VMware Automation PowerPacks

VMware Automation PowerPack version 102

VMware User-Initiated Automation PowerPack version 100

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to use the automation policies, automation actions, and custom action type found in the *VMware Automation* PowerPack

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

- *Datacenter Automation Pack*
- 2020 ScienceLogic Standard solution

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

This chapter covers the following topics:

What is the VMware Automation PowerPack?

The *VMware Automation* PowerPack includes an automation policy that:

- Enriches SL1 events for VMware devices (for example, from the *VMware vSphere Base* PowerPack) by automatically collecting diagnostic logs from the VMware vSphere Web Services API.

> **NOTE:** For information about this API, see the VMware vSphere Web Services API documentation.

- Associates events from the *VMware vSphere Base Pack* PowerPack to automation actions

The *VMware Automation* is executed on the SL1 All-In-One Appliance or Data Collector.

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

- Create your own automation policies that include the pre-defined action
- Use the supplied "Get VMware Diagnostic Logs" custom action type to configure your own automation action by supplying a set of parameters for diagnostic log collection

Installing the VMware Automation PowerPack

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

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

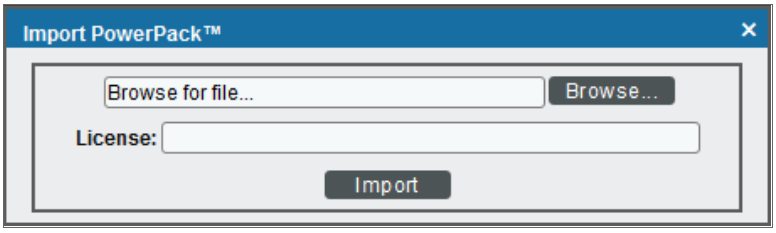
> **WARNING:** You must also install the *Datacenter Automation Utilities* PowerPack, which provides the output formats for the automation actions included in this PowerPack.

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

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site.

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



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

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

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

Chapter 2

VMware Automation Policies

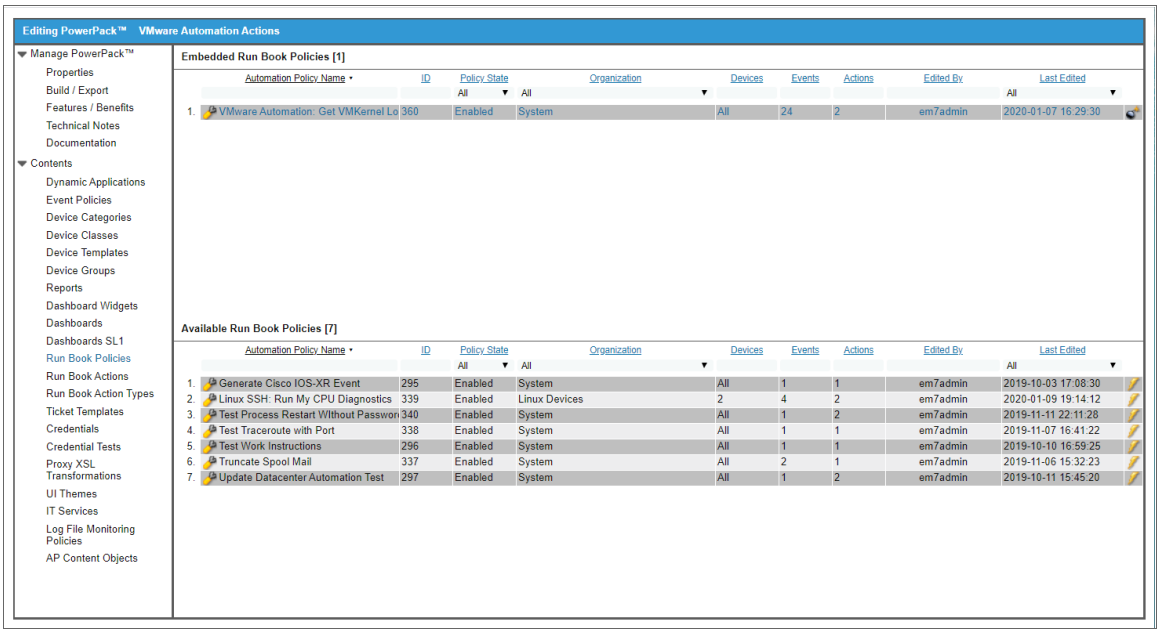
Overview

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

This chapter covers the following topics:

Standard Automation Policies

The *VMware Automation* PowerPack includes a standard automation policy, shown in the following figure. This policy triggers an automation action that collects VMkernel logs and syslog, and an action that formats the output as HTML. All of the automation actions use the same custom action type, "Get VMware Diagnostic Logs", which is supplied in the PowerPack.



All of the standard automation policies are tied to included ScienceLogic SL1 events generated by the Dynamic Applications from the *VMware: vSphere Base Pack* PowerPack.

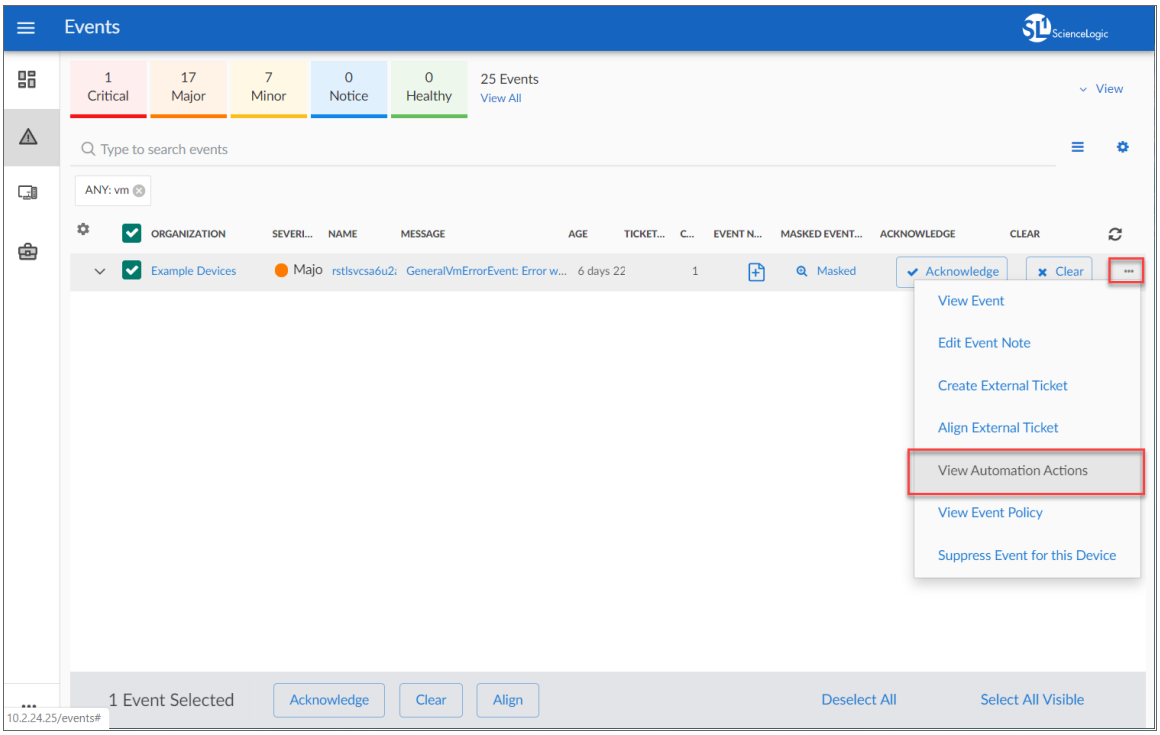
The following table shows the automation policy, its aligned events, and the automation action that runs in response to the events.

