Update picture with course product picture (Optional) or Delete

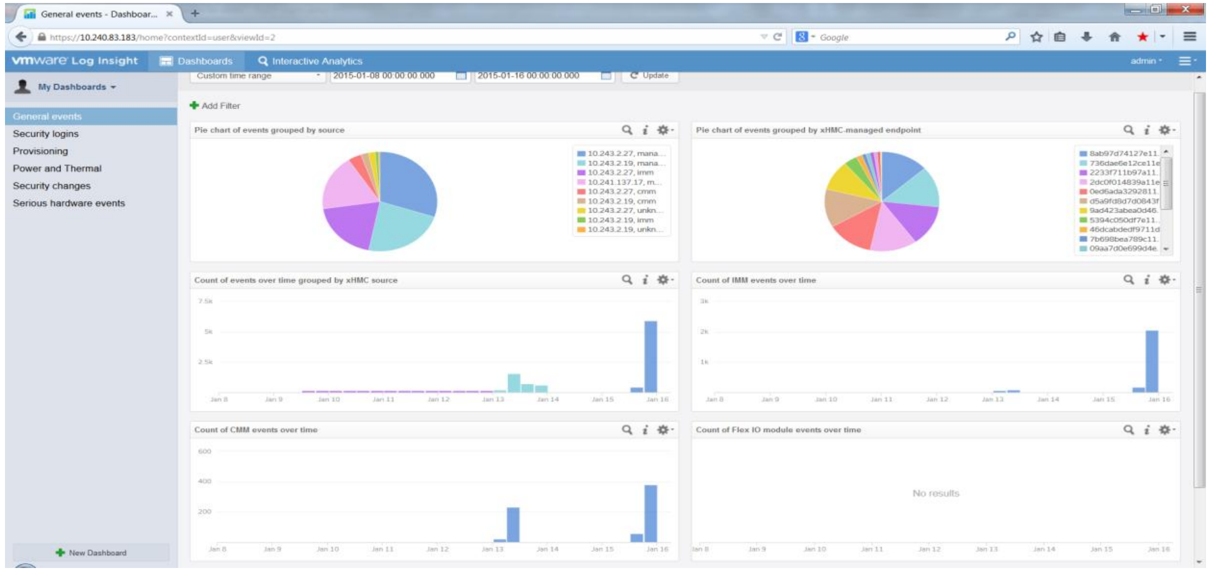
EBG Server Education - XClarity Administrator - VMWare vRealize Log Insight Content Pack

Jeff Van Heuklon | RAS architect – 4/15/15

Overview and Development work performed

What is VMWare vRealize Log Insight?

- Log Insight provides scalable log aggregation and indexing, with near real-time search and analytics capabilities.
- Log Insight collects, imports, and analyzes logs to provide real-time answers to problems related to systems, services, and applications, and derive important insights.



Value of XClarity Administrator integration with VMWare vRealize Log Insight

- Shows the value of XClarity Administrator for monitoring, by providing analytics based on its events, and the events forwarded from managed endpoints
- Shows users how to create simple queries of event data to build reports that they need
- Provides a historical view of events generated by XClarity, showing trends over time.

