

EMC® Smarts®

# SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers

Version 9.6

Release Notes

Copyright © 2018-2019 Dell Inc. or its subsidiaries. All rights reserved.

Published January 2019

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners.  
Published in the USA.

EMC Corporation  
Hopkinton, Massachusetts 01748-9103  
1-508-435-1000 In North America 1-866-464-7381  
[www.EMC.com](http://www.EMC.com)

# CONTENTS

<b>Figures</b>		<b>9</b>
<b>Tables</b>		<b>11</b>
<b>Chapter 1</b>	<b>Service Assurance Suite (SA Suite)</b>	<b>13</b>
	Revision history.....	14
	Service Assurance Suite overview.....	14
	Product installation directory.....	15
	Features and changes applicable for all products.....	15
	EMC M&R support for 9.6.....	15
	Third-party support 9.6 changes.....	15
	Device Certification for Nokia 7210 Service Access Switch.....	15
	Licensing update.....	15
	Platform support.....	16
	Environment and system requirements.....	16
	Security recommendations.....	16
	Upgrade and migration overview.....	17
	Fixed Issues in Service Assurance Suite.....	19
	Known problems in Service Assurance Suite.....	29
	Installation, uninstallation, or upgrade issues.....	29
	Windows platform issues.....	29
	Foundation issues.....	31
	EMC Smarts Failover System issues.....	33
	EMC Smarts client program issues.....	39
	FLEXnet issues.....	40
	Technical notes.....	41
	Replacing or importing TLS certificates.....	42
	Documentation.....	42
	EMC Smarts foundation documentation.....	42
	EMC Smarts documentation.....	43
	Software media, organization, and files.....	50
	Installation executables.....	50
	Installation.....	51
	Troubleshooting and getting help.....	51
<b>Chapter 2</b>	<b>Service Assurance Manager (SAM)</b>	<b>53</b>
	Service Assurance Manager overview.....	54
	New features and changes in Service Assurance Manager (SAM).....	55
	Fixed Issues in Service Assurance Manager.....	55
	Known problems in Service Assurance Manager.....	64
	EMC Smarts Service Assurance Manager with Notification Cache	
	Publishing issues.....	64
	EMC Smarts Service Assurance Manager issues.....	73
	NOTIF issues.....	85
<b>Chapter 3</b>	<b>IP Manager (IP)</b>	<b>89</b>
	IP Manager overview.....	90

New features and changes in IP Manager (IP).....	90
Maintain IP Manager Settings from the EMC M&R interface.....	90
Reference information from the 9.3 release applicable to 9.4 installations.....	90
Enhancement to Wireless Discovery.....	91
New IP Manager classes for host resource objects.....	94
Extending support for discovery of iSCSI- and FCoE-based IPStoragePath.....	103
Fixed issues in IP Manager.....	105
Known problems in IP Manager.....	135
License feature checkout messages appear in IP domain manager ... 135	
ASL error messages displayed in IP Server log file, while discovering SNMPv3 devices.....	135
SNMP Walk for the devices is not stored in archive directory and stored in the root directory.....	136
Debug tool does not support devices with SNMP V3.....	136
BEM and Blade Type attribute are displayed as Host instead of BLADEENCLOSUREMANAGER and BLADE respectively in SAM and OI.....	136
Error message seen if the SELinuxSetting security setting is enabled in a system with RHEL 5.x.....	137
AM-PM services are overwritten on upgrade when Configuration Manger is installed.....	137
No logout option for the Configuration Manager in the EMC M&R UI.....	137
9.4 Configuration Manager is not fully compatible with 9.1 IP Managers.....	137
IP Manager DASL library is not loaded in Windows.....	138
sm_snmpwalk --autovlan command does not walk voice VLANs..	138
Compute fabric class does not get removed while deleting Cisco UCS Blade Enclosure Manager.....	138
ICMP ping polling when PingControl is enabled.....	139
A stray license message is listed in the IP Manager log file.....	139
sysOIDs without rules in Topology Change Analysis Tool (TCAT) for IP Manager 9.4.2.....	139
sysOIDs without rules in TCAT.....	140
Supported IP Manager released versions by TCAT.....	140
Changes made using sm_edit to DASL files or any libraries or conf files kept in the local\dasl\ directories are not picked up by the IP Manager.....	141
OID Info tool (oidInfo.conf) is merged to the conf/discovery folder after upgrade.....	141
When the IP-Configuration Manager was started, exceptions were seen during uninstallation.....	141
Topology Change Analysis Tool (TCAT).....	142
Details tab for WirelessControllerRedundancyGroup::SwitchOverFailed displays incorrect values.....	143
The “Ask before adding new systems” option does not work for SNMP v3 autodiscovery.....	143
Manual settings for Java and Java tools option.....	143
hwEntityMemSize returns negative values for few entities.....	143
HighFDUsageWarning event is not reported in the SAM Notification Log Console.....	144

Monitoring Fabric Interconnect (FI) switches using floating IP address.....	144
Multiple root causes generated for FabricInterconnect ports with AdminDown status.....	145
IP Manager did not generate any events after an ESM MS cluster active node was powered off.....	145
ASL error messages in IP Server log file if both the management IP address and the primary address are used to discover Cisco UCS....	145
IP server log shows errors when started on Windows.....	146
ASL errors when discovering SNMPv3 devices with MD5 and DES protocols as seed in FIPS 140 mode.....	147
During sm_rebond, IP Manager generated core dump after SIGINT is received.....	147
Mangled (unprintable characters) in IP Objects when IP Tagging is enabled.....	147
Interface instances are created but monitoring is not possible.....	148
Defaults cannot be reset for some threshold settings in the Polling and Thresholds Console.....	148
Attribute Mismatch on NumberofIPs between first and second discovery.....	148
The brcontrol output may show the SAM Server PID as "0".....	148
IPSec exception messages appear in the log file.....	149
Incorrect status for IKE tunnels involving a Cisco 2800 router.....	149
Set operator "->" does not work with dynamic model.....	149
Multiple instances of Broker may try to use the same port (Windows-specific problem).....	150
Output from brcontrol utility differs based on operating system..	150
MR-CALL_ON_NULL_OBJECT- NULL repository object and Object Not Found errors.....	150
Servers could not be attached when services were restarted.....	151
ASL errors seen when discovering the seedfile.....	151
Router Processor HighUtilization value exceeds 100% when monitoring discovering a device.....	152
SNMP errors seen in the log file while discovering Hosts.....	152
<b>Chapter 4</b>	<b>Server Manager (ESM) 153</b>
Server Manager overview.....	154
Server Manager discovery and monitoring.....	154
New features and changes in Server Manager.....	155
Fixed Issues in Server Manager.....	155
Known problems in Server Manager.....	167
Error occurs while adding HTTPS credentials of M&R.....	167
ASL errors appear in SAM logs due to ScaleIO StorageClientService Disconnected event.....	167
Restore Defaults option in P&T is not working for DisablePollingList text box where user can specify the classnames .....	168
ScaleIO Host instance Discovery Method attribute shows wrong value as SNMP_Discovery in ESM server.....	168
Any change in OpenStack credentials requires a rediscovery to be triggered in ESM Server.....	168
Manually configured Process Monitoring applications are not getting listed in ESM Server post upgrade and migrate .....	168
Two RCA (Cable Down and Interface Down) are generated when cable between the Host and the Switch goes down.....	169

Wrong credentials are updated in ESM..... 169

ESM logs are getting dumped with "WMI-Configuration does not exist" messages..... 169

Duplicate entries are created for process monitoring on a Windows host.....169

Inconsistent EMC M&R name in the 9.4 Global Console..... 170

Cable not created properly between master Xen server and Switch.. 170

Deleting Xen Host and performing Discover All in IP server or ESM server does not remove associated Hypervisor instance..... 170

Unmanaging Xen Hypervisor instance does not unmanage its CPU, Memory, and VM instances..... 170

NSX discovery does not work in ESM server when server credentials are provided as hostnames.....171

Veritas Clusters are not supported.....171

Bulk credential configuration for WMI Access is deprecated.....171

Credentials to vCenter may fail in ESM server if legacy MD2 encryption is in use on the vCenter server..... 171

Port and disk data is not synchronized for EMC M&R reports..... 172

SNMP error messages in log files are not suppressed..... 172

VMAX and VNX RAID Group monitoring occurs in EMC M&R for only specific RAIDGROUP types.....173

Sticky applications are difficult to remove.....174

Duplicate FibreChannelSwitch instances appear in the topology.. 175

Name of the Virtual Machine did not update from the ESM server.... 175

Synchronization issue between ESM server and network configuration..... 175

Isolated event generated when vCenter physical connections get disconnected..... 176

ESX server in the vCenter gets duplicated..... 176

JVM fails due to letter case mismatch of SM\_HOME and SM\_JAVAHOME..... 176

Installation/uninstallation issues..... 176

**Chapter 5 Multi-Protocol Label Switching Manager (MPLS) 179**

Multi-Protocol Label Switching Manager overview..... 180

New features and changes in MPLS Manager..... 180

Fixed Issues in MPLS Manager.....180

Known Problems in MPLS Manager..... 181

ASL errors appear in the MPLS Manager log file during discovery.... 181

EMC Smarts Adapter for Cisco ISC is listed in the Uninstallation dialog box..... 182

SSH - CLI discovery was not happening on Windows platform....182

sm\_stats --show-dm-processes throw an ASL error..... 182

Remote ping server tools are available to unintended object types.... 183

MPLS VPN maps do not increment and decrement hops..... 183

Unable to unmanage LSP objects..... 183

Error if special characters are included in a server's name in the startup command line..... 183

Unable to determine which IP belongs to a logical router..... 184

Discovery settings are not preserved in the MPLS Topology Server's repository file..... 184

	Service for the MPLS VPN-Tagging Server should not include -- subscribe.....	184
	Device Certification tab appears on the Polling and Thresholds Console.....	185
	Not all LdpProtocolEndpoints and LdpAdjacencies are discovered for Cisco IOS devices.....	185
	BGPProtocolEndpoint is not discovered on Cisco routers if BGP is enabled only on VRF.....	185
	Changes in RemoteAS value are not updated in the MPLS Topology Server.....	186
	Discover All in IP Availability Manager is not triggering discovery in BGP Manager.....	186
	BGP object monitoring is disabled if the BGP Manager shuts down... 186	
	MPLS server tools cannot be imported by using the Import XML Configuration server tool.....	187
	Cannot monitor the status of TE LSPs on Cisco IOX devices.....	187
	LSP ping requests on Cisco devices return a “QQQQQ” status....	188
	MPLS Manager is generating false PseudoWire::Impacted events.... 188	
	VRF LSP Ping All does not work as intended.....	189
	LSP map is displayed when selecting LSP Hops map for a VPN object.....	189
<b>Chapter 6</b>	<b>Network Protocol Manager (NPM)</b>	<b>191</b>
	Network Protocol Manager overview.....	192
	New features and changes in Network Protocol Manager.....	192
	Configuring the monitoring of VRF based EIGRP sessions.....	192
	Enabling OSPF STUB area discovery.....	193
	Fixed Issues in Network Protocol Manager.....	193
	Known Problems in Network Protocol Manager.....	201
	Devices use incorrect access credentials from multiple IP Managers in NPM CLI discovery.....	201
	Errors appear in the Discovery Progress window for IPv6 devices.... 201	
	Unnecessary error message during startup of any Network Protocol Manager on Linux.....	201
	IP Manager populates SNMPAgents with incorrect attribute values .....	202
	Relationships are removed in Network Protocol Manager after tagging IPs in IP Availability Manager.....	202
	Network Protocol Manager for BGP issues.....	202
	Network Protocol Manager for EIGRP issues.....	204
	Network Protocol Manager for IS-IS issues.....	205
	Network Protocol Manager for OSPF issues.....	206
<b>Chapter 7</b>	<b>Optical Transport Manager (OTM)</b>	<b>207</b>
	Optical Transport Manager (OTM) overview.....	208
	New features and changes in OTM.....	208
	Support for addition of Card level events.....	208
	Foundation upgrade.....	208
	New WDM Manager for Next Generation WDM Devices.....	209
	Fixed Issues in Optical Transport Manager.....	209
	Known Problems in Optical Transport Manager.....	210

Autodiscovery is not automatically triggered after data collection in EMC M&R..... 211

Monitoring attributes are greyed out when using WDM-NG domain manager.....211

Spurious alarms occur during OTM-XD processing..... 211

Root cause alarms show incorrect impact notifications..... 211

Non-LCTPG CTP failure overwrites the LCTPG CTP failure in the UD2 field..... 211

FORCE\_POST\_PROCESSING\_ERROR displays in the discovery window of SDH Topology server..... 212

Userdefined1 field is updated though Userdefined1 field is deprecated..... 212

Error message when TMF 814 Adapter is started..... 212

Extraneous Fiberlink alarms display in OTM-XD-WDM server..... 212

Router to Switch configuration topology is not uploaded in the OTM-IP-XD server..... 212

ServiceAtRisk alarms event is not supported by cross-domain analysis.....212

No reference documentation for cross domain failure for mixed order IP using SDH and PDH..... 213

**Chapter 8 Voice over IP (VoIP) Availability Manager 215**

Voice over IP (VoIP) Availability Manager overview..... 216

New features and changes in VoIP..... 216

    Changes in the procedure to start VoIP Availability Manager..... 216

    Changes in the VoIP Availability Manager service installation..... 217

Fixed Issues in VoIP Availability Manager..... 217

Known Problems in VoIP Availability Manager..... 218

    SOAP credentials are not associated with CCM if multiple SOAP Access Groups are created.....218

    IP Availability Manager instances are missing from the VoIP Availability Manager topology.....219

    Error messages observed in the VoIP AM log file..... 219

    ASL errors appear in VoIP Availability Manager log when the trap adapter port is in use..... 220

    Inter-trunk data from VoIP Performance Manager GatewayService should be ignored..... 220

    IsActive attribute of H248RegistrationSession does not synchronize correctly..... 220

    H323Service call counts do not agree with VoIP Performance Manager values..... 221

    Misleading subscription change messages in VoIP Availability Manager log file.....221

    VoIP Availability Manager Avaya-related issues..... 221

    VoIP Availability Manager Cisco-related issues..... 222

# FIGURES

1	Example of an IPStoragePath instance.....	103
---	---	-----

## FIGURES

# TABLES

1	Revision History.....	14
2	Deployment scenarios.....	17
3	Fixed issues common for all Smarts domain managers.....	19
4	EMC Smarts Foundation documentation .....	42
5	Service Assurance Suite version 9.6 documentation.....	43
6	Fixed field definitions.....	47
7	Fixed issues in Service Assurance Manager.....	55
8	WirelessAccessPoint threshold settings.....	91
9	Attributes of WirelessAccessPoints.....	92
10	Parameters in tpmgr-param.conf file.....	92
11	Attributes for MemoryGroup.....	94
12	Attributes for ProcessorGroup .....	95
13	Vendor-specific notifications.....	96
14	Default values for threshold settings.....	97
15	Discovery.conf and tpmgr-param.conf file parameters for IPStoragePath .....	100
16	Attributes of IPStoragePath .....	101
17	IPStoragePath configuration parameters.....	103
18	IPStoragePath attributes.....	103
19	Fixed issues in IP Manager .....	105
20	Fixed issues in IP Manager 9.3.x.....	133
21	PingInterval and PingRetry default values when PingControl is enabled.....	139
22	Supported IP Manager versions with the Foundation version.....	140
23	Fixed issues in Server Manager (ESM) .....	155
24	Conditions for EMC M&R monitoring of RAIDGROUP.....	174
25	Fixed issues in MPLS Manager.....	180
26	Fixed issues in Network Protocol Manager.....	193
27	Notifications for Cisco BGP-enabled devices in IPv6 network.....	203
28	Fixed issues in Optical Transport Manager.....	209
29	Behavior of individual components.....	219

## TABLES

# CHAPTER 1

## Service Assurance Suite (SA Suite)

This chapter includes the following topics:

• <a href="#">Revision history</a> .....	14
• <a href="#">Service Assurance Suite overview</a> .....	14
• <a href="#">Features and changes applicable for all products</a> .....	15
• <a href="#">Platform support</a> .....	16
• <a href="#">Environment and system requirements</a> .....	16
• <a href="#">Upgrade and migration overview</a> .....	17
• <a href="#">Fixed Issues in Service Assurance Suite</a> .....	19
• <a href="#">Known problems in Service Assurance Suite</a> .....	29
• <a href="#">Technical notes</a> .....	41
• <a href="#">Documentation</a> .....	42
• <a href="#">Software media, organization, and files</a> .....	50
• <a href="#">Installation</a> .....	51
• <a href="#">Troubleshooting and getting help</a> .....	51

## Revision history

The following table presents the revision history of this document.

**Table 1** Revision History

Revision	Date	Description / Updates
01	January 2019	First release of Service Pack for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers Version 9.6.0.0.

## Service Assurance Suite overview

Service Assurance Suite supplies automated IT management insights, including

- intelligent, automated root-cause and impact analysis
- event correlation
- discovery and modeling of IT environments being monitored  
These insights enable IT operations personnel to visualize, analyze, and optimize the availability, performance, and configurations of their physical and virtual network, server, and storage environments so that service levels can be met or exceeded.

Service Assurance Suite is built on and composed of technologies such as:

- EMC Smarts domain managers
- EMC M&R core software

These release notes describe features and changes made to these EMC Smarts domain managers:

- [Service Assurance Manager \(SAM\)](#) on page 53
- [IP Manager \(IP\)](#) on page 89
- [Server Manager \(ESM\)](#) on page 153
- [Multi-Protocol Label Switching Manager \(MPLS\)](#) on page 179
- [Network Protocol Manager \(NPM\)](#) on page 191
- [Optical Transport Manager \(OTM\)](#) on page 207
- [Voice over IP \(VoIP\) Availability Manager](#) on page 215
- Review the *EMC Smarts Network Configuration Manager Release Notes* for detailed information about the NCM domain manager.

The EMC M&R core software provides performance reports and a graphical user interface to real-time notifications coming from EMC Smarts Service Assurance Manager and Network Configuration Manager. Use the UI that comes with EMC M&R to generate reports from data collected from mobile devices and other sources when you install SolutionPacks licensed as part of Service Assurance Suite.

The *EMC M&R 6.6u2, 6.7, 6.7u1, 6.8u2, 6.8u5 Release Notes* and the *Service Assurance Suite SolutionPack Release Notes* provide more information.

## Product installation directory

In this document, the term BASEDIR represents the location where EMC Smarts software is installed:

- For UNIX, this location is `/opt/InCharge/<product>`.
- For Windows, this location is `C:\InCharge\<product>`.

## Features and changes applicable for all products

### EMC M&R support for 9.6

If your Service Assurance Suite deployment includes the EMC M&R UI, then the EMC M&R 6.8u5 version is required to access the features introduced in release 9.6.

EMC M&R UI features and enhancements provided by the SolutionPack for EMC Smarts and other SolutionPacks are described in the *Service Assurance Suite SolutionPack Release Notes*.

### Third-party support 9.6 changes

The *EMC Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers Support Matrix* available from the EMC Online Support website provides the latest platform and interoperability information. High-level changes in version 9.6 of Service Assurance Suite are listed here:

- Java is upgraded to 1.8U181

### Device Certification for Nokia 7210 Service Access Switch

Smarts Adapter for Alcatel-Lucent 5620 SAM version 3.4.0.0 includes support for Nokia 7210 Service Access Switch in satellite mode. This is qualified on NFM-P version 17.9.

### Licensing update

The FlexNet license support has been removed in Service Assurance 9.6. Now there is no requirement to obtain the license file.

However, previous to 9.6, domain managers still need license, and they need to point to a license server. For example, if the deployment has ten 9.5.1 domain managers, and only four domain managers are upgraded to 9.6, all six existing 9.5.1 domain managers need license and have to point to the existing license server. If all domain managers are upgraded to 9.6, then license server is not required.

If you are planning to upgrade only a subset of domain managers in a deployment to 9.6, follow these guidelines for license server that is needed for older domain managers:

- If the domain manager is not active on the server, where the license server is installed, then it is not required to upgrade to 9.6. Existing license server required to serve the previous domain managers 9.5.1 (or previous versions).

- When the domain manager is active, where the license server is installed, and this domain manager needs to be upgraded, then perform the upgrade for 9.6 and bring up the license server.

## Platform support

The *EMC Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers Support Matrix* available from the EMC Online Support website provides the latest platform and interoperability information. For detailed information about platform support and interoperability, consult the support matrix for your release.

## Environment and system requirements

The *EMC Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers Support Matrix* provides information on supported operating systems, required operating system patches, and product and version compatibility. The document is available at EMC Online Support at: <https://support.emc.com>.

## Security recommendations

This section describes EMC security recommendations.

### **ESA-2016-118 issued to address various vulnerabilities in Smarts**

Refer to EMC Security Advisory ESA-2016-118 for more information.

Oracle Java SE is upgraded for Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers in the 9.4.2 release. Apache Common Collections is upgraded only for SAM. The Java and Apache Common Collections updates include fixes for multiple security vulnerabilities.

- Apache Common Collections is upgraded to version 3.2.2 for SAM only.
- Oracle Java SE is upgraded to Java 8 Update 91.

### **ESA-2016-115 issued to address vulnerabilities in the RC4 algorithm**

Refer to EMC Security Advisory ESA-2016-115 for more information.

In the 9.4.2 release, TLS communication is enhanced for the following products: SAM, IP Manager, ESM, MPLS, NPM, OTM, VoIP AM, and the SAM Global Console. The RC4 algorithm is a weaker cipher and vulnerable to attacks. You can disable it and specify a cipher suite list as an alternative. The *EMC Smarts Security Configuration Guide* provides the procedure.

### **ESA-2015-156 issued to address various vulnerabilities in Smarts**

Refer to EMC Security Advisory ESA-2015-156 for more information.

Oracle Java SE and Apache Tomcat are upgraded for Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers in the 9.4.1 release. The Java and Tomcat updates include fixes for multiple security vulnerabilities.

- Oracle Java is upgraded to Java 8 Update 51
- Apache Tomcat is upgrade to Apache Tomcat 8 Update 23.

### **BSAFE upgrade**

RSA BSAFE Micro Edition Suite and SSL-J Crypto modules are upgraded for Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers in the 9.4.1 release.

- "RSA BSAFE MES 4.0.6

- "RSA BSAFE SSL-J 6.1

#### Secure data erasure

For Government customers, or any other customer requiring a heightened level of application and information security, EMC recommends that applications should utilize host-based erasure. Alternatively, if data is held on off-box storage, storage level erasure should be utilized.

#### Data-at-rest encryption

For Government customers, or any other customer requiring a heightened level of application and information security, EMC recommends that this product be installed onto a host that supports native encryption of DAS, or a storage environment that supports SAN or Array encryption of all storage volumes utilized. Installing and operating this EMC product on encrypted drives or encrypted storage adds a secondary level of security against malicious actions.

#### FlexNet Publisher

In the EMC Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Manager 9.5 release, FlexNet Publisher Imgrd license server has been updated to version 11.12.1.5.

In the EMC Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Manager 9.4.1 release, security vulnerabilities in FlexNet Publisher Imgrd license server managers as well as vendor daemons are fixed. EMC Security Advisory ESA-2015-066 provides more information.

## Upgrade and migration overview

For EMC Smarts products, in-place upgrades from 9.5.1 to 9.6 are supported. Migrations from 9.5.1 to 9.6 are supported.

#### Deployment scenarios

The *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers* provides upgrade and migration instructions.

For the latest product interoperability information, consult the *EMC Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers Support Matrix* available from the EMC Online Support website.

**Table 2** Deployment scenarios

Scenario	Upgrade/migration order
Service Assurance Suite deployment that includes EMC M&R UI and SolutionPack for EMC Smarts	<ol style="list-style-type: none"> <li>1. Upgrade the Presentation SAM server to 9.6.</li> <li>2. Upgrade the EMC M&amp;R Core to 6.8u5.</li> <li>3. Upgrade the SolutionPack for EMC Smarts to the latest version shipped with EMC M&amp;R 6.8u5 (for example 3.0).</li> <li>4. Upgrade, if necessary, the Aggregation SAM server if it is a hierarchical SAM deployment.</li> <li>5. Upgrade, if necessary, the IP Manager.</li> <li>6. Upgrade, if necessary, in any order: Server Manager, MPLS Manager,</li> </ol>

**Table 2** Deployment scenarios (continued)

	<p>Network Protocol Manager, and VoIP Availability Manager</p> <p>Consult:</p> <ul style="list-style-type: none"> <li>• The <i>EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers</i></li> <li>• The <i>Service Assurance Suite Installation and Configuration Guide for EMC M&amp;R</i></li> <li>• The <i>SolutionPack for EMC Smarts Summary Sheet</i> article</li> <li>• The <i>How to Set Up SAM, EMC M&amp;R, and the SolutionPack for EMC Smarts</i> article</li> </ul>
<p>Service Assurance Suite deployment without EMC M&amp;R UI and without SolutionPack for EMC Smarts</p>	<ol style="list-style-type: none"> <li>1. Upgrade the top-most SAM server and related Service Assurance products and consoles in your deployment to 9.6, either a SAM server or the top SAM server in a hierarchical SAM deployment.</li> <li>2. Upgrade, if necessary, the Aggregation SAM server if it is a hierarchical SAM deployment.</li> <li>3. Upgrade, if necessary, the IP Manager.</li> <li>4. Upgrade, if necessary, in any order: Server Manager, MPLS Manager, Network Protocol Manager, and VoIP Availability Manager</li> </ol> <p>Consult the <i>EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers</i>.</p>
<p>Service Assurance Suite deployment that includes EMC M&amp;R UI and other SolutionPacks (minus SolutionPack for EMC Smarts)</p>	<ol style="list-style-type: none"> <li>1. Upgrade the Presentation SAM server to 9.6.</li> <li>2. Upgrade the EMC M&amp;R Core to 6.8u5.</li> <li>3. Upgrade the SolutionPacks to the latest versions shipped with EMC M&amp;R 6.8u5.</li> <li>4. Upgrade, if necessary, the Aggregation SAM server if it is a hierarchical SAM deployment.</li> <li>5. Upgrade, if necessary, the IP Manager.</li> <li>6. Upgrade, if necessary, in any order: Server Manager, MPLS Manager, Network Protocol Manager, and VoIP Availability Manager</li> </ol> <p>Consult:</p>

**Table 2** Deployment scenarios (continued)

	<ul style="list-style-type: none"> <li>• The <i>EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers</i></li> <li>• The <i>Service Assurance Suite Installation and Configuration Guide for EMC M&amp;R</i></li> <li>• The <i>Service Assurance SolutionPack Articles</i> document</li> </ul>
Service Assurance Suite deployment that uses EMC Smarts products prior to release 9.6	<p>For EMC Smarts products, in-place upgrades from 9.5.1 to 9.6 are supported. Migrations from 9.5.1 to 9.6 are supported.</p> <p>Consult the <i>EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers</i>.</p> <p>Consult the <i>EMC Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers Support Matrix</i>.</p>

## Fixed Issues in Service Assurance Suite

These are the fixed issues pertinent to all Smarts domain manager components of Service Assurance Suite.

**Table 3** Fixed issues common for all Smarts domain managers

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-11335 SR 10821605	ESM domain crashes while trying to access empty WMI-polling queue.	Code has been modified in DMT to handle null node access of WMI-polling RB-tree.	9.4.1.X	9.6
IS-11874 SR 11426133	<p>The reporting backup actions fail with error message while upgrading the Smarts Failover and the underlying domains from 9.4.2 to 9.5.1.</p> <p>The failover actions log reports that it is copying the INCHARGE-AM-PM domain from</p>	<p>Failover, while suspending actions, looks for a newly introduced feature named "Kafka-Subscription", even though such a feature does not exist in older versions of IP and ESM.</p> <p>Now the "Kafka-Subscription" feature existence</p>	9.5.1.X	9.6

**Table 3** Fixed issues common for all Smarts domain managers (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	the active to the standby server.	check has been introduced in the Failover script before performing suspend action.  Note: For proper functioning of the Failover system, the active and standby server must be on the same version.		
IS-9477 SR 08311986	ESM server goes down immediately after starting the service.	The crash was caused while parsing the encrypted Auth/Priv password having new lines. Code has been modified to properly parse the encrypted Auth/Priv passwords having new lines.	9.4.1.X	9.5.1
IS-8704/ SR 7230121	Service started with --noregister causes an attached service to unattach.	The code has been modified so that in case of --noregister, server never tries to connect with broker.	9.4.2	9.5
IS- 8327 SR 71319566	PCI Scan makes SAM server unresponsive and also there is an issue where server crashes when decoding URLs.	Decoding of URL used to cause a heap corruption which has been fixed. For the server unresponsiveness, a delay of 25 milliseconds is introduced while accepting any new connections and the HTTP worker threads	9.2.1.X	9.5

**Table 3** Fixed issues common for all Smarts domain managers (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
		are increased from 2 to 4, to allow processing of requests for closure.		
IS-5968 SR 75517670	Unable to update the RPS file in the domain.	Added check to not to pass the RPS file handle to any child process like sm_authority.	9.2.2.X	9.5
IS-6322 SR 78917372	Domain deadlock occurs, once the polling threads is set-up to 75.	The polling threads configuration limit is extended up-to 100 which need not cause the deadlocks anymore.	9.4.1	9.5
IS-6487 SR 71319566	PCI Scan for vulnerabilities made Smarts domain unresponsive.	Heap corruption caused a crash in URL decoding logic which has been fixed. During the scan, the fd limit 1024 was being used up which caused server to hang, the acceptor threads have been increased from two to four threads to close out the close_wait sockets to prevent server hangs.	9.2.1.X	9.5
IS-4942 SR 72710986	When running the dmctl command, the following error message is displayed: "SM-E-ENOPRIV-No privilege to	The fix is for the sm_authority crash. During the authentication process the user name and password provided are validated for	9.4	9.5

**Table 3** Fixed issues common for all Smarts domain managers (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	execute this operation".	stanadard unix users. If this fails then it is treated as smarts user name and password. When checking for unix user based authentication, if the user is not present, a null pointer is returned in RHEL 7. Code is changed to handle this null pointer return value to avoid the crash.		
SND-2756	FlexNet Version 11.10.1 Imutil Imhostid utility returns 000000 for names using enxx in Linux RHEL 7.1. For Linux RHEL 7.1, when you run the FlexNet utility Imutil Imhostid with network interface names that use enxx, the host id returns 000000 and the EMC Smarts License server will not start. On RHEL 7.1, the network interface naming convention by default follows a new standard like enxx, which is not the old style ethxx.	This issue is fixed. FlexNet Publisher has fixed this issue in the latest releases which support RHEL 7.x. In the EMC Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Manager 9.4.2 release, FlexNet Publisher Imgrd license server has been updated to version 11.12.1.5.	9.4.1	9.4.2

**Table 3** Fixed issues common for all Smarts domain managers (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
SND-3767, SND-3619	<p>Disabling RC4 by specifying tls suite doesn't work in the SAM Console. The SAM Global Console does not communicate with the Managers that use the RC4 cipher and the AES algorithm. The Managers do not attach to the console. This error also appears:</p> <pre data-bbox="663 961 858 1171"> Could not load console.smarts .tls suite list=AES256-GCM-SHA384. java.io.FileNotFoundException </pre>	<p>This issue is fixed. Add the SM_TLS_SUITE_LIST environment variable to the runcmd_env file for each Manager and apply the Java Cryptography Unlimited Strength Jurisdiction Policy Files 8 for each console. The <i>EMC Smarts Security Configuration Guide</i> provides the procedure.</p>	9.4.2	9.4.2
IS-5331 SR 76051732	<p>Failover does not properly backup and update changes made to user profiles.</p>	<p>A wrong variable was being checked for process execution status due to which backup would miss some changed configurations. Have modified the code to check the correct variable.</p>	9.4.0.X	9.4.2
IS-6077 SR 78114010	<p>Smarts SAM: banner causing rabbitMQ, tomcat and EDAA to appear as NOT RUNNING after failover.</p>	<p>Added the -q (quiet) and -p (preserve permissions) option for ssh and scp commands. The -q option by passes the</p>	9.4.1.0	9.4.2

**Table 3** Fixed issues common for all Smarts domain managers (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
		banner and gives only the required information.		
IS-6767 SR 78241258	Failover server not starting.	Timeout has been used in remote server interface used by Failover Manager. This allows requests from failover-server to other domain servers to timeout - if the domain manager is not responding.	9.4.0.X	9.4.2
IS-6768 SR 78241258	Topology mismatch in SAM and OI servers in failover environment.	Failover monitor will monitor SuspendTopologyManager flag and set it to False to enable toposync in SAM and OI Servers.	9.4.0.X	9.4.2
IS-6769 SR 78241258	Stale Alarms present in SAM server in failover environment.	Race in HyerNotif Driver restart and Domain Reconfigure has been handled to fix this issue.	9.4.0.X	9.4.2
IS-6770 SR 78241258	Backup operations from IP and other satellite domains fail when failover is configured as non root user.	In case of non-root user, the rps on standby site is removed before attempting a copy rps from active server.	9.4.0.X	9.4.2
IS-5595 SR 77027380	UNKNOWN status on AMPM domain after failover to Standby site.	IsRegistered property in Failover-Setting instance was not getting update properly in resync actions.	9.4.1.0	9.4.2

**Table 3** Fixed issues common for all Smarts domain managers (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		This has been fixed.		
IS-6298	Manual failover of APM leaves NPM domains subscribed to standby APM.	Failover actions will disconnect clients from standby server when manual failover happens.	9.3.0.X	9.4.2
IS-4011 SR 67599562	Failover Manager for a particular region is not starting. Backup actions during failover were not getting completed.	Issue is fixed by cleanup of existing Polling and Thresholds settings on the Standby Server prior to restoring the Active Server rps to Standby. Modified files: <ul style="list-style-type: none"> <li>actions/ backup_actions.sh</li> <li>rules/ failover/ removeConfig.asl</li> </ul>	9.3.0.X	9.4.1
IS-1819 SR 66607340	Security vulnerability reported for FlexNet License Manager v11.9.0.0. CVE-2011-1389 and CVE-2011-4135.	Upgraded FlexNet License Server and client libraries to version 11.10.1.0, which is safe. Modified files: <ul style="list-style-type: none"> <li>bin/system/lmgrd (.exe)</li> <li>bin/system/lmutil (.exe)</li> <li>bin/system/sm_lmgrp92 (.exe)</li> <li>Windows: <ul style="list-style-type: none"> <li>lib \sm_license.dll</li> <li>lib \sm_dmtlic.dll</li> </ul> </li> </ul>	9.3.0.X	9.4

**Table 3** Fixed issues common for all Smarts domain managers (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		<ul style="list-style-type: none"> <li>Linux: lib/ libsm_licens e.so  lib/ libsm_dmtlic. so</li> </ul>		
IS-144 SR 64470330	False alerts are generated when device attributes are added using dynamic modeling.	<p>When new properties are added to a class using dynamic modeling, the attributes and relationships indexes are shifted in that class and all of the child classes. The attributes which are referred in a computation expression using the "-&gt;" operator are grouped in a list as indirect references.</p> <p>Property indices for these indirect references were not getting updated after class refinement.</p> <p>Hence, the monitoring tree would show invalid/unrelated attributes, and the monitoring computations would fail. Fixed this, so that the attribute indices are updated after class refinement.</p> <p>Modified files:</p> <ul style="list-style-type: none"> <li>Windows:</li> </ul>	9.2.2.X	9.4

**Table 3** Fixed issues common for all Smarts domain managers (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		lib/ sm_repos.dll  • Linux: lib/ libsm_repos. so		
654678	sm_getinfo does not work after upgrading from Service Assurance Suite version 9.2.2 to 9.4		9.3	9.4
654750	sm_getinfo utility not working after an upgrade.		9.2.2	9.4
616809	Services are overwritten during in-place upgrade.		9.2	9.4
616466	Files for EMC Smarts Adapter for UIM/O are not removed after an upgrade.		9.2	9.4
643669 577859 SR 55343712	sm_edit did not exit. Moreover, if the SM_SITEMOD was set to any other directory other than local, recursive directories were created in the SM_SITEMOD folder.	Resolved by removing a recursive loop in the sm_edit tool.	9.2	9.3
640386	HA: Need to run failover server without root and passwordless access.		9.2	9.3
644153	Google: FAILOVER-MGR			9.3

**Table 3** Fixed issues common for all Smarts domain managers (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
	did not activate B-side in test			
644518	Following failover, servers status remains at UNKNOWN			9.3
649506	Dynmodel does not automatically copy the l10n files to the correct directory.	On compilation of dynamic model files, the ICU files generated during compilation will now be automatically copied to the l10 directory. But this requires the following runtime variable to be set to true in runcmd_env.sh SM_AUTO_COPY_ICU	9.2.0.4	9.3
649507 SR 56571340	brcontrol exhibited a timeout when displaying a large number of Domain Managers across a high-latency link.	Replaced multiple remote calls to the broker with a single remote call during the fetch operation for domain properties. Modified file: brcontrol	9.1	9.3
653080	The failover solution should not rely on a single broker.	The broker can now be deployed in active/standby modes. The Failover server can switch the broker on all domains in a failover deployment if the active broker goes down.	9.2.2	9.3

## Known problems in Service Assurance Suite

These problems affect the Smarts domain managers in the Service Assurance Suite.

