VMware Smart Assurance IP Manager Troubleshooting Guide

VMware Smart Assurance 10.0.0

vmware®

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.

Contents

1 Preface 5
- Purpose 5
- Audience 5

2 VMware Smart Assurance IP Manager installation directory 6

3 VMware Smart Assurance IP Manager products 7

4 IP Manager documentation 8

5 Related documentation 9

6 Conventions used in this document 10
- Typographical conventions 10

7 Where to get help 11

8 Your comments 12

9 Troubleshooting Installations 13
- Licensing Issues 13
- Frequently Asked Questions on Licensing 14

10 Troubleshooting Deployments and Configurations 16
- Deployment Issues 16
- Configuration Issues 16
- Frequently Asked Questions on deployment and configurations 20

11 Troubleshooting Certification 23
- Frequently Asked Questions on Certification 23

12 Troubleshooting Discovery, Performance and Monitoring 25
- Discovery Issues 25
- Performance and Monitoring Issues 28
- Frequently Asked Questions on Discovery, Performance and Monitoring 32

13 General Troubleshooting 38
- General Issues 38

Frequently Asked Questions 47

Preface

1

As part of an effort to improve its product lines, VMware periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your VMware technical support professional if a product does not function properly or does not function as described in this document.

Note This document was accurate at publication time. Go to VMware Online Support support.vmware.com to ensure that you are using the latest version of this document.

This chapter includes the following topics:

- Purpose
- Audience

Purpose

This document is part of the VMware Smart Assurance IP Manager documentation set and contains troubleshooting instructions and Frequently Asked Questions on VMware Smart Assurance IP Manager.

Audience

This document is intended for IT managers and system administrators.

VMware Smart Assurance IP Manager installation directory

2

In this document, the term BASEDIR represents the location where VMware Smart Assurance software is installed.

- For UNIX, this location is: /opt/InCharge/<productsuite>.

  On UNIX operating systems, VMware Smart Assurance IP Availability Manager is, by default, installed to: /opt/InCharge/IP/smarts.

  Optionally, you can specify the root of BASEDIR to be something different, but you cannot change the <productsuite> location under the root directory.

  The VMware Smart Assurance System Administration Guide provides more information about the directory structure of VMware Smart Assurance software.

VMware Smart Assurance IP Manager products

3

The VMware Smart Assurance IP Manager includes the following products:

- VMware Smart Assurance IP Availability Manager
- VMware Smart Assurance IP Performance Manager
- VMware Smart Assurance IP Availability Manager Extension for NAS

IP Manager documentation

4

The following documents are relevant to users of the IP Manager. Electronic versions of the updated manuals are available on VMware Smart Assurance Online Support at: docs.vmware.com.

- VMware Smart Assurance IP Manager Release Notes
- *VMware Smart Assurance Open Source License and Copyright Information*
- *VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers*
- *VMware Smart Assurance IP Manager Deployment Guide*
- *VMware Smart Assurance IP Manager Concepts Guide*
- *VMware Smart Assurance IP Manager User Guide*
- VMware Smart Assurance IP Manager Reference Guide
- VMware Smart Assurance Topology Split Manager User Guide
- VMware Smart Assurance IP Manager Troubleshooting Guide
- *VMware Important Notice*
- *VMware Smart Assurance IP Manager Certification Matrix*

Related documentation

5

The following VMware Smart Assurance publications provide additional information:

- *VMware Smart Assurance System Administration Guide*
- *VMware Smart Assurance Common Information Model (ICIM) 1.11 Reference for Non-Service Assurance Manager Products*
- VMware Smart Assurance Common Information Model (ICIM) Reference for Service Assurance Manager
- *VMware Smart Assurance ASL Reference Guide*
- *VMware Smart Assurance Perl Reference Guide*
- *VMware Smart Assurance MODEL Reference Guide*
- *VMware Smart Assurance Dynamic Modeling Tutorial*
- Smarts Foundation EMC Data Access API (EDAA) Programmer Guide

  In addition to this document, Smart Assurance Corporation provides a Help system for command line programs.

Conventions used in this document

6

VMware Smart Assurance uses the following conventions for special notices:

Note NOTICE is used to address practices not related to personal injury.

A note presents information that is important, but not hazard-related.

An important notice contains information essential to software or hardware operation.

Typographical conventions

VMware uses the following type style conventions in this document:

Bold	Use for names of interface elements
Italic	Use for full titles of publications referenced in text
`Monospace`	Use for: ■ System output, such as an error message or script ■ System code ■ Pathnames, filenames, prompts, and syntax ■ Commands and options
`Monospace italic`	Use for variables.
`Monospace bold`	Use for user input.
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

7

VMware Smart Assurance support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about VMware Smart Assurance products, go to VMware Smart Assurance Online Support at:

docs.vmware.com

Technical support

Go to VMware Smart Assurance Online Support and click Service Center. You will see several options for contacting VMware Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your VMware sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

8

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Provide your feedback of this document to: docs.vmwre.com.

Troubleshooting Installations

9

This chapter includes the following topics:

- Licensing Issues
- Frequently Asked Questions on Licensing

Licensing Issues

This section provides the following troubleshooting information:

Starting a new domain after the trial license expires

Discovery failures after license expires

Starting a new domain after the trial license expires

Symptom

Unable to start a new domain and restart an existing domain after the trial license expired.

Possible Cause

New devices can be added to the topology and discovery can be performed during the grace period, but new domains cannot be started using the same license. A fresh license is required start new domain servers.

Recommended Action

The domain using a trial license that has expired will continue to run for a year as long as it is not restarted. If you attempt to restart the existing domain or start a new domain it will not start.

Request for a new trial license that has a new expiration date.

Discovery failures after license expires

Symptom

Discovery failed after the IP Manager license expired.

Possible Cause

Discovery and auto-discovery depends on the AP_SYSTEM_VOLUME license feature.

For example, if the licence is expiring on 9/15/2011 and five domains are pointing to the license server, even after expiry, the five domains will continue to work till 9/15/2012. However if we start a new domain server after 9/15/2011 that is pointing to the same license file, it will not work.

Recommended Action

If your temporary license expires and you are within the grace period, you will not be able to either restart existing domain managers if they are stopped.

Frequently Asked Questions on Licensing

Licensing questions

Question

Can I split available volume licenses between multiple domains?

Answer

As long as the devices are in the same datacenter and they connect to the same license server, it will be possible to create two completely separate platforms, else new base licenses have to be acquired.

Question

Which host ID should be used while requesting for a permanent license file from the following permanent FLEXnet license?

```
lmutil - Copyright (c) 1989-2010 Flexera Software, Inc. All Rights Reserved. The FLEXnet host ID of
this machine is ""002128a2aea2 002128a2aea3 002128a2aea4 002128a2aea5""
```

Answer

It is recommended to use the first host ID.

Question

Should we restart domains to load new license licenses?

Answer

You need to restart your domains.

Question

Should we restart the license server after receiving a new permanent license?

Answer

You need to place the license file in <BASEDIR>/smarts/local/conf in the installation directory of the license server.

Use the following command to read the new license:

```
<BASEDIR>/smarts/bin/lmutil lmreread -c port@license_server
```

or

```
<BASEDIR>/smarts/bin/system/lmutil lmreread -c port@license_server
```

Question

I have loaded a new permanent license into the license server, do I need to restart my domains?

Answer

Yes, if you have loaded features that enable new functionality such as NOTIF for Service Assurance Manager or IP Performance Manager.