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

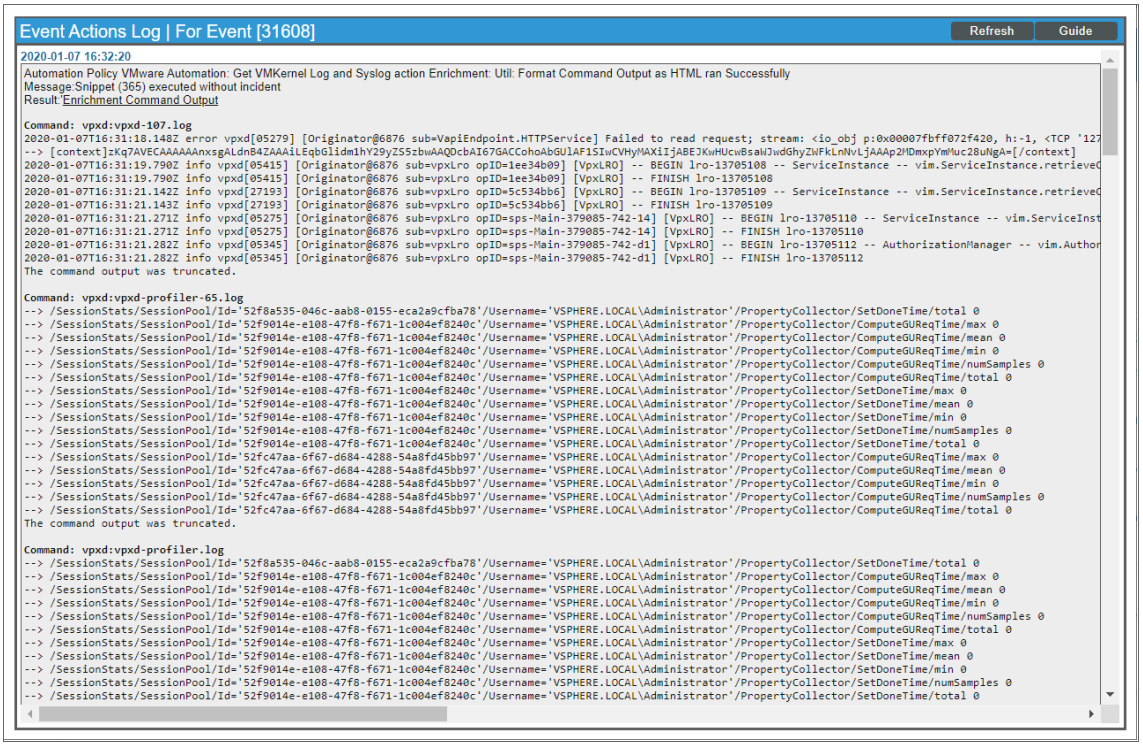
Automation Policy Name	Aligned Events	Automation Action
VMware Automation: Get VMKernel Log and Syslog	• VMware: Datastore Utilization Has Exceeded Threshold • VMware: Host CPU Aggregate Usage Has Exceeded Threshold • VMware: Host CPU Instance Usage Has Exceeded Threshold • VMware: Host Free Memory Has Dropped Below High Threshold • VMware: Host Memory Usage Has Exceeded Threshold	Get VMware Diagnostic Logs

Automation Policy Name	Aligned Events	Automation Action
	• VMware: AlarmEmailFailedEvent • VMware: AlarmScriptFailedEvent • VMware: AlarmSnmpFailedEvent • VMware: AlarmStatusChangedEventRed • VMware: AlarmStatusChangedEventToRed • VMware: com.vmware.vc.HA.DasHostCompleteDatastoreFailureEvent • VMware: com.vmware.vc.HA.DasHostCompleteNetworkFailureEvent • VMware: com.vmware.vc.vcp.VmDatastoreFailedEvent • VMware: com.vmware.vc.vcp.VmNetworkFailedEvent • VMware: esx.problem.apei.bert.memory.error.corrected • VMware: esx.problem.apei.bert.memory.error.fatal • VMware: esx.problem.apei.bert.memory.error.recoverable • VMware: esx.problem.apei.bert.pcie.error.corrected • VMware: esx.problem.apei.bert.pcie.error.fatal • VMware: esx.problem.apei.bert.pcie.error.recoverable • VMware: esx.problem.net.connectivity.lost • VMware: esx.problem.net.dvport.connectivity.lost • VMware: GeneralHostErrorEvent • VMware: GeneralVmErrorEvent	

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 log files collected. The following figure shows an example of this output.