### Installation, uninstallation, or upgrade issues

The following issues relate to the install, uninstall, or upgrade processes.

#### Upgrading to EMC M&R 6.6uX before upgrading Service Assurance Suite breaks functionality

Service Assurance Suite 9.3 or 9.4 customers who upgrade to EMC M&R 6.6uX before upgrading to Service Assurance Suite 9.4.1 will break functionality, because the EMC Smarts 9.4 components are not compatible with 6.6uX. As result, some of the functionality after the upgrade will not work.

Impacts of upgrading to EMC M&R 6.6uX without upgrading to SAM 9.4.1 or if the Presentation SAM is not installed first:

- Aggregatelink visualization is not available. You cannot expand the aggregate link in the Topology map to access the detailed information on the underlying links.
- Topology Group map displays an error.
- Topology map does not display by default.

Impacts of upgrading to EMC M&R 6.6u1 without upgrading the SolutionPack for EMC Smarts (available in EMC M&R 6.6u1) and upgrading to SAM 9.4.1. The impacts vary depending on the existing SolutionPack for EMC Smarts version.

- Topology Map displays an error or will not be available.
- In the Notification view, user actions on Notification context click (Acknowledge/Unacknowledge, Take/Release Ownership, Email, Add to audit log) will not work.

Impacts of upgrading to SAM 9.4.1 without upgrading to EMC M&R 6.6uX:

- New features provided by the SolutionPack for EMC Smarts on EMC M&R 6.6u1 are not available. The features are described in the *Service Assurance Suite SolutionPack Release Notes*.

At a high-level, they are:

- Aggregatelink visualization
- Right-click menu items
- Browse details right-click menu options
- Topology map filtering

#### Resolution

First, upgrade the Presentation SAM server to 9.4.1 and follow the upgrade order as described in the *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Manager*.

### Windows platform issues

The following issues are specific to running software on the Windows platforms.

### sm\_service show command displays error message

The output of `sm_service show` on the Windows 2016 operating systems returns the correct output with the following error message:

```
"sm_service: The resource loader failed to find MUI file."
```

SND-5751

#### **Resolution**

No functionality is impacted by this issue. There is currently no resolution for this issue.

### sm\_service show command returns incorrect output

The output of `sm_service show` on other operating systems shows the name and status of the services installed on the SAM server.

In Windows, the output of `sm_service show` command is the same as `sm_service show --cmdline`. The output shows the service commands of all the services that are installed on the SAM server.

CQ 577383 / CQ 577366

#### **Resolution**

There is currently no resolution for this issue.

### Internet Explorer displays garbage text in browser window after exiting Web Console or Business Dashboard

When you exit Web Console or Business Dashboard (by clicking File > Exit), the Internet Explorer browser window does not clear.

The browser window displays whatever was displayed in the window at the time you exited the application. If you move another window over the browser window and then bring the browser window back into focus, the content of the window that was on top of the browser window displays in the browser window.

CQ 448240

#### **Resolution**

No functionality is impacted by this issue. Ignore the garbage text displayed in the Internet Explorer browser window. Instead of exiting the browser, you can either:

- Close the Web browser
- Type a new URL in the Web browser

### Multiple instances of Broker may try to use the same port

Multiple instances of a Broker are able to use same port on the same machine (Windows-specific). There is no message to explain that the address or port is in use.

CQ 506290

#### **Resolution**

End all Broker and Domain Manager processes that are listening on the same port, and start only one process listening on that port.

## Unable to start SNMP Trap Adapter service on Windows operating system

The SNMP Trap Adapter service fails to start while trying to parse the rules parameter.

CQ 493564/515943/515944 /SR33268064

### Resolution

Install the service with the `--rules` parameter before the `--config` parameter in the command line. An example is provided below:

```
sm_service.exe install --force --name=ic-trapd-receiver --
startmode=runonce --description="EMC Smarts SNMP Trap Adapter"
<BaseDir>\smarts\bin\sm_trapd.exe --name=TRAP-INCHARGE-OI --
server=INCHARGE-OI --port=162 --model=sm_actions --rules=iccoi-trapd/
trap_mgr_parse.asl --config=iccoi --output
```

## Output generated from commands within Windows PowerShell is unusable

PowerShell automatically converts all piped and redirected command output into the UTF-16LE encoding scheme format. (UTF-16 refers to the ISO standard 16-bit Unicode Transformation Format that maps each character to a sequence of 16-bit words.) EMC Smarts software expects the UTF-8 format for input files, so if the output of an EMC Smarts application is redirected to a file that is to be consumed by a second EMC Smarts application, the second EMC Smarts application will fail to parse the file.

CQ 463092

### Resolution

Because PowerShell expects the application to behave in a “cmd.exe”-compatible way, leave all `SM_ENCODING_XXXX` variables unset. The defaults already auto-initialize to “cmd.exe”-compatible values. Because PowerShell itself post-processes output from “cmd.exe” style into UTF-16LE, the only way to get the output back into a form that EMC Smarts software accepts (UTF-8) is to further post-process the output with a transcoder utility. PowerShell provides “Out-File” for this purpose.

Examples:

```
sm_server "--version" > version.out
sm_server "--version" | Out-File -Encoding utf8 version.out
```

The first example will result in a “version.out” file that is encoded as UTF-16LE, and the second example will result in a “version.out” file that is encoded as UTF-8. If the output is to be parsed by another EMC Smarts application, use the second example.

## Foundation issues

The following issues apply to the Foundation on which EMC Smarts domain managers are built.

### Longer Global Manager event processing time when TLS is enabled

In an EMC Smarts deployment, the Transport Layer Security (TLS) inter-process communication (IPC) protocol is enabled by default.

Under certain circumstances, the event processing throughput at the Global Manager might be slightly reduced due to TLS, which could result in a performance impact when event flooding occurs at the Global Manager.

**Resolution**

Under those circumstances, consider disabling TLS for the Global Manager by stopping the Global Manager and restarting it with the `--env=SM_NO_TLS=1` option in the startup command.

**Note**

Setting the `SM_NO_TLS` environment variable to Yes disables TLS and resetting `SM_NO_TLS` to No enables TLS.

Here is a sample Global Manager service command for UNIX that includes the `--env=SM_NO_TLS=1` option:

```
/opt/InCharge/SAM/smarts/bin/sm_service install
--force
--unmanaged
--name=ic-sam-server
--startmode=runonce
--description="EMC Smarts Service Assurance Manager"
--env=SM_NO_TLS=1
/opt/InCharge/SAM/smarts/bin/sm_server
--name=INCHARGE-SA
--config=ics
--port=0
--ignore-restore-errors
--output
```

As an alternative, and assuming that the Broker and the Global Manager are started from different installations, you could use the `sm_edit` utility to open the `BASEDIR/smarts/local/conf/runcmd_env.sh` file in the Global Manager installation area and add `SM_NO_TLS=1` to the file, then restart the Global Manager for the change to take effect.

For any underlying EMC Smarts application to communicate with a Global Manager that has TLS disabled, the underlying foundation software falls back to using the EMC Smarts IPC protocol. For the IPC protocol between the underlying applications, themselves, however, the underlying foundation software continues to use TLS.

**Turn off built-in line folding works only on server logs**

When you enable `SM_LOG_STYLE=SINGLELINE` in the `runcmd_env.sh` file, only the domain server logs support `SINGLELINE` logging.

This feature does not work for other logs such as audit, archive, or notif.

CQ 653806

**Resolution**

There is no workaround.

**Some Server logs follow LEGACY mode even though SINGLELINE is set**

Here is an example of the use of `LEGACY` mode from `VOIP-AM.log`

```
March 27, 2014 4:50:14 AM EDT +096ms 72 9464 ALWAYS
InCharge Framework RSVI_MSG-SUB_CHG Subscription change:
propertySubscribeAll client: SubscriberFE choice:
UnitaryComputerSystem::*:IsUnresponsive::[EXPAND-SUBCLASSES,EXPAND-
SUBCLASSES-EVENTS,STICKY]
Vendor License Feature Feature-VOIP_ACME is enabled.
Vendor License Feature Feature-VOIP_AVAYA is enabled.
March 27, 2014 4:50:14 AM EDT +377ms 78 9464 ALWAYS
```

```
InCharge Framework      RSVI_MSG-SUB_CHG      Subscription change:
propertySubscribeAll    client: SubscriberFE  choice:
ICF_PolicyManager::.*::reconfigureStatus::[EXPAND-SUBCLASSES,EXPAND-
SUBCLASSES-EVENTS,STICKY]
```

CQ 653349

**Resolution**

There is no workaround.

## SNMPv3 EngineID appears blank in the SNMP Trap Manager

The Engine ID generated by Smarts does not have a permanent true value which could impact the processing of SNMPv3 traps.

Smarts generates its own SNMPv3 EngineID so that devices can receive SNMPv3 traps or informs.

CQ 576556 / 638899

**Resolution**

You can override the automatic random generation of Engine ID by manually setting the Engine ID. When starting the trap adapter, type a value for the following parameter, `--localengine=<engine>`.

## EMC Smarts Failover System issues

The following issues relate to the EMC Smarts Failover System.

### Failover server fails to detect newly added Domain Managers

When domain managers are started post failover start, then it is observed that the domain managers do not get registered with Failover Server.

SND-5730

**Resolution**

It is mandatory to start the Failover server, after all Domain Managers are started.

In case user needs to start a new Domain Manager, then perform the following steps:

**Procedure**

1. Shutdown the Failover server.
2. Start the new Domain Manager.
3. Start the Failover Server.

Ensure that all the Domain Managers are detected as Active/Standby by the Failover server.

### Smarts Failover Feature is not supported in Docker Environment

EMC Smarts Failover feature is not supported in the Docker environment.

SND-5756

**Resolution**

No workaround.

### A mixed-case name value in the Trap Exploder service install command causes errors

In the Trap Exploder `service install` command, a mixed-case value for `--name` (`--name=TRAP-INCHARGE-Exploder`) causes errors in the Failover Manager log.

Since the Trap Exploder name in the service command does not match the value in the `failover.conf` file, the Failover Manager may crash and will not be able to register the Trap Exploder properly. The EMC Smarts Failover System User Guide incorrectly lists the mixed-case value on Page 92.

IS-4931

### Resolution

Specify `--name=TRAP-INCHARGE-EXPLODER` in the Trap Exploder service install command. Page 92 of the *EMC Smarts Failover System User Guide* should read:

Configure the Trap Exploder service on Active and Standby locations

Install the service for the Trap Exploder on both the Active (Host A) and Standby (Host B) servers in the `--noregister` mode, using the following command:

Example:

```
./sm_service install --force --unmanaged --startmode=runonce \
'--name=ic-trapd-exploder' \
'--description=EMC Smarts SNMP Trap Exploder' \
'<BASEDIR>/SAM/smarts/bin/sm_trapd' \
'--name=TRAP-INCHARGE-EXPLODER' \
'--config=trapd' \
'--sport=2999' \
'--port=1025' \
'--model=sm_actions' \
'--rules=default' \
'--seed=seedfile' \
'--noregister'\
'--output=TRAP-EXPLODER-OI.log'
```

## Missing section in the Failover hook script in non root user mode for Linux

When any action script passes arguments to the hook script, there are missing quotes in the transfer command and remote command arguments.

This issue is seen in a multi collector failover scenario in non-root user mode. As a result the hook script is not able to parse the incoming arguments properly.

When the hook script gets executed, there is an error message. For example:

```
failover_post.pl': RC=2, result: Failed to bounce collectors: Unable
to connect to failover server: /usr/bin/ssh: [8] Cant find domain
'/usr/bin/ssh' in broker '10.241.172.73:1426', stopped at /data/
mensha/9.3_GCD/SAM/smarts/local/actions/failover_post.pl line 167 at /
data/mensha/9.3_GCD/SAM/smarts/perl/5.16.2/InCharge/remote.pm line
300.
```

SND-1871

### Resolution

Add the following section in the sample hook script after line 120.

```
#CHANGE THE VALUES AS SPECIFIED IN failover.conf
$transferCmd = "/usr/bin/scp -i /home/user1/.ssh/id_rsa";
$remoteCmd = "/usr/bin/ssh -i /home/user1/.ssh/id_rsa";
$failover_server_name = "FAILOVER";
$user = "user1";
#End of modification
```

Do this only when using multi collector failover functionality in non root user mode.

## Failover Manager sends data in clear text between Windows hosts

Failover Manager synchronizes data from the Active to Standby server like the repository, configuration files, and local scripts.

Data is not encrypted during this synchronization between Windows hosts.

SND-1848

### Resolution

You need to modify seven scripts in the `FAILOVER_BASEDIR/smarts/local/script` directory.

- `backup_actions.pl`
- `detach_sibling.pl`
- `failover_actions.pl`
- `restart_broker.pl`
- `restart_server.pl`
- `restart_service.pl`
- `resync_actions.pl`

## Edit Failover Manager scripts to correct clear text display between Windows hosts

Modify seven scripts in the `FAILOVER_BASEDIR/smarts/local/script` directory.

### Procedure

1. For each script, repeat Steps 1a-d:
  - a. Open the file with the `sm_edit` utility. For example, go to the `BASEDIR/smarts/bin` directory and open the `bootend.conf` file.  
  
Type `./sm_edit script/backup_actions.pl`
  - b. Locate the line, `$command = "$remoteCmd -NonInteractive "`
  - c. Add this line, `"-UseSSL -SessionOption $(New-PsSessionOption -SkipCACheck) "`

One blank space before the closing double quotation mark is required.

The modified code reads as follows:

```
. $command = "$remoteCmd -NonInteractive "
.   "\$host.UI.RawUI.BufferSize = "
.   "new-object
System.Management.Automation.Host.Size(512,50); "
. "Invoke-Command -Computername ${remote_host} "
. "-UseSSL -SessionOption $(New-PsSessionOption -
SkipCACheck) "
. "{ ${remote_basedir}/bin/sm_perl -e ' $script ' } ";
```

- d. Save the file.
2. Install self-signed certificates for server authentication on the Failover Manager's host and each Domain Manager's host (including hosts running SAM servers).

This uses `makecert`, which is available as part of the Windows 7 SDK. At the Windows command prompt, run the following command with your host name, organization name, and location:

```
makecert -sk itops-dev-239.lss.emc.com -ss My -sr localMachine -r -n "CN=itops-dev-239.lss.emc.com, O=EMC Corp, L=White Plains NY" -a sha1 -eku 1.3.6.1.5.5.7.3.1
```

- `-a sha1` specifies the cryptographic algorithm to use.
  - `-eku 1.3.6.1.5.5.7.3.1` makes the certificate good for Server Authentication.
3. Configure `winrm` to listen on HTTPS, instead of HTTP, on each host running a Domain Manager (including hosts running SAM).
- a. Get the thumbprint of the server authentication certificate created above.

For example, given the certificate created above, run the following command at the Windows command prompt: `powershell ls cert:\LocalMachine\My` and copy the thumbprint in the output (so you can paste it later).

Example of thumbprint output:

```
Directory:Microsoft.PowerShell.Security
\Certificate::LocalMachine\My
Thumbprint                               Subject
-----
38D1EE64C25E0C963962169EDA2A058BD68EE68F CN=itops-
dev-239.lss.emc.com, O=EM...
```

- a. Create a `winrm` HTTPS listener using the certificate. For example, at the Windows command prompt, run the following:

```
winrm create winrm/Config/Listener?Address=*
+Transport=HTTPS @{Hostname="itops-
dev-239.lss.emc.com";CertificateThumbprint="38D1EE64C25E0C96
3962169EDA2A058BD68EE68F";Port="5986"}
```

- b. Delete the HTTP listener. At the Windows command prompt, run the following:

```
winrm delete winrm/Config/Listener?Address=*+Transport=HTTP
```

- c. Verify that the HTTPS listener is active. At the Windows command prompt, run the following command:

```
winrm enumerate winrm/Config/Listener
```

You should see the HTTPS listener in the output, but not the HTTP listener. For example:

```
Listener
Address = *
```

```

Transport = HTTPS
Port = 5986
Hostname = itops-dev-239.lss.emc.com
Enabled = true
URLPrefix = wsman
CertificateThumbprint =
38D1EE64C25E0C963962169EDA2A058BD68EE68F
ListeningOn = 10.9.13.239, 127.0.0.1, ::1,
2001:0:9d38:6abd:147b:3010:f5f6:f210, 3ffe:80c0:22c:
84:7104:cca5:73f6:2657, fe80::5efe:10.9.13.239%11,
fe80::147b:3010:f5f6:f210%12, fe80::7104:cca5:73f6:2657%10

```

d. Open port 5986 in the firewall.

For the Windows firewall, click **Start > Administrative Tools > Windows Firewall with Advanced Security** to configure the firewall.

e. Try connecting to the Domain Manager host from the Failover Manager host, using Powershell. For example, at the Windows command prompt run:

```

powershell invoke-command -ComputerName itops-
dev-234.lss.emc.com -UseSSL -SessionOption $(New-
PsSessionOption -SkipCACheck) -ScriptBlock { hostname }

```

### Results

You should see the hostname of the Domain Manager's host, not the hostname of the Failover Manager's host.

## Linux non-root passwordless communication does not work after re-start

For Failover Manager, non-root passwordless communication does not work after ic-serviced is re-started.

SND-1496

### Resolution

The work-around is:

1. Edit /etc/init.d/ic-serviced.
2. Find the following line:

```
check_startup() {
```

3. Add these lines after done in the check\_startup section:

```

sleep 5
chown -R root:smartsgrp /var/smarts
sleep 5
chmod 770 /var/smarts/pipes/sm_service

```

The section should look like this:

```

check_startup(){
COUNT=1
while true
do
sleep 1
isRunning
if [ $? -eq 1 ]; then

```

```

        [ "$OS" = "Linux" ] && touch $LOCKFILE
        break
    fi
    COUNT=`expr ${COUNT} + 1`
    if [ ${COUNT} -gt 60 ];
    then
        echo "$SERVICED failed to start."
        exit 1
    fi
done
sleep 5
chown -R root:smartsgrp /var/smarts
sleep 5
chmod 770 /var/smarts/pipes/sm_service
}

```

#### 4. Save the file and exit.

Ignore SM\_RUNAS. Introduced in the 9.4 release, SM\_RUNAS should not be used. On Linux, it is incompatible with the way EMC Smarts servers start as root, open privileged ports, then change user to a specified non-root user. SM\_RUNAS is expected to be removed in the next release.

### The sm\_configureFailover.pl utility does not overwrite the failover configuration file

The sm\_configureFailover.pl utility does not provide an option to overwrite the failover configuration file. As a result, it appends duplicate domains.

CQ 654390

#### Resolution

Whenever you are editing the failover configuration files multiple times, either include comments for the previously added domains in the input file or use different input files.

### ASL errors in failover server logs when failover is started from ESM install

Errors appear in the server logs when you try to start the Failover server from ESM install location.

SND-1395

#### Resolution

Addressing this requires changes in ESM design to use init-settings file shipped with DMT. The workaround is to start the Failover server from other product installations like IP or SAM. Starting failover server from the ESM installation will not work. This is a legacy issue not specific to 9.4 release.

### Failover server is not getting registered to broker when failover is started from IP.

When Failover server is started from IP installations, where `SM_IP_VERSIONS=v6v4` in `runcmd_env.sh`, the Failover server tries to register itself with the Broker using the v6 port. This registration fails.

SND-1342

#### Resolution

Start Failover server specifying `--port=port_number`.

## EMC Smarts client program issues

The following issues are applicable if you are using EMC Smarts client programs from the terminal.

For example, these issues apply to the execution of the `dmctl` program from an `xterm` Window.

### Unexpected exit by client disables terminal echo (UNIX)

When the `clientConnect.conf` file is configured to prompt the user for a password, the terminal echo is disabled so that the typed password is not displayed. If the client program exits during the password prompt, the terminal's echo state remains disabled.

PR 6328 / CQ 257908

#### Resolution

To restore the terminal's echo state, type the following command: `% stty echo icanon`

Because the terminal echo is disabled, you will not be able to see the command as you type it.

### Unbalanced quotes in dmctl command causes dmctl to hang

Entering a `dmctl` command containing an unbalanced number of double quotation marks causes the `dmctl` program to hang.

The program hangs because it interprets the newline character as ending a quoted string and then continues to wait for a newline character that never comes.

For a similar reason, entering a `dmctl` command having an unbalanced (odd) number of single quotation marks causes the `dmctl` program to hang.

PR 15249 / CQ 213156

#### Resolution

EMC Corporation intends to modify its `quotedString` and `singleQuotedString` definitions in a future release to resolve the `dmctl` hanging problem. Until then, ensure that a `dmctl` command contains a balanced number of double or single quotation marks before entering the command. If the `dmctl` program hangs due to an unbalanced number of quotation marks, type an additional newline to complete the `dmctl` command.

### The sm\_getinfo utility generates error messages on Red Hat Enterprise Linux 7.2

The `sm_getinfo.pl` utility generates many error messages during execution on RHEL 7.2.

An example of the error message is:

```
Getting hardware Info...
/usr/bin/top: /opt/InCharge/SAM/smarts/lib/libz.so.1: no version
information available (required by /lib64/libdw.so.1)
```

SND-3645

**Resolution**

Workaround: To suppress the `no version information available` messages, rename the application shipped library so that the operating system libraries are taking precedence. To do so, type the command:

```
mv <Install>/smarts/lib/libz.so.1 to <install>IP/smarts/lib/old_libz.so.1.
```

**The sm\_getinfo utility generates exceptions on Linux**

On the Linux platform, the `sm_getinfo.pl` utility generates exceptions although the command works successfully.

An example of the error message is:

```
Output of ./bin/sm_perl ./bin/sm_getinfo.pl --help #####
defined(@array) is deprecated at /opt/InCharge/IP/smarts/bin/sm_getinfo.pl line 379.
```

CQ 654751

**Resolution**

Modify the `sm_getinfo.pl` script located in the `BASEDIR/smarts/bin` directory. Use the `sm_edit` command and replace Line 379 that reads:

```
if ( defined( @{$list_dir} )) {
```

with the following text:

```
if ( ( @{$list_dir} )) {
```

**FLEXnet issues**

The following issues relate to the FLEXnet license server.

**FLEXnet backward-compatible limitation for Windows**

For Windows only, FLEXnet software is not backward-compatible if it is installed on a dual stack system. An IPv4-specific application or product cannot connect to the FLEXnet license server version 10.8.5.0 that supports the IPv6 protocol even if the Windows system is configured as a dual stack machine.

**Configuring VENDOR line in the permanent license file**

Incorrect configuration of the VENDOR line in the permanent license file prevents startup of the EMC Smarts products.

PR 17543

**Resolution**

The VENDOR line includes the name of the vendor daemon for EMC Smarts (`sm_lmgrd92`) and the directory path to the vendor daemon.

In the VENDOR line of the permanent license file, replace `USER_DEFINED` with the directory path to the vendor daemon. For example, replace

```
VENDOR sm_lmgrd92 USER_DEFINED
```

with

```
VENDOR sm_lmgrd92 /opt/InCharge7/SAM/smarts/bin/system/sm_lmgrd92
```

See the *EMC Smarts Foundation System Administration Guide* for more information.

## IPv6 address fails for FLEXnet license server

When an EMC Smarts product resides on a system that uses only an IPv6 address and the FLEXnet license server resides on a dual stack system, the product cannot connect to the FLEXnet license server.

The IPv6 address was used for the SM\_LICENSE environment variable instead of the system name (hostname) with a port number (port@host). The variable is used in the runcmd\_env.sh file.

The following is an example of the error message that appears in the Manager's log file:

```
RSRV-E-ELICENSE-Unable to obtain license
LIC-ECHECKOUT-While attempting to check out license for AP_ICSRV
LIC-EGENERIC-License server machine is down or not responding.
. See the system administrator about starting the license server
system, or
. make sure you're referring to the right host (see
LM_LICENSE_FILE).
```

CQ 498689, CQ 415985, CQ 415658

### Resolution

The use of an IPv6 address to connect to a FLEXnet license server is not yet supported by Macrovision® Corporation. The IPv6 address does not resolve to a hostname. This issue has been submitted to Macrovision Corporation as ticket #SIOA-000116201.

Do not specify an IPv6 address for the environment variable SM\_LICENSE when you specify a system name (hostname) and a port number for port@host. For the host, acceptable values are either the system name (hostname) or an IPv4 address.

The value of this environment variable is either the full pathname to the license file itself, or it is port@host, which means that there is a FLEXnet license server running at that port on that host.

## Uninstalling permanent license does not remove cached license key

Once a permanent license is installed, it is cached in the registry key. When the license manager is removed, the key remains in the registry.

CQ 331608

### Resolution

Windows users must manually remove the registry key after the license manager is uninstalled. Use regedit for Windows.

Linux users need to remove /root/.flexlmrc.

## Technical notes

This release contains the following technical notes:

- [Replacing or importing TLS certificates](#) on page 42

## Replacing or importing TLS certificates

By default, a Smarts Domain Manager generates a self-signed TLS certificate that it will present to the incoming TLS connections.

You can configure a certificate to use by performing the following steps:

### Procedure

1. Place the certificate and key files in `$SM_SITEMOD/conf/tls/$DOMAIN.crt` and `$SM_SITEMOD/conf/tls/$DOMAIN.key` where `$DOMAIN` is the name of the domain used to register with the broker.

The files must be in PKCS#8, PEM encoded form with no password.

Self-signed certificates generated by Smarts are stored in the process memory.

2. To regenerate default self-signed TLS certificates, stop and restart the Smarts processes.

## Documentation

Relevant release notes for Service Assurance Suite include:

- *EMC Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers Release Notes*
- *EMC Smarts Network Configuration Manager Release Notes*
- *EMC M&R 6.6u2, 6.7, 6.7u1, 6.8u2, 6.8u5 Release Notes*
- *Service Assurance Suite SolutionPack Release Notes*
- [EMC Smarts foundation documentation](#) on page 42
- [EMC Smarts documentation](#) on page 43

Obtain product documentation including release notes and installation instructions on EMC Online Support at: <https://support.emc.com> **Support by Product > Product Name > Documentation** or from the EMC Community Network (ECN).

A Documentation Index with links to relevant articles and guides is available on the EMC Community Network. Log in and search for the Documentation Index for your product. (<https://community.emc.com/community/products>).

PDF portfolios are available for each domain manager, and these portfolios hold both version 9.4.x and applicable 9.x guides from earlier releases. Not all documentation is included in the PDF portfolios. Release notes and documentation in html format (such as SolutionPack articles, ICIM Reference or EDAA API guides) are posted outside of the portfolios.

## EMC Smarts foundation documentation

The Smarts foundation documents are product-independent and thus relevant to users of all Smarts products.

**Table 4** EMC Smarts Foundation documentation

Part number	Revision	Item
302-002-291	01	EMC Smarts Foundation System Administration Guide

**Table 4** EMC Smarts Foundation documentation (continued)

Part number	Revision	Item
302-001-491	01	EMC Smarts Failover System User Guide
302-003-636	01	Smarts Foundation EMC Data Access API (EDAA) Programmer Guide
302-003-637	01	Service Assurance Suite Alert EMC Data Access API (EDAA) Programmer Guide
302-000-676	01	EMC Smarts Foundation Common Information Model (ICIM) 1.11 Reference for Non-Service Assurance Manager Products (Applicable for all products except SAM)
302-000-677	01	EMC Smarts Foundation Common Information Model (ICIM) Reference for Service Assurance Manager (Applicable only for SAM)
302-002-289	01	EMC Smarts Foundation ASL Reference Guide
302-002-290	01	EMC Smarts Foundation Perl Reference Guide
302-002-287	01	EMC Smarts Foundation MODEL Reference Guide
302-002-288	01	EMC Smarts Foundation Dynamic Modeling Tutorial (Applicable only for SAM and IP)
Not applicable	Not applicable	FlexNet Publisher 11.12.1 License Administration Guide

## EMC Smarts documentation

These documents are relevant for the Service Assurance Suite 9.6 release:

**Table 5** Service Assurance Suite version 9.6 documentation

Part number	Revision	Item
302-004-755	01	EMC Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Release Notes
302-004-754	01	EMC Smarts Installation Guide for SAM, IP, ESM,

**Table 5** Service Assurance Suite version 9.6 documentation (continued)

Part number	Revision	Item
		MPLS, NPM, OTM, and VoIP Managers
302-004-756	01	EMC Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers Support Matrix
302-004-753	01	EMC Smarts Security Configuration Guide
302-004-785	01	EMC SAS 9.6 M&R Release Notes
302-004-778	01	Service Assurance Suite Installation and Configuration Guide for EMC M&R
302-004-857	02	EMC M&R 6.8u4 Security Configuration Guide
302-004-776	01	Service Assurance Suite Documentation Portfolio
302-004-757	01	Service Assurance Suite SolutionPack Release Notes
302-004-758	01	Service Assurance Suite SolutionPack Articles
302-003-617	01	EMC Smarts Server Manager User and Configuration Guide
302-004-752	01	EMC Smarts Server Manager Documentation Portfolio
302-004-761	01	EMC Smarts IP Manager Documentation Portfolio
302-004-760	01	EMC Smarts IP Manager Certification Matrix
302-004-762	01	EMC Smarts MPLS Manager Documentation Portfolio
302-004-773	01	EMC Smarts Network Protocol Manager Documentation Portfolio
302-004-772	01	EMC Smarts Optical Transport Manager Documentation Portfolio
302-004-759	01	EMC Smarts Service Assurance Manager Documentation Portfolio
302-004-775	01	EMC Smarts VoIP Availability Manager Certification Matrix

**Table 5** Service Assurance Suite version 9.6 documentation (continued)

Part number	Revision	Item
302-004-774	01	EMC Smarts VoIP Availability Manager Documentation Portfolio
302-004-777	01	EMC Service Assurance Suite Product Documentation Index

### The non-root user step in the Failover Guide passwordless procedure is incorrect

In the *EMC Smarts Failover System User Guide* (P/N 302-001-491 Rev 01), Step 8 on Page 27 in the Set up Passwordless Communication Between Active and Standby Hosts procedure is incorrect. You should uncomment the lines of code in Step 8.

