

VMware Automation PowerPacks

VMware Automation PowerPack version 102

VMware User-Initiated Automation PowerPack version 100

Table of Contents

Introduction	3
What is the VMware Automation PowerPack?	4
Installing the VMware Automation PowerPack	4
VMware Automation Policies	6
Standard Automation Policies	7
Creating and Customizing Automation Policies	11
Prerequisites	12
Creating an Automation Policy	12
Example Automation Configuration	15
Customizing an Automation Policy	16
Removing an Automation Policy from a PowerPack	18
Customizing VMware Automation Actions	19
Creating a Custom Action Policy	20
Customizing Automation Actions	21
Creating a VMware Automation Action	
VMware Automation User-Initiated Policies	24
What is the VMware User-Initiated Automation PowerPack?	25
Installing the VMware User-Initiated Automation PowerPack	25
Standard Automation Policy	
Running a User Initiated Automation Policy	
Viewing Automation Actions for an Event	29

Chapter

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?	4
Installing the VMware Automation PowerPack	4

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 AutomationPowerPack.

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

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

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

To download and install a PowerPack:

1. Download the PowerPack from the <u>ScienceLogic Support Site</u>.

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

Import PowerPack™			×
Browse for file	Import	Browse	

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

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

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 Policie	s	7
-----------------------------	---	---

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.

 Manage PowerPack — 	Embedded Run Book Policies [1]								
Properties	Automation Policy Name •	<u>ID</u>	Policy State	Organization	Devices	Events	Actions	Edited By	Last Edited
Build / Export			All 🔻	All	•				All 🔻
Features / Benefits	1. 🤌 VMware Automation: Get VMKernel	Lo 360	Enabled	System	All	24	2	em7admin	2020-01-07 16:29:30
Technical Notes									
Documentation									
 Contents 									
Dynamic Applications									
Event Policies									
Device Categories									
Device Classes									
Device Templates									
Device Groups									
Reports									
Dashboard Widgets									
Dashboards	Available Run Book Policies [7]								
Dashboards SL1	Automotion Deliny Name -	ID	Delin: Olela	Ormanization	Deviews	Fuenda	Antione	Edited Do	Lest Edited
Run Book Policies	Automation Policy Name *	iD				Evenus	ACIONS	Edited by	
Run Book Actions	1 Generate Cisco IOS-XR Event	295	Enabled	System	ΔII	1	1	em7admin	2019-10-03 17:08:30
Run Book Action Types	2. A Linux SSH: Run My CPU Diagnostic	s 339	Enabled	Linux Devices	2	4	2	em7admin	2020-01-09 19:14:12
Ticket Templates	3. A Test Process Restart Without Passw	or 340	Enabled	System	All	1	2	em7admin	2019-11-11 22:11:28
	4. 🤌 Test Traceroute with Port	338	Enabled	System	All	1	1	em7admin	2019-11-07 16:41:22
Credentials		296	Enabled	System	All	1	1	em7admin	2019-10-10 16:59:25
Credentials Credential Tests	5. 🥜 Test Work Instructions		Conclute of	System	All	2	1	em7admin	2019-11-06 15:32:23
Credentials Credential Tests Proxy XSL	 Fest Work Instructions Fruncate Spool Mail 	337	Enabled	-/					2010 10 11 15 45 20
Credentials Credential Tests Proxy XSL Transformations	 Fest Work Instructions Fruncate Spool Mail JUpdate Datacenter Automation Test 	337 297	Enabled	System	All	1	2	em/admin	2010-10-11 10:40.20
Credentials Credential Tests Proxy XSL Transformations UI Themes	5. JP Test Work Instructions 6. JP Truncate Spool Mail 7. JP Update Datacenter Automation Test	337 297	Enabled	System	All	1	2	em/admin	2013-10-11 13:43:20
Credentials Credential Tests Proxy XSL Transformations UI Themes IT Services	 Pest Work Instructions Particular Spool Mail Pupdate Datacenter Automation Test 	337 297	Enabled	System	All	1	2	em/admin	2010-10-11 13.43.20
Credentials Credential Tests Proxy XSL Transformations UI Themes IT Services Log File Monitoring Policies		337 297	Enabled	System	All	1	2	em/admin	2010-10-11 10:40:20
Credentials Credential Tests Proxy XSL Transformations UI Themes IT Services Log File Monitoring Policies AP Content Objects	5 J Test Work Instructions J Transie Spool Mail 7 J Update Datacenter Automation Test	337 297	Enabled	System	All	1	2	em/admin	2013-10-11 12:40:20