lenovo

Distribution and Support

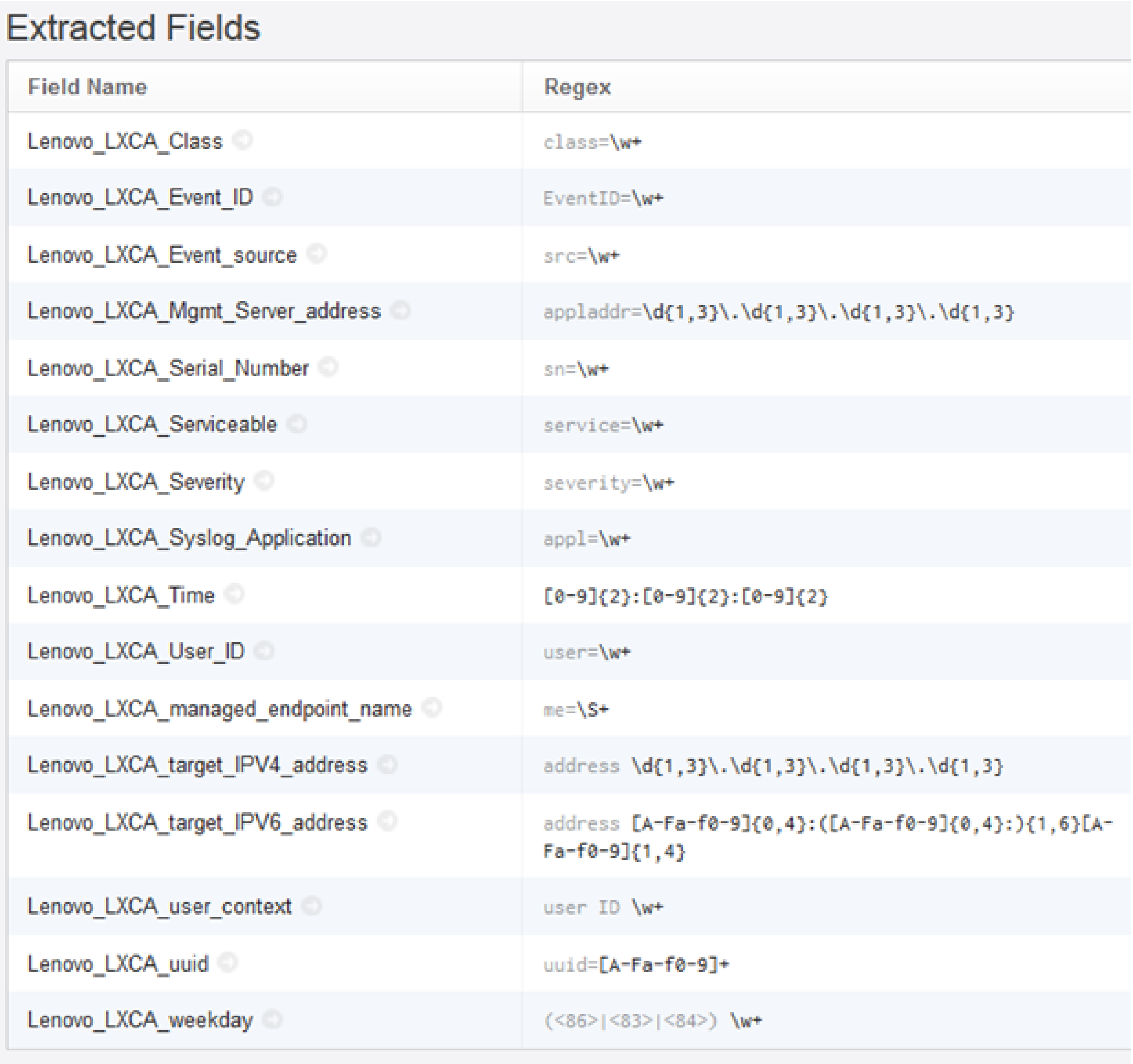
- The XClarity Administrator content pack for VMWare vRealize Log Insight will be distributed on the VMware solution exchange (VSX) website
  - The Lenovo Networking content pack was released in the same manner in December

- No support is being provided. This will be "as-is" for customers. (Same as the Networking pack)

- In the future, it could be decided to tie support to customers with XClarity support contracts if desired.

XClarity Administrator content pack for VMWare vRealize Log Insight

- Log Insights content pack customizes view for XClarity-forwarded events (via Syslog)
  - Extracted event fields that are unique to System x and XClarity
  - Dashboards for different categories
  - Graphs that analyze the event data, to provide visual insights to system administrators
  - Added sample alerts

