

Linux SSH Automation PowerPacks

Linux SSH Automation PowerPack version 104

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	
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	
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	32
Creating a New Linux SSH Automation Action	
Linux SSH User-Initiated Automations	
What is the Linux SSH User-Initiated Automation PowerPack?	.37
Installing the Linux SSH User-Initiated Automation PowerPack	
Standard Automation Policies	.38
Running a User Initiated Automation Policy	. 43
Viewing Automation Actions for an Event	
Run Book Variables	
Run Book Variables	.47

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
- 2020 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 <u>Release Notes</u>.

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 <u>ScienceLogic Support Site</u>.
- 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:

Import F	PowerPack™	×
Lic	Browse for file Browse Ernse: Import	

- 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.

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.

Automation Policy Name *	<u>10</u>	Policy State All	All	Organization	Devices	Events	Actions	Edited By	Last Edited
1 Bit inux SSH Illinit Drocese Demeritation		All 🔻	All						
1 A Linux SSH: Illicit Process Demediation					•				All
	127	Enabled	System		All	1	2	em7admin	2019-12-17 11:59:29
2. A Linux SSH: Process Restart Remediation	126	Enabled	System		All	1	2	em7admin	2019-12-17 11:59:29
3. 🤌 Linux SSH: Run CPU Diagnostic Commands	123	Enabled	System		All	3	2	em7admin	2019-12-17 11:59:29
4. A Linux SSH: Run File System Diagnostic Commands	124	Enabled	System		All	2	2	em7admin	2019-12-17 11:59:29
5. A Linux SSH: Run Interface Error/Discard Diagnostic Command	s 129	Enabled	System		All	50	2	em7admin	2019-12-17 11:59:29
6. A Linux SSH: Run Interface Utilization Diagnostic Commands	128	Enabled	System		All	25	3	em7admin	2019-12-17 11:59:29
7. 🤌 Linux SSH: Run Memory/Swap Diagnostic Commands	125	Enabled	System		All	5	3	em7admin	2019-12-17 11:59:29
8. A Linux SSH: Run System-Storage Diagnostic Commands	130	Enabled	System		All	1	2	em7admin	2019-12-17 11:59:29
Available Run Book Policies [1]									
Automation Policy Name -	ID	Policy State		Organization	Devices	Events	Actions	Edited By	Last Edited
			All						All
1. A Email for CPU 100	120	Enabled	System		2	5	1	em7admin	2019-11-27 09:45:34
			0,000			•			
	3 Juni SSH Bain CPU Disponish Commands 4 Juni SSH Bain Féb System Disponish Commands 5 Juni SSH Ruin Interface Utilization Disponsitic Commands 6 Juni SSH Ruin Interface Utilization Disponsitic Commands 7 Juni SSH Ruin Menny System Jagonotic Commands Juni SSH Ruin System Storage Dispositic Commands Available Ruin Book Policies [1]	A Junium SSH: Run CPU Dagnostic Commands 124 Junium SSH: Run File System Dagnostic Commands 124 Junium SSH: Run Interface Error/Discard Dagnostic Commands 126 Junium SSH: Run Interface Utilization Dagnostic Commands 127 Junium SSH: Run Interface Utilization Dagnostic Commands 128 Junium SSH: Run Rendom/service Disposite Commands 130 Available Run Book Policies [1] Automation Policy/Iams*	3. J Linux SSH Run CRU Diagnostic Commands 123 Enabled 4 Linux SSH Run File System Diagnostic Commands 124 Enabled 5 J Linux SSH Run Interface Error/Discard Diagnostic Commands 125 Enabled 7 J Linux SSH Run Interface Utilization Diagnostic Commands 126 Enabled 8 J Linux SSH Run Interface Utilization Diagnostic Commands 128 Enabled 8 J Linux SSH Run Rend System Storage Diagnostic Commands 120 Enabled 8 J Linux SSH Run System-Storage Diagnostic Commands 130 Enabled 8 Addition Policy Tame 10 Policy State Addition Policy Tame Al	3. PLInum SSH Rain CPU Diagnostic Commands 123 Enabled System 124 1 Linux SSH Rain File System Diagnostic Commands 124 Enabled System 125 Enabled System 128 Enabled System 129 Linux SSH Rain Interface Utilization Diagnostic Commands 128 Enabled System 129 Linux SSH Rain Interface Utilization Diagnostic Commands 128 Enabled System 129 Linux SSH Rain Interface Utilization Diagnostic Commands 128 Enabled System 129 Linux SSH Rain Interface Utilization Diagnostic Commands 128 Enabled System 129 Linux SSH Rain Interface Utilization Diagnostic Commands 120 Enabled System 120 Linux SSH Rain System-Storage Diagnostic Commands 130 Enabled System 120 Automation Diagnostic Commands 120 Enabled System 120 Automation 120	3. Junice SSH: Rain CPU Dogenotic Commands 124 Enabled System 4. Junice SSH: Rain Enterface EmailDocard Diagnostic Commands 124 Enabled System Software SSH: Rain Interface EmailDocard Diagnostic Commands 125 Enabled System Software SSH: Rain Interface Utilization Diagnostic Commands 126 Enabled System Software SSH: Rain Interface Utilization Diagnostic Commands 126 Enabled System Software SSH: Rain Interface Utilization Diagnostic Commands 126 Enabled System Software SSH: Rain Interface Utilization Diagnostic Commands 126 Enabled System Software SSH: Rain Interface Utilization Diagnostic Commands 126 Enabled System Auture SSH: Rain System-Storage Diagnostic Commands 130 Enabled System Available Run Book Policies [1] Austration Policy Jame • ID Policy State Ormatization Al • All	3. J Lunur SSH: Run CPU Dagnonic Commands 123 Enabled System All 41 Lunur SSH: Run Interface Email/Dagnotic Commands 124 Enabled System All 5 Junur SSH: Run Interface Utilization Dagnotic Commands 125 Enabled System All 7 Junur SSH: Run Interface Utilization Dagnotic Commands 125 Enabled System All 6 Junur SSH: Run Interface Utilization Dagnotic Commands 125 Enabled System All 7 Junur SSH: Run Interface Utilization Dagnotic Commands 125 Enabled System All 7 Junur SSH: Run Interface Utilization Dagnotic Commands 125 Enabled System All 7 Junur SSH: Run Rundwing/swige Dagnotic Commands 130 Enabled System All 7 Junur SSH: Run System-Storage Dagnotic Commands 130 Enabled System All 7 Junur SSH: Run System-Storage Dagnotic Commands 130 Enabled System All 7 Junur SSH: Run System-Storage Dagnotic Commands 130 Enabled System All 7 Junur SSH: Run System-Storage Dagnotic Commands 130 Enabled System All 7 Junur SSH: Run System-Storage Dagnotic Commands 130 Enabled System All	3. J. Lunux SSH: Run CRU Disposite Commands 123 Enabled System All 3 4. Junux SSH: Run Fiels System Disposite Commands 124 Enabled System All 2 5. Junux SSH: Run Interface Utication Disposite Commands 129 Enabled System All 50 6. Junux SSH: Run Interface Utication Disposite Commands 120 Enabled System All 25 7. Junux SSH: Run Interface Utication Disposite Commands 125 Enabled System All 5 8. Junux SSH: Run Interface Utication Disposite Commands 130 Enabled System All 1 All 25 All 25 Junux SSH: Run Englose Disposite Commands 130 Enabled System All 1 All 25 All 25 Junux SSH: Run System-Storage Disposite Commands 130 Enabled System All 1 Automic System Storage Disposite Commands 130 Enabled System All 1 Automic Site Run Book Policies [1]	3. Junix SSH: Run CHU Disponsite Commands 123 Enabled System Al 3 2 4. Junix SSH: Run Fiels System Disponsite Commands 124 Enabled System Al 5 2 5. Junix SSH: Run Interface Uticated Disponsite Commands 125 Enabled System Al 50 2 6. Junix SSH: Run Interface Uticated Disponsite Commands 125 Enabled System Al 5 3 7. Junix SSH: Run Interface Uticated Disponsite Commands 125 Enabled System Al 5 3 8. Junix SSH: Run Interface Utication Disponsite Commands 130 Enabled System Al 1 2 8. Junix SSH: Run Interface Utication Disponsite Commands 130 Enabled System Al 1 2	3. Junc SSH Run CEU Disposite Commands 123 Enabled System All 3 2 em/Jarimi 5. Junc SSH Run Fle System Daporatic Commands 124 Enabled System All 50 2 em/Jarimi 5. Junc SSH Run Interface Utilization Disposite Commands 129 Enabled System All 50 2 em/Jarimi 6. Junc SSH Run Interface Utilization Disposite Commands 129 Enabled System All 25 3 em/Jarimi 7. Junc SSH Run Interface Utilization Disposite Commands 128 Enabled System All 5 3 em/Jarimi 8. Junc SSH Run Englishing Disposite Commands 129 Enabled System All 1 2 em/Jarimi 8. Junc SSH Run System-Storage Disposite Commands 130 Enabled System All 1 2 em/Jarimi Addensite Set Run System-Storage Disposite Commands 130 Enabled System All 1 2 em/Jarimi

