Linux SSH Automation PowerPacks

Linux SSH Automation PowerPack version 105

Linux SSH User-Initiated Automation PowerPack version 100

Table of Contents

Introduction 3
What is the Linux SSH Automation PowerPack? 4
Installing the Linux SSH AutomationPowerPack 4
Linux SSH Automation Policies 6
Standard Automation Policies 7
Configuring Device Credentials 18
Authentication for Linux Devices with the Linux SSH Automations PowerPack 19
Creating a Credential 19
Creating and Customizing Automation Policies 21
Prerequisites 22
Creating an Automation Policy 22
Example Automation Configuration 25
Customizing an Automation Policy 26
Removing an Automation Policy from a PowerPack 28
Customizing Linux SSH Actions 29
Creating a Custom Action Policy 30
Customizing Automation Actions 31
Creating a New Linux SSH Automation Action 34
Linux SSH User-Initiated Automations 35
What is the Linux SSH User-Initiated Automation PowerPack? 36
Installing the Linux SSH User-Initiated Automation PowerPack 36
Standard Automation Policies 37
Running a User Initiated Automation Policy 42
Viewing Automation Actions for an Event 43
Run Book Variables 45
Run Book Variables 46

Chapter 1

Introduction

Overview

This manual describes how to use the automation policies, automation actions, and custom action types found in the *Linux SSH Automation* PowerPack.

This PowerPack requires a subscription to one of the following solutions:

- *Datacenter Automation Pack*
- ScienceLogic Standard solution

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

This chapter covers the following topics:

What is the Linux SSH Automation PowerPack? 4
Installing the Linux SSH AutomationPowerPack 4

What is the Linux SSH Automation PowerPack?

The *Linux SSH Automation* PowerPack includes automation policies that:

- Enrich SL1 events for Linux devices (for example, from the *Linux Base Pack* PowerPack and native SNMP collection) by automatically running diagnostic commands via a remote SSH connection. The command output is added to the SL1 event log or associated incident. Supported events include CPU, swap, file system, interface, and system process issues.
- Run remediation commands via a remote SSH connection in response to SL1 system process events for Linux devices in the "Linux Automation" device group.

The Linux SSH Automation actions are executed on the SL1 All-In-One Appliance or Data Collector.

In addition to using the standard content, you can use the content in the *Linux SSH Automation* PowerPack to:

- Create your own automation policies that include the pre-defined actions that run different sets of diagnostic commands.
- Use the supplied "Execute Shell Commands" custom action type to configure your own automation action by supplying a set of commands to be executed via SSH.

Installing the Linux SSH AutomationPowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Linux SSH Automation* PowerPack.

IMPORTANT: You must install the *Datacenter Automation Utilities* PowerPack before using the Linux SSH Automations PowerPack.

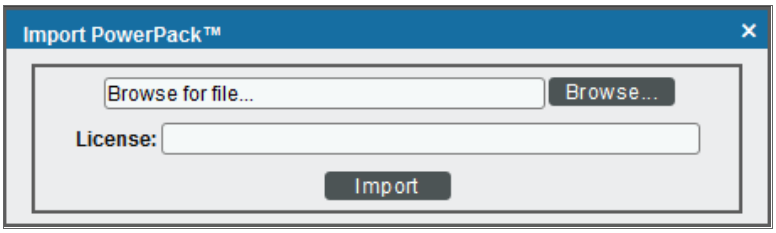
NOTE: The *Linux SSH Automation* PowerPack requires SL1 version 8.10.0 or later. For details on upgrading SL1, see the appropriate SL1 Release Notes.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the ***System Administration*** manual.)

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.

4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

TIP: If you will have the *Linux Base Pack* PowerPack installed and are monitoring your Linux devices, no other configuration is necessary. The automation policies in the *Linux SSH Automation* PowerPack will run in response to aligned events.

Chapter 2

Linux SSH Automation Policies

Overview

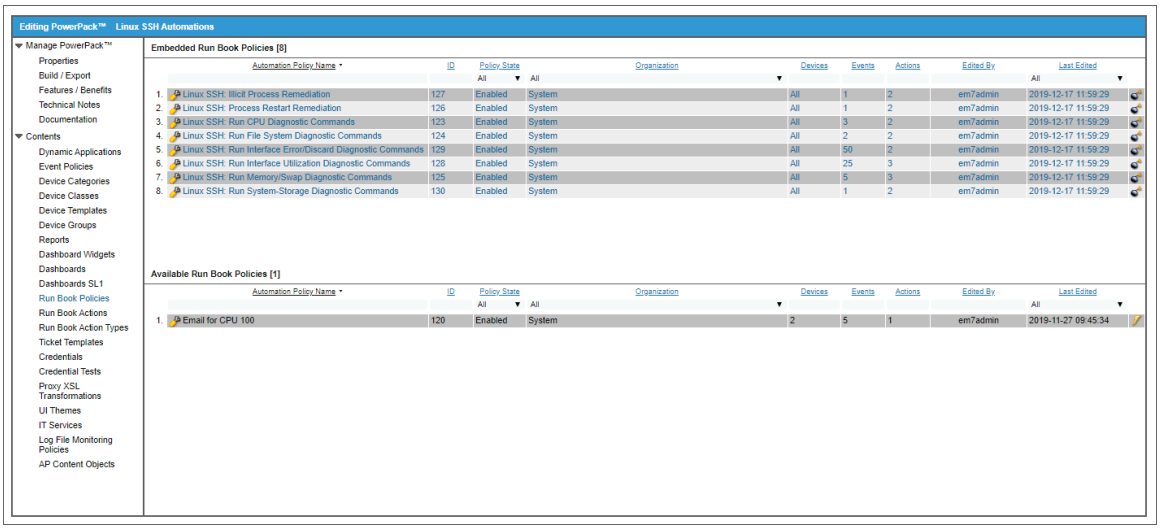
This chapter describes how to use the automation policies, automation actions, and custom action types found in the *Linux SSH Automation* PowerPack.

This chapter covers the following topics:

Standard Automation Policies 7

Standard Automation Policies

The *Linux SSH Automation* PowerPack includes eight standard automation policies and a "Linux Automation" device group. Each policy triggers an automation action that collects diagnostic data or runs a remediation command over SSH for events associated with devices in the "Linux Automation" device group, and an action that formats the output. All of the automation actions use the same custom action type, "Execute Shell Commands", which is supplied in the PowerPack.



All of the standard automation policies are tied to included SL1 events generated by:

- Dynamic Applications from the Host Resources PowerPack
- Dynamic Applications from the Net-SNMP PowerPack
- Dynamic Applications from the Linux Base PowerPack
- Interface collection
- File System Collection
- System Process Monitoring Policies

Several of the automation actions use the substitution character feature of the "Execute Shell Commands" custom action type. If an event variable is included in a command (such as "%Y" for the sub-entity name), the custom action type automatically replaces that variable with the value from the triggering event.

The following table shows the standard automation policies, their aligned events, the aligned device group, and the automation actions that runs in response to the events.

NOTE: The aligned events are included as part of this PowerPack and are not installed with the SL1 platform. You must install the PowerPack to obtain these events.

Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
Linux SSH: Illicit Process Remediation	• Poller: Illicit process running	Linux Automation	• Linux Illicit Process Remediation • Datacenter Automation: Format Output as HTML
Linux SSH: Process Restart Remediation	• Poller: required process not running	Linux Automation	• Linux Process Restart Remediation • Datacenter Automation: Format Output as HTML
Linux SSH: Run CPU Diagnostic Commands	• Linux SSH: CPU utilization above threshold • Net-SNMP: CPU has exceeded threshold • Host Resource: CPU has exceeded threshold	Linux Automation	• Linux CPU Diagnostic Commands • Datacenter Automation: Format Output as HTML
Linux SSH: Run File System Diagnostic Commands	• Linux SSH: File System over usage threshold • Poller: File system usage exceeded (critical) threshold • Poller: File system usage exceeded (major) threshold	Linux Automation	• Linux File System Diagnostic Commands • Datacenter Automation: Format Output as HTML
Linux SSH: Run Interface Error/Discard Diagnostic Commands	• Poller: Interface reporting discards • Interface inbound discards has exceeded the Falling-High threshold • Interface inbound discards has exceeded the Falling-Low threshold • Interface inbound discards has exceeded the Falling-Medium threshold • Interface inbound discards has exceeded the Rising-High threshold	Linux Automation	• Linux Interface Error/Discard Diagnostic Commands • Datacenter Automation: Format Output as HTML

Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
	• Interface inbound discards has exceeded the Rising-Low threshold • Interface inbound discards has exceeded the Rising-Medium threshold • Interface inbound discards percentage has exceeded the Falling-High threshold • Interface inbound discards percentage has exceeded the Falling-Low threshold • Interface inbound discards percentage has exceeded the Falling-Medium threshold • Interface inbound discards percentage has exceeded the Rising-High threshold • Interface inbound discards percentage has exceeded the Rising-Low threshold • Interface inbound discards percentage has exceeded the Rising-Medium threshold • Interface outbound discards has exceeded the Falling-High threshold • Interface outbound discards has exceeded the Falling-Low threshold		

Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
	• Interface outbound discards has exceeded the Falling-Medium threshold • Interface outbound discards has exceeded the Rising-High threshold • Interface outbound discards has exceeded the Rising-Low threshold • Interface outbound discards has exceeded the Rising-Medium threshold • Interface outbound discards percentage has exceeded the Falling-High threshold • Interface outbound discards percentage has exceeded the Falling-Low threshold • Interface outbound discards percentage has exceeded the Falling-Medium threshold • Interface outbound discards percentage has exceeded the Rising-High threshold • Interface outbound discards percentage has exceeded the Rising-Low threshold • Interface outbound discards percentage has exceeded the Rising-Medium threshold • Interface inbound errors has exceeded Rising-Medium threshold		

Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
	• Interface inbound errors has exceeded the Falling-High threshold • Interface inbound errors has exceeded the Falling-Low threshold • Interface inbound errors has exceeded the Falling-Medium threshold • Interface inbound errors has exceeded the Rising-High threshold • Interface inbound errors has exceeded the Rising-Low threshold • Interface inbound errors percentage has exceeded the Falling-High threshold • Interface inbound errors percentage has exceeded the Falling-Low threshold • Interface inbound errors percentage has exceeded the Falling-Medium threshold • Interface inbound errors percentage has exceeded the Rising-High threshold • Interface inbound errors percentage has exceeded the Rising-Low threshold • Interface inbound errors percentage has exceeded the Rising-Medium threshold		

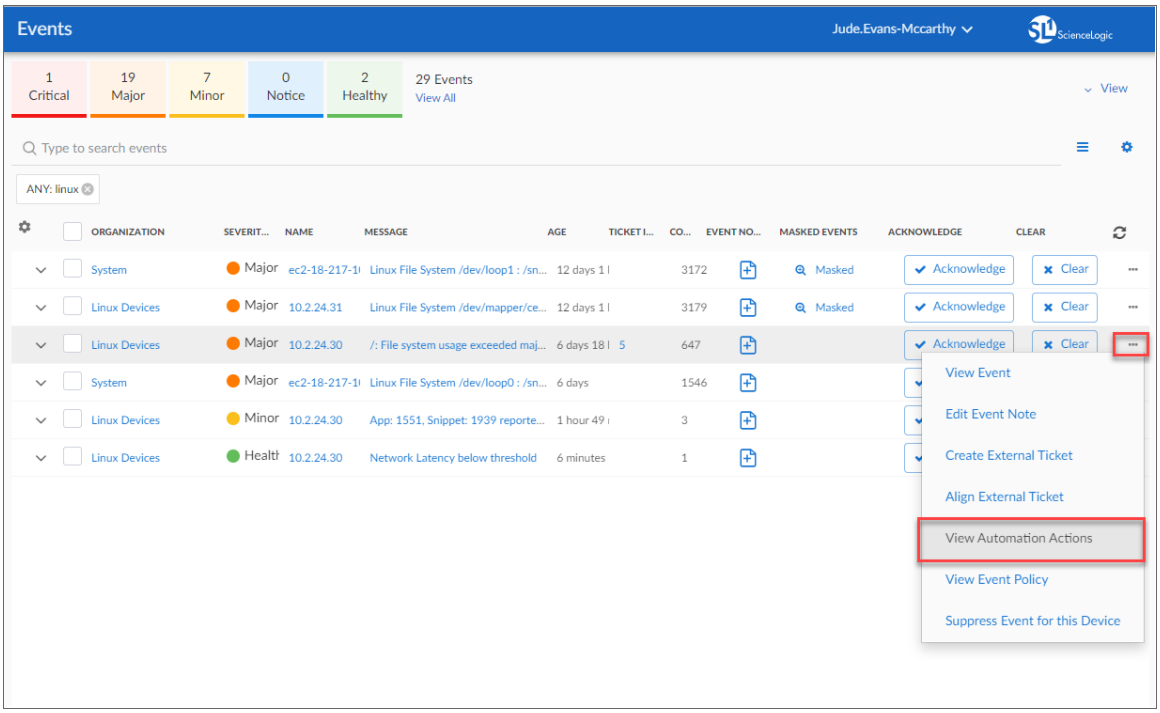
Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
	• Interface outbound errors has exceeded the Falling-High threshold • Interface outbound errors has exceeded the Falling-Low threshold • Interface outbound errors has exceeded the Falling-Medium threshold • Interface outbound errors has exceeded the Rising-High threshold • Interface outbound errors has exceeded the Rising-Low threshold • Interface outbound errors has exceeded the Rising-Medium threshold • Interface outbound errors percentage has exceeded the Falling-High threshold • Interface outbound errors percentage has exceeded the Falling-Low threshold • Interface outbound errors percentage has exceeded the Falling-Medium threshold • Interface outbound errors percentage has exceeded the Rising-High threshold • Interface outbound errors percentage has exceeded the Rising-Low threshold		

Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
	• Interface outbound errors percentage has exceeded the Rising-Medium threshold • Poller: Interface reporting packet errors		
Linux SSH: Run Interface Utilization Diagnostic Commands	• Poller: Bandwidth usage exceeded threshold • Interface inbound usage percentage has exceeded the Falling-High threshold • Interface inbound usage percentage has exceeded the Falling-Low threshold • Interface inbound usage percentage has exceeded the Falling-Medium threshold • Interface inbound usage percentage has exceeded the Rising-High threshold • Interface inbound usage percentage has exceeded the Rising-Low threshold • Interface inbound usage percentage has exceeded the Rising-Medium threshold • Interface inbound usage rate has exceeded the Falling-High threshold • Interface inbound usage rate has exceeded the Falling-Low threshold • Interface inbound usage rate has exceeded the Falling-Medium threshold	Linux Automation	• Automation Utilities: Calculate Memory Size for Each Action (from the *Datacenter Automation Utilities* PowerPack) • Linux Interface Utilization Diagnostic Commands • Linux Tcpdump Command • Datacenter Automation: Format Output as HTML

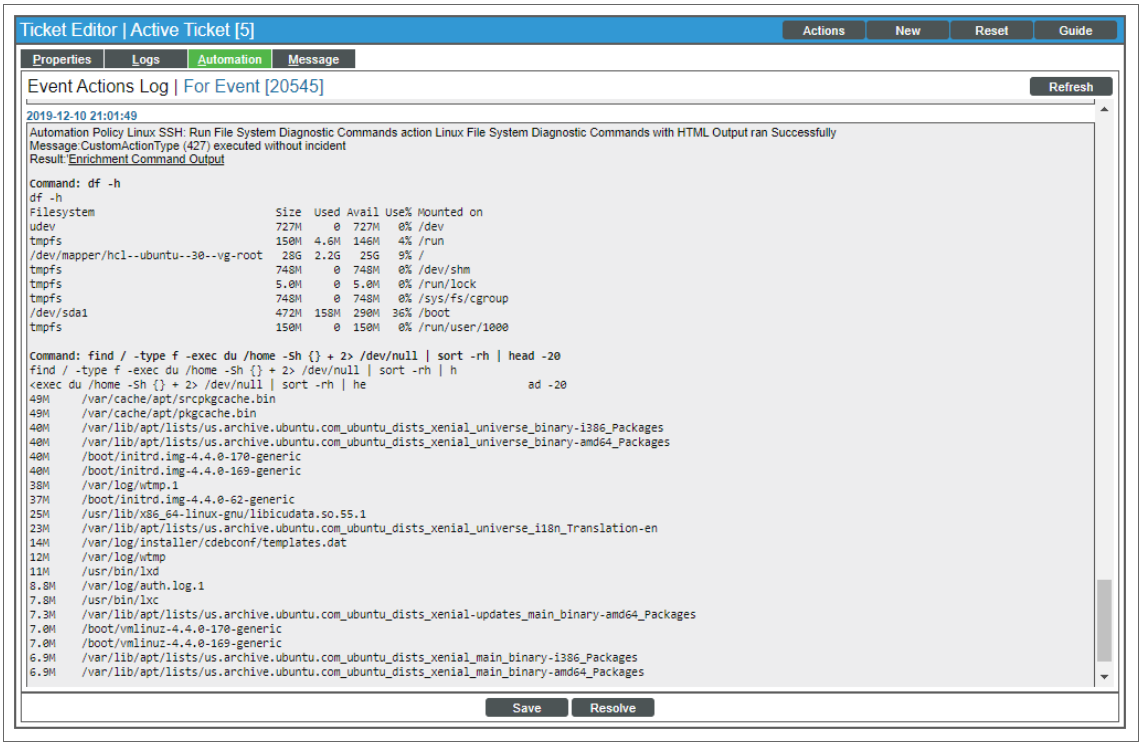
Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
	• Interface inbound usage rate has exceeded the Rising-High threshold • Interface inbound usage rate has exceeded the Rising-Low threshold • Interface inbound usage rate has exceeded the Rising-Medium threshold • Interface outbound usage percentage has exceeded the Falling-High threshold • Interface outbound usage percentage has exceeded the Falling-Low threshold • Interface outbound usage percentage has exceeded the Falling-Medium threshold • Interface outbound usage percentage has exceeded the Rising-High threshold • Interface outbound usage percentage has exceeded the Rising-Low threshold • Interface outbound usage percentage has exceeded the Rising-Medium threshold • Interface outbound usage rate has exceeded the Falling-High threshold • Interface outbound usage rate has exceeded the Falling-Low threshold		

Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
	• Interface outbound usage rate has exceeded the Falling-Medium threshold • Interface outbound usage rate has exceeded the Rising-High threshold • Interface outbound usage rate has exceeded the Rising-Low threshold • Interface outbound usage rate has exceeded the Rising-Medium threshold		
Linux SSH: Run Memory/Swap Diagnostic Commands	• Linux SSH: Swap usage above threshold • Net-SNMP: Swap has exceeded threshold • Host Resource: Swap Memory has exceed threshold • Host Resource: Physical Memory has exceeded threshold • Net-SNMP: Physical Memory exceeded threshold	Linux Automation	• Automation Utilities: Calculate Memory Size for Each Action (from the *Datacenter Automation Utilities*PowerPack) • Linux Memory/Swap Diagnostic Commands • Linux Memory Dmidecode Command • Datacenter Automation: Format Output as HTML
Linux SSH: Run System-Storage Diagnostic Commands	• Linux SSH: File System over usage threshold	Linux Automation	• Linux System-Storage Diagnostic Commands • Datacenter Automation: Format Output as HTML

The following figure shows a file system usage threshold exceeded event with major criticality on the **Events** page. Click the **[Actions]** button (···) for an event, and select *View Automation Actions* to see the automation actions triggered by the events.