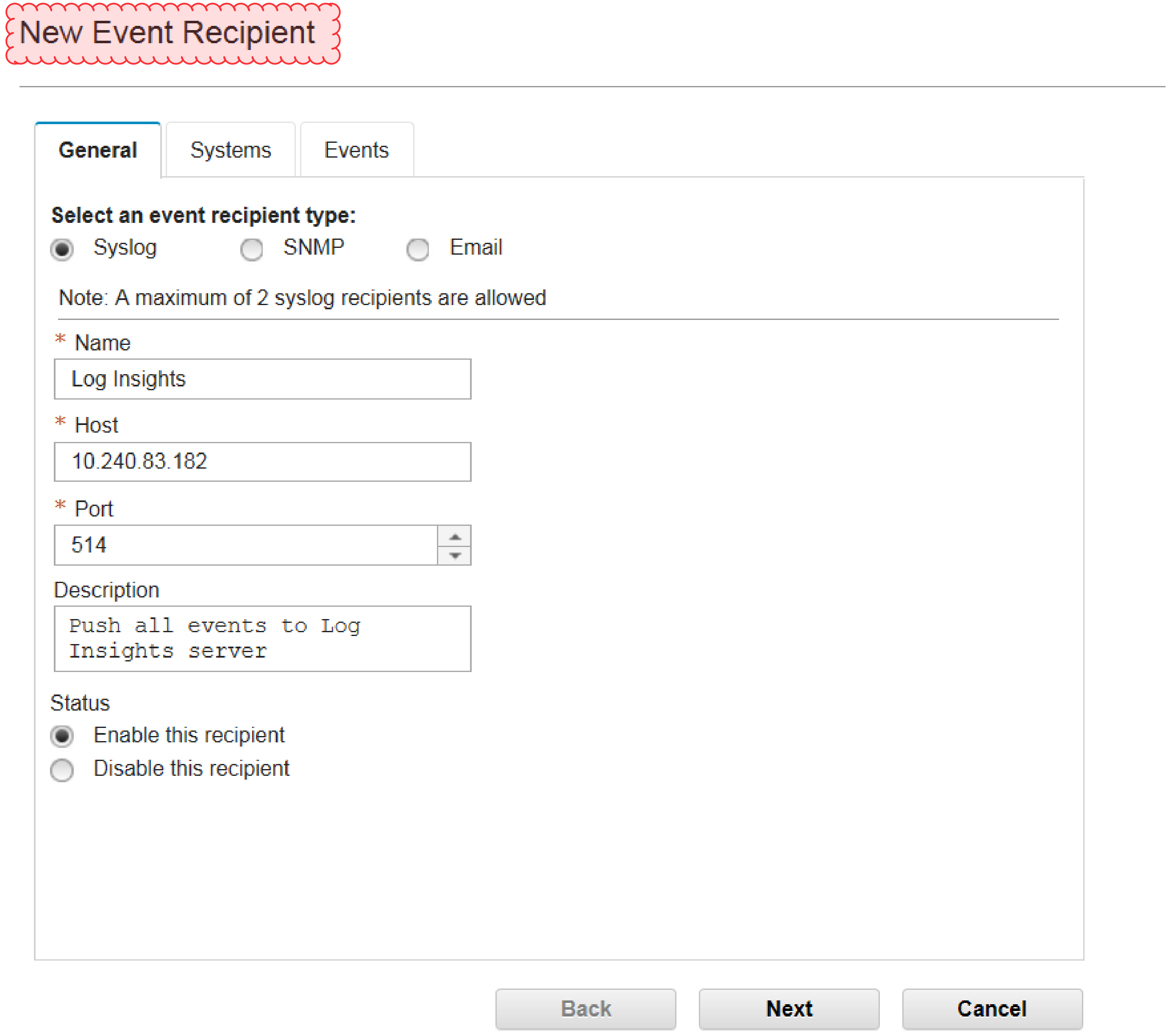


Extracted Fields

Field Name	Regex
Lenovo_LXCA_Class	class=\w+
Lenovo_LXCA_Event_ID	EventID=\w+
Lenovo_LXCA_Event_source	src=\w+
Lenovo_LXCA_Mgmt_Server_address	appladdr=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
Lenovo_LXCA_Serial_Number	sn=\w+
Lenovo_LXCA_Serviceable	service=\w+
Lenovo_LXCA_Severity	severity=\w+
Lenovo_LXCA_Syslog_Application	appl=\w+
Lenovo_LXCA_Time	[0-9]{2}:[0-9]{2}:[0-9]{2}
Lenovo_LXCA_User_ID	user=\w+
Lenovo_LXCA_managed_endpoint_name	me=\S+
Lenovo_LXCA_target_IPV4_address	address \d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
Lenovo_LXCA_target_IPV6_address	address [A-Fa-f0-9]{0,4}:([A-Fa-f0-9]{0,4}:){1,6}[A-Fa-f0-9]{1,4}
Lenovo_LXCA_user_context	user ID \w+
Lenovo_LXCA_uuid	uuid=[A-Fa-f0-9]+
Lenovo_LXCA_weekday	(<86>|<83>|<84>) \w+

Configure XClarity syslog event forwarder to Log Insights

- From XCLarity Administrator toolbar, click on Monitoring -> Event Forwarding
- Click on "New" icon to create new forwarder
- Select "Syslog" as the recipient type
- Fill in the IP address and port number of Log Insight server
- Click 'Next' to select the systems to forward events for
- Click 'Next' to select the types of events to forward



New Event Recipient

Select an event recipient type:

● Syslog ○ SNMP ○ Email

Note: A maximum of 2 syslog recipients are allowed

* Name

Log Insights

* Host

10.240.83.182

* Port

514

Description

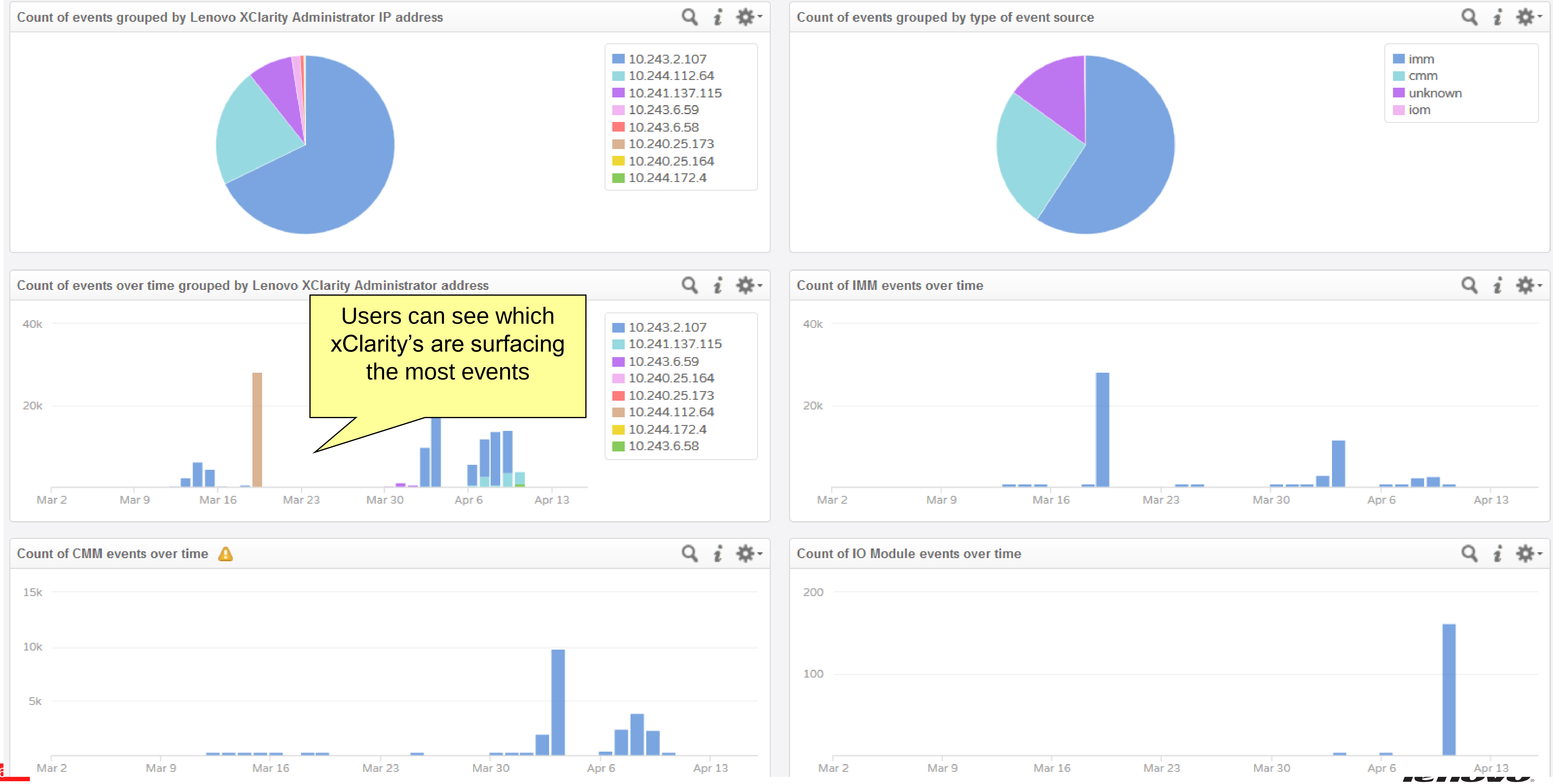
Push all events to Log Insights server

Status

● Enable this recipient

○ Disable this recipient

XClarity General Events



Count of events grouped by Lenovo XClarity Administrator IP address

Count of events grouped by type of event source