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 Falling-Medium threshold Interface inbound discards has exceeded the Rising-High 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-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 		
	 Interface outbound discards has exceeded the Falling-Medium threshold 		

Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
	 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 		
	 Interface inbound errors has exceeded the Falling-High threshold 		

Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
	 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 		
	 Interface outbound errors has exceeded the Falling-High threshold 		

Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
	 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		
	 Interface outbound errors percentage has exceeded the Rising- Medium threshold 		
	Poller: Interface reporting packet errors		

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

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

Automation Policy Name	Aligned Events	Aligned Device Group	Automation Action
Linux SSH: Run Memory/Swap Diagnostic Commands	 Interface outbound usage rate has exceeded the Rising-Low threshold Interface outbound usage rate has exceeded the Rising-Medium threshold 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 UtilitiesPowerPack) 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.

.ogic		vans-Mccarthy 🗸	Jude.E									Events
View	v						9 Events ïew All	2 Healthy	0 otice	7 Minor N	19 Major	1 Critical
0	=										search events	Q Type to
											3	ANY: linux 🔇
С	CLEAR	ACKNOWLEDGE	MASKED EVENTS	EVENT NO	I CO	AGE T		MESSAG	NAME	SEVERIT	ORGANIZATION	•
] •	X Clear	✓ Acknowledge	Q Masked	2 🕂	3	12 days 1 l	System /dev/loop1 : /sn	-1 Linux	ec2-18-2	🛑 Major	System	~
] •	X Clear	 Acknowledge 	Q Masked	9 🕂	3	12 days 1 l	System /dev/mapper/ce	Linux	10.2.24.3	🔴 Major	Linux Devices	~
	1.1.	 Acknowledge 		+	6	6 days 18 l	em usage exceeded maj.	/: File	10.2.24.3	🔴 Major	Linux Devices	~
	t	View Event		6 🕂	1	6 days	System /dev/loop0 : /sn	-1 Linux	ec2-18-2	🔴 Major	System	~
	Note	Edit Event N		+	3	1 hour 49 i	, Snippet: 1939 reporte.	App: 1	10.2.24.3	😑 Minor	Linux Devices	~
	ernal Ticket	Create Exte		+	1	6 minutes	atency below threshold	Netwo	10.2.24.3	🔵 Healt	Linux Devices	~
	mal Ticket	Align Extern										
	mation Actions	View Auton										
	t Policy	View Event										
	vent for this De	Suppress Ev										

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.

Ticket Editor Active Ticket [5]				Actions	New	Reset	Guide
Properties Logs Automation	<u>M</u> essage						
Event Actions Log For Event	[20545]						Refresh
2019-12-10 21:01:49							^
Automation Policy Linux SSH: Run File Syste Message:CustomActionType (427) executed v Result: <u>Enrichment Command Output</u>			ds action Linux File System Diagnostic Commands with HTML Output ra	n Successfully			
Command: df -h							
df -h							
Filesystem	Size Used	Avail	Use% Mounted on				
udev	727M Ø	727M	0% /dev				
tmpfs	150M 4.6M						
/dev/mapper/hclubuntu30vg-root			9% /				
tmpfs			0% /dev/shm				
tmpfs	5.0M 0	5.0M	0% /run/lock				
tmpfs			0% /sys/fs/cgroup				
/dev/sda1	472M 158M						
tmpfs	150M 0	150M	0% /run/user/1000				
40M /var/lib/apt/lists/us.archive 40M /boct/initrd.img.4.4.0-170-ge 40M /boct/initrd.img.4.4.0-169-ge 30M /var/log/wtmp.1 37M /boct/initrd.img.4.4.0-62-ger 25M /usr/lib/x86_64-linux-gnu/lib	sort -rh .ubuntu.com_ .ubuntu.com_ eneric meric .ucudata.so.5 .ubuntu.com_	he _ubuntu _ubuntu 55.1 _ubuntu	ad -20 _dists_xenial_universe_binary-i386_Packages _dists_xenial_universe_binary-amd64_Packages _dists_xenial_universe_i18n_Translation-en				
7.0M /boot/vmlinuz-4.4.0-170-gener 7.0M /boot/vmlinuz-4.4.0-169-gener	nic	-	_dists_xenial-updates_main_binary-amd64_Packages _dists_xenial_main_binary-i386_Packages				
			dists_xenial_main_binary-amd64_Packages				Ŧ
			Save Resolve				

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.