IS-6525

### SNMP INFORMS is missing from SAM documentation

SNMP INFORMS information is missing from the SNMP Trap Adapter chapter in the *EMC Smarts Service Assurance Manager Adapter Platform User Guide*. The SNMP Trap Adapter or Trap Exploder processes the SNMP INFORMS packet. When the trap adapter successfully receives the SNMP INFORMS packet, it sends acknowledgment back to the Agent which sent the inform packet.

SND-197

### Notification Lifecycle Auditing feature is incorrectly mentioned as disabled by default

These errors are in the Lifecycle Auditing procedure in documentation.

In the *EMC Smarts Service Assurance Manager Configuration Guide*, it is incorrectly mentioned that the Notification Lifecycle Auditing feature is disabled by default. By default, the Notification Lifecycle Auditing feature is set to TRUE in Service Assurance Manager.

There is a spelling error in the command to enable Notification Lifecycle Auditing in the *EMC Smarts Service Assurance Manager Configuration Guide* (page 84). <Domain Name> is misspelled as <omain Name> in the command.

CQ 649806

### The useMIBThreshold attribute is missing from IP Manager documentation

The useMIBThreshold attribute is missing from IP Manager documentation. For IP Manager, the useMIBThreshold attribute is only applicable for two instrumentation classes of Cisco devices: VoltageSensor\_Fault\_CiscoEntitySensor and TemperatureSensor\_Fault\_CiscoEntitySensor.

IS-2156

### EMC Smarts Health Monitor may still appear in user documentation

EMC Smarts Health Monitor (SHM) was deprecated in 9.2.0.x and has been replaced by the SolutionPack for EMC M&R Health. Product user documentation may still mention EMC Smarts Health Monitor (SHM).

IS-3810, IS-4981

### Resolution

If any user guide refers to EMC Smarts Health Monitor or SHM, use the SolutionPack for EMC M&R Health instead.

## The Topology Split Manager service command is incorrect in the guide

For the Topology Split Manager on UNIX, the `sm_service install` command incorrectly lists the `--daemon` option in the guide.

IS-4005

### Resolution

Do not specify the `--daemon` option in the `sm_service install` command for the Topology Split Manager. In the *EMC Smarts Topology Split Manager User Guide*, on p. 24, the command syntax for UNIX should read:

```
/opt/InCharge/TSM/IP/smarts/bin/sm_service install
--force
--name=ic-tsm
--startmode=runonce
--description="EMC Smarts Topology Split Manager"
/opt/InCharge/TSM/IP/smarts/bin/sm_server
--name=INCHARGE-TSM
--config=icf
--bootstrap=bootstrap-tsm.conf
--port=0
--ignore-restore-errors
--noreconfigure
--output
```

## SystemRestarted event

These sections incorrectly document the conditions when IP Availability Manager considers the system to have been restarted:

- “Enabling the SystemRestarted and ConfigChange events”, on pages 49-52 of the *EMC Smarts IP Manager Version 9.2 User Guide*
- “Parameters for the SystemRestarted event” on page 249 of the *EMC Smarts IP Manager Version 9.2 Reference Guide*

Assuming that the SystemRestarted trap capability is enabled, the IP Availability Manager responds as follows upon polling a system and receiving a `sysUptime` value that is less than the `MaxUpTimeThreshold` value for consecutive polling cycles:

- Places the system on the Pending Devices list
- Generates a SystemRestarted trap for input to the Adapter Platform

During the next pending discovery, the IP Availability Manager will send SNMP polls to the system to rediscover the system and its components.

The polled `sysUptime` value for a managed system is compared to the `MaxUpTimeThreshold` value. If the `sysUptime` value for a system is less than the `MaxUpTimeThreshold` value, the IP Availability Manager considers the system to have been restarted.

CQ 652157

## Earlier version of documents are not removed after an upgrade

After an upgrade, the installer does not remove earlier version of documents at `BASEDIR/smarts/doc/pdf` folder.

CQ 640216

### Resolution

The `emc_important_notice.pdf` and the `thirdparty_copyright_readme.pdf` documents are applicable for the release.

## Enhanced Domain Audit Logging Format

Documentation for enabling Audit Logging in 9.2 EMC Smarts Service Assurance Manager Configuration Guide makes reference to directory that is not in the installation.

SND-323

### Resolution

The audit log contains one line per entry. The entry consists of multiple tab-delimited fields. The first N fields are of fixed meaning and order, with additional fields in a "tag=value" format. The tagged fields that are present depend on the action that is logged. Different actions will have different additional data available. For example, for an "invoke", the tag "oper" would indicate the operation being invoked.

The order of the tab-delimited fields in an entry is: `date login ID ClientDescription pid IP user@host action [tag1=value [tag2=value [...]]]`

**Example:** `2015/03/25 12:52:21 +442ms admin 2 dmctl 23168 127.0.0.1 root@host01.example.com createInstance object=MyClass::MyInstance`

### Note

This example text displays as one line in the log; the line is wrapped in this document.

**Table 6** Fixed field definitions

Field	Description
Date	The date and time at which the event occurred, formatted according to the setting of <code>SM_DATETIME_FORMAT</code> .
ID	The client identification number for this session.
Login	The login identifier used to authenticate to the domain
Client description	Information on the kind of client, eg <code>dmctl</code> , <code>console</code> , etc. This information is self-reported by the client as it cannot independently verified. A malicious user could conceivably forge this information.
PID	The process ID of the client on the system where the connection originated. This

**Table 6** Fixed field definitions (continued)

Field	Description
	information is self-reported by the client as it cannot be independently verified. A malicious user could conceivably forge this information.
IP	The network address of the system from which the connection originated. This is obtained from the network stack and is trustworthy, modulo presence of NAT between the domain and client. See Host, which may be of use in the presence of NAT.
User	The OS login name of the user on the system where the connection originated. This information is self-reported by the client as it cannot be independently verified. A malicious user could conceivably forge this information.
Host	The hostname of the system where the connection originated. This name is self-reported by the client and is subject to forgery. If there is any doubt, perform a reverse lookup on the IP provided instead. This field is provided as it may allow identification of individual clients behind a NAT, while a reverse lookup of the IP would resolve to a single router.
Action	The API operation called by the client. Most commonly, "put", "create", "delete", or "invoke".

Actions defined include the following. It is possible new actions may be added in the future. Many actions are read-only and thus would not appear in the audit log normally, and so are not listed here. Not all of these will be commonly seen.

**consistencyUpdate**

Requests that the codebook be recomputed.

**correlate**

Causes the domain manager to begin a correlation.

**create**

Create a new object instance in the domain. Tagged values include "object", the class name and instance name of the object to create.

**delete**

Delete the object with the given name. Tagged values include "object", the object to be deleted.

**exec**

Causes the domain to executes a program object (.po). Tagged values include "program"

**insert**

Add a new value to a table of an object. Tagged values include "attribute", which identifies the object and attribute to be affected, and "value", the desired new value.

**invoke**

Invoke a model operation. Tagged values include "object", the name of the object on which to invoke the operation, "oper", the name of the operation, and "args", the list of argument values.

**loadLibrary**

Requests that the domain manager load a shared library, such as one containing a compiled model. Tagged values include "library".

**loadProgram**

Request to load a program object (.po) into the domain. Tagged values include "program"

**put**

Sets an attribute of an object. Tagged values include "attribute", which identifies the object and attribute to be affected, and "value", the desired new value.

**remove**

Remove a value from a table of an object. Tagged values include "attribute", which identifies the object and attribute to be affected, and "value", the value to be removed.

**removeByKey**

Remove a value from a table of an object. Tagged values include "attribute", which identifies the object and attribute to be affected, and "key", the key of the value to be removed.

**restore**

Restore object instances from a file. Tagged values include "filename", the file to restore from.

**save**

Store the repository to a file. Tagged values include "filename", the file the objects will be stored in, and "class" if the request was to save a subset of instances by class.

**shutdown**

Requests that the domain manager shut down.

**transactionAbort**

Abort a previously started repository transaction.

**transactionCommit**

Commit a previously started repository transaction.

**transactionStart**

Start a repository transaction. Tagged values that may appear include:

- **args**  
A list of values used as argument to an operation.
- attribute**  
The fully-qualified name of an attribute of an object, in the format `ClassName::InstanceName::AttributeName`
- class**  
The name of a MODEL class.
- filename**  
The name of a file (whose use will be clear from the action)
- value**  
A value used as a table key.
- library**  
The name of a shared library
- object**  
The name of an object instance, in the format `"ClassName::InstanceName"`
- oper**  
The name of a model operation.
- program**  
The name of a program object (.po) loaded or executed
- value**  
The value of an attribute.

## Software media, organization, and files

Obtain product documentation including release notes and installation instructions for this product on EMC Online Support.

<https://support.emc.com> **Support by Product > Type a Product Name > Documentation.**

For product licenses, navigate to <https://support.emc.com> **Service Center > Product Registration & Licenses.**

### Installation executables

The names of the files comply with the following naming convention for EMC Smarts installation executables:

```
setup-<suite>-<version>-<os>.<bin|exe>
```

## Installation

For EMC Smarts products, in-place upgrades from 9.4 to 9.5.1 are supported. Migrations from 9.4 to 9.5.1 are supported.

The *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers* describes new installation, upgrade, and migration procedures.

## Troubleshooting and getting help

EMC support, product, and licensing information can be obtained as follows.

Product information

- For documentation, release notes, software updates, or for information about EMC products, go to EMC Online Support at: <https://support.emc.com>

Technical support

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



# CHAPTER 2

## Service Assurance Manager (SAM)

This chapter includes the following topics:

- [Service Assurance Manager overview](#) ..... 54
- [New features and changes in Service Assurance Manager \(SAM\)](#) ..... 55
- [Fixed Issues in Service Assurance Manager](#) ..... 55
- [Known problems in Service Assurance Manager](#) ..... 64

## Service Assurance Manager overview

EMC Smarts Service Assurance Manager (SAM) correlates topology and event data from multiple EMC Smarts managed domains to diagnose root-cause problems in the network. Managed domains can include IP networks, storage networks, routing protocols, ATM/Frame Relay, applications, and business entities.

When EMC M&R platform and the SolutionPack for EMC Smarts are deployed with Service Assurance Manager, these features may be accessed from the EMC M&R interface:

- Notifications
  - New reports
    - EMC Smarts Geography shows the Location on the map having Smarts network devices.
    - Physical Inventory by Device Group provides a list of device groups based on the device's vendor.
    - Physical Inventory by IP Network provides a list of devices configured over the IP networks
  - IP Configuration Manager settings such as polling and thresholds
  - Discovery and topology settings for underlying domain managers
- In addition, the EMC Smarts Failover System now supports failover of the services used to communicate between Service Assurance Manager and EMC M&R platform. The *EMC Smarts Failover System User Guide* provides more information.

These articles, available from the EMC support website or from the EMC Community Network, describe the EMC Smarts features when EMC M&R platform is deployed:

- *SolutionPack for EMC Smarts Summary Sheet*
- *How to Set Up SAM, EMC M&R, and the SolutionPack for EMC Smarts*
- *How to Maintain IP Manager Settings*
- *Troubleshooting the Deployment of SAM, EMC M&R, and the SolutionPack for EMC Smarts*

## New features and changes in Service Assurance Manager (SAM)

There are no new features in 9.6 release for SAM.

## Fixed Issues in Service Assurance Manager

Here are the fixed issues for Service Assurance Manager.

**Table 7** Fixed issues in Service Assurance Manager

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-10592 SR 09906348	Apache Tomcat needs enhancement/upgrade.	<p>The Tomcat version 8.0.38 has been upgraded to 8.5.27 and placed at the location, &lt;SAM_BASEDIR/SAM_CONSOLE_BASEDIR&gt;/smarts/local/tomcat. This ensures that SAM uses Tomcat version 8.5.27.</p> <p>The SAM product uses the Tomcat libraries for launching Web Consoles. The installation of SAM 9.4.2 Patch 27 removes Tomcat 8.0.38 library files and keeps them backed up as ZIP and TAR files. The uninstallation of this patch restores the library files to as they were before the patch.</p> <p>All Tomcat 8.0.38 files are backed up at the location:</p> <p>For Linux:</p> <pre>&lt;SAM_BASEDIR/SAM_CONSOLE_BASEDIR&gt;/smarts/tomcat.tar</pre> <p>For Windows:</p> <pre>&lt;SAM_BASEDIR/SAM_CONSOLE_BASEDIR&gt;\smarts\tomcat.zip</pre> <p>Post uninstallation, the tar/zip file will be extracted and the files will be placed back in path &lt;SAM_BASEDIR/SAM_CONSOLE_BASEDIR&gt;/smarts/tomcat.</p>	9.4.2.X	9.6

**Table 7** Fixed issues in Service Assurance Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
IS-10599 SR 09574096	The data from Smarts EDAA feed displays incorrect values for CurrentUtilization and PeerSystemName columns, which affect M&R report.	The missing fields of the map_containment table have been modified.	9.4.1.X	9.5.1
IS-10316 SR 09443963	The notifications are being generated for devices that are flagged as In Maintenance.	The maintenance notifications are by default acknowledged, and BIM does not schedule the devices in peer server if they are acknowledged. Now such constraint has been removed, because of which the devices are scheduled for maintenance by BIM and timestamp is getting populated in the passive SAM server.	9.4.2.X	9.5.1
IS-9903 SR 08933237	During the MSIT failover, the SAM-03 backup server hangs.	The SAM server hangs because of a deadlock between the sm_config and FastDXA for repository lock. Code has been modified so that the xml handler for BIMTopology can be made responsive to an ongoing DXA, and based on whether there is an ongoing postProcessing of DXA it takes repository lock.	9.4.2.X	9.5.1
IS-9904 SR 08933251	During the MSIT Failover, the OI server crashes.	An exception thrown from ci_vector has been handled such that the process continues execution. In case, the key is not found, a serverIF instance has been created for it and stored to the hashmap.	9.4.2.X	9.5.1
IS-8489 SR 07021932	In failover, SAM services do not respond.	Unescaping of special characters was not performed over a period of time. These escape characters were in huge numbers consuming a lot of memory and causing blockage for parsing.	9.4.1.X	9.5.1

**Table 7** Fixed issues in Service Assurance Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
		During topology sync, escaping has been performed in order to preserve the actual meaning of special characters inside topology. Unescaping was performed to maintain the special characters, which was recursive in nature. In some cases, this might lead to a stack overflow. This has been restricted by adding a limit to the number of recursions the logic can take.		
IS-9838 SR 88660290	The difference occurs in IP and SAM containment view for Aggregate instance. So, the column values does not match with column headers.	The issue has been resolved by implementing the modified MAP-CONTAINMENT.import in SAM and global SAM.	9.4.1.X	9.5.1
IS-9691 SR 08645777	The HostedBy relationship of IP address instances is null in OI.	When there are multiple book keeping from the same source for the relationship, it must avoid the null, invalid value.	9.3.0.X	9.5.1
IS-9345 SR 08194171	Unable to launch web Console.	There were issues with Jar signing, which has been addressed.  Note: It is recommended to upgrade the SAM Console from 9.4.2.x to 9.4.2 patch 12.	9.4.2.9	9.5
IS-8489 SR 07021932	SAM services do not respond.	After every topology sync, the additional escaping added to the topology buffer is removed.	9.4.1.X	9.5
IS-8972 SR 07729176	After the upgrade to 9.4.2 patch 9, the edaaClientConnect.conf file is not present in the <BASE-DIR>/smarts/conf, and is not being	Code has been modified to build the sub-system, by disabling the deletion of edaaClientConnect.conf file.	9.4.2.X	9.5

**Table 7** Fixed issues in Service Assurance Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
	passed to tomcat.			
IS-8346 SR 06477937	NOTIF issue occurs without delaying notifications.	Code has been added to change the behavior, where Auto-Acknowledge was calling changed function on the notification even if the notification is in the Active state.	9.4.2	9.5
IS-9036 SR 07496357	Acknowledge state is different between SAM services.	The notification property updation is done after the notify method is invoked on a notification, which prevents the acknowledged-active notification received from aggregate-sam to be set active-unacknowledged notification in presentation-sam.	9.4.2.X	9.5
IS-7120 SR 81325424	Alerts are not in synchronization between the SAM layers. The problem being addressed is: <ul style="list-style-type: none"> <li>Mismatch of alerts due to notifications from Trap and syslog adapter in OI Server.</li> <li>Mismatch of alerts due to InMaint and SchedMaint notifications.</li> </ul>	<ul style="list-style-type: none"> <li>In case of Manual failover and Automatic failover, in the new standby OI Server, the alerts existing from Trap adapter and syslog adapter will be cleared.</li> <li>When the sched Maint and InMaint notifications are cleared, those notifications gets acked by MBIM server, along with the ack operation, the changedoperation is also invoked on the notification which allows the ack message to be propagated to standby servers. This will allow, the cleared InMaint and SchedMaint alerts to be archived.</li> </ul>	9.4.0	9.5
IS-8106 SR 84438338	The dynamic model error message appears when the user tries to bring over the 'Type' properties from interface class in the IP domain	The 'Type' attribute has been removed from the 'TransportConnector' model class which eliminates the dynamic model error message.	9.4.2.X	9.5

**Table 7** Fixed issues in Service Assurance Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
	into the SAM domain.			
IS-7973 SR 84382184	The Failover manager version is not compatible with the latest version of Smarts Solution pack.	Failover manager had specific checks for 2.0 and 2.1 versions. This was added since the ways to update EDAA in MnR were different between both the versions. We now have removed the explicit checks and made it generalized since post 2.1, the mechanism to update EDAA remains the same.	9.4.2	9.5
IS-8037 SR 06274922	The smarts-edaa directory is missing.	The installation code has been modified to copy the war files from patch, rather than deleting from base installation.	9.4.1.X	9.5
IS-8022 SR 81714352	The SAM domain crashes on incorrect user login.	In Red Hat 7.0 there is a Unix user called admin. But this user is not configured with any password. So the getpwnam_r does not return a NULL but a spwd struct an empty password. This results in an ep value being NULL. And in this case we do a strcmp of ep and the fetched_pw resulting a sigsegv. Added ep == NULL condition to Authentication None.	9.4.1.X	9.5
IS-8058 SR 83809604	An additional source-notify messages are seen in SAM when there is no notify message seen in underlying domains.	The ics-nl-processing.asl file has been modified to prevent invoking ICS_Notificaiton::notify, when the notification from the same source exists as active notification in the sam / oi server.	9.4.2.X	9.5
IS-8105 SR 6249773	When copying fields in a SAM-to-SAM configuration, the DXA copies certain fields wrongly.	During clear message processing, the causes and causedBy fields are taken into consideration to fix the issue by resetting the O_FloatingImpacts variable.	9.4.1	9.5
IS-6357 SR 73823462	Errors occur when Smarts EDAA tries to	Edaa encryption support for communication between edaa and SAM server using the	9.4.1	9.5

**Table 7** Fixed issues in Service Assurance Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
	connect to a SAM domain.	edaaClientConnect.conf. Previously, the passwords in edaaClientConnect.conf was in plain text. It is possible to encrypt password in edaaClientConnect.conf using sm_edit and with this fix, the communication between edaa and SAM is taken care with encrypted passwords.		
IS-6816 SR 77784396	Cannot configure process monitoring (defining multiple templates with same processes).	Code has been updated to handle multiple templates with the same processes.	9.3.0.X	9.5
IS-6910 SR 78988586	Test SAM is very slow to update notifications from TEST IP AMPM domain.	When there is a burst of 1000s of events, the time taken for the notifications to be reflected in NL Console is huge due to impact updates for the events. This fix introduces a variable called SKIP_IMPACTS which when TRUE skips impact processing when events come in and schedules the same when the load on the server is less. This variable is present in ics-event-processing.asl.	9.4.1.1	9.5
IS-5643, IS-5655 SR 77068086, 77047430	Notification synchronization issue between Presentation and Aggregate SAM.	During short disconnect between SAM domains, the "hyper notif" driver(s) consistently would try to pull notifications from Aggregate SAM servers which would result in notifications going out of sync between the SAM domains. To avoid this scenario, the "hyper notif" driver(s) are explicitly stopped when DISCONNECT is received for Aggregate SAM server and restarted when a subsequent CONNECT is received.	9.2.2.X	9.5
Fixed problems in SAM 9.4.2				

**Table 7** Fixed issues in Service Assurance Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
IS-5263 SR 75849088	Trap Adapter is getting stuck and no trap flow via TE & TA.	Timeout of 600 seconds has been added to the trap drivers so that the remote calls timeout and continues its processing.	9.4.1.X	9.4.2
IS-3976 SR 71319566	PCI Scan for vulnerabilities made SAM unresponsive.	Changed the decodeURL method to calculate offset when encountering % character in URL. This was causing a heap memory corruption.	9.4.1.X	9.4.2
IS-6535 SR 79052820	Trap Exploder keeps crashing - Continuation to SAM forum post 69321.	Error handling added for wrong varbind values instead of crashing the server.	9.3.0.X	9.4.2
IS-5209 SR 73907876	Calling the "Pingall" command from a notification fails.	In Hierarchical setups, topmost SAMs have the next lower SAM in MemberOf relationships for devices. The script when executed on top level SAM executes the getIPs on the lower SAM which throws errors in the output since getIPs is not part of SAM domain. Have modified the code to handle this condition.	9.3.0.X	9.4.2
IS-4747 SR 73823462	Errors when Smarts EDAA tries to connect to a SAM domain.	Added the support for encryption in the edaaClientConnect.conf file.	9.4.0.X	9.4.2
IS-6786 SR 79676520	AggregateInterfaceLink data is not propagated from Aggregate SAM to Presentation SAM.	Added the entry in dxa-sam.conf file to propagate AggregateInterfaceLink data in hierarchical SAM setup.	9.4.1.X	9.4.2
IS-3877 SR 71952808	Seven out of eight trap threads hung on vxunbind trap.	Default event type defined if the event type value is misspelled by the user in the trap_mgr.conf file.	9.2.1.X	9.4.2
IS-4617 SR 73518426	Enrichment issue in UDF11-20 fields	Impact Offset was not getting reset while processing clear messages in ics-nl-processing.asl	9.4.0.X	9.4.2
IS-5888 SR 77770012	SAM Console installation on	Installer check for the compat-libstdc++-296-2.96-144.el6.i686	9.4.1.X	9.4.2

**Table 7** Fixed issues in Service Assurance Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
	RHEL 7.x requires an unavailable package.	has been removed since it is no longer supported in RHEL 7.X.		
Fixed problems in SAM 9.4.1				
IS-4010 SR 67325824/ SR 70386812	Traps from new source are not published in Adapter Platform (OI). Incoming NOTIFY traps are cleared when they should not have.	The trap manager was not considering the timestamp of incoming traps and in some cases could use previously received CLEAR traps to clear newly received NOTIFY traps. The code has been changed to consider the timestamp of a trap. Modified file: icoi-trapd/ trap_mgr_parse.asl	9.2.2.X	9.4.1
IS-4012 SR 69106668	Interface alerts active in ESM are not being passed through to SAM.	This could happen in situations when a notification is notified by multiple Domain Managers. If one of the Domain Managers disconnects, the notification in SAM changes to the WAS_ACTIVE status and further updates from other Domain Managers do not update the Source. Notification processing logic has been changed not to mark notifications as WAS_ACTIVE if there is another source Domain Manager listed as ACTIVE. Modified files: <ul style="list-style-type: none"> <li>Windows: lib\sm_ics_ems.dll</li> <li>Linux: lib/libsm_ics_ems.so</li> </ul>	9.2.2.X	9.4.1
IS-4016 SR 62373896	When running the failover actions script to activate SAM A from SAM B, the console did not follow the active SAM.	A deadlock situation during failover was creating this issue which has been fixed. Modified file: masterpiece.jar	9.1	9.4.1

**Table 7** Fixed issues in Service Assurance Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
IS-4221 SR 72253518	When services are restarted, the Trap Adapter is failing because Adapter Platform (OI) is on the Broker.			9.4.1
EMP-2927 SND-1424 / SND-2327 SR 67271642	Notification List created at Smarts SAM level is not showing in Watch4Net.	A flag ReplayNotificationsOnListCreation is introduced in the ICS_NLManager class. When TRUE, any change in notification lists or creation of notification lists will be updated without service restart. Modified files: <ul style="list-style-type: none"> <li>Windows: lib\sm_ics_ems.dll</li> <li>Linux: lib/libsm_ics_ems.so</li> </ul>	9.3	9.4.1
IS-2586 SR 69082894	SAM 9.4 crashes when MR_ManagedObject refined through Dynamic Model.	Redefinition of the classes already declared is removed which was resulting in crash while loading dynamically. Modified files: <ul style="list-style-type: none"> <li>Windows: lib\sm_storage_ext.dll lib/libsm_otm_sam.dll</li> <li>Linux: lib/libsm_storage_ext.so lib/libsm_otm_sam.so</li> </ul>	9.4	9.4.1
<b>Fixed problems in SAM 9.3</b>				
608594 605417 SR 56478058	On Windows, during Notification Archival, SAM domains crashed without coring and with no errors in the log files. Problem occurred because of an incorrect Buffer length used	Buffer length has been modified to the correct value. Modified file: sm_ics_ems.dll	9.2.0.1	9.3

**Table 7** Fixed issues in Service Assurance Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	during Notification Archival.			
614845 652313 SR 59076960	sm_config export generated invalid output xml syntax that sm_config was unable to import back.	Removed invalid Text element that were being added to the generated xml files. Modified file: sm_config	92.2.	9.3
649171 644708 SR 57172456	Certain attributes of Application class were not imported from ESM to SAM.	Resolved by modifying conf files and a model file to import the following properties to SAM: <ul style="list-style-type: none"> <li>• IsMissingProcess</li> <li>• MissingProcesses</li> <li>• IsCountThresholdViolated</li> <li>• CountThresholdsViolated</li> </ul> Modified files: <ul style="list-style-type: none"> <li>• dxa-esm.conf</li> <li>• dxa-sam.conf</li> <li>• esm_sam.mdl</li> </ul>	9.2.0.1	9.3

## Known problems in Service Assurance Manager

These problems affect Service Assurance Manager.

### EMC Smarts Service Assurance Manager with Notification Cache Publishing issues

The following issues arise when EMC Smarts Service Assurance Manager is configured with the Notification Cache Publishing option enabled.

You will observe some of these problems from the EMC M&R User Interface when the SolutionPack for EMC Smarts is installed. Related issues are described in the *Service Assurance Suite Release Notes for EMC M&R* and in the article, *Troubleshooting the Deployment of SAM, EMC M&R, and the SolutionPack for EMC Smarts* available from the EMC Support website.

#### Error message is displayed while scrolling down the notifications in M&R Smarts SolutionPack

Error message is displayed while scrolling down notifications in M&R Smarts SolutionPack, if the number of notification in SAM is more than 10k.

SND-5803

**Resolution**

You need to execute the following command in SAM to set the number of notification to be viewed:

```
curl -XPUT "http://<hostname or ip address of SAM>:9200/smarts/_settings" -d '{ "index" : { "max_result_window" : <no_of_Notification> } }'
```

**TLS errors are seen in the server log even after adding the flags in runcmd\_env.sh**

The Service Assurance Manager log file located in the `BASEDIR/smarts/setup/logs` directory contains Transport Layer Security (TLS) errors similar to the following:

```
[December 4, 2014 5:12:28 AM EST +600ms] t@409978624 HTTP #1
CI-E-EWHILE-While executing function ""CI_FlowTLS_U::handshake""
CI-CVFC-Certificate verification failure, code 11
CI-BSAFE-error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown
protocol: ; in file "s23_srvr.c" at line 1143
CI-TLSPE-TLS protocol error
```

**SND-1547****Resolution**

These TLS errors in the Service Assurance Manager log file might indicate that you have not upgraded the installation directory where EMC Data Access API (EDAA) is running. For example, in the deployment, 9.3 SAM with EDAA is communicating with 9.4 Domain Managers which is not a supported configuration.

Upgrade or migrate the SAM installation directory to version 9.4, as described in the *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers*.

In the meantime, use this workaround to prevent the TLS errors. For all of the 9.4 Domain Managers, include the environment variables, `SM_TLS_PROTOCOLS` and `SM_ALLOW_LEGACY_CRYPTO` in the `BASEDIR/smarts/local/conf/runcmd_env.sh` file.

1. Go to the `BASEDIR/smarts/bin` directory and enter this command to open the `runcmd_env.sh` file: `sm_edit conf/runcmd_env.sh`

2. Add the environment variables:

```
SM_TLS_PROTOCOLS=+TLSv1.1,+TLSv1
SM_ALLOW_LEGACY_CRYPTO=TRUE
```

3. Save and close the file.

**Inconsistent EMC M&R name in the 9.4 Global Console**

When the 9.4 Domain Manager Administration Console is attached to the 9.4 or 9.3 Server Manager, EMC M&R appears as a choice in the Configure ESM Credentials window. In the Polling and Thresholds Console, the W4NServer Polling Group and W4NServer Polling setting appear.

**SND-1718**

**Resolution**

No functionality is impacted because of this difference in the naming convention. The term EMC M&R replaces Watch4net or W4N.

**Discovery:** Clicking on Refresh launches the Topology tab instead of refreshing data in all tabs

Refresh is operational, however it takes the user to the first tab instead of refreshing all tabs.

SND-1352

**Resolution**

There is no work-around at this time.

**Browser refresh for the Configuration Manager polling and thresholds page loads with blank screen**

The Services ticket is appended to the URL in the browser when you refresh the polling and thresholds page for Configuration Manager in EMC M&R user interface.

SND-1339

**Resolution**

Delete the service ticket from the URL.

**Screen display is distorted in the user interface (Internet Explorer)**

Screen displays are distorted in the user interface when using Internet Explorer (IE) as the browser.

SND-1269

**Resolution**

Turn off compatibility mode setting when using Internet Explorer.

**Cannot use certain special characters when creating group names in EMC M&R with SolutionPack for EMC Smarts**

Special characters like the ampersand character, “&,” and | and spaces between the group name are not supported when naming groups. User-defined groups that are created with special characters like & , | and spaces will not render in group maps, even though there are device listed in the Centralized Management for those groups.

SND-1268, SND-2520

**Resolution**

Avoid use of the ampersand character, |, and spaces in names. Special characters other than the above mentioned characters are supported while creating user-defined groups.

**Manually reconfigure Broker in Data Collection and Events blocks in SolutionPack for EMC Smarts**

During Broker failover, Smarts Failover manager attempts to restart a failed Broker. If the Boker cannot be restarted, the Broker configured in the SolutionPack for EMC Smarts may not be accessible

SND-1635, SND-1240

**Resolution**

Manually configure the Broker in the Events and Data Collection sections of SolutionPack for EMC Smarts. Broker details present in Reports Section are automatically updated by Smarts Failover manager

The causedby info of INCHARGE-SA-PRES Down needs to be notified to the user in a failover scenario

When Service Assurance Manager with Notification Cache Publishing enabled is configured for failover, then any component UI service failure (SAM Server, Rabbit MQ, EDAA Service, or Elastic Search) will be treated as a SAM Server failure and will cause failover to occur.

These component UI services are not modeled as separate services. If there is a failover, the SAM failover event that is generated does not indicate which component service failed.

SND-347, SND-1005

**Resolution**

Execute the `sm_service show` command to determine which component UI service failed.

FIPS 140 mode limitation

If FIPS140 mode is enabled on a SAM installation hosting a Notification Cache and Notification Exchange, those features and related services will interoperate with FIPS-compliant SAM and other domains, but will not themselves operate in a FIPS compliant mode.

SMARTS EDAA is not FIPS 140 compliant

Service Assurance Manager supports FIPS mode when using the legacy console, but not when using the EMC M&R User Interface with the SolutionPack for EMC Smarts. The EMC M&R platform does not support FIPS mode.