The results shown for this event, in the Event Actions Log, include the automation policy that ran (shown at the top of the following figure), along with the automation actions (commands) that ran. Results for each command are also displayed. The following figure shows an example of this output.



To learn more about which commands are executed by default for a given automation action, see *Customizing Actions*.

TIP: Although you can edit the automation policies described in this section, it is a best practice to use "Save As" to create a new automation policy, rather than to customize the standard automation policies.

Chapter 3

Configuring Device Credentials

Overview

This chapter describes how to configure the credentials required by the automation actions in the *Linux SSH Automation* PowerPack.

NOTE: If you already have the *Linux Base Pack* PowerPack installed and monitoring your Linux devices, you do not need to configure an additional credential.

This chapter covers the following topics:

Authentication for Linux Devices with the Linux SSH Automations PowerPack *19*

Creating a Credential *19*

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

Authentication for Linux Devices with the Linux SSH Automations PowerPack

The "Execute Shell Commands" custom action type supports hard-coded credentials (wherein you specify the ID of a credential in the automation action), or the custom action type can dynamically determine the credential to use. By default, the automation actions use the dynamic method (by specifying credential ID 0 in the input parameters). The dynamic method uses the first credential that matches the following rules:

- If the "Linux: Configuration Cache" Dynamic Application (from the *Linux Base Pack* PowerPack) is aligned to the device associated with the triggering event, the credential aligned to that Dynamic Application is used.
- If the "Linux: Performance Cache" Dynamic Application (from the Linux Base Pack PowerPack) is aligned to the device associated with the triggering event, the credential aligned to that Dynamic Application is used.
- If neither of the listed Dynamic Applications is aligned to the device associated with the triggering event, the first available SSH/Key credential aligned to the device as a secondary credential is used.

Creating a Credential

NOTE: If you already have the *Linux Base Pack* PowerPack installed and monitoring your Linux devices, you do not need to configure an additional credential.

If you do not have the *Linux Base Pack* PowerPack installed, you must create an SSH credential that includes the username and password, or username and private key, combination to communicate with your Linux devices.

To create a credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click **[Actions]** and select *Create SSH/Key credential*. The Create New SSH/Key Credential page appears.
3. Supply values in the following fields:
    - ***Credential Name***. Enter a name for the credential.
    - ***Hostname/IP***. Hostname or IP address of the device from which you want to retrieve data.
        - You can include the variable %D in this field. SL1 will replace the variable with the IP address of the current device (device that is currently using the credential).
        - You can include the variable %N in this field. SL1 will replace the variable with hostname of the current device (device that is currently using the credential). If SL1 cannot determine the hostname, SL1 will replace the variable with the primary, management IP address for the current device.
    - ***Port***. To use SSH to connect to the device, enter "22" in this field.
    - ***Timeout(ms)***. Enter a timeout, in milliseconds, for the connection.
    - ***Username***. Enter the username for an SSH user or user account on the device to be monitored.

- ***Password***. Enter the password for the user you entered in the ***Username*** field.
- ***Private Key (PEM Format)***. Enter the SSH private key that you want SL1 to use, in PEM format.

4. Click **[Save]**.

For more information about configuring credentials in SL1, see the ***Discovery and Credentials*** manual .

Chapter 4

Creating and Customizing Automation Policies

Overview

This chapter describes how to create automation policies using the automation actions in the *Linux SSH Automation* PowerPack.

This chapter covers the following topics:

Prerequisites 22

Creating an Automation Policy 22

Example Automation Configuration 25

Customizing an Automation Policy 26

Removing an Automation Policy from a PowerPack 28

Prerequisites

Before you create an automation policy using the automation actions in the *Linux SSH Automation* PowerPack, you must determine:

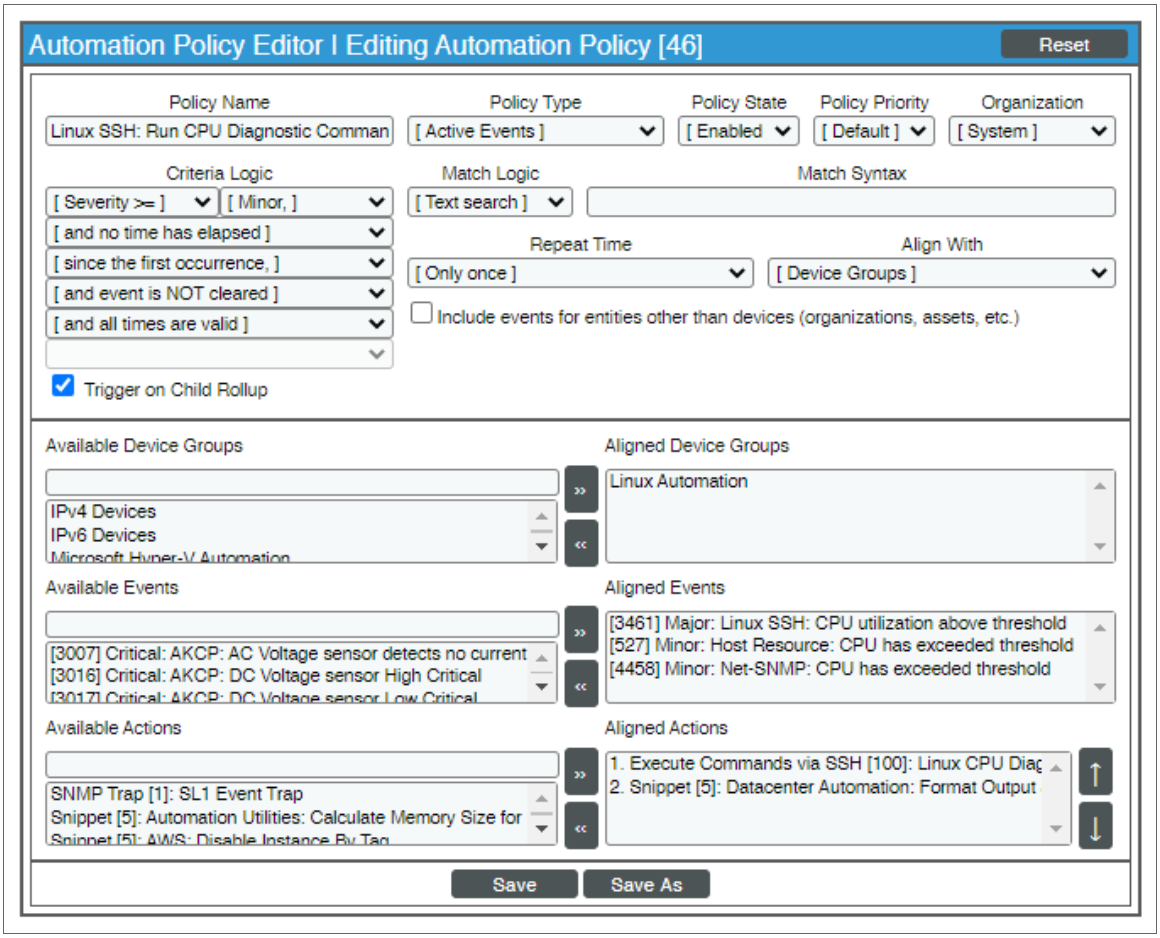
- Which set of commands you want to run on a monitored device when an event occurs. There are eight automation actions in the PowerPack that run the "Execute Shell Commands" action type with different commands and output formats. You can also create your own automation actions using the custom action type supplied in the PowerPack.
- What event criteria you want to use to determine when the automation actions will trigger, or the set of rules that an event must match before the automation is executed. This can include matching only specific event policies, event severity, associated devices, and so on. For a description of all the options that are available in Automation Policies, see the ***Run Book Automation*** manual.

Creating an Automation Policy

To create an automation policy that uses the automation actions in the *Linux SSH Automation* PowerPack, perform the following steps:

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).

2. Click **[Create]**. The **Automation Policy Editor** page appears.



3. Complete the following required fields:
    - ***Policy Name***. Enter a name for the automation policy.
    - ***Policy Type***. Select whether the automation policy will match events that are active, match when events are cleared, or run on a scheduled basis. Typically, you would select *Active Events* in this field.
    - **Policy State**. Specifies whether the policy will be evaluated against the events in the system. If you want this policy to begin matching events immediately, select *Enabled*.
    - **Policy Priority**. Specifies whether the policy is high-priority or default priority. These options determine how the policy is queued.
    - ***Organization***. Select one or more organizations to associate with the automation policy. The automation policy will execute only for devices in the selected organizations (that also match the other criteria in the policy). To configure a policy to execute for all organizations , select *System* without specifying individual devices to align to.
    - ***Align With***. Select *Device Groups*.

- ***Aligned Device Groups***. The "Linux Automation" device group needs to be aligned. To add the device group to the ***Aligned Device Groups*** field, select the "Linux Automation" device group in the ***Available Device Groups*** field and click the right arrow (>>).
- ***Aligned Actions***. This field includes the actions from the *Linux SSH Automation*PowerPack. To add an action to the ***Aligned Actions*** field, select the action in the ***Available Actions*** field and click the right arrow (>>). To re-order the actions in the ***Aligned Actions*** field, select an action and use the up arrow or down arrow buttons to change that action's position in the sequence.

> **NOTE:** You must have at least two Aligned Actions: one that runs the automation action and one that provides the output format. The actions providing the output formats are contained in the *Datacenter Automation Utilities* PowerPack, which is a prerequisite for running automations in this PowerPack.