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].
- 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.

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	
Creating an Automation Policy	
Example Automation Configuration	
Customizing an Automation Policy	
Removing an Automation Policy from a PowerPack	

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.

Automation Policy Editor I Edition	ng Automation P	olicy [46]		Reset
Policy Name Linux SSH: Run CPU Diagnostic Comman Criteria Logic [Severity >=] [Minor,] [and no time has elapsed] [since the first occurrence,] [and event is NOT cleared] [and all times are valid] Trigger on Child Rollup	Policy Type [Active Events] Match Logic [Text search] Repeat [Only once] Include events for exercise	~	Match Syntax Aligr [Device Groups]	Organization [System] Twith Sector, etc.)
Available Device Groups IPv4 Devices IPv6 Devices Microsoft Huper-V Automation Available Events [3007] Critical: AKCP: AC Voltage sensor de [3016] Critical: AKCP: DC Voltage sensor Lo Available Actions	gh Critical 🚽 🏢	[527] Minor: Host F	ups SSH: CPU utilization Resource: CPU has ex SNMP: CPU has excee	ceeded threshold
SNMP Trap [1]: SL1 Event Trap Snippet [5]: Automation Utilities: Calculate N Snippet [5]: AWS: Disable Instance By Tag	Memory Size for 🔶 🤕		inds via SSH [100]: Lir acenter Automation: Fo	

- 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:

Policy Name	Policy Type	Policy	State	Policy Prio	rity C	Organization	
Linux SSH: Run My CPU Diagnostic Commar	Active Events]	✓ [Enable	ed] 🖌	[Default]	🖌 🛛 🕻 Sys	stem]	~
Criteria Logic	Match Logic		1	Match Syntax			
[Severity >=] V [Minor,] V	Text search]						
[and no time has elapsed]	Repeat	Time			Alian With		
[since the first occurrence,]				vice Groups]			~
[and event is NOT cleared]			-				-
[and all times are valid]	Include events for ent	ities other than devi	ces (orga	anizations, as	sets, etc.)		
~							
Available Device Groups Aligned Device Groups IPv4 Devices a IPv6 Devices a Microsoft Hyper-V Automation a							
Microsoft Hyper-V Automation	▲						
Microsoft Hyper-V Automation	★	Aligned Events					-
Microsoft Hyper-V Automation Available Events Example	α	[4474] Major: Exar					-
Microsoft Hyper-V Automation Available Events Example [5238] Major: Example Major Event	α • α	[4474] Major: Exar [3461] Major: Linu	CSSH: C	CPU utilization	n above thre		
Microsoft Hyper-V Automation Available Events Example [5238] Major: Example Major Event [5306] Major: Example VMware Event	▲ (() ▼ () ↓ ()	[4474] Major: Exar	c SSH: C Resource	CPU utilizatior e: CPU has e:	n above thre xceeded thre	eshold	-
Microsoft Hyper-V Automation Available Events Example [5238] Major: Example Major Event [5306] Major: Example VMware Event [5239] Minor: Example Minor Event	▲ ▼ (() ↓	[4474] Major: Exar [3461] Major: Linu [527] Minor: Host	c SSH: C Resource	CPU utilizatior e: CPU has e:	n above thre xceeded thre	eshold	-
Microsoft Hyper-V Automation Available Events Example [5238] Major: Example Major Event	»	[4474] Major: Exar [3461] Major: Linu [527] Minor: Host [4458] Minor: Net-	(SSH: (Resource SNMP: (ands via	CPU utilizatior e: CPU has e: CPU has exce SSH [100]: L	n above thre xceeded thre eeded thresh inux CPU D	eshold hold iagnosti 🔺	↓ ↓

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 (*P*) for that policy . The **Automation Policy Editor** page appears:

Policy Name	Policy Type	Policy State Policy Priority Organization
Linux SSH: Run CPU Diagnostic Comman	[Active Events]	✓ [Enabled ✓ [Default] ✓ [System] ✓
Criteria Logic	Match Logic	Match Syntax
[Severity >=] 🗸 [Minor,] 🗸	[Text search] 🗸	
[and no time has elapsed]	Repeat	t Time Alian With
[since the first occurrence,]	[Only once]	[Device Groups]
[and event is NOT cleared]		
[and all times are valid]	Include events for e	entities other than devices (organizations, assets, etc.)
~		
Trigger on Child Rollup		
Thigger on onlid Holidp		
wailable Device Groups		Aligned Device Groups
		Linux Automation
IPv4 Devices IPv6 Devices		
	~ «	
Microsoft Hyper-V Automation	v	Aligned Events
Microsoft Hyper-V Automation	•	
Microsoft Hyper-V/Automation Wailable Events	× «	Aligned Events [3461] Major: Linux SSH: CPU utilization above threshold [527] Minor: Host Resource: CPU has exceeded threshold
Microsoft Hyper-V Automation Available Events [3007] Critical: AKCP: AC Voltage sensor d		[3461] Major: Linux SSH: CPU utilization above threshold
Wicrosoft Hyper-V Automation Available Events (3007] Critical: AKCP: AC Voltage sensor d (3016] Critical: AKCP: DC Voltage sensor H	ligh Critical 🚽 🖉	[3461] Major: Linux SSH: CPU utilization above threshold [527] Minor: Host Resource: CPU has exceeded threshold
Wicrosoft Huper-V Automation Wailable Events 3007] Critical: AKCP: AC Voltage sensor d 3016] Critical: AKCP: DC Voltage sensor F 30171 Critical: AKCP: DC Voltage sensor L	ligh Critical 🚽 🖉	[3461] Major: Linux SSH: CPU utilization above threshold [527] Minor: Host Resource: CPU has exceeded threshold
Microsoft Hyper-V Automation	figh Critical 🗸 «	[3461] Major: Linux SSH: CPU utilization above threshold [527] Minor: Host Resource: CPU has exceeded threshold [4458] Minor: Net-SNMP: CPU has exceeded threshold Aligned Actions
Microsoft Huper-V Automation Available Events [3007] Critical: AKCP: AC Voltage sensor d [3016] Critical: AKCP: DC Voltage sensor L [3017] Critical: AKCP: DC Voltage sensor L Available Actions	ligh Critical 🚽 🖉	[3461] Major: Linux SSH: CPU utilization above threshold [527] Minor: Host Resource: CPU has exceeded threshold [4458] Minor: Net-SNMP: CPU has exceeded threshold Aligned Actions
Wicrosoft Hyper-V Automation Available Events [3007] Critical: AKCP: AC Voltage sensor d [3016] Critical: AKCP: DC Voltage sensor H [3017] Critical: AKCP: DC Voltage sensor L	iigh Critical	[3461] Major: Linux SSH: CPU utilization above threshold [527] Minor: Host Resource: CPU has exceeded threshold [4458] Minor: Net-SNMP: CPU has exceeded threshold Aligned Actions 1. Execute Commands via SSH [100]: Linux CPU Diac (*)
Microsoft Huner-V Automation Available Events [3007] Critical: AKCP: AC Voltage sensor d [3017] Critical: AKCP: DC Voltage sensor L 3017] Critical: AKCP: DC Voltage sensor L Available Actions [SNMP Trap [1]: SL1 Event Trap	iigh Critical	[3461] Major: Linux SSH: CPU utilization above threshold [527] Minor: Host Resource: CPU has exceeded threshold [4458] Minor: Net-SNMP: CPU has exceeded threshold Aligned Actions 1. Execute Commands via SSH [100]: Linux CPU Diac (*)