No, if the new license contains additional blocks of volume licenses

Troubleshooting Deployments and Configurations

10

This chapter includes the following topics:

- Deployment Issues
- Configuration Issues
- Frequently Asked Questions on deployment and configurations

Deployment Issues

This section provides the following troubleshooting information:

Unable to discover WAN connection with VPNIP deployment

Unable to discover WAN connection with VPNIP deployment

Symptom

Unable to discover a WAN link with VPNIP between a Cisco and Juniper device with /30 subnet mask.

Possible cause

The IPNetwork must contain two IP addresses and have a /30 or /31 subnet mask.

When you create a VPNIP address, you are attempting to connect a Provider Edge to a Customer Edge device. The Provider Edge device must be aware of Route Distinguisher (RD) that provides the tag.

Recommended action

Use the MPLS VPN Tagging solution to discover a WAN link with VPNIP.

VPNIPNetwork is a subclass of IPNetwork. Standard connections are built using /30 subnet.

The rules/discovery/ic-post-wan-link.asl file provides more details on the logic of how the VPNIP connections are formed.

Configuration Issues

This section provides the following troubleshooting information:

Incremental reconfiguration entries were not displayed

False reports for voltage and temperature thresholds

NAS adapter was not supported in FIPS mode

Unable to connect to the broker in FIPS mode

Incremental reconfiguration entries were not displayed

Symptom

Incremental reconfiguration entries were not displayed in the domain log during discovery.

Possible cause

IP 8.1.x introduced incremental reconfiguration which displays reconfiguration entries in the domain log. If new devices are added to the topology, a full reconfiguration happens which is time consuming.

Recommended action

To enable incremental reconfigure, set ThresholdOfChangedUCSForIncReconfig 10 in the <BASEDIR>/smarts/conf/discovery/tpmgr-param.conf file. The value of this flag controls the maximum number of devices for which incremental reconfigure will run. For example, if the value is 10, incremental reconfigure will run if the number of the last discovered device is less then 10, otherwise a bulk reconfigure will run.

By default, ThresholdOfChangedUCSForIncReconfig parameter is set to 10 in tmpgr-param.conf file. Any discovery that contains less than 10 systems, the reconfigure started and reconfigure finished message will not be logged in the domain log. However, when reconfigure occurs, to view incremental reconfigure messages, set DebugReconfigure parameter to TRUE in tmpgr-param.conf file.

The tmpgr-param.conf file is located at:

```
<BASEDIR>/smarts/bin/sm_edit conf/discovery/tpmgr-param.conf
```

Restart the IP domain or reload tmpgr-param.conf for the change to take affect by running:

```
<BASEDIR>/smarts/bin/sm_tpmgr -s <IP 8.1.X domain> --load-conf=tpmgr-param.conf
```

To verify the ThresholdOfChangedUCSForIncReconfig setting run:

```
<BASEDIR>/smarts/bin/dmctl -s <IP 8.1.X domain> invoke ICF_TopologyManager::ICF-TopologyManager
findParameter ThresholdOfChangedUCSForIncReconfig
```

To change the parameter without restarting the IP domain run:

```
<BASEDIR>/smarts/bin/dmctl -s <IP 8.1.X domain> invoke ICF_TopologyManager::ICF-TopologyManager
insertParameter ThresholdOfChangedUCSForIncReconfig <value>
```

To debug the setting run:

```
<BASEDIR>/smarts/bin/dmctl -s <IP 8.1.X domain> invoke ICF_TopologyManager::ICF-TopologyManager
findParameter DebugReconfigure
```

False reports for voltage and temperature thresholds

Symptom

False reports were generated for voltage and temperature thresholds of a switch.

Possible cause

The voltage threshold was set to a range of 1 to 5, hence OutOfRange alarms were generated. Thresholds values were low as compared to the average switch threshold settings.

Recommended action

The threshold value will be same for devices in a particular group such as, routers, and switches. In most cases, the voltage value for switches will be in the range of 0 to 1.

Click the **Details** tab to verify if the notifications have values within the threshold range.

NAS adapter was not supported in FIPS mode

Symptom

Errors were seen in the NAS log while running NAS discovery in FIPS mode.

Recommended Action

If you want to switch back from FIPS mode to non-FIPS mode, reset SM_FIPS140 to False. You do not need to remove the Unlimited Strength Jurisdiction Policy Files. If you require FIPS support, you need to download additional JAR (Java Archive) files.

For example:

```
NAS Log Error Snippet:
MAIN_MSG-*-STDFD_OUT-stdout: javax.net.ssl.SSLException:
java.security.InvalidKeyException: Illegal key size
[June 17, 2011 6:37:49 PM GMT+05:30 +227ms] t@1084229984 platform MAIN_MSG-*-STDFD_OUT-stdout:
at com.rsa.sslj.x.aJ.b(Unknown Source)
at com.rsa.sslj.x.aJ.a(Unknown Source)
at com.rsa.sslj.x.aJ.b(Unknown Source)
at com.rsa.sslj.x.aU.d(Unknown Source)
at com.rsa.sslj.x.aU.a(Unknown Source)
at com.rsa.sslj.x.aU.h(Unknown Source)
at com.rsa.sslj.x.cI.startHandshake(Unknown Source)
at
com.smarts.nas_probe.ControlStationInterface.getSSLSocket(ControlSta
```

```
tionInterface.java:314)
at
com.smarts.nas_probe.ControlStationInterface.post(ControlStationInte
rface.java:75)
at
com.smarts.nas_probe.ControlStationInterface.getReply(ControlStation
Interface.java:58)
at com.smarts.nas_probe.XMP.NasXML(XMP.java:25)
Caused by: com.rsa.sslj.x.ax: java.security.InvalidKeyException:
Illegal key size
at com.rsa.sslj.x.aJ.b(Unknown Source)
at com.rsa.sslj.x.cR.k(Unknown Source)MAIN_MSG-*-STDFD_OUT-stdout: e
Caused by: java.security.InvalidKeyException: Illegal key size
at javax.crypto.Cipher.a(DashoA13*..)
at javax.crypto.Cipher.init(DashoA13*..)
at javax.crypto.Cipher.init(DashoA13*..)
at com.rsa.sslj.x.Y.<init>(Unknown Source)
......
```

With BSAFE SSL-J, some of the FIPS cryptographic algorithms require Unlimited Strength Jurisdiction Policy Files.

Download and install the Unlimited Strength Jurisdiction Policy Files to run the NAS adapter in FIPS mode by doing the following:

Versions starting at IP 8.1.2 use JRE 1.6, therefore go to, http://www.oracle.com/technetwork/java/javase/downloads/index.html http://www.oracle.com/technetwork/java/javase/downloads/index.html and download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6 from the Additional Resources section.

Extract the local_policy.jar and US_export_policy.jar files from the downloaded zip file.

Go to the <BASEDIR>/smarts/jre/lib/security directory and then backup the existing policy files in this path.

Overwrite the local_policy.jar and US_export_policy.jar files to the <BASEDIR>/smarts/jre/lib/security directory.

Unable to connect to the broker in FIPS mode

Symptom

After upgrading from IP 8.1.1 to IP 8.1.2, the IP server was unable to connect to the broker in FIPS mode. Also, the server could not be connected using both the dmctl and brcontrol commands.

Possible Cause

IP 8.1.1 does not use FIPS 140-2 approved encryption algorithm to protect imk.dat. Upgrades to non-FIPS mode work as expected.

