vRealize Operations Management Pack for Smart Assurance Adapter Guide

VMware Smart Assurance 10.0



You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc. 3401 Hillview Ave. Palo Alto, CA 94304 www.vmware.com

Copyright [©] 2019 VMware, Inc. All rights reserved. Copyright and trademark information.

VMware, Inc.

Contents

- **1** About This Book 4
- 2 Introduction to the vRealize Operations Management Pack for Smart Assurance Adapter 5
- **3** Solution Overview 6
- 4 Installing and Configuring the Management Pack 7 Post Installation Task 8
- 5 Configure the Smart Assurance Adapter 9
- 6 Management Pack for Smart Assurance Adapter 11
 Environment Tab 11
 Dashboard Tab 13
- 7 Management Pack for Smart Assurance Adapter Metrics 18
 Statistical Metrics of the Management Pack for Smart Assurance Adapter 18
 Physical Device Metrics 18
 vIMS Performance Metrics 20
- 8 Troubleshooting Methodologies 22

About This Book

The *vRealize Operations Management Pack for Smart Assurance Adapter Guide* describes how to install and configure the Management Pack for Adapters for vRealize Operations Manager. It also explains how this management pack works and how to configure its adapters.

Intended Audience

The information in this guide is intended for storage administrators, data center architects, and IT operators.

Purpose

This document provides detail information about the Smart Assurance Adapter configuration and usages information.

Introduction to the vRealize Operations Management Pack for Smart Assurance Adapter

The Telco service providers needs consolidation of various services to serve their customers. Those services are running on complex, dynamic, and heterogeneous infrastructures. End-to-end service assurance of such systems becomes increasingly complicated with the deployment of rapidly growing cloud computing services and virtualized environments.

End-to-end Service Assurance involves collecting data from heterogeneous data sources, processing different types of data and presenting it in a visualization layer. The Smart Assurance Adapter implementation provide generic solution for collecting data from several heterogenous systems and represent it in a unified model which provides customers a seamless experience of visualization of topology and metrices in single glass of pane.

3

Solution Overview

The Smart Assurance Adapter uses the existing management pack framework of vRealize Operations Manager to provide the solution. This management pack has uses the unified modeling to represent the collected data.

The management pack for Smart Assurance has the following outlines:

- The describe.xml file in management pack contains the information about the various network elements and the supported metric is designed in accordance with the unified data model.
- The describe.xml file is being read during the initialization process of adapter. The processed information then stored in the internal data structure for further future reference.
- The Kafka bus is one of the major subsystem of the solution. The management pack implements the kafka consumer to read the data from the kafka bus.
- The vRelalize Operation Manager framework periodically invokes onCollect() hook method of management pack and subsequently the management pack poll kafka bus in order to receive the data.
- The received data is checked for acceptability condition before processing. This check is driven by the information present in the describe.xml file. If the data is not modelled, then it is discarded.
- After the data passes the pre-condition:
 - The resulting data is parsed
 - The output data is passed through a filter
 - Non-monitored network adapter metrics may need to be filtered for certain usages.

For example, non-monitored network adapter metrices may needs to be filtered for certain usages.

 After the data passes through the filter it is mapped to vROps resource which is again defined in unified model. Also, the unified model is used to convert the received data to metrices associated with resource.

Installing and Configuring the Management Pack

4

To install a management pack, download the PAK file as part of the solution, and install it. Once installed you can configure the management pack and the adapter instance settings.

Prerequisites

Smart Assurance adapter needs following subsystems to be installed and pre-configured for it to be functional:

- DCF collectors
- Kafka
- Various data sources (for example SMART IP server)
- vROps

Procedure

- 1 Log in to the vRealize Operations Manager user interface with administrator privileges.
- 2 In the menu, click Administration and then in the left pane, click Solutions.
- 3 On the **Solutions** page, click the **Add** icon.
- 4 Browse to locate the temporary folder and select the PAK file.

For example, managementpack_name_buildnumber.pak.

5 Click Upload.

The upload might take several minutes.

6 Read and accept the EULA and then click **Next**.

Installation details appear in the window during the process.

- 7 Ensure that you install the PAK file on the master node.
- 8 When the installation is complete, click **Finish**.

What to do next

Configure the adapter instance for the management pack.

Post Installation Task

After installing the Smart Assurance Adapter Management Pack, admin needs to edit the notifications.html file to point to the Notification log view GUI serve.

