

Lenovo® XClarity™ Orchestrator App for Splunk

User's Guide

Version 1.0.0

November 2022

© Copyright Lenovo 2020,2022. All rights reserved.

Introduction

Splunk is a tool for data-center operators to track and analyze event logs and other data. Lenovo provides a Lenovo XClarity Orchestrator app for Splunk that analyzes events that are surfaced by XClarity Orchestrator and presents the analysis in a set of dashboards. You can monitor the dashboards in this app as an aid to find potential problems in your environment so that you can react before serious issues occur.

Lenovo XClarity Orchestrator app for Splunk Overview

The Lenovo XClarity Orchestrator app for Splunk analyzes events that are surfaced by the Lenovo XClarity Orchestrator and the resources that it manages. These insights can help systems administrators find potential problems in their environment so that you can react before serious issues occur.

The XClarity Orchestrator app provides the following functions:

- Monitoring of hardware events in an XClarity Orchestrator managed environment.

Quickly identify trends based on hardware events, including hardware failures, power/thermal thresholds that were exceeded, and predictive failure alerts (PFAs).

Events are categorized by source, type of device that generated the events, and whether service is required.

- Auditing for security changes that occur in the resource managers (such as XClarity Administrator).

Security events can help identify whether unauthorized personnel are attempting 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 XClarity Orchestrator, the time and dates when they are accessing resources, and any changes to the security settings of the XClarity Orchestrator (including user IDs on the XClarity Orchestrator).

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

- Auditing for the provisioning of resources that are managed by XClarity Orchestrator, including:
 - Configuration pattern deployment
 - Bare-metal OS deployments

This can help identify how much change is occurring to the configuration of servers and if the changes were authorized.

Dashboards

The following dashboards are defined in the Lenovo XClarity Orchestrator app for Splunk.

Dashboard	Description
Security Changes	Summarizes changes to user accounts, security settings, and security policies
Security Logins	Summarizes information about login attempts
Devices	Summarizes the types and overall health of managed devices
Events Recommending Service	Summarizes information about the types and serviceability of events and alerts
General Events	Summarize general information about the events
Power and Thermal Events	Summarizes power and thermal events
Provisioning	Summarizes provisioning tasks

Installing and configuring the Lenovo XClarity Orchestrator app for Splunk

Before you begin

The following software is required for the Lenovo XClarity Orchestrator app for Splunk.

- Splunk, Version 7.0.3 or later
- Lenovo XClarity Orchestrator, version 1.0.0 or later

Installing the Lenovo XClarity Orchestrator app

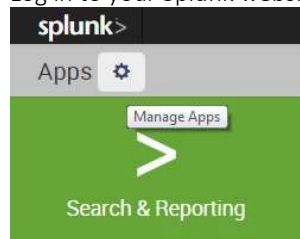
Procedure

To install the Lenovo XClarity Orchestrator app for Splunk, perform the following steps.

1. Download the Lenovo XClarity Orchestrator app from the [Splunkbase website](#).
2. Search for "Lenovo XClarity Orchestrator" to find the web page for the Lenovo XClarity Orchestrator app for Splunk.
3. Click **Login to Try** in the upper right corner.
4. Log in with your account information.
5. Save and extract the package (zip file) to your local system.

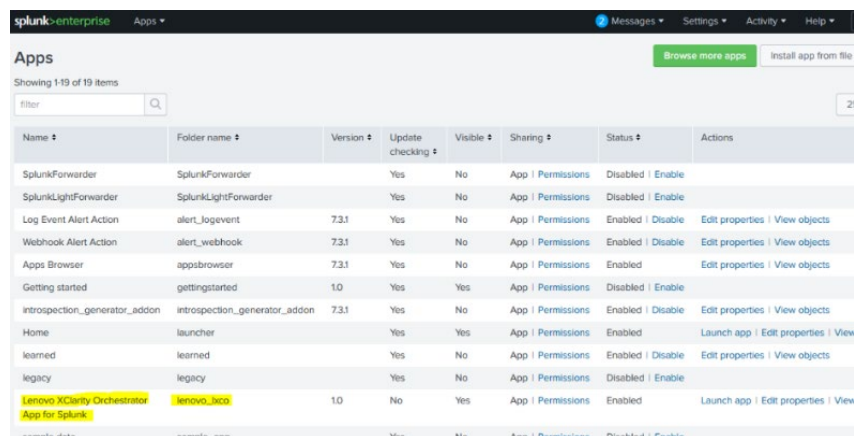
The package contains several files, including the Lenovo XClarity Orchestrator app for Splunk (.spl file), license agreement, and user's guide.

6. Import the Lenovo XClarity Orchestrator app into Splunk.
 - a. Log in to your Splunk website, and click the **Manage Apps** gear icon next to "Apps."