Count of events over time grouped by Lenovo XClarity Administrator address

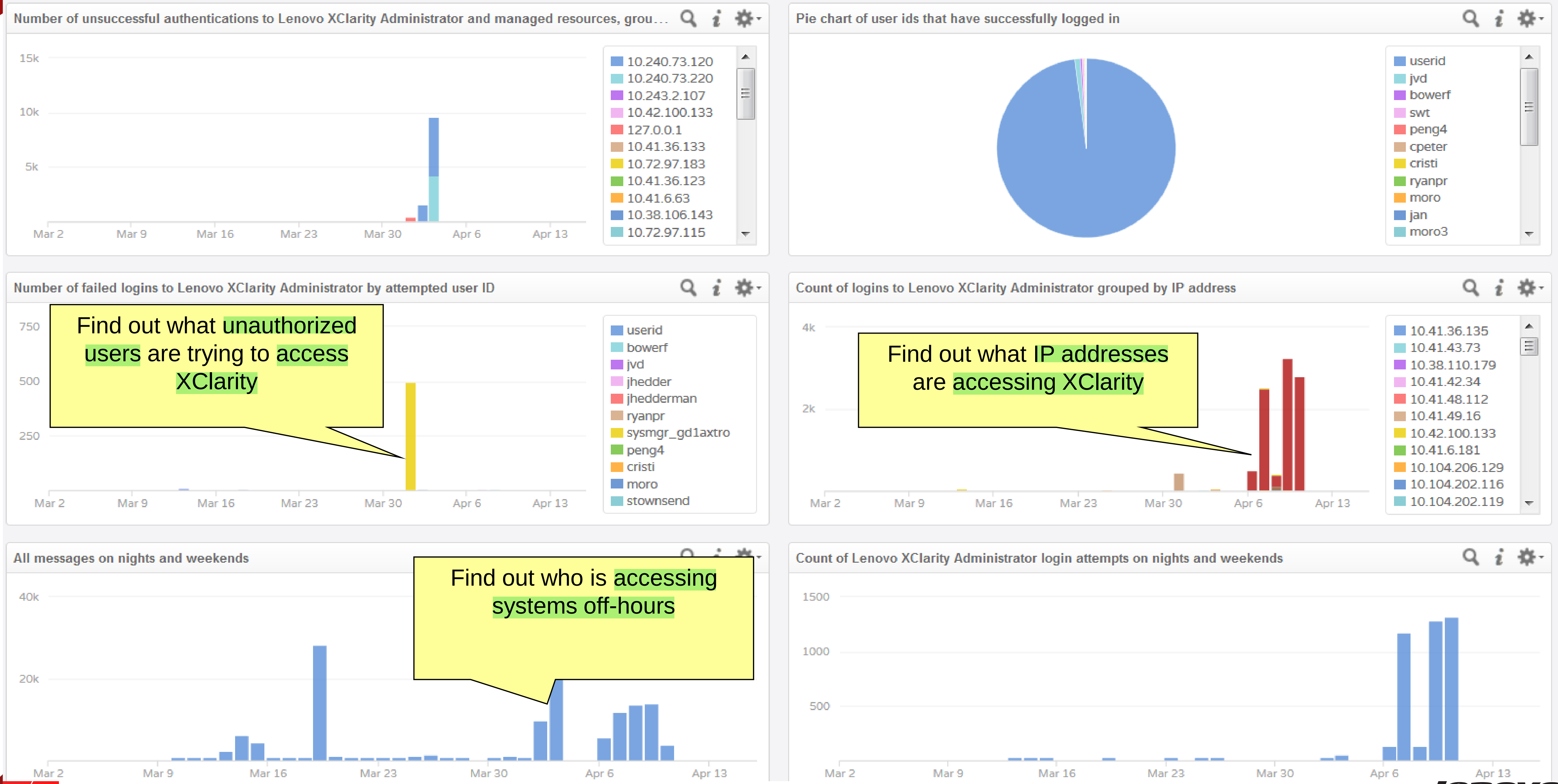
Users can see which xClarity's are surfacing the most events

Count of IMM events over time

Count of CMM events over time

Count of IO Module events over time

XClarity Security - Logins



Number of unsuccessful authentications to Lenovo XClarity Administrator and managed resources, grou…