Resolution

While upgrading from IP 8.1.1 to IP 8.1.2, the imk.dat file needs to be regenerated in order to run in FIPS mode. Further, IP 8.1.1 imk.dat file uses MD5, which is not a FIPS-approved algorithm. In order to convert an existing installation to FIPS mode, use sm_rebond in non-FIPS mode first to re-encode the algorithm and make it FIPS compatible.

Frequently Asked Questions on deployment and configurations

Deployment questions

Question

How many servers are needed to monitor an environment with 4000 devices? Should we use a Topology Split Server to handle this environment?

Answer

The main factor in deciding to split a topology is the number of managed ports or interfaces per domain and the polling interval and not the number of devices.

The secondary factors influencing the environment setup are :

- The solutions that are being positioned, such as IP Manager, Service Assurance Manager, Server Manager, ACM, or VoIP.
- The types of devices to be managed, for example, routers, switches, layer 3 switches, load balancers, servers, or virtual machines, and the device vendors in the environment, for example Juniper, Cisco, Dell, IBM, or VMware.
- The management requirements such as, operational monitoring, performance, or response times.
- The technologies used, such as IP L2/L3, MPLS L3 VPNs, L2 VPNs, or SANs.
- The networks that connect the managed devices, such as local, global, cities, T3 links, or metro Ethernet.
- The end users and end user locations, such as 24x7 monitoring, follow-the-sun, one NOC, multiple-NOCs, or managed service provider.

  To set up the environment calculate the percentage of routers and switches, and then the number of managed ports and interfaces. Refer to the IP and SAM deployment guides to choose the tiers and verify the hardware needed and platform desired. Allot an extra 30 percent for the growth of the network.

For example, if you have 4000 routers with 10 interfaces to be managed, it will generate 40,000 managed interfaces. You will need 2 CPUs and 4GB RAM per domain manager and no more than 20,000 managed ports and interfaces per domain manager, which means you will have at least 2 IP domain managers and hardware that can support up to 4 CPUs and 8GB RAM, which does not include SAM, OI or adapters. If you have more domain managers, then more CPUs and memory are needed.

If the environment is highly meshed, then you will need intelligent topology splitting. With only 4K devices, you do not need the topology split server. It is recommended to have a split based on geography or IP networks for a long term maintenance.

Configuration questions

Question

How is HighBufferMissThreshold calculated?

Answer

MemoryBufferMissThreshold is a configurable value in polling and threshold tab of system group in the processor and memory tab. The default value is 10 and it can be configured till 100.

All the configured values are directly taken as the upper threshold for the number of buffer misses and expressed as a percentage of the total number of buffer requests.

While calculating the event HighBufferMissRate, the value set in MemoryBufferMissThreshold will be used when:

The number of buffer misses that exceeded its threshold and if BufferMissThreshold is less than 100

Also, check if BufferMissPct is greater than BufferMissThreshold.

The event HighBufferMissRate indicates the rate of buffer misses that exceeds BufferMissThreshold.

Question

Can the trap exploder send traps to both BGP and receiver?

Answer

The trap exploder can send traps to both the BGP and the receiver. Traps can be sent to any destination.

Question

Does IP Manager distinguish multi-mode and single mode interfaces of a router? Also, does IP distinguish FPC types of routers?

Answer

IP Manager is based on an abstract model, hence it can be customized based on requirements such as polling status OIDs for different interface types.

Question

Where can we find details on SNMP Traps that can be used by the IP Manager?

Answer

The MIB's polled and traps processed section in the
VMware Smart Assurance IP Manager Reference Guide lists the SNMP Traps that are processed by correlation. Further, in the <BASEDIR>/smarts/rules/devstat/devstat-snmp-trap.asl file, the code for the processing traps and actions taken, such as, attributes changed can be found.

Troubleshooting Certification

11

Frequently Asked Questions on Certification

Certification questions

Question

How do I find out if a particular device is certified?

Answer

To do a field certification and validate the LLDP connections, invoke the LLDP framework by specifying the NEIGHBOR probe as LLDP in the configuration file oid2type_<vendor>.conf file.

Question

Where do I find details on the devices that are certified?

Answer

The IP Certification Matrix posted provides details on the devices that are certified. You can also run:

```
./dmctl –s <DM_NAME> get
ICF_TopologyManager::ICF–TopologyManager| grep <Sys_OID>
.1.3.6.1.4.1.9.1.947.2.2
./dmctl –s <DM_NAME> get
ICF_TopologyManager::ICF–TopologyManager| grep
.1.3.6.1.4.1.9.1.947.2.2
```

where .1.3.6.1.4.1.9.1.947.2.2 is the SystemOID.

If the command does not return a result, then device is not certified.

Question

Where can I find a database of Cisco Object IDs?

Answer

The following link provides details on Cisco Object IDs:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Click **ftp.cisco.com pub** > **Management (mibs)** > **OID subdirectory** > **Cisco-product-mib**.

Within this file, the device name can be found along with Object OID.

Question

What is the certification process of devices?

Answer

The vendor can go through the accreditation process in the VMware Velocity Partner program. Typically, it is managed by the Strategic Alliances team. Refer to a section of the program called Velocity ISV (Independent Software Vendor) Partner.

Question

How can I verify if a particular OID is certified?

Answer

You can verify the certification by running the below command before, and after you add a certification or remove a certification.

```
./dmctl -s duganm-ampm-703-2 get
ICF_TopologyManager::ICF-TopologyManager| grep .1.3.6.1.4.1.9.1.947.2.2
```

where. .1.3.6.1.4.1.9.1.947.2.2 is a sample OID.

Question

How can I find out all the OIDs used for discovery and monitoring of a device?

Answer

The OID Info tool introduced in the IP Manager and SAM Console versions 9.2 enable you to view the list of OIDs that are used to discover and monitor devices such as Host, Router, Switch, and so on. The OID information helps identify faults in the configuration of the SNMP agent of the device and displays the list of OIDs and their SNMP values for a device. It fetches the value of the OIDs from the device and compares the SNMP values against the values in the topology.

The “OID Info Tool” section in the VMware Smart Assurance IP Manager User Guide provides more information on configuring the OID Info tool, displaying OIDs in the command line and console, and sm_oidInfo modes of operation.

Troubleshooting Discovery, Performance and Monitoring

12

This chapter includes the following topics:

- Discovery Issues
- Performance and Monitoring Issues
- Frequently Asked Questions on Discovery, Performance and Monitoring

Discovery Issues

This section provides the following troubleshooting information:

Error messages for ASNMP related discovery errors (CQ 634137/CQ 634327/CQ 633581)

Cards were removed from devices in the topology after a rediscovery (CQ 557137/CQ 634165/SR43403952)

IP Manager Version 8.1.1 discovers less number of processors and more interfaces than IP 7.0.3

Delay during post-processing

Devices not detected during rediscovery

Devices deleted during rediscovery

Error messages for ASNMP related discovery errors (CQ 634137/CQ 634327/CQ 633581)

Symptom

Devices are discovered partially and added into the pending list.

Possible cause

There can be an ASNMP request failure during discovery.