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

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.

≡	Events					Stincetoge	:
88	1 Critical	17 Major	7 Minor	0 Notice	0 Healthy	25 Events View All	ew
	Q Type to	search events				=	•
	ANY: vm 🕲						
æ	۵ 🔽	ORGANIZATION	SEVERI	NAME	MESSAGE	AGE TICKET C EVENT N MASKED EVENT ACKNOWLEDGE CLEAR	C
	~ 🗹	Example Device	s 🥚 Maj	o rstlsvcsa6u2	2: GeneralVmE	mErrorEvent: Error w 6 days 22 1 🕑 Q Masked 🗸 Acknowledge 🗴 Clear	
						View Event	
						Create External Ticket	
						Align External Ticket	
						View Automation Actions	
						View Event Policy	
						Suppress Event for this Device	e
							_
10.2.24.25	1 Eve /events#	ent Selected	Ack	nowledge	Clear	Align Deselect All Select All Visible	

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.

Event Actions Log For Event [31608]	
2020-01-07 16:32:20	
Automation Policy Wiware Automation: Get VMKernel Log and Syslog action Enrichment: Util: Format Command Output as HTML ran Successfully Message Snippet (355) executed without incident Result: <u>Enrichment Command Output</u>	Ī
Command: vpxd:vpxd-107.log 2020-01-0716:31:18.1482 error vpxd[05279] [Originator@6876 sub=VapiEndpoint.HTTPService] Failed to read request; stream: <io_obj '12<br="" <tcp="" h:-1,="" p:0x000007bff072f420,="">-> [context]stq7AVECAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</io_obj>	27 ≥C st pr
Command: vpxd:vpxd-profiler-65.log > /SessionStats/SessionPool/Id='52f9014-e-08-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/CemputeGUReqTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014-e-018-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/CemputeGUReqTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014-e-018-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/CemputeGUReqTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014-e-018-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/CemputeGUReqTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014-e-018-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/CemputeGUReqTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014-e-018-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014-e-018-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014-e-018-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014-e-018-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014-e-018-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014-e-018-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 ->> /SessionStats/SessionPool/Id='52f047aa-6f67-6684-4288-5486fd5b97'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/CemputeGUReqTime/max 0 ->> /SessionStats/SessionPool/Id='52fc47aa-6f67-6684-4288-5486fd5b97'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeGUReqTime/max 0 ->> /SessionStats/SessionPool/Id='52fc47aa-6f67-6684-428	
Command: vpxd:vpxd-profiler.log > /SessionStats/SessionPool/Id='52f8014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/total 0 > /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeGUReqTime/max 0 > /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeGUReqTime/max 0 > /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeGUReqTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeGUReqTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 ->> /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/min 0 ->> /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/min 0 ->> /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/min 0 ->> /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/min 0 ->> /SessionStats/SessionPool/Id='52f9014e-e108-47f8-f671-1c004ef82	•
	1

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



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

Prerequisites

Before you create an automation policy using the automation actions in the 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).