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

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

Chapter 3

Creating and Customizing Automation Policies

Overview

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

This chapter covers the following topics:

Prerequisites

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

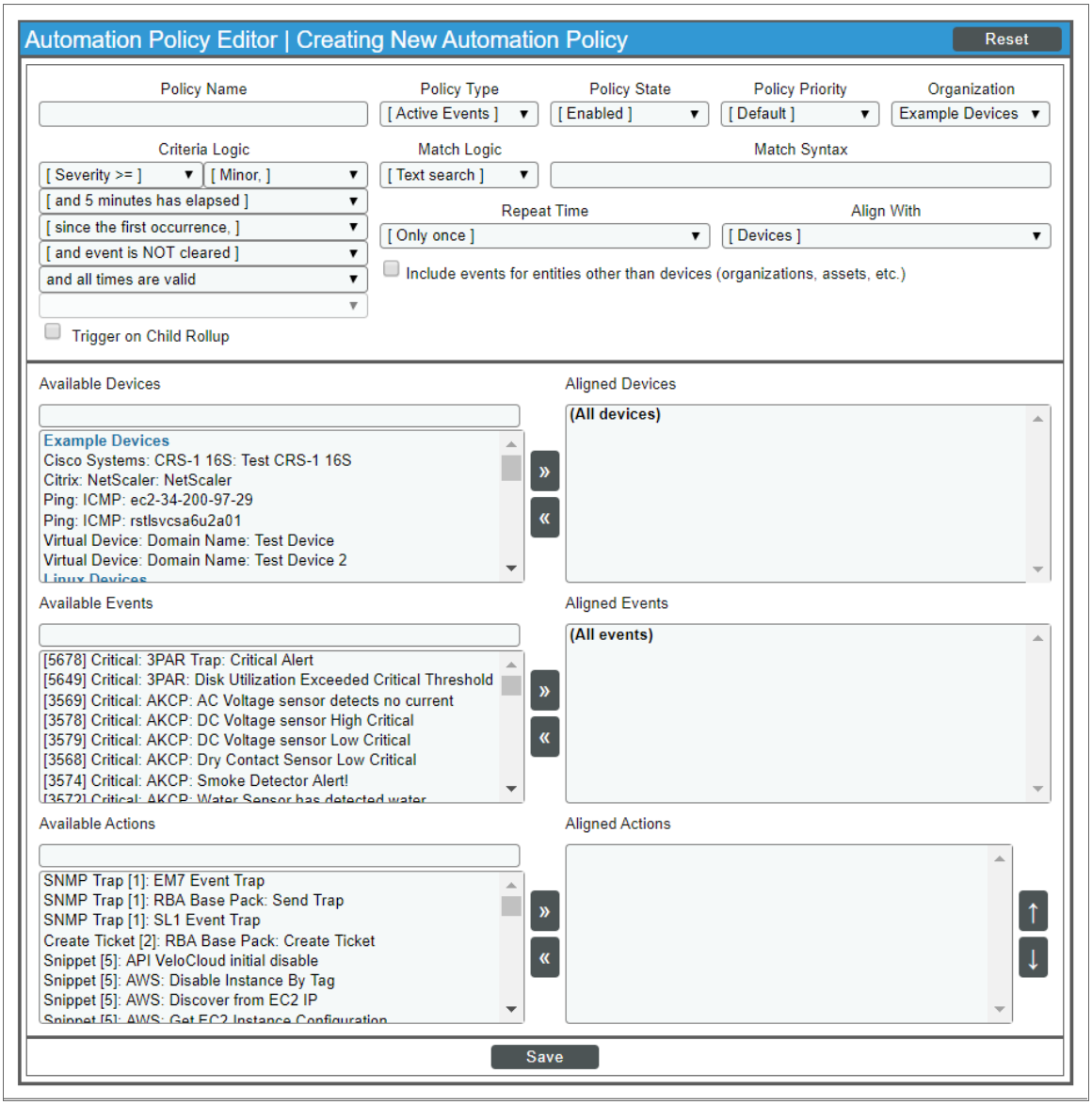
- Which log files you want to collect from vCenter when this action runs. There are two automation actions in the PowerPack that run the "Get VMware Diagnostic Logs" action type with different parameters. You can also create your own automation actions using the custom action type supplied in the PowerPack.
- How many lines of the log file you want returned. The action goes to the end of the log file and returns the last *n* number of lines. 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*VMware Automation* PowerPack, perform the following steps:

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

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



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

- ***Organization***. Select one or more organizations to associate with the automation policy. The automation policy will execute only for devices in the selected organizations (that also match the other criteria in the policy). To configure a policy to execute for all organizations , select *System* without specifying individual devices to align to.
- ***Aligned Action***s. This field includes the actions from the *VMware Automation* PowerPack. To add an action to the ***Aligned Actions*** field, select the action in the ***Available Actions*** field and click the right arrow (>>). To re-order the actions in the ***Aligned Actions*** field, select an action and use the up arrow or down arrow buttons to change that action's position in the sequence.

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

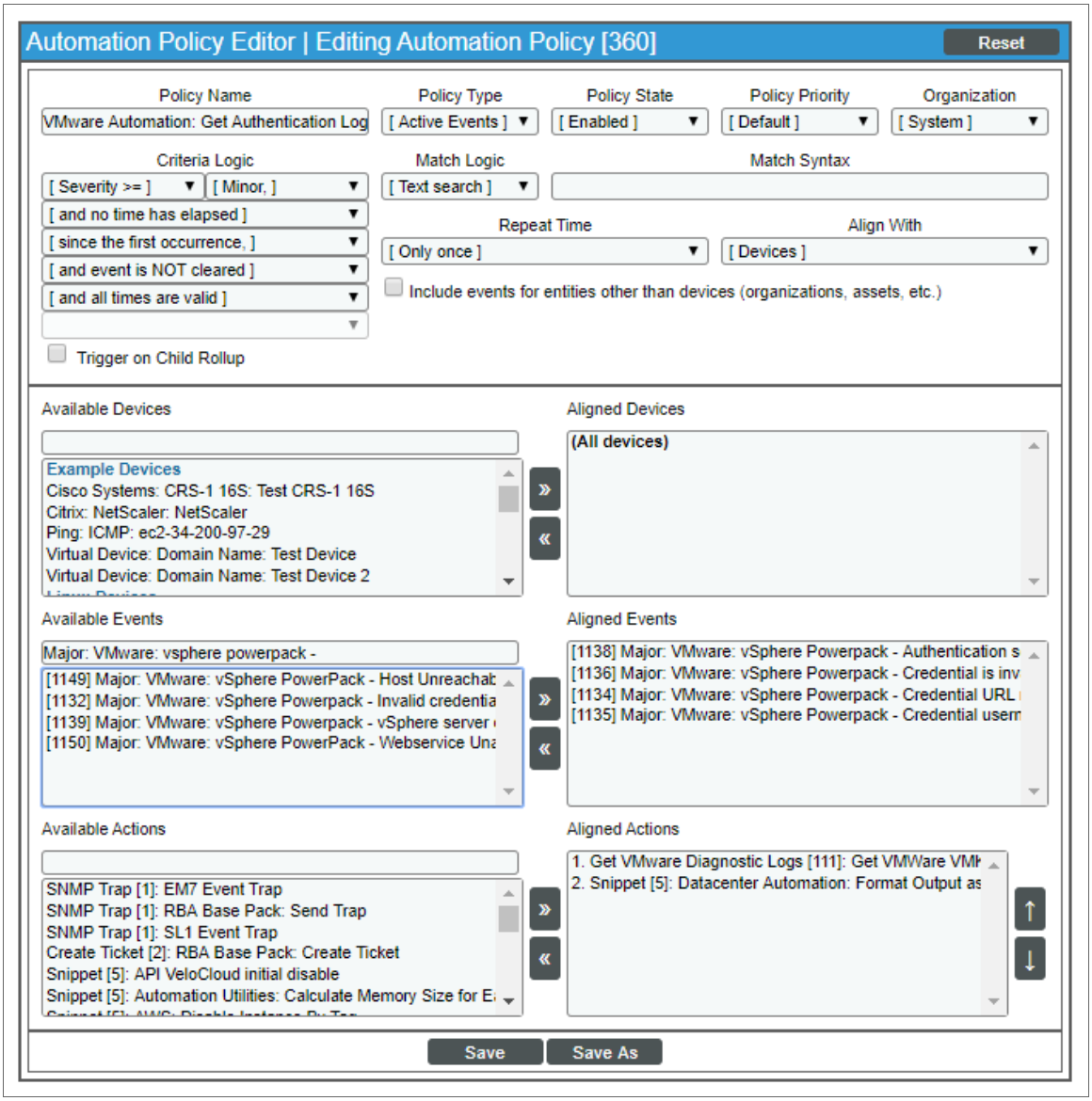
> **NOTE:** If you are selecting multiple collection actions that use the "Get VMware Diagnostic Logs" action type, you may want to include the "Calculate Memory Size for Each Action" automation action, found in the *Datacenter Automation Utilities* PowerPack, in your automation policy.