If using SAM in FIPS mode, the Smarts EDAA can still be supported as an API, without EMC M&R. The Smarts EDAA will interoperate with Smarts domains in FIPS mode, but it will NOT itself operate using FIPS-compliant cryptography.

CQ 654162

**Resolution**

There is no workaround at this time.

SAM EDAA is not installed in silent mode during an upgrade

The EMC Data Access API (installed with Service Assurance Manager) is not installed in Silent mode during an upgrade.

This was observed when the new EDAA features were enabled in the response file prior to performing the upgrade. The feature was not installed.

CQ 654730

**Resolution**

Upgrade using GUI or Console mode and select the EDAA feature.

## Popout option in Notifications in EMC M&R User Interface shows blank page

Popout option in Notifications shows a blank page.

CQ 654719

### **Resolution**

The Pop-out option is no longer available as of release 9.4.1. Instead, in the EMC M&R UI, select **Tools > Display > View in Full Page**.

## The number of refresh cycles in which the action reflects in the UI is inconsistent

When you right-click on a Notification and select Acknowledge, the number of refresh cycles for each action is inconsistent.

CQ 654627

### **Resolution**

There is no workaround at this time.

## Last Clear attribute filter fails for "Never" value

In some notifications, the Last Clear column value is added as "never" instead of displaying the date.

The current filter on this attribute is currently based on Date and time. So the filter for the value "never" cannot be applied.

CQ 654612

### **Resolution**

There is no workaround at this time.

## Alert Service response feeds display host IP address instead of FQDN

AlertService response feeds display the host IP address instead of a Fully Qualified Domain Name (FQDN).

CQ 654569

### **Resolution**

- Ensure you configure SAM and EMC M&R hosts to use either FQDN or IP addresses. Do not mix them in your configuration settings.
- If the port on the Smarts EDAA host is set to something other than 8080, then SM\_TOMCAT\_SERVER must be set. For example, if the name of the SAM host is sam.example.com, but the URL other hosts know it by is not http://sam.example.com:8080, then you must edit runcmd\_env.sh and set SM\_TOMCAT\_SERVER=http://<public\_hostname>:<public\_port>.
- In the event that a misconfiguration occurs, the easiest way to fix it is to stop all the services, correct SM\_TOMCAT\_SERVER, clear the notification cache. The article, *Troubleshooting the Deployment of SAM, EMC M&R, and the Smarts SolutionPack* provides more information.

## Domain Tagging enabled devices are not seen in the Browse Details tab in EMC M&R

A device that displays in Availability Manager as DeviceA displays in SAM as DeviceA\_tag. There is an expectation that you will see DeviceA\_tag display in the EMC M&R interface in the Explore tree with the name, DeviceA.

CQ 654516

**Resolution**

There is no workaround at this time.

**Interoperability issue where ASAM Devices are not synchronized in the EMC M&R topology**

ASAM devices displayed in SAM topology may not display in the EMC M&R topology.

CQ 654447

**Resolution**

There is no workaround at this time.

**Notification Cache contains notifications from old server**

After SAM is restarted with a different RPS file, SAM publishes notifications in the new file to the cache, but has no way of knowing what was in the cache previously from the first RPS that is no longer valid.

The cache should be cleared before starting with a new RPS to ensure the cache is in sync with SAM. You have two options to synchronize SAM and the Notification cache:

CQ653789

**Resolution A: Stopping the SAM publisher to clear the Notification cache**

This is the recommended method of clearing the Notification cache. It has less impact on the system because you are only stopping the SAM Notification Cache Publisher.

## 1. Stop the Notification Cache Publisher

```
$ bin/dmctl -s INCHARGE-SA-PRES invoke
SM_AMQPNotificationPublisher::SM-AMQPNotificationPublisher stop
```

## 2. Clear the Notifications cache by typing these commands:

```
$ bin/sm_service stop smarts-elasticsearch
$ rm -rf local/repos/emc-alerts-es
$ bin/sm_service start smarts-elasticsearch
```

## 3. Restart the Publisher:

```
$ bin/dmctl -s INCHARGE-SA-PRES invoke
SM_AMQPNotificationPublisher::SM-AMQPNotificationPublisher start
```

**Resolution B: Stopping SAM to clear the Notification cache**

This method of clearing the Notification cache has a substantial impact on the system.

## 1. Stop SAM:

```
$ bin/sm_service stop ic-sam-pres
```

## 2. Clear the Notifications cache by typing these commands:

```
$ bin/sm_service stop smarts-elasticsearch
$ rm -rf local/repos/emc-alerts-es
$ bin/sm_service start smarts-elasticsearch
```

### 3. Restart SAM:

```
$ bin/sm_service start ic-sam-pres
```

## EMC M&R color changes apply only to the Notifications view

In the EMC M&R UI, if you change the colors of the notification severities in the Notifications view (Gear Wheel icon > Manage Colors), the changes apply to that specific Notifications view or report.

When you select a notification to examine its details, the color changes do not apply to the Notifications tab that appears in the Object Details view. The Object Details Notifications view uses the preset default color scheme.

CQ 652478

#### **Resolution**

There is no resolution.

## Multithreading issue in Smarts EMC Data Access API (EDAA)

All requests to smarts-edaa return error code 500 (Internal Server error). The smarts-edaa log shows stacktraces with java.lang.NullPointerException.

This may happen when multiple EDAA requests are issued simultaneously against newly started smarts-edaa service. The smarts-edaa log would contain java.util.ConcurrentModificationException logged shortly after the start of smarts-edaa.

CQ 616794

#### **Resolution**

Restart the Smarts Tomcat server.

## Misleading error message about Maintenance operation

When SAM is configured to send notifications to the EMC M&R User Interface, there is a misleading error message:

```
Maintenance Operation is not available for this object.
```

The user, in this scenario, does not have rights to place the notification in Maintenance. If you click on the notification in SAM (while logged as the user with the same profile), Maintenance is not an option.

CQ 616646

#### **Resolution**

There is no workaround at this time.

## EMC M&R Notifications view sort order unintentionally changes

In the EMC M&R UI, if your Notifications view does not include a unique field like Name or InternalEventHandle, the following user actions unintentionally change the sort order of notifications in the view: Ownership, Release Ownership, Acknowledge, and Unacknowledge.

CQ 616598

**Resolution**

Add a unique field like Name or InternalEventHandle to your Notifications view. To do so:

1. In your Notifications View, select the **Gear Wheel** icon and then **Multi Sort**.
2. In the Manage Default Sort dialog box, click **Add**.
3. In the added row, click the **Column** field and select Internal Event Handle.
4. Click **Save**.

**Add multiple notification views in EMC M&R User Interface**

If you need to configure multiple notification views in the same EMC M&R report, there are two choices.

1. Pin the report to My Reports multiple times. Then go to My Reports and arrange the multiple notification views however you want.
2. Use Edit mode to build a mixed report containing two or more notification views. Then copy and paste the existing notification view into another report.  
CQ 616543

**SAM configuration for CAS is not activated following SAM restart**

If you make configuration changes that affect the Notification Cache or Smarts EDAA, the changes do not take effect until you restart the Tomcat server.

Variables that may be affected include *SM\_TOMCAT\_SERVER*, *SAM\_CAS\_SERVER*, or *SM\_NO\_TLS* in the `runcmd_env.sh` file.

CQ 616342

**Resolution**

The method used to restart Tomcat depends on how it was started and which OS is in use.

**Linux service**

```
sm_service stop smarts-tomcat
sm_service show
sm_service start smarts-tomcat
```

**Linux interactive console**

Click `ctrl + c` from the window it was started in.

Use `sm_tomcat` to restart it.

This process needs to be changed in the normal ways if started in a console and then sent to background

**Windows service:**

Use the Service control panel to stop the service named "EMC Smarts Data Web Applications (Tomcat)"

Use the Service control panel to start the service named "EMC Smarts Data Web Applications (Tomcat)"

## Windows console

Click `Ctrl + C` from the window it was started in or close the window it is running in.

Use `sm_tomcat` to restart it

## Invalid return feed when executing console Operations like ack or take ownership

There is an invalid return feed.

Example: When issuing the Post on the URL below:

```
http://itops-qa-155.lss.emc.com:8080/smarts-edaa/msa/SAM-RMQP/instances/ICS_Notification::NOTIFICATION-Router_R1_Down/action/takeOwnership
{ "arguments": {
  "User" : "oper_123",
  "AuditTrailText" : "Venkat Test ack",
}
}
```

The output displays this feed:

```
<atom:title type='text'>Action Returns from Instance:
ICS_Notification::NOTIFICATION-Router_R1_Down,
ActionName:takeOwnership, Parameters:</atom:title>
<atom:id>http://itops-qa-155.lss.emc.com:8080/smarts-edaa/msa/
SAM-RMQP/instances/ActionReturn::1d033d0c-69b5-4a7a-9ef5-
db3bad0d8fc8</atom:id>
<atom:updated>2014-03-31T11:07:59-04:00</atom:updated>
<atom:link rel='self' href='http://itops-qa-155.lss.emc.com:
8080/smarts-edaa/msa/SAM-RMQP/instances/ActionReturn::
1d033d0c-69b5-4a7a-9ef5-db3bad0d8fc8' />
<atom:link rel='alternate' href='http://itops-
qa-155.lss.emc.com:8080/smarts-edaa/msa/SAM-RMQP/instances/
ActionReturn::1d033d0c-69b5-4a7a-9ef5-db3bad0d8fc8' />
<atom:link rel='http://schemas.emc.com/msa/common/reln/type'
href='http://itops-qa-155.lss.emc.com:8080/smarts-edaa/msa/SAM-RMQP/
types/ActionReturn' />
<atom:content type='application/xml'>
  <vsc:ActionReturn
    xmlns:vsc='http://schemas.emc.com/vs-xml/namespace/
Common/1.0'
    xmlns:inst='http://schemas.emc.com/msa/sam-
presentation/2.0'>
    <vsc:displayName>1d033d0c-69b5-4a7a-9ef5-
db3bad0d8fc8</vsc:displayName>
    <atom:link rel='self' href='http://itops-
qa-155.lss.emc.com:8080/smarts-edaa/msa/SAM-RMQP/instances/
ActionReturn::1d033d0c-69b5-4a7a-9ef5-db3bad0d8fc8' />
    <atom:link rel='http://schemas.emc.com/msa/common/
reln/type' href='http://itops-qa-155.lss.emc.com:8080/smarts-edaa/msa/
SAM-RMQP/types/ActionReturn' />
  </vsc:ActionReturn>
</atom:content>
</atom:entry>
</atom:feed>
```

Traversing the actionReturn feed gives an error because that type is not implemented:

```
<atom:feed
  xmlns:atom="http://www.w3.org/2005/Atom"
  xmlns:msa="http://schemas.emc.com/msa/common"
  xmlns:vsc="http://schemas.emc.com/vs-xml/namespace/Common/1.0">
<atom:title/>
<atom:updated>2014-03-31T11:10:45-04:00</atom:updated>
```

```

    <atom:author>
      <name>EDAA Feed</name>
    </atom:author>
    <atom:id>urn:uuid:4f2f45bb-4ea3-4181-bb80-f0fe799c6c28</atom:id>
    <atom:entry>
      <atom:title type="text">MsaError - Unknown type ActionReturn</
atom:title>
      <atom:id>http://itops-qa-155.lss.emc.com:8080/smarts-edaa/msa/
SAM-RMQP/instances/MsaError::4024</atom:id>
      <atom:updated>2014-03-31T11:10:45-04:00</atom:updated>
      <atom:link rel="http://schemas.emc.com/msa/common/reln/type"
href="http://itops-qa-155.lss.emc.com:8080/smarts-edaa/msa/SAM-RMQP/
types/MsaError"/>
      <atom:content type="application/xml">
        <vsc:MsaError
          xmlns:inst="http://schemas.emc.com/vs-xml/namespace/
Common/1.0"
          xmlns:vsc="http://schemas.emc.com/vs-xml/namespace/
Common/1.0">
          <vsc:displayName>Unknown type ActionReturn</
vsc:displayName>
          <inst:Code>4024</inst:Code>
          <inst:CodeString>msa.type.not.found.error</
inst:CodeString>
          <inst:ErrorMessage>Unknown type ActionReturn</
inst:ErrorMessage>
          <inst:RequestUri>http://itops-qa-155.lss.emc.com:8080/
smarts-edaa/msa/SAM-RMQP/instances/ActionReturn::
1d033d0c-69b5-4a7a-9ef5-db3bad0d8fc8</inst:RequestUri>
          <inst:Time>2014-03-31T11:10:45-04:00</inst:Time>
          <inst:Type>OPERATION_ERROR</inst:Type>
          <atom:link rel="http://schemas.emc.com/msa/common/
reln/type" href="http://itops-qa-155.lss.emc.com:8080/smarts-edaa/msa/
SAM-RMQP/types/MsaError"/>
        </vsc:MsaError>
      </atom:content>
    </atom:entry>
  </atom:feed>

```

**CQ 615921**

**Resolution**

There is no work-around at this time.

**If user profile doesn't exist on SAM, request /SAM/instances doesn't return an error**

If a user profile does not exist in SAM, request /SAM/instances does not return an error. It returns a feed without entries for ICS\_Notification and without scheduled Maintenance links.

**CQ 615717**

**Resolution**

Ensure user profiles are set up in the Service Assurance Manager and that corresponding EMC M&R user roles are configured operators are using EMC M&R to manage notifications.

## EMC Smarts Service Assurance Manager issues

The following issues apply to EMC Smarts Service Assurance Manager.

## The Web Console is not getting launched in the latest version of the browsers

The Web Console is not getting launched in the latest version of the following browsers:

- Chrome
- Firefox
- Internet Explorer
- Safari

SND-5743

### **Resolution:**

The support for NPAPI plugin, which is required for the launching the Web console has been removed.

To launch the Web Console on these browsers:

1. Launch the Web Console using the below URL:

```
http://<IP Address of SAM Console Server>:8080/webconsole/globalConsoleApp.jnlp
```

2. Download the .jnlp file manually and run it.
3. Authentication prompt to launch the Console will be displayed. Login to the Console using the username and password.

## SAM web console does not getting launched, when the console is installed in a Docker

When the SAM Console is installed inside the Docker container, after installation the following entry in the "globalConsoleApp.jnlp" is modified with the containers ip:

```
codebase="http://d1e7c521d3a4:8080"
```

Here localhost is replaced with d1e7c521d3a4.

SND-5780

### **Resolution**

The work-around is:

1. You need to modify the globalConsoleApp.jnlp file to reflect the container IP on which the docker is running (File path:<BASE\_DIR>/CONSOLE/smarts/tomcat/webapps/webconsole/globalConsoleApp.jnlp)

For example:

```
codebase="http://10.9.2.134:8080"
```

2. Restart the Tomcat services.

## The Web Console and Dashboard will not be launched in Google Chrome

The Web Console and the Dashboard will not be launched in Google Chrome 45 or later. Google has discontinued the support for NPAPI as of September 1, 2015. The deprecated support for NPAPI causes Java plugins to be disabled.

SND-2655, SND-2715

### **Resolution: EMC Smarts support for Google Chrome version 44**

To launch the Web Console and Dashboard on Chrome version 44 and versions prior to version 45:

1. Enable the NPAPI using `chrome://flags/#enable-npapi`.

2. Download the `jnlp` file from the Chrome browser (all versions).
3. Click on the `jnlp` file to launch the Global Console as a Java application outside of the Chrome browser:

```
http://hostname:8080/webconsole/globalConsoleApp.jnlp.
```

#### **Resolution: Launching the Dashboard for Google Chrome version 45 and later**

To configure the Dashboard to launch on Chrome version 45 and later:

1. Locate the sample `.iccon` files in the `CONSOLE\smarts\tomcat\webapps\templates` directory of SAM console installation.
2. In each of these `.iccon` files, update:
  - `<Host:Port>` with the hostname/IP address and port number of the SAM server.
  - `<SAM Server Name>` with the SAM server name.
3. In the SAM Global Console, click **File > Open > Open Local** and open the `CONSOLE\smarts\tomcat\webapps\templates` directory to select the sample console.

#### **Resolution: Launching the Dashboard for specific users**

To configure the Dashboard for specific users to launch on Chrome version 45 and later:

1. Locate the sample `.iccon` files in the `CONSOLE\smarts\tomcat\webapps\templates` directory of SAM console installation.
2. In each of these `.iccon` files, update:
  - `<Host:Port>` with the hostname/IP address and port number of the SAM server.
  - `<SAM Server Name>` with the SAM server name.
3. Create a directory with name of the user under the `SAM/smarts/local/consoles/` directory.  
For example for the administrator user, create: `/opt/InCharge/SAM/smarts/local/consoles/admin`
4. Copy the required sample `.iccon` file that you want to use for the user from the SAM console installation to the SAM server Installation.  
For example, copy the sample `.iccon` file from the `CONSOLE\smarts\tomcat\webapps\templates` directory to the `SAM/smarts/local/consoles/admin` directory.
5. In the SAM Global Console, the administrator clicks **File > Open > Open Remote**.
6. In the **Open Remote** dialog box, the administrator selects the required console from the **Load from** drop-down option and clicks **OK** to open the sample console.

### The 9.4.2 Web Console is not launching on the Internet Explorer 11 browser

When the Web Console is launched on the Internet Explorer (IE) 11 browser, it opens with a blank page, the Java loader does not load, and no error message appears.

SND-3897

#### **Resolution**

On the client host where the browser will be used, install JRE 1.8u91 before using the SAM Web Console.

## The 9.4.1 Web Console is not launching on the Internet Explorer browser

The Web Console does not launch on the Internet Explorer (IE) browser. Pop-up messages or information about missing plugins is not displayed.

SND-2700

### Resolution

The work-around is:

1. Update the following in the **Browser Compatibility** section for Internet Explorer:
  - a. Modify the Internet Explorer setting **Compatibility View Settings**.
  - b. Clear (uncheck) the checkbox **Disable Intranet sites in compatibility view**.
  - c. Reload the Web Console.

## globalConsoleCached.jnlp should be pointing to JRE version 1.8.25

There is no auto download for JRE 1.8u25 from Oracle. If you select, "Click here to download..." from jnlp, the JRE software does not download.

SND-1064

### Resolution

Manually download the JRE and install it in your environment. Then launch it again.

The "globalConsoleCached.html" will now work on all versions except IE 10 on Windows Server 2008 R2.

## "FibreChannelSwitch::FCSWITCH could not be created" messages in the SAM log file

The following incorrect "FibreChannelSwitch::FCSWITCH could not be created" messages are observed in the SAM log file during Topology sync from ESM to SAM, stating FibreChannelSwitch Objects could not be created, while later they were actually created.

### Example

```
DXA MESSAGE-E-DXA_ENOCREATE-ics-topology-sync.asl: [esm-92-lin5]
'FibreChannelSwitch::FCSWITCH-100000051E361F16' could not be created
```

```
[October 14, 2013 7:26:55 AM EDT +800ms] t@1343367488 esm-92-
lin5_Topo-Driver
```

```
DXA MESSAGE-E-DXA_ENOCREATE-ics-topology-sync.asl: [esm-92-lin5]
'FibreChannelSwitch::FCSWITCH-100000051E345472' could not be created
```

```
[October 14, 2013 7:26:55 AM EDT +801ms] t@1343367488 esm-92-
lin5_Topo-Driver
```

```
DXA MESSAGE-E-DXA_ENOCREATE-ics-topology-sync.asl: [esm-92-lin5]
'FibreChannelSwitch::FCSWITCH-1000000533A6AD0F' could not be created
```

```
[October 14, 2013 7:26:55 AM EDT +802ms] t@1343367488 esm-92-
lin5_Topo-Driver
```

```
DXA_MESSAGE-E-DXA_ENOCREATE-ics-topology-sync.asl: [esm-92-lin5]
'FibreChannelSwitch::FCSWITCH-10000005338FBFC2' could not be created
```

```
[October 14, 2013 7:26:55 AM EDT +932ms] t@1343367488 esm-92-
lin5_Topo-Driver
```

```
DXA_MESSAGE-E-DXA_ENOCREATE-ics-topology-sync.asl: [esm-92-lin5]
'FibreChannelSwitch::FCSWITCH-100000051E0E5D50' could not be created
```

```
[October 14, 2013 7:26:56 AM EDT +042ms] t@1343367488 esm-92-
lin5_Topo-Driver
```

```
DXA_MESSAGE-E-DXA_ENOCREATE-ics-topology-sync.asl: [esm-92-lin5]
'FibreChannelSwitch::FCSWITCH-100000051E3613F6' could not be created
```

CQ 609869 / CQ 609853

### Resolution

The log messages appear because of incorrect logging. Even if the log messages state that certain FibreChannelSwitch objects could not be created, they were later created properly in SAM. These log messages do not impact any functionality and can be ignored.

## SAM logs contains messages related to old active notifications

In 9.1, the SAM log file contains timer alarm messages for old notifications that are active. For example,

```
[November 3, 2012 9:32:11 PM GMT+05:30 +124ms] t@1227610432 INCHARGE-
ESM_Event-Driver
ASL_MSG-*-ASLP-ics/ics-event-processing.asl: TIMER_ALARM processing
oldNotification NOTIFICATION-
Interface_IF-172.16.42.2/2_InterfaceLostConnection
```

CQ 596145 / 576853

### Resolution

No functionality is impacted. These messages are useful in identifying the old notifications that are active when SAM reconnects.

## Delay in launching SAM Console on RHEL 6

SAM Console takes longer to launch on RHEL 6 as compared to RHEL 5. The shortage of entropy in the kernel's entropy pool was causing a delay in gathering bits of entropy from the entropy gathering device. By default, java uses file:/dev/random as the entropy gathering device which blocks bits of entropy during a shortage.

CQ 637437

### Resolution

Use cryptographically secure pseudo-random bits which do not block bits of entropy during a shortage. Pseudo random bits can be generated using `file:/dev/./urandom` as the entropy gathering device.

Type the following command to launch the SAM Console: `./sm_gui -Djava.security.egd=file:/dev/./urandom`

## Connected Systems details missing in containment view for VSS Port

The Connected Systems tab in the containment view for `VirtualSwitchSystemLink` port shows no data, except for the values for `IsUnresponsive` fields.

CQ 636049

### Resolution

EMC is investigating this problem. There is no known workaround at this time. However, the containment for `VirtualSwitchSystem` presents all the information, and the `VirtualSwitchSystemLink` data is present in the `TopologyBrowser` related to connected systems. Use the browse option to view this data.

## CE-VLAN ServiceOffering objects are not created for an underlying IP AM-PM domain

For the Metro Ethernet CE-VLAN impacted notifications feature, the Global Manager creates CE-VLAN `ServiceOffering` objects for an underlying IP Availability Manager (service type = AM), but not for an underlying IP Availability Manager and IP Performance Manager that are running as a single process (service type = AMPM).

CQ 575341

### Resolution

As a workaround, perform the following procedure:

1. Go to the `BASEDIR/smarts/bin` directory in the Global Manager installation area and type the following command to open the `dxa-post-hook-mvpn-dispnames.asl` file: `sm_edit rules/ics/dxa-post-hook-mvpn-dispnames.asl`  
Press `Enter`
2. Find the following line: `if ((domainObj->Type == ipamDomainTopologyType) {`
3. Add text to the line. For example: `if ((domainObj->Type == ipamDomainTopologyType) || (domainObj->Type == ipampmDomainTopologyType)) {`
4. Save and close the file.  
The modified version of the `dxa-post-hook-mvpn-dispnames.asl` file is saved to the `BASEDIR/smarts/local/rules/ics` directory.
5. If the Global Manager was running before you edited the `dxa-post-hook-mvpn-dispnames.asl` file, restart the Global Manager.

## Security certificate not loaded after enabling FIPS 140 mode

After enabling FIPS 140 mode, when you start the Broker and the SAM server, you may see the following error message in the server log:

```
CI-W-NOCGSS-No certificate loaded for INCHARGE-AM, generating self-signed certificate
```

This error is generated because FIPS 140 requires secure communication, which can be achieved using SSL. As this certificate is not available, the SAM Manager generates a self-signed certificate.

CQ 581691

**Resolution**

No functionality is impacted because of this error. You may ignore this error message.

**JIIM error messages displayed when OI server is started**

The following JIIM-related error messages is displayed in the `icoi-init.asl` file, when the OI server is started:

```
[August 12, 2011 4:51:08 AM GMT+05:30 +901ms] t@2532 InCharge
Framework
JIIM-E-SYS_EUNKNOWNERR-Attempt to log unknown error
'ICS_EINITMESSAGE' with severity 'W'
JIIM-SYS_EARG2-Argument 1: icoi-init.asl
. Argument 2: ICOI
[August 12, 2011 4:51:09 AM GMT+05:30 +042ms] t@2532 InCharge
Framework
JIIM-E-SYS_EUNKNOWNERR-Attempt to log unknown error
'ICS_ERECONFIGURERESULT' with severity 'W'
JIIM-SYS_EARG2-Argument 1: icoi-init.asl
. Argument 2: <reconfigure status="SUCCESS"
timestamp="1313104869"></reconfigure>Resolution
```

CQ 574710

**Resolution**

The resolution will be available in a future release.

**DISCARD\_TRAP displays incorrect values**

When configuring a trap adapter in `trap_mgr.conf`, the `my_trap_rules.asl` file is invoked on receipt of a trap. The `DISCARD-TRAP` variable in `my_trap_rules.asl` file registers the values as TRUE or FALSE, instead of YES or NO.

CQ 579129

**Resolution**

Using the `sm_edit` command, modify `rules/icioi-trapd/my_trap_rules.asl` to change the value for DISCARD\_TRAP to Yes or NO.

**ASL errors when stating up BIM with service groups & weights**

ASL errors are displayed when the SAM server is started after you enable the service groups in `service.group.data.template` and add the corresponding weights in `weights.conf` file to start the BIM functionality.

CQ 637304

**Resolution**

No functionality is impacted. The resolution will be available in a future release.

**IPv6 network cloud icon tooltip displays IPv6 keyword**

The tooltip is not displaying the correct keyword for the IPv6 network cloud icon.

CQ 413283

**Resolution**

The resolution will be available in a future release.

## Notify Business process event generates notifications with invalid inputs

When an invalid input, such as an alphabetical character, is provided as the severity under Notify Business process event server tool, the value is accepted and a notification with severity 5 is generated.

However, if a numeric value greater than 5 or less than 1 is provided as the severity, then an error message stating an invalid input is displayed.

CQ 579187

### **Resolution**

There is currently no resolution.

## Unable to launch Web Console when Tomcat is running on a non-default port

When the Web Console server is running on a non-default port, the Global Console could not be launched from the following URL:

<http://%3Ctomcat%3Ehost%3E:port/webconsole/globalConsoleCached.html>

CQ 578987

### **Resolution**

Update the `globalConsoleApp.jnlp` file under `BASEDIR/CONSOLE/smarts/tomcat/webapps/webconsole` with the non-default port number.

## Changes made by concurrent users fails to take effect

In SAM 9.1 when two administrators simultaneously try to make changes to System Defaults in the Global Admin Console, an error is displayed stating that the changes failed to take effect.

CQ 574176

### **Resolution**

Refresh the Global Admin Console, or close and reopen the console when the error occurs.

## Discovery Time Information dialog box issues

When the Discovery Time Information dialog box is started for one InChargeDomain instance, and then, without closing the dialog box, it is started for another instance, the action appears to proceed normally, but the information in the dialog box is not updated with the additional instance.

The dialog box only displays the first-selected instance. Also, the title of the dialog box does not display the domain name associated with the information.

CQ 466762

### **Resolution**

Each time you want to start a Show Discovery Time action, if a Discovery Time Information dialog box is open, close it (click OK at the bottom of the dialog), before starting the Show Discovery Time action. Then, start the Show Discovery Time action for the desired instance. The new Discovery Time Information dialog box lists information for the selected instance.

## Unable to put multiple interfaces in maintenance through a single entry

A separate entry is required in the configuration file for every interface that is placed in maintenance even though multiple interfaces have the same maintenance period.

CQ 424873

### Resolution

The resolution will be available in a future release.

## Support absent for IPv6 literal addresses in URLs

Microsoft Internet Explorer (IE) web browser running on Windows XP does not support IPv6 literal addresses in URLs.

This limits the IPv6 console support in the Web Console and Business Dashboard because the URL for the Business Dashboard and/or Web Console HTML file cannot be specified as an IPv6 literal address in IE. Microsoft documents this as a known limitation in "IPv6 for Microsoft Windows: [Frequently Asked Questions \(http://www.microsoft.com/technet/network/ipv6/ipv6faq.msp\)](http://www.microsoft.com/technet/network/ipv6/ipv6faq.msp).

---

### Note

Firefox and Mozilla web browsers support IPv6 literal addresses in URLs.  
CQ 367755

---

### Resolution

Use Firefox instead of Microsoft IE if you need to use an IPv6 literal address to access the Web Console or Business Dashboard.

## Incorrect certainty values displayed in Service Assurance Manager

When the Service Assurance Manager server subscribes to Adapter Platform notifications, the server ignores the certainty and smoothing parameters.

CQ 285466

### Resolution

Set up a notification list with an ASL filter which rejects anything with a certainty parameter value of  $\leq 0.1$ , and have the Service Assurance Manager server subscribe to that list.

If, at a later time, the notification was "bumped" for certainty above 0.1 and called on again, the ASL filter will notice it and display the notification in the Service Assurance Manager server.

## Tooltips display error

Tooltips are displayed only for Business Dashboard viewlets that are currently in focus. If you position the cursor over an item in a viewlet that is not in focus, no tooltip appears.

CQ 240014

### Resolution

To display tooltips in a viewlet other than the focused viewlet, click the second viewlet to cause it to gain focus. Tooltips will now appear associated with the second viewlet, but not with the former viewlet.

This issue is due to a change from Java 1.4.x to Java 1.5.x, and is described in the Sun Bug Parade Bug Report #6178004. A future release of Java is expected to permit re-enabling of tooltips for all viewlets, including those which are currently not in focus.

### File exported using sm\_xml command is saved in wrong location

When a file is exported using the sm\_xml command and only the filename is specified, it is incorrectly saved in the `BASEDIR/smarts/bin` directory. The file should be saved in the `/xml-if/directory` or in the location that is mentioned.

CQ 578675

#### Resolution

By default, the exported file is saved in the current directory unless the full path is provided.

### InMaintenance Events does not run at the defined time period

The InMaintenance event runs at some random time, even though the time period is specified correctly in the Schedule Maintenance event.

This is observed when the device is placed in maintenance during topology synchronization. The SAM-DXA-DRV driver holds a Writelock, and takes more time to process the groups and their relationship. Meanwhile, the ICS-MaintenanceHandler-Driver is waiting with a Readlock and is not able to process the Schedule Maintenance notifications.

CQ 578710

#### Resolution

- Avoid scheduling devices for maintenance when topology synchronization is in progress.
- When no devices are scheduled for maintenance, add the devices to a new group before starting the ICS-Group-Driver.
- Break groups that contain large number of devices into subgroups to reduce the number of devices being scheduled for maintenance in each subgroup.

### Errors generated during a 'get' operation

Performing a 'get' operation on an attribute that has an <unknown> or uninitialized value, generates errors.

The generation of the XML file is not affected due to these errors, except that the attributes are skipped from the XML file.

CQ 503274

#### Resolution

You may ignore this message.

### Unable to use special characters for user authentication

Users are unable to use the <SYS> option in the `serverConnect.conf` file.

CQ 574301

#### Resolution

There is currently no resolution for this issue.

## Event flooding causes sm\_adapter to backlog trouble tickets

An alarm flooding occurred while starting the adapter service, resulting in 7000 plus events queuing up for action.

CQ 550582 / 544652

### Resolution

Subscribe to a customized Notification List containing adequate filters to avoid unwanted notifications.

## Web Console or viewlets may run out of memory

Depending on the heap space (“heap size”) configured for the web browser in which the Web Console or Business Dashboard runs, the Web Console or the viewlets in the Business Dashboard may run out of memory.

By default, the Web Console and viewlets allocate less heap space than the Global Console. Less heap space may result in out-of-memory errors in the Web Console or viewlets. For example, an out-of-memory error may occur in a Web Console that heavily uses large map background images.

### Resolution

If the Web Console or viewlets run out of memory, adjust the maximum amount of heap space that the Java Plug-in uses for dynamic memory allocation. For example, by specifying `-Xmx256M` as a runtime parameter you can increase the heap space allocation to 256 MB. The number can be set larger or smaller than 256 MB, depending on the resources available on the client machine running the web browser.

To increase the heap space for the Java Plug-in:

1. Launch the Java Plugin Control Panel. For instructions, see <http://java.sun.com/j2se/1.5.0/docs/guide/deployment/deployment-guide/jcp.html>.
2. In the **Java Plug-in Control Panel**, click the **Java** tab.
3. In the **Java** tab page, click **View** in the **Java Applet Runtime Settings** box.
4. The **Java Runtime Settings** dialog box appears.
5. In the **Java Runtime Settings** dialog box, in the **Java Runtime Parameters** text entry field for your JRE, type the maximum heap-space runtime parameter (`-Xmx`) and a value for the parameter. For example, `-Xmx256M`
6. **Save** your entry. Click **OK** to close the Java Runtime Settings dialog box. Then click **OK** to close the Java Control Panel.  
Close and restart any web browser running on the host machine.