Procedure

- 1 After installing the Smart Assurance Adapter Management Pack, notifications.html is present at /usr/lib/vmwarevcops/user/plugins/inbound/SMARTSAssuranceAdapter/conf/dashboards/
- **2** Open the notifications.html file.
- 3 Update the "href" value with the actual notification log view server details, for example:

<a href="<IpAddress/hostname>"

4 Go to the below location:

/usr/lib/vmware-vcops/tools/opscli

5 Import notifications.html, by invoking the below command:

VMWARE_PYTHON_BIN ops-cli.py file import txtwidget /usr/lib/vmwarevcops/user/plugins/inbound/SMARTSAssuranceAdapter/conf/dashboards/notifications.h tml

Configure the Smart Assurance Adapter

5

After you install the management pack, add and configure an instance to start collecting data. Primarily SmartAssurance adapter needs kafka broker details to be configured for functioning.

Procedure

- 1 In the menu, click **Administration** and then in the left pane, click **Solutions**.
- 2 On the Solutions page, click Smart Assurance Adapter, and click the Configure icon.
- 3 Select the instance in the left pane and configure the instance settings.

Option	Description	Default Value
Display Name	Enter a name for the adapter instance.	
Description	Enter a description for the adapter instance.	
KafkaBrokerIP:Port	Enter the FDQN or the IP address for the Kafka broker IP and port.	
	Note The kafka broker IP and port needs to be separated by ":" and the multiple IP Addresses must be separated by comma ",".	
Kafka Topic(s)	Enter the kafka topic name. These topics must be pre-configured on kafka and various DCF collector must be producing data in that topic. The multiple topic must be separated by comma ",".	
Kafka read time out Interval	Waiting period in seconds for kafka client to get the data on the kafka bus before it times out in that particular collection cycle.	120 seconds
Kafka Message Start Offset	Enter the kafka message. Kafka client will start reading messages from the specified offset value.	0

Option	Description	Default Value
Number of Retry	Number of retries attempted to read the data on failure.	2
Number of Iteration	Enter the number of times Kafka consumer poll data from kafka bus in one vROps polling cycle.	2

- 4 To add the credentials used to access the Kafka Server, click the **Add** icon.
 - a To add the credentials used to access the Kafka Server with authentication enabled:

Option	Description
Credential Name	Enter the name by which you are identifying the configured credentials.
USERNAME	Enter the username with which you connect to kafka.
PASSWORD	Enter the password with which you connect to kafka.

b To add the credentials used to access the Kafka Server with authentication disabled:

Option	Description
Credential Name	Enter the name by which you are identifying the configured credentials.
USERNAME	Leave the username blank.
PASSWORD	Leave the password field blank.

Note SASL_SSL and SSL authentication mechanism are not supported.

- 5 Click **OK** and then click **Test Connection** to validate the connection.
- 6 You can configure the **Advanced Settings** or leave it as default.
- 7 Click Save Settings.

The adapter instance is added to the list.

Management Pack for Smart Assurance Adapter

6

The Management Pack for Smart Assurance Adapter contains prepackaged dashboards for alerts, health, performance, capacity, and top utilization metrics. Post installation, it adds the preconfigured dashboards and alert definitions to monitor and troubleshoot the components in your storage area network. Once the data collection started from kafka bus the collected information can be viewed primarily from two panes Environment and Dashboard.

This chapter includes the following topics:

- Environment Tab
- Dashboard Tab

Environment Tab

The environment tab represents the tree view of the collected data. It also captures the parent child relationship of the object. Upon selecting the object from tree view it displays the Health Status of the object and the collected metrices in *About Me* pane.

Tree view of the physical network elements

BACK ~ «	1 Aggregat Summary A	ePort-10.107.1 lerts All Metrics	19.10/5001-L Capacity	ACP Compliance E	vents more	🗢 🥥 💈 vSphe	ere Solution's Default Policy (Mar 07, 2019 6	:29:35 PM)
Container Container EP Ops Adapter	Recommended	Actions					About Me	
NHTP Post	Me	AggregatePort (1) Port (8)			Badge Compliance:	-1
SmartAssuranceAdapter							BadgelEfficiency:	100 %
 AggregatePort 		He	alth Status			Badge: 🔲 🎓 🔎	BadgelHealth:	100 %
r AggregatePort-10.10							BadgelRisk:	0 %
T AggregatePort-10.10							NetworkAdapter/CurrentUtilization:	0.0043
> Erewall		1	O Critical				NetworkAdapterlifInDiscards:	0
> Host		Objects	0 Immediate				Network Adapter liftn Errors:	0
> M I/S-CSCF							Notwork Advetorifiabil lossfolder	
> F Interface							NetworkAdapterininiocastPkts.	0
							NetworkAdapterinnuCastPkts:	
> 14 Memory					All Filters ¥	Y Quick filter (Alert)	NetworkAdapter/ifOutDiscards:	0
> P-CSCF	() Name	Alert	Alert Typ	e Alert S Time	Suggested Fix	Action		
> E Port								
> B Processor								
> 🔂 Router								
> 🔐 SmartAssuranceAdapte								
> 🗙 Switch								
🛃 vCenter Adapter								