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

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

Example Automation Configuration

The following is an example of an automation policy that uses a custom automation action we created to retrieve authentication logs in the *VMware Automation* PowerPack:



The policy uses the following settings:

- ***Policy Name***. The policy is named "VMware Automation: Get Authentication Logs".
- ***Policy Type***. The policy runs when an event is in an active state. *Active Events* is selected in this field.
- ***Policy State***. *Enabled* is selected in this field. This policy is active and ready to use.

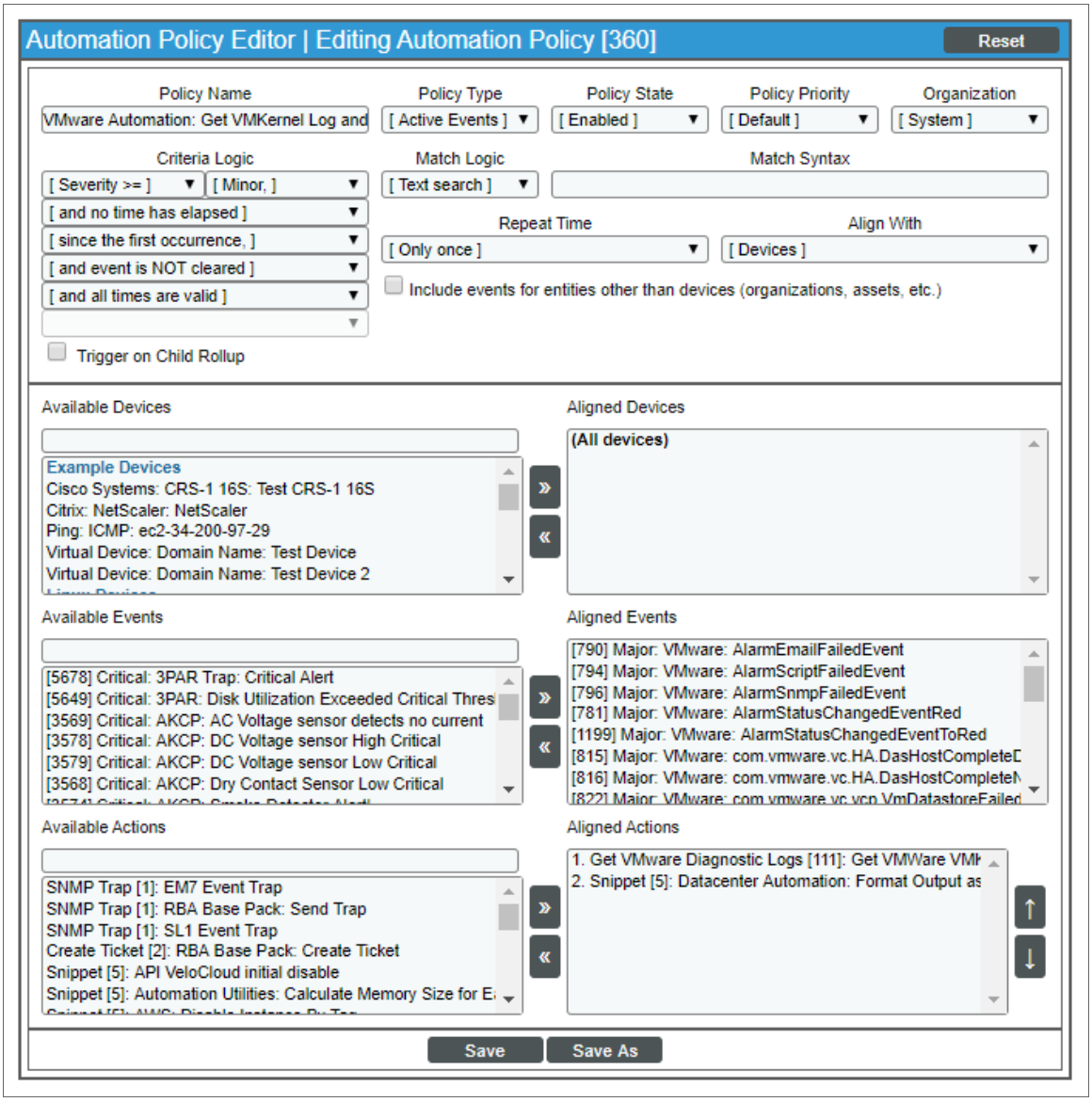
- ***Organization***. The policy executes for the Example Devices organization.
- ***Criteria Logic***. The policy is configured to execute immediately when an event matches these criteria: "Severity >= Notice, and no time has elapsed since the first occurrence, and event is NOT cleared, and all times are valid".
- ***Aligned Devices***. The policy is configured to trigger for any device.
- ***Aligned Events***. The policy is configured to trigger only when selected authentication events are triggered.
- ***Aligned Actions***. The automation includes the following actions. This action allows you to view the output of the diagnostic commands in the Automation Log, accessed through the SL1 **Events** page:
    - Get VMware Diagnostic Logs: Get VMware Authentication Logs
    - Snippet [5]: Enrichment: 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 *VMware 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 *VMware Automation* PowerPack. You should see "Get VMware Diagnostic Logs" action in this field. To add an action to the ***Aligned Actions*** field, select the action in the ***Available Actions*** field and click the right arrow (**>>**). Aligned Actions are run in order starting with the number 1. To re-order the actions in the ***Aligned Actions*** field, select an action and use the up arrow or down arrow buttons to change that action's position in the sequence.