## Topology Builder refers to Web Transaction Recorder

The Topology Builder includes references to the Web Transaction Recorder. This Application Insight component is only available for deployments supported by Custom Engineering.

CQ 236798

### Resolution

No user action required.

## Status Table Console does not refresh correctly

The Status Table Console does not refresh correctly after a secondary class instance is deleted from the topology.

CQ 237076, CQ 239182

### Resolution

User action is not required.

## ASL errors in MBIM log file

The following ASL error is displayed in the bim-maint-monitor.asl file located under SAM\smarts\rules\bim folder:

```
[August 23, 2011 4:13:34 PM EDT +664ms] t@5616 ICS-MaintenanceMonitor-Driver
ASL-W-ERROR_RULE SOURCE-While executing rule set 'E:\data\SAM\8.1.1_upgrade\SAM\smarts\rules\bim\bim-maint-monitor.asl'
ASL-ERROR_ACTION-While executing action at:
  ASL-CALL_STACK_RULE-   RuleName: PARSE_MESSAGE, Line: 88
  ASL-CALL_STACK_RULE-   RuleName: START, Line: 39
ASL-ERROR_INVOKE-While attempting to invoke operation 'start' of object 'GA_Driver::ICS-MaintenanceCleanup-Driver'
MR2-MR_WHILE_OPERATION_INVOKE-While invoking operation start in object 'GA_Driver::ICS-MaintenanceCleanup-Driver'
MR-OBJECT_NOT_FOUND_EX-Cannot find object 'GA_Driver::ICS-MaintenanceCleanup-Driver'
MR-CALL_ON_NULL_OBJECT-Tried to make a call on a NULL repository object; in file "t:/DMT-9.1.0.X/1358/smarts/repos/servif/SM_RepositoryServer.c" at line 1089
```

CQ 574754

### Resolution

No functionality is impacted because of this error. You may ignore this error message.

## Related classes are not added or deleted from Domain Manager Console

When you add or delete topology from a domain (either with a seedfile or by adding an agent), the Domain Manager Administration Console may not show the changes in the related classes.

For instance, if you add a Router, the Cards and Interfaces that are added to the topology may not appear in the topology tree.

CQs210866, CQ 211641

### Resolution

Refresh the tree to see the instances of component classes that were added or deleted from the topology. To refresh the tree:

1. Right-click on the tree window.
2. Click **Refresh**.

## Copy function does not update domain group name in Notification Log Console Source field

When creating a new domain group that includes domains named with identical domain names of an existing group, the domain names are not unique. This results with the existing domain group name appearing in the Notification Log Console Source field,

which is not accurate. The new domain group name needs to appear in the Notification Log Console Source field.

---

#### Note

If you create a new group by copying an existing group and giving the new group new unique domain names, notifications being sent to the Service Assurance Manager from either groups are distinct and the information displaying in the Source field is accurate.

---

#### Resolution

To display the new domain group name in the Notification Log Console Source field:

1. Disable the existing group and click **Reconfigure**. All notifications being sent from the this group are cleared.
2. Create the new group.
3. Verify that the new group is enabled.  
By default new groups are enabled.
4. Click **Reconfigure**. All notifications sent from the previous domain group are resent with the new domain group name appearing in the **Notification Log Console Source** field.
5. Delete the previously existing group.

### Program list is blank when creating client tools from Web Console

The Program list is empty when creating client tools from the Web Console.

CQ 397507

#### Resolution

In a Windows environment, copy the client action script files you are interested in from your Service Assurance Manager installation to an actions/client directory located on your machine's desktop. This results in the action script files displaying in the client tools Create and Modify list box of the Global Administration Console.

You can also type a name of a script directly into the Program list box to create (or modify) client tools in the Web Console. This can be useful when administrators have different client tools available to them than the script's target users because the script name does not display in the Program list box but can still be typed manually into the Program list box and used by the administrator.

## NOTIF issues

The following are issues may occur when using NOTIF.

### NOTIF Editor drop-down menus are difficult to read

NOTIF Editor drop-down menus blackout on Windows 7 Enterprise Edition operating system. The menu items can only be read if you hover the mouse over individual menu items.

CQ 637954 / 576383

#### Resolution

Change the compatibility mode of the "javaw" executable for the JRE shipped with your SAM Console using the following steps:

1. Go to the BASEDIR/smarts/jre/bin folder.
2. Right-click on **javaw.exe**.
3. Go to the **Compatibility** tab.
4. Change the compatibility to **Windows 2008 Server (SP1)**.
5. Click **Apply** > **OK**.
6. Restart NOTIF.

## Lag in NOTIF thread startup

In the event where NOTIF does not start within the default of 20 seconds, while starting the SAM or OI server, it is expected that the NOTIF thread is killed and servers start processing events.

However, NOTIF thread starts after a delay. Hence, when the servers are started, both NOTIF and general event processing run in parallel. This issue is usually observed when servers are started in the FIPS-140 mode.

CQ 581805 / 581848 / 581808

### Resolution

In case the SAM server is installed in a low performance server, the wait time for the Domain Manager must be configured to a higher value. As such, the default value for the “maxNotifWaitTimer” parameter in the ics-event-processing.asl file has been set to 60 seconds. This file is located in the SAM server installation area in the BASEDIR/smarts/conf/ics folder.

## Display issues in NOTIF Editor tree view

The following issues were found in the NOTIF Editor tree view.

- The left pane does not display correctly when the user adds an element to multiple packages.
- Extra branches were found where none should exist.
- Changed fields between saves were not shown.
- A selected object in the NOTIF Editor does not show updates related to file import.

### Resolution

There is no workaround for these NOTIF Editor display issues.

## Undefined variables or run time errors delay NOTIF processing

The presence of undefined variables in ASL hook scripts or run time errors during execution significantly slows down NOTIF processing.

### Resolution

Define all variables in ASL hook scripts to ensure that NOTIF processing is efficient. If the hook script is making a remote call, add ? LOG , IGNORE at the end of the command to avoid runtime errors.

## Original EVM objects reappear in table

When EVM objects are modified or deleted from the NOTIF user interface, the original objects reappear in the table when a **Retrieve the running configuration from the server** operation is performed to overwrite the configuration to the server.

CQ 543791

**Resolution**

Delete any unwanted EVM objects stored in the `BASEDIR/smarts/local/logs/<server name>.running.ncf` file before performing a reconfiguration.

**Packages are not deleted from the NOTIF server**

When packages are deleted from the NOTIF user interface, they start reappearing when a Retrieve the running configuration from the server operation is performed to overwrite the configuration to the server.

The instances belonging to the packages are deleted whereas, the main entries remain because of which the packages reappear.

CQ 543983

**Resolution**

Delete the package information stored in the `BASEDIR/smarts/local/logs/<server name>.running.ncf` file before performing a **Retrieve the running configuration from the server** operation.

**Incorrect trap count for momentary notifications part of NOTIF NCI aggregation**

In the SAM console, if a NCI is aggregated from momentary trap notifications, then the count of those momentary notifications is greater than the correct number by 1.

CQ 579079

**Resolution**

There is currently no resolution.

**Notification Log Console opens directly in browser window when using Web Console**

Launching a Notification Log Console from the Web Console opens a blank console, which is embedded within the browser window. But, launching a new Notification Log Console or other consoles such as, Global Manager Admin Console or, topology browser, launches the console outside the browser window.

CQ 574276

**Resolution**

Click on **File > Topology browser** to launch a topology browser for the attached domain manger.



# CHAPTER 3

## IP Manager (IP)

This chapter includes the following topics:

- [IP Manager overview](#) ..... 90
- [New features and changes in IP Manager \(IP\)](#) ..... 90
- [Fixed issues in IP Manager](#) ..... 105
- [Known problems in IP Manager](#) ..... 135

## IP Manager overview

IP Manager includes the following products:

- IP Availability Manager
  - IP Performance Manager
  - IP Availability and Performance Manager
  - IP Server Performance Manager
  - IP Availability Manager Extension for NAS
- IP Server Performance Manager is an enhanced version of IP Performance Manager and is available through a feature license.

In this document, “IP Manager” is used to collectively represent IP Availability Manager, IP Performance Manager, and IP Server Performance Manager.

## New features and changes in IP Manager (IP)

There are no new features in 9.6 release for IP.

## Maintain IP Manager Settings from the EMC M&R interface

There is now support for IP Configuration Manager in the EMC M&R interface.

The article, *How to Maintain IP Manager Settings*, available in the IP Manager Documentation Portfolio on support.emc.com or from the Documentation Index on the EMC Community Network, provides more information. You must install the IP Configuration Manager, the Service Assurance Manager and EMC M&R with the SolutionPack for EMC Smarts in order to configure polling and threshold settings from the EMC M&R interface.

## Reference information from the 9.3 release applicable to 9.4 installations

These changes were introduced in the 9.3 release. They are included here for your reference:

- [Vblock certification for IP Manager](#) on page 90
- [Enhancement to Wireless Discovery](#) on page 91
- [Configuration Manager in CLI mode](#) on page 92
- [New IP Manager classes for host resource objects](#) on page 94
- [New IP Manager class for IP storage paths](#) on page 99

## Vblock certification for IP Manager

Vblock System 300 will now be discovered and managed by IP Manager.

CQ 654545

1. VCE Vblock devices will be discovered as ConvergedInfrastructureManager [CIM] in SMARTS-IP. The sysOID of the Vblock model certified in IP 9.3 is:

```
.1.3.6.1.4.1.38819.1.5.10.300.4 (vb300modelFX)
```

2. Discovery is based on Vision SNMP Agent running on the VCE Vblock and the Entity-MIB providing the serial numbers of the components within the VBlock, which should be synonymous with the serial number returned by the SNMP agent

on the individual devices. Based on this co-relation the components will be discovered as part of ConvergedInfrastructureManager.

If this co-relation does not exist, the individual components will still be discovered and displayed on the topology based on their device type. If the serial number co-relation exists, the CIM will display the following relationship:

CIM -> composedOf -> individual components of the Vblock.

#### RCA limitation

- If the CIM VCE SNMP agent is Down, it does not imply that the individual Vblock components (UCS, Nexus, or MDS Switch) are Down.
- If all the components of a Vblock are down and the CIM VCE SNMP agent is also down, all the components will send individual Down notifications.
- The CIM VCE SNMP Down notification will not suppress the individual component Down alarms.  
Therefore, the RCA limitations preclude an optimal behavior under the current implementation. Future releases might provide finer control of alarm suppression.

## Enhancement to Wireless Discovery

Wireless discovery was enhanced in the 9.3 release.

### Threshold Settings

Here are the available threshold settings for WirelessAccessPoint.

To change Threshold settings for WirelessAccessPoint, access **Polling and Threshold > Threshold > SystemResourceGroup > WirelessAccessPoint > Settings**.

**Table 8** WirelessAccessPoint threshold settings

Threshold setting	Default value	Description
MaxAPRetentionTime Threshold	0 (in seconds)	This is the time duration for which the WirelessAccessPoint is retained after getting disassociated from the WirelessController. If APRetentionTimeThreshold < (Current time — WAPDownAt), then after rediscovery of WirelessController, the WirelessAccessPoint is removed from the topology.

### Attributes of WirelessAccessPoint

Here are the attributes that define the class, WirelessAccessPoints.

**Table 9** Attributes of WirelessAccessPoints

Attributes	Value	Description
APRetentionTimeThreshold	Integer	Determines the time duration for which the WirelessAccessPoint is retained in the topology after getting disassociated from the WirelessController. If APRetentionTimeThreshold < (Current time — WAPDownAt), which means ElapsedTime since AP went down is greater than APRetentionTimeThreshold, then after rediscovery of the WirelessController, the WirelessAccessPoint is removed from the topology.
WAPDownAt	Integer	Indicates the time when the WirelessAccessPoint went down.

## Enhancement to WirelessAccessPoint discovery

A parameter has been added to the `tpmgr-param.conf` file.

**Table 10** Parameters in tpmgr-param.conf file

Attributes	Value	Description
EnableRogueAPDiscovery	TRUE	Determines the discovery of Rogue Access Points.

## Configuration Manager in CLI mode

The Configuration Manager provides a method for applying a consistent set of polling and threshold settings to all target domains.

It is now possible to apply the polling and threshold settings to target domains with the Configuration Manager import file.

### Note

Each Polling &Threshold group of settings in the import file starts with the keyword, `config`.

Each group of configurations is separated from the next group by a blank line.

## Modify the polling and threshold import files

Apply the polling and threshold setting to the target domain.

### Procedure

1. List the domain names in the import file just after the group name of the settings using the domain name separator "|" followed by ":".

2. Use the regular expression `*ampm*` to apply the setting across all 3 domains as shown below:

```
config Proxy Devices: ampm3|ampm2|ampm3
match IsProxy TRUE
priority 10300
param IsReadOnly FALSE
param Description
setting Connectivity_ExternalPolling_Setting
param InstrumentBlades FALSE
param InstrumentIPs TRUE
param InstrumentCards FALSE
param InstrumentFibreChannelPort FALSE
param InstrumentNetworkAdapters TRUE
param DisplayName Connectivity Polling - External Poller
param InstrumentComputeFabricManager FALSE
param AnalysisMode ENABLED
param InstrumentSNMPAgents TRUE
param InstrumentEVCEndPoints FALSE
param InitialStatus UNKNOWN
param Description
```

---

#### Note

If nothing is specified after the config group, `*` is assumed the default, and the settings are applied to all the target domains.

---

## Adding additional group of settings to the Configuration Manager using import file

The easiest method of adding settings to the Configuration Manager is to first import all common Polling and Threshold settings, and then add other domain specific groups.

### Procedure

1. To create the import file, first generate a common group of settings by selecting the domain with the most common set of Polling and Threshold settings . Export them from that domain using the command:

```
./sm_perl sm_settings.pl -s ampm1 -export=cm-export
```

The export file `cm-export` is written to the `BASEDIR/IP/smarts/local/logs` directory.

If some of your target domains have settings that are unique for that domain you can add domain specific settings by editing the exported file and including the domain specific settings that are required to be added to the Configuration Manager.

2. Import settings to the INCHARGE-CM. Settings defined in this file will be applied to all target domains added to the Configuration Manager with below mention commands.

```
./sm_perl sm_settings.pl -s INCHARGE-CM --import cm-export
```

## Usage notes for adding settings with the import file

If you are adding a certain settings for a domain that is not yet managed by configuration manager, then this domain will be added as a target.

- The settings added using import file are not pushed by default to the target domains. This is done as a precaution and you can push the settings after you have verified them.
  - If you would like to skip the verification step you can use `--force` option. This helps in applying in the settings to target domains without any verification.
- Verify your settings by attaching Domain Manager Admin Console to the Configuration Manager. Browse to the settings and verify that settings are added to the correct target domains defined.

## New IP Manager classes for host resource objects

Release 9.3 introduced two new classes for IP Manager that enable you to discover and monitor groups of processors and memory on hosts:

- MemoryGroup
- ProcessorGroup

### MemoryGroup attributes

Key attributes for the MemoryGroup class are provided here.

**Table 11** Attributes for MemoryGroup

Attribute	Description	Allowed values
AverageFreeMemoryPct	The average percentage of free memory. Computed as an average of FreeMemoryPct from all the Memory instances in ComposedOf.	Double
AverageFreeMemoryThreshold	The threshold for minimum amount of free memory (AverageFreeMemoryPct) expressed as a percentage of the total amount of memory.	Integer
AverageFreeMemoryExceededTime	Indicates the absolute timestamp when the value of IsAverageFreeMemoryExceeded changed the last time.	Integer
FreeMemory	The total amount of free memory currently available in KBytes on this device. Computed as a sum of FreeMemory from all the Memory instances in ComposedOf.	Unsigned-Long
IsAverageFreeMemoryExceeded	TRUE, if the value of AverageFreeMemoryPct is	Boolean

**Table 11** Attributes for MemoryGroup (continued)

Attribute	Description	Allowed values
	below AverageFreeMemoryThreshold.	
IsInsufficientFreeMemoryActive	TRUE, if the InsufficientFreeMemory event is active on the group.	Boolean
NumberOfMemoryInstances	Total number of Memory instances in this group.	Integer
SmoothingInterval	Indicates the interval in seconds to smooth/delay the InsufficientFreeMemory event. Default: 0.	Integer
TotalMemory	The total amount of memory in KBytes present on this device. Computed as a sum of TotalMemory from all the Memory instances in ComposedOf.	Unsigned-Long

## ProcessorGroup attributes

Key attributes for the ProcessorGroup class are provided here.

**Table 12** Attributes for ProcessorGroup

Attribute	Description	Allowed values
AverageUtilization	The average value for CurrentUtilization of Processors in the ComposedOf relationship.	Numeric (float)
AverageUtilizationThreshold	The upper threshold for ProcessorGroup average utilization expressed as a percentage of the total utilization.	Integer
IsAnyProcessorUtilizationHigh	TRUE if any of the Processors in this group are reporting HighUtilization.	Boolean
AverageUtilizationExceededTime	Indicates the absolute timestamp when the value of IsAverageUtilizationExceeded changed the last time.	Unsigned-int
IsAverageUtilizationExceeded	TRUE, if the value of AverageUtilization has exceeded AverageUtilizationThreshold.	Boolean

**Table 12** Attributes for ProcessorGroup (continued)

Attribute	Description	Allowed values
IsHighUtilizationActive	TRUE, if the HighUtilization event is active.	Boolean
IsEveryProcessorUtilizationHigh	TRUE if all of the Processors in this group are reporting HighUtilization.	Boolean
NumberOfProcessors	Total number of Processors in this group.	Integer
SmoothingInterval	Indicates the interval in seconds to smooth/delay the HighUtilization event.	Unsigned-int
UtilizationAlertMode	Indicates the mode in which HighUtilization is alerted for Processor elements. Possible values: <ul style="list-style-type: none"> <li>PROCESSOR_ONLY - Events on Processor instances only</li> <li>PROCESSORGROUP_ONLY - Events on ProcessorGroup instances only</li> <li>PROCESSOR_AND_PROCESSORGROUP - Events on Processor and ProcessorGroup instances</li> </ul>	Enum: <ul style="list-style-type: none"> <li>PROCESSOR_ONLY</li> <li>PROCESSORGROUP_ONLY</li> <li>PROCESSOR_AND_PROCESSORGROUP</li> </ul>

### ProcessorGroup relationship

The ProcessorGroup class has a `ComposedOf` relationship which consists of all Processor instances that are part of the ProcessorGroup.

### MemoryGroup and ProcessorGroup Notifications for IP Manager

Vendor-specific notifications are listed here.

**Table 13** Vendor-specific notifications

Network objects	Events	Description	Threshold
Memory	InsufficientFreeMemory	Indicates that the system is running out of memory resources.	FreeMemoryThreshold SmoothingForInsufficientMemory
MemoryGroup	InsufficientFreeMemory	Indicates that the system is running out of the memory resources and the percentage of average free memory is	MemoryGroupUtilizationThreshold SmoothingForMemoryGroupUtilization

**Table 13** Vendor-specific notifications (continued)

Network objects	Events	Description	Threshold
		below the value of the AverageFreeMemoryThreshold attribute.	
Processor	HighUtilization	Indicates that the utilization of the systems processor exceeds UtilizationThreshold.	ProcessorUtilizationThreshold ProcessorUtilizationAlertMode SmoothingForProcessorUtilization
ProcessorGroup	HighUtilization	Indicates when the ProcessorGroupUtilizationThreshold of the ProcessorGroup exceeds the threshold, the HighUtilization event becomes active based on the smoothing interval value.	ProcessorGroupUtilizationThreshold ProcessorUtilizationAlertMode SmoothingForProcessorGroupUtilization

## Thresholds settings for MemoryGroup and ProcessGroup for IP Manager

Default threshold settings for IP Manager are listed here.

**Table 14** Default values for threshold settings

Parameters	Thresholds	Default value	Description
Processor and Memory Thresholds	MemoryGroupUtilizationThreshold	20	The threshold for minimum amount of free memory on the group utilization expressed as a percentage of the total memory.
	ProcessorGroupUtilizationThreshold	90	The upper threshold for processor group utilization expressed as a percentage of the total capacity of the processor.
	SmoothingForMemoryGroupUtilization	0	Interval to smooth/delay the InsufficientFreeMemory Event (secs) By default value is set to 0 sec which means there is no delay introduced
	SmoothingForProcessorGroupUtilization	0	Interval to smooth/delay the HighUtilization Event [secs] By default value

**Table 14** Default values for threshold settings (continued)

Parameters	Thresholds	Default value	Description
			is set to 0 sec which means there is no delay introduced
	ProcessorGroupUtilizationThreshold	90	The upper threshold for processor group utilization expressed as a percentage of the total capacity of the processor. This setting is applicable to Hosts only.
	MemoryGroupUtilizationThreshold	20	The threshold for minimum amount of free memory on the group utilization expressed as a percentage of the total memory. This setting is applicable to Hosts only.
	SmoothingForInsufficientMemory	0	Interval to smooth/delay the InsufficientFreeMemory Event [secs] By default value is set to 0 sec which means there is no delay introduced.
	SmoothingForProcessorUtilization	0	Interval to smooth/delay the HighUtilization Event [secs] By default value is set to 0 sec which means there is no delay introduced.
	SmoothingForProcessorGroupUtilization	0	Interval to smooth/delay the HighUtilization Event [secs] By default value is set to 0 sec which means there is no delay introduced.

**Table 14** Default values for threshold settings (continued)

Parameters	Thresholds	Default value	Description
			This setting is applicable to Hosts only.
	SmoothingForMemoryGroupUtilization	0	Interval to smooth/delay the InsufficientFreeMemory Event [secs] By default value is set to 0 sec which means there is no delay introduced.  This setting is applicable to Hosts only.
	ProcessorUtilizationAlertMode	PROCESSOR_AND_PROCESSORGROUP	Indicates the mode in which HighUtilization is alerted for Processor elements. PROCESSOR_ONLY - Events on Processor instances only.  PROCESSORGROUP_ONLY - Events on ProcessorGroup instances only.  PROCESSOR_AND_PROCESSORGROUP - Events on Processor and ProcessorGroup instances.  This setting is applicable to Hosts only.

## New IP Manager class for IP storage paths

Release 9.3 introduced a new IPStoragePath class for IP Manager that enables you to discover and monitor the topology in network paths from an ESX Host instance to a file server instance for Network attached storage (NAS) data transfer.

### IPStoragePath class

An IPStoragePath is a logical entity which represents possible network paths from an ESX Host instance to a file server (FileServer) for Network attached storage (NAS) data transfer in an IP network.

Note that there can be multiple paths between the same end points (same FileServer and ESX Host).

## IPStoragePath configuration parameters

To discover an IPStoragePath instance or to enable or disable difference features for the IPStoragePath, configure the parameters.

**Table 15** Discovery.conf and tpmgr-param.conf file parameters for IPStoragePath

Parameters	Default value	Description
discovery.conf file		
DisableIPStoragePathDiscovery	TRUE	Enables or disables IPStoragePath discovery in the IP Manager topology. An IPStoragePath is a logical path from a FileServer to an ESX Host. An IPStoragePath contains all physical nodes and connections which form the IPStoragePath.  To discover IPStoragePath, set the value to FALSE.
DisableIPStoragePathVLANCheck	TRUE	Enables or disables VLAN checking during the discovery of IPStoragePath in the IP Manager topology. When VLAN checking is enabled, it does not create any IPStoragePath if there is a VLAN mismatch in the path. The VLAN mismatch checking is only valid when the FileServer and the ESX Host are in the same IPNetwork.  This parameter is only valid when IPStoragePath discovery is enabled (DisableIPStoragePathDiscovery is set to FALSE).
IPStoragePathHopCount	10	Determines how many hops (nodes) to travel in a particular topology to find the IPStoragePath. After traversing the specified number of nodes, the IP Manager discovery process stops searching for the IPStoragePath. This is used to stop the unnecessary traversal of the topology, when you know how many hops (nodes) are between a FileServer and an ESX Host in their topology.

**Table 15** Discovery.conf and tpmgr-param.conf file parameters for IPStoragePath (continued)

Parameters	Default value	Description
		This parameter is only valid when IPStoragePath discovery is enabled (DisableIPStoragePathDiscovery is set to FALSE).
tpmgr-param.conf file		
IgnoreVlanList		Is a list of VLANs to be excluded for VLAN mismatch checking during the creation of an IPStoragePath. This is only valid if the DisableIPStoragePathVLANCheck and DisableIPStoragePathDiscovery parameters are both set to FALSE in the discovery.conf file. Add the list of VLAN number entries.  Example : IgnoreVlanList 20 10 300

## IPStoragePath Relationships

An IPStoragePath has the following relationships:

- A\_End relationship with NetworkAdapters of the FileServer (Ports, Interfaces, AggregatePorts), which is the starting point of the IPStoragePath.
- ComposedOf relationship with AggregateLink, AggregatePort, Cable, Card, FileServer, Host, Interface, Port, TrunkCable, NetworkConnection, Blade, BladeEnclosureManager, Switch, Router, and any Relay Device (Firewall, LoadBalancer, for example).
- ConnectedSystems relationship with FileServer and Host (the two endpoint nodes of the IPStoragePath).
- Z\_End relationship with NetworkAdapters of the ESX Host (Ports, Interfaces, AggregatePorts), which is the end point of the IPStoragePath.

## IPStoragePath attributes

Key attributes of IPStoragePath are provided here.

**Table 16** Attributes of IPStoragePath

Attributes	Description	Values
HostEnd	Is the ESX Host Name, one end of the IPStoragePath.	Any ESX Host
IPStoragePathKey	Is the unique key for an IPStoragePath.	Integer

**Table 16** Attributes of IPStoragePath (continued)

Attributes	Description	Values
Path	Is the list of nodes (FileServer, Switch, Router, Host, and so on) in the order in which they are discovered in the IPStoragePath, separated by <-> characters.	String
StorageEnd	Is the FileServer, one end of the IPStoragePath.	Any FileServer

### Discovery steps for IPStoragePath

Perform these steps to discover the vCenter with IP Manager.

#### Procedure

1. Set the DisableIPStoragePathDiscovery parameter to **False** in the BASEDIR/smarts/conf/discovery/discovery.conf file.
2. For VLANs:
  - a. If VLAN checking is needed, set the DisableIPStoragePathVLANCheck parameter to **False** in the BASEDIR/smarts/conf/discovery/discovery.conf file.
  - b. If you want to ignore any VLAN, add that VLAN to the IgnoreVlanList parameter in the BASEDIR/smarts/conf/discovery/tpmgr-param.conf file.  
If VLAN checking not needed, ignore this step.
3. If the FileServer and the ESX host are more than ten hops away, increase the value of the IPStoragePathHopCount parameter in the discovery.conf file from 10 to any other suitable value.
4. Discover the two-end points of IPStoragePath FileServer and ESX Host in IP Manager.
5. Discover all of the relay devices (Router/Switches/Firewall/LoadBalancer etc.) which are in the path of the IPStoragePath.
6. Discover the host (vCenter in which this particular ESX is using NAS Datastore).
7. In Server Manager, do the following:
  - a. Configure the credentials for the above mentioned vCenter.
  - b. Discover the vCenter.

The *EMC Smarts Server Manager User and Configuration Guide* provides information about configuring the vCenter credentials and discovery.

### Managing the IPStoragePath class

Perform these steps to manage the IPStoragePath class.

#### Procedure

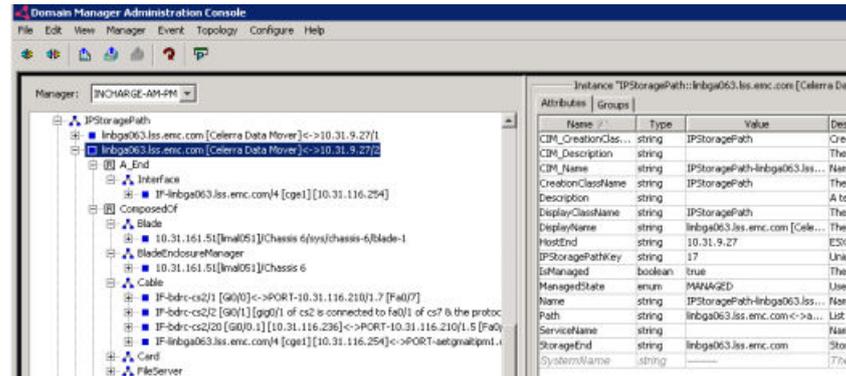
1. Open the Domain Manager Administration Console.
2. Expand the IPStoragePath class and right-click on the IPStoragePath instance.

3. Select **Manage** or **Unmanage**.

The ManagedState attribute for the IPStoragePath class changes to EXPLICITLY\_MANAGED or EXPLICITLY\_UNMANAGED. By default, the value of ManagedState is MANAGED.

**Topology tree example with the IPStoragePath class**

**Figure 1** Example of an IPStoragePath instance



**Extending support for discovery of iSCSI- and FCoE-based IPStoragePath**

Support for the existing IPStoragePath class for IP Manager is extended to allow discovery and monitoring of the topology in network paths from an ESX Host instance to storage arrays connected through Fibre Channel over Ethernet (FCoE) and Internet Small Computer System Interface (iSCSI).

Here are the configuration parameters and attributes.

**Table 17** IPStoragePath configuration parameters

tmpmr-param.conf file	Description
VnxHostSysOids	This parameter should contain a list of VNX Block Array SNMP Host SystemObjectOIDs. This list is used to identify Hosts that are of VNX Block Array type when IPStoragePath is created on IP Domain Manager. Use this syntax while adding new OID's to the list. [Separate entries with PIPE( )]. Example: VnxHostSysOids . 1.3.6.1.4.1.1981.1.1 .  . 1.3.6.1.4.1.311.1.1.3.1.2

**Table 18** IPStoragePath attributes

Attribute	Description	Values
IPStoragePathType	The type (NAS, SAN_iSCSI or SAN_FCoE) of the IPStoragePath	Examples: UNKNOWN,NAS, SAN_iSCSI and SAN_FCoE. Attribute available on IPStoragePath class present

**Table 18** IPStoragePath attributes

Attribute	Description	Values
		in the ESM Server Manager topology.

**Note**

FCoE-based IPStoragePath is supported only in an environment where the VNX host and ESX host are connected via Fiber Channel Brocade 8000 switches. Currently VNX hosts with sys-oid ".1.3.6.1.4.1.1981.1.1" and Brocade 8000 switch with sys-oid ".1.3.6.1.4.1.1588.2.1.1.1" are supported. No other vendors are supported at this time.

**Discovery steps for IPStoragePath (extended support)**

In IP Manager, perform the following steps:

**Procedure**

1. Set the DisableIPStoragePathDiscovery parameter to False in the BASEDIR/smarts/conf/discovery/discovery.conf file.
2. For VLANs (If VLAN checking not needed, ignore this step.)
  - a. If VLAN checking is needed, set the DisableIPStoragePathVLANCheck parameter to False in the BASEDIR/smarts/conf/discovery/discovery.conf file.
  - b. If you want to ignore any VLAN, add that VLAN to the IgnoreVlanList parameter in the BASEDIR/smarts/conf/discovery/tpmgr-param.conf file.
3. If the FileServer and the ESX host are more than ten hops away, increase the value of the IPStoragePathHopCount parameter in the discovery.conf file from 10 to any other suitable value. Do the same for iSCSI- and FCoE-based IPStoragePath where StorageArray host and the ESX host are separated by more than ten hops.
4. Refer to the *EMC Smarts Server Manager User and Configuration Guide* for the configurations that are required to discover FCoE based IPStoragePath in IP Manager.
5. Discover the two-end points of IPStoragePath as FileServer or Storagearray and ESX Host in IP Manager.
6. Discover all of the relay devices (Router/Switches/Firewall/LoadBalancer etc.) which are in the path of the IPStoragePath.
7. Discover the host (vCenter in which this particular ESX is using NAS Datastore or the iSCSI/FCoE DataStore).
8. In Server Manager, do the following:
  - a. Configure the credentials for the above mentioned vCenter.
  - b. Discover the vCenter.

The *EMC Smarts Server Manager User and Configuration Guide* provides information about configuring the vCenter credentials and discovery.

## Enhancement for IP network failures on virtual infrastructures

Server Manager monitors and performs root-cause analysis on the logical network paths and their components for Network attached storage (NAS) or Storage Array data transfer failure in an IP network.

The logical network path is represented as an IPStoragePath instance in the topology. The two end-points of the path are ESX Host and FileServer or StorageArray. The components of the path include ESX Host, File Server or StorageArray(Host), any relay device (Switches, Router, Firewall, etc.), VMware Datastores, virtual machines, and so on. This feature is supported for NAS, iSCSI and FCoE.