Tree view of KPI Metrices

vm vRealize Operations Ma	nager H	ome Dashboar	ds Alerts	Environment	Administration		Q	C A A
BACK ~ «	KPI-vIM	S-10.106.230.10 Alerts All Metric	00-snap0100 s Capacity	Compliance Eve	nts more		a 8 a	Befault Policy ?
Container P Container P EP Ops Adapter Http Post	Recommend	ed Actions				*	About Me	
A SmartAssuranceAdapter	Me	I/S-CSCF (1)	P-CSCF (1) Health Status		В	adge: 🔲 🎕 🛢	BadgelCompliance: BadgelEfficiency: BadgelHealth:	-1 100 % 100 %
 AggregatePort FileSystem Firewall 		\bigcap	O Critical				BadgelRisk: KPIldeploymentid:	0 % snap0100
Host K-CSCF Finterface Fin		Objects	0 immediate				KPildevtype: KPilicscf-network-session- establishment-success- rate:	VIMS 78.09
✓ KPI ★ KPI-VIMS-10.106.230.	⊠ ⊠				All Filters 👻 🍸	Quick liter (Alert)	KPIlicscf-user-session- establishment-success-	1.01
KPI-VIMS-I0.106.230.	🕐 🏟 Sug	ggested Fix	Name	Alert	Alert Type	Alert Si Time	KPilorchestrator:	10.106.230.100
> 引 Memory ~ 🛐 P-CSCF							KPIIscscf-audio-session- average-setup-time:	40

Tree view of vIMS Metrices

The vIMS metrices are represented as children of the I/S-CISF and P-CSCF objects.



Parent child relationship in physical network

Typically, the parent objects are placed on the top of the child objects in the display pane.



Dashboard Tab

Smart Assurance Adapter provides some default dashboards for customer to view various metrices. These dashboards can be reached by clicking the Dashboard tab. vROps provides various options to create dash board that user can use for various requirements.

Physical Network Dashboard - Physical Device Details

This dashboard displays the various physical network devices and their relationship along with its containment information. The topology graph displays the associated topological elements of the selected physical device.



Physical Network Dashboard - Physical Network Adapters

This dashboard displays various network adapters (interface, Port, Aggregate Port) and it's metrices along with connected topology details. It also displays the collected metrices in a trend graph.



Physical Network Dashboard - Top-N-Adapter-Utilization

This report displays the Top 5 Network-Adapters that are highly utilized.

"	vkealize Operations Manager	Home Dashboards Alerts	Environmen	Administration		Q	C	부	
	Top-N-Adapter-Utilization	ctions 👻 All Dashboards 👻						Shared	0
	Top-N-Utilization			Metric Chart					
	CurrentUtilization	Objects		IF-61-25-42-1.revhome.ne.jp/4900	IF-61-25-42-1.rev.home.ne.jp/49001			<u>.</u>	
	0.6	IF-61-25-42-1.rev.home.ne.jp/49001			NetworkAdapter)CurrentUtilization				
	0	PORT-61-25-61-252 rev home ne jp/-	47	•H: 1.45				10	
	0	PORT-61-25-42-1 rev.home.ne.jp/47							
	0 0	PORT-10.107.119.10/1.24		•L: 0.352				-10	
0 PORT-10.107.119.9/1.21				12:00 PM 01:00 PM 0	2.00 PM 03.00 PM 04.00 PM 05.00	PM	06:00 PM	PM	
	Sparkline Chart								
	BadgelCompliance (%)	•	-1						
	BadgelEfficiency (%)		100						
	BadgelPick (%)		0						
	NetworkAdapter/CurrentUtilization		0.57						
	NetworkAdapterlifInDiscards		0						
	NetworkAdapterlifInErrors		0						
	NetworkAdapterlifInNUcastPkts	manyman	0.65						
	NetworkAdapterlifInUcastPkts		17,771.53						
	NetworkAdapterlifOutDiscards		o *						

