



---

## **Network Connectivity Automation PowerPacks**

Network Connectivity Automation PowerPack version 105

Network Connectivity User-Initiated Automation PowerPack version 100

---

# Table of Contents

|   |           |
|---|-----------|
| <b>Introduction</b> .....   | <b>3</b>  |
| What is the Network Connectivity Automation PowerPack? .....                  | 3         |
| Installing the Network Connectivity AutomationPowerPack .....                 | 4         |
| <b>Network Connectivity Automation Policies</b> .....                         | <b>6</b>  |
| Standard Automation Policies .....  | 6         |
| Standard Ping Automation Policy .....   | 12        |
| Standard Traceroute Automation Policy .....                                   | 13        |
| Standard NSLOOKUP Automation Policy .....                                     | 15        |
| Standard NMAP Automation Policies .....                                       | 16        |
| Run NMAP on Affected Port .....   | 16        |
| Run NMAP on Common Port List .....  | 17        |
| Run NMAP on Monitored Ports .....   | 19        |
| <b>Creating and Customizing Automation Policies</b> .....                     | <b>21</b> |
| Prerequisites .....   | 22        |
| Creating an Automation Policy .....   | 22        |
| Example Automation Configuration .....  | 25        |
| Customizing an Automation Policy .....  | 26        |
| Removing an Automation Policy from a PowerPack .....                          | 28        |
| <b>Customizing Network Connectivity Actions</b> .....                         | <b>29</b> |
| Creating a Custom Action Policy with Network Connectivity Actions .....       | 29        |
| Customizing Ping Actions .....  | 31        |
| Custom Ping Action Parameters .....   | 31        |
| Custom Ping Action Examples .....   | 32        |
| Customizing Traceroute Actions .....  | 34        |
| Custom Traceroute Action Parameters .....                                     | 34        |
| Custom Traceroute Action Examples .....                                       | 35        |
| Customizing NSLOOKUP Actions .....  | 35        |
| Custom NSLOOKUP Action Parameters .....                                       | 36        |
| Custom NSLOOKUP Action Examples .....   | 36        |
| Customizing NMAP Actions .....  | 37        |
| Custom NMAP Action Parameters .....   | 38        |
| Custom NMAP Action Examples .....   | 38        |
| Customizing SNMP Actions .....  | 39        |
| Custom SNMP Walk Action Parameters .....                                      | 39        |
| Custom SNMP Action Examples .....   | 39        |
| <b>Network Connectivity User-Initiated Automations</b> .....                  | <b>41</b> |
| What is the Network Connectivity User-Initiated Automation PowerPack? .....   | 42        |
| Installing the Network Connectivity User-Initiated Automation PowerPack ..... | 42        |
| Standard Automation Policies .....  | 43        |
| Running a User Initiated Automation Policy .....                              | 46        |
| Viewing Automation Actions for an Event .....                                 | 47        |
| <b>Run Book Variables</b> .....   | <b>49</b> |
| Run Book Variables .....  | 50        |

---

# Chapter

# 1

## Introduction

---

### Overview

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

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

- *Datacenter Automation Pack*
- ScienceLogic Standard solution

This chapter covers the following topics:

|  |   |
|--|---|
| <a href="#">What is the Network Connectivity Automation PowerPack?</a> .....   | 3 |
| <a href="#">Installing the Network Connectivity Automation PowerPack</a> ..... | 4 |

---

### What is the Network Connectivity Automation PowerPack?

The *Network Connectivity Automation PowerPack* enriches SL1 network connectivity events, such as availability and latency issues, by automatically running common network diagnostic commands and adding the output to the SL1 event log or an associated incident. This PowerPack includes custom action types for running ping, traceroute, nslookup, and nmap commands with parameters that you specify. The PowerPack also includes two dynamic device groups for IPv4 devices and IPv6 devices.

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

# Installing the Network Connectivity Automation PowerPack

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

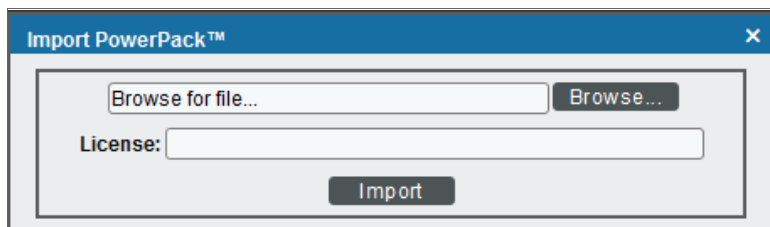
**NOTE:** The *Network Connectivity Automation* PowerPack requires SL1 version 8.10.0 or later. For details on upgrading SL1, see the appropriate SL1 [Release Notes](#).

**CAUTION:** You must install version 101 of the *Datacenter Automation Utilities* PowerPack before proceeding.

**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 at <https://support.sciencelogic.com/s/powerpacks>.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*. The **Import PowerPack** dialog box appears:



4. Click the **[Browse]** button and navigate to the PowerPack file.
5. 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:** 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 Automation PowerPack*.

This chapter covers the following topics:

|   |   |
|---|---|
| <i>Standard Automation Policies</i> ..... | 6 |
|---|---|

---

### Standard Automation Policies

The *Network Connectivity Automation PowerPack* includes six standard automation policies, shown in the figure below. These automation policies run automatically in response to network availability events to diagnose problems. 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 [11]                   |     |              |              |         |        |         |           |                     |  |  |
| Automation Policy Name                            | ID  | Policy State | Organization | Devices | Events | Actions | Edited By | Last Edited         |  |  |
| 1. Network Connectivity: Run IPv6 NMAP            | 422 | Enabled      | System       | 1 group | 2      | 2       | em7admin  | 2020-05-01 15:22:42 |  |  |
| 2. Network Connectivity: Run IPv6 NMAP            | 423 | Enabled      | System       | 1 group | 7      | 2       | em7admin  | 2020-05-01 15:22:42 |  |  |
| 3. Network Connectivity: Run IPv6 NMAP            | 424 | Enabled      | System       | 1 group | 6      | 2       | em7admin  | 2020-05-01 15:22:42 |  |  |
| 4. Network Connectivity: Run NMAP on A            | 363 | Enabled      | System       | 1 group | 2      | 2       | em7admin  | 2020-05-01 15:22:42 |  |  |
| 5. Network Connectivity: Run NMAP on C            | 364 | Enabled      | System       | 1 group | 7      | 2       | em7admin  | 2020-05-01 15:22:42 |  |  |
| 6. Network Connectivity: Run NMAP on H            | 365 | Enabled      | System       | 1 group | 6      | 2       | em7admin  | 2020-05-01 15:22:42 |  |  |
| 7. Network Connectivity: Run Nslookup (I          | 294 | Enabled      | System       | All     | 9      | 2       | em7admin  | 2020-05-01 15:22:42 |  |  |
| 8. Network Connectivity: Run Ping (IPv4)          | 293 | Enabled      | System       | 1 group | 9      | 2       | em7admin  | 2020-05-01 15:22:42 |  |  |
| 9. Network Connectivity: Run Ping (IPv6)          | 421 | Enabled      | System       | 1 group | 9      | 2       | em7admin  | 2020-05-01 15:22:42 |  |  |
| 10. Network Connectivity: Run Traceroute          | 292 | Enabled      | System       | 1 group | 9      | 2       | em7admin  | 2020-05-01 15:22:42 |  |  |

| Available Run Book Policies [12]       |     |              |               |         |        |         |                |                     |  |  |
|--|-----|--------------|---------------|---------|--------|---------|----------------|---------------------|--|--|
| Automation Policy Name                 | ID  | Policy State | Organization  | Devices | Events | Actions | Edited By      | Last Edited         |  |  |
| 1. Device Discovery Automation         | 366 | Enabled      | System        | All     | 1      | 2       | Alfredo Robles | 2020-04-13 19:25:49 |  |  |
| 2. EMC Unity: LUN Information          | 379 | Enabled      | System        | All     | 1      | 1       | em7admin       | 2020-03-13 17:38:06 |  |  |
| 3. Generate Cisco IOS-XR Event         | 295 | Enabled      | System        | All     | 1      | 1       | em7admin       | 2019-10-03 17:08:30 |  |  |
| 4. Linux SSH: Run My CPU Diagnostics   | 339 | Disabled     | Linux Devices | 2       | 4      | 2       | em7admin       | 2020-04-29 21:58:29 |  |  |
| 5. Run IS Diagnostics                  | 367 | Enabled      | System        | All     | 1      | 1       | em7admin       | 2020-02-24 21:26:17 |  |  |
| 6. Test Expiry Clears                  | 361 | Enabled      | System        | All     | 1      | 1       | em7admin       | 2020-01-14 18:39:58 |  |  |
| 7. Test Process Restart Without Passwo | 340 | Enabled      | System        | All     | 1      | 2       | em7admin       | 2019-11-11 22:11:28 |  |  |
| 8. Test Traceroute with Port           | 338 | Enabled      | System        | All     | 1      | 1       | em7admin       | 2019-11-07 16:41:22 |  |  |
| 9. Test Work Instructions              | 296 | Disabled     | System        | All     | 1      | 1       | em7admin       | 2020-03-13 15:56:40 |  |  |
| 10. Truncate Spool Mail                | 337 | Enabled      | System        | All     | 2      | 1       | em7admin       | 2019-11-06 15:32:23 |  |  |