You can confirm that by looking into the "Description" field of the pending list (AD_PendingData):

If it shows any one of the following or both the error messages in the "Description" field of the pending list (AD_PendingData) , then this is due to any ASNMP error occurs during discovery:

```
"ASNM-E-ASNMP_SEND_RECEIVE_ERROR-ASNMP request failure: Error when sending or receiving SNMP data for
Host '<IP address of the device>' (Maybe bad credentials)."
"ASNM-E-ASNMP_SNMP_ERROR-ASNMP request failure: Error <Error Code>: <Error Message> when receiving
SNMP Packet from '<IP address of the device, port<port number>'"
```

Recommended action

ASNMP is faster than Synchronous SNMP, since requests are fired without waiting for a response. But it may possible that some of the devices will not be able to respond to an ASNMP request. To resolve this issue use one of following options:

1 Set EnableASNMPForMIB2 in the <BASEDIR>/smarts/conf/discovery/tpmgr-param.conf file to FALSE to disable asynchronous requests for all devices.

2 To disable ASNMP for a particular device, and not for all the devices, use DoNotUseASNMPPattern in the tpmgr-param.conf file.

3 DoNotUseASNMPPattern will allow you to disable asynchronous requests only for specific devices by sysOID. If you want to disable ASNMP for multiple devices, add the sysOID entries separated by |

4 maxOIDsPerPacketForASNMP flag in tpmgr-param.conf file configures the maximum number of OIDs/packet that can be sent using ASNMP. The default value is 19. You can decrease the number of OIDs.

5 SingleOIDPerPacketForASNMPPattern in the tpmgr-param.conf file allows you to disable the sending of multiple OIDs/packets using asynchronous requests only for specific devices using sysOID. You can add the list of sysOID entries separated by |.

Cards were removed from devices in the topology after a rediscovery (CQ 557137/CQ 634165/SR43403952)

Symptom

Cards were removed from devices in the topology after a rediscovery. For example, on initial discovery, the Cisco router displayed both cards in the topology (Card A and Card B). Now when the card A was removed from the device and then a rediscovery performed on the router, both the cards were removed from the topology.

Possible cause

Cisco uBR10012 (SysOID: .1.3.6.1.4.1.9.1.317) does not have the framework to support the auto switchover feature. There is currently no resolution.

IP Manager Version 8.1.1 discovers less number of processors and more interfaces than IP 7.0.3

Symptom

Less number of processors and more interfaces are discovered in IP 8.1.1 when compared to IP 7.0.3.

Possible cause

In earlier releases, processors were created by polling the values from hrDeviceDescr and the processor utilization was taken from the UCD-Mib for all the processors created. Thus CPUs were created for Hosts in huge numbers. In IP 8.1.1, processors are created from the Host-resources-MIB, based only on the polled values of hrProcessorLoad. If hrProcessorLoad does not populate a value, then the processors are created based on the values from ssCpuIdle(UCD-Mib). If no data is populated for hrProcessorLoad (Host-Resources-Mib) and ssCpuIdle(UCD-Mib) has an entry, only a single CPU will be created for many hosts. More interfaces seen in IP 8.1.1 may be because of the NIC teaming feature, which is enabled by default. However, if many Host SNMP agents are slow, on querying the NIC teaming OIDs, the agents may stop responding which may result in a partial discovery. If you are not using the NIC teaming feature, disable it by setting EnableTeamedNICDiscovery to False in the <BASEDIR>/smarts/conf/discovery/tpmgr-param.conf file and then verify.

Further, ASNMP for specific devices may be timing out due to which the devices are added to the pending list. The devices will either go to the pending list or it will get discovered partially with a message, "SNMP request timed out or had an error".

Recommended action

To resolve this issue, reduce the maxOIDsPerPacketForASNMP value to less than 19 or disable ASNMP for the devices by setting the DoNotUseASNMPPattern flag in the <BASEDIR>/smarts/conf/discovery/tpmgr-param.conf file to True. Then restart the server and rediscover the topology.

Delay during post-processing

Symptom

While running several discoveries there was a delay during post-processing to complete before starting another discovery.

Possible cause

Discovery of the new device happens after the postprocessing of already discovered devices.

Recommended action

To disable the post processor, set PostProcessingEnabled flag to False using dmctl in the ICF_TopologyManager::ICF-TopologyManager class.

To start post-processing, run:

```
sm_tpmgr option --start-post
```

Devices not detected during rediscovery

Symptom

Devices that need to be rediscovered are not placed in the pending list..

Possible cause

The IP domain was not configured to receive ConfigChange traps.

Recommended action

In the <BASEDIR>/smarts/conf/discovery/tpmgr-param.conf file:

- If the EnableConfigChange flag is set to True, the ConfigChange event will add the device to the pending device list.
- If the EnableSystemRestart flag is set to True, the SystemRestart event will add the device to the pending device list.

Devices deleted during rediscovery

Symptom

Devices with common MAC addresses were deleted during rediscovery. These devices were discovered successfully during the initial discovery.

Possible cause

If devices share the same MAC address, both devices will get deleted.

Recommended action

Set the rigorousMACTest parameter to True in the <BASEDIR>/smarts/conf/discovery/tpmgr-param.conf file. The rigorousMACTest flag tests for duplicate MAC addresses of the devices.

The parameter can be set using one of the following commands:

```
./sm_tpmgr -s DCN-TSM-APM --load-conf=tpmgr-param.conf
```

or

```
./dmctl -s DCN-TSM-APM-after get ICF_TopologyManager::ICF-TopologyManager | grep rigorousMACTest
```

Set the parameter and restart the server before further discovery.

Performance and Monitoring Issues

This section provides the following troubleshooting information:

Switches were not correctly building the cable connections to multiple hosts

Unable to remove devices from pending list (CQ 634159)

ASL-W-ERROR_RULE_SOURCE error upon starting IP Manager

ASL error during discovery of IPv6 address in IP 8.1.2

Setting the PartitionEnabled parameter

Updating the Availability Manager partition

Switches were not correctly building the cable connections to multiple hosts

Symptom

Switches were not correctly building the cable connections to multiple hosts.

Possible cause

This issue occurred because the ports were bridging more than one MAC address.

In an ideal scenario, connections will be formed only when a port is bridging only one MAC. In this particular case, a port is bridging two MACs out of which one is stale.

Recommended action

To remove the stale MAC, set the PruneSystemlessMAC parameter to TRUE in the <BASEDIR>/smarts/conf/discovery/tpmgr-param.conf file. This parameter is used to enable or disable pruning of Systemless MAC addresses.

Unable to remove devices from pending list (CQ 634159)

Symptom

The IP address of devices in pending list were reported as 0.0.0.0 and it was not possible to remove the devices from the list.

Possible cause

One of the reason can be, during discovery of the device the probing was unsuccessful due to ASNMP error and the device was added to the pending list. This entry was added in the pending list due to FAIL_PROBE error in the ic-mib2-hyper-data.asl file.

You can confirm that by looking into the "Description" field in the "Pending List(AD_PendingData)".

In this case the "Description" will have one of the following or both the error messages:

"ASNM-E-ASNMP_SEND_RECEIVE_ERROR-ASNMP request failure: Error when sending or receiving SNMP data for Host '<IP address of the device>' (Maybe bad credentials)."

"ASNM-E-ASNMP_SNMP_ERROR-ASNMP request failure: Error <Error Code>: <Error Message> when receiving SNMP Packet from '<IP address of the device, port<port number>'"

Recommended action

Refer to Error messages for ASNMP related discovery errors (CQ 634137/CQ 634327/CQ 633581) the recommended action for this issue.