Physical Network Dashboard - Top-N-Network-Device-CPU-Utilization

This report displays the Top 5 CPU that are highly utilized along with the device information.

vm	vRealize Operations Manager	Home Dashboards Alerts Em	vironment Administ	ration	d G	¢,	°Ŭ
	Top-N-Network-Device-CPL	I-Utilization Actions - All Dashboards -			1	Shared	Ś
	Device-Cpu-Utilization		Device				
	CurrentUtilization	Objects	Object Type	Name	Adapter Type		
	14	PSR-10.107.119.10/1	Switch	10.107.119.10	SmartAssuranceAda		^
	12	PSR-10.107.119.9/1					
	7	PSR-61-25-42-1 rev.home.ne.jp/3					
	7	PSR-61-25-61-252.rev.home.ne.jp/3					
	6	PSR-61-25-42-1 rev.home.ne.jp/1					
	Related Elements				1-1	of 1 items	*
	PSI	10.107.119.10 -0.107.119.10/1					

Physical Network Dashboard - Top-N-Network-Device-Memory-Utilization

This report displays the Top 5 Memory that are highly utilized along with the device information.

Fop-N-Network		Shared	α					
Top-N		Object List						
FreeMemoryPct	Objects	Name	Adapter Type	Object Type	Policy			
0.2	MEM-61-25-42-1.rev.home.ne.jp/7	61-25-42-1 rev.home.ne.jp	SmartAssuranceAda	Switch	vSphere Solution's D.			
48	MEM-61-25-61-252.rev.home.ne							
41.2	MEM-61-25-42-1.rev.home.ne.jp/1							
42.1	MEM-61-25-61-252.rev.home.ne							
56.2	MEM-10.107.119.10/2							
		<		_	, ×			
					1-1 of 1 items			
Rolling View Chart								
	MEM-61-25-42 Badgeli	-1 rev.home.ne.jp/1 fliciency (%)						
•H: 100								
				100				
•L: 100								

Physical Network Dashboard - Network-Adapters-Performance-Params

This report displays various network adapters and available performance metrices. Upon selecting the adapter, the various collected metrics gets displayed in the right most frame.

	Network-Adapters-r	-errormance-Pa	dills Actions • All	i Dashboards Y		onared
ishboards	Network-Adapters			Scoreboard		
(PI-Dashboard	Name	Adapter Type	Object Type	CurrentUt 0 00054	• ifInDiscards	0
/IMS-Dashboard	IF-10.107.116.235/6	SmartAssuranceAda	Interface ^	0.00034		0
Physical-Device-Details Physical-Network-Adapters	IF-61-25-61-252.rev.home.ne.j.	SmartAssuranceAda	Interface	• ifInErrors C	ifInNUcastPkts	0
op-N-Network-Device-Memory-Utilization	PORT-10.107.119.9/1.24	SmartAssuranceAda_	Port			
Fop-N-Network-Device-CPU-Utilization Fop-N-Adapter-Utilization	IF-61-25-61-252.rev.home.ne.j.	SmartAssuranceAda	Interface	• ifInUcastPkts 0.27	• ifOutDiscards	0
fop-N-Adapter-Errors	IF-10.107.116.243/6	SmartAssuranceAda_	Interface			
Network-Adapters-Performance-Params Setting Started	IF-61-25-42-1.rev.home.ne.jp/_	SmartAssuranceAda	Interface	• ifOutErrors C	ifOutNUcastPkts	0
ews	IF-61-25-42-1.rev.home.ne.jp/	SmartAssuranceAda_	Interface			
ports	<		× *	ifOutUcastPkts 0.1		
		1 - 50 of 8	6 items (1 2)			

KPI - Dashboards

This dashboard provides the details of KPI collected by Smart Aassurance Adapter. The "List of KPIs" displays the list of KPIs. The Scoreboard displays the current values of various metrices and right most frame provides the metric chart.