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 NMAP on Affected Port      | <ul style="list-style-type: none"> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> </ul>   | <ul style="list-style-type: none"> <li>• Run NMAP: Single Port from Event</li> <li>• Datacenter Automation: Format Command Output as HTML</li> </ul>      |
| Network Connectivity: Run IPv6 NMAP on Affected Port | <ul style="list-style-type: none"> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> </ul>   | <ul style="list-style-type: none"> <li>• Run IPv6 NMAP: Single Port from Event</li> <li>• Datacenter Automation: Format Command Output as HTML</li> </ul> |
| Network Connectivity: Run NMAP on Common Ports       | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> </ul> | <ul style="list-style-type: none"> <li>• Run NMAP: Common Port List</li> <li>• Datacenter Automation: Format Command Output as HTML</li> </ul>            |

| Automation Policy Name                                 | Aligned Events   | Automation Action (Default)   |
|--|--|---|
|  | <ul style="list-style-type: none"> <li>• Transactions: Round trip mail did not arrive within threshold</li> </ul>  |   |
| Network Connectivity: Run IPv6 NMAP on Common Ports    | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> <li>• Transactions: Round trip mail did not arrive within threshold</li> </ul> | <ul style="list-style-type: none"> <li>• Run IPv6 NMAP: Common Port List</li> <li>• Datacenter Automation: Format Command Output as HTML</li> </ul> |
| Network Connectivity: Run NMAP on Monitored Ports      | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> </ul>  | <ul style="list-style-type: none"> <li>• Run NMAP: Monitored Ports</li> <li>• Datacenter Automation: Format Command Output as HTML</li> </ul>       |
| Network Connectivity: Run IPv6 NMAP on Monitored Ports | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> </ul>  | <ul style="list-style-type: none"> <li>• Run IPv6 NMAP: Monitored Ports</li> <li>• Datacenter Automation: Format Command Output as HTML</li> </ul>  |
| Network Connectivity: Run Nslookup (IPv4)              | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> </ul>   | <ul style="list-style-type: none"> <li>• Run Nslookup: Default Options</li> </ul>   |



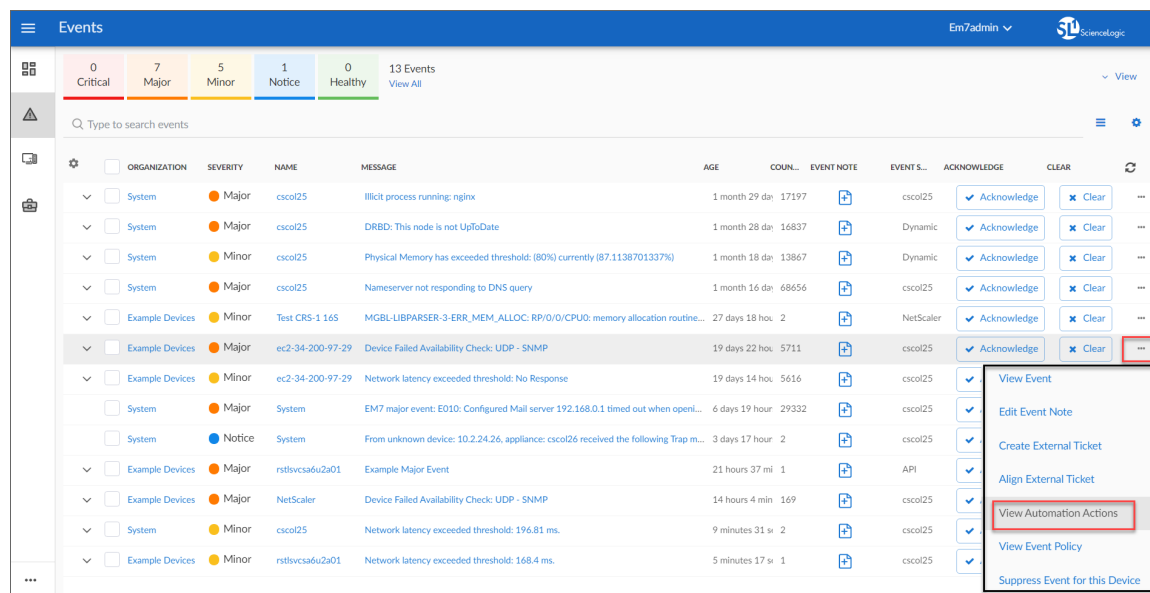
| Automation Policy Name                | Aligned Events  | Automation Action (Default)  |
|---------------------------------------|---|--|
|                                       | <ul style="list-style-type: none"> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: DNS hostname resolution time above threshold</li> <li>• Poller: Failed to resolve hostname</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> <li>• Transactions: Round trip mail did not arrive within threshold</li> </ul>  | <ul style="list-style-type: none"> <li>• Datacenter Automation: Format Command Output as HTML</li> </ul>                                       |
| Network Connectivity: Run Ping (IPv4) | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Network Latency Exceeded Threshold</li> <li>• Poller: TCP connection time above threshold</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> <li>• Transactions: Round trip mail did not arrive within threshold</li> </ul> | <ul style="list-style-type: none"> <li>• Run Ping: Default Options</li> <li>• Datacenter Automation: Format Command Output as HTML</li> </ul>  |
| Network Connectivity: Run Ping (IPv6) | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: Device not responding to ping (high frequency)</li> </ul>  | <ul style="list-style-type: none"> <li>• Run Ping6: Default Options</li> <li>• Datacenter Automation: Format Command Output as HTML</li> </ul> |

| Automation Policy Name                      | Aligned Events  | Automation Action (Default)  |
|---|---|--|
|   | <ul style="list-style-type: none"> <li>• Poller: Network Latency Exceeded Threshold</li> <li>• Poller: TCP connection time above threshold</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> <li>• Transactions: Round trip mail did not arrive within threshold</li> </ul>   |  |
| Network Connectivity: Run Traceroute (IPv4) | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Network Latency Exceeded Threshold</li> <li>• Poller: TCP connection time above threshold</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> <li>• Transactions: Round trip mail did not arrive within threshold</li> </ul> | <ul style="list-style-type: none"> <li>• Run Traceroute: Default Options</li> <li>• Datacenter Automation: Format Command Output as HTML</li> </ul>      |
| Network Connectivity: Run Traceroute (IPv6) | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Network Latency Exceeded Threshold</li> <li>• Poller: TCP connection time above threshold</li> <li>• Poller: TCP/UDP port not responding</li> </ul>  | <ul style="list-style-type: none"> <li>• Run IPv6 Traceroute: Default Options</li> <li>• Datacenter Automation: Format Command Output as HTML</li> </ul> |

| Automation Policy Name | Aligned Events  | Automation Action (Default) |
|------------------------|---|-----------------------------|
|                        | <ul style="list-style-type: none"> <li>• Poller: TCP/UDP port not responding (SMTP)</li> <li>• Transactions: Round trip mail did not arrive within threshold</li> </ul> |                             |

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:



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 NMAP, Ping, and Nslookup information in the following figure. The log indicates that the following actions ran successfully and indicates which SL1 appliance ran the action:

