



Lenovo XClarity Administrator app for Splunk

Author : Lenovo

Table of Contents

1. Introduction.....	2
2. Lenovo XClarity Administrator app for Splunk Overview	2
Dashboards.....	3
Technical Specifications	4
3. Installing the XClarity Administrator Splunk app	4
Import the XClarity Administrator app into Splunk	5
Changing the data input settings	8
Configuring Lenovo XClarity Administrator to forward logs to Splunk	9
4. Lenovo XClarity Splunk app Specifications.....	12
4.1 Dashboards.....	12
4.1.1 Overview Dashboard	13
4.1.2 Security - Logins Dashboard	13
4.1.3 Provisioning Dashboard.....	13
4.1.4 Power and Thermal Dashboard.....	14
4.1.5 Security - Changes Dashboard.....	14
4.1.6 Events Recommending Service	15
4.2 Alerts	15
Lenovo XClarity Administrator syslog format	16

1. Introduction

Splunk is a tool in that allows data center operators to track and analyze event logs and other data. Lenovo provides a Splunk app for this product to enable the analysis of activities surfaced by the Lenovo XClarity Administrator product.

The presence of this app aids in monitoring System x and Flex System hardware events, so that you can more easily find problems in your environment.

2. Lenovo XClarity Administrator app for Splunk Overview

The Splunk app enables the analysis of events from the Lenovo XClarity Administrator product and the resources managed by the Lenovo XClarity Administrator. These insights can help systems administrators find potential problems in their environment.

The app provides the following functions:

- Monitoring of hardware events in a Lenovo XClarity Administrator-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 that you can react before more serious issues occur.

- Auditing for security changes occurring within the Lenovo XClarity Administrator.

Security events surfaced by Lenovo XClarity Administrator can help identify if unauthorized personnel are 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 Lenovo XClarity Administrator, the time and dates when they are accessing resources, and any changes to the security settings of the Lenovo XClarity Administrator (or user IDs on the Lenovo XClarity Administrator).

Visual representations can show changes in these activities, which could identify if an attack is occurring.

- Auditing for the provisioning of Lenovo XClarity Administrator-managed resources, including:
 - o Firmware updates
 - o Configuration pattern deployment
 - o Bare-metal OS deployments

Lenovo XClarity Administrator specializes in helping system administrators make desired changes on their computing resources. This includes updating the firmware of Lenovo XClarity Administrator-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.

Dashboards

The following dashboards are defined in this Splunk app.

Dashboard	Description
-----------	-------------

General Events	Provides a consolidated listing for all messages coming from Lenovo XClarity Administrator servers (including events from Lenovo XClarity Administrator-managed resources).
Security - Logins	Provides statistics on any security related events, such as user logins or failures.
Security - Changes	Shows any security changes made to the Lenovo XClarity Administrator, such as security policy changes, or changes for individual Lenovo XClarity Administrator users.
Provisioning	Shows events related to the provisioning of managed resources. Lenovo XClarity Administrator can provision changes to managed resources, including updating firmware, pushing configuration changes, and deploying operating system images.
Power and Thermal	Graphically depicts power/thermal thresholds. Any time a power or thermal threshold is exceeded, the events associated with that situation are reflected in the graphs
Events Recommending Service	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)

Technical Specifications

The following are the prerequisites for using the Lenovo XClarity Administrator Splunk app:

- Splunk, Version 6.3.3
- Lenovo XClarity Administrator, version 1.1.0

3. Installing the XClarity Administrator Splunk app

Download the Lenovo XClarity Administrator app from the Splunkbase website (<https://splunkbase.splunk.com/>).

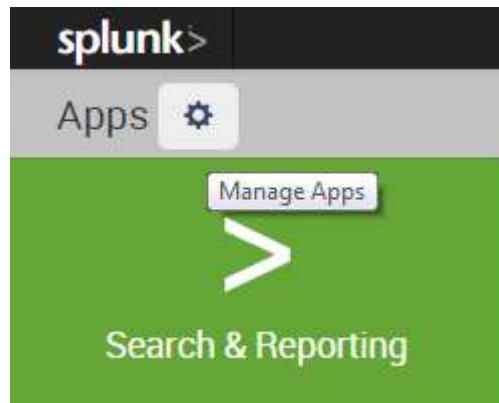
1. Search for “Lenovo XClarity Administrator” to find the web page for the Lenovo XClarity Administrator Splunk app.
2. Right-click the blue button in the upper right hand side titled “Log in to Try.”
3. After logging in with your account information, you have the option to download a zipped file to your workstation. Place this file anywhere convenient on your workstation.