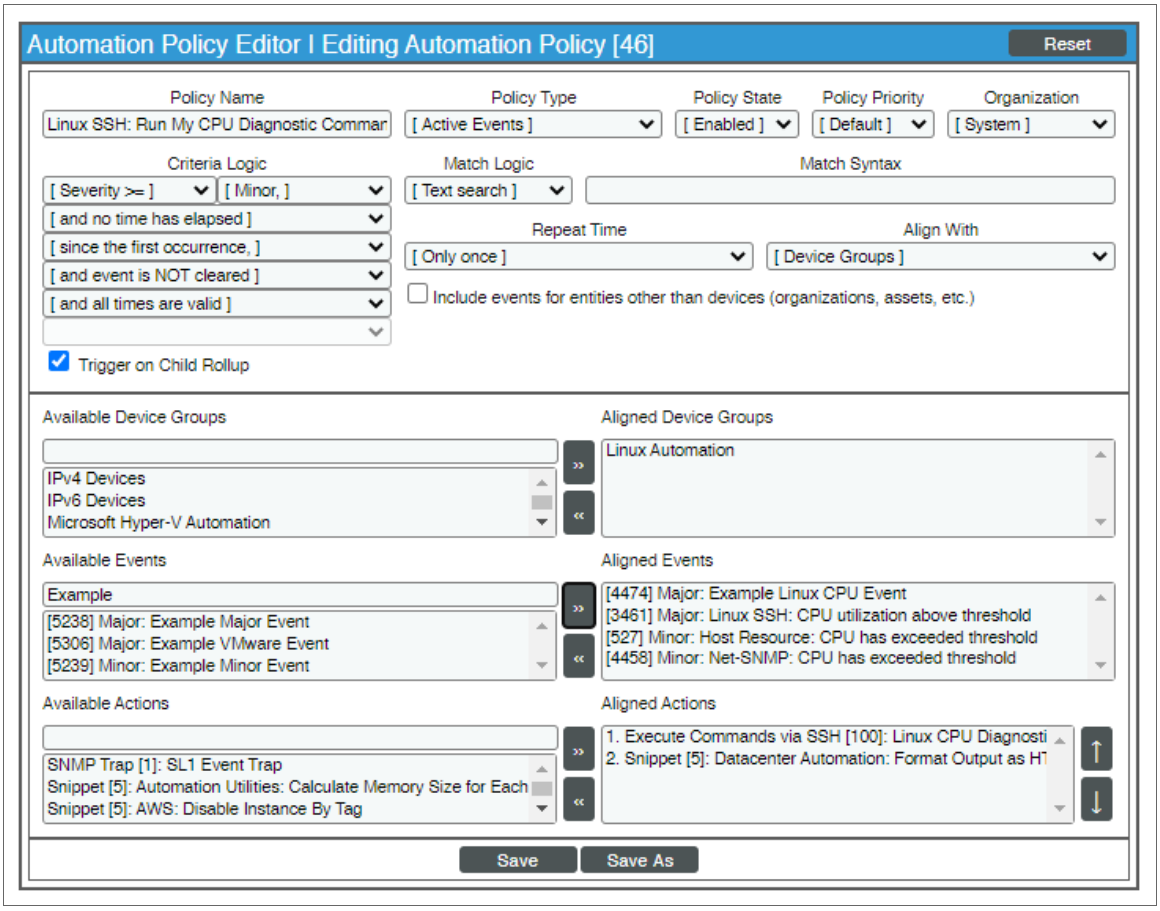
> **NOTE:** If you are selecting multiple collection actions that use the "Execute Shell Commands" action type, you may want to include the "Calculate Memory Size for Each Action" automation action, found in the *Datacenter Automation Utilities* PowerPack, in your automation policy.

4. Optionally, supply values in the other fields on this page to refine when the automation will trigger.
5. Click **[Save]**.

> **NOTE:** You can also modify one of the automation policies included with this PowerPack. Best practice is to use the **[Save As]** option to create a new, renamed automation policy, instead of customizing the standard automation policies. For more information, see *Customizing an Automation Policy*.
>
> **NOTE:** If you modify one of the included automation policies and save it with the original name, the customizations in that policy will be overwritten when you upgrade the PowerPack unless you remove the association between the automation policy and the PowerPack before upgrading.

Example Automation Configuration

The following is an example of an automation policy that uses the automation actions in the *Linux SSH Automation* PowerPack:



The policy uses the following settings:

- ***Policy Name***. The policy is named "Linux SSH: Run My CPU Diagnostics".
- ***Policy Type***. The policy runs when an event is in an active state. *Active Events* is selected in this field.
- ***Policy State***. *Enabled* is selected in this field. This policy is active and ready to use.
- ***Organization***. The policy executes for the Linux Devices organization.
- ***Criteria Logic***. The policy is configured to execute immediately when an event matches these criteria: "Severity >= Notice, and no time has elapsed since the first occurrence, and event is NOT cleared, and all times are valid".
- ***Aligned With***. The policy is configured to align with devices in the selected device group.

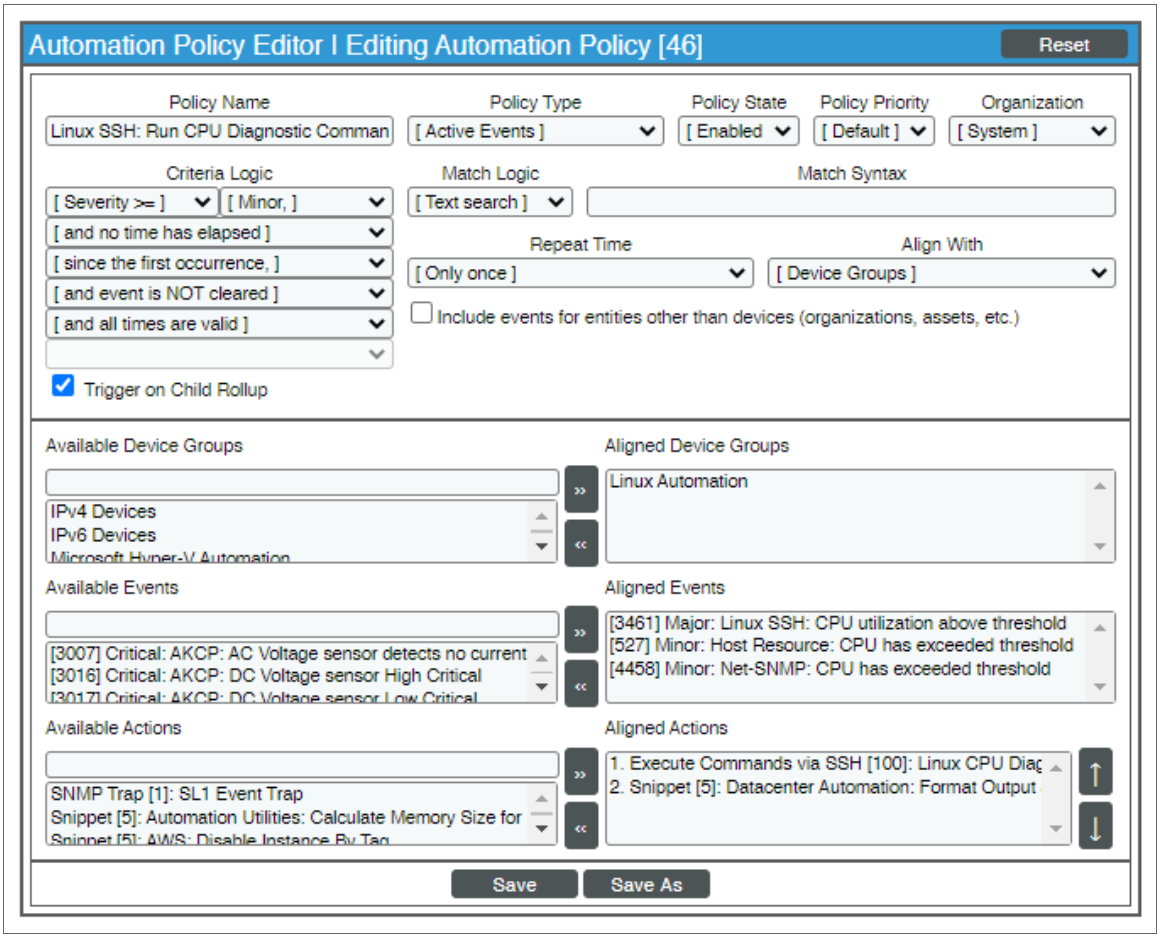
- ***Aligned Device Groups***. The policy is configured to trigger for devices in the "Linux Automation" device group.
- ***Aligned Events***. The policy is configured to trigger only when the following events are triggered:
    - Major: Example Linux CPU Event
    - Major: Linux SSH: CPU utilization above threshold
    - Minor: Host Resource: CPU has exceeded threshold
    - Minor: Net-SNMP: CPU has exceeded threshold
    - Notice: F5: BIG-IP: CPU fan speed signal not received
- ***Aligned Actions***. The automation includes the following actions. This action allows you to view the output of the diagnostic commands in the Automation Log, accessed through the SL1 **Events** page:
    - Execute Commands via SSH: Linux CPU Diagnostic Commands
    - Snippet [5]: Datacenter Automation: Format Output for ServiceNow Non-Scoped

Customizing an Automation Policy

To customize an automation policy:

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).

2. Search for the *Linux SSH Automation* automation policy you want to edit and click the wrench icon (🔧) for that policy . The **Automation Policy Editor** page appears:



3. Complete the following fields as needed:

   - ***Policy Name***. Type a new name for the automation policy to avoid overwriting the default policy.
   - ***Policy Type***. Select whether the automation policy will match events that are active, match when events are cleared, or run on a scheduled basis. Typically, you would select *Active Events* in this field.
   - ***Policy State***. Specifies whether the policy will be evaluated against the events in the system. If you want this policy to begin matching events immediately, select *Enabled*.
   - **Policy Priority**. Specifies whether the policy is high-priority or default priority. These options determine how the policy is queued.
   - ***Organization***. Select the organization that will use this policy.