- b. Click **Install app from file** to install Splunk apps. The Upload an app dialog is displayed.
- c. Click **Choose file**, and select the Lenovo XClarity Orchestrator app for Splunk application file (for example, lenovo_lxco_splunk_app.v1.0.spl).
- d. After the app is successfully imported, go back to the Manage Apps page, and verify that Lenovo XClarity Orchestrator is listed in the table of installed apps, as shown in the following example.

If it is not listed, ensure that you have the correct set of privileges to install Splunk apps, and try the import again. If you still have issues, see your Splunk administrator.

A screenshot of the Splunk 'Apps' management page. The page shows a table of installed applications. The table has columns for Name, Folder name, Version, Update checking, Visible, Sharing, Status, and Actions. The application 'Lenovo XClarity Orchestrator App for Splunk' is highlighted in yellow in the original image. The table also shows other installed apps like SplunkForwarder, SplunkLightForwarder, and various alert actions.

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
Log Event Alert Action	alert_logevent	7.3.1	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Webhook Alert Action	alert_webhook	7.3.1	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Apps Browser	appsbrowser	7.3.1	Yes	No	App Permissions	Enabled	Edit properties View objects
Getting started	gettingstarted	1.0	Yes	Yes	App Permissions	Disabled Enable	
introspection_generator_addon	introspection_generator_addon	7.3.1	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit properties View
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
legacy	legacy		Yes	No	App Permissions	Disabled Enable	
Lenovo XClarity Orchestrator App for Splunk	lenovo_lxco	1.0	No	Yes	App Permissions	Enabled	Launch app Edit properties View
sample data	sample_app		Yes	No	App Permissions	Disabled Enable	

Configuring Lenovo XClarity Orchestrator to forward logs to Splunk



To forward events from the Lenovo XClarity Orchestrator to Splunk, you must configure an event forwarder in XClarity Orchestrator.

Tips:

- You can define multiple Splunk configurations; however, XClarity Orchestrator can forward events to only one Splunk instance. Therefore, only one Splunk configuration can be enabled at a time.
- You cannot filter events that are forwarded to Splunk applications.
- The credentials that you provide are used to create an HEC token. Thereafter LXCO uses the HEC token for forwarding. If you ever need to revoke access to Splunk, you also need to revoke this token.

For more information about forwarding events from XClarity Orchestrator, see in the XClarity Orchestrator online documentation.

To configure an event forwarder to Splunk, complete the following steps.

1. From the XClarity Orchestrator menu bar, click **Monitoring**  > **Event Forwarding**, and then click **Forwarders** in the left navigation to display the Event Forwarders card.
2. Click the **Create** icon  to display the Create Forwarder dialog.
3. Specify the event-forwarder name and optional description.
4. Choose to enable the event forwarder by clicking the **State** toggle.
5. Select **Splunk** as the event-forwarder type.
6. Click **Configuration**, and fill in the protocol-specific information.
 - Enter the hostname or IP address of the Splunk application.
 - Specify the user account and password to use to log in to the Splunk service.
 - Specify the REST API and data port numbers to use to connect to the Splunk service.
 - Specify one or more HTTP event-collector indices. The default index is "lxco."
 - Enter the time-out period (in seconds) for the request. Default is 30 seconds.
7. Click **Create** to create the event forwarder.

Monitoring your environment

From the Showcase page, you can learn about the dashboards that are available in Splunk.

You can click the Dashboards tab to monitor a summary of events that were surfaced by Lenovo XClarity Orchestrator, or click the Alerts tab to enable predefined alerts.

Dashboards

The Lenovo XClarity Orchestrator app provides a set of dashboards and cards that you can monitor and analyze Lenovo hardware events from your Lenovo XClarity Orchestrator environment.

To view a description of the dashboards, click **Apps > Lenovo XClarity Orchestrator app for Splunk**, and then click **Showcase**.

To view the dashboards, click **Dashboards**.

You can filter data on the dashboards by index and Lenovo XClarity Administrator host (by its IP address).

Security Changes

Summarizes changes to user accounts, security settings, and security policies, including:

- Number of user accounts there were created over time
- Number of user accounts that were deleted over time
- Number of user accounts that changed over time
- Number of user-account security setting that were changed over time
- Number of user-account security setting that were changed, per XClarity Administrator
- Number of security policy changes over time

Security Logins

Summarizes information about login attempts, including:

- Number of successful login attempts to an XClarity Administrator over time, per XClarity Administrator
- Number of successful login attempts to XClarity Administrator over time, by user account
- Number of failed login attempts to XClarity Administrator over time, per user account
- Number of failed login attempts to a managed resource over time, per XClarity Administrator
- Number of messages that were generated during nights and weekends over time
- Number of logins that were attempted during nights and weekends over time

