



Network Connectivity PowerPack

Beta Version

Network Connectivity PowerPack version 100

Table of Contents

Introduction to Network Connectivity Automation	3
What is the Network Connectivity PowerPack?	3
Installing the Network ConnectivityPowerPack	3
Network Connectivity Automation Policies	5
Standard Automation Policies	5
Standard Ping Automation Policy	9
Standard Traceroute Automation Policy	10
Standard NSLOOKUP Automation Policy	12
Creating and Customizing Automation Policies	14
Prerequisites	15
Creating an Automation Policy	15
Example Automation Configuration	17
Customizing an Automation Policy	18
Removing an Automation Policy from a PowerPack	19
Customizing Network Connectivity Actions	20
Creating a Custom Action Policy with Network Connectivity Actions	21
Customizing Ping Actions	22
Custom Ping Action Parameters	23
Custom Ping Action Examples	23
Customizing Traceroute Actions	25
Custom Traceroute Action Parameters	26
Custom Traceroute Action Examples	27
Customizing NSLOOKUP Actions	27
Custom NSLOOKUP Action Parameters	28
Custom NSLOOKUP Action Examples	28
Available Output Formats	29
Variables	1
Variables	1

Introduction to Network Connectivity Automation

Overview

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

This chapter covers the following topics:

What is the Network Connectivity PowerPack?	3
Installing the Network ConnectivityPowerPack	3

What is the Network Connectivity PowerPack?

The *Network Connectivity PowerPack* includes automation policies that examine connectivity-related events and trigger a set of automation actions. The PowerPack also includes custom action types for running ping, traceroute, and nslookup commands with parameters that you specify.

The *Network Connectivity PowerPack* does not contain or require credentials to operate. The Network Connectivity actions are executed from the SL1 All-In-One Appliance or Data Collector.

Installing the Network ConnectivityPowerPack

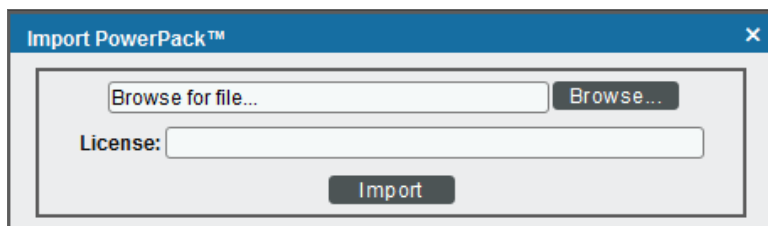
Before completing the steps in this manual, you must import and install the latest version of the *Network ConnectivityPowerPack*.

NOTE: The *Network Connectivity* PowerPack requires SL1 version 8.10.0 or later. For details on upgrading SL1, see the appropriate SL1 [Release Notes](#).

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

To download and install a PowerPack:

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



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal page 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: To use the standard automation policies, no other configuration is necessary. These automation policies run in response to network connectivity-related events that are included in SL1.

Network Connectivity Automation Policies

Overview

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

This chapter covers the following topics:

<i>Standard Automation Policies</i>	5
<i>Standard Ping Automation Policy</i>	9
<i>Standard Traceroute Automation Policy</i>	10
<i>Standard NSLOOKUP Automation Policy</i>	12

Standard Automation Policies

The *Network Connectivity PowerPack* includes three standard automation policies: Network Connectivity: Run Nslookup, Network Connectivity: Run Ping (IPv4), and Network Connectivity: Run Traceroute. These automation policies run automatically in response to network connectivity events and return output as HTML. To use these standard policies, you do not have to do any additional configuration after you install the PowerPack.

Editing PowerPack™ Network Connectivity PowerPack										
Embedded Run Book Policies [3]										
Automation Policy Name	ID	Policy State	Organization	Devices	Events	Actions	Edited By	Last Edited		
1. Network Connectivity: Run Nslookup (IPv4)	103	Enabled	System	All	9	1	em7admin	2019-10-04 12:50:51		
2. Network Connectivity: Run Ping (IPv4)	102	Enabled	System	All	9	1	em7admin	2019-10-04 12:50:51		
3. Network Connectivity: Run Traceroute	101	Enabled	System	All	9	1	em7admin	2019-10-04 12:50:50		

Available Run Book Policies [0]										
Automation Policy Name	ID	Policy State	Organization	Devices	Events	Actions	Edited By	Last Edited		
No results to display.										

The following table shows the standard automation policies, their aligned events, and the automation action that runs by default in response to the events.

Automation Policy Name	Aligned Events	Automation Action (Default)
Network Connectivity: Run Ping (IPv4)	<ul style="list-style-type: none"> • Poller: Availability and Latency checks failed • Poller: Availability Check Failed • Poller: Availability Flapping • Poller: Device not responding to ping (high frequency) • Poller: Network Latency Exceeded Threshold • Poller: TCP connection time above threshold • Poller: TCP/UDP port not responding • Poller: TCP/UDP port not responding (SMTP) • Transactions: Round trip mail did not arrive within threshold 	Run Ping: Default Options with HTML Output
Network Connectivity: Run Traceroute (IPv4)	<ul style="list-style-type: none"> • Poller: Availability and Latency checks failed • Poller: Availability Check Failed • Poller: Availability Flapping 	Run Traceroute: Default Options with HTML Output

Automation Policy Name	Aligned Events	Automation Action (Default)
	<ul style="list-style-type: none"> • Poller: Device not responding to ping (high frequency) • Poller: Network Latency Exceeded Threshold • Poller: TCP connection time above threshold • Poller: TCP/UDP port not responding • Poller: TCP/UDP port not responding (SMTP) • Transactions: Round trip mail did not arrive within threshold 	
Network Connectivity: Run Nslookup (IPv4)	<ul style="list-style-type: none"> • Poller: Availability and Latency checks failed • Poller: Availability Check Failed • Poller: Availability Flapping • Poller: Device not responding to ping (high frequency) • Poller: DNS hostname resolution time above threshold • Poller: Failed to resolve hostname • Poller: TCP/UDP port not responding • Poller: TCP/UDP port not responding (SMTP) • Transactions: Round trip mail did not arrive within threshold 	Run Nslookup: Default Options with HTML Output

For every device that has an IP address, SL1 monitors availability every five minutes. If you have enabled Critical Ping for a device and enabled the event "Poller: Device not responding to ping (high frequency)", you can monitor availability at a higher frequency than five minutes. The automation policies included in this PowerPack respond to events from Critical Ping, as well.