- ***Aligned Actions***. This field includes the actions from the Linux SSH Automation PowerPack. You should see "Execute Commands via SSH" action in this field. To add an action to the ***Aligned Actions*** field, select the action in the ***Available Actions*** field and click the right arrow (**>>**). To re-order the actions in the ***Aligned Actions*** field, select an action and use the up arrow or down arrow buttons to change that action's position in the sequence.

> **NOTE:** You must have two Aligned Actions: one that runs the diagnostic or remediation commands and one that provides the output format. The actions providing the output formats are contained in the *Datacenter Automation Utilities* PowerPack, which is a prerequisite for running Linux SSH automations.

> **NOTE:** If you are selecting multiple collection actions that use the "Execute Shell Commands" action type, you may want to include the "Calculate Memory Size for Each Action" automation action, found in the *Datacenter Automation Utilities* PowerPack, in your automation policy.

4. Optionally, supply values in the other fields on the **Automation Policy Editor** page to refine when the automation will trigger.
5. Click **[Save As]**.

Removing an Automation Policy from a PowerPack

After you have customized a policy from a *Linux SSH Automation PowerPack*, you might want to remove that policy from that PowerPack to prevent your changes from being overwritten if you update the PowerPack later. If you have the license key with author's privileges for a PowerPack or if you have owner or administrator privileges with your license key, you can remove content from a PowerPack.

To remove content from a PowerPack:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Find the *Linux SSH Automation* PowerPack. Click its wrench icon ( ).
3. In the **PowerPack Properties** page, in the navigation bar on the left side, click **Run Book Policies**.
4. In the **Embedded Run Book Polices** pane, locate the policy you updated, and click the bomb icon ( ) for that policy. The policy will be removed from the PowerPack and will now appear in the bottom pane.

Chapter 5

Customizing Linux SSH Actions

Overview

This manual describes how to customize the automation actions embedded in the *Linux SSH Automation* PowerPack to create automation actions to meet your organization's specific requirements.

For more information about creating automation policies using custom action types, see *Creating and Customizing Automation Policies*.

This chapter covers the following topics:

Creating a Custom Action Policy 30

Customizing Automation Actions 31

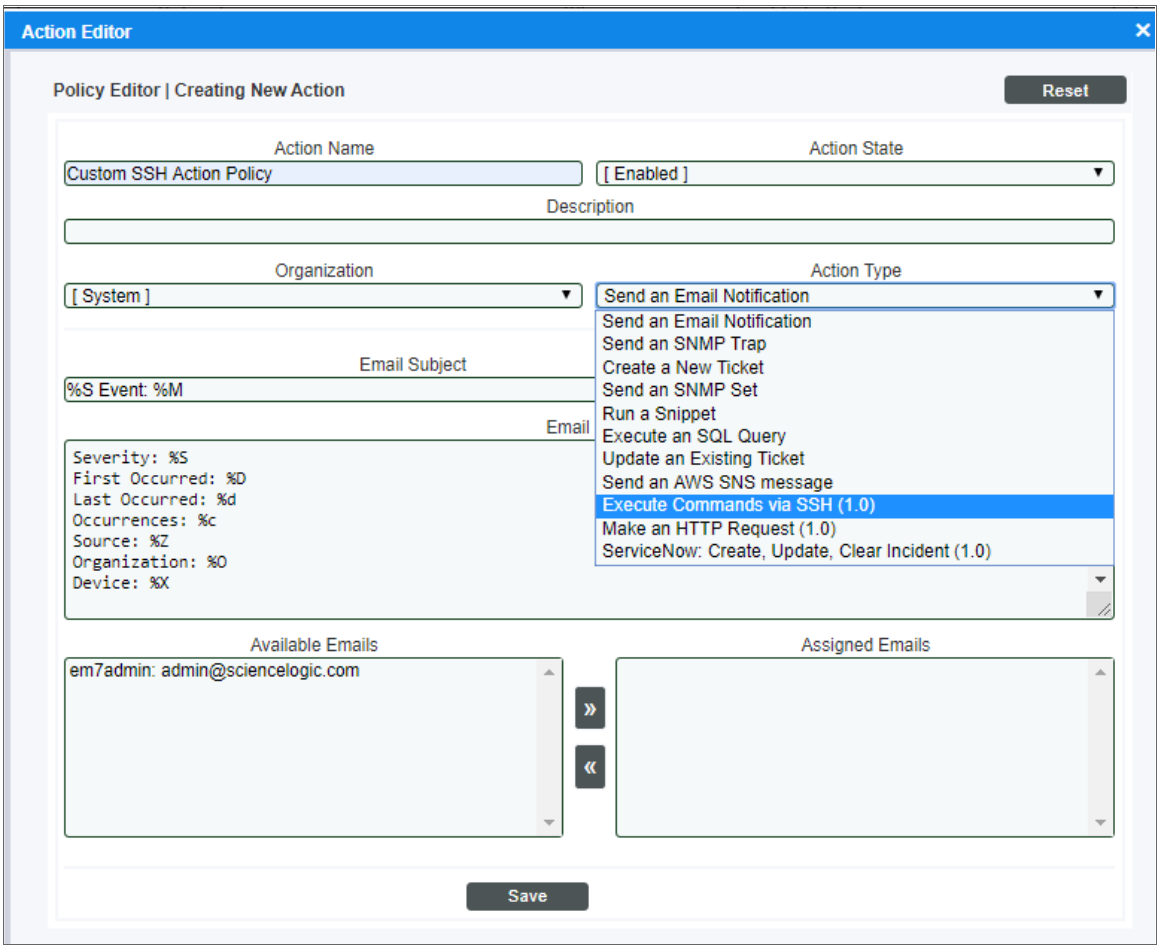
Creating a New Linux SSH Automation Action 34

Creating a Custom Action Policy

You can use the "Execute Shell Commands" action type included with the Linux SSH Automation PowerPack to create custom automation actions that you can then use to build custom automation policies.

To create a custom action policy using the "Execute Shell Commands" action type:

1. Navigate to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. In the **Action Policy Manager** page, click the **[Create]** button.
3. The **Action Policy Editor** modal appears.



4. In the **Action Policy Editor** page, supply a value in each field.

   - ***Action Name***. Specify the name for the action policy.
   - ***Action State***. Specifies whether the policy can be executed by an automation policy (enabled) or cannot be executed (disabled).
   - ***Description***. Allows you to enter a detailed description of the action.
   - ***Organization***. Organization to associate with the action policy.

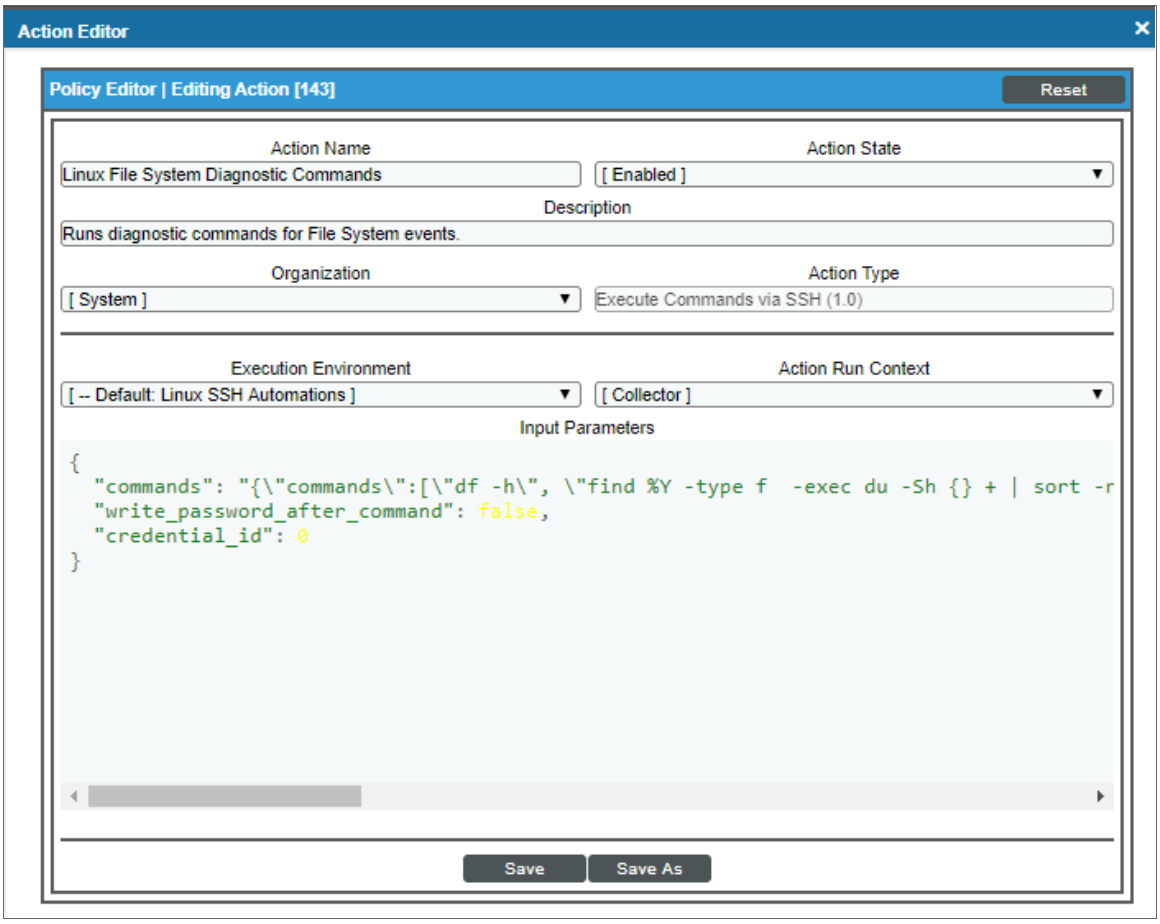
- ***Action Type***. Type of action that will be executed. Select the "Execute Shell Commands" action type (highlighted in the figure above).
- ***Execution Environment***. Select from the list of available Execution Environments. The default execution environment is *System*.
- ***Action Run Context***. Select *Database* or *Collector* as the context in which the action policy will run.
- ***Input Parameters***. A JSON structure that specifies each input parameter. Each parameter definition includes its name, data type, and whether the input is optional or required for this Custom Action Type. For more information about the available input parameters, see the table in *Creating a New Linux SSH Automation Action.*

NOTE: Input parameters must be defined as a JSON structure, even if only one parameter is defined.