 vRealize Operations Manager	Home Dashb	oards Alerts					Q C	Δ,
KPI-Dashboard Actions ~	All Dashboards 🛩							Shar
List Of KPIs				* 0	? ©	Metric Chart		
Name	Adapter Type	Object Type	Policy	Collection State	Collect	KPI-vIMS-10.106	230.99-snap099	=~
KPI-vIMS-10.106.230.99-snap099	SmartAssuranceAdapter	KPI	Default Policy		• •	KPI3cscf-network-session-	-establishment-success-rab	9
KPI-vIMS-10.106.230.100-snap0100	SmartAssuranceAdapter	KPI	Default Policy			•H: 100		
KPI-vIMS-default-default	SmartAssuranceAdapter	KPI	Default Policy	~ ~		*******		100
						•L: 100		
						02:00 PM 0	4:00 PM 06:00 PM	-
						8	04:00 PM	8
(>	KPI-viMS-10.106	230.99-snap099	11
				1.2	of 1 James	KPflicscf-user-session-er	stablishment-success-rate	
				1.0	101000			
Scoreboard				114		•H: 100		
Scoreboard				113		•H: 100		100
Scoreboard icscf-network-session-estat	blishment-succes 100) • icscf-user-:	session-establishme	ent-success-ra	100	•H: 100		100
scoreboard icscf-network-session-estat	blishment-succes 100) • icscf-user-:	session-establishme	int-success-ra	100	•H: 100 •L: 100 02:00 PM 0	4:00 PM 06:00 PM	100
coreboard icscf-network-session-estate	blishment-succes 100) • icscf-user-	session-establishme	ent-success-ra	100	•H: 100 •L: 100 02:00 PM D	6:00 PM 06:00 PM	100
scoreboard icscf-network-session-estat scscf-audio-session-averag	blishment-succes 100 e-setup-time () • icscf-user-+	session-establishme -reg-success-rate	int-success-ra	100	•H: 100 •L: 100 02:00 PM 0- 0 KPI-vIMS-10:106	6.00 PM 06:00 PM 04:00 PM 1230.99-snap099	100
Scoreboard icscf-network-session-estat scscf-audio-session-averag	blishment-succes 100 e-setup-time () • icscf-user-	session-establishme -reg-success-rate	nt-success-ra	100	•H: 100 •L: 100 02:00 PM 00 KPI-vINS-10:106 KPIScscf-audio-sess	600 PM 06:00 PM 06:00 PM 230 99-snap099 on-average-setup-time	100
scorebaard sicscf-network-session-estat sicscf-audio-session-averag	blishment-succes 100) • icscf-user-t	session-establishme -reg-success-rate	int-success-ra	100 100	•H: 100 •L: 100 02:00 PM 0 KPH-vMS-10:106 KPRiscal-audio-sessi •H: 0	600 PM 06:00 PM 08:00 PM 230:99-snap099 on-average-setup-time	100

Smart Metric Dashboard

This dashboard provides information about collected metrices of Smart deployment and topology information.

vRealize Operations Management Pack for Smart Assurance Adapter Guide



Management Pack for Smart Assurance Adapter Metrics

The Management Pack for Smart Assurance Adapter collects metrics for objects. It also displays object properties in the vRealize Operations Manager user interface.

This chapter includes the following topics:

- Statistical Metrics of the Management Pack for Smart Assurance Adapter
- Physical Device Metrics
- vIMS Performance Metrics

Statistical Metrics of the Management Pack for Smart Assurance Adapter

The Management Pack for Smart Assurance Adapter collects statistical metrics of objects.

You can view these metrics from the vRealize Operations Manager user interface, click Administration > Configuration > Inventory Explorer > Adapter Instances > SmartAssuranceAdapter Instance. Alternately, you can also click Environment > All Objects> SmartAssuranceAdapter Instance.

Physical Device Metrics

The Management Pack for Smart Assurance Adapters collects metrics about the devices discovers in SMARTS IP.

Device	Metric Name
Switch	Reachability
	ip
	vendor
	model
	devdesc
Router	Reachability
	ip
	vendor

Table 7-1. Physical Device Metrics

Table 7-1. Physical Device Metrics (Continued)

Device	Metric Name
	model
	devdesc
Host	Reachability
	ip
	vendor
	model
	devdesc
Firewall	Availability
	ip
	vendor
	model
	devdesc
Port	CurrentUtilization
	ifInDiscards
	ifInUcastPkts
	ifOutOctets
	ifOutUcastPkts
	ifOutErrors
	ifInOctets
	ifInNUcastPkts
	ifInErrors
	ifOutNUcastPkts
	ifOutDiscards
Interface	CurrentUtilization
	ifInDiscards
	ifInUcastPkts
	ifOutOctets
	ifOutUcastPkts
	ifOutErrors
	ifInOctets
	ifInNUcastPkts
	ifInErrors
	ifOutNUcastPkts
	ifOutDiscards