The following figure shows some network availability events on the **Events** page:

The screenshot shows the ScienceLogic Events page. At the top, there are filters for event severity: 0 Critical, 7 Major, 5 Minor, 1 Notice, and 0 Healthy. A search bar is present. The main table lists events with columns for Organization, Severity, Name, Message, Age, Count, Event Note, Event Source, Acknowledge, and Clear. A context menu is open for the event 'Device Failed Availability Check: UDP - SNMP' (ID: ec2-34-200-97-29), showing options like 'View Event', 'Edit Event Note', 'Create External Ticket', 'Align External Ticket', 'View Automation Actions' (highlighted), 'View Event Policy', and 'Suppress Event for this Device'.

ORGANIZATION	SEVERITY	NAME	MESSAGE	AGE	COUN...	EVENT NOTE	EVENT S...	ACKNOWLEDGE	CLEAR
System	Major	cscs025	Illicit process running: nginx	1 month 29 da	17197		cscs025	Acknowledge	Clear
System	Major	cscs025	DRBD: This node is not UpToDate	1 month 28 da	16837		Dynamic	Acknowledge	Clear
System	Minor	cscs025	Physical Memory has exceeded threshold: (80%) currently (87.1138701337%)	1 month 18 da	13867		Dynamic	Acknowledge	Clear
System	Major	cscs025	Nameserver not responding to DNS query	1 month 16 da	68656		cscs025	Acknowledge	Clear
Example Devices	Minor	Test CRS-1 165	MGBL-LIBPARSER-3-ERR_MEM_ALLOC: RPV0/0/CPU0: memory allocation routine...	27 days 18 hou	2		NetScaler	Acknowledge	Clear
Example Devices	Major	ec2-34-200-97-29	Device Failed Availability Check: UDP - SNMP	19 days 22 hou	5711		cscs025	Acknowledge	Clear
Example Devices	Minor	ec2-34-200-97-29	Network latency exceeded threshold: No Response	19 days 14 hou	5616		cscs025		
System	Major	System	EM7 major event: E010: Configured Mail server 192.168.0.1 timed out when openi...	6 days 19 hour	29332		cscs025		
System	Notice	System	From unknown device: 10.2.24.26, appliance: cscs026 received the following Trap m...	3 days 17 hour	2		cscs025		
Example Devices	Major	rstsvcsa6u2a01	Example Major Event	21 hours 37 mi	1		API		
Example Devices	Major	NetScaler	Device Failed Availability Check: UDP - SNMP	14 hours 4 min	169		cscs025		
System	Minor	cscs025	Network latency exceeded threshold: 196.81 ms.	9 minutes 31 s	2		cscs025		
Example Devices	Minor	rstsvcsa6u2a01	Network latency exceeded threshold: 168.4 ms.	5 minutes 17 s	1		cscs025		

To see the automation actions triggered by an event, click the **[Actions]** button (***) and select *View Automation Actions*. The **Event Actions Log** page appears. Notice the highlighted Traceroute and Nslookup information in the following figure. The log indicates that the following actions ran successfully:

- Run Traceroute: Default Options with HTML Output
- Run Nslookup: Default Options with HTML Output

The screenshot shows the 'Event Actions Log' for event [1366]. It contains two log entries. The first entry is for a Traceroute action, showing the path and response times for 30 hops. The second entry is for an Nslookup action, showing the server address and authoritative answers.

```

Automation Policy Network Connectivity: Run Traceroute (IPv4) action Run Traceroute: Default Options with HTML output ran Successfully
Message:CustomActionType (376) executed without incident
Result:
traceroute to 34.200.97.29 (34.200.97.29), 30 hops max, 60 byte packets
 1 10.2.24.4 (10.2.24.4) 0.557 ms 0.584 ms 0.671 ms
 2 10.128.3.5 (10.128.3.5) 0.526 ms 3.415 ms 3.471 ms
 3 efi001.dc2.corp.sciencelogic.com (10.128.1.1) 4.531 ms 4.547 ms 4.504 ms
 4 104.192.252.2 (104.192.252.2) 5.128 ms 5.053 ms 5.045 ms
 5 208.71.164.134 (208.71.164.134) 7.377 ms 7.415 ms 7.400 ms
 6 te-0-12-0-3-3-pe01.ashburn.va.ibone.comcast.net (66.208.233.253) 5.331 ms 1.044 ms 2.460 ms
 7 es4323-pe01.11greatoaks.ca.ibone.comcast.net (75.149.229.2) 2.547 ms 2.528 ms 2.535 ms
 8 52.93.40.53 (52.93.40.53) 26.204 ms 52.93.27.129 (52.93.27.129) 14.401 ms 52.93.27.137 (52.93.27.137) 17.252 ms
 9 52.93.114.99 (52.93.114.99) 4.304 ms 52.93.114.71 (52.93.114.71) 2.838 ms 52.93.114.55 (52.93.114.55) 2.748 ms
10 * * *
11 * * *
12 * * *
13 52.93.28.238 (52.93.28.238) 1.991 ms 52.93.28.204 (52.93.28.204) 1.936 ms 52.93.28.208 (52.93.28.208) 1.844 ms
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
.

Automation Policy Network Connectivity: Run Nslookup (IPv4) action Run Nslookup: Default Options with HTML Output ran Successfully
Message:CustomActionType (380) executed without incident
Result:
Server: 10.64.148.32
Address: 10.64.148.32#53
Non-authoritative answer:
29.97.200.34.in-addr.arpa name = ec2-34-200-97-29.compute-1.amazonaws.com.
Authoritative answers can be found from:

```


TIP: Although you can edit the automation actions described in this section, best practice is to "Save As" to create a new, renamed automation action, instead of customizing the standard automation policies.