ASL-W-ERROR_RULE_SOURCE error upon starting IP Manager

Symptom

The following ASL errors were observed when the IP Manager was started:

```
ASL-W-ERROR_RULE_SOURCE-While executing rule set
'C:\InCharge\IP\smarts\rules\health\health-init.asl'
ASL-ERROR_ACTION-While executing action at:
ASL-CALL_STACK_RULERuleName: INITIALIZE_SETTINGS, Line: 172
ASL-CALL_STACK_RULERuleName: START, Line: 34
ASL-ERROR_GETINSTANCES-While attempting to get the instances of class
'System_Environment_Setting' MR-CLASS_NOT_FOUND_EX-Cannot find class
'System_Environment_Setting'; in file "t:/DMT-9.0.0.X/1352/smarts/repos/servif/SM_RepositoryServer.c"
at line 515
```

Recommended action

Run:

```
$ ./dmctl.exe -s INCHARGE-AM-PM
```

When attached to INCHARGE-AM-PM run:

```
dmctl> invoke ICF_PersistenceManager::ICF-PersistenceManager save
dmctl> invoke ICF_PersistenceManager::ICF-PersistenceManager save
dmctl> exit
```

Then stop the server and restart to resolve the issue.

ASL error during discovery of IPv6 address in IP 8.1.2

Symptom

While running a discovery, the following error was displayed in the Availability Manager log:

```
ASL-W-ERROR_RULE_SOURCE-While executing rule set '/opt/InCharge/IP/smarts/rules/discovery/ic-name-
resolver.asl'
ASL-ERROR_ACTION-While executing action at:
ASL-CALL_STACK_RULE- RuleName: MODIFY_IP_PARAMS, Line: 1424
ASL-CALL_STACK_RULE- RuleName: SET_PROPERTIES, Line: 1375
ASL-CALL_STACK_RULE- RuleName: EOF, Line: 320
ASL-ERROR_PUT-While attempting to set property 'Tag' of object 'IPv6::IPv6-2001:1890:1226:41:0:0:0:1'
MR-PROPERTY_NOT_FOUND-Specified property 'Tag' not found in class; in file
"/work/blackcurrent/DMT-9.0.0.X/1304/smarts/repos/mr/classdef.c" at line 2455
```

Possible cause

There was no tag property in the IPv6 class. The tag property was removed in the underlying IPv6 class definition.

Recommended action

Avoid usage of tags in IPv6 address objects.

Setting the PartitionEnabled parameter

Symptom

Unable to set the PartitionEnabled parameter in the ic-post-partition.asl file.

Possible cause

Each discovery system will be displayed in one partition. A partition represents a connected (L2 and L3) network.

If a system has no neighbor or if a system is unsupported or unmanaged, the device will become a part of its own partition and will be the only device in the partition.

Recommended action

To disable a partition:

1 Set the parameter PartitionEnabled to False in the discovery.conf file and start the server.

2 If server is running, disable the server before discovery using the following command:

```
./dmctl -s INCHARGE-AM-PM put ICF_TopologyManager::ICF-TopologyManager::PartitionEnabled FALSE |
tee
```

3 Verify if the server is disabled using the below command:

```
./dmctl -s INCHARGE-AM-PM get ICF_TopologyManager::ICF-TopologyManager::PartitionEnabled | tee
FALSE
```

The file ic-post-partition.asl performs post-processing on created partitions. By default, partitions are created during discovery unless it is disabled manually.

Updating the Availability Manager partition

Symptom

When devices that are not attached to the parent network are added to the topology, the details of the partition are not updated in the topology.

Possible cause

IP Manager does not create partitions for single devices, hence devices that are not connected to any other device will not be considered as a partition. Conceptually, partition is a group of inter-connected devices.

Recommended action

No action is possible. Modifying the partition.conf file does not solve this because the partition.conf file is used to name a partition that is created and not create a partition.

Frequently Asked Questions on Discovery, Performance and Monitoring

Discovery questions

Question

Will IP Availability Manager discover and build logical connections for connecting a sub-interface such as, VLAN sub-interface?

For example, for a physical connection between two interfaces, with each interface having sub-interfaces that carry the traffic of VLANs, will the IP Availability Manager discover both physical and sub-interfaces?

Answer

Only the physical network connection will be discovered and created.

Question

What is the purpose of the autoVlan option in the sm_snmpwalk command?

Answer

The autoVlan option automatically walks through the VLAN configuration. This option works on Cisco device only.

For example:

```
sm_snmpwalk.exe  --autoVlan --vlanoidfile=<file>
```

or run:

```
./sm_snmpwalk --help
```

For details on the autoVlan option, see:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_configuration_example09186a008015773e.shtml
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_configuration_example09186a008015773e.shtml
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_configuration_example09186a008015773e.shtml

Question

How to poll routers with a specific Cisco MIB?

Answer

Add the attributes to the interface object within the dynamic model that is populated from the SNMP accessor.

Question

We already have a tool for discovery and want to keep it as a source for monitoring. Would it import the information into the IP Manager?

Answer

Most toolsets will not discover all the information and connectivity that is needed by the IP Manager. However, an external tool can be used for discovery by using the seed file from the tool to perform discovery using the IP Manager.

Question

How do we stop the IP Manager from creating the NetworkConnection relationship?

We have an ADSL service from a Internet Service provider with routers connected using different subnets. Some of the subnets have two ADSL routers and IP Manager creates a NetworkConnection which we do not require. The ISP cloud is in between the edge router and the ADSL routers which exist in the same /23 subnet and has a NeighboringSystem relationship.

Answer

It is not possible to stop the IP Manager from creating the NetworkConnection relationship.

A network connection is a connection between two interfaces. A network connection can be a logical connection or a physical connection. An example of a logical connection is when routers are connected using a virtual circuit and none of the intermediate network devices are included in the topology. An example of a physical connection is when routers are connected using a serial or point-to-point connection.

In this case, the Internet Service Provider places the ADSL routers in the same subnet. IP Manager does not discover routers in the Internet Service Provider cloud. When it discovers the ADSL routers which have no relationship, the NetworkConnection and NeighboringSystem relationships are created.

Question

How to override the default behavior of not generating a Down notification for a dial-on-demand interface which is in Admin UP Oper Down state?

Answer

IP does not allow you to override the default behavior of not generating a Down notification for dial-n-demand interfaces. If you would like to see Down alerts for those interfaces, they need to be removed from the interface group that has dial-on-demand setting.

Question

During discovery of a single Juniper Router, the following three router instances were created:

lwq3s002.lss.vmware.com

lwq3s002.lss.vmware.com/16.1.0.0/LCC0

lwq3s002.lss.vmware.com/16.2.0.0/LCC1

The SysOID for the device is .1.3.6.1.4.1.2636.1.1.1.2.17

All the three routers have the same IP address and are not performing an OpsMgr integration. How to avoid this situation?

Answer

The device that was discovered is a TX Matrix. The TX Matrix consists of one switch card chassis (SCC) and up to four line card chassis(LCC0-4- each one being a T-640). The entire setup behaves like a huge router with the SCC being central, and each LCC can operate as a separate router when it is not part of a matrix. This behavior is normal and also a similar matrix is displayed while discovery of T-1600s.

Performance and monitoring questions

Question

What is the dmdebug command to receive queues output?

Answer

The dmdebug --queues command prints information about all server queues in the system. For example:

```
SubscriberFE                                          [0 worker]
Current size 0, max 369; processed entries 21843
Size           0–0.00            0–0.00            0–0.00             0–0.00
Flow       21839+0.06        21803+0.05        21446+0.05         17895+0.06
Late      0.0000+0.00       0.0000+0.00       0.0000+0.00        0.0000+0.00
```

Question

Can you define the sm_adapter parameters, --loglevel, and --errlevel? What are the allowed values for these parameters?