At a minimum, the zipped file will feature the Splunk app (Lenovo XClarity Administrator Splunk app), User Guide, and Software License.

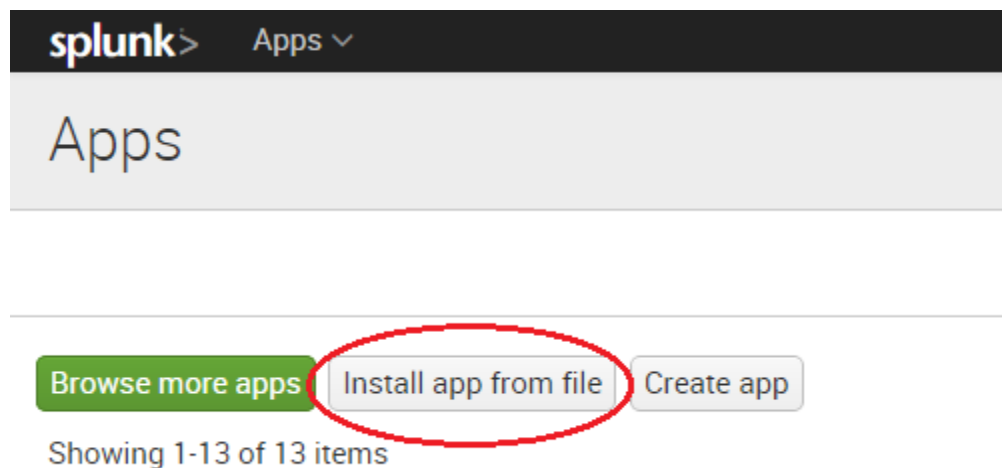
Import the XClarity Administrator app into Splunk

After you download the zip file, extract the package to a location on your computer. The package will contain the XClarity Splunk App (file with .spl extension) and the additional license agreement, user guide, etc., files.

Next, login to your Splunk website and click on the “Manage Apps” gear box next to “Apps”.



You will see the options for installing additional Splunk apps as in the picture below.



You can directly browse for the XClarity Splunk App on the Splunkbase website by clicking on “Browse more apps”. The steps below explain the procedure for importing the app after you downloaded it to your computer.

Click on “Install app from file”. In the next screen, click on “Choose file” button and point it to the .spl application file that you previously downloaded and extracted.

Upload an app


If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

No file chosen

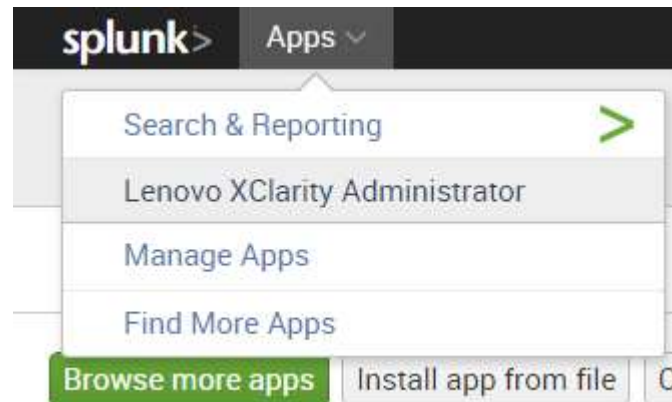
☐ Upgrade app. Checking this will overwrite the app if it already exists.

Name	Date modified	Type	Size
 lenovo_lxca_splunk_app.v1.0.spl	6/12/2015 4:14 PM	Shockwave Flash ...	8 KB

Once the App has been successfully imported, go back to “Manage Apps”. You will see the list of the installed Apps as shown below. Make sure “Lenovo XClarity Administrator” App is listed there. If it is not, then check to make sure you have the right set of privileges to install Apps and try the import again. If you still have issues, see your Splunk administrator.