- 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 (**S**) for that policy. The policy will be removed from the PowerPack and will now appear in the bottom pane.

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	. 32
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.

Action Nar	ne	Action State	
Custom SSH Action Policy		[Enabled]	
	Desc	ription	
Organizati	on	Action Type	
[System]	¥	Send an Email Notification	
		Send an Email Notification	
		Send an SNMP Trap	
	Email Subject	Create a New Ticket	
%S Event: %M		Send an SNMP Set	
	Emai	Run a Snippet	
(a. 1) va	Lina	Execute an SQL Query	
Severity: %S First Occurred: %D		Update an Existing Ticket	
Last Occurred: %d		Send an AWS SNS message	
Occurrences: %c		Execute Commands via SSH (1.0) Make an HTTP Request (1.0)	
Source: %Z		ServiceNow: Create, Update, Clear Incident (1.0)	
Organization: %O		Servicentow. Create, opdate, clear incident (1.0)	
Device: %X			
Available Ema		Assigned Emails	
em7admin: admin@sciencelogic.com		-	
		»	
		«	
		-	
	_		

- 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.

Policy Editor Editing Action [143] Reset Action Name Action State Linux File System Diagnostic Commands [Enabled] Description Runs diagnostic commands for File System events. Organization Action Type [System] Execute Commands via SSH (1.0) Execution Environment Action Run Context [-Default: Linux SSH Automations] [Collector] Input Parameters { * "commands": "{\"commands\":[\"df -h\", \"find %Y -type f -exec du -Sh {} + sort -r "write_password_after_command": false, "credential_id": 0	on Editor					
Linux File System Diagnostic Commands [[Enabled] Description Runs diagnostic commands for File System events. Organization Commands via SSH (1.0) Execute Commands via SSH (1.0) Execution Environment Commands via SSH (1.0) Commands via SSH Automations via Context [Default: Linux SSH Automations] Commands via Context [Default: Linux SSH Automations] Context [Default: Linux SSH Automations] Commands via Context [Default: Linux SSH Automations] Command via Context [D	Policy Editor Editing Action [143]	Reset				
Description Runs diagnostic commands for File System events. Organization Action Type [System] Execute Commands via SSH (1.0) Execution Environment Action Run Context [- Default: Linux SSH Automations] [Collector] Input Parameters { "commands": "{\"commands\":[\"df -h\", \"find %Y -type f -exec du -Sh {} + sort -r "write_password_after_command": false, "credential_id": 0 } }						
Runs diagnostic commands for File System events. Organization Action Type [System] Execute Commands via SSH (1.0) Execution Environment Action Run Context [Default: Linux SSH Automations] Icollector] Input Parameters Input Parameters { "commands": "{\"commands\":[\"df -h\", \"find %Y -type f -exec du -Sh {} + sort -r "credential_id": 0 }						
Organization Action Type [System] Execute Commands via SSH (1.0) Execution Environment Action Run Context [Default: Linux SSH Automations] [Collector] Input Parameters "commands": "{\"commands\":[\"df -h\", \"find %Y -type f -exec du -Sh {} + sort -r "write_password_after_command": false, "credential_id": 0 } 						
<pre>[[System] Execution Environment Action Run Context [Default: Linux SSH Automations] Input Parameters { "commands": "{\"commands\":[\"df -h\", \"find %Y -type f -exec du -Sh {} + sort -r "write_password_after_command": false, "credential_id": 0 }</pre>						
Execution Environment Action Run Context [Default: Linux SSH Automations] [Collector] Input Parameters "commands": "{\"commands\":[\"df -h\", \"find %Y -type f -exec du -Sh {} + sort -r "write_password_after_command": false, "credential_id": 0 } 						
<pre>[Default: Linux SSH Automations] Input Parameters { "commands": "{\"commands\":[\"df -h\", \"find %Y -type f -exec du -Sh {} + sort -r "write_password_after_command": false, "credential_id": 0 }</pre>	[System]	Execute Commands via SSH (1.0)				
<pre>[Default: Linux SSH Automations] Input Parameters { "commands": "{\"commands\":[\"df -h\", \"find %Y -type f -exec du -Sh {} + sort -r "write_password_after_command": false, "credential_id": 0 }</pre>						
<pre>Input Parameters { "commands": "{\"commands\":[\"df -h\", \"find %Y -type f -exec du -Sh {} + sort -r "write_password_after_command": false, "credential_id": 0 }</pre>						
<pre>{ "commands": "{\"commands\":[\"df -h\", \"find %Y -type f -exec du -Sh {} + sort -r "write_password_after_command": false, "credential_id": 0 }</pre>						
	"write_password_after_command": false,					
Save Save As						

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	Runs diagnostic commands for CPU events	• top -b -n 1
Commands		 ps -eo pid,ppid,%cpu,%mem,args sort=-%cpu head
		• pidstat
		• iostat -x 2 5
		• dmesg tail
Linux File System	Runs diagnostic commands for File System events	• df -h
Diagnostic Commands		 find / -type f -exec du /home -Sh {} + 2> /dev/null sort -rh head -20
Linux Illicit Process	Collects a list of users logged in to the system and	• sudo -S who
Remediation	sends a term signal to a Linux process.	• sudo -S kill %y
Linux Interface	Runs diagnostic commands for Interface	• ifconfig
Error/Discard Diagnostic Commands	Error/Discard events	• ethtool %Y
		• dmesg tail
		• netstat -i
Linux Interface	Runs diagnostic commands for Interface Utilization	• ethtool %Y
Utilization Diagnostic Commands	events	• 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	Runs diagnostic commands for Memory/Swap	• top -b -n 1
Diagnostic Commands	events	• ps -eo pid,ppid,%cpu,%mem,args
		sort=-%mem head
		• swapon -summary
		• vmstat 2 5
		• dmidecodetype 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

Action Name	Description	Commands Run
		 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	lnput 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.

