VMware Automation PowerPack

PowerPack version 103

Table of Contents

Chapter 1

Introduction to the VMware Automation PowerPack

Overview PowerPack

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

This PowerPack is intended to be used in conjunction with the "VMware: vSphere Base Pack" PowerPack.

> **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 the following content:

- Run book automation policies that are triggered when events from the "VMware: vSphere Base Pack" PowerPack occur:
    - **VMware Automation: Get vCenter Service Logs**(SOL-29765)
    - **VMware Automation: Get VMKernel Log and Syslog**(VA-11)
    - **VMware Automation: Get VMware hostd and vCenter Agent ESXi Logs**(SOL-29765)
- Run book actions that you can configure to collect additional diagnostic information when events occur:
    - **Get All Available VMware Diagnostic Logs**. This action attempts to retrieve the last 10 lines of data from all available log files on the target device (vCenter root device).(VA-8)
    - **Get vCenter Service Logs**. This action attempts to retrieve the last 50 lines from the **vpxd.log** file. (SOL-29765)
    - **Get VMware hostd and vCenter Agent ESXi Logs**. This action attempts to retrieve the last 50 lines from the **hostd.log** file and **vpxa.log** file. (SOL-29765)
    - **Get VMware VMKernel Log and Syslog**. This action attempts to retrieve the last 50 lines of data from the **vmkernel.log** and **syslog.log** log files on the target device (vCenter root device). (VA-10)
- A custom action type that you can use to create new run book actions:
    - **Get VMware Diagnostic Logs**(VA-1)

The "VMware Automation" run book actions are executed on the SL1 All-In-One Appliance or Data Collector.

In addition to using the standard content, you can use the content in the "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 run book action by supplying a set of parameters for diagnostic log collection.

The automation policies in this PowerPack can also be used as "User-Inititated" automations.

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.

WARNING: You must also install version 201 of the "Datacenter Automation Utilities" PowerPack, which provides the output formats for the run book 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 section on *Global Settings*.

IMPORTANT: Ensure that you are running version 12.1.2 or later of SL1 before installing this PowerPack. For details on upgrading SL1, see the relevant *SL1 Platform Release Notes*.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the ScienceLogic Support Site.
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** 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 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

Configuring VMware Automations

Overview

This chapter describes how to use the run book automation policies found in the "VMware Automation" PowerPack.

This chapter covers the following topics:

VMware Automation Policies

The "VMware Automation" PowerPack includes the following automation policies:

- VMware Automation: Get vCenter Service Logs
- VMware Automation: Get VMKernel Log and Syslog
- VMware Automation: Get VMware hostd and vCenter Agent ESXi Logs

These automation policies are tied to included ScienceLogic SL1 events generated by the Dynamic Applications from the "VMware: vSphere Base Pack" PowerPack.

The automation policies have a ***Policy Type*** of *Active Events/User Initiated*, which enables all of the features of the "Active Events" and the "User Initiated" policy types. As a result, this automation policy can be triggered by active events that meet the criteria in the policy, or you can manually trigger the automation.

You can run this automation policy as needed from the **Devices** page, the **Events** page, and the **Service Investigator** page. If there is an event policy specified in the automation policy, that event must be active for the policy to be run manually, and the policy can only be run on that event type. The same applies for the device groups list.

The automation policies trigger one of the following run book actions:

- Get All Available VMware Diagnostic Logs
- Get vCenter Service Logs
- Get VMware hostd and vCenter Agent ESXi Logs
- Get VMWare VMKernel Log and Syslog

These run book actions collect logs and syslog files, along with a "Datacenter Automation" run book action that formats the output as HTML.

All of the run book actions use the "Get VMware Diagnostic Logs" run book action type, which is also supplied in the PowerPack.

NOTE: The "Get All Available VMware Diagnostic Logs" run book action is not aligned to any of the automation policies in this PowerPack by default. As a result, you will need to add this action to a policy, and the action will retrieve data from all available log files on the target device.

NOTE: If the log files specified in a run book action are not present on the target vCenter or standalone ESXi host device, the automation policies will output an empty response instead of actual log data.