Name	Folder name	Version	Update checking	Visible
SplunkForwarder	SplunkForwarder		Yes	No
SplunkLightForwarder	SplunkLightForwarder		Yes	No
Webhook Alert Action	alert_webhook	6.3.3	Yes	No
Apps Browser	appsbrowser	6.3.3	Yes	Yes
framework	framework		Yes	No
Getting started	gettingstarted	1.0	Yes	Yes
introspection_generator_addon	introspection_generator_addon	6.3.3	Yes	No
Home	launcher		Yes	Yes
learned	learned		Yes	No
legacy	legacy		Yes	No
Lenovo XClarity Administrator	lenovo_lxca	1.1	No	Yes
sample data	sample_app		Yes	No
Search & Reporting	search	6.3.3	Yes	Yes
Splunk Archiver App	splunk_archiver	1.0	Yes	No
splunk_httpinput	splunk_httpinput		Yes	No
Distributed Management Console	splunk_management_console	6.3.3	Yes	Yes

If the App is showing as installed, you should be able to see it also listed under “Splunk → Apps” drop-down menu.

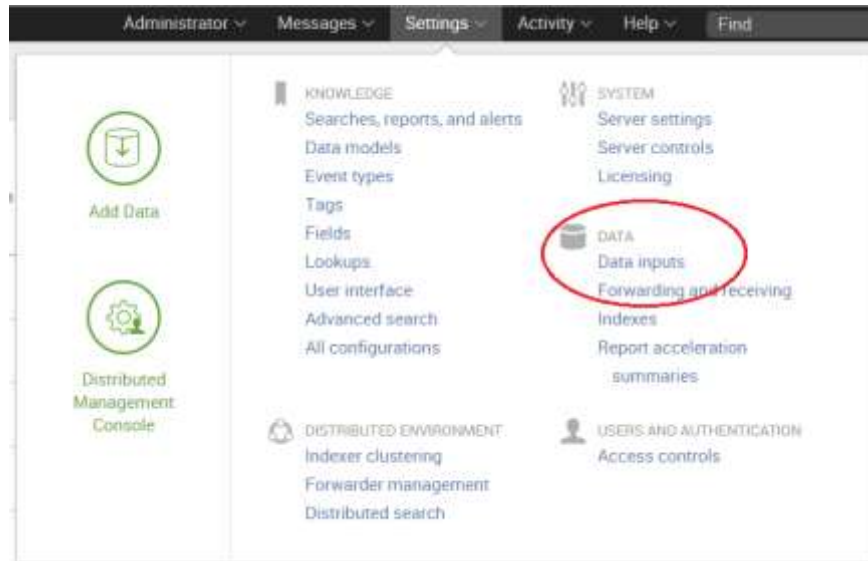


Click on “Lenovo XClarity Administrator” and it will open the main page of the App. From the top level menus, click on “Dashboards”. You should see the dashboards listed as in the picture below.

A screenshot of the Splunk Dashboards page for the 'Lenovo XClarity Administrator' app. The top navigation bar shows 'Search', 'Pivot', 'Reports', 'Alerts', and 'Dashboards' (highlighted). Below the navigation bar, the page title is 'Dashboards' with a subtitle 'Dashboards are comprised of multiple reports or inline searches.' A section titled '6 Dashboards' lists the following dashboards in a table:

i	Title ^
>	Lenovo XClarity - Security Changes
>	Lenovo XClarity - Security Logins
>	Lenovo XClarity Events Recommending Service
>	Lenovo XClarity General Events
>	Lenovo XClarity Power and Thermal events
>	Lenovo XClarity Provisioning

Changing the data input settings



XClarity Administrator app comes pre-configured for receiving log data events from XClarity. The default input ports are TCP and UDP port 10514. If this does not work in your environment because of firewall or other conflicts, you can change this port. To do this, go to “Data inputs” on the “Settings” drop-down menu. You will see the following.

Local inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you

Type

Files & directories

Index a local file or monitor an entire directory.

TCP

Listen on a TCP port for incoming data, e.g. syslog.

UDP

Listen on a UDP port for incoming data, e.g. syslog.

Scripts

Run custom scripts to collect or generate more data.