Standard Ping Automation Policy

The "Network Connectivity: Run Ping (IPv4)" automation policy is triggered by the following events:

- Poller: Availability and Latency checks failed
- Poller: Availability Check Failed
- Poller: Availability Flapping
- Poller: Device not responding to ping (high frequency)
- Poller: Network Latency Exceeded Threshold
- Poller: TCP connection time above threshold
- Poller: TCP/UDP port not responding
- Poller: TCP/UDP port not responding (SMTP)
- Transactions: Round trip mail did not arrive within threshold

Default Behavior. When these events occur, the automation policy "Network Connectivity: Run Ping (IPv4)" executes the action "Run Ping: Default Options with HTML Output". This action runs a standard ping (IPv4) command automatically. The output of the command is formatted for display in the SL 1 **Events** page, or in an incident ticket on an external system.

The following figure shows the details of the ping action:

Policy Editor | Editing Action [94] Reset

Action Name: Run Ping: Default Options with HTML output Action State: [Enabled]

Description: Runs a ping with default options and formats the output as HTML.

Organization: [System] Action Type: Run Ping (0.9)

Execution Environment: [-- Default: Network Connectivity PowerPack] Action Run Context: [Database]

Input Parameters

```
{
  "host": "%a",
  "options": "",
  "output_format": "html",
  "ipv6": false
}
```

Save Save As

Options. In some cases, you may want to modify the action that is run in response to the triggering events. For example, if you are monitoring an IPv6 network, you can select one of the Ping6 actions. The following ping actions are also available in this PowerPack:

- Run Ping: Default Options with Plaintext output
- Run Ping6: Default Options with HTML output
- Run Ping6: Default Options with Plaintext output

For information about customizing automation policies, see [Customizing an Automation Policy](#). For information about output formats, see [Output Formats](#).

Standard Traceroute Automation Policy

The "Network Connectivity: Run Traceroute (IPv4)" automation policy is triggered by the following events:

- Poller: Availability and Latency checks failed
- Poller: Availability Check Failed
- Poller: Availability Flapping
- Poller: Device not responding to ping (high frequency)

- Poller: Network Latency Exceeded Threshold
- Poller: TCP connection time above threshold
- Poller: TCP/UDP port not responding
- Poller: TCP/UDP port not responding (SMTP)
- Transactions: Round trip mail did not arrive within threshold

Default Behavior. When these events occur, the automation policy "Network Connectivity: Run Traceroute (IPv4)" executes the action "Run Traceroute: Default Options with HTML Output". This action runs a standard traceroute (IPv4) command automatically. The output of the command is formatted for display in the SL1 **Events** page, or in an incident ticket on an external system.

The following figure shows the details of the traceroute action:

The screenshot shows the 'Policy Editor | Editing Action [93]' window. The action is named 'Run Traceroute: Default Options with HTML output' and is currently 'Enabled'. The description is 'Runs an IPv4 traceroute with default options and formats the output as HTML.' The organization is set to '[System]' and the action type is 'Run Traceroute (0.9)'. The execution environment is '-- Default: Network Connectivity PowerPack]' and the action run context is '[Database]'. The input parameters are defined as a JSON object: { "host": "%a", "options": "", "packet_length": 0, "output_format": "html" }. At the bottom, there are 'Save' and 'Save As' buttons.

Options. In some cases, you may want to modify the action that is run in response to the triggering events. For example, if you are monitoring an IPv6 network, you can select one of the IPv6 traceroute actions. The following traceroute automation actions are also available in this PowerPack:

- Run IPv6 Traceroute: Default Options with HTML output
- Run IPv6 Traceroute: Default Options with Plaintext output

- Run Traceroute: Default Options with Plaintext output

For information about customizing automation policies, see [Customizing an Automation Policy](#). For information about output formats, see [Output Formats](#).

Standard NSLOOKUP Automation Policy

The "Network Connectivity: Run Nslookup (IPv4)" automation policy is triggered by the following events:

- Poller: Availability and Latency checks failed
- Poller: Availability Check Failed
- Poller: Availability Flapping
- Poller: Device not responding to ping (high frequency)
- Poller: DNS hostname resolution time above threshold
- Poller: Failed to resolve hostname
- Poller: TCP/UDP port not responding
- Poller: TCP/UDP port not responding (SMTP)
- Transactions: Round trip mail did not arrive within threshold

Default Behavior. When these events occur, the automation policy "Network Connectivity: Run Nslookup (IPv4)" executes the action "Run Nslookup: Default Options with HTML Output". This action runs a standard NSLOOKUP (IPv4) command automatically. The output of the command is formatted for display in the SL1 **Events** page, or in an incident ticket on an external system.

Policy Editor | Editing Action [95]
Reset

Action Name

Action State

[Enabled] ▼

Description

Runs an nslookup with default options and formats the output as HTML.

Organization

Action Type

[System] ▼

Run Nslookup (0.9)

Execution Environment

Action Run Context

[-- Default: Network Connectivity PowerPack] ▼

[Database] ▼

Input Parameters

```
{
  "host": "%a",
  "nameserver": "",
  "options": "",
  "output_format": "html"
}
```

Save

Save As

Options. In some cases, you may want to modify the action that is run in response to the triggering events. For example, you can run NSLOOKUP with plaintext output. This additional action is available in this PowerPack:

- Run Nslookup: Default Options with Plaintext output

For information about customizing automation policies, see [Customizing an Automation Policy](#). For information about output formats, see [Output Formats](#).

Creating and Customizing Automation Policies

Overview

This chapter describes how to create automation policies using the automation actions in the *Network Connectivity PowerPack*.