Policy Name	Policy Type	Policy State	_	Policy Priority	Organizati	on
	[Active Events]	[Enabled]	•	[Default]	Example Device	ces 1
Criteria Logic	Match Logic			Match Syntax		
[Severity >=] ▼ [Minor,] ▼	[Text search] 🔹					
[and 5 minutes has elapsed]	Banar	at Time		Δ	lian With	
[since the first occurrence,]		at time	•	[Devices]	ign with	
[and event is NOT cleared]			•	[Devices]		
and all times are valid 🔹 🔻	Include events for e	ntities other than de	vices (organizations, assets	i, etc.)	
Trigger on Child Rollup						
Available Devices		Aligned Devices				
		(All devices)				
Cisco Systems: CRS-1 16S: Test CRS-1 16S Citrix: NetScaler: NetScaler Ping: ICMP: ec2-34-200-97-29 Ping: ICMP: rstlsvcsa6u2a01 Virtual Device: Domain Name: Test Device Virtual Device: Domain Name: Test Device 2 Linux Devices	Ţ	» «				
Available Events		Aligned Events				
[5678] Critical: 3PAR Trap: Critical Alert [5649] Critical: 3PAR: Disk Utilization Exceeded [3569] Critical: AKCP: AC Voltage sensor detec [3578] Critical: AKCP: DC Voltage sensor High ([3579] Critical: AKCP: DC Voltage sensor Low ([3578] Critical: AKCP: Dry Contact Sensor Low [3574] Critical: AKCP: Smoke Detector Alert! [3572] Critical: AKCP: Water Sensor Los detect	Critical Threshold ts no current Critical Critical Critical Critical	(All events)				
Available Actions		Aligned Actions				
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 Ticke Snippet [5]: API VeloCloud initial disable Snippet [5]: AWS: Disable Instance By Tag	ıt	» «				1

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 Actions. 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:

Automation Policy Editor Editin	g Automation F	Policy [360]		Reset
Policy Name VMware Automation: Get Authentication Log Criteria Logic [Severity >=] V [Minor,] V [and no time has elapsed] V [since the first occurrence,] V [and event is NOT cleared] V [and all times are valid] V Trigger on Child Rollup	Policy Type [Active Events] Match Logic [Text search] Repe [Only once] Include events for	Policy State [Enabled] at Time entities other than	Policy Priority	Organization ▼ [System] ▼ lign With sssets, etc.)
Available Devices Example Devices Cisco Systems: CRS-1 16S: Test CRS-1 16S Citrix: NetScaler: NetScaler		Aligned Device (All devices)	s	*
Ping: ICMP: ec2-34-200-97-29 Virtual Device: Domain Name: Test Device Virtual Device: Domain Name: Test Device 2		« Aligned Events		~
Major: VMware: vsphere powerpack - [1149] Major: VMware: vSphere PowerPack - [1132] Major: VMware: vSphere Powerpack - [1139] Major: VMware: vSphere PowerPack - [1150] Major: VMware: vSphere PowerPack -	Host Unreachat Invalid credentia vSphere server Webservice Una	[1138] Major: \ [1136] Major: \ [1134] Major: \ [1135] Major: \ «	/Mware: vSphere Powerp /Mware: vSphere Powerp /Mware: vSphere Powerp /Mware: vSphere Powerp	oack - Authentication s oack - Credential is inv oack - Credential URL oack - Credential usern
Available Actions		Aligned Actions	1	
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 Tic Snippet [5]: API VeloCloud initial disable Snippet [5]: Automation Utilities: Calculate Me	ket mory Size for E	 A. Get VMvar Snippet [5]: 	e Diagnostic Logs [111]: C Datacenter Automation: I	Set VMWare VMF
	Save	Save As		