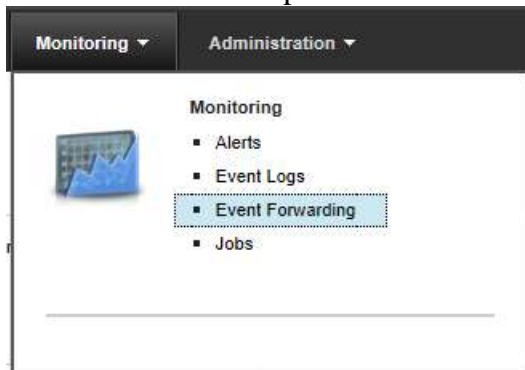
New		
Showing 1-1 of 1 item		
TCP port #	Host Restriction #	Source type #
10514		lenovo_lxca

Click on “TCP” and it will show you the “lenovo_lxca” source type associated with port 10514. You can delete this mapping or clone it. At that point, change the port number to your desired number. Ensure that the “source type” is still specified as “lenovo_lxca”. Once done, click on “save” and “enable” the new input. You may need to restart Splunk to ensure the new input ports are active. Also, ensure you have updated the forwarding port from your XClarity Administrator system to the new port in Splunk so that the events get routed properly.

Configuring Lenovo XClarity Administrator to forward logs to Splunk

To forward events from the Lenovo XClarity Administrator to Splunk, the syslog forwarding capability of Lenovo XClarity Administrator must be configured. The steps to do this are as follows:





1. After signing in to the Lenovo XClarity Administrator, mouse over “**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.

    All Actions ▾		
<input type="checkbox"/>	Name ▾	Notification Method
<input type="checkbox"/>	Splunk 2	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 Splunk server. Then click “**Next**.”

Change Event Recipient

General Systems Events

Select an event recipient type:

☒ Syslog ☐ SNMPv3 ☐ Email

Note: A maximum of 2 syslog recipients are allowed

* Name
Splunk 2 ?

* Host
10.240.37.218 ?

* Port
10514

Description
Push all events to Splunk server

Status
☒ Enable this recipient
☐ Disable this recipient

Back Next Cancel

4. Select the Lenovo XClarity Administrator-managed systems (and potentially the Lenovo XClarity Administrator management server itself) to forward events from:

New Event Recipient

General

Systems

Events

?

Select which systems to monitor for this event recipient.

Filter

<input checked="" type="checkbox"/>	Systems	Machine Type	UUID
<input checked="" type="checkbox"/>	Management Server	server	FFFFFFFFFFFFFFFFFFFFFFFFF...
<input checked="" type="checkbox"/>	+ SN#Y033BG24B00G	Chassis	FC5DC7721C6D4FEF94FC8497C...

Back

Next




Cancel

5. Select which event types that you want forwarded to Splunk. Then click **“Create.”** From this point forward, the selected event types will be forwarded to the Splunk server.

New Event Recipient

GeneralSystemsEvents

Select the event filter types to be forwarded. Event types available are based on the systems selected.
☒ Include All Audit events (Audit events are not filtered by status level)
Filter

Events	 Critical	 Warning	 Informational
All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cooling	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Disks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Memory	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Processors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Adaptor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Expansion	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

BackCreateCancel

4. Lenovo XClarity Splunk app Specifications

This section describes the Dashboards, Charts, and Fields that are defined in this Splunk app.

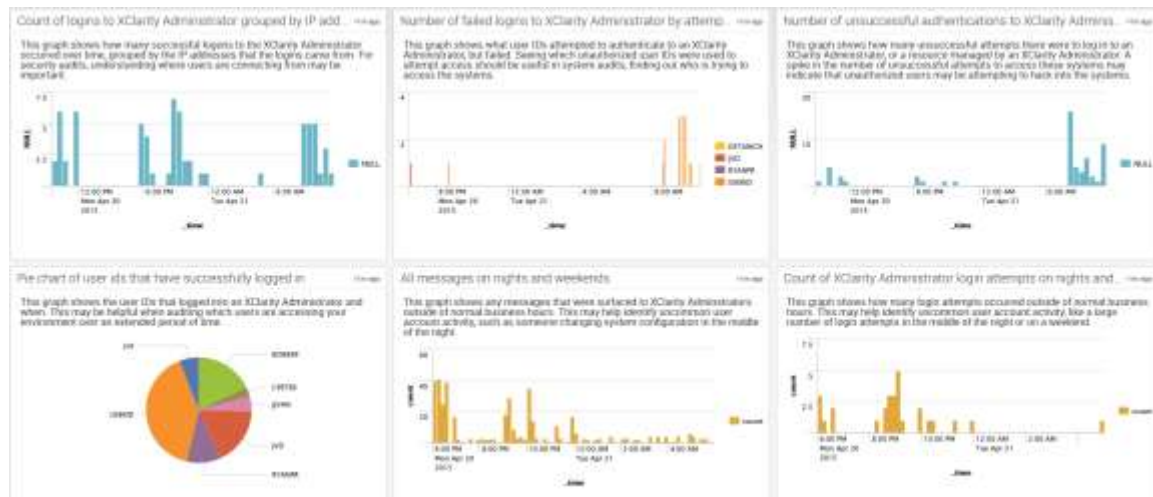
4.1 Dashboards

This section describes the layout of the charts in each dashboard.