- Run Nslookup (IPv4): Default Options and Datacenter Automation: Format Command Output as HTML
- Run NMAP on Common Ports and Datacenter Automation: Format Command Output as HTML
- Run Ping (IPv4): Default Options and Datacenter Automation: Format Command Output as HTML

```

Event Actions Log | For Event [177587] Refresh Guide
2020-05-04 13:45:28
Automation Policy Network Connectivity: Run NMAP on Monitored Ports action Datacenter Automation: Format Output as HTML ran Successfully
Message: Snippet (365) executed without incident
Result: {formatted_output: Enrichment Command Output
}
2020-05-04 13:44:55
Automation Policy Network Connectivity: Run Nslookup (IPv4) action Datacenter Automation: Format Output as HTML ran Successfully
Message: Snippet (365) executed without incident
Result: {formatted_output: Enrichment Command Output
}
Command: nslookup 10.40.3.5 Appliance: csc0126
5.3.40.10.in-addr.arpa name = t112r2-ex-01.mst112r2.com.
Authoritative answers can be found from:
}
2020-05-04 13:44:55
Automation Policy Network Connectivity: Run NMAP on Common Ports action Datacenter Automation: Format Output as HTML ran Successfully
Message: Snippet (365) executed without incident
Result: {formatted_output: Enrichment Command Output
}
Command: nmap -Pn -p 21,22,25,53,80,443,5985,5986 10.40.3.5 Appliance: csc0126
Starting Nmap 6.40 ( http://nmap.org ) at 2020-05-04 13:40 UTC
Nmap scan report for t112r2-ex-01.mst112r2.com (10.40.3.5)
Host is up (0.0017s latency).
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
25/tcp    closed smtp
53/tcp    closed domain
80/tcp    filtered http
443/tcp   filtered https
5985/tcp   filtered wspan
5986/tcp   filtered wspan
Nmap done: 1 IP address (1 host up) scanned in 2.76 seconds
}
2020-05-04 13:43:55
Automation Policy Network Connectivity: Run Ping (IPv4) action Datacenter Automation: Format Output as HTML ran Successfully
Message: Snippet (365) executed without incident
Result: {formatted_output: Enrichment Command Output
}
Command: ping -c 5 10.40.3.5 Appliance: csc0126
PING 10.40.3.5 (10.40.3.5) 56(84) bytes of data.
--- 10.40.3.5 ping statistics ---

```

**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.

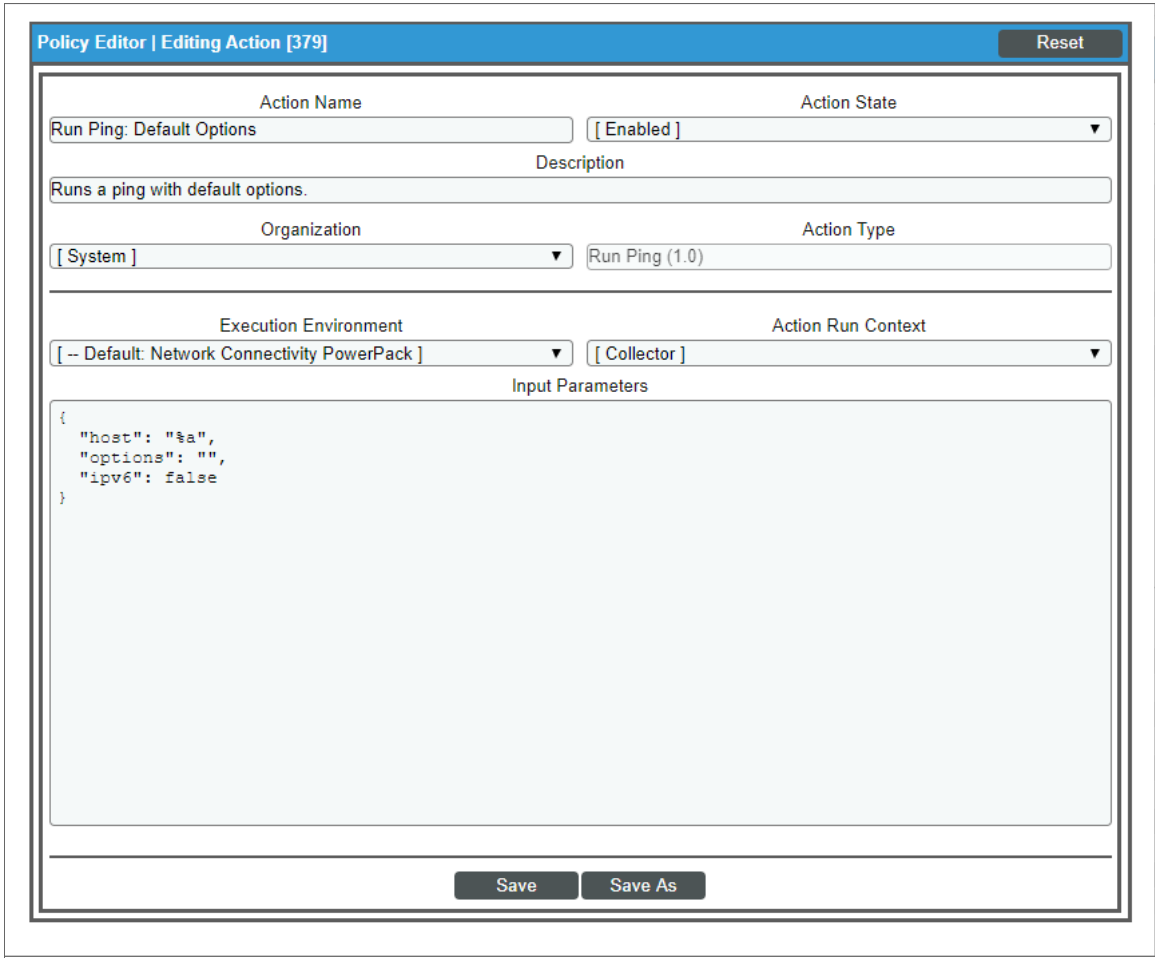
## Standard Ping Automation Policy

The "Network Connectivity: Run Ping (IPv4)" or "Network Connectivity: Run Ping (IPv6)" automation policies are triggered by the following events, depending on the address type of the device:

- 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 appropriate automation policy "Network Connectivity: Run Ping (IPv4)" or "Network Connectivity: Run Ping (IPv6)" executes the action "Run Ping: Default Options" or "Run Ping6: Default Options", respectively, and formats the output with "Datacenter Automation: Format Command Output as HTML". 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 IPv4 ping action:



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

## Standard Traceroute Automation Policy

The "Network Connectivity: Run Traceroute (IPv4)" or "Network Connectivity: Run Traceroute (IPv6)" automation policies are 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)" or "Network Connectivity: Run Traceroute (IPv6)" executes the "Run Traceroute: Default Options" or "Run IPv6 Traceroute: Default Options" action, depending upon the type of network address of the device that triggered the event. These actions run a standard traceroute 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 IPv4 traceroute action:

The screenshot shows the 'Policy Editor | Editing Action [378]' interface. At the top right is a 'Reset' button. The main form contains the following fields:

- Action Name:** Run Traceroute: Default Options
- Action State:** [ Enabled ]
- Description:** Runs an IPv4 traceroute with default options.
- Organization:** [ System ]
- Action Type:** Run Traceroute (1.0)
- Execution Environment:** [ -- Default: Network Connectivity PowerPack ]
- Action Run Context:** [ Collector ]
- Input Parameters:** A text area containing a JSON object:
 

```
{
  "host": "%a",
  "options": "",
  "packet_length": 0
}
```

At the bottom of the form are two buttons: 'Save' and 'Save As'.

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

## 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" and formats the output with "Enrichment: Util: Format Command Output as HTML". 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.

The screenshot shows the 'Policy Editor | Editing Action [380]' window. It contains the following fields and controls:

- Action Name:** Run Nslookup: Default Options
- Action State:** [ Enabled ]
- Description:** Runs an nslookup with default options.
- Organization:** [ System ]
- Action Type:** Run Nslookup (1.0)
- Execution Environment:** [-- Default: Network Connectivity PowerPack ]
- Action Run Context:** [ Collector ]
- Input Parameters:** A text area containing a JSON object:
 

```
{
  "host": "%a",
  "nameserver": "",
  "options": ""
}
```
- Buttons:** Save, Save As, and a Reset button in the top right corner.

**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.

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

## Standard NMAP Automation Policies

Three NMAP automation policies for IPv4 devices and three NMAP automation policies for IPv6 devices are included with this PowerPack. Each policy is described in more detail in this section.