Paramter	Input type	Description
		• If set to 0 (false), the custom action type will dynamically determine the credential. For more information, see <i>Authentication for Linux Devices</i> .
		 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.

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
- 2020 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?		
Installing the Linux SSH User-Initiated Automation PowerPack		
Standard Automation Policies	38	
Running a User Initiated Automation Policy		
Viewing Automation Actions for an Event		

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<u>Release Notes</u>.

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:

Import Pow	erPack™	×
Licens	wse for file Browse Browse	

- 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 Host Resource: CPU has exceeded threshold 	 Linux CPU Diagnostic Commands

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

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 	
	 Interface inbound discards percentage has exceeded the Falling-Low threshold 	

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

Automation Policy Name	Aligned Events	Automation Action
	 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 	
	 Poller: Bandwidth usage exceeded threshold 	

Automation Policy Name	Aligned Events	Automation Action
Run Memory/Swap Diagnostics (SSH)	Host Resource: Swap Memory has exceeded threshold	Automation Utilities: Calculate Memory Size for Each Action
	 Linux SSH: Swap usage above threshold Net-SNMP: Swap has exceeded threshold 	 Linux Memory/Swap
	·	Diagnostic Commands
	 Host Resource: Physical Memory has exceeded threshold 	 Linux Memory Dmidecode Command
	 Net-SNMP: Physical Memory exceeded threshold 	 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.

Eve	ents	;												🔍 Activity	Em7admin 🗸		ceLogic
	0 itical		11 2 Major Mino	r Notice	0 14 E Healthy View	Events v All										v	View
Q	Туре	e to sea	arch events													=	۵
¢] TES	ORGANIZATION	SEVERITY	NAME	MESSAGE			AGE	TICKET ID	COUNT	EVENTING	DTE MASKED EVENTS		ACKNOWLEDGE	CLEAR	c
]	System	 Notice 	System	Inbound Me	essage S	pikes: Device 127.0.0.1 is sending	24 days 3 ho	urs	1	÷			✓ Acknowledge	X Clear]
			System	 Major 	System	EM7 major	event: P	roc Mgr failed sanity check - mod	23 days 3 ho	urs	19	+			✓ Acknowledge	X Clear]
]	System	 Major 	System	EM7 major	event: 9	75.2","Error in app Dell EMC: Xtre	22 days 3 ho	urs	6358	÷			✓ Acknowledge	X Clear]
]	System	 Major 	System	EM7 major	event: 9	76.2","Error in app Dell EMC: Xtre	22 days 3 ho	urs	6356	÷			✓ Acknowledge	X Clear]
~]	System	 Major 	bl-db	DRBD: This	node is	not UpToDate	22 days 3 ho	urs	6357	÷	Q Masked		✓ Acknowledge	× Clear]
~			EMC	 Major 	ConsistencyLUN1-00	Unity LUN I	nealth st	atus is degraded.	9 days 2 hou	irs	12930	÷			✓ Acknowledge	× Clear]
^]	Linux Devices	 Major 	CentOS-Test	CPU usage	of 0.703	358537014 is above threshold of 0	9 days 2 hou	irs	2594	÷			 Acknowledge 	X Clear]
Vit	als					_	Tool	s					Logs				
	10	0				_	2	Type to run an action on	this device	9			AGE - SEVERITY	MESSAGE			
							4	≡ DEFAULT TOOLS	ARP	Lookup	-		5 minutes 😑 Majo	of 0	ge of 0.524394996988		
	» ⁶ 5	• _						Availability	ARP	Ping			11 minutes 15 s 🛛 Majo	of 0	ge of 0.936849410132		
								Ping	Trac	e Route			15 minutes 57 s e Majo	of 0	ge of 0.764492865765		
		0 18:0	0 11. Jun	06:00	12:00			Who Is	= R	UNBOOK ACTIONS			20 minutes 19 s e Majo	of 0	ge of 0.82631661524 is		
								Port Scan	Rest	art Ngiros				CPU usa	ee of 0.700559339868	is above thresh	old
~			System	 Minor 	bl-db	Physical M	mory h	Deep Port Scan	Run	CPU Diagnostics (SSH)		Ð			Acknowledge	X Clear	
~			EMC	 Major 	LUN 5.1	Unity LUN	ealth st	atus is degraded	9 days		12718	Ð			✓ Acknowledge	× Clear	
~		ו	EMC	 Major 	LUN1	Unity LUN I	nealth st	atus is degraded.	9 days		12451	÷			✓ Acknowledge	× Clear]
~]	EMC	 Major 	LUN 4	Unity LUN I	nealth st	atus is degraded.	9 days		12703	+			Acknowledge	X Clear	

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.