Pie chart of user ids that have successfully logged in

Number of failed logins to Lenovo XClarity Administrator by attempted user ID

Find out what unauthorized users are trying to access XClarity

Count of logins to Lenovo XClarity Administrator grouped by IP address

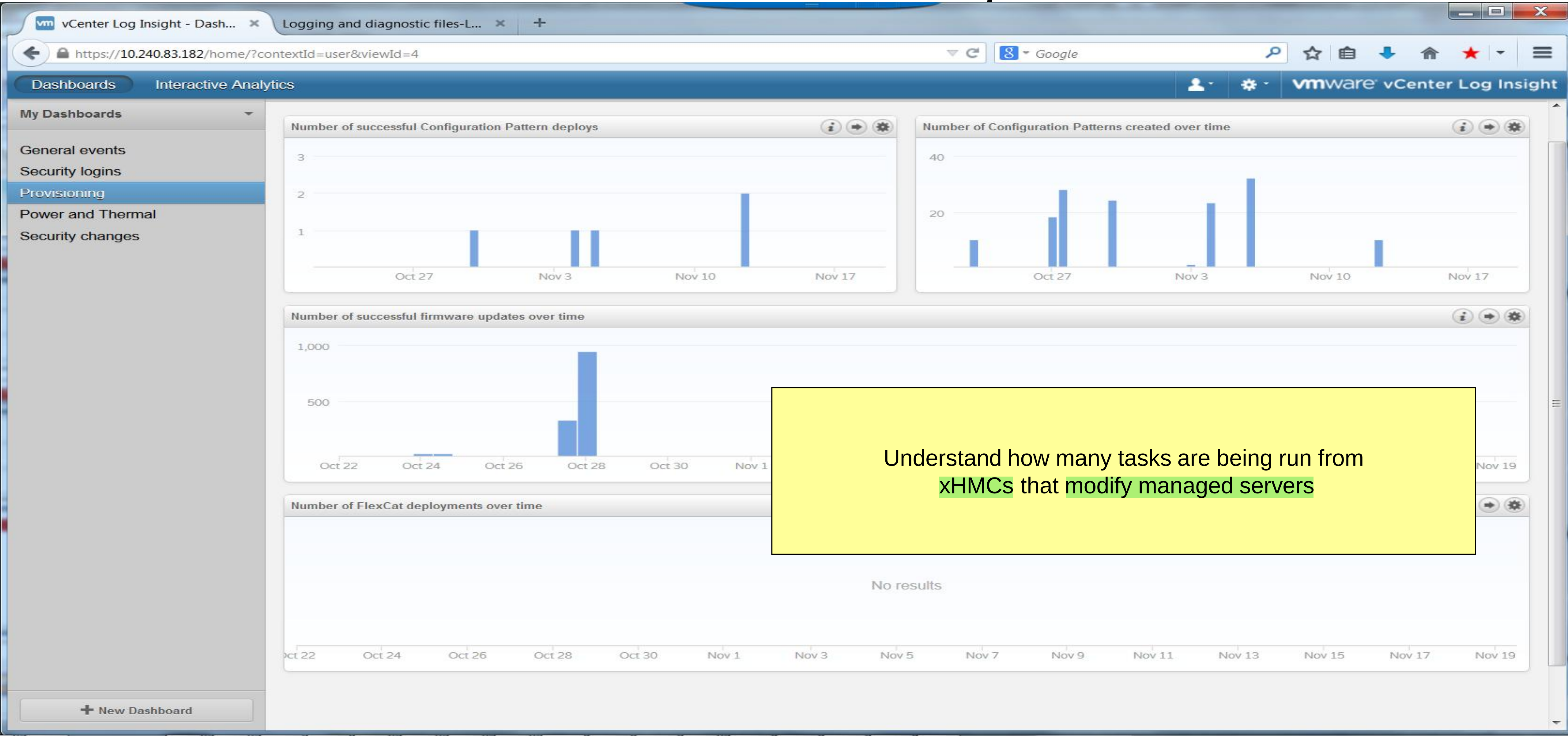
Find out what IP addresses are accessing XClarity

All messages on nights and weekends

Find out who is accessing systems off-hours

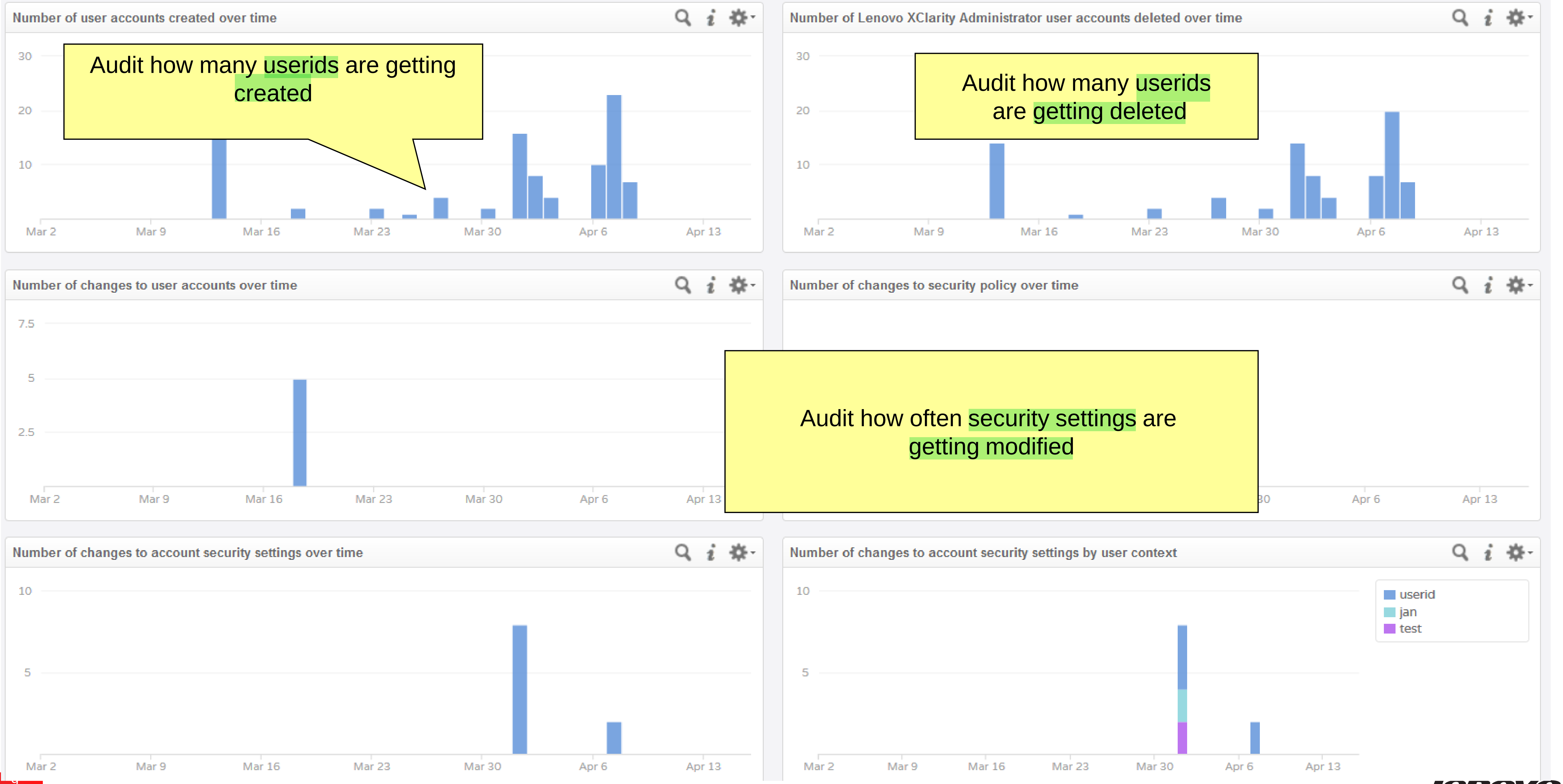
Count of Lenovo XClarity Administrator login attempts on nights and weekends