### Run NMAP on Affected Port

The "Network Connectivity: Run NMAP on Affected Port" or "Network Connectivity: Run IPv6 NMAP on Affect Port" automation policies are triggered by the following events:

- Poller: TCP/UDP port not responding
- Poller: TCP/UDP port not responding (SMTP)



**Default Behavior.** When these events occur for IPv4 devices, the automation policy "Network Connectivity: Run NMAP on Affected Port" executes the action "Run NMAP: Single Port from Event" and formats the output with "Datacenter Automation: Format Command Output as HTML". For IPv6 devices, the automation policy "Network Connectivity: Run IPv6 NMAP on Affected Port" executes the "Run IPv6 NMAP: Single Port from Event" action and formats the output with "Datacenter Automation: Format Command Output as HTML". Either action runs a standard NMAP command on the port provided in the event. 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 IPv4 NMAP action:

The screenshot displays the 'Policy Editor | Editing Action [483]' window. The interface includes a 'Reset' button in the top right corner. The main configuration area is divided into several sections:

- Action Name:** Run NMAP: Single Port from Event
- Action State:** [ Enabled ]
- Description:** Runs an NMAP command on the port provided in the event sub-entity.
- Organization:** [ System ]
- Action Type:** Run NMAP (1.0)
- Execution Environment:** [ -- Default: Network Connectivity PowerPack ]
- Action Run Context:** [ Collector ]
- Input Parameters:** A code editor containing the following JSON configuration:

```
{
  "host": "%a",
  "options": "-p %Y"
}
```

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

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

## Run NMAP on Common Port List

The "Network Connectivity: Run NMAP on Common Port List" or "Network Connectivity: Run IPv6 NMAP on Common Port List" automation policies are triggered by the following events:

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

- Poller: Availability Check Failed
- Poller: Availability Flapping
- 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 for IPv4 devices, the automation policy "Network Connectivity: Run NMAP on Common Port List" executes the action "Run NMAP: Common Port List" and formats the output with "Datacenter Automation: Format Command Output as HTML". When these events occur for IPv6 devices, the automation policy "Network Connectivity: Run IPv6 NMAP on Common Port List" executes the action "Run IPv6 NMAP: Common Port List" and formats the output with "Datacenter Automation: Format Command Output as HTML". Either action runs a standard NMAP command on ports 21, 22, 25, 53, 80, 443, 5985, and 5986. 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 IPv4 NMAP action:

The screenshot shows the 'Policy Editor | Editing Action [484]' window. The interface includes a 'Reset' button in the top right corner. The main configuration area is divided into several sections:

- Action Name:** Run NMAP: Common Port List
- Action State:** [ Enabled ]
- Description:** Runs an NMAP command using a list of common ports.
- Organization:** [ System ]
- Action Type:** Run NMAP (1.0)
- Execution Environment:** [ -- Default: Network Connectivity PowerPack ]
- Action Run Context:** [ Database ]
- Input Parameters:** A JSON object:
 

```
{
  "host": "%a",
  "options": "-p 21,22,25,53,80,443,5985,5986"
}
```

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

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

## Run NMAP on Monitored Ports

The "Network Connectivity: Run NMAP on Monitored Ports" or "Network Connectivity: Run IPv6 NMAP on Monitored Ports" automation policies are triggered by the following events:

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

**Default Behavior.** When these events occur for IPv4 devices, the automation policy "Network Connectivity: Run NMAP on Monitored Ports" executes the action "Run NMAP: Monitored Ports" and formats the output with "Datacenter Automation: Format Command Output as HTML". When these events occur for IPv6 devices, the automation policy "Network Connectivity: Run IPv6 NMAP on Monitored Ports" executes the action "Run IPv6 NMAP: Monitored Ports" and formats the output with "Datacenter Automation: Format Command Output as HTML". Either action runs a standard NMAP command on any ports that are currently monitored with a port monitoring policy on the triggering device. 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 IPv4 NMAP action:

Policy Editor | Editing Action [485]
Reset

---

Action Name  
Run NMAP: Monitored Ports

Action State  
[ Enabled ]

---

Description

Runs an NMAP command on the ports that are currently monitored on the device.

---

Organization  
[ System ]

Action Type  
Run NMAP (1.0)

---

Execution Environment  
[ -- Default: Network Connectivity PowerPack ]

Action Run Context  
[ Collector ]

---

Input Parameters

```

{
  "host": "%a",
  "options": "-p %_monitored_ports_"
}

```

---

Save
Save As

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

## Creating and Customizing Automation Policies

---

### Overview

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

This chapter covers the following topics:

|   |    |
|---|----|
| <i>Prerequisites</i> .....                    | 22 |
| <i>Creating an Automation Policy</i> .....    | 22 |
| <i>Example Automation Configuration</i> ..... | 25 |
| <i>Customizing an Automation Policy</i> ..... | 26 |

---

## Prerequisites

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

- Which commands (Ping, Traceroute, NSLOOKUP, or NMAP) you want to run on a device when an event occurs. There are 11 automation actions in the PowerPack that run these commands with different options. 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 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.

The screenshot shows the 'Automation Policy Editor | Creating New Automation Policy' interface. At the top right is a 'Reset' button. The main configuration area includes:

- Policy Name:** An empty text input field.
- Policy Type:** A dropdown menu set to '[ Active Events ]'.
- Policy State:** A dropdown menu set to '[ Enabled ]'.
- Policy Priority:** A dropdown menu set to '[ Default ]'.
- Organization:** A dropdown menu set to 'Example Devices'.
- Criteria Logic:** A series of dropdown menus: '[ Severity >= ]', '[ Minor, ]', '[ and 5 minutes has elapsed ]', '[ since the first occurrence, ]', '[ and event is NOT cleared ]', and 'and all times are valid'.
- Match Logic:** A dropdown menu set to '[ Text search ]'.
- Match Syntax:** An empty text input field.
- Repeat Time:** A dropdown menu set to '[ Only once ]'.
- Align With:** A dropdown menu set to '[ Devices ]'.
- Include events for entities other than devices (organizations, assets, etc.)
- Trigger on Child Rollup

Below these settings are four panels for selecting items to be included in the policy:

- Available Devices:** A list of devices including 'Example Devices', 'Cisco Systems: CRS-1 16S: Test CRS-1 16S', 'Citrix: NetScaler: NetScaler', 'Ping: ICMP: ec2-34-200-97-29', 'Virtual Device: Domain Name: Test Device', 'Virtual Device: Domain Name: Test Device 2', 'Linux Devices', and 'Linux: CentOS Linux 7 (Core): 10.2.24.31'. A '»' button is next to the list.
- Aligned Devices:** A list containing '(All devices)'. A '«' button is next to the list.
- Available Events:** A list of event IDs and descriptions such as '[5678] Critical: 3PAR Trap: Critical Alert', '[5649] Critical: 3PAR: Disk Utilization Exceeded Critical Threshold', '[3569] Critical: AKCP: AC Voltage sensor detects no current', '[3578] Critical: AKCP: DC Voltage sensor High Critical', '[3579] Critical: AKCP: DC Voltage sensor Low Critical', '[3568] Critical: AKCP: Dry Contact Sensor Low Critical', '[3574] Critical: AKCP: Smoke Detector Alert!', and '[3572] Critical: AKCP: Water Sensor has detected water'. A '»' button is next to the list.
- Aligned Events:** A list containing '(All events)'. A '«' button is next to the list.
- Available Actions:** A list of actions including 'SNMP Trap [1]: EM7 Event Trap', 'SNMP Trap [1]: RBA Base Pack: Send Trap', 'SNMP Trap [1]: SL1 Event Trap', 'Create Ticket [2]: RBA Base Pack: Create Ticket', 'Snippet [5]: API VeloCloud initial disable', 'Snippet [5]: Automation Utilities: Calculate Memory Size for Each A', and 'Snippet [5]: AWS: Disable Instance By Tag'. A '»' button is next to the list.
- Aligned Actions:** An empty list with '↑' and '↓' buttons next to it.

A 'Save' button is located at the bottom center of the interface.

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 Automation PowerPack*. You should see Run Ping, Run Traceroute, Run Nslookup, and Run NMAP 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. Select an output format action from the *Datacenter Automation Utilities PowerPack*.

**CAUTION:** Remember that you must include an output format action (from the *Datacenter Automation Utilities PowerPack*) for this action to produce output.

4. To align the policy with a device group ("IPv4 Devices" or "IPv6 Devices") supplied in the PowerPack, do the following:
  - a. In the **Align With** drop-down menu, select "Device Groups".
  - b. In the **Available Device Groups** field, select the "IPv4 Devices" or "IPv6 Devices" device group, and click the right arrow (>>).
5. Optionally, supply values in the other fields on this page to refine when the automation will trigger.
6. 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.