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

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

- ***Organization***. Select the organization that will use this policy.

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

Removing an Automation Policy from a PowerPack

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

To remove content from a PowerPack:

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

Chapter 4

Customizing VMware Automation Actions

Overview

This manual describes how to customize the automation actions included in the VMware Automation PowerPack to create automation actions to meet your organization's specific requirements.

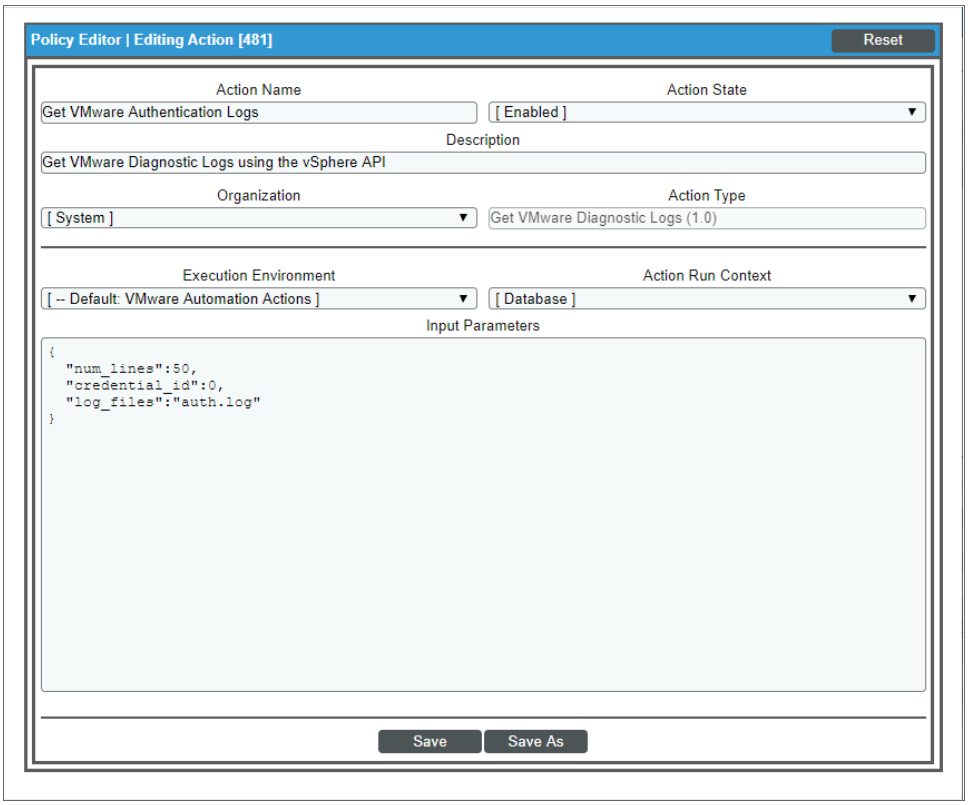
This chapter covers the following topics:

Creating a Custom Action Policy

You can use the "Get VMware Diagnostic Logs" action type included with the VMware Automation PowerPack to create custom automation actions that you can then use to build custom automation policies.

To create a custom action policy using the "Get VMware Diagnostic Logs" action type:

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



4. In the **Action Policy Editor** page, supply a value in each field.
   - ***Action Name***. Specify the name for the action policy.
   - ***Action State***. Specifies whether the policy can be executed by an automation policy (enabled) or cannot be executed (disabled).
   - ***Description***. Allows you to enter a detailed description of the action.
   - ***Organization***. Organization to associate with the action policy.
   - ***Action Type***. Type of action that will be executed. Select the "Get VMware Diagnostic Logs" action type.

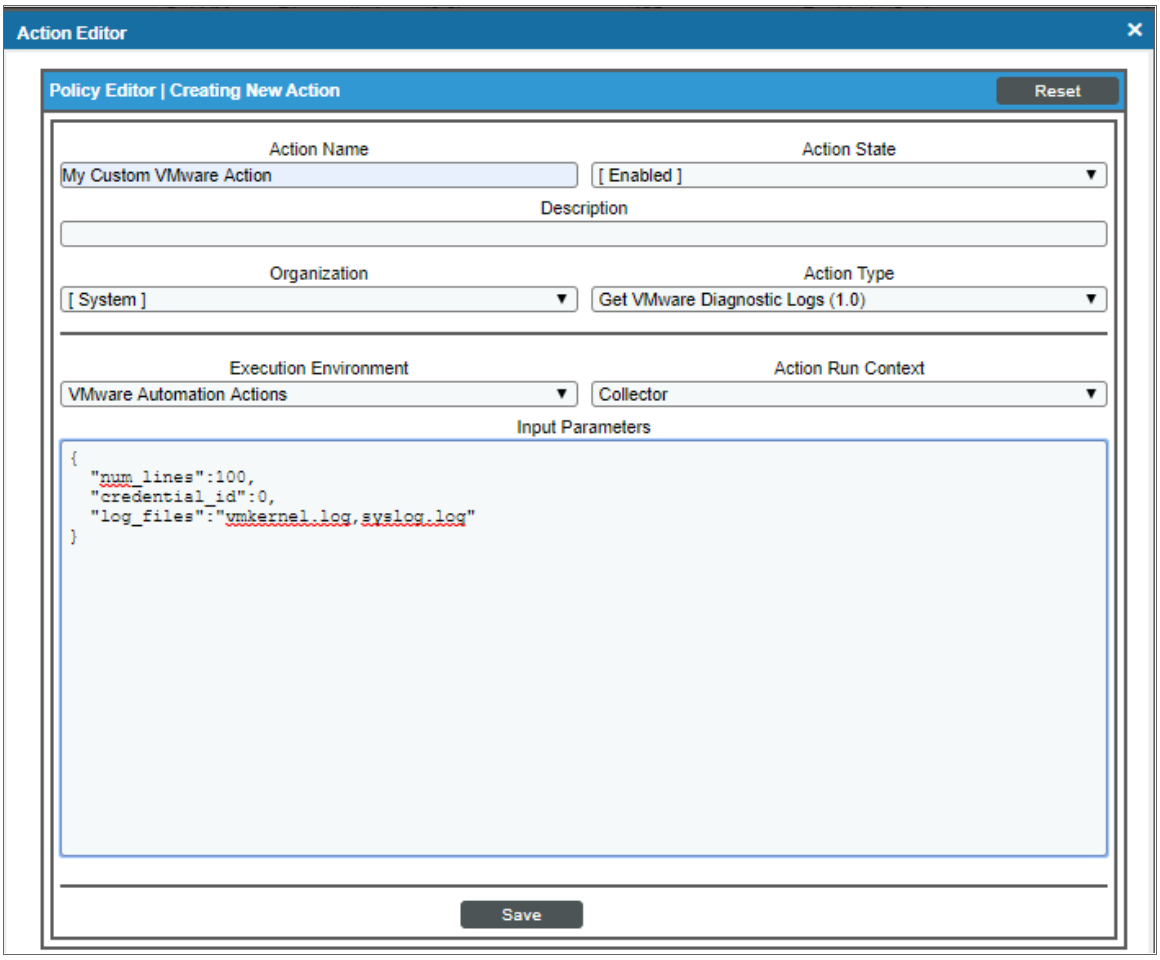
- ***Execution Environment***. Select from the list of available Execution Environments. The default execution environment is *System*.
- ***Action Run Context***. Select *Database* or *Collector* as the context in which the action policy will run.
- ***Input Parameters***. A JSON structure that specifies each input parameter. Each parameter definition includes its name, data type, and whether the input is optional or required for this Custom Action Type. In the example shown above, the automation action policy request the last 50 lines of the authentication log from vCenter.

