content Packs
Administration
admin
4/20/2021 00:00:00 to 5/15/2021 00:00:00 (25 days)
Snapshot
Add to Dashboard
Count of events over time grouped by lenovo_lxca_severity
warning
informational
50
25
0
Apr 20
Apr 22
Apr 24
Apr 26
Apr 28
Apr 30
May 2
May 4
May 6
May 8
May 10
May 12
May 14
Count of events
over time grouped by lenovo_lxca_severity
Apply
Reset
1 bar = 12 hours
Chart Type Column
Custom time range
5/8/2021, 05:30:00.000 to 5/8/2021, 17:29:59.999
Matchall of the following filters:
lenovo_lxca_syslog_a... contains LXCA
lenovo_lxca_mgmt_se... exists
lenovo_lxca_severity exists
lenovo_lxca_event_id contains FQXHMDM0165I FQXHMDM0165G FQXHMDM0166K FQXHMDM0167K FQXHMDM0168G FQXHMDM0169I FQXHMDM0170I
lenovo_lxca_severity contains warning
+ ADD FILTER
X CLEAR ALL FILTERS
CONTENT PACKS (Extract all fields)
Events
Field Table
Event Types
Event Trends
1 to 24 out of 24 events
View
Sort: Newest First
Fields
event_type
hostname
lenovo_lxca_class
lenovo_lxca_common_event...
lenovo_lxca_event_id
lenovo_lxca_event_source
lenovo_lxca_mgmt_server_a...
lenovo_lxca_serial_number
lenovo_lxca_serviceable
lenovo_lxca_severity
lenovo_lxca_syslog_applicati...
lenovo_lxca_time
lenovo_lxca_user_id

```
5/8/2021      May  8 06:59:25 localhost <84> Sat May 08 06:59:25 EDT 2021 [appl=LXCA service=NONE severity=WARNING class=SYSTEM appladdr=10.240.39.218 user=UNKNOWN src=ManagementServer uuid=B994D4378E2C40419EA818372371B2D4
16:29:25.584  sn=UNKNOWN resourceIP=UNKNOWN systemName=MM5CF3FC25D87B : Power Supply 04 : Bay 4 seq=449948 EventID=FQXHMDM0165G CommonEventID=FQXHMDM0165G The device health state changed from normal to warning.
              source event_type lenovo_lxca_time hostname lenovo_lxca_weekday lenovo_lxca_syslog_application lenovo_lxca_serviceable lenovo_lxca_severity lenovo_lxca_class lenovo_lxca_mgmt_server_address lenovo_lxca_user_id
              lenovo_lxca_event_source lenovo_lxca_uuid lenovo_lxca_serial_number lenovo_lxca_event_id lenovo_lxca_common_event_id

5/8/2021      May  8 06:47:40 localhost <84> Sat May 08 06:47:40 EDT 2021 [appl=LXCA service=NONE severity=WARNING class=SYSTEM appladdr=10.240.39.218 user=UNKNOWN src=ManagementServer uuid=B994D4378E2C40419EA818372371B2D4
16:17:40.346  sn=UNKNOWN resourceIP=UNKNOWN systemName=MM5CF3FC25D87B : Power Supply 04 : Bay 4 seq=449881 EventID=FQXHMDM0165G CommonEventID=FQXHMDM0165G The device health state changed from normal to warning.
              source event_type lenovo_lxca_time hostname lenovo_lxca_weekday lenovo_lxca_syslog_application lenovo_lxca_serviceable lenovo_lxca_severity lenovo_lxca_class lenovo_lxca_mgmt_server_address lenovo_lxca_user_id
              lenovo_lxca_event_source lenovo_lxca_uuid lenovo_lxca_serial_number lenovo_lxca_event_id lenovo_lxca_common_event_id

5/8/2021      May  8 06:37:30 localhost <84> Sat May 08 06:37:30 EDT 2021 [appl=LXCA service=NONE severity=WARNING class=SYSTEM appladdr=10.240.39.218 user=UNKNOWN src=ManagementServer uuid=B994D4378E2C40419EA818372371B2D4
16:07:30.167  sn=UNKNOWN resourceIP=UNKNOWN systemName=MM5CF3FC25D87B : Power Supply 04 : Bay 4 seq=449822 EventID=FQXHMDM0165G CommonEventID=FQXHMDM0165G The device health state changed from normal to warning.
              source event_type lenovo_lxca_time hostname lenovo_lxca_weekday lenovo_lxca_syslog_application lenovo_lxca_serviceable lenovo_lxca_severity lenovo_lxca_class lenovo_lxca_mgmt_server_address lenovo_lxca_user_id
              lenovo_lxca_event_source lenovo_lxca_uuid lenovo_lxca_serial_number lenovo_lxca_event_id lenovo_lxca_common_event_id
```