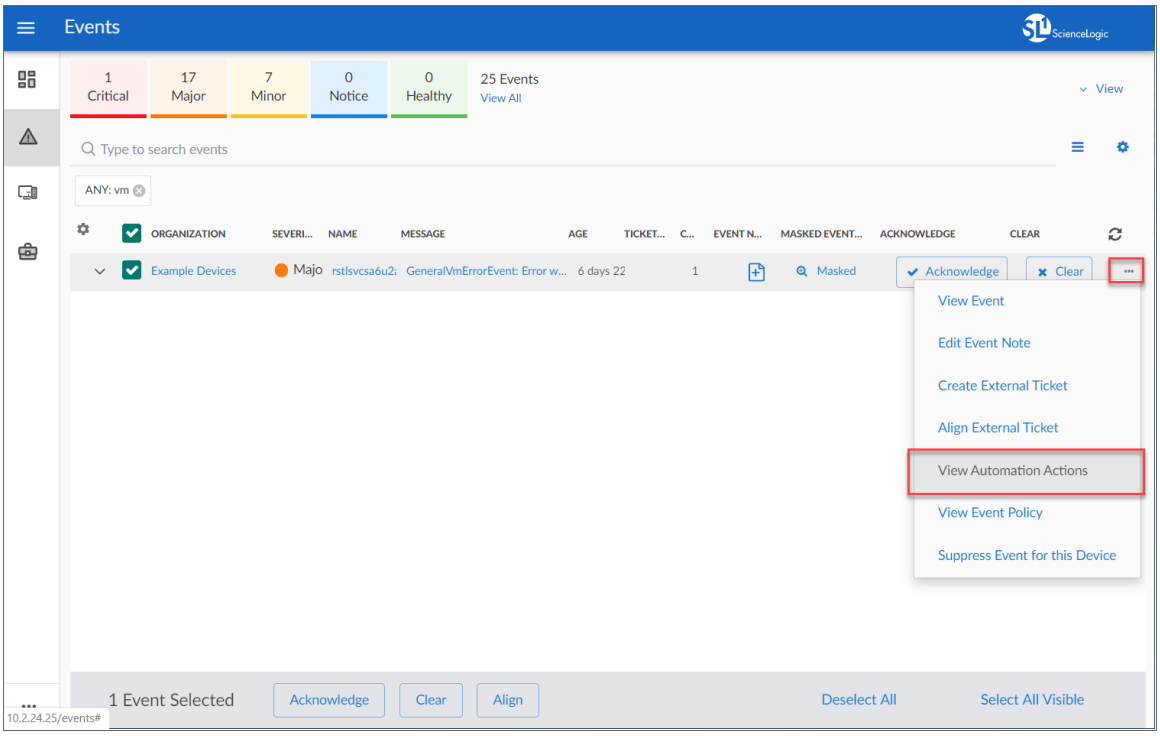
The following table shows the automation policy, its aligned events, and the run book actions that run in response to the events.

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.