Eve	nts												🔍 Activity	Em7admin 🗸		eLogic
) tical	11 2 Major Minor	1 Notice	0 14 E Healthy Viev	Events w All										v	View
Q	Type to s	earch events													=	۵
¢	Пте	S' ORGANIZATION	SEVERITY	NAME	MESSAGE		AGE	TICKET ID	COUNT	EVENT NO	DTE MA	SKED EVENTS	ACH	NOWLEDGE	CLEAR	c
		System	 Notice 	System	Inbound Messa	ge Spikes: Device 127.0.0.1 is sending	24 days 3 hours		1	÷			•	Acknowledge	X Clear	
		System	 Major 	System	EM7 major ever	nt: Proc Mgr failed sanity check - mod	23 days 3 hours		19	÷			•	Acknowledge	X Clear	
		System	 Major 	System	EM7 major ever	nt: 975.2", Error in app Dell EMC: Xtre	22 days 3 hours		6358	Ð			•	Acknowledge	X Clear	
		System	 Major 	System	EM7 major ever	nt: 976.2","Error in app Dell EMC: Xtre	22 days 3 hours		6356	÷			•	Acknowledge	X Clear	
~		System	 Major 	bl-db	DRBD: This not	de is not UpToDate	22 days 3 hours		6357	÷	Q	Masked		Acknowledge	X Clear	
~		EMC	 Major 	ConsistencyLUN1-00	Unity LUN heal	ith status is degraded.	9 days 2 hours		12930	÷			-	Acknowledge	X Clear	
^		Linux Devices	 Major 	CentOS-Test	CPU usage of 0	0.703358537014 is above threshold of 0	9 days 2 hours		2594	÷			•	Acknowledge	X Clear	
Vita						Tools					Logs			View Event		
	100					🖏 Type to run an action on	this device				🋱 AGE 🕶	SEVERITY	MESSAGE	Edit Event N	ote	
											5 minutes	😑 Major	CPU usage o of 0	Create Ticke	t	
Э	50				- 1						11 minutes 15	5 s 😑 Major	CPU usage o of 0	View Autom	ation Actions	٦
											15 minutes 57	7 s 😑 Major	CPU usage o of 0	View Event F	Policy	-
	0 18	:00 11. Jun	06:00	12:00							20 minutes 19	9 s 😑 Major	CPU usage o of 0 CPU usage o	Suppress Eve	ent for this De	vice
~		System	e Minor	bl-db	Physical Memor	ry has exceeded threshold: (80%) curr	9 days		2574	Đ				Acknowledge	X Clear	
~		EMC	 Major 	LUN 5.1	Unity LUN heal	Ith status is degraded.	9 days		12718	Ð				Acknowledge	× Clear	
~		EMC	 Major 	LUN1	Unity LUN heal	Ith status is degraded.	9 days		12451	÷			•	Acknowledge	X Clear	
~		EMC	 Major 	LUN 4	Unity LUN heal	Ith status is degraded.	9 days		12703	(+)				Acknowledge	× Clear	

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.