Figure 1. Interactive analytics of total analytic events over time for LXCA



```
6/10/2021     1198<2021-06-09T18:59:46.210457 {'groups': [], 'acls': [], 'local': None, 'eventID': '0E00210A', 'severity': 'Informational', 'sourceID':
00:29:59.698  'B50408EA067B49A69805B4BFA0112E96', 'componentID': '5F6B28A5F3C24B9AACA78DBDBB1157F3', 'msg': 'Discovered device Node 10 in Node Bay 10, CRC: 70A5E277.',
              'description': 'Hardware has been discovered successfully in the specified bay in the chassis.', 'userAction': 'Information only; no action is required.',
              'recoveryURL': None, 'flags': ['Unsequenced'], 'userid': None, 'action': 'None', 'eventClass': 'Blade', 'args': ['Node 10', 'Node Bay 10', '70A5E277'],
              'service': 'None', 'lxcaUUID': None, 'managerID': None, 'failFRUNumbers': '[00Y2773]', 'failFRUSNs': '[]', 'failFRUUUIDs':
              '[5F6B28A5F3C24B9AACA78DBDBB1157F3]', 'msgID': 'CMM0102', 'timeStamp': '2021-06-09T18:59:59.000Z', 'eventDate': '2021-06-09T18:59:57Z', 'commonEventID':
              'FQXCMCR0300I', 'sequenceNumber': '565233', 'details': None, 'device': {'name': 'rpx-c1-bv10', 'mtm': '9532/AC1', 'serialNumber': 'DSY900C'}, 'resourceType':
              'Server', 'componentType': 'Server', 'sourceType': 'Device', 'resourceName': 'rpx-c1-bv10', 'fruType': 'other', 'ipAddress': '10.243.2.224', '_id': 25104,
              'appl': 'LXCO'}
              source event_type hostname lenovo_lxco_event_id lenovo_lxco_severity lenovo_lxco_component_id lenovo_lxco_message lenovo_lxco_user_action
              lenovo_lxco_event_date lenovo_lxco_common_event_id lenovo_lxco_sequence_number lenovo_lxco_source_type lenovo_lxco_ip_address
```

Figure 2. Interactive analytics of total analytic events over time for LXCO

Fields

The following table lists the various LXCA fields that are used in the vRLI:

Field name	Regex	Notes
lenovo_lxca_class	Letters, Digits, and Underscores and \w+	Pre and post context(regexes)are "class=" and " " and Additional context is "LXCA"
lenovo_lxca_common_event_id	Letters, Digits, and Underscores and \w+	Pre and post context(regexes)are "CommonEventID=" and " " and Additional context is "LXCA"

Field name	Regex	Notes
lenovo_lxca_event_id	Any Character except whitespace and \S+	Pre and post context(regexes)are "EventID=" and " " and Additional context is "LXCA"
lenovo_lxca_event_source	Letters, Digits, and Underscores and \w+	Pre and post context(regexes)are "src=" and " " and Additional context is "LXCA"
lenovo_lxca_mgmt_server_address	IP Address(v4) and \d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}	Pre and post context(regexes)are "appladdr=" and " " and Additional context is "LXCA"
lenovo_lxca_serial_number	Letters, Digits, and Underscores and \w+	Pre and post context(regexes)are "sn=" and " " and Additional context is "LXCA"
lenovo_lxca_serviceable	Letters, Digits, and Underscores and \w+	Pre and post context(regexes)are "service=" and " " and Additional context is "LXCA"
lenovo_lxca_severity	Letters, Digits, and Underscores and \w+	Pre and post context(regexes)are "severity=" and " " and Additional context is "LXCA"
lenovo_lxca_syslog_application	Letters, Digits, and Underscores and \w+	Pre and post context(regexes)are "appl=" and " " and Additional context is "LXCA"
lenovo_lxca_target_ipv6_address	IP Address(v6) and [A-Fa-f0-9]{0,4}:([A-Fa-f0-9]{0,4}:){1,6}[A-Fa-f0-9]{1,4}	Pre and post context(regexes)are "address " and " " and Additional context is "LXCA"
lenovo_lxca_time	Custom Regex... and [0-9]{2}:[0-9]{2}:[0-9]{2}	Pre and post context(regexes)are " " and " " and Additional context is "LXCA"
lenovo_lxca_user_id	Letters, Digits, and Underscores and \w+	Pre and post context(regexes)are " user" and " " and Additional context is "LXCA"
lenovo_lxca_uuid	Hexadecimal and [A-Fa-f0-9]+	Pre and post context(regexes)are " uuid" and " " and Additional context is "LXCA"
lenovo_lxca_weekday	Letters, Digits, and Underscores and \w+	Pre and post context(regexes)are "(<86>|<83>|<84>) " and " " and Additional context is "LXCA"

The following table lists the various LXCA fields that are used in the vRLI:

Field name	Regex	Notes
lenovo_lxco_common_event_id	Letters, Digits, and Underscores and \w+	Pre and post context(regexes)are 'commonEventID': ' and ', and Additional context is LXCO
lenovo_lxco_event_id	Letters, Digits, and Underscores and \w+	Pre and post context(regexes) are 'eventID': ' and ', and Additional context is LXCO
lenovo_lxco_component_id	Hexadecimal and [A-Fa-f0-9]+	Pre and post context(regexes) are 'componentID': ' and ', and Additional context is LXCO

Field name	Regex	Notes
lenovo_lxco_event_date	Any character except Whitespace and \S+	Pre and post context(regexes) are 'eventDate': ' and ', and Additional context is LXCO
lenovo_lxco_ip_address	IP address(v4) and \d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}	Pre and post context(regexes) are 'ipAddress': ' and ', and Additional context is LXCO
lenovo_lxco_message	Custom regex... and [A-Za-z0-9 .]+	Pre context(regexes) is 'msg': ' and Additional context is LXCO
lenovo_lxco_severity	Letters, Digits, and Underscores and \w+	Pre and post context(regexes) are 'severity': ' and ', and Additional context is LXCO
lenovo_lxco_resource_name	Custom regex... and .[A-Za-z0-9 .]+	Pre context(regexes) is 'resourceName': ' and Additional context is LXCO
lenovo_lxco_user_action	Custom regex... and [A-Za-z0-9 ./;]+	Pre context(regexes) is 'userAction': ' and Additional context is LXCO
lenovo_lxco_sequence_number	Letters, Digits, and Underscores and \w+	Pre and post context(regexes) are 'sequenceNumber': ' and ', and Additional context is LXCO
lenovo_lxco_source_type	Letters, Digits, and Underscores and \w+	Pre and post context(regexes) are 'sourceType': ' and ', and Additional context is LXCO

Logs

LXCA receives events from different types of managed resources. It transforms them into a common format so that the log output from XClarity Administrator looks similar. The general format is:

```
<Severity code><Date/Time stamp> [appl=LXCA service=<serviceability> severity=<log severity> class=
<type of event> appladdr=<IPaddress of LXCA> src=<type of endpoint> uuid=<unique identifier> sn=<serial
number> seq=<sequence number> EventID=<event ID>] <Message>
```

Where

- `<Severity code>` depicts the code specifying the error, warning, or information.
- `<Date/Time stamp>` depicts the date and time when the message was surfaced.
- `appl=LXCA` depicts that the event came from an XClarity Administrator.
- `service=<serviceability>` depicts if this is a Serviceable event or not.
- `severity=<log severity>` depicts Error, Warning, or Informational.
- `class=<type of event>` depicts categorization of the type of endpoint.
- `appladdr=<IPaddress of LXCA>` depicts the IP address of the XClarity Administrator.
- `src=<type of endpoint>` depicts the general type of endpoint.
- `uuid=<unique identifier>` depicts a unique identifier for the managed endpoint.
- `sn=<serial number>` depicts the serial number of the managed endpoint
- `seq=<sequence number>` depicts the sequence number of the event from the endpoint. You can use this number to determine if an event is missing.
- `EventID=<event ID>` depicts the Event ID.
- `<Message>` depicts the text describing the specific event that occurred.

Here is an example for LXCA:

```
<84> Sat May 08 06:59:25 EDT 2021 [appl=LXCA service=NONE severity=WARNING class=SYSTEM appladdr=
10.240.39.218 user=UNKNOWN src=ManagementServer uuid=B994D4378E2C40419EA81B372371B2D4 sn=UNKNOWN
resourceIP=UNKNOWN systemName=MM5CF3FC25D87B : Power Supply 04 : Bay 4 seq=449948 EventID=
FQXHMDM0165G

CommonEventID=FQXHMDM0165G The device health state changed from normal to warning.
```

Here is an example for LXCO:

```
978<2021-06-07T11:59:44.438771 {'groups': [], 'acls': [], 'local': None, 'eventID': 'FQXHMJM0002I', 'severity':
'Informational', 'sourceID': 'FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF', 'componentID':
'FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF', 'msg': 'Job 889 was updated.', 'description': 'A job was updated.',
'userAction': 'N/A', 'recoveryURL': None, 'flags': ['Hidden'], 'userid': None, 'action': 'None', 'eventClass':
'System', 'args': ['889'], 'service': 'None', 'lxcaUUID': None, 'managerID': None, 'failFRUNumbers': None,
'failFRUSNs': None, 'failFRUUUIDs': '[FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF]', 'msgID': None, 'timeStamp': '2021-
06-07T11:59:55Z', 'eventDate': '2021-06-07T11:59:55Z', 'commonEventID': 'FQXHMJM0002I',
'sequenceNumber': None, 'details': None, 'device': {'name': None, 'mtm': None, 'serialNumber': None},
'resourceType': None, 'componentType': None, 'sourceType': 'Management', 'resourceName': 'Not Available',
'fruType': 'other', 'ipAddress': '10.240.54.38', 'appl': 'LXCO'}
```

Appendix A. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

Lenovo and the Lenovo logo are trademarks of Lenovo in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Lenovo