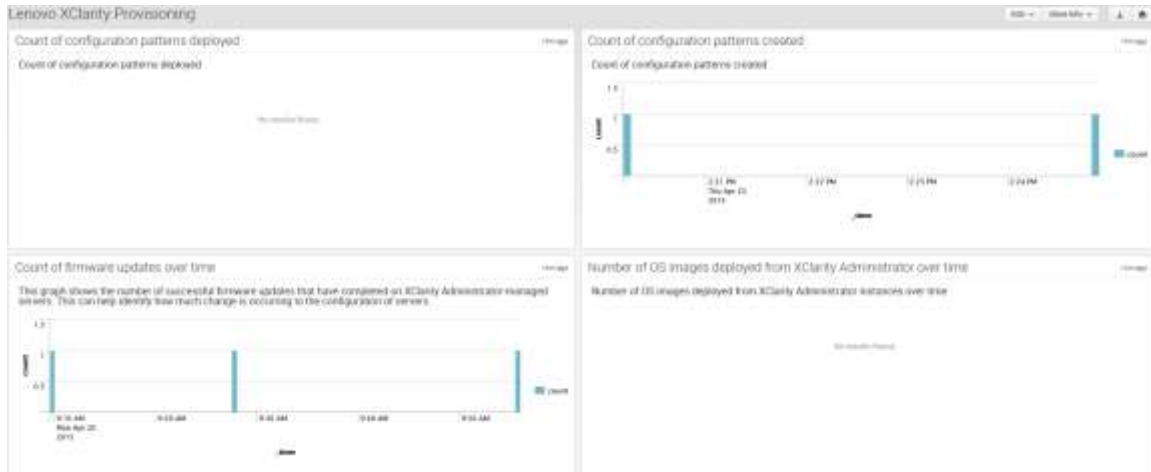
4.1.1 General Events Dashboard



4.1.2 Security - Logins Dashboard



4.1.3 Provisioning Dashboard



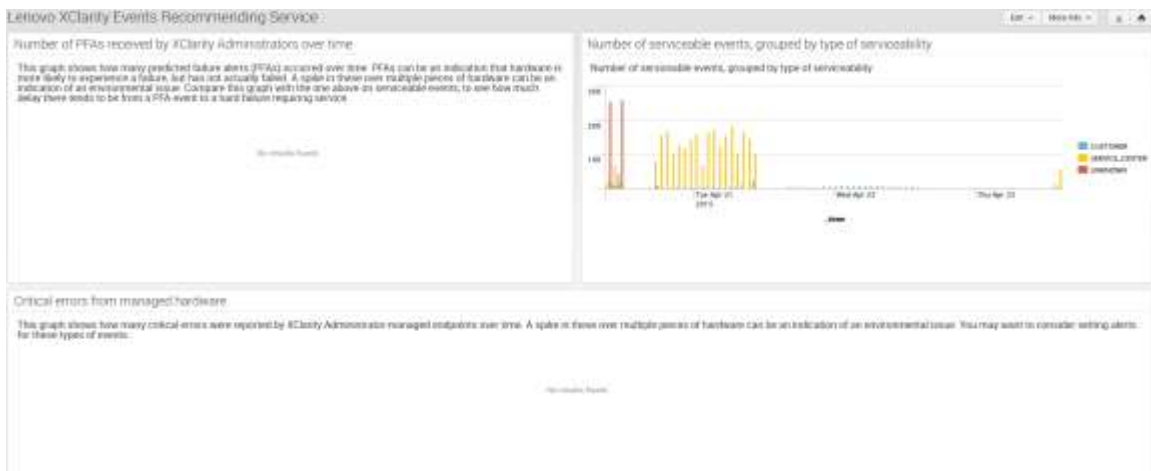
4.1.4 Power and Thermal Dashboard



4.1.5 Security - Changes Dashboard



4.1.6 Events Recommending Service

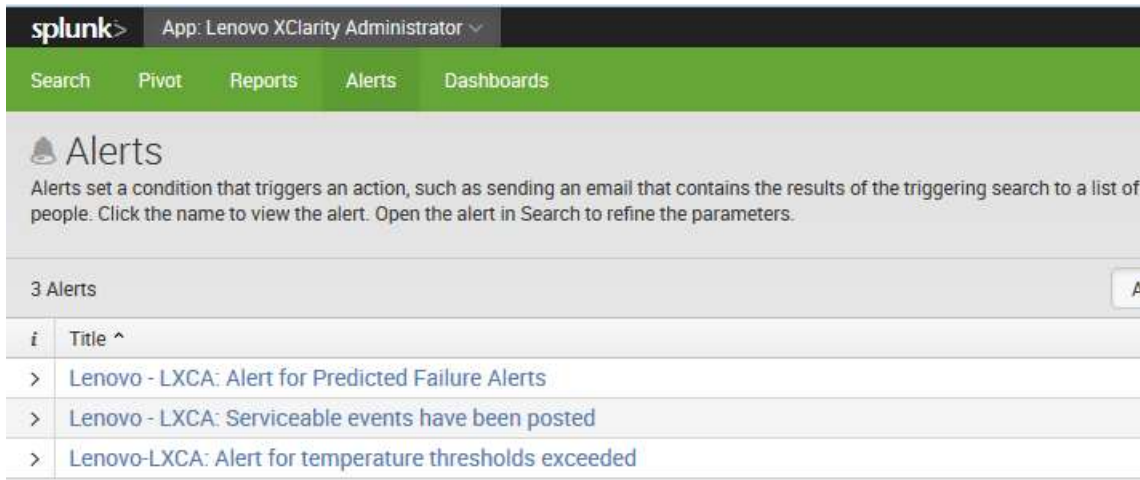


4.2 Alerts

The Splunk app provides predefined alerts that you can enable to define what type of notification to generate. For example, you can define that an email be sent to a specified user or that an event be sent to another application.

Alerts are coded to look for specific textual strings in syslog messages. If a syslog is received that contains that text, a notification is generated.

The following table shows the Alerts that are used in this Splunk app.



Lenovo XClarity Administrator syslog format

Lenovo XClarity Administrator receives events from different types of managed resources. It transforms them into a common format, so that the syslog output from XClarity Administrator looks similar no matter what format the event arrived at XClarity Administrator. The general format is:

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

Here is an example:

```
<86> Tue Apr 07 13:31:46 EDT 2015 [appl=LXCA service=NONE
severity=INFORMATIONAL class=SYSTEM appladdr=10.243.2.107 src=CMM
uuid=98CC4DD31AF649DAA2CD533D05909ABB sn=23KHF99 seq=9263
EventID=40050000] Hot air exiting from the rear of the chassis is not
being recirculated.
```

The following table shows the parameters for the syslog message.