5. Click **[Save]**. If you are modifying an existing action policy, click **[Save As]**. Supply a new value in the ***Action Name*** field, and save the current action policy, including any edits, as a new policy.

Customizing Automation Actions

The *Linux SSH Automation* PowerPack includes 10 automation actions that use the "Execute Shell Commands" action type to request diagnostic information or remediate an issue. You can specify the host and the options in a JSON structure that you enter in the ***Input Parameters*** field in the **Action Policy Editor** modal.



The following automation actions that use the "Execute Shell Commands" action type are included in the Linux SSH Automation PowerPack. Compare the commands run with the example in the image above. For more information about input parameter fields, see the table in *Creating a New Linux SSH Automation Action*.

Action Name	Description	Commands Run
Linux CPU Diagnostic Commands	Runs diagnostic commands for CPU events	• `top -b -n 1` • `ps -eo pid,ppid,%cpu,%mem,args --sort=-%cpu | head` • `pidstat` • `iostat -x 2 5` • `dmesg | tail`
Linux File System Diagnostic Commands	Runs diagnostic commands for File System events	• `df -h` • `find / -type f -exec du /home -Sh {} + 2> /dev/null | sort -rh | head -20`
Linux Illicit Process Remediation	Collects a list of users logged in to the system and sends a term signal to a Linux process.	• `sudo -S who` • `sudo -S kill %y`

Action Name	Description	Commands Run
Linux Interface Error/Discard Diagnostic Commands	Runs diagnostic commands for Interface Error/Discard events	• `ifconfig` • `ethtool %Y` • `dmesg | tail` • `netstat -i`
Linux Interface Utilization Diagnostic Commands	Runs diagnostic commands for Interface Utilization events	• `ethtool %Y` • `netstat -plunt` • `tcpdump -i %Y -c 100`
Linux Memory Dmidecode Command	Runs the dmidecode command with the memory option using sudo.	• `sudo -S dmidecode --type memory`
Linux Memory/Swap Diagnostic Commands	Runs diagnostic commands for Memory/Swap events	• `top -b -n 1` • `ps -eo pid,ppid,%cpu,%mem,args --sort=-%mem | head` • `swapon -summary` • `vmstat 2 5` • `dmidecode --type memory` • `dmesg | tail`
Linux Process Restart Remediation	Restarts a Linux service and collects service status before and after the restart command.	• `sudo -S service %Y status` • `sudo -S service %Y start` • `sudo -S service %Y status`
Linux System-Storage Diagnostic Commands	Runs diagnostic commands for File System events.	• `df -h` • `find / -type f -exec du -Sh {} + | sort -rh | head -n 20` • `find / -type f -mmin -10 -exec du -Sh {} + | sort -rh | head -n 20` • `find / -type d -exec du -Sh {} + | sort -rh | head -n 20` • `find / -type d -mmin -10 -exec du -Sh {} + | sort -rh | head -n 20`
Linux Tcpdump Command	Runs the tcpdump command using sudo.	• `sudo -S tcpdump -i %Y -c 100`

TIP: For more information about substitution variables, see *Appendix A*.

Creating a New Linux SSH Automation Action

You can create a new automation action that runs SSH commands using the supplied "Execute Shell Commands" custom action type. To do this, select "Execute Shell Commands" in the Action Type drop-down list when you create a new automation action. You can also use the existing automation actions in the PowerPack as a template by using the **[Save As]** option.

The SSH automation actions accept the following parameters in JSON:

Paramter	Input type	Description
commands	string	Specifies a single command or a list of commands, in JSON format, to execute. You can use substitution variables in the commands.
write_password_after_command	boolean	**Default value**: False (0) Set to True(1) if you know the automation must navigate a password prompt after running the command. The automation writes the password as a second input. This navigates the password prompt for commands that require sudo. Sudo commands run using this method must use the "-S" flag. **Example:** `sudo -S service nginx restart`
credential_id	integer	**Default value**: 0 Specifies the credential_id to use for the connection. • If set to 0 (false), the custom action type will dynamically determine the credential. For more information, see *Authentication for Linux Devices*. • If set to an ID number, it maps to the credential ID specified. You can find credential IDs by going to System > Manage > Credentials.

Using Substitution Values. The commands input can contain substitution values that match the keys in EM7_VALUES.

TIP: For more information about substitution variables, see *Appendix A*.

For a description of all options that are available in Automation Policies, see the ***Run Book Automation*** manual.

Chapter 6

Linux SSH User-Initiated Automations

Overview

This manual describes how to use the automation policies found in the *Linux SSH User-Initiated Automation* PowerPack

This PowerPack requires a subscription to one of the following solutions:

- *Datacenter Automation Pack*
- ScienceLogic Standard solution

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

This chapter covers the following topics:

What is the Linux SSH User-Initiated Automation PowerPack? 36
Installing the Linux SSH User-Initiated Automation PowerPack 36
Standard Automation Policies 37
Running a User Initiated Automation Policy 42
Viewing Automation Actions for an Event 43

What is the Linux SSH User-Initiated Automation PowerPack?

The *Linux SSH User-Initiated Automation* PowerPack includes automation policies that you can use to run Linux diagnostic commands from the SL1 event console , using Event Tools. This PowerPack is supplemental to the *Linux SSH Automation* PowerPack and is not meant for standalone use.

In addition to using the standard content, you can customize the automation policies, or you can create your own automation policies using any available automation actions.

Installing the Linux SSH User-Initiated Automation PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Linux SSH Automation* PowerPack and the *Linux Base Pack* PowerPack.

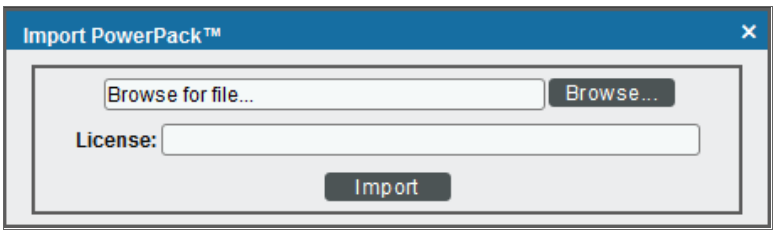
NOTE: The *Linux SSH User-Initiated Automation* PowerPack requires SL1 version 10.1.0 or later. For details on upgrading SL1, see the appropriate SL1 Release Notes.

WARNING: You must also install the *Datacenter Automation Utilities* PowerPack, which provides the output formats for the automation actions included in this PowerPack.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the ***System Administration*** manual.)

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Standard Automation Policies

The *Linux SSH User-Initiated Automation* PowerPack includes standard automation policies that trigger automation actions that will run Linux diagnostic commands from the SL1 event console.

The automation policies available in this release of the PowerPack are tied to included ScienceLogic SL1 events generated by the Dynamic Applications from the *Linux Base Pack* PowerPack.

The automation policies are of Policy Type, "User Initiated". This means that for an event that matches the criteria, you can run these automation policies from the **Event Console**.

For these automation policies to be visible from the Event Tools in the Event's drawer, the following three things must be true between the event and the automation policy configuration:

- ***Organization***. The organization associated with the event must match the organization configured in the automation policy. Policies in the "System" organization match all organizations.
- ***Aligned Devices***. The device for which the event is triggered must be configured as a Aligned Device in the automation policy.
- ***Aligned Event***. The event must match one of the Aligned Events configured in the automation policy.

The following table shows the automation policies, their aligned events, and the automation actions that run in response to the events.

NOTE: The aligned events are included as part of the *Linux Base Pack* PowerPack and are not installed with the SL1 platform. You must install the PowerPack to obtain these events.

Automation Policy Name	Aligned Events	Automation Action
Restart Process via SSH	• Poller: required process not running	• Linux Proces Restart Remediations • Datacenter Automation: Format Output as HTML
Run CPU Diagnostics (SSH)	• Linux SSH: CPU utilization above threshold	• Linux CPU Diagnostic Commands

Automation Policy Name	Aligned Events	Automation Action
	• Host Resource: CPU has exceeded threshold • Net-SNMP: CPU has exceeded threshold	• Datacenter Automation: Format Output as HTML
Run File System Diagnostics (SSH)	• Poller: File system usage exceeded (critical) threshold • Poller: File system usage exceeded (major) threshold	• Linux File System Diagnostic Commands • Datacenter Automation: Format Output as HTML
Run Interface Error/Discard Diagnostics (SSH)	• Interface inbound discards has exceeded the Falling-High threshold • Interface inbound discards has exceeded the Rising-High threshold • Interface inbound discards percentage has exceeded the Falling-High threshold • Interface inbound discards percentage has exceeded the Rising-High threshold • Interface inbound errors has exceeded the Falling-High threshold • Interface inbound errors has exceeded the Rising-High threshold • Interface inbound errors percentage has exceeded the Falling-High threshold • Interface inbound errors percentage has exceeded the Rising-High threshold • Interface outbound discards has exceeded the Falling-High threshold • Interface outbound discards has exceeded the Rising-High threshold • Interface outbound discards percentage has exceeded the Falling-High threshold • Interface outbound discards percentage has exceeded the Rising-High threshold • Interface outbound errors has exceeded the Falling-High threshold • Interface outbound errors has exceeded the Falling-High threshold • Interface outbound errors percentage has exceeded the Falling-High threshold • Interface outbound errors percentage has exceeded the Rising-High threshold	• Linux Interface Error/Discard Diagnostic Commands • Datacenter Automation: Format Output as HTML