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

Automation Policy Editor Editir	ng Automation I	^D olicy [360]		Reset				
Policy Name VMware Automation: Get VMKernel Log and	Policy Type	Policy State	Policy Priority	Organization				
Criteria Logic [Severity >=] ▼ [[Minor,] ▼	Match Logic [Text search]		Match Syntax					
[and no time has elapsed] ▼ [since the first occurrence,] ▼ [and event is NOT cleared] ▼	Repe	eat Time	Align	n With				
Trigger on Child Rollup			organizationa, Baa	olo, old.)				
Available Devices		Aligned Devices						
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								
Available Events		Aligned Events						
[5678] Critical: 3PAR Trap: Critical Alert [5649] Critical: 3PAR: Disk Utilization Exceed [3569] Critical: AKCP: AC Voltage sensor del [3578] Critical: AKCP: DC Voltage sensor Lo [3579] Critical: AKCP: DC Voltage sensor Lo [3568] Critical: AKCP: Dry Contact Sensor Lo (3568] Critical: AKCP: Dry Contact Sensor Lo	led Critical Thres lects no current gh Critical ww Critical ww Critical	 [790] Major: VMwa [794] Major: VMwa [796] Major: VMwa [781] Major: VMwa [1199] Major: VMwa [815] Major: VMwa [816] Major: VMwa 	re: AlarmEmailFailedEv re: AlarmScriptFailedEv re: AlarmStatusChange are: AlarmStatusChange are: AlarmStatusChang re: com.vmware.vc.HA. re: com.vmware.vc.HA.	vent vent dEventRed edEventToRed DasHostCompleteL DasHostCompleteN VmDatastoreEailed				
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 Tic Snippet [5]: API VeloCloud initial disable Snippet [5]: Automation Utilities: Calculate M	cket emory Size for Er 🗸	1. Get VMware Dia 2. Snippet [5]: Data «	ignostic Logs [111]: Get acenter Automation: For	VMWare VMF amat Output as				
	Save	Save As						

- 3. Complete the following fields as needed:
 - Policy Name. Type a new name for the automation policy to avoid overwriting the default policy.
 - **Policy Type**. Select whether the automation policy will match events that are active, match when events are cleared, or run on a scheduled basis. Typically, you would select *Active Events* in this field.
 - **Policy State**. Specifies whether the policy will be evaluated against the events in the system. If you want this policy to begin matching events immediately, select *Enabled*.

- **Policy Priority**. Specifies whether the policy is high-priority or default priority. These options determine how the policy is queued.
- Aligned Actions. This field includes the actions from the 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 AutomationPowerPack.

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 (**S**) 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	. 20
Customizing Automation Actions	. 21
Creating a VMware Automation Action	22

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.

Action Namo	Action State
et VMware Authentication Logs	[Enabled]
	Description
et VMware Diagnostic Logs using the vSphere API	
Organization	Action Type
System]	Get VMware Diagnostic Logs (1.0)
Execution Environment	Action Run Context
Default: VMware Automation Actions]	▼ [Database]
Inp	ut Parameters

- 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.

ction Editor					
Policy Editor Creating New Action	Reset				
Action Name	Action State				
My Custom VMware Action	[Enabled]				
Desc	ription				
Organization	Action Type				
[System]	Get VMware Diagnostic Logs (1.0)				
Execution Environment	Action Run Context				
VMware Automation Actions	Collector				
Input Pa	arameters				
"num_lines":100, "credential_id":0, "log_files":" <u>wmkernel.log</u> , <u>svslog.log</u> " }					
Save	l				

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	Collects the last 50 lines from the vmkernel.log	• num_lines 50
Log and Syslog	file and the syslog.log file.	 log_files vmkernel.log,syslog.log
Get VMware Diagnostic	Collects all lines in all logs from the vCenter	 num_lines {empty}
Logs	appliance.	 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 aping 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 AutomationPowerPack

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?	
Installing the VMware User-Initiated Automation PowerPack	25
Standard Automation Policy	
Running a User Initiated Automation Policy	
Viewing Automation Actions for an Event	

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<u>Release Notes</u>.

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

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

To download and install a PowerPack:

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

Import PowerPack™		×
Browse for file	Browse	
	Import	

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

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

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.