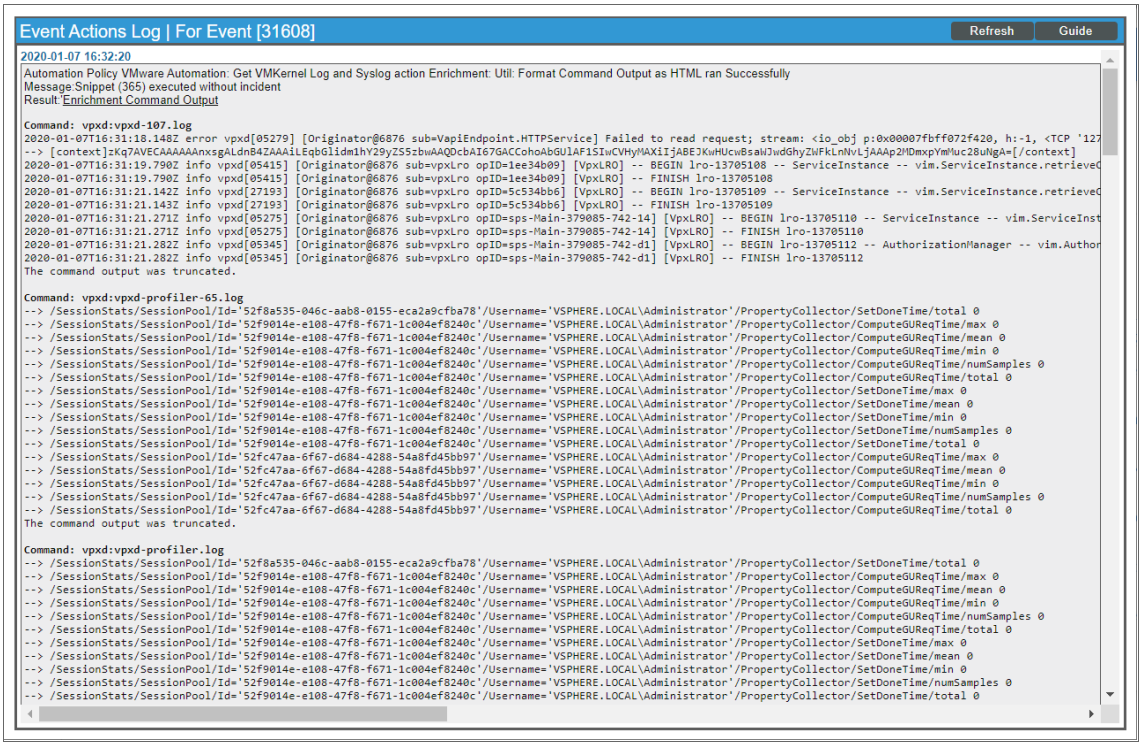
Automation Policy	Aligned Events	Run Book Action
VMware Automation: Get vCenter Service Logs	• VMware: AlarmEmailFailedEvent • VMware: AlarmScriptFailedEvent • VMware: AlarmSnmpFailedEvent • VMware: AlarmStatusChangedEventRed • VMware: AlarmStatusChangedEventToRed • VMware: com.vmware.vc.HA.DasHostCompleteDatastoreFailureEvent • VMware: com.vmware.vc.HA.DasHostCompleteNetworkFailureEvent • VMware: com.vmware.vc.vcp.VmDatastoreFailedEvent • VMware: com.vmware.vc.vcp.VmNetworkFailedEvent • VMware: Datastore Utilization Has Exceeded Threshold • 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 • 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 vCenter Service Logs • Datacenter Automation: Format Output as HTML
VMware Automation: Get VMKernel Log and Syslog	Same list of events as above.	• Get VMWare VMKernel Log and Syslog • Datacenter Automation: Format Output as HTML

Automation Policy	Aligned Events	Run Book Action
VMware Automation: Get VMware hostd and vCenter Agent ESXi Logs	Same list of events as above.	• Get VMware hostd and vCenter Agent ESXi Logs • Datacenter Automation: Format Output as HTML

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 run book 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.



To learn more about which logs are collected by default for a given run book action, see *Configuring VMware Run Book 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.

Creating and Customizing Automation Policies

You can use the default run book automation policies in this PowerPack, or you can create and customize the policies as needed.

TIP: You might need to configure a run book action policy before you can add it to the automation policy. For more information, see *Configuring VMware Run Book Actions*.