Answer

Most messages printed by the VMware code uses the exception logging mechanism. The exception logging mechanism sends messages to one of the following two receivers:

- Log files
- System error logger, which is the syslog mechanism on Unix systems.

  The exception logging mechanism is controlled by the severity level. The severity level is assigned to the message being logged. A message can have one of the following severity levels:

- Fatal
- Error
- Warning
- Notice
- Informational
- Debug

  You can assign the minimum severity level for messages to be sent to a receiver. By default, the log file receives severity warnings, and the system error logger receives severity errors. The following are the standard options that are available with VMware main programs:

- --errlevel: controls the minimum level for writing into the log file
- --loglevel: controls the minimum level for sending errors to the system logging facility

  Use --help to set the severity levels as a value for the above options. Set the severity level to None to completely disable a particular receiver.

Question

Can we use ASL to create or write a ACT_FILE file outside the logs directory?

Answer

ASL cannot be used to create or write a ACT_FILE file outside of the logs directory.

Question

Can a device be displayed in both the topology and pending list?

Answer

Yes, devices can be displayed in both the topology and on the pending list. Device existing in the topology can be placed on the pending list if it does not reply to ICMP or SNMP request during rediscovery, or a coldStart, and also if reconfigure traps have been received for the device.

Question

Why does IP Availability Manager ping all the HSRP Endpoints as a part of monitoring? Can we set the HSRPEnabled to True and stop the ICMP ping monitoring?

Answer

The HSRP Endpoints pings are essential for computing the IsVirtualIPUnresponsive attribute.

All the IP addresses which are part of HSRP Endpoints are considered to be Virtual IP addresses. The classification is due to its behavior of being associated to more than one system.

The only way to restrict the ping is to unmanage the underlying IP address in the HSRP Endpoint. By unmanaging the IP address, the instrumentation object is removed and the ICMP ping does not occur.

If there are many IP addresses to be unmanaged, a script can be written to unmanage only those IP addresses which are part of the HSRP Endpoints.

The event computation of SwitchOverFailed event will have an impact due to the dependency on the attribute IsVirtualIPUnresponsive.

Question

How to recover the list of devices that were not discovered by TSM and reason for the discovery not happening? The discovery was performed using a seed-file.

Answer:

Use the command sm_tpmgr to recover information on devices that were not discovered. For example:

```
sm_tpmgr -s INCHARGE-AM --status
Last Status Message: Last discovery completed at 24-Jan-2011 11:48:36 AM EST
Discovery Queue Size: 0
Discovery Pending List:
```

```
Host-abc [community='',reason='No response from SNMP agent, AUTODETECT, SNMP-E-ERESPONSE-No response
from 10.29.12.1, port 161
SNMP-ETIMEOUT-Timed out']
B9230558D [community='',reason='No response from SNMP agent, AUTODETECT, SNMP-E-ERESPONSE-No response
from 10.29.5.129, port 161
SNMP-ETIMEOUT-Timed out']
```

General Troubleshooting

13

This chapter includes the following topics:

- General Issues
- Frequently Asked Questions

General Issues

This section provides the following troubleshooting information:

Unusual growth in log file size

Disabling VLAN impact propagation through GUI or dmctl (CQ 634074)

IPv6 network connection was not displayed using 64 prefix for Juniper routers (CQ 634160/ CQ 634161)

IP server crashed on the failover/secondary host (CQ 634162)

Devices sharing a common MAC address were overwritten/deleted

IP Manager hangs after pstack or stacktrace (CQ 575017/CQ 553871/CQ 582036/SR43006286)

Incorrect layering of ATM interfaces resulted in erroneous notifications

Multiple user-defined-connections.conf files

VPN tagging issue

Virtual IP scenario not generating device down event

Adding or removing hosts

Keepalive issues through firewall

ConnectedVia relationship in ASL

IsManaged issue

Server tools issue

Etherchannel interfaces in Availability Manager and Performance Manager

String concatenation in dynamic models

Disabling polling in IP 8.1.2

Unusual growth in log file size

Symptom

A huge growth was seen in the log file size.

Recommended action

If you see a huge growth in the log file size, for instance in the broker log, do the following:

- Re-install the broker as service with environment setting SM_NO_LOG_CLIENTS=TRUE.
- Restart the broker service.

Note If you want to disable the client logging feature subscription for all the servers or domain managers, put the entry in the runcmd_env.sh file, and then restart the broker and domain managers.

Disabling VLAN impact propagation through GUI or dmctl (CQ 634074)

Symptom

When two switches A and B are part of one VLAN, for example, VLAN1, and if switch A becomes UnResponsive, then a switch A Down event is generated. The Impact tab of the Notification Properties window displays both the switches A and B.

Possible cause

The attribute isImpactPropOverVLANEnabled of a VLAN decides whether a VLAN should take part in an impact propagation or not. Because this attribute is set to True by default for all VLANs, all VLANs takes part in the impact propagation. Devices sharing the same VLAN may have an impact on each other. However, you may want to prevent the impact propagation through some VLANs, such as management VLANs and default VLANs.

Recommended action

To disable VLAN impact propagation from GUI, do the following:

1. Select the particular VLAN listed in the VLAN group in the **Domain Manager Administration Console**.
2. Select the attribute **isImpactPropOverVLANEnabled** in the **Attributes** tab.
3. Change the value from true to false.
4. Click, **Apply** and then perform a reconfigure using the following dmctl commands:

```
./dmctl.exe -s <server-name> -b <broker> put VLAN::<Name parameter of that particular
VLAN>::isImpactPropOverVLANEnabled FALSE
```

For example,

```
./dmctl.exe -s xxx_IP813 -b localhost:9740 put VLAN::VLAN-RSP-1::isImpactPropOverVLANEnabled FALSE
```

VLAN impact can be disabled using Problem Impact propagation policy over VLANs setting. Problem Impact Propagation policy over VLANs section in VMware Smart Assurance IP Manager User Guide, provides more information about this setting.

Note It is recommended that you disable VLAN impact propagation using either the Problem Impact propagation policy over VLANs setting or through the steps mentioned above. Do not use both the options to disable VLAN impact propagation at the same time.

IPv6 network connection was not displayed using 64 prefix for Juniper routers (CQ 634160/ CQ 634161)

Symptom

A network connection was not created when using 64 prefix for IPv6 Juniper routers.

Possible cause

When IPv6 IP addresses uses 64 bit prefix length, then the interface overlaying this IP address will not be considered for connection creation due the ping-pong issue, neighbour cache exhaustion (denial of service).

Other technical reasons for not using 64bit prefix length can be found at the following location.

http://tools.ietf.org/id/draft-kohno-ipv6-prefixlen-p2p-01.html#Recommendations

Recommended action

The current design of IP is to a create network connection only for interfaces underlying IPV6 with a prefix length configured to 126 or 127. You should avoid configuring the prefix with 64 bit length.

IP server crashed on the failover/secondary host (CQ 634162)

Symptom

Failover to secondary host did not work and IP domain crashed.

Possible cause

The shutdown was executed via sm_service stop without being logged in as root.

Recommended action

The issue is resolved in IP 8.1 and in IP 8.2. A crash might occur in the versions prior to IP 8.1. It is advised to stop the sm_service only as a root user of the system.