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 Automation PowerPack*:

The screenshot shows the 'Automation Policy Editor | Editing Automation Policy [421]' window. The configuration is as follows:

- Policy Name:** My NC Ping (IPv6)
- Policy Type:** [ Active Events ]
- Policy State:** [ Enabled ]
- Policy Priority:** [ Default ]
- Organization:** [ System ]
- Criteria Logic:** [ Severity >= ] [ Minor, ] [ and no time has elapsed ] [ since the first occurrence, ] [ and event is NOT cleared ] [ and all times are valid ]
- Match Logic:** [ Text search ]
- Match Syntax:** (empty)
- Repeat Time:** [ Only once ]
- Align With:** [ Device Groups ]
- Include events for entities other than devices (organizations, assets, etc.)
- Trigger on Child Rollup
- Available Device Groups:** IPv4 Devices, ScienceLogic Data Collectors, Servers
- Aligned Device Groups:** IPv6 Devices
- Available Events:** [5678] Critical: 3PAR Trap: Critical Alert, [5649] Critical: 3PAR: Disk Utilization Exceeded Critical Thre:, [3569] Critical: AKCP: AC Voltage sensor detects no current
- Aligned Events:** [1934] Critical: Poller: Availability and Latency checks failed, [4071] Critical: Poller: Device not responding to ping (high freq, [1932] Major: Poller: Availability Check Failed, [4011] Major: Poller: Availability Flapping
- Available Actions:** SNMP Trap [1]: EM7 Event Trap, SNMP Trap [1]: RBA Base Pack: Send Trap, SNMP Trap [1]: SL1 Event Trap
- Aligned Actions:** 1. Run Ping [113]: Run Ping6: Default Options, 2. Snippet [5]: Datacenter Automation: Format Output a

Buttons at the bottom: Save, Save As, Reset.

The policy uses the following settings:

- **Policy Name.** The policy is named "My NC Ping (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 "IPv6 Devices" dynamic device group.

- **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 actions. The formatting action allows you to view the output of ping in the Automation Log, accessed through the SL1 Event Console:
  - Run Ping6: Default options
  - Datacenter Automation: Format Command Output as HTML

---

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

3. Complete the following fields as needed:

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

- **Aligned Actions.** This field includes the actions from the Network Connectivity Automation PowerPack. You should see Run Ping, Run Traceroute, Run Nslookup, and Run NMAP 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. Select an output format action from the *Datacenter Automation Utilities* PowerPack.



**CAUTION:** Remember that you must include an output format action (from the *Datacenter Automation Utilities* PowerPack) for this action to produce output.

- **Organization.** Select the organization that will use this policy.
4. To align the policy with a device group ("IPv4 Devices" or "IPv6 Devices") supplied in the PowerPack, do the following:
    - a. In the **Align With** drop-down menu, select "Device Groups".
    - b. In the **Available Device Groups** field, select the "IPv4 Devices" or "IPv6 Devices" device group, and click the right arrow (> >).
  5. Optionally, supply values in the other fields on the **Automation Policy Editor** page to refine when the automation will trigger.
  6. Click **[Save]**.

## Removing an Automation Policy from a PowerPack

After you have customized a policy from a *Network Connectivity 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/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 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 Policies** 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 five action types embedded in the Network Connectivity 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:

|   |    |
|---|----|
| <a href="#">Creating a Custom Action Policy with Network Connectivity Actions</a> | 29 |
| <a href="#">Customizing Ping Actions</a>  | 31 |
| <a href="#">Customizing Traceroute Actions</a>                                    | 34 |
| <a href="#">Customizing NSLOOKUP Actions</a>                                      | 35 |
| <a href="#">Customizing NMAP Actions</a>  | 37 |
| <a href="#">Customizing SNMP Actions</a>  | 39 |

---

### Creating a Custom Action Policy with Network Connectivity Actions

You can use one of the Action Types included with the Network Connectivity Automation 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. At the top, it says 'Policy Editor | Creating New Action' with a 'Reset' button. The form contains the following fields:

- Action Name:** An empty text input field.
- Action State:** A dropdown menu currently set to '[ Enabled ]'.
- Description:** An empty text input field.
- Organization:** A dropdown menu currently set to '[ System ]'.
- Action Type:** A dropdown menu with a list of options:
  - Send an Email Notification
  - 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
  - Execute Commands via SSH (1.0)
  - Execute Remote PowerShell Request (1.0)
  - Get VMware Diagnostic Logs (1.0)
  - Make an HTTP Request (1.0)
  - Run Integration Service Application (1.0)
  - Run NMAP (1.0)
  - Run Nslookup (1.0)
  - Run Ping (1.0)** (highlighted in blue)
  - Run Traceroute (1.0)
  - ServiceNow: Create, Update, Clear Incident (1.0)
  - Update PowerPack Automation Policies (1.0)
- Email Subject:** A text input field containing '%S Event: %M'.
- Email:** A text area containing a template:
 

```
Severity: %S
First Occurred: %D
Last Occurred: %d
Occurrences: %c
Source: %Z
Organization: %O
Device: %X
..  ..
```
- Available Emails:** An empty list box.

At the bottom right of the form is a 'Save' button.

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
    - Run Traceroute
    - Run Nslookup

- Run NMAP
- Run SNMP Walk
- **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.

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 Ping Actions

The Network Connectivity Automation PowerPack includes two 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 Automation PowerPack.

| Action Name                | Description                       | host   | options                        | ipv6  |
|----------------------------|-----------------------------------|--|--------------------------------|-------|
| Run Ping: Default Options  | Runs a ping with default options  | Default is %a (IP address of current device) | Default is None (empty string) | false |
| Run Ping6: Default Options | Runs a ping6 with default options | Default is %a (IP address of current device) | Default is None (empty string) | true  |

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

## 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. Escape characters are not supported. 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. |
| 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"
  "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:

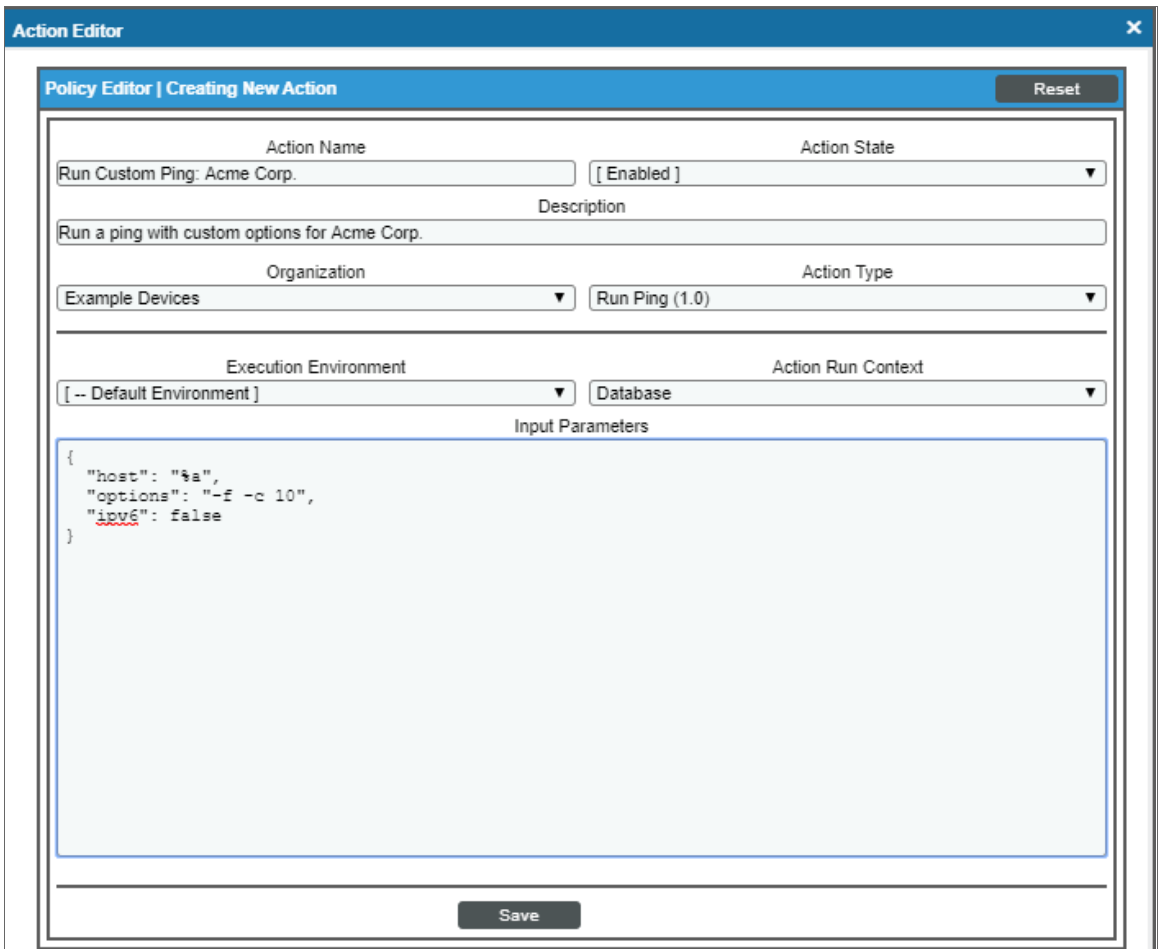
- **host.** 192.168.1.1
- **options.** -c 10

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"
  "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.