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

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

Customizing Automation Actions

The *VMware Automation* PowerPack includes two automation actions that use the "Get VMware Diagnostic Logs" action type to request logs through the VMware vSphere Web Services API. 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 "Get VMware Diagnostic Logs" action type are included in the VMware Automation PowerPack. Compare the commands run with the example in the image above.

Action Name	Description	Commands Run
Get VMware VMKernel Log and Syslog	Collects the last 50 lines from the vmkernel.log file and the syslog.log file.	• `num_lines 50` • `log_files vmkernel.log,syslog.log`
Get VMware Diagnostic Logs	Collects all lines in all logs from the vCenter appliance.	• `num_lines {empty}` • `log_files {empty}`

Creating a VMware Automation Action

You can create a new automation action that collects certain logs using the "Get VMware Diagnostic Logs" custom action type. To do this, select "Get VMware Diagnostic Logs" in the Action Type drop-down list when you create a new automation action. You can also use the existing automation actions in the PowerPack as a template by using the **[Save As]** option.

The automation actions accept the following parameters in JSON:

Paramter	Input type	Description
num_lines	integer	Specifies the number of log lines to return.
credential_id	integer	**Default value**: 0 Specifies the credential_id to use for the connection. • If set to 0 (false), the custom action type will dynamically determine the credential by using the credential aligned to the "VMware: Inventory Cache" Dynamic Application on the root device associated with the device triggering the event. • If set to an ID number, it maps to the credential ID specified. You can find credential IDs by going to System > Manage > Credentials.
log_files	string	**Default value**: none Specifies the log files you want to collect.

Chapter 5

VMware Automation User-Initiated Policies

Overview

This manual describes how to use the automation policy found in the *VMware User-Initiated Automation*PowerPack

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

- *Datacenter Automation Pack*
- 2020 ScienceLogic Standard solution

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

This chapter covers the following topics:

What is the VMware User-Initiated Automation PowerPack?

The *VMware User-Initiated Automation* PowerPack includes an automation policy that you can use to collect VMware logs from the SL1 event console on demand, using Event Tools. This PowerPack is supplemental to the *VMware Automation* PowerPack and is not meant for standalone use.

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

Installing the VMware User-Initiated Automation PowerPack

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

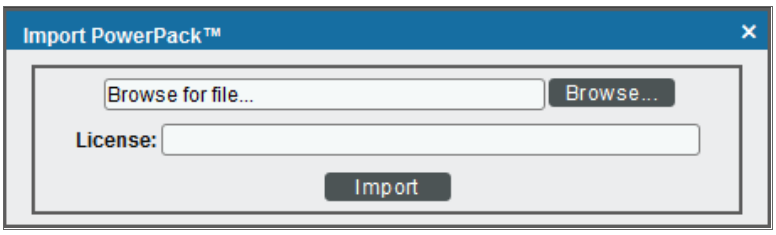
NOTE: The *VMware User-Initiated Automation* PowerPack requires SL1 version 10.1.0 or later. For details on upgrading SL1, see the appropriate SL1 Release Notes.

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

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

To download and install a PowerPack:

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

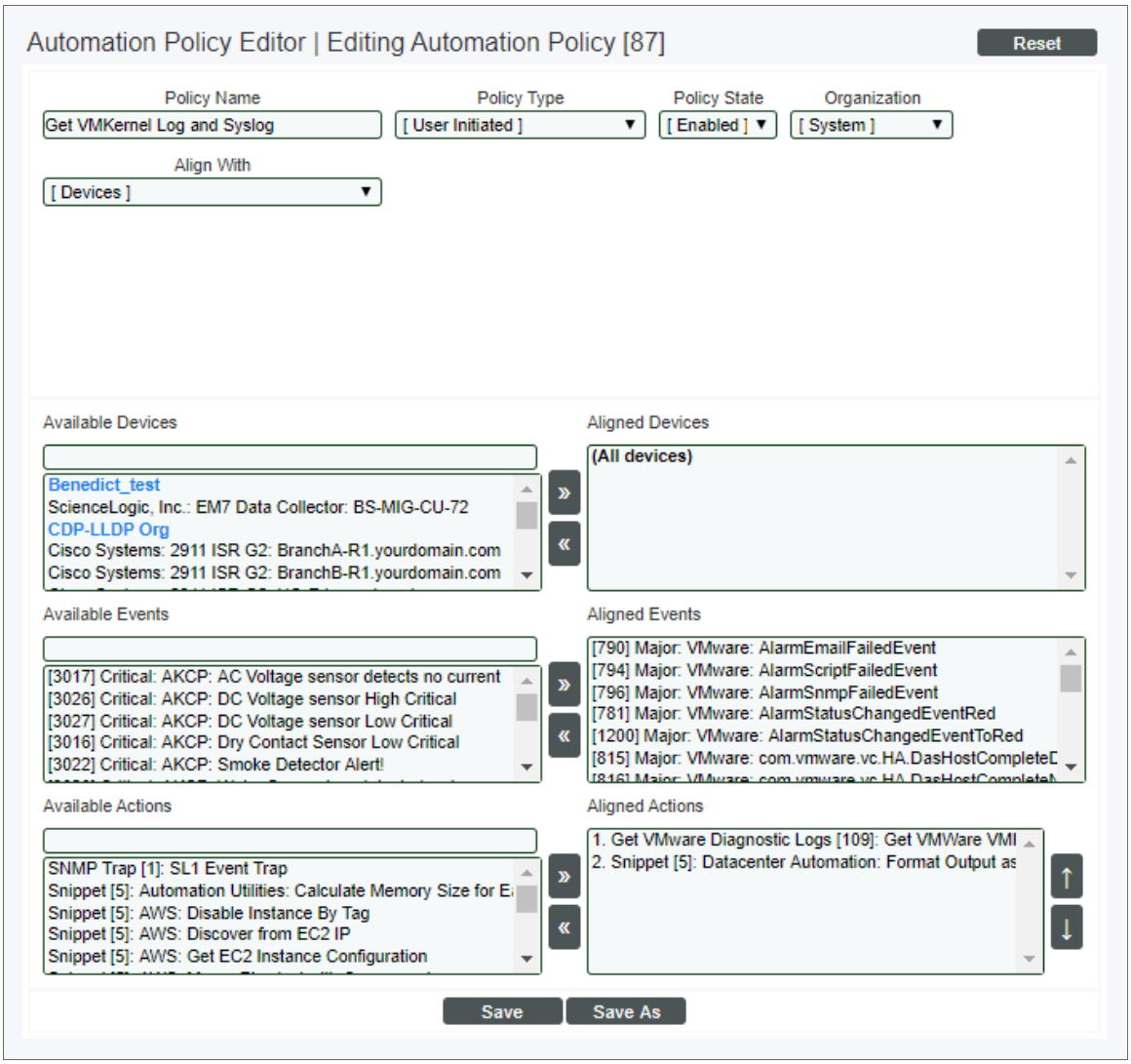


5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal appears, click the **[Install]** button to install the PowerPack.

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

Standard Automation Policy

The *VMware User-Initiated Automation* PowerPack includes a standard automation policy, shown in the following figure. This policy triggers an automation action that collects VMkernel logs and syslog, and an action that formats the output as HTML. The automation action that runs, "Get VMWare VMKernel Log and Syslog", is included in the VMware Automation PowerPack, which must be installed before you can use the policy in this PowerPack.



The standard automation policy available in this release of the PowerPack is tied to included ScienceLogic SL1 events generated by the Dynamic Applications from the *VMware: vSphere Base Pack* PowerPack.

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

For this automation policy 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.

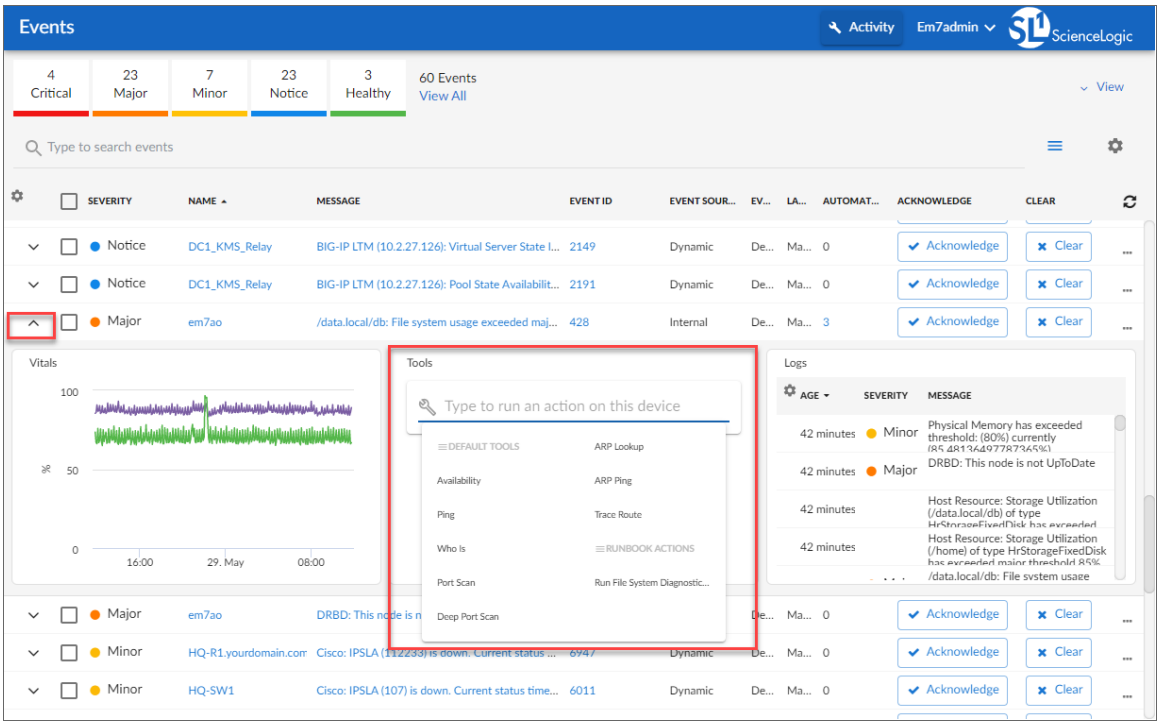
The following table shows the automation policy, its aligned events, and the automation action that runs in response to the events.