Device	Metric Name		
AggregatePort	CurrentUtilization		
	ifInDiscards		
	ifInUcastPkts		
	ifOutOctets		
	ifOutUcastPkts		
	ifOutErrors		
	ifInOctets		
	ifInNUcastPkts		
	ifInErrors		
	ifOutNUcastPkts		
	ifOutDiscards		
FileSystem	CurrentUtilization		
	Capacity		
	FreeCapacity		
Processor	CurrentUtilization		
Memory	FreeMemoryPct		
	TotalMemory		
	TotalBufferAllocationFailures		
	LargestFreeBuffer		
	FreeMemory		

Table 7-1.	Physical	Device	Metrics	(Continued)
		201100		(00

vIMS Performance Metrics

The Management Pack for Smart Assurance Adapter collects metrics about the Virtual IP Multimedia Subsystem(vIMS) components.

Source	Metric Name
Sprout	ICSCFSessionEstablishmentNetworkSuccesses_scopeCurrent5MinutePeriod
	ICSCFSessionEstablishmentNetworkAttempts_scopeCurrent5MinutePeriod
	ICSCFSessionEstablishmentNetworkFailures_scopeCurrent5MinutePeriod
	ICSCFSessionEstablishmentNetworkSuccessPercent_scopeCurrent5MinutePeriod
	SCSCFInitialRegistrationAttempts_scopeCurrent5MinutePeriod
	SCSCFInitialRegistrationSuccesses_scopeCurrent5MinutePeriod
	SCSCFInitialRegistrationFailures_scopeCurrent5MinutePeriod
	SCSCFInitialRegistrationSuccessPercent_scopeCurrent5MinutePeriod

Table 7-2. vIMS Performance Metrics

Table 7-2. vIMS Performance Metrics (Continued)

Source	Metric Name
	SCSCFAudioSessionSetupTimeAverage_scopeCurrent5MinutePeriod
	SCSCFAudioSessionSetupTimeVariance_scopeCurrent5MinutePeriod
	SCSCFAudioSessionSetupTimeHWM_scopeCurrent5MinutePeriod
	SCSCFAudioSessionSetupTimeLWM_scopeCurrent5MinutePeriod
	SCSCFAudioSessionSetupTimeCount_scopeCurrent5MinutePeriod
	SCSCFVideoSessionSetupTimeAverage_scopeCurrent5MinutePeriod
	SCSCFVideoSessionSetupTimeVariance_scopeCurrent5MinutePeriod
	SCSCFVideoSessionSetupTimeHWM_scopeCurrent5MinutePeriod
	SCSCFVideoSessionSetupTimeLWM_scopeCurrent5MinutePeriod
	SCSCFVideoSessionSetupTimeCount_scopeCurrent5MinutePeriod
	ICSCFSessionEstablishmentAttempts_scopeCurrent5MinutePeriod
	ICSCFSessionEstablishmentSuccesses_scopeCurrent5MinutePeriod
	ICSCFSessionEstablishmentFailures_scopeCurrent5MinutePeriod
	ICSCFSessionEstablishmentSuccessPercent_scopeCurrent5MinutePeriod
Bono	QueueSuccessFailSuccesses_scopeCurrent5MinutePeriod
	QueueSuccessFailFailures_scopeCurrent5MinutePeriod
	QueueSuccessFailSuccessPercent_scopeCurrent5MinutePeriod
	QueueSuccessFailAttempts_scopeCurrent5MinutePeriod
	LatencyAverage_scopeCurrent5MinutePeriod
	LatencyVariance_scopeCurrent5MinutePeriod
	LatencyHWM_scopeCurrent5MinutePeriod
	LatencyLWM_scopeCurrent5MinutePeriod
	LatencyCount_scopeCurrent5MinutePeriod
K4M	scscf-initial-reg-success-rate
	scscf-video-session-average-setup-time
	scscf-audio-session-average-setup-time
	icscf-user-session-establishment-success-rate
	icscf-network-session-establishment-success-rate

8

Troubleshooting Methodologies

Logs and log locations

Log for Smart Assurance Adapter is located at: /storage/vcops/log/adapters/SmartAssuranceAdapter

Logging and troubleshooting

How do I increase logging levels if required?

To change the log label follow the below steps:

- 1 Go to Administration> Support > Logs.
- 2 From the **Group by** drop-down, select **Log Type**.
- 3 Select COLLECTOR.
- 4 Click Edit Properties icon, Edit Logger Configuration window appears.
- 5 Add a new Log Class by pressing + icon.
- 6 Enter the name of a log class to add: as com.vmware.sas.smart.assurance.adapter.
- 7 Change the Logging Level to All to get all the log.