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

## Customizing Traceroute Actions

The Network Connectivity Automation PowerPack includes two 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 Connectivity AutomationPowerPack*.

| Action Name                          | Description   | host   | options                              | packet_length      |
|--------------------------------------|---|--|--------------------------------------|--------------------|
| Run Traceroute: Default Options      | Runs an IPv4 traceroute with default options              | Default value is %a (IP address of the current device) | Default value is None (empty string) | Default value is 0 |
| Run IPv6 Traceroute: Default Options | Runs an IPv6 traceroute with all other options as default | Default value is %a (IP address of the current device) | Default value is -6                  | Default value is 0 |

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

## 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 "-I", in this field. |
| packet_length | integer    | The packet length to include in the traceroute command. To use the default packet length, use "0".  |

**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
}
```

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
}
```

---

## Customizing NSLOOKUP Actions

The Network Connectivity Automation PowerPack includes an automation action that executes 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 Connectivity Automation* PowerPack.

| Action Name                   | Description                           | host   | options                              | nameserver                           |
|-------------------------------|---------------------------------------|--|--------------------------------------|--------------------------------------|
| Run Nslookup: Default Options | Runs an nslookup with default options | Default value is %a (IP address of the current device) | Default value is None (empty string) | Default value is None (empty string) |

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

## 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.                  |

**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"
}
```

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

```
nslookup 192.168.1.2 10.644.148.32
```

- **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": ""
}
```

## Customizing NMAP Actions

The Network Connectivity Automation PowerPack includes three automation actions that execute an NMAP 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 NMAP" action type are included in the Network Connectivity Automation PowerPack.

| Action Name                           | Description  | host   | options  |
|---------------------------------------|--|--|--|
| Run NMAP: Common Port List            | Runs an NMAP command using a list of common ports.                                 | Default is %a (IP address of current device) | Default ports are 21, 22, 25, 53, 80, 443, 5985, and 5986. |
| Run IPv6 NMAP: Common Port List       | Runs an IPv6 NMAP command using a list of common ports.                            | Default is %a (IP address of current device) | Default ports are 21, 22, 25, 53, 80, 443, 5985, and 5986. |
| Run NMAP: Monitored Ports             | Runs an NMAP command on the ports that are currently monitored on the device.      | Default is %a (IP address of current device) | Default is %_monitored_ports_                              |
| Run IPv6 NMAP: Monitored Ports        | Runs an IPv6 NMAP command on the ports that are currently monitored on the device. | Default is %a (IP address of current device) | Default is %_monitored_ports_                              |
| Run NMAP: Single Port from Event      | Runs an NMAP command on the port provided in the event sub-entity.                 | Default is %a (IP address of current device) | Default is %Y  |
| Run IPv6 NMAP: Single Port from Event | Runs an IPv6 NMAP command on the port provided in the event sub-entity.            | Default is %a (IP address of current device) | Default is %Y  |

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

## Custom NMAP Action Parameters

Custom NMAP action types accept the following parameters:

| Parameter | Input type | Description  |
|-----------|------------|--|
| host      | string     | The hostname or IP address to include in the NMAP command. You can use the substitution variable "%a" to specify the IP address of the current device. |
| options   | string     | The options string to include in the command. See the parameters for specific NMAP actions earlier in this section.                                    |

**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.

The special `%_monitored_ports_` substitution variable is supported for the "Run NMAP" and "Run IPv6 NMAP" action types. This variable replaces a comma-separated list of ports from the monitoring policies aligned to the triggering device.

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

## Custom NMAP Action Examples

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

```
nmap -p 22 192.168.1.1
```

- **host.** 192.168.1.1
- **options.** -p 22

The equivalent JSON structure would be:

```
{
  "host": "192.168.1.1"
  "options": "-p 22"
}
```

Suppose you want to scan a range of ports. In this example, we're scanning the ports from 1 to 100. For the following settings, the equivalent NMAP command string would be:

```
nmap -p 1-100 192.168.1.1
```

- **host.** 192.168.1.1
- **options.** -p 1-100

The equivalent JSON structure would be:

```
{
  "host": "192.168.1.2"
  "options": "-p 1-100"
}
```

## Customizing SNMP Actions

The Network Connectivity Automation PowerPack includes an automation action type that can be used to create automation actions that run the SNMP walk command. To do this, you specify the host, OID, and SNMP credential in the **Action Policy Editor** modal.

### Custom SNMP Walk Action Parameters

The SNMP Walk action type accepts the following parameters:

| Parameter     | Input type | Description   |
|---------------|------------|---|
| host          | string     | The hostname or IP address to include in the SNMP command. You can use the substitution variable "%a" to specify the IP address of the current device.  |
| oid           | string     | The OID to walk. You can use substitution characters in this field.   |
| credential_id | integer    | The ID of the SNMP credential to use when running the command. The SNMP credential specifies the SNMP version, community string, timeout, and other connection parameters. If you specify "0" (zero) in this field, the SNMP Read credential setting of the device associated with the triggering event will be used. |

**Using Substitution Values.** The host and oid inputs can contain substitution values that match the keys in EM7\_VALUES.

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

### Custom SNMP Action Examples

For example, settings to walk the System MIB using the IP address and SNMP Read credential of the device associated with the triggering event, the parameters would be::

- **host.** %a
- **oid.** .1.3.6.1.2.1.1

- **credential\_id**. ID of the SNMP credential to use when running the command.

The equivalent JSON structure would be:

```
{  
  "host": "%a"  
  "oid": ".1.3.6.1.2.1.1"  
  "credential_id": 0  
}
```



---

# Chapter

# 5

## Network Connectivity User-Initiated Automations

---

### Overview

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

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

- *Datacenter Automation Pack*
- ScienceLogic Standard solution

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

This chapter covers the following topics:

|   |    |
|---|----|
| <a href="#">What is the Network Connectivity User-Initiated Automation PowerPack?</a> .....   | 42 |
| <a href="#">Installing the Network Connectivity User-Initiated Automation PowerPack</a> ..... | 42 |
| <a href="#">Standard Automation Policies</a> .....  | 43 |

---

## What is the Network Connectivity User-Initiated Automation PowerPack?

The *Network Connectivity User-Initiated Automation* PowerPack includes automation policies that you can use to run common network diagnostic commands from the SL1 event console, using Event Tools. This PowerPack is supplemental to the *Network Connectivity 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 Network Connectivity User-Initiated Automation PowerPack

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

**NOTE:** The *Network Connectivity User-Initiated Automation* PowerPack requires SL1 version 10.1.0 or later. For details on upgrading SL1, see the appropriate SL1 [Release Notes](#).

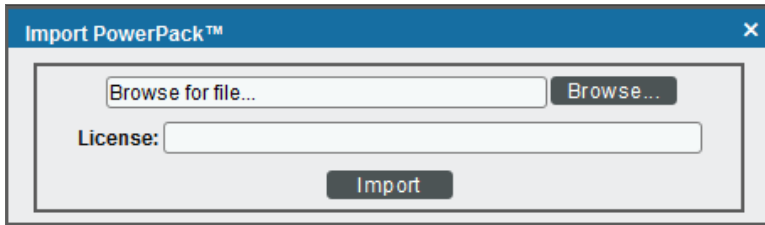
**WARNING:** You must also install the *Datacenter Automation Utilities* PowerPack, which provides the output formats for the automation actions included in this PowerPack.