Table 13. Lenovo XClarity Administrator syslog message parameters

Parameter	Definition
<Severity code>	Code specifying error, warning (84), or informational (86).
<Date/Time stamp>	Date and time that the message was surfaced.
appl=LXCA	Indicates that the event came from an XClarity Administrator.
service=<serviceability>	Signifies if this is a Serviceable event or not. Possible values are: <ul style="list-style-type: none"> - None (no user action required). - Customer (User should take action). - Service_Center (Lenovo Support Center should be contacted). If Call Home is enabled, a problem ticket will automatically get opened.
severity=<log severity>	Error, Warning, or Informational.
class=<type of event>	A categorization of the type of endpoint. Possible values are: <ul style="list-style-type: none"> • Audit

	<ul style="list-style-type: none"> • System • Power • Blade • IOModule • Processors • Memory
appladdr=<IPaddress of LXCA>	The IP address of the XClarity Administrator.
src=<type of endpoint>	The general type of endpoint. Possible values are: <ul style="list-style-type: none"> • managementserver • cmm • imm • iom • unknown
uuid=<unique identifier>	A unique identifier for the managed endpoint.
sn=<serial number>	The serial number of the managed endpoint
> seq=<sequence number>	The sequence number of the event from the endpoint. You can use this number to determine if an event is missing.
EventID=<event ID>	The Event ID.
<Message>	Text describing the specific event that occurred.

k