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

Automation Policy Name	Aligned Events	Automation Action
Get VMKernel Log and Syslog	• VMware: Datastore Utilization Has Exceeded Threshold • VMware: Host CPU Aggregate Usage Has Exceeded Threshold • VMware: Host CPU Instance Usage Has Exceeded Threshold • VMware: Host Free Memory Has Dropped Below High Threshold • VMware: Host Memory Usage Has Exceeded Threshold • VMware: AlarmEmailFailedEvent • VMware: AlarmScriptFailedEvent • VMware: AlarmSnmpFailedEvent • VMware: AlarmStatusChangedEventRed • VMware: AlarmStatusChangedEventToRed • VMware: com.vmware.vc.HA.DasHostCompleteDatastoreFailureEvent • VMware: com.vmware.vc.HA.DasHostCompleteNetworkFailureEvent • VMware: com.vmware.vc.vcp.VmDatastoreFailedEvent • VMware: com.vmware.vc.vcp.VmNetworkFailedEvent • VMware: esx.problem.apei.bert.memory.error.corrected • VMware: esx.problem.apei.bert.memory.error.fatal • VMware: esx.problem.apei.bert.memory.error.recoverable • VMware: esx.problem.apei.bert.pcie.error.corrected • VMware: esx.problem.apei.bert.pcie.error.fatal • VMware: esx.problem.apei.bert.pcie.error.recoverable • VMware: esx.problem.net.connectivity.lost • VMware: esx.problem.net.dvport.connectivity.lost • VMware: GeneralHostErrorEvent • VMware: GeneralVmErrorEvent	Get VMware Diagnostic Logs

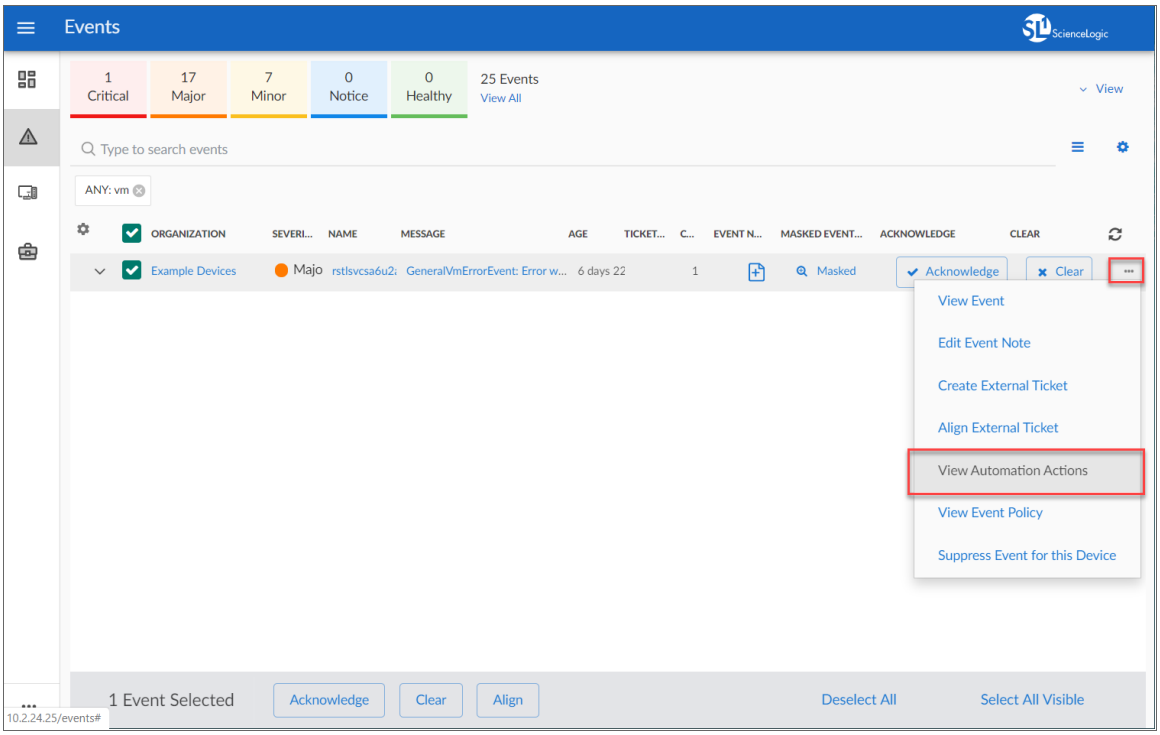
Running a User Initiated Automation Policy

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.

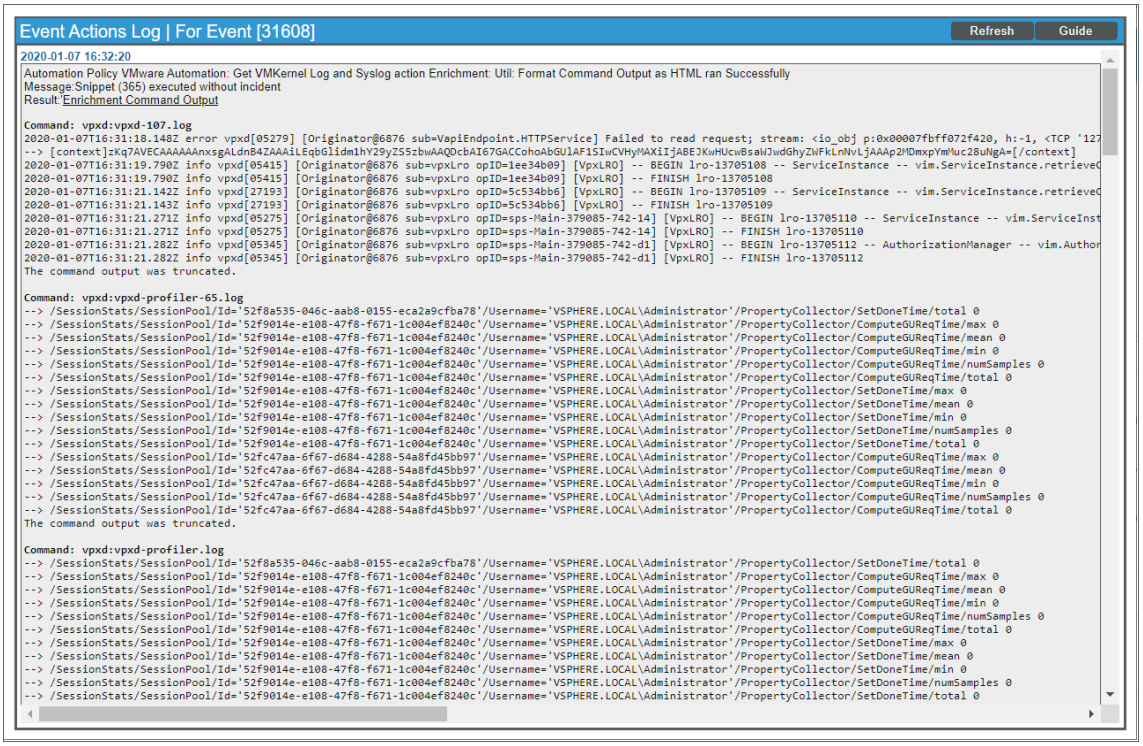


Viewing Automation Actions for an Event

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 log files collected. The following figure shows an example of this output.



NOTE: To learn more about which logs are collected by default for a given automation action, see the *Customizing VMware Automation 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.

Copyrights and Trademarks

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

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

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

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

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

Other

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

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

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

International: +1-703-354-1010