To enable this feature, the FileServer or StorageArray(Host), ESX Host, vCenter Host, and relay devices which are on the path between the ESX Host and Fileserver or StorageArray(Host) should be discovered with the parameter DisableIPStoragePathDiscovery set to false in IP Manager and in Server Manager. The vCenter credentials (where the particular ESX Host is using NAS or StorageArray) should be configured and that particular vCenter needs to be discovered.

You can configure the IP Manager to discover:

- IPStoragePath as part of VMware management configuration
  - IPStoragePath class in Server Manager topology
  - VMware Datastore management
- For IP Manager feature information about IPStoragePath, consult the "New IP Manager class for IP storage paths" in *EMC Smarts Server Manager User and Configuration Guide*.

## Correlating IPStoragePath performance exception to VM performance

Performance analysis is available for NAS/iSCSI/FCoE-based storage. This feature lets you identify the root cause for VM performance issues when there are no physical failures.

"PerformanceAffected" event on the IPStoragePath gets explained by one or more NetworkAdapter Performance problems such as HighBroadcastRateActive, HighCollisionRateActive, HighDiscardRateActive, HighErrorRateActive, HighQueueDropRateActive, HighUtilizationActive and so forth.

The *EMC Smarts Server Manager User and Configuration Guide* provides information.

## Fixed issues in IP Manager

Here are the fixed issues for IP Manager.

**Table 19** Fixed issues in IP Manager

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-12148 SR 11869635	The IP domain crashes during domain reconfiguration while processing Manage/Unmanage policies (script if-provision-setting.asl).	IP domain crashes during reconfigure (while managing/unmanage operation) due to a looping relationship between Aggregateport/AggregateInterface and ports/interface. SMARTS tries to iterate through the layeredOver relationship and ends up in a recursive call and gradually	9.5.1.0	9.6

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		exhausting the stack and crashing. As part of the fix, a rule have been introduced in post processing to detect and eliminate such looping relationship thus presenting a non-recursive layering in AggregatePorts/AggregateInterface before managing/unmanaging them.		
IS-11510 SR 10764921	The user is not able to poll InputPacketQueueDrop Pct attribute because it does not show proper value in GUI. Hence monitoring is impacted.	A locking mechanism has been added for attribute InputPacketQueueDropPct which ensures the access will be made through #MR_Refs#.	9.5.0.6	9.6
IS-11325 SR 10784189	When the user tries to reconfigure the ReconfigureAfterPush parameter in GUI as false, the IP Configuration Manager does not have any effect.	Code has been modified to ensure that the ReconfigureAfterPush parameter has an effect when the reconfiguration is triggered once the flag is set by the user.	9.5.0.0	9.6
IS-11390 SR 10941677	Interfaces for Juniper are not getting discovered.	The issue was with the snmpGetnext call that was not parsed for obtaining the next index. The logic has been modified to accommodate parsing of the index and obtain the subsequent value.	9.5.0.0	9.6
IS-11679 SR 92928642	The pending list discovery fails to rediscover in IP 9.4.2.26.	An inappropriate call-resolver function was called which could not resolve the hostname to IP address. Code has been modified to handle the proper edge case for decision variable. Now the discovery-pending process calls the Default call-resolver function which is resolving the hostname to IP address, so the discovery-pending process is performed successfully.	9.5.1.0	9.6
IS-11611 SR 92767562	The incorrect interface status is displayed in Smarts.	While updating the dynamic instrumentation for this interface instance, the correct index has been parsed and the topologyUpdateInfo table has been updated.	9.4.1	9.6
IS-10378 SR 09367925	IP addresses are getting removed inappropriately from the HSRP system during the post	When two devices that are part of different user network is added to the topology while one having the HSRPEndpoint configuration. A check has been made to avoid removal of IP address from the other	9.2.1.0	9.6

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	processing of the discovery process.	device when the same IP address is part of the HSRPEndpoint of the former one.		
IS-11325 SR 10784189	When the user tries to set the ReconfigureAfterPush parameter in GUI, the IP Configuration Manager does not have any effect.	Code has been modified to ensure that the ReconfigureAfterPush parameter has an effect when the reconfiguration is triggered once the flag is set by the user.	9.5.0.0	9.6
IS-11390 SR 10941677	Interfaces for Juniper are not getting discovered.	The issue was with the snmpGetnext call that was not parsed for obtaining the next index. The logic has been modified to accommodate parsing of the index and obtain the subsequent value.	9.5.0.0	9.6
IS-11611 SR 92767562	The incorrect interface status is displayed in Smarts.	While updating the dynamic instrumentation for this interface instance, the correct index has been parsed and the topologyUpdateInfo table has been updated.	9.4.1	9.6
IS-11679 SR 92928642	The pending list discovery fails to rediscover in IP 9.4.2.26.	An inappropriate call-resolver function was called which could not resolve the hostname to IP address.  Code has been modified to handle the proper edge case for decision variable. Now the discovery-pending process calls the Default call-resolver function which is resolving the hostname to IP address, so the discovery-pending process is performed successfully.	9.5.1.0	9.6
IS-10378 SR 09367925	IP addresses are getting removed inappropriately from the HSRP system during the post processing of the discovery process.	When two devices that are part of different user network is added to the topology while one having the HSRPEndpoint configuration. A check has been made to avoid removal of IP address from the other device when the same IP address is part of the HSRPEndpoint of the former one.	9.2.1.0	9.6
IS-11611 SR 92767562	The incorrect interface status is displayed in Smarts.	While updating the dynamic instrumentation for this interface instance, the correct index has been parsed and the topologyUpdateInfo table has been updated.	9.4.1	9.6
IS-11679 SR 92928642	The pending list discovery fails to rediscover in IP 9.4.2.26.	An inappropriate call-resolver function was called which could not resolve the hostname to IP address.  Code has been modified to handle the proper edge case for decision variable. Now the discovery-pending process calls the	9.5.1.0	9.6

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		Default call-resolver function which is resolving the hostname to IP address, so the discovery-pending process is performed successfully.		
IS-12430 SR 304526	The new certification is required for Cisco Host UCS C220 M5 . 1.3.6.1.4.1.9.1.2492.	The Cisco Host UCS C220 M5 (System OID: .1.3.6.1.4.1.9.1.2492) device has been certified for Card, Disk, Fan, Interface, Memory, MemoryGroup, PowerSupply, TemperatureSensor, and VoltageSensor.	9.4	9.6
IS-11815 SR 11307568	The user gets many HSRP alerts.	Many HSRP alerts are generated as an IsUnknownEndPointExist event is being called, on the basis of the default UNKNOWN_HSRP state of HSRPEndpoints. The Default state has been modified to INITIAL_UNKNOWN, and the code for IsUnknownEndPointExist has also been modified to encapsulate all the possible test cases.	9.4.1.X	9.6
IS-12283 SR 10764921	The user is not able to poll InputPacketQueueDrop Pct attribute because it does not show proper value in GUI. Hence monitoring is impacted.	A locking mechanism has been added for attribute InputPacketQueueDropPct which ensures the access will be made through #MR_Refs#.	9.4.2.X	9.6
IS-10841 SR 10135488	The shadow IPs are not created for all the IPs, however the IP shadowing is enabled in tpmgr-param.conf (EnableShadowIP TRUE) file.	Code has been modified to introduce a new flag EnableShadowIPForVPNIP. When this flag is set, the shadow IP is created for all the IPs.	9.4.2	9.5.1
IS-10268 SR 09034476	During rediscovery, the Smarts IP 9.4.2.9 crashes.	The null reference object has been modified when “enableStats” is set, and when the SNMP V3 device discovery has been performed.	9.4.2.9	9.5.1
IS-9181 SR 87068124	Non-existing AggregateLink is created.	The AggregateLinks, which are created as part of logical connections and does not have any physical connections, are removed.	9.4.2	9.5.1
IS-9470 SR 08215158	The GDC-SCM-Cont-Driver logic for discovery cards needs to be changed to check during discovery for	The user receives false alarms on card status for the cards that are not installed. The fix has been provided by creating cards with valid indexes of scmNodeOperStatus.	9.4.2.9	9.5.1

**Table 19** Fixed issues in IP Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
	scmNodeOperStatus of cards.			
IS-9314 SR 8780872	The AggregateInterface/AggregatePort logic for disabling LayeredOver/Underlying relationship needs to be changed.	Code has been modified to allow to create LayeredOver relationship for AggregatePort or AggregateInterface along with composedOf relationship if data exists for both.	9.4.2.X	9.5.1
IS-9584 SR 88104354	The VoltageSensor threshold is false.	Code has been modified so that the voltageSetting class have the UseMIBThreshold attribute populated.	9.4.2	9.5.1
IS-6196 SR 11111	The ASNMP issue occurs.	The selective probing of indices is performed to fix the ASNMP issue based on sysObjectID flag.	9.4.1.X	9.5.1
IS-10437 SR 09599993	The incorrect interface relationship is built for Juniper MX960.	The logic for creating layering of interfaces/ports on AggregateInterface/AggregatePorts has been enhanced along with the MaxSpeed computation on the AggregateInterface/AggregatePorts.	9.4.2.9	9.5.1
IS-10663 SR 09830202	The priorities of polling threshold are not preserved from Configuration Manager to IP Manager.	Check on the child configuration has been made appropriately, so the priorities are retained when pushing the configuration to the respective IP domain managers.	9.4.2	9.5.1
IS-10647 SR 90838072	Cards are not discovered for Juniper MX240 . 1.3.6.1.4.1.2636.1.1.1.2.29.	Code has been modified to create the SFP cards on juniper MX240 series routers.	9.4.2.16	9.5.1
IS-10777 SR 10125566	The connections created by using LACP data are not stable, and new connections are created during each discovery.	The ic-post-lag.asl file has been modified, to avoid recreations of such connections and to avoid clearing events that may be still active.	9.4.2.X	9.5.1
IS-8297 SR 84969162	For trunk ports, the polling period is set to 20 minutes though it was specified as 4 minutes in the settings.	The adapter-setting.asl file that instruments ports uses a wrong value for the polling period. The adapter-setting.asl is modified to use the polling period from the settings to instrument the trunk ports.	9.4.1	9.5.1
IS-9961 SR 89250868	The CPU_Performance_RiverbedSteelhead instrumentation calculation for CPU	The CPU utilization code has been modified in case of Idletime range out of unsignedint32.	9.4.2.9	9.5.1

**Table 19** Fixed issues in IP Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
	utilization must be changed.			
IS-9739 SR 08715014	In Smarts 9.4.1, the CTL TSM domain crashes and runs out of file handles.	The SNMPAct instances leads for FD leaks. All instances of the SNMPAct have been stopped and deleted in the respective asl files to avoid the leak.	9.4.1	9.5.1
IS-10167 SR 9124479	The discovery error occurs.	A customized version of asl file has been provided.	9.4.2.12	9.5.1
IS-9184 SR 09034476	The IP Manager rediscovery takes more time.	The SNMP V3 discovery has been enhanced to avoid sending a huge list of IP sets as part of resolver that caused delay in rediscovery.	9.4.2.X	9.5.1
IS-9823 SR 88226638	There is a discrepancy for a particular file in two different IP domain, as the changes in local files in base installation are not same, and after the merge, it resulted different.	The sm_migrate.pl file has been modified to copy new installation file to new local directory while there is a merge conflict. And, the "merge but don't use" option has been chosen.	9.4.2	9.5.1
IS-9949	Fix the issue in the debug tool.	Code has been modified so that the Snap file is now picked up during the archiving process.	9.5.0.0	9.5.1
IS-10062 SR 09150894	The Smarts IP Card module displays down notification when the admin status of the Card is down.	As per the feature enhancement, an additional status for the Card (which is DISABLED) has been introduced, that applies when the Card is set administratively DOWN (status perceived via oid : cefcModuleAdminStatus -- 1.3.6.1.4.1.9.9.117.1.2.1.1.1), and this status is excluded while computing the DOWN alarm for the same card.	9.4.1	9.5.1
IS-9775 SR 08576890	In Smarts 9.4.2, there is no discovery of VRP IPs for system OID . 1.3.6.1.4.1.6527.3.1.2.3.6.	Code has been modified, so that all the VRP IPs and associated interfaces can be discovered now.	9.4.2	9.5.1
IS-10153 SR 09292294	In IP 9.5 SP1, an issue occurs in ic-cisco-ucs-cseries.asl for Cards discovery. The Card creation in ic-cisco-ucs-cseries.asl is invoked against objChassis instance	The Card creation has been invoked via the node object rather than the chassis object so that the card to node relationship is getting created.	9.5.1.0	9.5.1

Table 19 Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	instead of nodeObj instance which creates problem in cards naming, and as a result same card becomes part of several devices.			
IS-9773 SR 08719844	The user gets many HSRP alerts.	Many HSRP alerts are generated as an IsUnknownEndPointExist Event is being called, on the basis of the default UNKNOWN_HSRP state of HSRPEndpoints. The Default state is modified to INITIAL_UNKNOWN, and the code for IsUnknownEndPointExist is also modified to encapsulate all the possible test cases.	9.4.2	9.5.1
IS-6196 SR 11111	The ASNMP issue occurs.	The selective probing of indices is performed to fix the ASNMP issue based on sysObjectID flag.	9.4.1.X	9.5.1
IS-9323 SR 08139909	Descriptions are not being appended/added to object display names in 9.4.1.	Description was not appearing properly because the wrong driver was being called that has been corrected.	9.4.1.X	9.5.1
IS-8594 SR 07134823	Hypervisor with sysOid 1.3.6.1.4.1.6876.4.1 does not show any memory component.	As part of the fix, memory components are created from hrDeviceVolatileMemory (oid - 1.3.6.1.2.1.25.2.1.20) for the Hypervisor (1.3.6.1.4.1.6876.4.1).	9.4.1	9.5.1
IS-9546 SR 08025664	Need to have ways to disable Impact Propagation for devices on the same IP Subnetwork.	<p>As part of the feature enhancement, the following setting has been introduced in the Polling and Threshold window:</p> <p>Group: IPNetwork IPNetwork Impact Propagation Group</p> <p>Setting: IPNetwork_ImpactPropagation_Setting</p> <p>Note: To get the preceding group populated, execute the following command: &lt;BaseDir&gt;/IP/smarts/bin&gt;sm_adapter -s &lt;server&gt; -b &lt;broker&gt; -f</p> <p>BASEDIR/IP/smarts/local/conf/discovery/settings.conf icf/init-settings.asl</p> <p>The user can add the IPNetwork under this newly created group and choose to either enable/disable impact propagation through the attribute: "ImpactPropagation".</p>	9.4.2.X	9.5.1

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		Once this value is set (either enable/disable), a reconfigure is essential for the respective attribute: "isImpactPropOverIPNetworkEnabled" to reflect the same Boolean value (TRUE/FALSE). Then, the newly generated event or the existing event will have the refined list of impacts as per the settings applied.		
IS-9021 SR 84969162	Polling delayed for devices with TRUNK connection.	The polling_interval which was used as a global variable. It only holds the latest value that corresponds to the last network adapter processed in the loop. As part of the fix, the right polling interval was passed when setting the instrumentation object to the accessor.	9.4.1	9.5
IS-7521 SR 06385178	Physical device and its virtual router share IP. After rediscovery, IP is randomly seen as duplicate and removed from agent address list.	The discovery logic for virtual routers has been modified to exclude the IPs being classified as duplicate IP between the physical routers to the virtual ones.	9.4.1	9.5
IS-7447 SR 81998476	Unable to manage Spanning Tree and Bridge Probe layer-2 protocols.	The STP instrumentation logic has been refined to fetch the right STP key so the monitoring sub-system is able to poll the status of STPNodes through specific STPKey key.	9.4	9.5
IS-8865 SR 86096344	Memory counters are not interpreted correctly for notification generation, it uses 32bits Gauge instead of 64bits.	Device sysoid (.1.3.6.1.4.1.9.1.1658 - Cisco CRS-8SB) health driver has been changed to look up for 64 bit counters (cempMemPoolHCUsedOID { ".1.3.6.1.4.1.9.9.221.1.1.1.1.18" }) as 1st priority and then fall back to look up 32 bit counters (cempMemPoolUsedOID { ".1.3.6.1.4.1.9.9.221.1.1.1.1.7" }) for creating memory instances associated with this device.	9.4.1.20	9.5
IS-8837 SR 86455718	Validation of IP log message during a discovery.	HostResrcs-MIB2-Checkpoint-Processor-Driver has been revamped to not delete the CPU instances as part of multiple CPU creation driver and streamlined the health driver and HostResource driver to only create the respective components than getting mixed up between these two driver.	9.4.2	9.5
IS-7072 SR 80573488	Receiving duplicate tickets on the clarify queue from SMARTS.	Set HasSingleEndPoint flag on hosts by default to FALSE to avoid duplicate alerts.	9.4.1	9.5

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-7236 SR 81760610	Juniper MX series temperature Sensor discovery logic needs to be changed, due to issue in DISCOVERY_JUNIPER .import file.	Added code to create temperature sensor when the temperature value is not zero.	9.4.1	9.5
IS-8551 SR 7163952	Two out of five IPv6 addresses are not discovered.	Added check to avoid tagging on IPv6 addresses.	9.4.2	9.5
IS-8378 SR 85638724	ASL error occurs in IP, during discovery in ic-protocol-discovery.asl. When lite synchronization is enabled in BGP domain.	Code has been enhanced to handle the IP and Interface objects properly.	9.4.2	9.5
IS-5417 SR 76021426	Smarts IP Juniper port is removed after rediscovery.	The history table is handled to retain the ports that are created as part of different source (like : BRIDGE, LAG, LLDP, STACK).	9.2.2.0	9.5
IS-7977 IS-797 SR 82822850	IP and interface are not discovered for the IXIA device.	There are multiple rules that match against various formats that follow the ifIndex in the IP table. All these matching rules are a slightly variant of the other. The common flaw in all these rules are how the IP address is parsed. The IP address matched as a word. This does not strictly enforce the a.b.c.d format for the IP address. Even an "a.b.c" matches for an IP address. Because of the flaw, the entries are matched against different unintended rule. This results in certain IP/interfaces not being created. As a fix, the a.b.c.d format is strictly checked in the parsing rules.	9.4.2	9.5
IS-7691 SR 82566722	Recertification is needed for the discovery of all CISCO devices currently certified for IPv6.	Modified logic has been added in the file ic-cisco-ipv6.asl where we selectively ignore creating IPv6 objects created using CISCO-IETF-IP-MIB as claimed by CISCO. And, we only retain the IPv6 objects created through the generic Mibs.	9.4	9.5
IS-7521 SR 06385178	Physical device and its virtual router share IP. After rediscovery, IP is randomly seen as duplicate and removed from agent address list.	The discovery logic for virtual routers has been modified to exclude the IP's being classified as duplicate IP between the physical routers to the virtual ones.	9.4.1	9.5

**Table 19** Fixed issues in IP Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
IS-7447 SR 81998476	Unable to manage Spanning Tree and Bridge Probe layer-2 protocols.	The STP instrumentation logic has been refined to fetch the right STP key so the monitoring sub-system is able to poll the status of STPNodes through specific STPKey key	9.4	9.5
IS-8865 SR 86096344	Memory counters are not interpreted correctly for notification generation, it uses 32bits Gauge instead of 64bits.	Device sysoid (.1.3.6.1.4.1.9.1.1658 - Cisco CRS-8SB) health driver has been changed to look up for 64 bit counters (compMemPoolHCUsedOID { ".1.3.6.1.4.1.9.9.221.1.1.1.18" } ) as 1st priority and then fall back to look up 32 bit counters (compMemPoolUsedOID { ".1.3.6.1.4.1.9.9.221.1.1.1.7" } ) for creating memory instances associated with this device.	9.4.1	9.5
IS-8837 SR 86455718	Validation of IP log message during a discovery.	HostResrcs-MIB2-Checkpoint-Processor-Driver has been revamped to not delete the CPU instances as part of multiple CPU creation driver and streamlined the health driver and HostResource driver to only create the respective components than getting mixed up between these two driver.	9.4.2	9.5
IS-7072 SR 80573488	Receiving duplicate tickets on the clarify queue from SMARTS.	Set HasSingleEndPoint flag on hosts by default to FALSE to avoid duplicate alerts.	9.4.1	9.5
IS-7236 SR 81760610	Juniper MX series temperature Sensor discovery logic needs to be changed, due to issue in DISCOVERY_JUNIPER .import file.	Added code to create temperature sensor when the temperature value is not zero.	9.4.1	9.5
IS-8551 SR 7163952	Two out of five IPv6 addresses are not discovered.	Added check to avoid tagging on IPv6 addresses.	9.4.2	9.5
IS-8282 SR 06644431	The router DOWN alarm is not getting generated.	Code has been modified to generate router DOWN alarm by avoiding the conflicting and exclusive symptoms to be listed together for the same problem. And, take away peer system MightBeDown from the symptom list for the interface Down problem.	9.4.2	9.5
IS-8284 SR 06340724	When the Smarts IP card is down, the interface belonging to the sub card on this parent card is not	The certainty has been increased for the NetworkAdapter Down symptom that is realized by the card while computing the Card DOWN problem. This avoids the	9.4.1	9.5

Table 19 Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	suppressing the DOWN notification.	unnecessary interface DOWN problem when the realizedBy card is DOWN.		
IS-8239 SR 06661874	The Alcatel-Timex-7750SR12-driver definition in the DISCOVERY_ALCATEL.import is incorrect.	The containment driver definition for Containment-Alcatel-Timex-7750SR12-Driver was having a bug. As part of the fix, the drivers are rearranged and priority is altered.	9.4.2	9.5
IS-8046 SR 82160000	The FileSystem calculations are not correct for some devices which use NetSNMP agent sysOID . 1.3.6.1.4.1.8072.3.2.10.	For sysOid "1.3.6.1.4.1.8072.3.2.10", code has been written to select the type of instrumentation class based on the host type (which is a normal host, firewall). For this, the value of sysOid ". 1.3.6.1.4.1.2620.1.1.21" (fwProdName) has been pulled first and checked if its value is "firewall". If it's a firewall, the instrumentation class is overridden with "FileSystem_Performance_HostResources".	9.4.2	9.5
IS-8043 SR 84371510	The ic-cisco-loadbalancer-ace.asl script logic needs to be changed because during the devices rediscovery, Smarts concatenates the card serial number in the location attribute which is multiplying it.	Code has been modified to populate the card serial number which was getting appended indefinitely during multiple discoveries.	9.4.2	9.5
IS-7914 SR 05809041	The system VLAN tag groups are not supported for / Router/. 1.3.6.1.4.1.9.1.1935.	The VLAN tagging logic has been implemented to those devices that have been certified to create Vlans using "Cisco-CVI-Vlan" driver.	9.4.1	9.5
IS-7869 SR 79879638	Many false positive notifications are generated during rediscovery.	The ic-end-virtualip.asl has been fixed to use the UCS HostsAccessPoint relationship so that all the virtual IPs are removed from the agentAddressList.	9.4.1	9.5
IS-7842 SR 82959280	Smarts IP shows wrong FS details in the containment view of the device.	The containment view in SAM now does not match to the IP domain's FileSystem description attribute rather than the root attribute.	9.4.2	9.5
IS-7722 SR 05674826	Physical device and its virtual router share IP. After rediscovery, IP is randomly seen as	The discovery logic for virtual routers has been modified to exclude the IPs being classified as duplicate IP between the physical routers to the virtual ones.	9.4.2.X	9.5

**Table 19** Fixed issues in IP Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
	duplicate and removed from agent address list.			
IS-7714 SR 05499710	Existing notifications are cleared and notified again as an instrumentation is deleted during domain reconfigure.	When "Interface Management Policy" is applied to an interface group and when the Unmanaged setting is applied to that group, the EXPLICITLY_MANAGED interfaces are getting set to Unmanaged. As part of the fix, additional condition check has been made in file "if-provision-setting.asl" for the explicitly_managed interfaces.	9.4.2	9.5
IS-7671 SR 79280834	The aggregation ports are not created for CISCO UCS when CLI credential are supplied.	As the aggregation ports are for Nexus 6K, devices are created via CLI probing. And, the same nexus 6K device (which is . 1.3.6.1.4.1.9.12.3.1.3.1063) is excluded from the EtherChannel probe.	9.4.1	9.5
IS-7670 SR 81493316	The AggregateInterface class notification is missing.	When a WAN link is established at the LACP identified interfaces, the WAN link created between the same indexes is removed to avoid duplicate connection representation of the same WAN link.	9.4.1	9.5
IS-7283 SR 04695661	The IP tagging and shadowing affect the device discovery.	Altered the internal logic while performing findIP to avoid duplicate key insertion into the MR_AnyVal structure.	9.3.0.0	9.5
IS-7629 SR 0502205	Verizon reports false DOWN alerts on multiple devices that last only one polling cycle.	The solution is for XDIP domain. And, from the IP domain perspective, there is an additional attribute introduced for the partition class "lastPartitionCreatedAt" that reflects the timestamp of the partition created which is utilized by the XDIP domain.	9.4	9.5
IS-7577 SR 9090	The polling and the threshold matching criteria for proxy devices are incorrect.	The polling and the threshold matching criteria for proxy devices have been changed from Isproxy to domain.	9.4.0.X	9.5
IS-7401 SR 82292716	An Instrumentation for the EXPLICITLY_MANAGED vPorts for CISCO Nexus1KV is deleted by ic-post-port-manager.asl.	Added further logic to check for managedState for Nexus1K devices in ic-post-port-manager.asl.	9.4.2	9.5
IS-7994 SR 84438338	In Smarts SAM 9.4.2, the dynamic model error occurs.	The 'Type' attribute has been removed from the 'TransportConnector' model class which eliminates the dynamic model error message.	9.4.2.X	9.5

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-7978 SR 82822850	IP and interface are not discovered for the IXIA device.	There are multiple rules that match against various formats that follow the ifIndex in the IP table. All these matching rules are a slightly variant of the other. The common flaw in all these rules is how the IP address is parsed. The IP address matched as a word. This does not strictly enforce the a.b.c.d format for the IP address. Even an "a.b.c" matches for an IP address. Because of the flaw, the entries are matched against different unintended rule. This results in certain IP/interfaces not being created. As a fix, the a.b.c.d format is strictly checked in the parsing rules.	9.4.2.X	9.5
IS-7877 SR 05809041	The system VLAN tag groups are not supported for / Router/. (1.3.6.1.4.1.9.1.1935).	The Vlan tagging logic has been implemented to those devices that have been certified to create Vlans using "Cisco-CVI-Vlan" driver.	9.4.1	9.5
IS-7046 SR 79879638	Many false positive notifications are generated during rediscovery.	The ic-end-virtualip.asl has been fixed to use the UCS HostsAccessPoint relationship so that all the virtual IPs are removed from the agentAddressList.	9.4.1	9.5
IS-7827 SR 82959280	Smarts IP displays wrong FS details in the containment view of the device.	The containment view in SAM now does not match to the IP domain's FileSystem description attribute rather than the root attribute.	9.4.2	9.5
IS-7072 SR 80573488	The user receives duplicated tickets on the Clarify queue from SMARTS.	The model has been modified to not to generate HOST down event when partition is down.	9.4.1	9.5
IS-7475 SR 82566722	Recertification needed for the discovery of all CISCO devices currently certified for IPv6.	Added refined logic in file ic-cisco-ipv6.asl where we selectively ignore creating IPv6 objects created through CISCO-IETF-IP-MIB as claimed by cisco and only retain the IPv6 objects created through the generic Mibs.	9.4	9.5
IS-6763 SR 303194	Certification for the McAfee host.	The following devices/components are certified to discover and monitor using the McAfee MIB: <ul style="list-style-type: none"> <li>• Interface</li> <li>• Card</li> <li>• Fan</li> <li>• Powersupply</li> </ul>	9.4.0.X	9.5

**Table 19** Fixed issues in IP Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
IS-6611 SR 71328918	When adding elements using the seed file, the IP domain AM-PM stops and the sm_server process crashes.	Fixed the code logic where the "previousCachedValue" is being checked before raising an exception.	9.4.0.1	9.5
IS-7061 SR 79988522	Port channel between VSS and Nexus Cluster is not being managed.	The post port manager code logic has been enhanced to detect if the underlying ports are having connection and based on this check, the logical port channel will be managed.	9.4	9.5
IS-7100 SR 78528908	In the CISCO SYSTEMS Nexus-9332 . 1.3.6.1.4.1.9.12.3.1.3.162 5, the following devices are not discovered in the IP: <ul style="list-style-type: none"> <li>• Neighbor Discovery Cards</li> <li>• Ports, Memory</li> <li>• Processor</li> <li>• TempSensor</li> <li>• PowerSupply</li> </ul>	Certified the Cisco Nexus device for Neighbor Discovery Cards, Ports, Memory, Processor, TempSensor and PowerSupply device in IP.	9.2.1.0	9.5
IS-7103 SR 78528908	The ASL error displays, when CISCO SYSTEMS Nexus 9372 is discovered in the IP.	Certified the Cisco Nexus device for Neighbor Discovery Cards, Ports, Memory, Processor, TempSensor and PowerSupply device in IP.	9.2.1.0	9.5
IS-7145 SR 78528908	Certification for Cisco APIC Controller was not done, as there was no data for network adapters in the snapfile.	Certified Cisco APIC Controller Switch. Certified for Memory, Processor, PowerSupply, TempSensor. There was no data for Network Adapters in the snapfile provided to us from the customer.	9.2.1.0	9.5
IS-7263 SR 81864046	Due to known discovery bug in the Smarts release (9.4.1.0), the card CARD-osc-csct-ch-zhr-s-276/1.3.1.6.1, still polls the old index value and changes it to NOTPRESENT status.	The re-indexing has been taken care during re-discovery of the device which was causing wrong index being polled. Due to this re-indexing, the monitoring system is updated with the latest card Index thus the right status is fetched and updated.	9.4.1.X	9.5
IS-7274 SR 79280834	The aggregation ports are not created for	The nexus device ". 1.3.6.1.4.1.9.12.3.1.3.1063" has been added	9.4.1	9.5

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	Cisco UCS when CLI credential are supplied.	to the null driver to avoid calling the SNMP based driver and to create the aggregate ports as the same has been created via the CLI driver.		
IS-7288 SR 81493316	The aggregate interface notification is missing.	Modified the logic while creating aggregate interface link to remove the existing network connection as this will cause duplicate connection representation.	9.4.1	9.5
IS-7315 SR 81760610	Juniper MX series temperature Sensor discovery logic needs to be changed, due to issue in DISCOVERY_JUNIPER .import file.	Added code to create temperature sensor when the temperature value is not zero.	9.4.1	9.5
IS-7187 SR 80573488	Receiving duplicate tickets on the clarify queue from SMARTS.	Set HasSingleEndPoint flag on hosts by default to FALSE to avoid duplicate alerts.	9.4.1	9.5
IS-7386 SR 82135462	The bug occurs when OID is missing in DISCOVERY_CISCO.i mport file for Performance-Nexus-Entity-Driver and VoltageSensor Type is not matched.	Added the missing OID : cefcFanTrayOperStatusOID .1.3.6.1.4.1.9.9.117.1.4.1.1.1 to the DISCOVERY_CISCO.import file which is used to create TemperatureSensor and VoltageSensor.	9.4.1.X	9.5
IS-7390 SR 4695661	IP tagging and shadowing affects device discovery.	Fixed the code bug where the Managed taggedIP rediscovery is not happening. Now if all other IPs are unmanaged and only the managed IP (which is tagged) is managed, the re-discovery will go through.	9.3.0.0	9.5
IS-4985 SR 74821432	Modelling of the new AggregateInterface/ AggregateInterfaceLink introduced in IP 9.4 patch1 has some bugs.	Fixed all the open bugs in the AggregateInterfaceLink for creation and monitoring.	9.4.0.1	9.5
IS-5284 SR 74466680	Ports are not changing from Managed to Unmanaged during rediscovery - No more connections exists.	Added check for port objects "ConnectedVia" and "OpenStatus" status and set the managed status properly. Added additional checks for port objects with "ConnectedVia" state.	9.4.1.X	9.5
IS-5296 SR 74215336	Smarts IP Configuration Manager 9.4: Configuration Manager settings fail to fully synchronize.	The problem is surfacing because some configuration does not have ChildConfiguration. This is causing failure in sync between config manager and the IP domain manager. To handle this we need to	9.4.0.X	9.5