xHMC Provisioning



Understand how many tasks are being run from xHMCs that modify managed servers

XClarity Security Changes



Number of user accounts created over time

Audit how many userids are getting created

Number of Lenovo XClarity Administrator user accounts deleted over time

Audit how many userids are getting deleted

Number of changes to user accounts over time

Number of changes to security policy over time

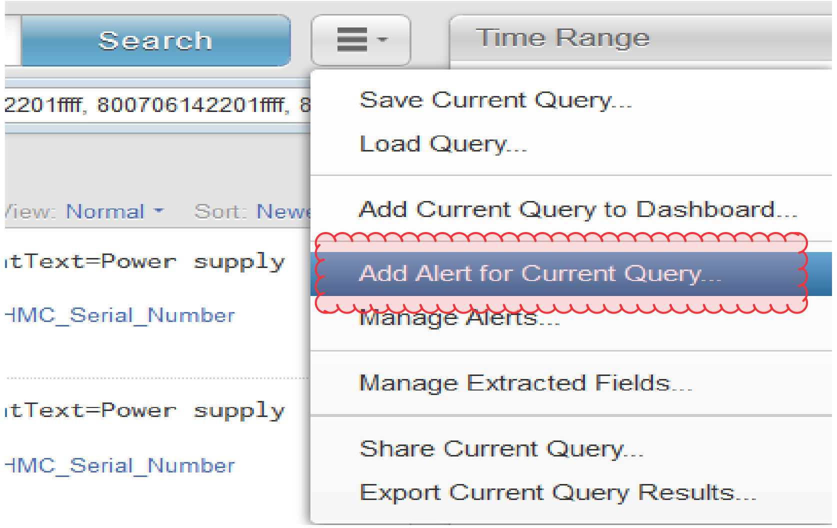
Audit how often security settings are getting modified