Event Actions Log I For Event [445]	Refresh Guide
020-06-03 16:34-28	
Automation Policy Restart Nginx action Datacenter Automation: Format Output as HTML ran Successfully Message:Snippet (50) executed without incident Result:{formatted_output': <u>Enrichment Command Output</u>	
Command: systemctl restart nginx	
systemctl restart nginx	
Command: systemctl status nginx systemctl status nginx	
(x1b[1;32m*\x1b[@m nginx.service - nginx - high performance web server Loaded: Loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled) Active: \x1b[1;32mctive (running)\x1b[@m since Wed 2020-06-03 16:33:42 EDT: 755ms ago	
ACTIVE: (XLD[1,52mmClTVE (Tuminig)/XLD[am Since Wed 2626-66-65 16:55:42 EDT, 755m5 agu Docs: http://nginx.org/en/docs/	
Process: 17852 ExecStop=/bin/kill -s TERM \$MAINPID (code=exited, status=0/SUCCESS)	
Process: 17855 ExecStart=/usr/sbin/nginx -c /etc/nginx/nginx.conf (code=exited, status=0/SUCCESS)	
Main PID: 17856 (nginx) CGroup: /system.slice/nginx.service	
Large nginx: master process /usr/sbin/nginx -c /etc/nginx/nginx	
-17857 nginx: worker process	
un 03 16:33:42 hcl-centos-31 systemd[1]: Stopped nginx - high performance w	
Jun 03 16:33:42 hcl-centos-31 systemd[1]: Starting nginx - high performance	
Jun 03 16:33:42 hcl-centos-31 systemd[1]: Can't open PID file /var/un/nginxy	
Jun 03 16:33:42 hcl-centos-31 systemd[1]: Started nginx - high performance w	
Jun 03 16:33:42 hcl-centos-31 systemd[1]: Started nginx - high performance w	
un 03 16:33:42 hcl-centos-31 systemd[l]: started nginx - high performance w int: some lines were ellipsized, use -l to show in full.	
un 03 16:33:42 hCl-centos-31 systemd[1]: Started nginx - high performance w int: Some lines were ellipsized, use -l to show in full. 020-06-03 16:33:58	
Jun 03 16:33:42 hCl-centos-31 Systemd[1]: Started nginx - high performance w int: Some lines were ellipsized, use -l to show in full.) 020-06-03 16:33:58 Automation Policy Restart Nginx action Restart Nginx ran Successfully Automation Policy Restart Nginx action Restart Nginx ran Successfully	
Jun 03 16:33:42 hCl-centos-31 Systemd[1]: Started nginx - high performance w int: Some lines were ellipsized, use -l to show in full.) <u>020-06-03 16:33:58</u> Jutomation Policy Restart Nginx action Restart Nginx ran Successfully Wessage/CustomActionType (433) executed without incident Pacult(Command Lisc.put; "Evistement estation and incident action of the start nginx/n", None), ("systemati status nginx, "systemati status nginx/n") 1:32m/we2V97v&	Wx1b[0m nginx.service - nginx - high_
Jun 83 16:33:42 hCl-centos-31 Systemd[1]: Started nginx - high performance w iint: Some lines were ellipsized, use -l to show in full.) <u>020-06-03 16:33:58</u> Automation Policy Restart Nginx action Restart Nginx ran Successfully Message:CustomactionType (43) executed without incident Result:Command_List_out:[(systemct] restart nginx,"systemct] restart nginx\n'n, None), (systemct] status nginx\"n\x1b[1,32m\x2v97x6 Resoframance web serverivh_Loaded: loaded (usrIb/bsystemMsystem/nginx.service; enabled; vendor preset: disabled)\vn Active: \x1b[1,32m\x2v97x6 Resoframance web serverivh_Loaded: loaded (usrIb/bsystemMsystem/nginx.service; enabled; vendor preset: disabled)\vn Active: \x1b[1,32m\x2v1b]Om	since Wed 2020-06-03 16:33:42 EDT;
<pre>un @3 16:33:42 hcl-centos-21 systemd[1]: Started nginx - high performance w int: some lines were ellipsized, use -l to show in full. 2020-06:03 16:33:58 Uutomation Policy Restart Nginx action Restart Nginx ran Successfully //essage/CustomActionType (43) executed without incident //esult/command_list_out: [Systemct] restart nginx, 'systemct] restart nginx/vin, None), (systemct] status nginx, "systemct] status nginx/viny1b[1.32m/ve2v97vc2 reformance web server/vin Loaded (bus/fib/system/disystem/figinx.service, enabled, vendor preset: disabled/vin Active: xtb[1].32mactive (running)/xtb[0m 75m sag/vin Doc: http://ginu.cgfendices/vin Process: 1785 Execs(hop-hin/lini = TERN/SMINIPD] (code=execd, status-GOVCESS)/vin Process: 1785 Execs(hop-hin/lini = TERN/SMINIPD) (code=execd, status-GOVCESS)/vin Process: 1785 Execs(hop-hin/lini = TERN/SMINIPD)</pre>	since Wed 2020-06-03 16:33:42 EDT; ecStart=/usr/sbin/nginx -c
<pre>Lun 03 16:33:42 hcl-centos-21 systemd[1]: Started nginx - high performance w int: some lines were ellipsized, use -l to show in full. DCO-06-03 16:33:58 Lutomation Policy Restart Nginx action Restart Nginx ran Successfully Aessage CustomActionType (43): executed without incident result Command_Lisc.ut: [Systemcl restart nginx, 'systemcl restart nginx\'n', None), ('systemct status nginx, 'systemct! status nginx\'n'x1b[1,32m/ve2V97v& performance web serverVn Loaded: loaded (/usr/lib/system/drystem/system/inix.service; enabled; vendor preset: disabled/vin Active: x1b[1,32m.ezV97v& performance web serverVn Loaded: loaded (/usr/lib/system/drystem/system/ini/Lib TERN KMINPID [code=exite, status-0/SUCCESS]Vn Process: 17855 ExetChpinxhginx.com/ (code=exite, status-0/SUCCESS)Vn Process: 17855 techpinxhginx.com/code=otied, status-0/SUCCESS)Vn Process: 17855 methor/uncited, status-0/SUCCESS)Vn Process: 17855 techpinxhginx.com/code=otied, status-0/SUCCESS)Vn Process: 17855 techpinxhginx.com/system/liber/pinxbervinyling Performance web pervervin vezv94vs2044vs2</pre>	n since Wed 2020-06-03 16:33:42 EDT; tecStant=/usr/sbin/nginx -c jinx: master process /usr/sbin/nginx -c VnJun 03 16:33:42 hcl-centos-31
un 83 16:33:42 hcl-centos-31 systemd[1]: started nginx - high performance w int: some lines were ellipsized, use -1 to show in full. 200-06-03 16:33:58 utomation Policy Restart Nginx action Restart Nginx ran Successfully lessage:CustomActionType (453) executed without incident restmance were in Loaded: loaded (Lustin)/Systemicity setemicity enabled, vendor preset: disabled/wh.Active: xtb[1]:32mactive (running/xtb[0m 55ms ago/vh.Docs: http://nginx.org/endocs/wh Process: 17852 ExectStop=/bin/kill -s TERM SMAINPy incode=xstude, status=0/SUCCESS)/vh.Process: 17852 ExectStop=/bin/kill -s TERM SMAINPy incode: status-0/SUCCESS)/vh.Process: 17852 ExectStop=/bin/kill -s TERM SMAINPy incode: status=0/SUCCESS)/vh.Process: 17852 ExectStop=/bin/kill -s TERM SMAINPy incode=xstude, status=0/SUCCESS)/vh.Process: 17852 ExectStop=-bin/kill -s TERM SMAINPy incode=xstude, status=0/SUCCESS)/vh.Process: 17852 ExectStop=-bin/kill -s TERM SMAINPy incode=xstude, status=0/SUCCESS)/vh.Process: 17852 ExectStop=-bin/kill -s TERM SMAINPy incode: status=0/SUCCESS)/vh.Process: 17852 ExectStop=-bin/kill -s TERM SMAINPy incode=xstude, status=0/SUCCESS)/vh.Process: 17852 ExectStop=-bin/kill -s TERM SMAINPy incode: status=0/SUCCESS)/vh.Process: 17852 ExectStop=-bin/kill -s topped nginx - high performance w system(1]]: status ng i	n since Wed 2020-06-03 16:33:42 EDT; tecStant=/usr/sbin/nginx -c jinx: master process /usr/sbin/nginx -c VnJun 03 16:33:42 hcl-centos-31
un 03 16:33:42 hcl-centos-31 systemd[1]: started nginx - high performance w int: some lines were ellipsized, use -1 to show in full. 2020-06-03 16:33:58 Automation Policy Restart Nginx action Restart Nginx ran Successfully Resage:CustomActionType (453) executed without incident Resage:CustomActionType (453) executed (132) Resage:	n since Wed 2020-06-03 16:33:42 EDT; tecStant=/usr/sbin/nginx -c jinx: master process /usr/sbin/nginx -c VnJun 03 16:33:42 hcl-centos-31