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

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site at <https://support.sciencelogic.com/s/powerpacks>.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).

3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*. The **Import PowerPack** dialog box appears:



4. Click the **[Browse]** button and navigate to the PowerPack file.
5. 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 *Network Connectivity User-Initiated Automation* PowerPack includes standard automation policies that trigger automation actions that will run network diagnostic commands from the SL1 event console.

The automation policies available in this release of the PowerPack are tied to default SL1 events for availability and monitoring policies.

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 *Network Connectivity* PowerPack and are not installed with the SL1 platform. You must install the PowerPack to obtain these events.

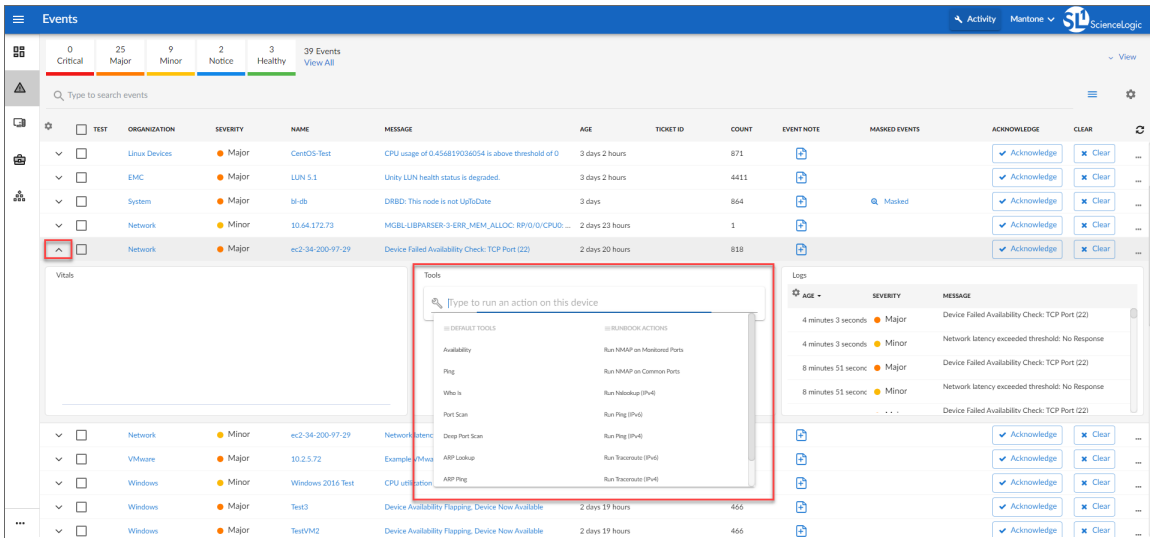
| Automation Policy Name      | Aligned Events   | Automation Action  |
|-----------------------------|--|--|
| Run NMAP on Affected Port   | <ul style="list-style-type: none"> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> </ul>  | <ul style="list-style-type: none"> <li>• Run NMAP: Single Port from Event</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul> |
| Run NMAP on Common Ports    | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> <li>• Transactions: Round trip mail did not arrive within threshold</li> </ul>   | <ul style="list-style-type: none"> <li>• Run NMAP: Common Port List</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul>       |
| Run NMAP on Monitored Ports | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> </ul>  | <ul style="list-style-type: none"> <li>• Run NMAP: Monitored Ports</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul>        |
| Run Nslookup (IPv4)         | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: Failed to resolve hostname</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> <li>• Transactions: Round trip mail did not arrive within threshold</li> <li>• Poller: DNS hostname resolution time above threshold</li> </ul> | <ul style="list-style-type: none"> <li>• Run Nslookup: Default Options</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul>    |

| Automation Policy Name | Aligned Events  | Automation Action   |
|------------------------|---|---|
| Run Ping (IPv4)        | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> <li>• Transactions: Round trip mail did not arrive within threshold</li> <li>• Poller: Network Latency Exceeded Threshold</li> <li>• Poller: TCP connection time above threshold</li> </ul> | <ul style="list-style-type: none"> <li>• Run Ping: Default Options</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul>       |
| Run Ping (IPv6)        | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> <li>• Transactions: Round trip mail did not arrive within threshold</li> <li>• Poller: Network Latency Exceeded Threshold</li> <li>• Poller: TCP connection time above threshold</li> </ul> | <ul style="list-style-type: none"> <li>• Run Ping6: Default Options</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul>      |
| Run Traceroute (IPv4)  | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: TCP/UDP port not responding</li> </ul>   | <ul style="list-style-type: none"> <li>• Run Traceroute: Default Options</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul> |

| Automation Policy Name | Aligned Events  | Automation Action  |
|------------------------|---|--|
|                        | <ul style="list-style-type: none"> <li>• Poller: TCP/UDP port not responding (SMTP)</li> <li>• Transactions: Round trip mail did not arrive within threshold</li> <li>• Poller: Network Latency Exceeded Threshold</li> <li>• Poller: TCP connection time above threshold</li> </ul>  |  |
| Run Traceroute (IPv6)  | <ul style="list-style-type: none"> <li>• Poller: Availability and Latency checks failed</li> <li>• Poller: Device not responding to ping (high frequency)</li> <li>• Poller: Availability Check Failed</li> <li>• Poller: Availability Flapping</li> <li>• Poller: TCP/UDP port not responding</li> <li>• Poller: TCP/UDP port not responding (SMTP)</li> <li>• Transactions: Round trip mail did not arrive within threshold</li> <li>• Poller: Network Latency Exceeded Threshold</li> <li>• Poller: TCP connection time above threshold</li> </ul> | <ul style="list-style-type: none"> <li>• Run IPv6 Traceroute: Default Options</li> <li>• Datacenter Automation: Format Output as HTML</li> </ul> |

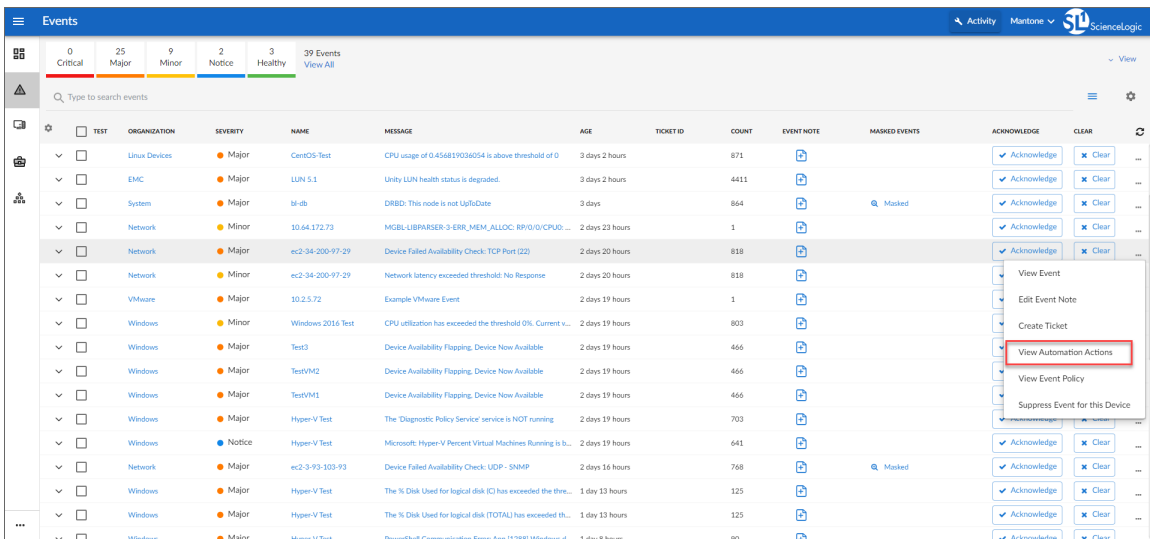
## Running a User Initiated Automation Policy