Devices sharing a common MAC address were overwritten/deleted

(CQ 553751/CQ 634164)

Symptom

Devices sharing a common MAC address were overwritten or deleted even after the RigorousMACTest flag was set to TRUE.

Possible cause

When multiple devices that are configured in a VM environment and when all the devices are assigned MAC addresses from a common MAC pool, they share a common MAC address. The IP Manager considers devices sharing common MACs as duplicates and overwrites the existing device with a new device.

Recommended action

1 Add the common MACs under the invalidMACPattern parameter in the ./sm_edit conf/icf/DISCOVERY.import file to exclude the creation of the virtual MAC addresses.

The default invalid MAC pattern included are as follows:

invalidMACPattern = {"000021000000|0000000100*|*0000000000|FFFFFFFFFFFF","00000C07AC*"}

The higlighed MAC patterns are the ones which are being added in the following example:

invalidMACPattern = {"001243DC6F02|001B245C3EC2|001B24F053EC|001E6804C04E|001E6804C05A|001E6804C072|001E6804C976|001E68AA0D5C|001E68AA0D62|001E68AA0D6E|00238B0376B9|00238B0376BF|00238B0376E9|00238B0376FE|00238B037704|00238B03770A|00238B037716|00238B03771C|00238B037722|00238B03775E|00238B03764D|000021000000|0000000100*|*0000000000|FFFFFFFFFFFF","00000C07AC*"}

Add the MAC address to the beginning or end by appending a Pipe(|) symbol or use a regular expression.

Note The above changes require a server restart for the changes to take effect.

2 Use the command sm_edit conf/discovery/tpmgr-param.conf to set RigorousMACTest to True. This will ensure that there is an unique set of MAC addresses between the discovered devices.

The default value is RigorousMACTest FALSE

Note The above scenario is applicable only for devices which are configured under a Virtual Machine such as the Cisco LoadBalancer.

IP Manager hangs after pstack or stacktrace (CQ 575017/CQ 553871/CQ 582036/SR43006286)

Symptom

The IP Manager hung after pstack or other stacktrace was executed. This occurred if sm_monitor was run with low disk space.

Possible cause

The issue occurs because the stacktrace (-z parameter) results in verbose logging and a possible hang condition.

Recommended action

The sm_monitor is a debugging tool that is invoked on demand. Before executing the debugging activity, add more disc space or free up some disc space before running sm_monitor or set the SM_WRITEABLE = path (different partition with sufficient disk space) when starting the server, so that all the logs and the sm_monitor data is redirected to that path instead of the default local/logs directory.

If the server goes into a Traced state, free up some disc space and send CONT signal (Kill - CONT pid) to resume the process from where it left off.

Incorrect layering of ATM interfaces resulted in erroneous notifications

Symptom

The Root Cause Analysis (RCA) did not function when there was a custom setting for managing the AAL5/ATM subinterfaces.

Possible cause

As per the design, IP unmanages certain AAL5|ATM subinterfaces interfaces in ic-post-port-manager.asl file. This is done to produce proper Root Cause Analysis. In this case, these unmanaged interfaces were managed explicitly by the user script. This resulted in an incorrect RCA of Interface::Down for the AAL5 interface that was explicitly managed by the user but the actual problem was Router DOWN. When the underlying AAL5/ATMSUBINTERFACE interfaces are managed, IP Manager has an additional symptom set to deduce the AAL5/ATMSUBINTERFACE as DOWN instead of arriving to Router DOWN.

Recommended action

When you expect a router DOWN event, the custom management policy for the AAL5/ATMSUBINTERFACE must be removed.

Multiple user-defined-connections.conf files

Symptom

Unable to add additional user-defined-connections.conf to enable dynamic user-defined-connections.conf files and not interfere with the default user-defined-connetions.conf.

Possible cause

You can create many user-defined-connections.conf files, but presently the code defines one file.

Recommended action

To run two different user defined connections files in post-processing, some code changes are required in the installation.

VPN tagging issue

Symptom

When devices are imported to a system using a seedfile, the IP Manager addresses are configured as LAN addresses on other devices, the old IP address of the devices are deleted and the devices are not managed.

Possible cause

Whenever an IP address is classified as an Duplicate IP address, it is removed from the AgentAddressList ,hence the device will not be discovered using the same IP address. IP Tagging feature does not allow the IP address to be listed in the AgentAddressList, but allows the end-user to identify the IP addresses that are shared across networks or devices.

When a management IP address is classified as a Duplicate IP, it will be removed from the AgentAdressList and the device rediscovery will select any available IP address from the AgentAddressList. The DuplicateIP address cannot be used as management IP, the Management IP has to send or receive packets and wont be able to determine the source of the packet even after using the tag. An overlapping IP address is unreachable as no routes exist between the host running on the IP Manager and the overlapping IP address.

Recommended action

An overlapping IP address is on a client-side physical interface of a router or switch and is managed by a Managed Service Provider (MSP). The MSP discovers the router, its interfaces and IP addresses, but does not discover the client equipment that is accessible through the overlapping IP address.

The inclusion of the overlapping IP addresses in the modelled topology allows the MSP to observe the status of the client equipment associated with the overlapping IP addresses, which enables the MSP to respond immediately to customer outages.

When the VPNIP parameter is set to True, VPNIP and VPNIPNetwork objects are created, instead of tagged IP under the IP class.

Virtual IP scenario not generating device down event

Symptom

Unable to check if an IP address in a cluster with two virtual IP address nodes is marked as virtual or not.

Possible cause

Virtual IP address is an IP address that is not connected to a specific computer or Network Interface Card (NIC) on a computer. Incoming packets are sent to the VIP address, but they are redirected to physical network interfaces. Once an IP is classified as a Virtual IP, it is removed from the agent address list and will not be used to monitor the device.

Recommended action

Virtual IP addresses are mostly used for connection redundancy. For example, in the case of HSRP, an HSRPEndPoint is a virtual IP address and the properties tab describes the virtual IP address used by that end point. In some cases the ifdescr command can also be used to determine whether it is a Virtual IP.

Adding or removing hosts

Symptom

Unable to add and remove hosts in SAM topology browser.

Possible cause

Devices are not added in an ad-hoc manner. They are discovered by the Availability Manager, and the Service Assurance Manager server subscribes to the topology and notifications that are managed by the Availability Manager . Discovery can be seeded, ad-hoc, or automatic using filters.

Devices first need to be removed from IP domain and then they will automatically be removed from SAM after topology synchronization completes. If you have deployed the OI domain or any other analysis domain that subscribes to the IP domain, then those domains need to synchronize their topology with IP Manager and Service Assurance Manager to completely remove the device.

Recommended action

The VMware Smart Assurance IP Manager User Guide provides more information on adding and removing hosts.

Keepalive issues through firewall

Symptom

When VMware Smart Assurance domain communicates using a firewall, such as Cisco ASA some known issues were encountered. The packets were not discarded, but the domains were constantly disconnecting and reconnecting.

Recommended action

You need to allow the firewalls to pass the data packets by turning the keep alives off in the VMware Smart Assurance servers and consoles. This approach is not recommended because it can result in memory leaks if connections are brought down badly.

ConnectedVia relationship in ASL

Symptom

Unable to list the ConnectedVia, ConnectedTo or PartOf data using ASL.