Automation Policy Name	Aligned Events	Automation Action
	• Interface inbound discards has exceeded the Falling-Medium threshold • Interface inbound discards has exceeded the Rising-Medium threshold • Interface inbound discards percentage has exceeded the Falling-Medium threshold • Interface inbound discards percentage has exceeded the Rising-Medium threshold • Interface inbound errors has exceeded the Falling-Medium threshold • Interface inbound errors has exceeded the Rising-Medium threshold • Interface inbound errors percentage has exceeded the Falling-Medium threshold • Interface inbound errors percentage has exceeded the Rising-Medium threshold • Interface outbound discards has exceeded the Falling-Medium threshold • Interface outbound discards has exceeded the Rising-Medium threshold • Interface outbound discards percentage has exceeded the Falling-Medium threshold • Interface outbound discards percentage has exceeded the Rising-Medium threshold • Interface outbound errors has exceeded the Falling-Medium threshold • Interface outbound errors has exceeded the Falling-Medium threshold • Interface outbound errors percentage has exceeded the Falling-Medium threshold • Interface outbound errors percentage has exceeded the Rising-Medium threshold • Interface inbound discards has exceeded the Falling-Low threshold • Interface inbound discards has exceeded the Rising-Low threshold	

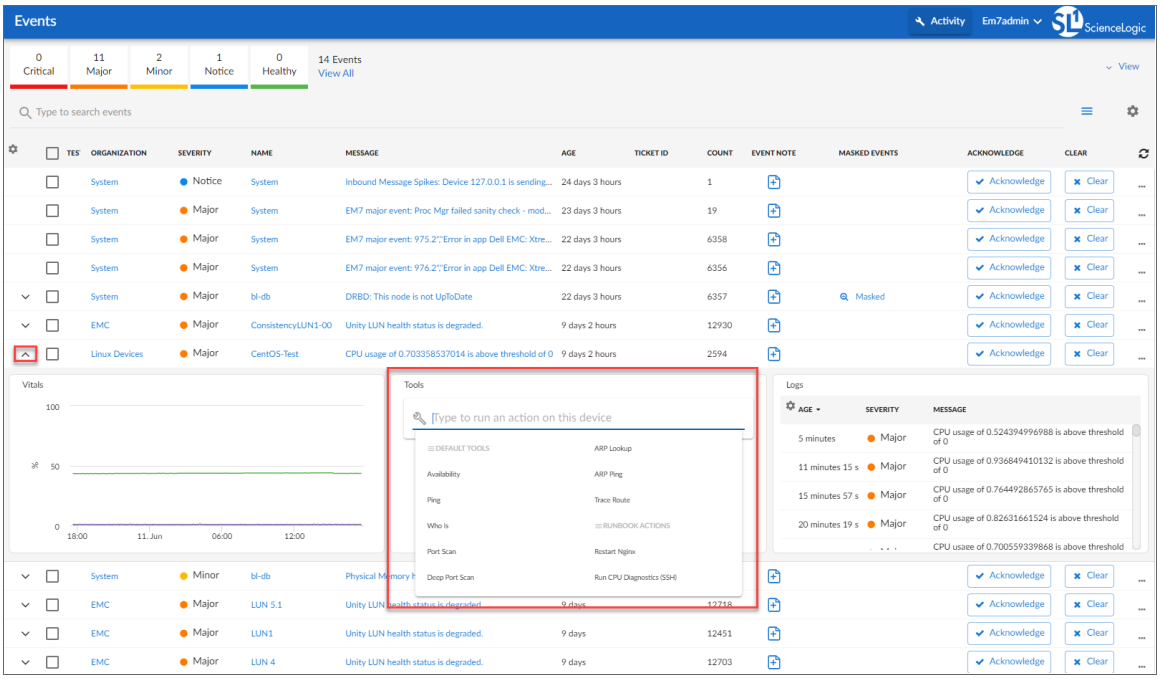
Automation Policy Name	Aligned Events	Automation Action
	• Interface inbound discards percentage has exceeded the Falling-Low threshold • Interface inbound discards percentage has exceeded the Rising-Low threshold • Interface inbound errors has exceeded the Falling-Low threshold • Interface inbound errors has exceeded the Rising-Low threshold • Interface inbound errors percentage has exceeded the Falling-Low threshold • Interface inbound errors percentage has exceeded the Rising-Low threshold • Interface outbound discards has exceeded the Falling-Low threshold • Interface outbound discards has exceeded the Rising-Low threshold • Interface outbound discards percentage has exceeded the Falling-Low threshold • Interface outbound discards percentage has exceeded the Rising-Low threshold • Interface outbound errors has exceeded the Falling-Low threshold • Interface outbound errors has exceeded the Falling-Low threshold • Interface outbound errors percentage has exceeded the Falling-Low threshold • Interface outbound errors percentage has exceeded the Rising-Low threshold • Poller: Interface reporting discards • Poller: Interface reporting packet errors	
Run Interface Utilization Diagnostics (SSH)	• Interface inbound usage percentage has exceeded the Falling-High threshold • Interface inbound usage percentage has exceeded the Rising-High threshold • Interface inbound usage rate has exceeded the Falling-High threshold • Interface inbound usage rate has exceeded the Rising-High threshold • Interface outbound usage percentage has exceeded the Falling-High threshold	• Automation Utilities: Calculate Memory Size for Each Action • Linux Interface Utilization Diagnostic Commands • Linux Tcpdump Command • Datacenter Automation: Format Output as HTML

Automation Policy Name	Aligned Events	Automation Action
	• Interface outbound usage percentage has exceeded the Rising-High threshold • Interface outbound usage rate has exceeded the Falling-High threshold • Interface outbound usage rate has exceeded the Rising-High threshold • Interface inbound usage percentage has exceeded the Falling-Medium threshold • Interface inbound usage percentage has exceeded the Rising-Medium threshold • Interface inbound usage rate has exceeded the Falling-Medium threshold • Interface inbound usage rate has exceeded the Rising-Medium threshold • Interface outbound usage percentage has exceeded the Falling-Medium threshold • Interface outbound usage percentage has exceeded the Rising-Medium threshold • Interface outbound usage rate has exceeded the Falling-Medium threshold • Interface outbound usage rate has exceeded the Rising-Medium threshold • Poller: Bandwidth usage exceeded threshold • Interface inbound usage percentage has exceeded the Falling-Low threshold • Interface inbound usage percentage has exceeded the Rising-Low threshold • Interface inbound usage rate has exceeded the Falling-Low threshold • Interface inbound usage rate has exceeded the Rising-Low threshold • Interface outbound usage percentage has exceeded the Falling-Low threshold • Interface outbound usage percentage has exceeded the Rising-Low threshold • Interface outbound usage rate has exceeded the Falling-Low threshold • Interface outbound usage rate has exceeded the Rising-Low threshold	

Automation Policy Name	Aligned Events	Automation Action
	• Poller: Bandwidth usage exceeded threshold	
Run Memory/Swap Diagnostics (SSH)	• Host Resource: Swap Memory has exceeded threshold • Linux SSH: Swap usage above threshold • Net-SNMP: Swap has exceeded threshold • Host Resource: Physical Memory has exceeded threshold • Net-SNMP: Physical Memory exceeded threshold	• Automation Utilities: Calculate Memory Size for Each Action • Linux Memory/Swap Diagnostic Commands • Linux Memory Dmidecode Command • Datacenter Automation: Format Output as HTML
Run System Storage Diagnostics (SSH)	• Linux SSH: File System over usage threshold	• Linus System-Storage Diagnostic Commands • Datacenter Automation: Format Output as HTML
Stop Illicit Process via SSH	• Poller: Illicit process running	• Linux Illicit Process Remediation • Datacenter Automation: Format Output as HTML

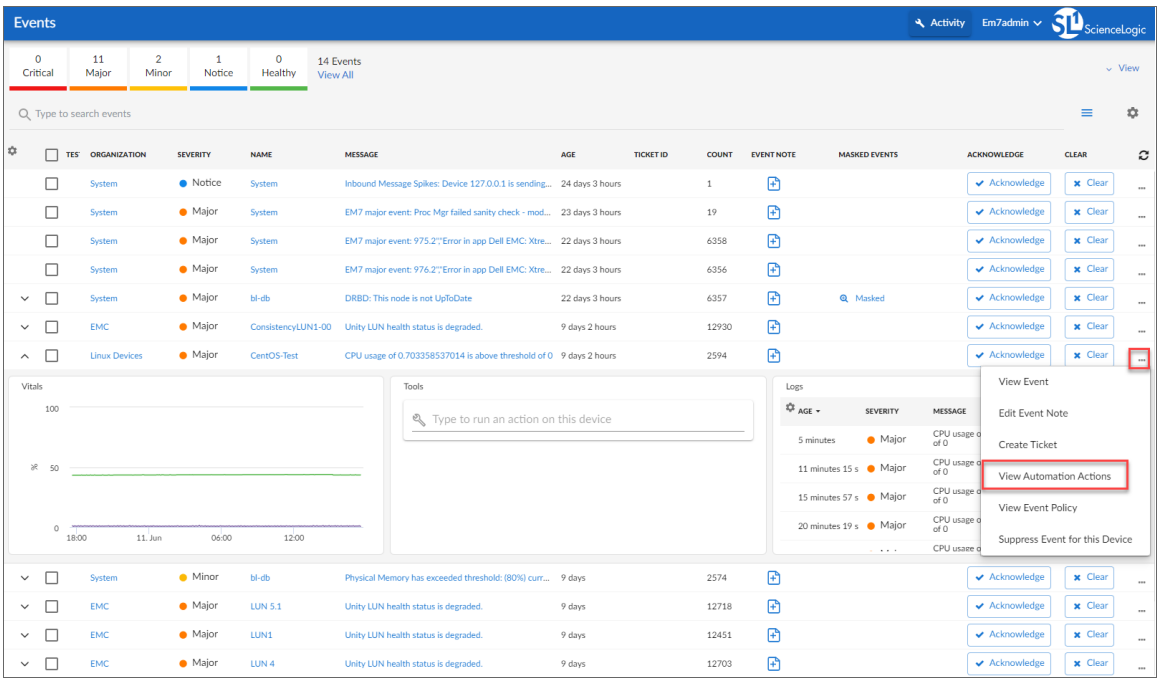
Running a User Initiated Automation Policy

To run a user initiated automation policy, open the drawer for the event and click in the Tools section. Any available user initiated automation policy will be available to run on demand.