This chapter covers the following topics:

<i>Prerequisites</i>	15
<i>Creating an Automation Policy</i>	15
<i>Example Automation Configuration</i>	17
<i>Customizing an Automation Policy</i>	18
<i>Removing an Automation Policy from a PowerPack</i>	19

Prerequisites

Before you create an automation policy using the automation actions in the *Network Connectivity PowerPack*, you must determine:

- Which commands (Ping, Traceroute, or NSLOOKUP) you want to run on a monitored device when an event occurs. There are 10 automation actions in the PowerPack that run the three commands with different options and output formats. You can also create your own automation actions using the custom action types 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 *Network Connectivity 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.

The screenshot displays the 'Automation Policy Editor' interface for editing a policy named 'Cisco UCS Fabric Incident Enrichment'. The interface is organized into several sections:

- Policy Configuration:** Fields for Policy Name, Policy Type (Active Events), Policy State (Enabled), Policy Priority (Default), and Organization (System).
- Criteria Logic:** A dropdown menu with options like 'Severity >=', 'and no time has elapsed', 'since the first occurrence', 'and event is NOT cleared', and 'and all times are valid'. A 'Minor' checkbox is also present.
- Match Logic:** A dropdown menu with 'Text search' selected.
- Match Syntax:** A text input field.
- Repeat Time:** A dropdown menu with 'Only once' selected.
- Align With:** A dropdown menu with 'Devices' selected.
- Include events for entities other than devices (organizations, assets, etc.):** An unchecked checkbox.
- Trigger on Child Rollup:** An unchecked checkbox.
- Available Devices:** A list of devices including 'System', 'AWS: Account: AIDAIHXVQSNXTUJBFOWYE', and 'AWS: API Gateway Service: us-east-1 API Gateway Service'.
- Aligned Devices:** A dropdown menu showing '(All devices)'.
- Available Events:** A list of events including '[3283] Critical: AKCP: AC Voltage sensor detects no current', '[3292] Critical: AKCP: DC Voltage sensor High Critical', and '[3293] Critical: AKCP: DC Voltage sensor Low Critical'.
- Aligned Events:** A list of events including '[3418] Minor: Cisco: UCS Fabric PSU Amperes has exceeded threshold.', '[3412] Minor: Cisco: UCS Fabric PSU Voltage has exceeded threshold.', and '[3416] Minor: Cisco: UCS Fabric PSU Wattage has exceeded threshold.'
- Available Actions:** A list of actions including 'SNMP Trap [1]: EM7 Event Trap', 'SNMP Trap [1]: Example Event Trap', and 'SNMP Trap [1]: SL1 Event Trap'.
- Aligned Actions:** A list of actions including '1. Snippet [5]: Enrichment: Cisco:UCS: Fabric Show Commands', '2. Snippet [5]: Enrichment: Util: Collect Enrichment Data', '3. Snippet [5]: Enrichment: Util: Show Commands Enrichment Data HTML', and '4. Snippet [5]: Enrichment: Util: Load Work Instructions'.

At the bottom of the editor, there are 'Save' and 'Save As' buttons.

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*.
 - **Aligned Actions.** This field includes the actions from the *Network Connectivity* PowerPack. You should see Run Ping, Run Traceroute, and Run Nslookup actions 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.
4. Optionally, supply values in the other fields on this page to refine when the automation will trigger.
5. Click **[Save]**.

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.

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 *Network Connectivity PowerPack*:

The screenshot shows the 'Automation Policy Editor' interface for editing a policy. The policy name is 'Network Connectivity: My Run Traceroute (IPv6)'. The policy type is 'Active Events', the state is 'Enabled', the priority is 'Default', and the organization is 'System'. The criteria logic is configured with the following conditions: 'Severity >= Minor', 'no time has elapsed since the first occurrence', 'event is NOT cleared', and 'all times are valid'. The match logic is 'Text search' and the repeat time is 'Only once'. The policy is aligned with 'Devices'. The available devices list includes 'Cisco Systems: CRS-1 16S: Test CRS-1 16S' and 'Citrix: NetScaler: NetScaler'. The available events list includes '[5678] Critical: 3PAR Trap: Critical Alert', '[5649] Critical: 3PAR: Disk Utilization Exceeded Critical Threshold', and '[3569] Critical: AKCP: AC Voltage sensor detects no current'. The available actions list includes 'trace', 'Run Traceroute [101]: Run IPv6 Traceroute: Default Options with HTML output', and 'Run Traceroute [101]: Run IPv6 Traceroute: Default Options with Plaintext output'. The aligned devices list is '(All devices)'. The aligned events list includes '[1934] Critical: Poller: Availability and Latency checks failed', '[4071] Critical: Poller: Device not responding to ping (high frequency)', '[1932] Major: Poller: Availability Check Failed', and '[4011] Major: Poller: Availability Flapping'. The aligned actions list includes '1. Run Traceroute [101]: Run IPv6 Traceroute: Default Options with Plaintext output'. The 'Trigger on Child Rollup' checkbox is checked. The 'Save' and 'Save As' buttons are visible at the bottom.