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



## Viewing Automation Actions for an Event

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



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

Event Actions Log | For Event [3104] Refresh Guide

---

**2020-06-19 20:21:25**  
Automation Policy Network Connectivity: Run NMAP on Common Ports action Datacenter Automation: Format Output as HTML ran Successfully  
Message Snippet (50) executed without incident  
Result: formatted\_output: [Enrichment Command Output](#)

```

Command: nmap -Pn -p 21,22,25,53,80,443,5985,5986 34.200.97.29 Appliance:csc0126
Starting Nmap 6.40 ( http://nmap.org ) at 2020-06-19 20:20 UTC
Nmap scan report for ec2-34-200-97-29.compute-1.amazonaws.com (34.200.97.29)
Host is up.
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    filtered http
443/tcp   filtered https
5985/tcp   filtered wsman
5986/tcp   filtered wsman
Nmap done: 1 IP address (1 host up) scanned in 3.65 seconds

```

---

**2020-06-19 20:21:10**  
Automation Policy Network Connectivity: Run Traceroute (IPv4) action Datacenter Automation: Format Output as HTML ran Successfully  
Message Snippet (50) executed without incident  
Result: formatted\_output: [Enrichment Command Output](#)

```

Command: traceroute 34.200.97.29 Appliance:csc0126
traceroute to 34.200.97.29 (34.200.97.29), 30 hops max, 60 byte packets
 1 10.2.24.5 (10.2.24.5) 0.865 ms 0.840 ms 0.822 ms
 2 10.128.3.9 (10.128.3.9) 1.963 ms 1.996 ms 2.037 ms
 3 efw01.dc2.corp.sciencelogic.com (10.128.1.1) 1.659 ms 1.660 ms *
 4 104.192.252.2 (104.192.252.2) 2.024 ms * *
 5 208.71.164.134 (208.71.164.134) 3.398 ms * *
 6 te-0-12-0-3-pe01.ashburn.va.ibone.comcast.net (66.208.233.253) 2.883 ms 2.116 ms 2.035 ms
 7 75.149.229.2 (75.149.229.2) 1.967 ms 3.858 ms 50.248.117.66 (50.248.117.66) 5.154 ms
 8 52.93.40.49 (52.93.40.49) 19.181 ms 52.93.40.61 (52.93.40.61) 15.047 ms 52.93.40.55 (52.93.40.55) 18.054 ms
 9 52.93.114.37 (52.93.114.37) 3.919 ms 52.93.114.7 (52.93.114.7) 4.483 ms 52.93.114.65 (52.93.114.65) 4.428 ms
10 * * *
11 * * *
12 * * *
13 52.93.28.200 (52.93.28.200) 1.382 ms 52.93.28.234 (52.93.28.234) 1.465 ms 52.93.28.198 (52.93.28.198) 1.499 ms
14 * * *
15 * * *
16 * * *
17 * * *

```

**NOTE:** To learn more about which logs are collected by default for a given automation action, see the [Customizing Network Connectivity Actions](#) section.

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



---

# Appendix

# A



## Run Book Variables

---

### Overview

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

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

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

This appendix covers the following topics:

This chapter covers the following topics:

|                                 |    |
|---------------------------------|----|
| <i>Run Book Variables</i> ..... | 50 |
|---------------------------------|----|

## Run Book Variables

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

- In an action policy of type **Send an Email Notification**, you can include one or more of these variables in the fields **Email Subject** and **Email Body**.
- In an action policy of type **Send an SNMP Trap**, you can include one or more of these variables in the **Trap OID** field, **Varbind OID** field, and the **Varbind Value** field.
- In an action policy of type **Create a New Ticket**, you can include one or more of these variables in the **Description** field or the **Note** field of the related Ticket Template.
- In an action policy of type **Send an SNMP Set**, you can include one or more of these variables in the **SNMP OID** field and the **SNMP Value** field.
- In an action policy of type **Run A Snippet**, you can access variables from the global dictionary **EM7\_VALUES**.
- In a policy of type **Execute an SQL Query**, you can include one or more of these variables in the **SQL Query** field.

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

| Variable        | Source        | Description   |
|-----------------|---------------|---|
| "eye")          |               | from SNMP. For events with a source of "syslog" or "trap", this variable contains the value that matches the <b>Identifier Pattern</b> field in the event definition.   |
| %T              | Dynamic Alert | Value returned by the Threshold function in a Dynamic Application Alert.  |
| %V              | Dynamic Alert | Value returned by the Result function in a Dynamic Application Alert.   |
| %L              | Dynamic Alert | Value returned by the label variable in a Dynamic Application Alert.  |
| %a              | Entity        | IP address  |
| _%category_id   | Entity        | Device category ID associated with the entity in the event.   |
| _%category_name | Entity        | Device category name associated with the entity in the event.   |
| _%class_id      | Entity        | Device class ID associated with the entity in the event.  |
| _%class_name    | Entity        | Device class description associated with the entity in the event.   |
| _%parent_id     | Entity        | For component devices, the device ID of the parent device.  |
| _%parent_name   | Entity        | For component devices, the name of the parent device.   |
| _%root_id       | Entity        | For component devices, the device ID of the root device.  |
| _%root_name     | Entity        | For component devices, the name of the root device.   |
| %1 (one)        | Event         | Entity type. Possible values are: <ul style="list-style-type: none"> <li>• 0. Organization</li> <li>• 1. Device</li> <li>• 2. Asset</li> <li>• 4. IP Network</li> <li>• 5. Interface</li> <li>• 6. Vendor</li> <li>• 7. Account</li> <li>• 8. Virtual Interface</li> <li>• 9. Device Group</li> <li>• 10. IT Service</li> <li>• 11. Ticket</li> </ul> |
| %2              | Event         | Sub-entity type.<br>Possible values for organizations are: <ul style="list-style-type: none"> <li>• 9. News feed</li> </ul> Possible values for devices are: <ul style="list-style-type: none"> <li>• 1. CPU</li> <li>• 2. Disk</li> <li>• 3. File System</li> <li>• 4. Memory</li> <li>• 5. Swap</li> <li>• 6. Component</li> </ul>                  |

| Variable         | Source       | Description   |
|------------------|--------------|---|
|                  |              | <ul style="list-style-type: none"> <li>• 7. Interface</li> <li>• 9. Process</li> <li>• 10. Port</li> <li>• 11. Service</li> <li>• 12. Content</li> <li>• 13. Email</li> </ul>   |
| %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.<br><br><b>NOTE:</b> When referring to an event, %7 represents severity (for previous versions of SL1). When referring to a ticket, %7 represents the subject line of an email used to create a ticket. |
| %c               | Event        | Event counter   |
| %d               | Event        | Date/time when last event occurred.   |
| %D               | Event        | Date/time of first event occurrence.  |
| %e               | Event        | Event ID  |
| %H               | Event        | URL link to event   |
| %M               | Event        | Event message   |
| %s               | Event        | severity (0 - 4). 0=healthy, 1=notify, 2=minor, 3=major, 4=critical.  |
| %S               | Event        | Severity (HEALTHY - CRITICAL)   |
| %_user_note      | Event        | Current note about the event that is displayed on the <b>Events</b> page.   |
| %x               | Event        | Entity ID   |
| %X               | Event        | Entity name   |
| %y               | Event        | Sub-entity ID   |
| %Y               | Event        | Sub-entity name   |
| %Z               | Event        | Event source (Syslog - Group)   |
| %z               | Event        | Event source (1 - 8)  |
| %_ext_ticket_ref | Event        | For events associated with an external Ticket ID, this variable contains the external Ticket ID.  |
| %3               | Event Policy | Event policy ID   |
| %E               | Event Policy | External ID from event policy   |
| %f               | Event Policy | Specifies whether event is stateful, that is, has an associated event that will clear the current event. 1 (one)=stateful; 0 (zero)=not stateful.   |

| Variable             | Source       | Description   |
|----------------------|--------------|---|
| %G                   | Event Policy | External Category   |
| %R                   | Event Policy | Event policy cause/action text  |
| _%_event_policy_name | Event Policy | Name of the event policy that triggered the event.  |
| %B                   | Organization | Organization billing ID   |
| %b                   | Organization | Impacted organization   |
| %C                   | Organization | Organization CRM ID   |
| %o (lowercase "oh")  | Organization | Organization ID   |
| %O (uppercase "oh")  | Organization | Organization name   |
| %r                   | System       | Unique ID / name for the current SL1 system   |
| %7                   | Ticket       | <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><b>NOTE:</b> 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   |
| %J                   | Ticket       | Description field from the SL1 ticket.  |

© 2003 - 2022, ScienceLogic, Inc.

All rights reserved.

#### LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

#### Copyrights and Trademarks

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

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

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

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

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

#### Other

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

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

ScienceLogic

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

International: +1-703-354-1010