Devices

Summarizes the types and overall health of managed devices, including:

- Number of managed devices, by device type
- Number of managed devices in critical, warning, and normal states
- Number of managed devices that are powered on and off

Events Recommending Service

Summarizes information about the types and serviceability of events and alerts, including:

- Number of predicted failure alerts (PFAs) that were received by XClarity Orchestrator over time
- Number of serviceable events over time, by type and serviceability
- Number of critical events that were generated over time, by managed devices

General Events

Summarizes general information about events, including:

- Number of events, per XClarity Administrator
- Number of events, per source type
- Number of events over time

Power and Thermal Events

Summarizes power and thermal events, including:

- Number of power-threshold events that were generated over time
- Number of thermal events that were generated over time
- Number of low or failed battery events that were generated over time

Provisioning

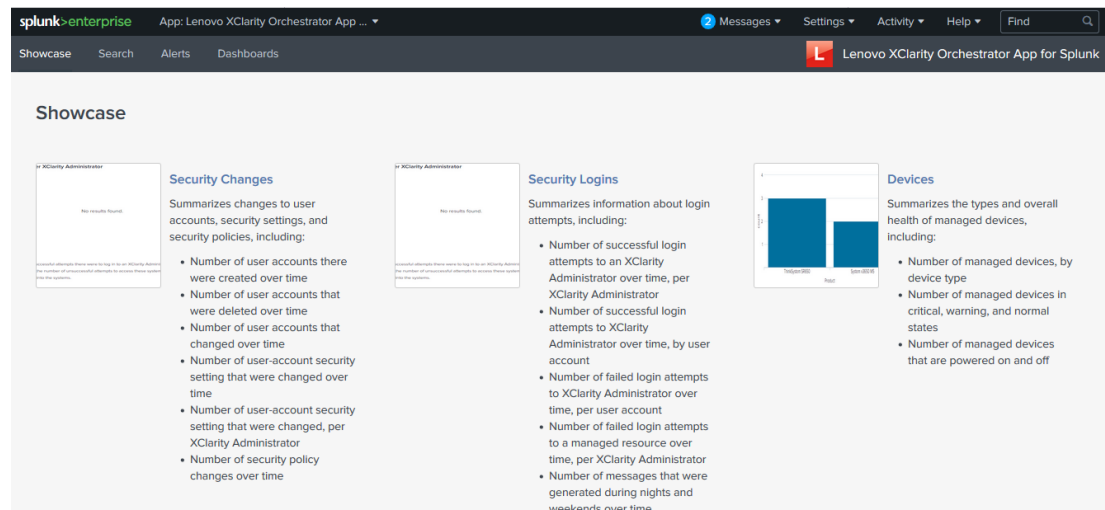
Summarizes provisioning tasks, including:

- Number of configuration patterns that were created over time
- Number of configuration patterns that were deployed over time
- Number of operating systems that were deployed over time

Alerts

The Lenovo XClarity Orchestrator app for Splunk provides predefined alerts that you can enable to define the type of notification that you want the app to generate. For example, you can choose to send events as to another application or as an email to a specified user.

The following table shows the Alerts that are used in this Lenovo XClarity Orchestrator app.



The screenshot shows the Splunk interface for the Lenovo XClarity Orchestrator app. The top navigation bar includes 'splunk>enterprise', 'App: Lenovo XClarity Orchestrator App ...', and various utility icons like 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation bar, there are tabs for 'Showcase', 'Search', 'Alerts', and 'Dashboards'. The main content area is titled 'Showcase' and features three alert cards:

- Security Changes:** Summarizes changes to user accounts, security settings, and security policies, including:
 - Number of user accounts there were created over time
 - Number of user accounts that were deleted over time
 - Number of user accounts that changed over time
 - Number of user-account security setting that were changed over time
 - Number of user-account security setting that were changed, per XClarity Administrator
 - Number of security policy changes over time
- Security Logins:** Summarizes information about login attempts, including:
 - Number of successful login attempts to an XClarity Administrator over time, per XClarity Administrator
 - Number of successful login attempts to XClarity Administrator over time, by user account
 - Number of failed login attempts to XClarity Administrator over time, per user account
 - Number of failed login attempts to a managed resource over time, per XClarity Administrator
 - Number of messages that were generated during nights and weekends over time
- Devices:** Summarizes the types and overall health of managed devices, including:
 - Number of managed devices, by device type
 - Number of managed devices in critical, warning, and normal states
 - Number of managed devices that are powered on and off

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.

1009 Think Place

Morrisville, NC 27560

U.S.A.

Attention: Lenovo VP of Intellectual Property

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 XCLARITY are trademarks of Lenovo. All other trademarks are the property of their respective owners.