The policy uses the following settings:

- **Policy Name.** The policy is named "Network Connectivity: My Run Traceroute (IPv6)".
- **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.
- **Organization.** The policy executes for all organizations, so *System* is selected in this field.
- **Criteria Logic.** The policy is configured to execute immediately when an event matches these criteria: "Severity >= Minor, and no time has elapsed since the first occurrence, and event is NOT cleared, and all times are valid".
- **Aligned Devices.** The policy is configured to trigger for all devices in the system.
- **Aligned Events.** The policy is configured to trigger only when the following events are triggered:
 - Critical: Poller: Availability and Latency checks failed
 - Critical: Poller: Device not responding to ping (high frequency)
 - Major: Poller: Availability Check Failed
 - Major: Poller: Availability Flapping

- Major: Poller: TCP/UDP port not responding (SMTP)
 - Major: Transactions: Round trip mail did not arrive within threshold
 - Minor: Poller: Network Latency Exceeded Threshold
 - Minor: Poller: TCP connections time above threshold
- **Aligned Actions.** The automation includes the following action. This action allows you to view the output of traceroute in the Automation Log, accessed through the SL1 Event Console:
 - Run Traceroute (101): Run IPv6 Traceroute: Default options with HTML output

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 *Network Connectivity* automation policy you want to edit and click the wrench icon () for that policy. The **Automation Policy Editor** page appears:

Automation Policy Editor | Editing Automation Policy [102] Reset

Policy Name: Network Connectivity: Run Ping (IPv4) | Policy Type: [Active Events] | Policy State: [Enabled] | Policy Priority: [Default] | Organization: [System]

Criteria Logic: [Severity >=] [Minor,] | Match Logic: [Text search] | Match Syntax: []

[and no time has elapsed] | Repeat Time: [Only once] | Align With: [Devices]

[since the first occurrence.] | Include events for entities other than devices (organizations, assets, etc.)

[and event is NOT cleared] | Trigger on Child Rollup

[and all times are valid]

Available Devices: Bananaquit, AWS: Service: JEM-Virtual, Cardinal | Aligned Devices: (All devices)

Available Events: [3186] Critical: AKCP: AC Voltage sensor detects no current, [3195] Critical: AKCP: DC Voltage sensor High Critical, [3196] Critical: AKCP: DC Voltage sensor Low Critical | Aligned Events: [1453] Critical: Poller: Availability and Latency checks failed, [3577] Critical: Poller: Device not responding to ping (high freq), [1451] Major: Poller: Availability Check Failed, [3517] Major: Poller: Availability Flapping

Available Actions: SNMP Trap [1]: EM7 Event Trap, Snippet [5]: AWS: Disable Instance By Tag, Snippet [5]: AWS: Discover from EC2 IP | Aligned Actions: 1. Run Ping [108]: Run Ping: Default Options with HTML



Save Save As

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.
 - **Aligned Actions.** This field includes the actions from the Network Connectivity PowerPack. You should see Run Ping, Run Traceroute, and Run Nslookup actions 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.
 - **Organization.** Select the organization that will use this 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]**.

Removing an Automation Policy from a PowerPack

After you have customized a policy from a *Network Connectivity 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/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 *Network Connectivity* PowerPack. Click its wrench icon ()
3. In the **PowerPack Properties** page, in the navigation bar on the left side, click **Run Book Policies**.
4. In the **Embedded Run Book Polices** pane, locate the policy you updated, and click the bomb icon () for that policy. The policy will be removed from the PowerPack and will now appear in the bottom pane.

Customizing Network Connectivity Actions

Overview

This manual describes how to customize the three action types embedded in the Network Connectivity 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:

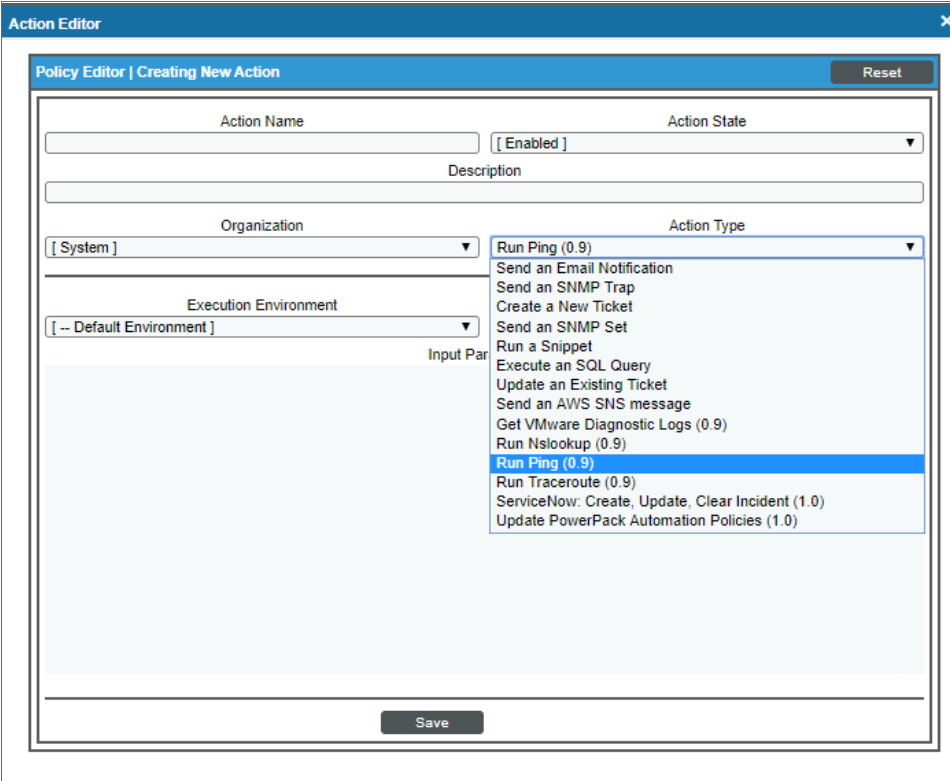
<i>Creating a Custom Action Policy with Network Connectivity Actions</i>	21
<i>Customizing Ping Actions</i>	22
<i>Custom Ping Action Parameters</i>	23
<i>Custom Ping Action Examples</i>	23
<i>Customizing Traceroute Actions</i>	25
<i>Custom Traceroute Action Parameters</i>	26
<i>Custom Traceroute Action Examples</i>	27
<i>Customizing NSLOOKUP Actions</i>	27
<i>Custom NSLOOKUP Action Parameters</i>	28
<i>Custom NSLOOKUP Action Examples</i>	28
<i>Available Output Formats</i>	29

Creating a Custom Action Policy with Network Connectivity Actions

You can use one of the Action Types included with the Network Connectivity PowerPack to create custom actions that you can then use to build custom automation policies.

To create an action policy:

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.