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		add check if the Configuration has ChildConfiguration then only proceeds further.		
IS-5801 SR 77201756	The CARD DOWN notification appears.	The CARD DOWN notifications are coming because of incorrect marking of card initial status to CRITICAL.  Modified the code of instrumented attribute apEnvMonPhyCardState to mark it as ""OTHER"" for card initial status, instead of ""CRITICAL"".	9.4.1.X	9.5
IS-6001 SR 77818566	All router interfaces are displayed as unknown in SMARTS.	Fixed the code logic where the Bay device interface is monitored through the following OIDs: wflplntfCfgEnable (.1.3.6.1.4.1.18.3.5.3.2.1.24.1.2) and wflplntfCfgState (.1.3.6.1.4.1.18.3.5.3.2.1.24.1.3) oids.	9.2.1.X	9.5
IS-6182 SR 77966416	Wrong computation of alerts on power supply of CRS routers.	Modified the computation of Powersupply event to be "Not Normal" when status is "offAdmin".	9.4.0.1	9.5
IS-6196 SR 11111	ASNMP issue in Adtran discovery fix.	Invoke ASNMP driver by default. If ASNMP errors out, then the default synchronous SNMP walk will be invoked. The choice of this fall back will also be controlled by a user defined flag per system object identifier. It gives a better control on the number of devices invoking this solution. File modifications will be ASL and conf files.	9.4.1.X	9.5
IS-6212 SR 7231322	Necessary OID information is missed while EIGRP discovery on Cisco ASA \ PIX firewalls.	"Firewall" class and new CLI command has been added in the EIGRP DM to get the new device (certification) discovered under this class.	9.4	9.5
IS-6218 SR 78329580	While calculating free memory on the Alcatel 7750 routers, the bug occurs.	The value of sgiMemoryAvailable indicates the amount of free memory in the overall system, which is not allocated to memory pools, and hence removed the subtraction of sgiMemoryUsed while calculating FreeMemory.	9.4.1.X	9.5
IS-6307 SR 79015710	Cisco Nexus and ASR devices are not discovering all components.	Handled the Agent bug where the IPaddressIfIndex Oid is being polled and parsed at the ASL level which takes care of discovering all the necessary Interfaces.	9.4.1.X	9.5
IS-6325 SR 77658576	Aggregate ports marked at explicitly_managed are	Added additional condition checks in post port manager code to take care of Explicitly managed AggregatePorts.	9.3.0.0	9.5

**Table 19** Fixed issues in IP Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
	being unmanaged during rediscovery.			
IS-6390 SR 78961012	Unable to add SEEDNAME to the PERL API for xmlCreate.	Re-arranged the xmlCreate method arguments to match the function declaration.	9.2.1.X	9.5
IS-6425 SR 78980720	The False Card Down notifications with NOTPRESENT status occurs when user upgrades the IOS.	Handled the history table mechanism that was causing re-indexing of card index causing wrong alarms.	9.3.0.X	9.5
IS-6550 SR 77748956	Received incorrect card down alerts, once upgraded to Cisco NX-OS switch to revision m9100-s3ek9-mz, version 6.2(13a).	Handled the history table mechanism that was causing re-indexing of card index causing wrong alarms.	9.2.2.0	9.5
IS-6639 SR 78608472	Discovery of VRs times out on Juniper ERX1440.	Added additional OID to be walked to create Vendor specific interfaces junilpAdEntIfIndexOID {"1.3.6.1.4.1.4874.2.2.12.1.2.2.1.2"}.	9.4	9.5
IS-6615 SR 67694068	Memory utilization growth occurs on IP domain for version 9.2.2.	Introduced further cleanUp mechanism in post clean up process to delete all the intermediate global tables that no longer being used/referred.	9.2.2.X	9.5
IS-6774 SR 79961274	SMARTS IP Manager is reporting TrunkCable Down alerts between the two Juniper switches that are at two different remote sites and are not connected to each other.	Introduced a way to detect VSS MAC ranges in the VSS switches and avoid them being used during the post stp trunk creation.	9.4.1	9.5
IS-6295 SR 78602150	The temperature sensors alert on Nexus devices.	Added the flag "UseMIBThreshold" to the TemperatureSensor group under the Polling and Threshold tabs.	9.4.1	9.5
<b>Fixed problems in IP 9.4.2</b>				
IS-6293 SR 78917372	Deadlocks on domain after setting polling threads up to 75	The default polling threads limit from 50 has been increased to 100. This should avoid the hang and the maximum number of configurable polling threads is 100.	9.4.1.X	9.4.2
IS-4479 SR 72710986	Intermittently getting SM-E-ENOPRIV-No	In RedHat 7.0, there is a UNIX user called admin. But this user is not configured with any password. So the getpwnam_r doesn't	9.4.0.X	9.4.2

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	privilege to execute this operation message when running the dmctl command	return a NULL but a spwd struct a empty password. This results in a ep value being NULL. And in this case, we do a strcmp of ep and the fetched_pw resulting in a sigsegv. Added ep == NULL condition to Authentication None that will avoid the crash.		
IS-4205 SR 71328918	When adding elements via a seed file, the IP domain AM-PM stops and the sm_server process crashes.	When childValue and lastChildValue are pointing to the same value and previousCacheValue is null, the previousCachedValue is populated before proceeding to avoid the crash.	9.4.0.X	9.4.2
IS-4995 SR 74536374	Multiple security vulnerabilities are found on Smarts server	As part of the fix, by default enabling cipher suite preference from console to help block weak cipher like RC4.	9.2.1.X	9.4.2
IS-4985 SR 74821432	Modelling of the new AggregateInterface/AggregateInterfaceLink introduced in IP 9.4 patch1 has some bugs.	Fixed the logic flaw while creating the AggregateInterfaceLink.	9.4.0.X	9.4.2
IS-5713 SR 77456850	MCAST probe is not running.	End-Device-CISCO-Selective-Driver is being called twice. That is causing MCAST driver to halt. As part of the fix, the redundant call to the driver has been removed.	9.4.1.X	9.4.2
IS-6004 SR 77966416	Wrong computation of alerts on Powersupply of CRS Routers	PSU was not marked as critical when the status was "offAdmin" while reading status from cefcFRUPowerOperStatus. As part of the fix, the offAdmin status will be marked CRITICAL for powerSupply instances that are instrumented through the PowerSupply_Fault_CiscoEntityFRU class.	9.4.0.X	9.4.2
IS-6188 SR 78329580	Bug in memory usage is in calculation on Alcatel 7750 Routers	The logic for computing free memory for the memory components on Alcatel devices using the instrumentation class "Memory_Performance_AlcatelTimex" has been fixed.	9.4.1.X	9.4.2
IS-6036 SR 77658576	Aggregateports marked as explicitly managed are being unmanaged during rediscovery.	The ic-post-port-manager.asl had a logic flaw that ignored managing the AggregatePorts whose underlying physical ports are connected. The logic has been refined to manage the AggregatePorts if any one port that it composes has a connection.	9.3.0.X	9.4.2
IS-6303 SR 78961012	How to add SEEDNAME to the	AD_TopologyManager::xmlCreate" does call create method swapping the NameFormat and seedName variable. As part of the fix,	9.2.1.X	9.4.2

Table 19 Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	PERL API for xmlCreate.	these two variables are matched according to the function signature .		
IS-6402 SR 78980720	Discovery Bug: false Card Down Notifications with NOTPRESENT status after upgrading IOS	Addressed the TopologyUpdateInfo table mechanism to accommodate the index change of the cards and remove the old/ stale entries thus causing wrong DOWN alarm post IOS upgrade.	9.3.0.X	9.4.2
IS-5462 SR 75947518	Cisco Nexus 7000 switches are not fully discovering.	This is to address a known device bug acknowledged by Cisco: <a href="https://tools.cisco.com/bugsearch/bug/CSCuw75860/?reffering_site=dumpcr">https://tools.cisco.com/bugsearch/bug/CSCuw75860/?reffering_site=dumpcr</a> Smarts alters the way the addressable are queried thus working around the reported problem.	9.4.0.X	9.4.2
IS-6514 SR 77748956	After upgraded Cisco NX-OS switch to revision m9100-s3ek9-mz, version 6.2(13a) receiving incorrect Card down alerts.	Altered the logic to handle the topology update info table correctly and remove the stale entries thus causing the wrong card alarms.	9.2.2.X	9.4.2
IS-6305 SR 79015710	Cisco Nexus and ASR devices are not discovering all components.	FAN instances were not discovered as the walk FE was not supplied with the OID: cefcFanTrayOperStatusOID . Altered the logic to create fans by passing the above OID to the walk FE.	9.4.1.X	9.4.2
IS-5984 SR 77818566	All Router interfaces show up as unknown in SMARTS.	OID wflplntfCfgEnable and wflplntfCfgState appends the index as an IP address and projects the status which will not properly mapped to the actual interface that was created through MIB-2 index. Due to the improper mapping, the monitoring system is not able to associate the status with the right index and hence while querying the data with the index that was actually discovered, the device agent will respond with "NoSuchObject".  As part of the fix, the ASL is parsed accordingly to map the status correctly.	9.2.1.X	9.4.2
IS-5563 SR 76961082	F5 Load Balancer: Memory monitoring	The memory was represented in Bytes. As part of the fix, it will be represented in Kilobytes (KB) thus giving accurate representation on memory utilization.	9.4.1.X	9.4.2
IS-6598 SR 75570286	Prefix and PrefixLength not	The driver that is supposed to update the Prefix and prefix length was not called.	9.4.1.X	9.4.2

**Table 19** Fixed issues in IP Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
	updated for IPv6 addresses on Juniper devices.	Now, the driver is called to update the prefix and prefixlength for every device discovery.		
IS-5414 SR 76239896	Extraordinary values for file system usage	The file system utilization has been refined for "FileSystem_Performance_HostResources_RedHat" thus reflecting the right utilization as reported by the host.	9.4.0.X	9.4.2
IS-5156 SR 75170200	Interfaces got created and deleted as they are AggregatePorts.	The history table mechanism has been fixed to not delete the interface/ AggregateInterface while performing the discovery.	9.4.1.X	9.4.2
IS-5291 SR 75638866	IP AMPM 9.4.1 crash	The crash is due to the dasl having multiple threads having the same context. As part of the fix, the dasl sessions are made single threaded thus avoiding the crash.	9.4.1.X	9.4.2
IS-6187 SR 78608472	Discovery of VRs times out on Juniper ERX1440.	Added logic to create VR specific interface through "junilpAdEntIfIndex".	9.4.0.X	9.4.2
IS-2625 SR 67694068	Memory utilization growth on IP domain for version 9.2.2	The thread specific MIB-2 tables that are retained in the topology contributing to the memory growth has been removed during post clean-up process.	9.2.2.X	9.4.2
IS-6748 SR 79961274	Smarts IP Manager reporting TrunkCable Down alerts between two Juniper switches that are at two different remote sites and are not connected to each other.	Those VSS MACs are excluded during the STP post processing that is creating the wrong trunk cable connection. The attribute VSSMACRange is where the virtual VSS MAC ranges are specified that will be excluded.	9.4.1.X	9.4.2
IS-6402 SR 78980720	Discovery Bug: false Card Down Notifications with NOTPRESENT status after upgrading IOS	This is due to the logic flaw while handling the indexes being changed after IOS upgrade. The TopologyUpdateInfo table is fixed to hold only unique values thus avoiding the wrong CARD down events.	9.3.0.X	9.4.2
IS-5031 SR 74466680	Port is not changing from Managed to Unmanaged during rediscovery – No more connection.	The post manager code was reworked to handle all of the cases to manage port/ AggregatePorts.	9.3.0.X	9.4.2
IS-6717 SR 80121714	False alert on an external power supply fan on a Cisco switch	The certification is altered to poll the status of PowerSupply through the oid : chassisPs1Status that expose the right status.	9.2.1.X	9.4.2

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-6211 SR 72313228	EIGRP discovery on Cisco ASA/PIX firewalls	Enhanced the Smarts lite discovery to identify Cisco ASA/PIX firewalls to be part of the NPM topology collection.	9.4.1.X	9.4.2
IS-4155 SR 62996904	Unable to discover SNMPv3 devices added to the pending list using dmctl.	<p>Added additional error handling for the condition described in IS-2463. AuthPass, PrivPass and EngineID are now optional parameters while adding SNMP V3 device to the pending list using dmctl. These parameters were earlier mandatory and hence were not allowing discovery when the parameters were empty.</p> <p>Modified files:</p> <ul style="list-style-type: none"> <li>• Windows: local/lib/sm_auto_discovery.dll</li> <li>• Linux: local/lib/libsm_auto_discovery.so</li> </ul>	9.3.0.X	9.4.1
IS-4160 SR 65823972	IPSEC Alerts showing wrong status	<p>The issue is because the short containment driver definition is missing for many containment drivers that discover IPSEC tunnel interfaces.</p> <p>Added the appropriate short containment driver for those needed devices.</p> <p>Modified files:</p> <ul style="list-style-type: none"> <li>• conf/discovery/ DISCOVERY_CISCO.import</li> <li>• conf/discovery/oid2Type_Cisco.conf</li> </ul>	9.2	9.4.1
IS-4161 SR 67289066	<p>Even though the IP Manager was started in Availability Mode (AMONLY), it generated discovery errors related to performance discovery. Example error:</p> <p>SWFE-E-EGETNEXT- While getting next of OID . 1.3.6.1.4.1.9.9.109.1.1.1.1.2, SNMP-ERESPONSE-No response from 167.84.168.18, port 161 SNMP-ETIMEOUT-Timed out; in file "/work/tancurrent/</p>	<p>A new condition check has been introduced into the discovery code to ensure that performance related OIDs are not probed if the IP Manager is started in AMONLY mode.</p> <p>Modified files:</p> <ul style="list-style-type: none"> <li>• conf/discovery/ DISCOVERY_CISCO.import</li> <li>• rules/discovery/ic-cisco-end-device-CPUProc.asl</li> </ul>	9.3.0.X	9.4.1

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	DMT-9.3.0.0/116/smarts/snmp/lib/SNMP_RequestsSender.c" at line 1337			
IS-4162 SR 66126622	Enhancement to support creation of LAG 3 port channel: AggregateInterface. NetworkConnection is not built between AggregatePorts.	<p>A new class AggregateInterface has been introduced that is derived from Interface. It retains the underlying IP relationship which is used for creating a NetworkConnection.</p> <p>Modified files:</p> <ul style="list-style-type: none"> <li>• rules/devstat/settings/thr-setting.asl</li> <li>• rules/discovery/ic-clear-interface-layering.asl</li> <li>• rules/Discovery/adapter/ic-etherChannel-perfInst.asl</li> <li>• rules/discovery/adapter/ic-lag-dot3ad.asl</li> <li>• rules/discovery/ic-post-stp-trunk.asl</li> <li>• rules/Discovery/cisco/ic-lag-cisco-pagp.asl</li> <li>• conf/discovery/discovery/cisco/DISCOVERY_CISCO.import</li> <li>• conf/health/settings.conf</li> <li>• Windows: lib/ sm_health.dll lib/sm_icim.dll</li> <li>• Linux: lib/libsm_icim.so lib/ libsm_health.so</li> </ul>	9.2.2.X	9.4.1
SND-1455 SND-1870	9.4 IP Manager crashes using 9.1 IP Manager repository with Virtual Switch Systems	This issue has been addressed.	9.4	9.4.1
IS-2588 SR 68548850	Smarts IP Configuration Manager will not push the ProcessorUtilizationAlertMode setting to IP Manager.	The necessary attributes including ProcessorUtilizationAlertMode, SmoothingForMemoryGroupUtilization, MemoryGroupUtilizationThreshold, ProcessorGroupUtilizationThreshold, SmoothingForProcessorUtilization, SmoothingForProcessorGroupUtilization and SmoothingForInsufficientMemory are being pushed to the underlying IP Managers from the IP Configuration Manager under Processor_Performance_Setting class.	9.3.0.X	9.4.1

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		Modified file: conf/icf-c/push.conf		
IS-4163 SR 68694738	<p>The exception 'MR2-MR_TRANS_BAD_PROP-Prop' appears in logs while deleting a pending entry. Following error message appears in the server log during discovery:</p> <p>MR2-MR_TRANS_BAD_PROP-Prop: PendingList; in file "n:/DMT-9.3.0.0/116/smarts/repos/mr/transactions.c" at line 3560</p> <p>MR2-MR_TRANS_BAD_OBJECT-Object: AD-Pending; in file "n:/DMT-9.3.0.0/116/smarts/repos/mr/transactions.c" at line 3557</p> <p>MR-KEY_VALUE_NOT_FOUND-Specified key value not found in table; in file "AD_Pending.c" at line 1393</p>	<p>A race condition may occur where one discovery thread is deleting a pending entry while another thread is trying to access it. The fix here is to check if the entry persists before accessing/deleting it.</p> <p>Modified files:</p> <ul style="list-style-type: none"> <li>• Windows: lib/sm_auto_discovery.dll</li> <li>• Linux: lib/libsm_auto_discovery.so</li> </ul>	9.3.0.X	9.4.1
IS-4164 SR 68892656	StateNotNormal alarm is not generated for a Juniper device when a power supply is out of chassis.	<p>The PowerSupply_Fault_JuniperEnvMon instrumentation class has been changed to map NOSUCHINSTANCE to CRITICAL status resulting in the StateNotNormal alarm. The fix applies to all Juniper devices using PowerSupply_Fault_JuniperEnvMon instrumentation.</p> <p>Modified files:</p> <ul style="list-style-type: none"> <li>• Windows: lib/ sm_health_juniper.dll</li> <li>• Linux: lib/libsm_health_juniper.so</li> </ul>	9.2.2.X	9.4.1

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-4165 SR 68914338	Managing Cisco Nexus with VRF and SNMPv3	Enhanced to walk the MIB: 1.3.6.1.4.1.9.9.468 (CISCO-CONTEXT-MAPPING-MIB) to fetch the context data present in the Cisco device. Modified files: <ul style="list-style-type: none"> <li>conf/discovery/ DISCOVERY_CISCO.import</li> <li>rules/discovery/ic-cisco-find-context.asl</li> </ul>	9.2.1.X	9.4.1
IS-4246 SR 68568216	Smarts IP Manager is not providing data for some interfaces during discovery. Smarts IP Manager is not monitoring some interfaces for performance during discovery.	DuplexMode and Duplex Source interface attributes were cleared during discovery if they had been discovered using NEIGHBOR_MIB. The values are set back during post processing. In long discovery cases, the values may not be set for hours. The IP Manager will not monitor interfaces for performance until the Duplex value is set. The code has been changed to avoid resetting the Interface DuplexMode/ DuplexSource in pre-processing and incorporated in the discovery code. Modified files: <ul style="list-style-type: none"> <li>rules/discovery/ic-cisco-cdp.asl</li> <li>rules/discovery/ic-cisco-post-processor.asl</li> <li>rules/discovery/ic-pre-processor.asl</li> </ul>	9.3.0.X	9.4.1
IS-3967 SR 68120502	Certification request: Sonus 5200 . 1.3.6.1.4.1.2879.1.9.2	This device is certified in IP Manager. Modified files: <ul style="list-style-type: none"> <li>local/conf/discovery/ oid2type_Sonus.conf</li> <li>local/conf/discovery/ DISCOVERY_SONUS.import</li> <li>local/rules/discovery/ic-sonus-sbc5200-create-card.asl</li> <li>local/rules/discovery/ic-sonus-sbc5200-create-interface.asl</li> <li>local/rules/discovery/ic-sonus-sbc5200-create-port.asl</li> <li>local/lib/libsm_devstat_sonus.so</li> </ul>		9.4.1
IS-3968	Certification request: Sonus 5110 1.3.6.1.4.1.2879.1.9.3	This device is certified in IP Manager. Modified files:		9.4.1

Table 19 Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		<ul style="list-style-type: none"> <li>local/conf/discovery/oid2type_Sonus.conf</li> <li>local/conf/discovery/DISCOVERY_SONUS.import</li> <li>local/rules/discovery/ic-sonus-sbc5200-create-interface.asl</li> <li>local/rules/discovery/ic-sonus-sbc5200-create-port.asl</li> <li>local/lib/libsm_devstat_sonus.so</li> </ul>		
IS-4247	Smarts is reporting negative values for CPU utilization for Solaris systems causing W4N reports to look bad.		9.4	9.4.1
IS-4248 SR 69368428	Voltage sensors on Cisco Nexus 3K devices are discovered as temperature sensors.	<p>Created health components based on the unit value in the entSensorType MIB (that is, if the value type is Celsius, then create temperatureSensor and if the value type is volt, then create VoltageSensor).</p> <p>Modified files:</p> <ul style="list-style-type: none"> <li>conf/discovery/DISCOVERY_CISCO.import</li> <li>rules/discovery/ic-nexus-health.asl</li> </ul>	9.2.2.X	9.4.1
IS-4249 SR 69545606	IP Manager is raising notifications for unused power supplies.	<p>The discovery code has been changed to ignore power supplies that are marked as disabled in the hh3cEntityExtOperStatus MIB.</p> <p>Modified file:</p> <p>rules/discovery/ic-huawei-H3C-health.asl</p>	9.4	9.4.1
IS-4252	WiFi elements were not discovered if IP Manager was started in the AM Only mode.	<p>To include IP Availability Manager in the discovery-init.asl while initializing the WiFi probe.</p> <p>The fix is to start the WiFi probe when the IP Manager is started in AM Only mode. This driver creates and monitors WiFi components such WirelessController, WirelessAccessPoints, AuthenticationServer and WirelessClients.</p> <p>Modified file:</p> <p>rules/discovery/discovery-init.asl</p>	9.3	9.4.1

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-4253 SR 69214978	The TemperatureSensor is showing UNKNOWN for status for Ciena switches.	Modified the MODEL code to map the polled attribute to the Status attribute for TemperatureSensor. Modified files: <ul style="list-style-type: none"> <li>Windows: lib/sm_health_ciena.dll</li> <li>Linux: lib/libsm_health_ciena.so</li> </ul>	9.3.0.X	9.4.1
IS-4254 SR 69578978	Warning messages appear in discovery logs. Example: [February 27, 2015 7:40:37 AM CST +920ms] t@102284 Discovery #3  ASL_MSG-* -ASLP-discovery/ic-teamedif-hostvendorinfo.asl: *** WARNING *** *** DEFAULT *** line: . 1.3.6.1.4.1.232.11.2.2.12.0  4956522D53384D502D434647505032	Warning messages have been added to be logged in the debug mode. Modified file:  local/rules/discovery/ic-teamedif-hostvendorinfo.asl	9.2.2.X	9.4.1
IS-4255	Enhancement on PTX device (. 1.3.6.1.4.1.2636.1.1.1.2.69) to discover CSE2000 cards and its composedOf Interfaces/Ports.	This device is certified in IP Manager for discovering and monitoring of CSE2000 card modules and its composedOf NetworkAdapters. Modified files: <ul style="list-style-type: none"> <li>local/conf/discovery/ DISCOVERY_JUNIPER.import</li> <li>local/rules/discovery/ic-juniper-chassis-ptx.asl</li> <li>local/rules/discovery/ic-juniper-Post-Processor.asl</li> <li>local/conf/discovery/tpmgr-param.conf</li> </ul>	9.2.2.5	9.4.1
IS-3947	Certification request: CheckPoint 2450 . 1.3.6.1.4.1.2620.1.6.123.1.24	This device is certified in IP Manager. Modified file:  local/conf/discovery/oid2type_Checkpoint.conf		9.4.1
IS-3949	Certification request: CheckPoint 12400 .	This device is certified in IP Manager. Modified file:		9.4.1

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	1.3.6.1.4.1.2620.1.6.123.1.41	local/conf/discovery/oid2type_Checkpoint.conf		
IS-3950	Certification request: CheckPoint 12600 . 1.3.6.1.4.1.2620.1.6.123.1.42	This device is certified in IP Manager. Modified file: local/conf/discovery/oid2type_Checkpoint.conf		9.4.1
IS-3952	Certification request: CheckPoint 21400 . 1.3.6.1.4.1.2620.1.6.123.1.45	This device is certified in IP Manager. Modified file: local/conf/discovery/oid2type_Checkpoint.conf		9.4.1
IS-3872	Certification request: CheckPoint 21700 . 1.3.6.1.4.1.2620.1.6.123.1.47	This device is certified in IP Manager. Modified files: <ul style="list-style-type: none"> <li>• local/conf/discovery/oid2type_Checkpoint.conf</li> <li>• local/conf/discovery/DISCOVERY_GENERIC.import</li> <li>• local/conf/discovery/DISCOVERY_CHECKPOINT.import</li> <li>• local/rules/discovery/ic-checkpoint-environment.asl</li> <li>• local/rules/discovery/ic-hostresources-checkpoint-other.asl</li> <li>• local/lib/libsm_health_checkpoint.so</li> </ul>		9.4.1
IS-3954	Certification request: CheckPoint 13500 . 1.3.6.1.4.1.2620.1.6.123.1.44	This device is certified in IP Manager. Modified files: local/conf/discovery/oid2type_Checkpoint.conf		9.4.1
IS-3955	Certification request: CheckPoint-Secure-Platform 1.3.6.1.4.1.2620.1.6.123.1.13	This device is certified in IP Manager. Modified file: local/conf/discovery/oid2type_Checkpoint.conf		9.4.1
IS-3956	Certification request: CheckPoint-Secure-Platform . 1.3.6.1.4.1.2620.1.6.123.1.36	This device is certified in IP Manager. Modified file: local/conf/discovery/oid2type_Checkpoint.conf		9.4.1
IS-3957	Certification request: Checkpoint 4800 . 1.3.6.1.4.1.2620.1.6.123.1.38	This device is certified in IP Manager. Modified file: local/conf/discovery/oid2type_Checkpoint.conf		9.4.1

**Table 19** Fixed issues in IP Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
IS-3959	Certification request: CheckPoint 1280 . 1.3.6.1.4.1.2620.1.6.123. 1.23	This device is certified in IP Manager. Modified file: local/conf/discovery/ oid2type_Checkpoint.conf		9.4.1
IS-3960	Certification request: CheckPoint 390 . 1.3.6.1.4.1.2620.1.6.123. 1.20	This device is certified in IP Manager. Modified file: local/conf/discovery/ oid2type_Checkpoint.conf		9.4.1
IS-3961	Certification request:- CheckPoint 3150 . 1.3.6.1.4.1.2620.1.6.123. 1.54	This device is certified in IP Manager. Modified file: local/conf/discovery/ oid2type_Checkpoint.conf		9.4.1
IS-3962	Certification request: CheckPoint 150 . 1.3.6.1.4.1.2620.1.6.123. 1.16	This device is certified in IP Manager. Modified file: local/conf/discovery/ oid2type_Checkpoint.conf		9.4.1
IS-3350	Certification request: Linux Net-SNMP- Agent 1.3.6.1.4.1.8072.3.2.10	This device is certified in IP Manager. Modified file: local/conf/discovery/oid2type_Misc.conf		9.4.1
IS-3828	IP server is unable to form connections and relationship between various components of HP c7000 Blade System.		9.4	9.4.1
IS-4268	Smarts IP Configuration Manager will not push the ProcessorUtilizationAle rtMode setting to IP Manager.			9.4.1
IS-4309 SR 70637832	Smarts IP 9.4.0.1 device discovery error and every discovery ends with an error.		9.4.0.1	9.4.1
IS-4308	4G Tunnel interface monitoring support enhancement. To support 4G support monitoring by mapping DORMANT state to	Support included for monitoring 4G tunnel interfaces. Added a flag: MapCellularInterfaceDORMANTtoDOWN to enable this functionality. Modified files:	9.2.2.X	9.4.1

**Table 19** Fixed issues in IP Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	DOWN on the cellular interface.	<ul style="list-style-type: none"> <li>local/conf/discovery/import/tpmgr-param.conf</li> <li>local/rules/discovery/ic-cisco-cellular-interface-inst.asl</li> <li>local/conf/discovery / DISCOVERY_CISCO.import</li> <li>local/lib/libsm_devStat.so</li> </ul>		
IS-4310	Certification request: Enhance audioCodes certification to read enterprise MIB to create IPs.		9.2.1.X	9.4.1
IS-4123	Enhancement in certification			9.4.1
IS-4124	Certification request: Cisco UCS LS2 . 1.3.6.1.4.1.9.1.1683			9.4.1
IS-4126	attribute QueueDropThreshold missing from push.conf			9.4.1
IS-4127	Certification request: Cisco UCS LS2 . 1.3.6.1.4.1.9.1.1682	<p>Provided support for new device UCS LS2 . 1.3.6.1.4.1.9.1.1682</p> <p>Modified file: conf/discovery/ oid2type_Cisco.conf</p>		9.4.1
IS-2433 SR 68025616	Port Channels that have IP address on second VRF are not being managed and connections using these port channels are not being created.	<p>Used the deviceID to form the CDP connection if we fail to identify the neighbor device through VRF IPs.</p> <p>Modified file: rules/discovery/ic-cisco-post-processor.asl</p>	9.2.1.X	9.4

**Table 20** Fixed issues in IP Manager 9.3.x

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
652037 651303 SR26015342	Juniper EX4300 device with syOID . 1.3.6.1.4.1.2636.1.1.1.2.63 was required to be certified for virtual channel connection (VCC).	<p>The device was re-certified to support VCC discovery using CLI.</p> <p>But, if you do not provide CLI credentials in IP Manager, then the</p>	9.2.1	9.3

**Table 20** Fixed issues in IP Manager 9.3.x (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		corresponding Unitary Computer System will go to the pending list and VCC components via CLI will not be discovered. However, all the SNMP related components will be discovered.		
577300	CM domain should have a record in the log file when it imports a new set of settings.			9.3
609549	Need to be able to export and import Target Domains in the configuration manager.			9.3
642878 601224 SR 53917098	ASL errors similar to the following were seen during server restart: ASL-W-ERROR_RULE_SOURCE-While executing rule set '/opt/InCharge9/IP/smarts/rules/icf/init-settings.asl' ASL-ERROR_ACTION-While executing action at: ASL-CALL_STACK_RULE-RuleName: MATCH, Line: 175 ASL-ERROR_UNDEFINED_VARIABLE_ACCESS-Variable 'newLen' has not been assigned a value	init-settings.asl was modified to the right variable name.	9.2.0.1	9.3
652413 650041 SR 58610736	On subscribing to the MightBeDown event for Cisco UCS devices in SAM, the MightBeDown event had IsRoot set to TRUE.	Added the MightBeDown event to the impact list of Down problem. Now the MightBeDown has the IsRoot set to FALSE in SAM.	8.1.4	9.3
653104	Merge : CLI Credentials not found error			9.3

**Table 20** Fixed issues in IP Manager 9.3.x (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	message to be suppressed.			
654039	To fix in 9.3 : IP discovering broadcast addresses and classifying them as duplicateIP			9.3
654355	Wifi probe should be excluded in TSM discovery and WirelessClient/ WirelessAccessPoint classes should be excluded during TopoSync.			9.3

## Known problems in IP Manager

These problems affect IP Manager.

### License feature checkout messages appear in IP domain manager

In IP domain manager, the license feature checkout messages are observed in the logs.

SND-7361

#### Resolution

This has no impact on the functionality and there is no license checkout happening. It is only a message in a log file.

### ASL error messages displayed in IP Server log file, while discovering SNMPv3 devices

After successful discovery of SNMPv3 devices, the following ASL error messages are observed in the IP log file:

```
[April 23, 2018 3:57:44 PM GMT+05:30 +651ms] t@1077929728 File-
Importer-Driver
ASL_MSG-*-ASLP-discovery/ic-file-importer.asl: April 23, 2018 3:57:45
PM GMT+05:30 ImportFromSeedfile: /opt/SNMPV3_Seed.txt
[April 23, 2018 3:57:44 PM GMT+05:30 +652ms] t@1077929728 File-
Importer-Driver
AD_MSG-*-TMG2_STATUS_DISCOVERY_START-Last discovery started at April
23, 2018 3:57:45 PM GMT+05:30
[April 23, 2018 3:57:44 PM GMT+05:30 +664ms] t@1077929728 File-
Importer-Driver
ASL-W-ERROR_RULE_SOURCE-While executing rule set '/opt/Jira-
Vallidation/IP/smarts/rules/discovery/ic-file-importer.asl'
ASL-ERROR_ACTION-While executing action at:
```

```

ASL-CALL_STACK_RULE- RuleName: ENTRY, Line: 239
ASL-CALL_STACK_RULE- RuleName: START, Line: 92
ASL-ERROR_INVOKE-While attempting to invoke operation 'create' of
object 'MR_Object::ICF-TopologyManager'
SNMP-EINVALID-Invalid argument
[April 23, 2018 3:57:44 PM GMT+05:30 +791ms] t@1190131456 Discovery #1
SNMP-E-AGENTERRORSTATS-Below message for SNMP agent at
'10.31.119.3:161', was suppressed 0 times since The Epoch
SNMP-EAGENTUSMUSER-Agent REPORT [USM]: Unknown User Name
'automd5desuser'

```

SND-6485

**Resolution**

There is currently no resolution.

## SNMP Walk for the devices is not stored in archive directory and stored in the root directory

SNMP Walk for the devices is not stored in archive directory and stored in the root directory.

SND-5804

**Resolution**

Copy the <Device ipaddress>.snap, <Device ipaddress>.walk, and <Device ipaddress>.mimic from the root directory to archive directory. Ship this additional tar file <New tar file name>.tar to DellEMC Support.

**Example**

```

tar -cvf <New tar file name>.tar /<Device ipaddress>* <IP_BASE_DIR>/
smarts/local/logs/archive

```

## Debug tool does not support devices with SNMP V3

The Debug tool cannot be used for the devices which are discovered via SNMP V3.

SND-5793

**Resolution**

No resolution available.

## BEM and Blade Type attribute are displayed as Host instead of BLADEENCLOSUREMANAGER and BLADE respectively in SAM and OI

When you discover HP Blade System OA 10.31.91.101 in IP, in SAM topology browser console the BEM and Blade Type attribute are displayed as Host instead of BLADEENCLOSUREMANAGER and BLADE respectively in SAM and OI.