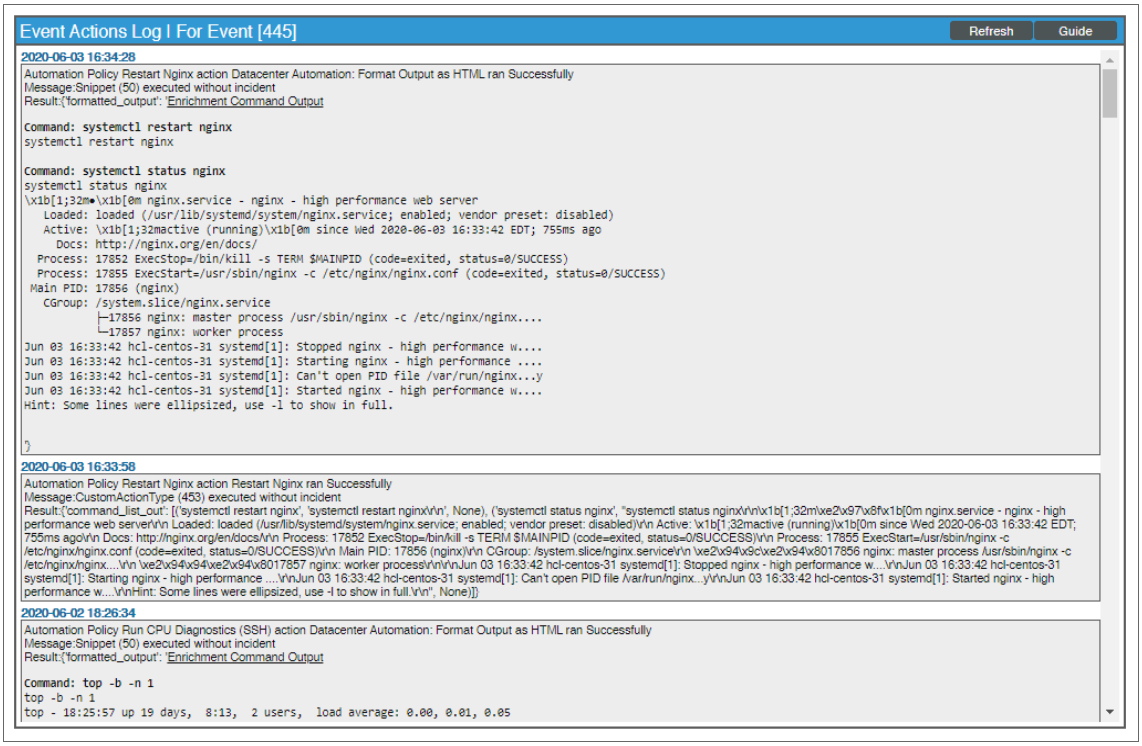


Viewing Automation Actions for an Event

The following figure shows a VMware event with major criticality on the **Events** page. Click the **[Actions]** button (⋯) for an event, and select *View Automation Actions* to see the automation actions triggered by the events.



The results shown for this event, in the **Event Actions Log**, include the automation policy that ran (shown at the top of the following figure), along with the collected data. The following figure shows an example of this output.



NOTE: To learn more about which logs are collected by default for a given automation action, see the *Customizing Linux SSH Actions* section.

TIP: Although you can edit the automation policy described in this section, it is a best practice to use "Save As" to create a new automation policy, rather than to customize the standard automation policies.

Appendix

A

Run Book Variables

Overview

This appendix defines the different variables you can use when creating an action policy.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all the menu options, click the Advanced menu icon (•••).

This appendix covers the following topics:

Run Book Variables *46*

Run Book Variables

You can include variables when creating an action policy. These variables are listed in the table below.

- In an action policy of type ***Send an Email Notification***, you can include one or more of these variables in the fields ***Email Subject*** and ***Email Body***.
- In an action policy of type ***Send an SNMP Trap***, you can include one or more of these variables in the ***Trap OID*** field, ***Varbind OID*** field, and the ***Varbind Value*** field.
- In an action policy of type ***Create a New Ticket***, you can include one or more of these variables in the ***Description*** field or the ***Note*** field of the related Ticket Template.
- In an action policy of type ***Send an SNMP Set***, you can include one or more of these variables in the ***SNMP OID*** field and the ***SNMP Value*** field.
- In an action policy of type ***Run A Snippet***, you can access variables from the global dictionary ***EM7_VALUES***.
- In a policy of type ***Execute an SQL Query***, you can include one or more of these variables in the ***SQL Query*** field.

Variable	Source	Description
%A	Account	Username
%N	Action	Automation action name
%g	Asset	Asset serial
%h	Asset	Device ID associated with the asset
%i (lowercase "eye")	Asset	Asset Location
%k	Asset	Asset Room
%K	Asset	Asset Floor
%P	Asset	Asset plate
%p	Asset	Asset panel
%q	Asset	Asset zone
%Q	Asset	Asset punch
%U	Asset	Asset rack
%u	Asset	Asset shelf
%v	Asset	Asset tag
%w	Asset	Asset model
%W	Asset	Asset make
%m	Automation	Automation policy note
%n	Automation	Automation policy name
%F	Dynamic Alert	Alert ID for a Dynamic Application Alert
%I (uppercase	Dynamic Alert	For events with a source of "dynamic", this variable contains the index value

Variable	Source	Description
"eye")		from SNMP. For events with a source of "syslog" or "trap", this variable contains the value that matches the ***Identifier Pattern*** field in the event definition.
%T	Dynamic Alert	Value returned by the Threshold function in a Dynamic Application Alert.
%V	Dynamic Alert	Value returned by the Result function in a Dynamic Application Alert.
%L	Dynamic Alert	Value returned by the label variable in a Dynamic Application Alert.
%a	Entity	IP address
%_category_id	Entity	Device category ID associated with the entity in the event.
%_category_ name	Entity	Device category name associated with the entity in the event.
%_class_id	Entity	Device class ID associated with the entity in the event.
%_class_name	Entity	Device class description associated with the entity in the event.
%_parent_id	Entity	For component devices, the device ID of the parent device.
%_parent_name	Entity	For component devices, the name of the parent device.
%_root_id	Entity	For component devices, the device ID of the root device.
%_root_name	Entity	For component devices, the name of the root device.
%1 (one)	Event	Entity type. Possible values are: • 0. Organization • 1. Device • 2. Asset • 4. IP Network • 5. Interface • 6. Vendor • 7. Account • 8. Virtual Interface • 9. Device Group • 10. IT Service • 11. Ticket
%2	Event	Sub-entity type. Possible values for organizations are: • 9. News feed Possible values for devices are: • 1. CPU • 2. Disk • 3. File System • 4. Memory • 5. Swap • 6. Component

Variable	Source	Description
		• 7. Interface • 9. Process • 10. Port • 11. Service • 12. Content • 13. Email
%4	Event	Text string of the user name that cleared the event.
%5	Event	Date/time when event was deleted.
%6	Event	Date/time when event became active.
%7	Event	Event severity (1-5), for compatibility with previous versions of SL1. 1=critical, 2=major, 3=minor, 4=notify, 5=healthy. **NOTE**: When referring to an event, %7 represents severity (for previous versions of SL1). When referring to a ticket, %7 represents the subject line of an email used to create a ticket.
%c	Event	Event counter
%d	Event	Date/time when last event occurred.
%D	Event	Date/time of first event occurrence.
%e	Event	Event ID
%H	Event	URL link to event
%M	Event	Event message
%s	Event	severity (0 - 4). 0=healthy, 1=notify, 2=minor, 3=major, 4=critical.
%S	Event	Severity (HEALTHY - CRITICAL)
%_user_note	Event	Current note about the event that is displayed on the **Events** page.
%x	Event	Entity ID
%X	Event	Entity name
%y	Event	Sub-entity ID
%Y	Event	Sub-entity name
%Z	Event	Event source (Syslog - Group)
%z	Event	Event source (1 - 8)
%_ext_ticket_ref	Event	For events associated with an external Ticket ID, this variable contains the external Ticket ID.
%3	Event Policy	Event policy ID
%E	Event Policy	External ID from event policy
%f	Event Policy	Specifies whether event is stateful, that is, has an associated event that will clear the current event. 1 (one)=stateful; 0 (zero)=not stateful.

Variable	Source	Description
%G	Event Policy	External Category
%R	Event Policy	Event policy cause/action text
%_event_policy_name	Event Policy	Name of the event policy that triggered the event.
%B	Organization	Organization billing ID
%b	Organization	Impacted organization
%C	Organization	Organization CRM ID
%o (lowercase "oh")	Organization	Organization ID
%O (uppercase "oh")	Organization	Organization name
%r	System	Unique ID / name for the current SL1 system
%7	Ticket	Subject of email used to create a ticket. If you specify this variable in a ticket template, SL1 will use the subject line of the email in the ticket description or note text when SL1 creates the ticket. **NOTE**: When referring to a ticket, %7 represents the subject line of an Email used to create a ticket. When referring to an event, %7 represents severity (for previous versions of SL1).
%t	Ticket	Ticket ID
%J	Ticket	Description field from the SL1 ticket.

© 2003 - 2022, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010