Policy Name Set VMKernel Log and Syslog Align With Devices 1	Policy Type User Initiated]	Policy State ▼ [Enabled] ▼	Organization [System]	
vailable Devices		Aligned Devices		
Benedict_test ScienceLogic, Inc.: EM7 Data Collector: BS-MIG CDP-LLDP Org Disco Systems: 2911 ISR G2: BranchA-R1.your Cisco Systems: 2911 ISR G2: BranchB-R1.your	+-CU-72 domain.com	(All devices)		•
vailable Events		Aligned Events		
3017] Critical: AKCP: AC Voltage sensor detect 3026] Critical: AKCP: DC Voltage sensor High C 3027] Critical: AKCP: DC Voltage sensor Low C 3016] Critical: AKCP: Dry Contact Sensor Low (3022] Critical: AKCP: Smoke Detector Alert!	s no current Critical Critical	[790] Major: VMware: Ala [794] Major: VMware: Ala [796] Major: VMware: Ala [786] Major: VMware: Ala [1200] Major: VMware: Ala [815] Major: VMware: con [816] Major: VMware: con	IrmEmailFailedEvent IrmScriptFailedEvent IrmSnmpFailedEvent IrmStatusChangedEventRed IarmStatusChangedEventToF m.vmware.vc.HA.DasHostCom m.vmware.vc.HA.DasHostCom	Red mpleteE
vailable Actions		Aligned Actions		
SNMP Trap [1]: SL1 Event Trap Snippet [5]: Automation Utilities: Calculate Memo Snippet [5]: AWS: Disable Instance By Tag Snippet [5]: AWS: Discover from EC2 IP	ory Size for E	1. Get VMware Diagnosti 2. Snippet [5]: Datacente	c Logs [109]: Get VMWare V r Automation: Format Output	as Î

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	VMware: Datastore Utilization Has Exceeded Threshold	Get VMware
and Syslog	 VMware: Host CPU Aggregate Usage Has Exceeded Threshold 	Diagnostic Logs
	• 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	

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.

Ev	ents											🔦 Activ	ity E	m7admin 🗸		eLogic
C	4 itical	23 Major	7 Minor	23 Notice	3 Health	iy i	60 Events View All								~	View
Q	Туре	to search event	S												≡	\$
۵		SEVERITY	NAME .	м	IESSAGE			EVENT ID	EVENT SOUR	EV	LA	AUTOMAT	ACKN	OWLEDGE	CLEAR	e
~		 Notice 	DC1_KMS_	Relay B	IG-IP LTM (1	10.2.27.	126): Virtual Server State I	2149	Dynamic	De	Ma	0	~	Acknowledge	X Clear	
~		 Notice 	DC1_KMS_	Relay B	IG-IP LTM (10.2.27.	126): Pool State Availabilit	2191	Dynamic	De	Ma	0	~	Acknowledge	× Clear	
^		😑 Major	em7ao	/0	data.local/dt	o: File sy	ystem usage exceeded maj	428	Internal	De	Ma	3	~	Acknowledge	X Clear	
Vi	als					Тос	ols				Logs					
	100	مىرىلىرلىيىرلىرى ام ^{ارىي} لىرىر	مادارومانو. _{الام} رانغارورومايداره	د	ياويا والمراجع المراجع		🖏 Type to run an act	ion on this de	vice		¢ 40	GE ▼ SEV	ERITY	MESSAGE		
		والمرب أرابير الإرزاد وال	unin in the	, disebut policitation		9	■DEFAULT TOOLS	ARP Lookup	_	L	42	2 minutes 😑	Minor	Physical Memor threshold: (80% (85 481364977	y has exceeded) currently 87365%)	
	۶ ۶O						Availability	ARP Ping		L	42	2 minutes 🛛 😑	Major	DRBD: This nod	e is not UpToDate	
							Ping	Trace Route		L	42	2 minutes		Host Resource: (/data.local/db) HrStorageFixed	Storage Utilization of type Disk has exceeded	
	0	16:00	29. May	08:00			Who Is	≡ RUNBOOK	ACTIONS	L	42	? minutes		Host Resource: (/home) of type	Storage Utilization HrStorageFixedDi aior threshold 859	sk K
							Port Scan	Run File System	n Diagnostic					/data.local/db: F	ile svstem usage	
~		😑 Major	em7ao	D	RBD: This n	cde is n	Deep Port Scan			De	Ma	0	~	Acknowledge	X Clear	
~		 Minor 	HQ-R1.your	domain.com C	isco: IPSLA ((11223)	3) is down. Current status	6947	Dynamic	De	Ma	0	~	Acknowledge	X Clear	
~		Minor	HQ-SW1	с	isco: IPSLA ((107) is	down. Current status time	6011	Dynamic	De	Ma	0	~	Acknowledge	X Clear	