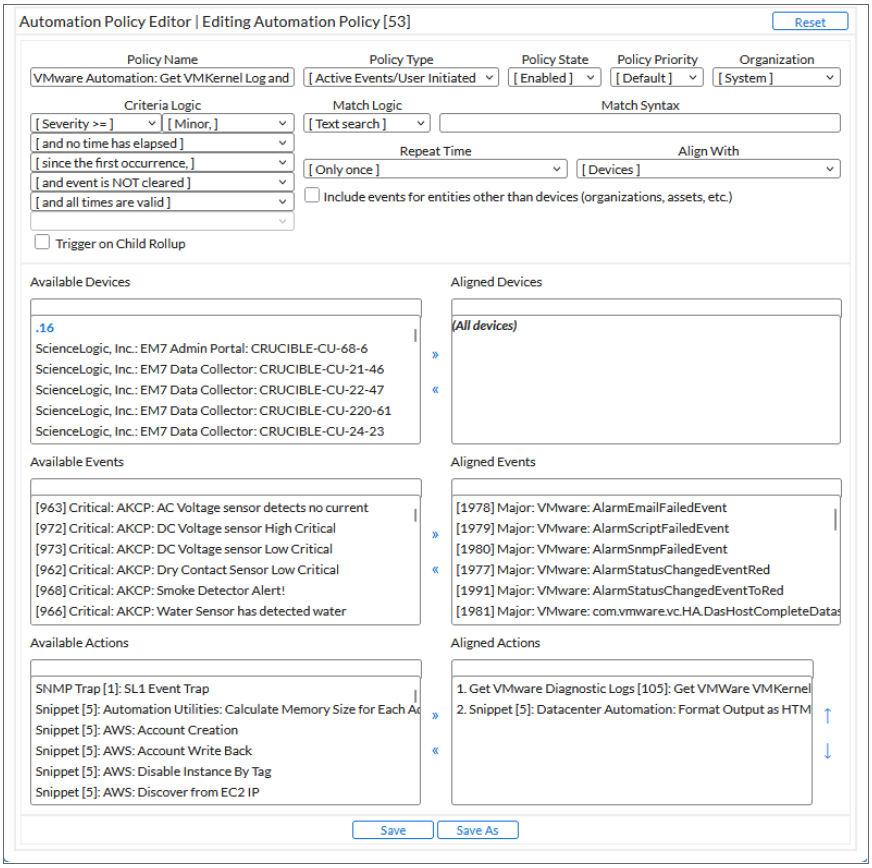
Before you create an automation policy using the run book actions in this PowerPack, you must determine:

- Which log files you want to collect from vCenter when this action runs. The run book actions in the PowerPack run the "Get VMware Diagnostic Logs" action type with different parameters. You can also create your own run book 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.

To create an automation policy that uses the run book actions in this PowerPack:

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).
2. Click the **[Create]** button to create an automation policy, or search for an existing automation policy that you want to edit and click the wrench icon (🔧) for that policy. 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* or *Active Events/User Inititiated* 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 run book 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.

4. Optionally, supply values in the other fields on this page to refine when the automation will trigger.
5. Click **[Save]** or click **[Save As]** if you are customizing an existing policy. If you modify one of the included automation policies and save it with the original name, any customizations you made to that policy will be overwritten when you upgrade the PowerPack.

> **NOTE:** If the log files specified in a run book action are not present on the target vCenter or standalone ESXi host device, the automation policies will output an empty response instead of actual log data.

Removing an Automation Policy from a PowerPack

If you have customized a policy from the "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 3

Configuring VMware Run Book Actions

Overview

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

This chapter covers the following topics:

VMware Run Book Actions

The "VMware Automation" PowerPack includes the following run book actions, all of which use the "Get VMware Diagnostic Logs" action type to request logs through the VMware vSphere Web Services API:

- Get All Available VMware Diagnostic Logs
- Get vCenter Service Logs
- Get VMware hostd and vCenter Agent ESXi Logs
- Get VMWare VMKernel Log and Syslog

Each run book action has the following parameters in the ***Input Parameters*** field in the **Action Policy Editor** modal:

- `num_lines`. Specifies the number of log lines to retrieve from the logs. The combined total of log lines across all log files in one action is limited to 120 lines before the response output begins to be truncated. As a result, if you use the `log_files` parameter to specify multiple log files in one action and you try to get more lines from each than is supported, you might see the outputs for each log file get truncated. If you need more lines from a specific log file, you can create a new run book action that specifies only that log file to get the maximum 120 log lines.
- `credential_id`. Lets you align a specific SOAP/XML credential or Universal Credential on the SL1 stack with this run book action. You can find the credential ID on the **Credentials** page (Manage > Credentials), in the **ID** column. The default value of this field is 0. If you want the action to get credential information from the "VMware: Inventory Cache" Dynamic Application aligned to the device, leave the value as 0.
- `log_files`. Specifies the log files you want to collect.

The following run book 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. For more information about input parameter fields, see the table in *Creating a VMware Run Book Action*.