The screenshot shows the 'Action Editor' modal window. The title bar reads 'Action Editor' with a close button. The main content area is titled 'Policy Editor | Creating New Action' and includes a 'Reset' button in the top right. The form contains several fields: 'Action Name' (text input), 'Action State' (dropdown menu showing '[Enabled]'), 'Description' (text input), 'Organization' (dropdown menu showing '[System]'), 'Execution Environment' (dropdown menu showing '[-- Default Environment]'), and 'Input Parameters' (text input). A large list of 'Action Type' options is displayed on the right side of the form, including 'Run Ping (0.9)', 'Send an Email Notification', 'Send an SNMP Trap', 'Create a New Ticket', 'Send an SNMP Set', 'Run a Snippet', 'Execute an SQL Query', 'Update an Existing Ticket', 'Send an AWS SNS message', 'Get VMware Diagnostic Logs (0.9)', 'Run Nslookup (0.9)', 'Run Ping (0.9)', 'Run Traceroute (0.9)', 'ServiceNow: Create, Update, Clear Incident (1.0)', and 'Update PowerPack Automation Policies (1.0)'. The 'Run Ping (0.9)' option is currently selected. A 'Save' button is located at the bottom center of the modal.

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. Your choices are:

- Run Ping (0.9)
- Run Traceroute (0.9)
- Run Nslookup (0.9)
- **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.

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

6. 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 Ping Actions

The Network Connectivity PowerPack includes four automation actions that execute a Ping or Ping6 command. You can specify the host and the options in a JSON structure that you enter in the **Input Parameters** field in the **Action Policy Editor** modal.

The following automation actions that use the "Run Ping" action type are included in the Network Connectivity PowerPack.

Action Name	Description	host	options	ipv6	output_ format
Run Ping: Default Options with HTML Output	Runs a ping with default options and formats the output as HTML	Default is %a (IP address of current device)	Default is None (empty string)	false	html
Run Ping: Default Options with Plaintext output	Runs a ping with default options and formats the output as plain text	Default is %a (IP address of current)	Default is None (empty string)	false	text
Run Ping6: Default Options with HTML output	Runs a ping6 with default options and formats the output as HTML	Default is %a (IP address of current device)	Default is None (empty string)	true	html
Run Ping6: Default Options with Plaintext output	Runs a ping6 with default options and formats the output as plain text	Default is %a (IP address of current device)	Default is None (empty string)	true	text

TIP: For more information about substitution variables, see [Appendix A](#).

NOTE: For more information about output formats, see [Available Output Formats](#).

Custom Ping Action Parameters

The Ping actions accepts the following parameters in JSON:

Parameter	Input type	Description
host	string	The hostname or IP address to include in the ping command. You can also use the substitution variable "%a" to specify the IP address of the current device.
options	string	The options string to include in the command. You can include any of the options supported by the ping command-line utility in this field. If you do not include the "-c" or "-w" options in this field, the ping command will automatically include the option "-c 5", meaning that Ping will send five ECHO_REQUEST packets.
output_format	string	For more information about the output_format options, see "Available Output Formats" on page 29
ipv6	boolean	(optional) If the ipv6 option is true, the ping6 command will be executed. If the ipv6 option is false, the ping command will be executed.

NOTE: The pipe (|) and semi-colon (;) characters are not permitted as input to the "host" and "options" parameters.

Using Substitution Values. The host and options inputs can contain substitution values that match the keys in EM7_VALUES. For example, to run a ping against the IP address of the device that triggered the event, you can specify "%a" in the "host" parameter.

TIP: For more information about substitution variables, see [Appendix A](#).

Custom Ping Action Examples

IPv4. If the options parameter contains either "-c" or "-w" as a sub-string, and the ipv6 parameter is false or not supplied, the ping command string is built in the following format:

```
ping [options input] [host input]
```

For example, for the following settings:

- **host.** 192.168.1.1
- **options.** -c 10

The equivalent ping command string would be: `ping -c 10 192.168.1.1`

The equivalent JSON structure would be:

```
{
  "host": "192.168.1.1"
  "options": "-c 10"
  "output_format": "html"
  "ipv6": false
}
```

IPv6. If the options parameter contains either "-c" or "-w" as a sub-string and the ipv6 parameter is true, a ping command string is built in the following format:

```
ping6 [options input] [host input]
```

For example, for the following settings:

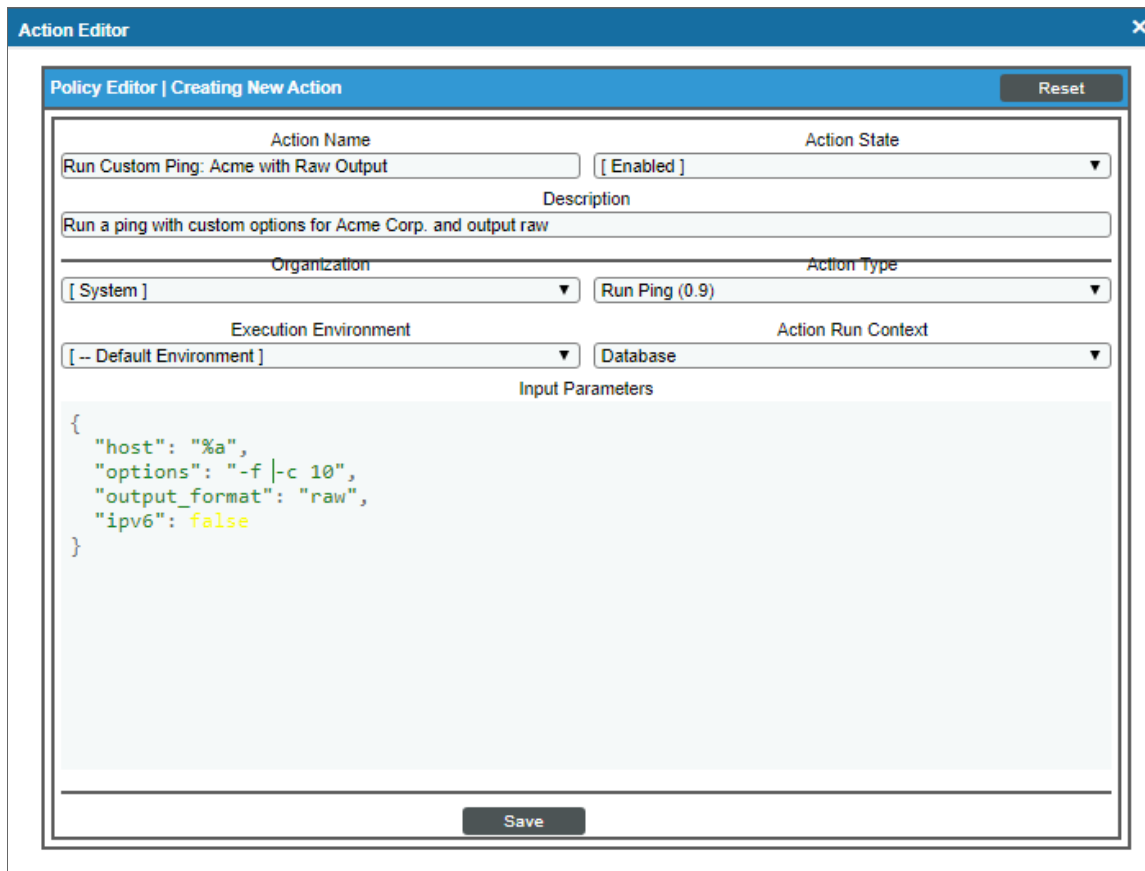
- **host.** 192.168.1.1
- **options.** -c 10

The equivalent ping command string would be: `ping6 -c 10 192.168.1.1.`

The equivalent JSON structure would be:

```
{
  "host": "192.168.1.1"
  "options": "-c 10"
  "output_format": "html"
  "ipv6": true
}
```

The following figure shows a custom ping action for a fictitious company. This custom action is designed to ping IPv4 addresses 10 times without fragmenting the ICMP packets. The action will use the IP address of the current device as the IP address argument. Output will be in the raw format, which can then be fed into snippet actions.



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

Customizing Traceroute Actions

The Network Connectivity PowerPack includes four automation actions that execute a traceroute command. You can specify the host and the options in a JSON structure (name:value pairs) that you enter in the **Input Parameters** field in the **Action Policy Editor** modal..

The following automation actions that use the "Run Traceroute" custom action type are included in the *Network ConnectivityPowerPack*.

Action Name	Description	host	options	packet_length	output_format
Run Traceroute: Default Options with HTML Output	Runs an IPv4 traceroute with default options and formats the output as HTML	Default value is %a (IP address of the current device)	Default value is None (empty string)	Default value is 0	html
Run Traceroute: Default Options with Plaintext output	Runs an IPv4 traceroute with default options and formats the output as plain text	Default value is %a (IP address of the current device)	Default value is None (empty string)	Default value is 0	text
Run IPv6 Traceroute: Default Options with	Runs an IPv6 traceroute with all other options as default and	Default value is %a (IP address of the	Default value is -6	Default value is	html

Action Name	Description	host	options	packet_length	output_format
HTML output	formats the output as HTML	current device)		0	
Run IPv6 Traceroute: Default Options with Plaintext output	Runs an IPv6 traceroute with all other options as default and formats the output as plain text	Default value is %a (IP address of the current device)	Default value is -6	Default value is 0	text

TIP: For more information about substitution variables, see [Appendix A](#).

NOTE: For more information about output formats, see [Available Output Formats](#).

Custom Traceroute Action Parameters

The custom Traceroute action type accepts the following parameters:

Parameter	Input type	Description
host	string	The hostname or IP address to include in the traceroute command. You can also use the substitution variable "%a" to specify the IP address of the current device.
options	string	The options string to include in the command. You can include any of the options supported by the traceroute command-line utility, except for "-T" and "-l", in this field.
packet_length	integer	The packet length to include in the traceroute command. To use the default packet length, use "0".
output_format	string	For more information about the output_format options, see "Available Output Formats" on page 29

NOTE: The pipe (|) and semi-colon (;) characters are not permitted as input to the "host" and "options" parameters.

Using Substitution Values. The host and options inputs can contain substitution values that match the keys in EM7_VALUES. For example, to run a traceroute against the IP address of the device that triggered the event, you can specify "%a" in the "host" parameter.

TIP: For more information about substitution variables, see [Appendix A](#).

Custom Traceroute Action Examples

For the following settings, the equivalent traceroute command string would be: `traceroute -T 192.168.1.1`

- **host.** 192.168.1.1
- **options.** -T
- **packet_length.** 0

The equivalent JSON structure would be:

```
{
  "host": "192.168.1.1"
  "options": "-t"
  "packet_length": 0
  "output_format": "html"
}
```

For the following settings, the equivalent traceroute command string would be: `traceroute 192.168.1.2 100`

- **host.** 192.168.1.2
- **options.** An empty string
- **packet_length.** 100

The equivalent JSON structure would be:

```
{
  "host": "192.168.1.2"
  "options": ""
  "packet_length": 100
  "output_format": "html"
}
```

Customizing NSLOOKUP Actions

The Network Connectivity PowerPack includes four automation actions that execute an NSLOOKUP command. You can specify the host and the options in a JSON structure (name:value pairs) that you enter in the **Input Parameters** field in the **Action Policy Editor** modal

The following automation actions that use the Run Nslookup custom action type are included in the *Network ConnectivityPowerPack*.