<pre>Lun 03 16:33:42 hcl-centos-21 systemd[1]: Started nginx - high performance w int: some lines were ellipsized, use -1 to show in full. D20-06-03 16:33:58 Lutomation Policy Restart Nginx action Restart Nginx ran Successfully Alessage CustomActionType (43) executed without incident esult(command_list_out: [Systemcl restart nginx, 'systemcl restart nginx/vn', None), (systemct status nginx, 'systemct status nginx/vhv/tb[1;32m/ve2V97vs erformance web server/vh Loaded: loaded (/usr/lib/system/disystem/diginx.service; enabled; vendor preset: disabled/vh Active: xh[1]:32mactive (running)/xh[0/m 75m ago/vh Docs: http://nginx.org/endocs/vhv Process: 17855 Execstop-bin/will = TERN SMINIPID (code=exited, status=0/SUCCESS)/vh Process: 17855 te etchginx/hginx.com/ (code=exited, status=0/SUCCESS)/vh IAiai PID: 17856 (nginx;Vin/ GGroup: /systemc][1]: Sorsen[1]: Storged nginx - high performance wvhulu 03 16:33:42 hcl-centos-31 systemd[1]: Can't open PID file /var/run/nginxv/vhulu 03 16:33:42 hcl-centos- systemd[1]: Starting nginx - high performancevhulu 03 16:33:42 hcl-centos-31 systemd[1]: Can't open PID file /var/run/nginxv/nJun 03 16:33:42 hcl-centos- informance wv/nhint: Some lines were ellipsized, use -1 to show in full /vn', None)])</pre>	n since Wed 2020-06-03 16:33:42 EDT; tecStant=/usr/sbin/nginx -c jinx: master process /usr/sbin/nginx -c VnJun 03 16:33:42 hcl-centos-31
<pre>Jun 89 16:33:42 hcl-centos-31 systemd[1]: started nginx - high performance w Hint: Some lines were ellipsized, use -1 to show in full.) 0020-06:03 16:33:58 Automation Policy Restart Nginx action Restart Nginx ran Successfully Wessage:CustomActionType (4S) executed without incident Result[command_list_out:[(systemct] restart nginx," systemct] restart nginx/n', None), (systemct] status nginx, "systemct] status nginx/hivt1b[1,32mactive (running)Xt1b[0m Result[command_list_out:[(systemct] restart nginx," systemct] restart nginx/n', None), (systemct] status nginx, "systemct] status nginx/hivt1b[1,32mactive (running)Xt1b[0m Result[command_list_out:[(systemct] restart nginx," systemct] restart nginx/n', None), (systemct] status nginx, "systemct] status-0/SUCCESS(Nh Natcive (running)Xt1b[0m 780ms ago/\n Docs: http://nginx.org/en/docs/Nn Process: 17832 ExectStop=/bin/kill -s TERM SMAINPID (code=exited, status=0/SUCCESS)(Nh Process: 17835 Exe technginx/nginxVin Wes2Vs4Vs4Vs4Vs4Vs4Vs4Vs4Vs4Vs17857 nginx: worker process/in/vin/ul 0a 16:33:42 hcl-centos-31 systemd[1]: Stopped nginx high performance w. systemd[1]: Stopped nginxVin Nat 31:63:33:42 hcl-centos-31 systemd[1]: Can't open PID Hie /var/fun/hginxv/vin/ul 03 16:33:42 hcl-centos-31 systemd[1]: Stopped nginx/sin bis/enginx/sinti Scome lines were ellipsized, use -1 to show in full Vin", None)]) N202-06-02 18:26:34 Automation Policy Run CPU Diagnostics (SSH) action Datacenter Automation: Format Output as HTML ran Successfully</pre>	n since Wed 2020-06-03 16:33:42 EDT; tecStart=/usr/sbin/nginx -c jinx: master process /usr/sbin/nginx -c VnJun 03 16:33:42 hcl-centos-31
Jun 83 16:33:42 hcl-centos-31 systemd[1]: Started ng1nx - high performance w ifnt: Some lines were ellipsized, use -1 to show in full.) 0020-06-03 16:33:58 Automation Policy Restart Nginx action Restart Nginx ran Successfully Message:CustomActionType (453) executed without incident Result:Command, List.out: [Systemoti restart nginx, 'systemoti restart nginx\'n', None), ('systemoti status nginx', 'systemoti status nginx\'n'x1b[1:32m/ve2V97vs Peoluticommand, List.out: [Systemoti restart nginx, 'systemoti restart nginx\'n', None), ('systemoti status nginx', 'systemoti status nginx\'n'x1b[1:32m/ve2V97vs Peoluticommand, List.out: [Systemoti restart nginx', 'systemoti restart nginx'n', None), ('systemoti status nginx', 'systemoti status nginx\'n'x1b[1:32m/ve2V97vs Peoluticommand, List.out: [Systemoti restart nginx', 'systemoti restart nginx', 'n'y2Setmoti status nginx', 'systemoti restart Peoluticommand, List.out: [Systemoti restart nginx', 'systemoti restart nginx', 'n'y2Setmoti status nginx', 'systemoti restart Peoluticommand: List.out: [Systemoti restart nginx', 'n'y2Setmotic', 'systemoti status nginx', 'systemoti status nginx', 'ny2Setmotic', 'systemotic', 'sy	n since Wed 2020-06-03 16:33:42 EDT; tecStant=/usr/sbin/nginx -c jinx: master process /usr/sbin/nginx -c VnJun 03 16:33:42 hcl-centos-31
Jun 83 16:33:42 hcl-centos-31 systemd[1]: Started ng1nx - high performance w ithr: Some lines were ellipsized, use -1 to show in full. D020-06-03 16:33:58 Automation Policy Restart Nginx action Restart Nginx ran Successfully Message:CustomActionType (453) executed without incident Result:Command, List.out: [Kystemot restart nginx; hystemot restart nginx/n, None), [Systemot status nginx, "systemot status nginx/vhv/tb[1,32m/ve2V97vs Peol/to:Som ago/to hoos: http://nginx.org/endocs/the?endocs/testart/Seconds/testa	n since Wed 2020-06-03 1633:42 EDT; tecStant=/usr/sbin/nginx -c jinx: master process /usr/sbin/nginx -c VnJun 03 16:33:42 hcl-centos-31
Jun 83 16:33:42 hcl-centos-31 systemd[1]: Started ng1nx - high performance w ithr: Some lines were ellipsized, use -1 to show in full.) 000-06-03 16:33:58 Automation Policy Restart Nginx action Restart Nginx ran Successfully Message:CustomActionType (453) executed without incident Result:Command, List.out: [Systement restart nginx; hystemct1 restart nginx/n, None), [Systemct1 status nginx, "systemct1 status nginx/vhv1b[1;32m/ve2V97vs Peol/tichomand, List.out: [Systement restart nginx; hystemct1 restart nginx/nn; None), [Systemct1 status nginx, "systemct1 status nginx/vhv1b[1;32m/ve2V97vs Peol/tichomand, List.out: [Systement restart nginx; hystemct1 restart nginx/vhn; None), [Systemct1 status nginx, "systemct1 status nginx/vhv1b[1;32m/ve2V97vs Peol/tichomand; List.out: [Systement restart nginx; hystemc1] restart nginx/vhn; List.out: Italia Peol/tichomand; List.out: [Systement1 restart nginx; hystemc1] restart nginx/vhn; List.out: Italia Peol/tichomand; List.out: [Systement1]; Started Peol/tichol	n since Wed 2020-06-03 1633:42 EDT; tecStant=/usr/sbin/nginx -c jinx: master process /usr/sbin/nginx -c VnJun 03 16:33:42 hcl-centos-31

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



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 (三).
- To view a page containing all the menu options, click the Advanced menu icon (…).

This appendix covers the following topics:

Run Book Variables	s	47	7
--------------------	---	----	---

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
%р	Asset	Asset panel
%q	Asset	Asset zone
%Q	Asset	Asset punch
%U	Asset	Asset rack
%υ	Asset	Asset shelf
%∨	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
%l (uppercase	Dynamic	For events with a source of "dynamic", this variable contains the index value from

Variable	Source	Description
"eye")	Alert	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.
%Т	Dynamic Alert	Value returned by the Threshold function in a Dynamic Application Alert.
%∨	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

Variable	Source	Description
		• 4. Memory
		• 5. Swap
		6. Component
		• 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.
%с	Event	Event counter
%d	Event	Date/time when last event occurred.
%D	Event	Date/time of first event occurrence.
%e	Event	Event ID
%Н	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
%у	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.
		Event policy ID

Variable	Source	Description
%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.
%G	Event Policy	Event Category
%R	Event Policy	Event policy cause/action text
%_event_ policy_name	Event Policy	Name of the event policy that triggered the event.
%В	Organization	Organization billing ID
%b	Organization	Impacted organization
%С	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 - 2021, 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