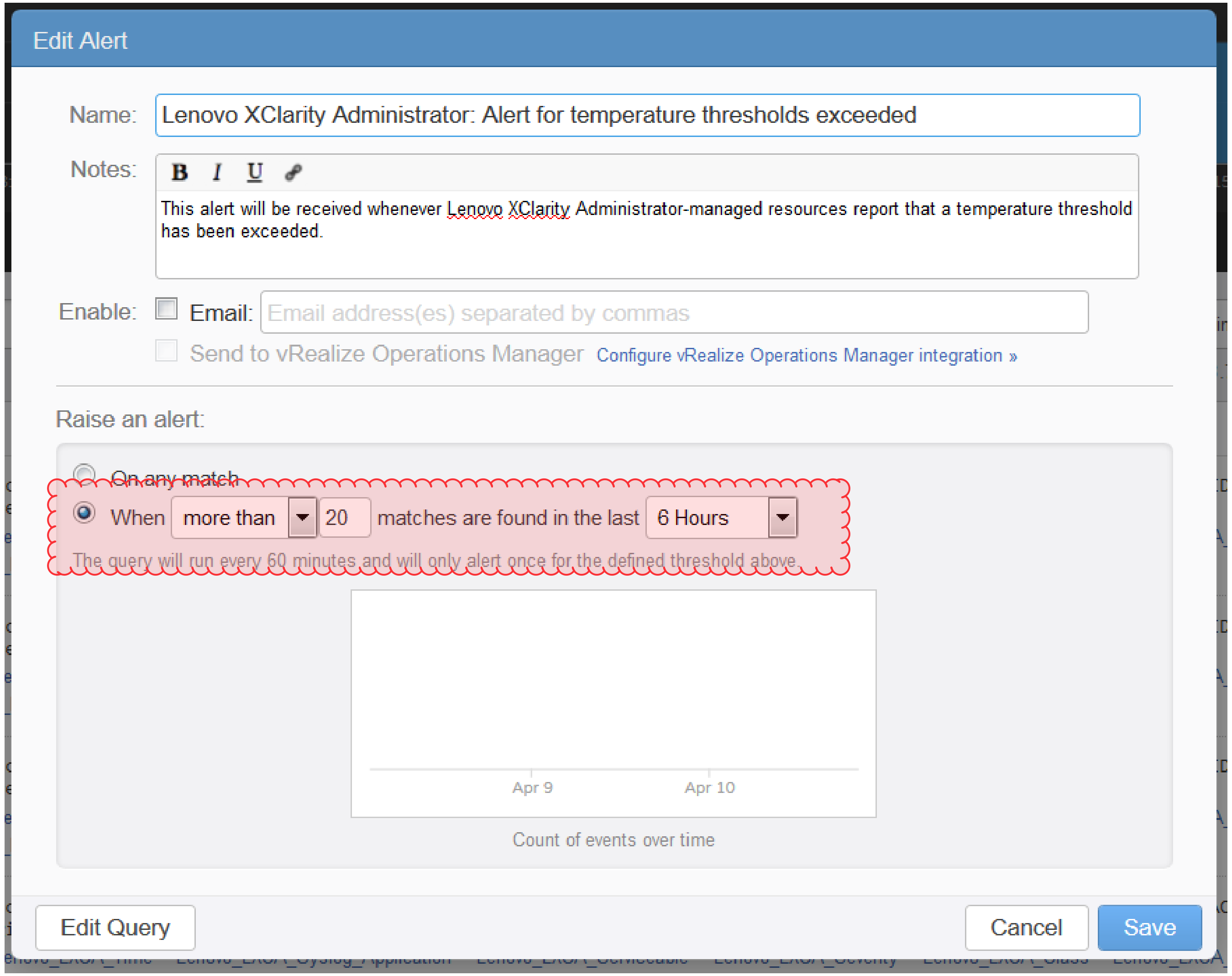
Number of changes to account security settings over time

Number of changes to account security settings by user context

Alerts

- Can configure alerts when a condition occurs





Edit Alert

Name: Lenovo XClarity Administrator: Alert for temperature thresholds exceeded

Notes: This alert will be received whenever Lenovo XClarity Administrator-managed resources report that a temperature threshold has been exceeded.

Enable: □ Email: Email address(es) separated by commas

□ Send to vRealize Operations Manager Configure vRealize Operations Manager integration »

Raise an alert:

○ On any match

● When more than 20 matches are found in the last 6 Hours

The query will run every 60 minutes and will only alert once for the defined threshold above.

Troubleshooting content pack

- Symptom: No events are not being received by Log Insight
  - Action: Ensure correct IP address and port were configured for XClarity event forwarder. Ensure no firewalls are blocking traffic
- Symptom: Security events are not being received by Log Insight
  - Action: Ensure that “audit events” were selected when configuring XClarity event forwarder
- Symptom: Users wants additional event ID’s to be surfaced in a graph
  - Action: Using Infocenter, find the event ID’s that match what the customer wants. Then select a graph, select “Edit query”. Add a query for the field “Lenovo_LXCA_Event_ID that contains the event ID desired. Click on “Save”
- Symptom: Events shows up in the “Interactive Analytics” view, but not in a graph
  - Action: Check the scale of the graph. If there were thousand of entries in a graph, the scale may be such that you can’t see a couple events on a particular day on the graph

THANK YOU GRAZIE MERCI DANKE GRAZIAS 謝謝 СПАСИБО

GRACIAS OBRIGADO ありがとう DANK TAKK BEDANKT DAKUJEM