Action Name	Description	host	options	nameserver	output_format
Run Nslookup: Default Options with HTML Output	Runs an nslookup with default options and formats the output as HTML	Default value is %a (IP address of the current device)	Default value is None (empty string)	Default value is None (empty string)	html
Run Nslookup: Default Options with	Runs an nslookup with default options and formats	Default value is %a (IP address of the	Default value is None	Default value is None	text

Action Name	Description	host	options	nameserver	output_format
Plaintext output	the output as plain text	current device)	(empty string)	(empty string)	

TIP: For more information about substitution variables, see [Appendix A](#).

NOTE: For more information about output formats, see [Available Output Formats](#).

Custom NSLOOKUP Action Parameters

The custom NSLOOKUP action type accepts the following parameters:

Parameter	Input type	Description
host	string	The hostname or IP address to include in the NSLOOKUP command. You can also use the substitution variable "%a" to specify the IP address of the current device.
nameserver	string	The IP address or hostname of the nameserver to include in the NSLOOKUP command
options	string	The options string to include in the command. You can include any of the options supported by the NSLOOKUP command-line utility in this field.
output_format	string	For more information about the output_format options, see "Available Output Formats" on the next page

NOTE: The pipe (|) and semi-colon (;) characters are not permitted as input parameters.

Using Substitution Values. The host and options inputs can contain substitution values that match the keys in EM7_VALUES. For example, to run a traceroute against the IP address of the device that triggered the event, you can specify "%a" in the "host" parameter.

TIP: For more information about substitution variables, see [Appendix A](#).

Custom NSLOOKUP Action Examples

For example, for the following settings, the equivalent NSLOOKUP command string would be:

```
nslookup -timeout=10 192.168.1.1
```

- **host.** 192.168.1.1
- **options.** -timeout=10

- **nameserver.** An empty string

The equivalent JSON structure would be:

```
{
  "host": "192.168.1.1"
  "nameserver": ""
  "options": "-timeout=10"
  "output_format": "html"
}
```

For the following settings, the equivalent NSLOOKUP command string would be:

```
nslookup 192.168.1.2 10.64.148.32
```

- **host.** 192.168.1.2
- **options.** An empty string
- **nameserver.** 10.64.148.32

The equivalent JSON structure would be:

```
{
  "host": "192.168.1.2"
  "nameserver": "10.64.148.32"
  "options": ""
  "output_format": "html"
}
```

Available Output Formats

The output from the ping, traceroute, or nslookup command is processed based on the value of the *output_format* parameter. The following values for the parameter are supported:

- **html** - The output is formatted with newlines and tabs replaced with HTML tags that will render correctly in the SL1 event action log user interface. The executed command is included in the output.
- **text** - The output is formatted as plain text. The executed command is included in the output.
- **raw** - The output is not modified. For each executed command, a dictionary is added to the list with the following keys:
 - **command** - The command that was executed.
 - **output** - The raw output of the command.

NOTE: If the *output_format* is not specified, HTML is used by default.

Appendix

A

A

Variables

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 these 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

Variable	Source	Description
%i (lowercase "eye")	Asset	Asset Location
%k	Asset	Asset Room
%K	Asset	Asset Floor
%P	Asset	Asset plate
%p	Asset	Asset panel
%q	Asset	Asset zone
%Q	Asset	Asset punch
%U	Asset	Asset rack
%u	Asset	Asset shelf
%v	Asset	Asset tag
%w	Asset	Asset model
%W	Asset	Asset make
%m	Automation	Automation policy note
%n	Automation	Automation policy name
%F	Dynamic Alert	Alert ID for a Dynamic Application Alert
%l (uppercase "eye")	Dynamic Alert	For events with a source of "dynamic", this variable contains the index value from SNMP. For events with a source of "syslog" or "trap", this variable contains the value that matches the Identifier Pattern field in the event definition.
%T	Dynamic Alert	Value returned by the Threshold function in a Dynamic Application Alert.
%V	Dynamic Alert	Value returned by the Result function in a Dynamic Application Alert.
%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.



Variable	Source	Description
_%_class_name	Entity	Device class name 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: <ul style="list-style-type: none">• 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

Variable	Source	Description
%2	Event	<p>Sub-entity type.</p> <p>Possible values for organizations are:</p> <ul style="list-style-type: none"> • 9. News feed <p>Possible values for devices are:</p> <ul style="list-style-type: none"> • 1. CPU • 2. Disk • 3. File System • 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	Timestamp of when event was deleted.
%6	Event	Timestamp for event becoming active.
%7	Event	<p>Event severity (1-5), for compatibility with previous versions of SL1. 1=critical, 2=major, 3=minor, 4=notify, 5=healthy.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>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.</p> </div>
%c	Event	Event counter
%d	Event	Timestamp of last event occurrence.
%D	Event	Timestamp of first event occurrence.
%e	Event	Event ID



Variable	Source	Description
%H	Event	URL link to event
%M	Event	Event message
%s	Event	severity (0 - 4). 0=healthy, 1=notify, 2=minor, 3=major, 4=critical.
%S	Event	Severity (Healthy - Critical)
_%user_note	Event	Current note about the event that is displayed on the Events page.
%x	Event	Entity ID
%X	Event	Entity name
%y	Event	Sub-entity ID
%Y	Event	Sub-entity name
%Z	Event	Event source (Syslog - Group)
%z	Event	Event source (1 - 8)
_%ext_ticket_ref	Event	For events associated with an external Ticket ID, this variable contains the external Ticket ID.
%3	Event Policy	Event policy ID
%E	Event Policy	External ID from event policy
%f	Event Policy	Specifies whether event is stateful, that is, has an associated event that will clear the current event. 1 (one)=stateful; 0 (zero)=not stateful.
%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.
%B	Organization	Organization billing ID
%b	Organization	Impacted organization
%C	Organization	Organization CRM ID
%o (lowercase "oh")	Organization	Organization ID
%O (uppercase "oh")	Organization	Organization name

Variable	Source	Description
%r	System	Unique ID / name for the current SL1 system
%7	Ticket	<p>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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>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).</p> </div>
%t	Ticket	Ticket ID

© 2003 - 2019, 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



ScienceLogic

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

International: +1-703-354-1010