Viewing Automation Actions for an Event

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

≡	Events					et intercatogic
88	1 Critical	17 Major	7 Minor	0 Notice	0 Healthy	25 Events View All
	Q Type to	search events				= •
	ANY: vm 😒					
æ	۵ 🔽	ORGANIZATION	SEVERI	NAME	MESSAGE	AGE TICKET C., EVENT N.,, MASKED EVENT ACKNOWLEDGE CLEAR 🔁
2	~	Example Device	s 🥚 Maj	jo rstlsvcsa6u	2a GeneralVmE	ErrorEvent: Error w 6 days 22 1 🗗 🍳 Masked 🗸 Acknowledge 🗶 Clear
						View Event
						Edit Event Note
						Create External Ticket
						Align External Ticket
						View Automation Actions
						View Event Policy
						Suppress Event for this Device
10.2.24.25	1 Eve /events#	ent Selected	Ack	nowledge	Clear	Align Deselect All Select All Visible

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.

Event Actions Log For Event [31608] Refresh Guide	
2020-01-07 16:32:20	
Automation Policy VMware Automation: Get VMKernel Log and Syslog action Enrichment: Util: Format Command Output as HTML ran Successfully Message Snippet (365) executed without incident Result: <u>Enrichment Command Output</u>	
Command: vpxd:vpxd-107.log 2020-01-0716:31:13.1452 error vpxd[05279] [Originator@6076 sub=VapiEndpoint.HTPFservice] Failed to read request; stream: <io_obj '127<br="" <tcp="" h:-1,="" p:0x00007fbff072f420,="">-> [context] zkq7AVECAAAAAAnxsgALdn84ZAAALEqbGlidmlNY29Z55:buAAQDcbAI67GAtCchoabGULAF151wCVHyM4X11jABE3KnHUcmSaAiJudGHyZHFkInNvLjAAAp2HDmxyYmMuc28uHgAe[/context] 2020-01-0716:31:19,7002 info vpxd[05415] [Originator@6076 sub=vpxLro op1D=1ce34009] [VpxLR0] BEGIN 1ro-13705108 ServiceInstance vim.ServiceInstance.retrieved 2020-01-0716:31:19,7002 info vpxd[0515] [Originator@6076 sub=vpxLro op1D=ce34009] [VpxLR0] BEGIN 1ro-13705109 ServiceInstance vim.ServiceInstance.retrieved 2020-01-0716:31:21.422 info vpxd[2719] [Originator@6076 sub=vpxLro op1D=c534bb6] [VpxLR0] BEGIN 1ro-13705109 ServiceInstance vim.ServiceInstance.retrieved 2020-01-0716:31:21.422 info vpxd[2729] [Originator@6076 sub=vpxLro op1D=c534bb6] [VpxLR0] BEGIN 1ro-13705109 ServiceInstance vim.ServiceInstance.retrieved 2020-01-0716:31:21.422 info vpxd[05275] [Originator@6076 sub=vpxLro op1D=sps-Hain-370655.742-14] [VpxLR0] BEGIN 1ro-13705110 2020-01-0716:31:21.2122 info vpxd[05345] [Originator@6076 sub=vpxLro op1D=sps-Hain-370685-742-14] [VpxLR0] BEGIN 1ro-13705110 2020-01-0716:31:21.2122 info vpxd[05345] [Originator@6076 sub=vpxLro op1D=sps-Hain-370685-742-14] [VpxLR0] BEGIN 1ro-13705112 2020-01-0716:31:21.2122 info vpxd[05345] [Originator@6076 sub=vpxLro op1D=sps-Hain-370685-742-14] [VpxLR0] BEGIN 1ro-13705112 2020-01-0716:31:21.2122 info vpxd[05345] [Originator@6076 sub=vpxLro op1D=sps-Hain-370685-742-14] [VpxLR0] BEGIN 1ro-13705112 2020-01-0716:31:21.222 info vpxd[05345] [Originator@6076 sub=vpxLro op1D=sps-Hain-370685-742-14] [VpxLR0] BEGIN 1ro-13705112 2020-01-0716:31:21.222 info vpxd[05345] [Originator@6076 sub=vpxLro op1D=sps-Hain-370685-742-14] [VpxLR0] BEGIN 1ro-13705112 2020-01-0716:31:21.222 info vpxd[05345] [Originator@6076 sub=vpxLro op1D=sps-Hain-370685-742-14] [VpxLR0] EBGIN 1ro-13705112</io_obj>	