Run Book Action	Description	Parameters
Get All Available VMware Diagnostic Logs	Collects all lines in all logs from the vCenter device. If you run this action used with the `log_files` parameter set to `"log_files":""` (no log files specified), the action will try to capture all the log files that are available on the device.	• `"num_lines":10` • `"credential_id":0` • `"log_files":""`
Get vCenter Service Logs	Collects the last 50 lines from the **vpxd.log** file.	• `"num_lines":50` • `"credential_id":0` • `"log_files":"vpxd.log"`
Get VMware hostd and vCenter Agent ESXi Logs	Collects the last 50 lines from the **hostd.log** file and **vpxa.log** file.	• `"num_lines":50` • `"credential_id":0` • `"log_files":"hostd.log,vpxa.log"`

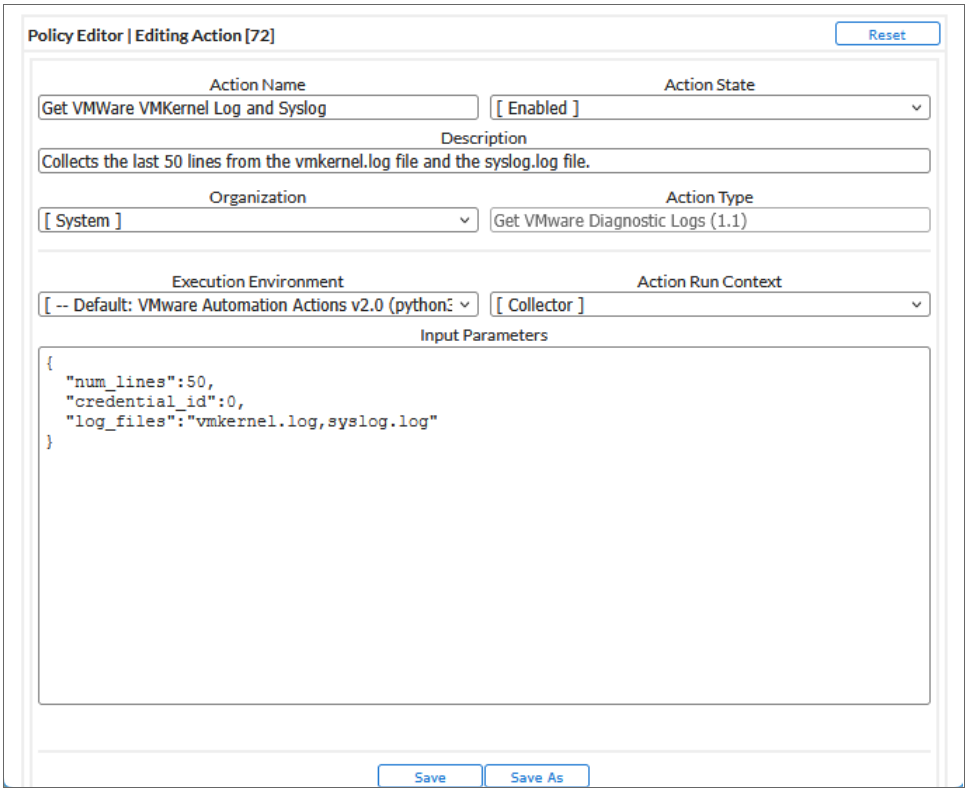
Run Book Action	Description	Parameters
Get VMware VMKernel Log and Syslog	Collects the last 50 lines from the **vmkernel.log** file and the **syslog.log** file.	• `"num_lines":50` • `"credential_id":0` • `"log_files":"vmkernel.log,syslog.log"`

Creating a VMware Run Book Action

You can create a new run book action that collects certain logs using the "Get VMware Diagnostic Logs" custom action type. You can also use one of the existing run book actions in the PowerPack as a template by using the **[Save As]** option.

To create a custom run book action 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. The **Action Policy Editor** modal appears:



3. 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 run book action policy request the last 50 lines of the logs from vCenter. Input parameters must be defined as a JSON structure, even if only one parameter is defined.

  The run book actions accept the following parameters in JSON:

Parameter	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.

4. Click **[Save]**, or 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.

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. For more information, see https://sciencelogic.com/company/legal.

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

International: +1-703-354-1010