Recommended action

You can remove the inner loop in the ConnectedVia relationship and treat the return value of pObj->ConnectedVia as an object handle.

```
foreach probe (getInstances("Probe")) {
    pObj = object("Probe", probe);
    foreach ipNet (pObj->ConnectedVia) {
// This returns all of the objects in the ConnectedVia relationshipset
        if (ipNet->CreationClassName == "IPNetwork") {
            print(probe . " is ConnectedVia ".ipNet);
        }
    }
}
```

IsManaged issue

Symptom

During discovery of switches, the interfaces are displayed as IsManaged and are certified upon discovery.

Some ports were displayed as IsManaged = False, and the rest were displayed as IsManaged = True. The ports were configured in the UP/UP state before discovery.

Possible cause

By default, if a port has no device connected to it or is not managed by IP Manager then it is automatically is set to the unmanaged state and the port does not create unnecessary notifications.

If there are servers or other devices connected to these ports, then the devices have to be discovered, or the managed status of these ports will be set to managed in the post discovery script.

Recommended action

Check if the devices connected to the ports are discovered.

Server tools issue

Symptom

Escalation policies were set to run automatic server tools which sends texts or emails to various recipients. Only the first notification of an event invokes the tool, until the notification is archived.

Recommended action

Use the following escalation policies and tag values in user defined fields:

- The escalation policy triggers the following conditions and executes the automatic tool:

  ```
  STATUS == ACTIVE
  USERDEFINED != TAG
  ```

- The escalation policy triggers the following conditions and clears out the tagged field:

  ```
  STATUS == INACTIVE
  USERDEFINED == TAG
  ```

  If the notification becomes active again, the criteria for the first escalation policy are met and the automatic tool will be invoked.

Etherchannel interfaces in Availability Manager and Performance Manager

Symptom

Etherchannel port channels on several switches were created to alleviate bandwidth congestion and allow monitoring of port channels instead of single interfaces that comprise of portchannels. During rediscovery, the devices and new portchannel interfaces were not displayed.

Possible cause

If the port channels are not displayed in the topology, then they are not supported by VMware Smart Assurance.

Recommended action

It is suggested to provide a certification request.

You can create your own objects in the NetworkAdapterRedundencyGroup that contains each interface as a member. You can use dmctl, asl, perl, or java APIs. The console filters can be used to ignore alarms on the individual interface, but they display alarms in the groups.

String concatenation in dynamic models

Symptom

Unable to concatenate strings in a dynamic model.

Recommended action

Use the following command:

```
DisplayName = Address . " [" . BladeName . "]"
```

Disabling polling in IP 8.1.2

Symptom

Unable to disable polling in IP 8.1.2

Recommended action

To disable SNMP monitoring run:

```
./dmctl -s <server name> put SNMP_AccessorInterface::DEVSTAT-SNMP-Poller::suspendMonitoring TRUE
```

To disable ICMP Polling run:

```
./dmctl -s <server name> put ICMP_AccessorInterface::DEVSTAT-IP-Pinger::suspendMonitoring TRUE
```

Frequently Asked Questions

General questions

Question

List the SNMP Traps that can be used by the IP Manager?

Answer

The MIBs polled and traps processed section in the
VMware Smart Assurance IP Manager Reference Guide lists the SNMP Traps that are processed by correlation. Further, in the file <BASEDIR>/smarts/rules/devstat/devstat-snmp-trap.asl, the code for the processing traps and actions taken, such as, attributes changed can be found.

Question

How to open a ticket on Powerlink?

Answer

In Powerlink, select **Support**> **Request Support**> **Create Service Request**.

Question

What happens if the access to disks fails when the repositories are written on the disk?

Answer

This depends on the Operating System and Hardware level resilience. If the system recovers, then the RPS would be re-written during the next reconfiguration. This process can also be done using dmctl.

Question

Does the IP Manager lock the physical memory or paged memory of the Operating System?

Answer

IP Manager locks memory of the operating system using memory allocator.

Question

Is it possible to know the memory used by the codebook of a Domain Manager?

Answer

It is not possible to determine the memory used by the codebook.

Question

What is the time taken by a Domain Manager to generate a new codebook?

Answer

Run the following command:

```
sm_tpmgr --show-dm-processes
```

The output contains the codebook generation duration (NewMatrix), correlation time in seconds. The new codebook is swapped once it is generated, the domain manager runs the old codebook until the new codebook is generated.

NewMatrix < 10 secs is "Good"; NewMatrix = 10-30 secs is "Acceptable" and NewMatrix > 30 secs is "Bad"

Correlation = 0 secs is "Good"; Correlation < 20 secs is "Acceptable" and Correlation > 20 secs is "Bad"

The fix for "Bad" is to split topology, or run a CPU with higher speed.

Question

Do we support layer 2 port channels?

Answer

As of now we do not support layer 2 port channels.

Question

What does DeviceID specify in the OID2Type files. For example:

Environment = DellOpenManageEnvMon:DeviceID

Answer

DeviceID informs the SNMP accessor to poll the Environment OID specified.

Question

What is the naming convention of a DuplicateIP object?

Answer

The name of DuplicateIP object will have a prefix, IP-. For example, DuplicateIPv6, the naming convention is "IPv6-".

Question

Which MIB-2 oid is used to populate the value of layered over and underlying? What is the logic used to populate the attribute values?

Answer

The following OID is used for creating the layering relationship for network adapters:

ifStackOID { ".1.3.6.1.2.1.31.1.2.1.3" }

Indexes:

ifStackHigherLayer

ifStackLowerLayer

The MIB-2 OID provides information on a particular relationship between two sub-layers, specifying that one sub-layer runs on top of the other sub-layer. Each sub-layer corresponds to a conceptual row in the ifTable.

The file ic-ifmib-stack.asl is responsible for creating the layering.

Question

Does TSM delete a device everytime it is rediscovered? How can this be prevented?

Answer

Devices are deleted by TSM during:

- Name resolution when:
  - Two devices map to the same name, the existing topology device gets deleted.
  - Two IP addresses in the seedfile map to the same device, then the existing device gets deleted.
- When two devices have the same IP address and MAC addresses then auto-discovery deletes the existing device.

Question

Is there a document that specifies VMware Smart Assurance device naming convention and limitation, such as maximum length and special characters?

Answer

The VMware Smart Assurance IP Manager Reference Guide provides more information on VMware Smart Assurance naming conventions.

The name of the device has no limit in terms of size. The name of a device is an attribute and can use a lot of memory. The name is referenced in all relationships in the repository that has a reference to the instance. You can customize the DisplayName.

Question

Insight Manager displays alerts on hard drive health based on predictive S.M.A.R.T failure data. IP Manager monitors the same servers but does not issue any events.

Can we add such an event to IP Manager directly or using Dynamic Modeling?

Answer

HP Insight Manager forwards traps to the trap adapter and the traps are then converted to alerts. Dynamic model can be used to allow the IP Manager to define problems and events for drive health. If you want to poll for data, extend the discovery process with probes for the MIBs that cover drive health.

You can extend IP Manager with dynamic model to define the new problems and events, and use traps from HP Insight Manager to update data in the IP server instead of creating notifications.

Question

EMS forwards SNMP notifications to the IP Manager. The InstanceName has been changed to display EmsTrapOriginator= $V5$ in the trap rule instead of SYS. The $V5$ is an IP Address and not a System Name. Is there an ASL script that looks at an IP address from a varbind and then preform a DNS lookup so that the DNS name can be displayed?

Answer

SM_System::SM-System addrToName

Use the ASL, directive to execute an ASL file.