Command: vpxd:vpxd-profiler-65.log -> /SessionStats/SessionPool/Id*'52f8035-046c-aab8-0155-eca2a9cfba78'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/total 0 -> /SessionStats/SessionPool/Id*'52f9014e-e108-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeOUReqTime/max 0 -> /SessionStats/SessionPool/Id*'52f9014e-e108-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeOUReqTime/max 0 -> /SessionStats/SessionPool/Id*'52f9014e-e108-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeOUReqTime/max 0 -> /SessionStats/SessionPool/Id*'52f9014e-e108-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeOUReqTime/max 0 -> /SessionStats/SessionPool/Id*'52f9014e-e108-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeOUReqTime/max 0 -> /SessionStats/SessionPool/Id*'52f9014e-e108-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 -> /SessionStats/SessionPool/Id*'52f9014e-e108-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 -> /SessionStats/SessionPool/Id*'52f9014e-e108-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 -> /SessionStats/SessionPool/Id*'52f9014e-e108-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 -> /SessionStats/SessionPool/Id*'52f9014e-e108-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 -> /SessionStats/SessionPool/Id*'52f9014e-e108-47f8-f671-10004ef8240c'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 -> /SessionStats/SessionPool/Id*'52f47aa-6f67-6f84-4288-5486fd45bb97'/Username='VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeOUReqTime/max 0 -> /SessionStats/SessionPool/Id*'52f47aa-6f67-6f84-4288-5486fd45bb97'	
Command: updd:updd:updfler.log > /sssionStats/SssionPool/id '52f835-046c-ab8-0155-sca2a0cfba78 //Username'VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/total 0 > /sssionStats/SssionPool/id '52f8014-e180-47f8-f671-1004ef8240c'/Username'VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/total 0 -> /sssionStats/SssionPool/id '52f8014-e180-47f8-f671-1004ef8240c'/Username'VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/total 0 -> /sssionStats/SssionPool/id '52f8014-e180-47f8-f671-1004ef8240c'/Username'VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeSUMEqTime/man 0 -> /sssionStats/SssionPool/id '52f8014-e180-47f8-f671-1004ef8240c'/Username'VSPHERE.LOCAL\Administrator'/PropertyCollector/ComputeSUMEqTime/min 0 -> /sssionStats/SssionPool/id '52f8014-e180-47f8-f671-1004ef8240c'/Username'VSPHERE.LOCAL\Administrator'/PropertyCollector/SetDoneTime/max 0 -> /sssi	•

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.

© 2003 - 2021, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

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

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

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

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

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

Other

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

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



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

International: +1-703-354-1010