**Resolution**

This has no impact on the functionality.

## Error message seen if the SELinuxSetting security setting is enabled in a system with RHEL 5.x

When you start IP Manager in a system with RHEL 5.x, you might see the following error:

```
[09-Sep-2010 12:05:11 AM+383ms EDT] t@-143386224 <Primary Thread> CI-E-EPRGNOTLOAD-Program "dmboot" could not be loaded CI-ESYSINFO-System information: /opt/InCharge/IP/smarts/local/lib/libsm_license.so: cannot restore segment prot after reloc: Permission denied RTLD-SI_ELOADERR-Dynamic loader error
```

### Resolution

The error message appears if the SELinuxSetting security setting is enabled. To correct the problem, run the following command from the command prompt:

```
chcon -t textrel_shlib_t /opt/InCharge/IP/smarts/local/lib/libsm_license.so
```

## AM-PM services are overwritten on upgrade when Configuration Manger is installed

ic-am-pm-server is overwritten when you install Configuration Manager in EDAA mode.

If you select option 2, (standalone), then the service stays as is. For example:

Choose the required option:

1 - Yes, Install Configuration Manager in EDAA enabled mode.

2 - No, Install Configuration Manager standalone.

SND-1834

### Resolution

This issue only happens when installing Configuration Manager during an upgrade. Start the services manually. There is no workaround at this time.

## No logout option for the Configuration Manager in the EMC M&R UI

If you use the Configuration Manager in the EMC M&R UI to configure IP Manager settings, there is no logout selection option.

SND-1255

### Resolution

Use the browser X option to exit the EMC M&R UI session.

## 9.4 Configuration Manager is not fully compatible with 9.1 IP Managers

If you are using the Configuration Manager in the EMC M&R UI to control discovery configuration settings, the Topology and Discovery Filters tabs for 9.1 IP Managers return these errors:

- The Topology tab does not return any data and an error message “No Priority Response” is displayed.
- The Discovery tab does return the details but the Extended Filter View does not load. The Discovery tab filter does not get saved.

SND-1773

**Resolution**

Upgrade 9.1 IP Managers to version 9.4 and start their services with the `--edaa=ip/2.0` option as described in the *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers*.

The EMC M&R UI does not support functionality in the Topology and Discovery Filters tab for 9.1 IP Managers. SNMPv3 credentials are not supported in the 9.1 IP Managers, so the EMC M&R UI does not load them and generates the errors.

Other functionality is supported for 9.1 IP Managers. You can use the Configuration Manager to control other configuration settings like polling, threshold, and device access settings for 9.1 IP Managers.

**IP Manager DASL library is not loaded in Windows**

If the machine where IP Manager is installed also has Network Configuration Manager installed, following errors may be encountered in the IP server logs due to conflicting libraries of the same name present in the C:\Windows\System32 directory:

```
[March 7, 2014 4:46:47 AM EST +899ms] t@6256 InCharge Framework
80 EMC Smarts SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers Version
9.4 Release Notes
ASL-W-EERROR_RULE_SOURCE-While executing rule set
'C:\darshan\IP\smarts\rules\import.asl'
ASL-EERROR_ACTION-While executing action at:
ASL-CALL_STACK_RULE- RuleName: OBJECT_NAME, Line: 151
ASL-CALL_STACK_RULE- RuleName: OBJECT_VALUE, Line: 137
ASL-EERROR_CREATE-While attempting to create the object
'DaslRuntimeEnv::IPDaslRuntimeEnv'
MR-CLASS_NOT_FOUND-Class of given name 'DaslRuntimeEnv' not found; in
file "n:/DMT-9.3.0.0/86/smarts/repos/mr/dyn_acc.c" at line 1746
```

SND-263

**Resolution**

IP Manager should not be running on the same host as that of the NCM installation.

**sm\_snmpwalk --autovlan command does not walk voice VLANs**

The command, `sm_snmpwalk --autoVlan <device>`, does not perform a walk of Voice-related VLANs.

Instead, this command creates walks for other VLAN instances.

CQ 643041, CQ 643045

**Resolution**

No resolution available.

**Compute fabric class does not get removed while deleting Cisco UCS Blade Enclosure Manager**

Compute Fabric Chassis class is not removed when its parent class or Cisco UCS blade enclosure manager is deleted.

Because of this issue, Vblock Chassis is not removed when you delete a Vblock device.

CQ 615852, CQ 615850

**Resolution**

To workaroud the problem, manually delete each Compute Fabrics instance individually, when you delete the corresponding Cisco UCS blade enclosure manager.

## ICMP ping polling when PingControl is enabled

PingControl overrides the default values for PingInterval and PingRetries parameters in the Connectivity polling setting.

CQ 651503

### Resolution

This is a known behavior in IP Manager. By default, the PingControl parameter is set to DISABLED. When a device goes down and does not respond to the first ping request, you can enable the PingControl parameter for the Connectivity polling setting in the Polling and Thresholds Console and then increase the values of PingInterval and PingRetries. When PingControl is enabled, the PingRetries value is used instead of the Retries value.

**Table 21** PingInterval and PingRetry default values when PingControl is enabled

When PingControl is	PingInterval default is	PingRetries default is	Retries default is
ENABLED	20 seconds	3 retries	
DISABLED (default)	180 seconds	6 retries	3 retries
	PingInterval acceptable values: 20-3600 seconds	PingRetries acceptable values: 0-10 retries	Retries acceptable values: 0-10 retries

## A stray license message is listed in the IP Manager log file

When you start the 9.3 IP Manager, a stray license message displays in the log file.

```
ICF_MAIN_MSG-*--UNLICENSEDFEATURE-The following feature(s) are not licensed: Certification for Cisco Devices
```

CQ 654502

### Resolution

Ignore the stray UNLICENSEDFEATURE message. As of IP Manager version 9.0 and later, the license key enables IP Manager to discover all vendor devices including Cisco devices. You should also see the following message in the log file:

```
ICF_MAIN_MSG-*--LICENSEDFEATURE-Enabling the following licensed feature(s):Certification of All Vendor Devices
```

## sysOIDs without rules in Topology Change Analysis Tool (TCAT) for IP Manager 9.4.2

If the following devices are present in the topology and you run the TCAT tool, the ID field for these devices will be populated as blank because the Topo rule file does not contain these devices currently.

- .1.3.6.1.4.1.12383.3.1.1
- .1.3.6.1.4.1.3417.1.1.36
- .1.3.6.1.4.1.119.2.3.76.2
- .1.3.6.1.4.1.41916.3.2.4

- .1.3.6.1.4.1.9.1.1855
- .1.3.6.1.4.1.9.1.1999
- .1.3.6.1.4.1.6527.6.2.1.2.2.1
- .1.3.6.1.4.1.6527.1.3.8
- .1.3.6.1.4.1.10734.1.3.35
- .1.3.6.1.4.1.3375.2.1.3.4.94
- .1.3.6.1.4.1.9.1.2133
- .1.3.6.1.4.1.25506.11.1.188
- .1.3.6.1.4.1.9.1.1830
- .1.3.6.1.4.1.1991.1.3.34.2.3.2.2

IS-7240

**Resolution**

This has no impact on the functionality.

**sysOIDs without rules in TCAT**

Five SysOIDs currently do not have rules updated in the TCAT rules file.

These will not display the explanation for differences in the TCAT report.

- .1.3.6.1.4.1.9.12.3.1.3.606
  - .1.3.6.1.4.1.9.1.525
  - .1.3.6.1.4.1.9.1.1043
  - .1.3.6.1.4.1.9.1.896
  - .1.3.6.1.4.1.9.1.658
- CQ 649759

**Resolution**

This has no impact on the functionality.

**Supported IP Manager released versions by TCAT**

A description or an explanation is not available in the TCAT report for devices certified or recertified in unsupported versions of IP Manager releases.

**Table 22** Supported IP Manager versions with the Foundation version

IP Manager version	Foundation version
9.1.0.0	9.1.0.0
9.2.0.0	9.2.0.0
9.2.1.0	9.2.1.0
9.2.1.x	9.2.1.1
9.2.2.x	9.2.2.0
9.3	9.3

CQ 649760

**Resolution**

This is a known behavior in TCAT and has no impact on the functionality.

## Changes made using sm\_edit to DASL files or any libraries or conf files kept in the local\dasl\ directories are not picked up by the IP Manager

Changes made using sm\_edit to DASL files (any library or configuration files kept in the local\dasl\ directories) are not picked up by the IP Manager.

Any file modified using sm\_edit would generally be copied to the local folder. Any customization done in this way, for DASL related files (files that exist in the BASEDIR/dasl folder), would go to the SM\_SITEMOD location, but these will not be picked up by the IP Manager.

With respect to changes to files in the BASEDIR/dasl/package folder, IP Manager would have the capability to pick the changes from the BASEDIR/local/dasl/package folder, but the SM\_SITEMOD location would not be honored.

CQ 649369

**Resolution**

The workaround is to modify the files directly in BASEDIR/dasl folder without using sm\_edit utility, with the help of some external editors.

## OID Info tool (oidInfo.conf) is merged to the conf/discovery folder after upgrade

The OID Info tool, oidInfo.conf file, is merged to the `conf/discovery` folder after upgrade.

CQ 643224

**Resolution**

In IP 9.2, the OID Info tool, oidInfo.conf, was under the `Basedir/smarts/conf/discovery` folder. Now the oidInfo.conf file is placed under `Basedir/smarts/conf/oidinfo/` folder.

If the oidInfo.conf file was modified in the IP 9.2 release, the customized configuration file will be merged by the migrate utility under `Basedir/IP/smarts/discovery` folder after upgrading to later IP versions.

After upgrade, if you run the sm\_oidinfo.pl script, it looks for the oidInfo.conf in the `conf/oidinfo` directory.

To resolve this, run sm\_oidinfo.pl with `--input=<conf>`

## When the IP-Configuration Manager was started, exceptions were seen during uninstallation

Exceptions were observed in the uninstall logs during uninstallation, when the IP-Configuration Manager was started.

**Example**

```
ServiceException: (error code = 315; message = "product bean
SERVICE_CM does not
exist"; severity = 0)
at
com.installshield.product.service.product.PureJavaProductServiceImpl.g
```

```

etProduct
Bean(Unknown Source)
at
com.installshield.product.service.product.PureJavaProductServiceImpl.g
etProduct
Bean(Unknown Source)
at
com.installshield.product.service.product.PureJavaProductServiceImpl.g
etProduct
BeanProperty(Unknown Source)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
at java.lang.reflect.Method.invoke(Unknown Source)
at
com.installshield.wizard.service.LocalImplementorProxy.invoke(Unknown
Source)
at
com.installshield.wizard.service.AbstractService.invokeImpl(Unknown
Source)
at
com.installshield.product.service.product.GenericProductService.getPro
ductBeanP
roperty(Unknown Source)
at
com.smarts.production.wizard.actions.RemoveSmartsServices.resolveServi
ceFeature
(Unknown Source)
at
com.smarts.production.wizard.actions.RemoveSmartsServices.execute(Unkn
own
Source)
at com.installshield.wizard.StandardWizardListener.execute(Unknown
Source)
at
com.installshield.wizard.StandardWizardListener.currentBeanChanged(Unk
nown
Source)
at com.installshield.wizard.Wizard$RunThread.run(Unknown Source)

```

CQ 641786

### Resolution

This issue was observed in RHEL 5 and RHEL 6 platforms and was not always reproducible. There is no resolution.

## Topology Change Analysis Tool (TCAT)

The following issues were observed for TCAT.

- The device type “FibreChannelSwitch” is not supported. Hence, for this device type, ignore the report generated by TCAT . This will be supported in a future release of this tool.
- Several instances having system names such as “F4-7F-35-50-C1-B0” and model names such as “AIR-CAP3502I-E-K9” were reported. As these could not be traced to any SYSOID, these changes could not be explained. This is currently under investigation.

CQ 643503

## Details tab for WirelessControllerRedundancyGroup::SwitchOverFailed displays incorrect values

The Details tab for the WirelessControllerRedundancyGroup::SwitchOverFailed event displays incorrect values for NumOfWAPsDownAfterSwitchover attribute. This will be fixed in a future release.

CQ 642181

## The “Ask before adding new systems” option does not work for SNMP v3 autodiscovery.

When triggering SNMP v3 autodiscovery, if the option, Ask before adding new systems, is selected, then the new devices will not be discovered using SNMP v3 discovery. IP Manager will try to discover the new devices using SNMP v2.

If SNMP v2 is not configured on the real device, discovery will fail. However, if the option is not selected, then SNMP v3 autodiscovery works without any errors.

CQ 641626

## Manual settings for Java and Java tools option

NAS probe failed to start a VNX or Celerra discovery.

CQ 638924

### Resolution

If a NAS probe fails to start a VNX or Celerra discovery, set the following options manually to start the NAS probe:

```
set JAVA_TOOL_OPTIONS=  
set _JAVA_OPTIONS=
```

Then run the following command to start the NAS probe:

```
sm_adapter_java -n remote-nas -b <broker> -J  
nas_probe.jar --output=remote_nas
```

You can now discover both VNX and Celerra along with FileServers automatically. The clientConnect.conf file should have credentials for VNX or Celerra discovery.

## hwEntityMemSize returns negative values for few entities

For Router with SYSOID .1.3.6.1.4.1.2011.2.62.2.8, hwEntityMemSize returns negative values for few entities.

CQ 587589 / CQ 639069

### Resolution

This is due to the vendor not implementing appropriate MIBs/Data types for these values. These values are displayed in the IP Manager. There is no functionality impact.

## HighFDUsageWarning event is not reported in the SAM Notification Log Console

The HighFDUsageWarning event is generated in the IP Manager but not displayed in the SAM Notification Log Console.

CQ 637288 / CQ 576275 / CQ 634626 / CQ 634935

### Resolution

The SM\_ElementManager class keeps track of the file descriptors used for new connections and uses this to estimate the number of descriptors currently in use.

The read-only attribute “fdLimit” in the SM\_ElementManager class indicates the maximum number of descriptors the domain is allowed to use. The configurable attribute “fdWarningHeadroom” indicates how close to this limit the server can get before the situation should be concerning. When the limit is exceeded, the event “HighFDUsageWarning” is asserted. This event is applicable only on the Linux operating system and not on Windows.

To display the “HighFDUsageWarning” event in the SAM Notification Log Console:

1. Find the dxa conf file used by the particular domain. For example, in the SAM Global Console, “Show Type Details” provides the file name. For INCHARGE-AM-PM, the dxa file name is dxa-conn-perf.conf.
2. Edit the dxa file under `SAM BASEDIR/conf/ics` to add a new event subscription for the SM\_ElementManager.

```
sub SM_ElementManager::.*::*/e
```

3. Save the dxa file and then reconfigure the Domain Manager.

---

### Note

The SM\_ElementManager receives the file descriptor (socket number) for a new client connection. On Linux hosts, there is a hard limit to the number of file descriptors that an application can use at any one time. Exceeding that limit is an irrecoverable condition that forces the application to exit with a fatal error. SM\_ElementManager keeps track of the file descriptors and uses its FDLimit and FDWarningHeadroom attribute values to determine when the number of file descriptors increases to an unacceptable level. When that limit is exceeded, the SM\_ElementManager asserts the HighFDUsageWarning event. The HighFDUsageWarning event is not supported for Windows.

---

## Monitoring Fabric Interconnect (FI) switches using floating IP address

If an IP server uses a floating IP address to monitor the Fabric Interconnect (FI) switches in a UCS, it cannot generate the switch Down root cause.

For instance, FI 1 and FI 2 are the two Fabric Interconnect switches that comprise a UCS. The Fabric Interconnect switches are added to IP server for monitoring by using floating IP address. When the active Fabric Interconnect switch (FI 1) goes down, the floating IP address moves to FI 2 and continues to respond. As a result, IP does not generate the FI 1::Down root cause.

CQ 635869 /CQ 635868

### Resolution

Discover the UCS Fabric Interconnect switches using their respective IP addresses instead of the floating IP address.

- If the Fabric Interconnect switch is discovered using a floating IP address, then delete the Fabric Interconnect switch and add it to the IP topology using a non-floating IP address.
- If the Fabric Interconnect switch is discovered by autodiscovery using floating IP address, then create a filter which does not match the floating IP address. This will prevent discovery of Fabric Interconnect switches using floating IP address.

## Multiple root causes generated for FabricInterconnect ports with AdminDown status

When ports connecting a Fabric Interconnect (switch) and BladeEnclosureManager are made AdministrativelyDown, the events Disabled (for Ports) and Down (for BladeEnclosureManager) are generated.

CQ 632923 / CQ 632845

### Resolution

The expected behavior is that only the event Disabled should be generated for ports. When computing the Down problem for BladeEnclosureManager, the operational status of the port should be considered and not the administrative status.

## IP Manager did not generate any events after an ESM MS cluster active node was powered off

Migration of the virtual IP address from active node(A) to active node(B) does not take place on the IP topology unless there is a rediscovery of all the cluster nodes.

In a cluster environment, the active node always holds the virtual IPAddress. The virtual IPAddress is released by the active node and brought up on one of the standby nodes whenever a protection switch is required.

If an active node(A) is powered off, the protection switch mechanism occurs. So the virtual IPAddress of active node(A) gets associated with the new active node(B). Thus all the IP addresses of active node(A) become unresponsive except the floating IP address because the floating IP address is now associated with the new active node (B). This results in the earlier active node (A) as Responsive because the floating IP address is still Responsive.

That is why the IP Manager did not generate any Host Down or Unresponsive events after the cluster active node was powered off.

CQ 574716 / CQ 574715

### Resolution

To avoid this scenario, manually unmanage the virtual IPAddress object from the IP Manager topology.

## ASL error messages in IP Server log file if both the management IP address and the primary address are used to discover Cisco UCS

A Switch address may be overwritten if both the Management IP address and the Primary IP address are used for discovery.

This creates ASL errors because both the Management IP address and the Primary IP address point to the same Switch.

Example

```
[September 5, 2011 9:25:49 AM GMT+05:30 +582ms] t@76 Discovery #1
ASL-W-EERROR_RULE SOURCE-While executing rule set
'/opt/InCharge/IP/smarts/rules/discovery/ic-br-stp.asl'
ASL-EERROR_ACTION-While executing action at:
ASL-CALL_STACK RULE- RuleName: __INIT__, Line: 99
ASL-EERROR_INIT_ACTION-While executing initialization actions
ASL-EERROR_GET-While attempting to get property 'PortNumber' of object
'Port::PORT-10.31.9.5/sys/switch-A/slot-1/switch-ether/port-13'
MR-CALL_ON_NULL_OBJECT-Tried to make a call on a NULL repository
object; in file
"ICIM_Network.h" at line 15834
```

CQ 574814

### Resolution

To avoid such a scenario, discover either:

- The Primary IP address and Secondary IP address, or
- The Management IP address and the Secondary IP address

## IP server log shows errors when started on Windows

After the IP server is started on Windows and devices discovered, errors display in the server log.

Example:

```
[August 3, 2011 8:24:34 PM GMT+05:30 +637ms] t@4424
MON-E-EXTERNAL_ERROR-Error encountered by the monitoring system when
calling
MON_MonitoringInterface::stopMonitoring on variable
NetworkAdapter_PerformanceData_ifMIB::I-
NetworkAdapter_PerformanceData_ifMIB-IF
-FAHRVERGNUGEN.MIT.EDU/8::ifHCOutOctets
ACC-PROPERTY_NOT_MONITORED-Property
'NetworkAdapter_PerformanceData_ifMIB::I-
NetworkAdapter_PerformanceData_ifMIB-I
F-FAHRVERGNUGEN.MIT.EDU/8::ifHCOutOctets' is not monitored; in file
"t:/DMT-9.0.0.X/1358/smarts/repos/accessors/MR_Accessor.c" at line
2214
[August 3, 2011 8:24:34 PM GMT+05:30 +637ms] t@4424
MON-E-EXTERNAL_ERROR-Error encountered by the monitoring system when
calling
MON_MonitoringInterface::stopMonitoring on variable
NetworkAdapter_PerformanceData_ifMIB::I-
NetworkAdapter_PerformanceData_ifMIB-IF
-FAHRVERGNUGEN.MIT.EDU/8::ifHCInOctets
ACC-PROPERTY_NOT_MONITORED-Property
'NetworkAdapter_PerformanceData_ifMIB::I-
NetworkAdapter_PerformanceData_ifMIB-I
F-FAHRVERGNUGEN.MIT.EDU/8::ifHCInOctets' is not monitored; in file
"t:/DMT-9.0.0.X/1358/smarts/repos/accessors/MR_Accessor.c" at line
2214
```

CQ 581768

### Resolution

The errors are benign in nature. They do not cause any impact on the functionality and can be ignored.

## ASL errors when discovering SNMPv3 devices with MD5 and DES protocols as seed in FIPS 140 mode

If you discover SNMPv3 devices with MD5 and DES protocols as seed in FIPS 140 mode, discovery fails and the devices go to the Pending List and display as “Invalid” or “Unsupported SNMP V3 protocol”.

The following ASL error exception messages are observed in the IP server logs.

```
[August 7, 2011 2:56:09 PM GMT+05:30 +890ms] t@4176 File-Importer-Driver
ASL-W-E-R-R-O-R _R-U-L-E _S-O-U-R-C-E-While executing rule set
'C:\IP812B60\IP\smarts\rules\discovery\ic-file-importer.asl'
ASL-E-R-R-O-R _A-C-T-I-O-N-While executing action at:
ASL-C-A-L-L _S-T-A-C-K _R-U-L-E- RuleName: ENTRY, Line: 222
ASL-C-A-L-L _S-T-A-C-K _R-U-L-E- RuleName: START, Line: 76
ASL-E-R-R-O-R _I-N-V-O-K-E-While attempting to invoke operation 'create' of
object
'MR_Object::ICF-TopologyManager'
ADTM-AD_EININVALID_PROTOCOL-Invalid SNMPv3 protocol: MD5, for
10.31.116.234, TM:
create
```

CQ 581703

### Resolution

MD5 and DES protocols are not supported SNMPv3 protocols in FIPS 140 mode. The ASL messages can be safely ignored and currently there is no resolution.

## During sm\_rebond, IP Manager generated core dump after SIGINT is received

When the sm\_rebond utility prompted to reenter the new pass phrase for confirmation and if Ctrl+C was issued after the prompt, the session terminated.

Any operating system commands issued after that on the console did not get printed on it and only the output was seen. SIGINT was received and the IP Manager generated core files.

When working normally, the sm\_rebond utility changes the secret phrase and re-encrypts the files affected by the secret. This utility prompts for the old secret phrase and the new phrase, then generates an imk.dat file and updates all the files containing encrypted information.

CQ 581606 / CQ 581572

### Resolution

The IP Manager generated core files because the newly generated imk.dat file was already present in the BASEDIR/smarts/local/conf directory. Move the imk.dat file to another location and then issue the sm\_rebond command.

## Mangled (unprintable characters) in IP Objects when IP Tagging is enabled

If a device responds with non printable characters for the RouteDistinguisher (RD), IP tagging creates garbage characters in the object names.

Because these objects can only be accessed through ASL, and not using dmctl or sm\_gui, the object properties cannot be seen. Also, because IP accesses through ASL, it does not restrict the creation of IP tagging for some vendors even if the configuration is not proper. That is, it responds to non-printable characters in SNMP queries.

CQ 581111 / CQ 550001 / SR41222470

**Resolution**

There is currently no resolution.

## **Interface instances are created but monitoring is not possible**

For the Omnitronix SL100 .1.3.6.1.4.1.3052.40.1.1 certification, interface instances are created but the ifOperStatus is not available for the Host device under Interface. Hence monitoring is not possible and fault alarms are not created.

CQ 579045 / CQ 578713

**Resolution**

There is currently no resolution.

## **Defaults cannot be reset for some threshold settings in the Polling and Thresholds Console**

Some parameters do not have default values defined in the Thresholds group of the Polling and Thresholds Console.

Changing the value of those parameters and then clicking Restore Defaults will not revert the value to the previous default value.

CQ 573825 / CQ 573735

**Resolution**

There is currently no resolution.

## **Attribute Mismatch on NumberofIPs between first and second discovery**

Attribute Mismatch errors on NumberofIPs were observed on every alternate rediscovery of some devices.

Example

- On every alternate rediscovery of a Juniper T640 device, IPs under Line Card Chassis(LCC) were deleted.
- First discovery: Switch Card Chassis(SCC) and LCCs were created with all components including IPs.
- Second discovery: Only IPs under LCCs were deleted with everything else intact.
- Third discovery: IPs under LCCs were again created.

CQ 572826 / CQ 572931

**Resolution**

Rediscover the device.

## **The brcontrol output may show the SAM Server PID as "0"**

The output after executing brcontrol showed the SAM server process ID as 0, although the SAM server was running.

CQ 570690 / CQ 570692

**Resolution**

This issue was observed once and was not reproducible. There is no functionality impact because of this and can be ignored.

**IPSec exception messages appear in the log file**

IPSec exception messages might appear in the IP Manager's log file during IPSec short discovery.

**Example:**

```
CI-E-ESRVTHEXCEPTION-Service thread closure for queue ShortDiscovery
#5 threw
exception MR-CALL_ON_NULL_OBJECT-Tried to make a call on a NULL
repository
object; in file
"i:\ip-x.x.x\117\smarts\auto-discovery\winnt-x86-32\optimize
\TopologyManager.h"
at line 16963
[June 11, 2009 3:20:12 PM GMT+05:30 +453ms] t@12792 ShortDiscovery #3
CI-E-ESRVTHEXCEPTION-Service thread closure for queue ShortDiscovery
#3 threw
exception MR-CALL_ON_NULL_OBJECT-Tried to make a call on a NULL
repository
object; in file
"i:\ip-x.x.x\117\smarts\auto-discovery\winnt-x86-32\optimize
\TopologyManager.h"
at line 16963
```

CQ 496770, CQ 373854

**Resolution**

No user action is required. The IP Manager will successfully recover from the exception and continue to function properly.

**Incorrect status for IKE tunnels involving a Cisco 2800 router**

When an Internet Key Exchange (IKE) tunnel goes down on a Cisco 2800 router, the IP Manager does not generate a DownOrFlapping event.

CQ 498699, CQ 286338, CQ 224286,

**Resolution**

This issue is due to a problem in the SNMP agent running on a Cisco 2800 series router, running Cisco IOS release Version 12.4(6)X2, (fc1)m. In this scenario, the GET and GETNEXT SNMP operations on the cikeTunStatus OID return different values. There is no workaround at this time.

**Set operator "->" does not work with dynamic model**

During dynamic model compilation, computed attributes or relationships that have expressions involving the "->" set operator get generated without the flag that indicates "Uses Propagation".

As a result, trying to evaluate the expression causes the MR\_MULTIPLE\_OBJECT\_LOCKS error.

CQ 500279, CQ 500244

**Resolution**

Do not use the "->" set operator for dynamic modelling.

**Multiple instances of Broker may try to use the same port (Windows-specific problem)**

Multiple instances of Broker are able to use the same port on the same machine (Windows-specific). There is no message to explain that the address or port is in use.

CQ 506290

**Resolution**

There is currently no resolution. This is a limitation of the Windows operating system.

**Output from brcontrol utility differs based on operating system**

Output from the brcontrol utility differs between IPv6-only Windows Broker and IPv6-only Linux Broker.

CQ 506320

**Resolution**

Two entries of the same server (one registered to IPv4 port and one to IPv6 port) are listed in the brcontrol output when run on an IPv6-only Windows operating system. The brcontrol output shows one entry RUNNING that is registered to the IPv6 port. (The IPv4 DEAD entry is pruned off in the Linux platform.)

The IPv4 address appears on the IPv6-only Windows operating system because we cannot completely remove the hard-coded local loopback address, 127.0.0.1.

**MR-CALL\_ON\_NULL\_OBJECT- NULL repository object and Object Not Found errors**

ASL errors associated with DuplicateIP instance appear during discovery.

NULL repository object and Object Not Found errors are seen in the log file if multiple instances of the same device are discovered at the same time. This is observed if duplicate devices are present in the seed file used for discovery. For example,

```
[July 20, 2010 9:30:40 PM EDT +139ms] t@66 Discovery #5
ASL-W-E-R-R-O-R_R-U-L-E_S-O-U-R-C-E-While executing rule set
'/opt/emc/torrecl/ip8Single/9/solaris8-sparc-64/IP/smarts/rules/
discovery/ic-ip
-address.asl'
ASL-E-R-R-O-R_A-C-T-I-O-N-While executing action at:
ASL-C-A-L-L_S-T-A-C-K_R-U-L-E- RuleName: __INIT__, Line: 106
ASL-E-R-R-O-R_I-N-I-T_A-C-T-I-O-N-While executing initialization actions
ASL-E-R-R-O-R_G-E-T-While attempting to get property 'DuplicatedBy' of
object
'DuplicateIP::IP-10.148.16.254'
Known problems and limitations 95
MR-O-B-J-E-C-T_N-O-T_F-O-U-N-D-Object of given name and class
DuplicateIP::IP-10.148.16.254
not found; in file
"/work/blackcurrent/DMT-9.0.0.X/1248/smarts/repos/mr/dyn_acc.c" at
line 1587
[July 21, 2010 12:20:43 AM EDT +113ms] t@70 Discovery #9
ASL-W-E-R-R-O-R_R-U-L-E_S-O-U-R-C-E-While executing rule set
'/opt/emc/torrecl/ip8Single/9/solaris8-sparc-64/IP/smarts/rules/
discovery/ic-ip
-address.asl'
```

```

ASL-ERROR_ACTION-While executing action at:
ASL-CALL_STACK_RULE- RuleName: DATA, Line: 208
ASL-CALL_STACK_RULE- RuleName: START, Line: 169
ASL-ERROR_PUT-While attempting to set property 'Netmask' of object
'IP::IP-10.1.168.2'
MR-CALL_ON_NULL_OBJECT-Tried to make a call on a NULL repository
object; in file
"ICIM_Network.h" at line 27575

```

CQ 528757, CQ 528758, CQ 528759, CQ 528760, CQ 528761

#### Resolution

The errors, found during an initial seeding of the topology or during an initial autodiscovery cycle, do not impact any functionality and can be ignored.

## Servers could not be attached when services were restarted

In Windows, when services were restarted, the servers could not be attached since the GUI did not list the servers, although the brcontrol command displayed that servers were running.

CQ 565498 / CQ 565544

#### Resolution

This is a limitation of the Windows operating system. Ensure that you do not start multiple Brokers on the same host.

## ASL errors seen when discovering the seedfile

When discovering the seedfile, the following ASL error occurred:

```

[November 16, 2010 2:31:54 PM EST +019ms] t@65 Discovery #2
ASL-W-ERROR_RULE_SOURCE-While executing rule set
'/IP/smarts/rules/discovery/ic-create-port-ifdescr.asl'
ASL-ERROR_ACTION-While executing action at:
ASL-CALL_STACK_RULE- RuleName: __INIT__, Line: 106
ASL-ERROR_INIT_ACTION-While executing initialization actions
ASL-ERROR_INVOKE-While attempting to invoke operation 'findInterface'
of object
'Switch::10.5.26.1'
MR2-MR_WHILE_OPERATION_INVOKE-While invoking operation findInterface
in object
'Switch::10.5.26.1'
MR-OBJECT_NOT_FOUND_EX-Cannot find object 'Switch::10.5.26.1'
MR-CALL_ON_NULL_OBJECT-Tried to make a call on a NULL repository
object; in file
e "/work/blackcu

```

CQ 571628

#### Resolution

The last message indicates that the device on which the discovery is being performed has been removed while the discovery is taking place. This can happen if there are duplicate entries in the seed file, or the device has multiple IPs with different DNS names and when autodiscovery is enabled. Messages higher in the stack are random since the deletion can occur at any point in the discovery cycle.

The error is benign in nature and can be ignored since the device is likely to be discovered using a different name.

## Router Processor HighUtilization value exceeds 100% when monitoring discovering a device

When some devices were discovered during certification, the processor utilization value is displayed over 100%.

CQ 572599

### Resolution

This occurs for some vendor devices if the SNMP agent returns an incorrect value due to an error in the device MIB in presenting the data. The IP Manager is currently not able to fix the upper cap for processor utilization at 100% for all vendor devices.

## SNMP errors seen in the log file while discovering Hosts

SNMP errors were seen in the log file while discovering Hosts.

Example:

```
SNMP-E-AGENTERRORSTATS-Below message for SNMP agent at  
'10.10.11.22:161', was suppressed 0 times since The Epoch SWFE-ELOOP-  
Agent loops in response to GET_NEXT: Agent: 10.10.11.22, First OID: .  
1.3.6.1.4.1.2021.4.3
```

CQ 572742 / CQ 570939

### Resolution

This is seen while discovering Hosts which have subagents, such as Dell OpenManage, IBM Director, NetSNMP, and HP Insight Manager, installed. IP Manager has to query at least one OID specific to these subagents to find their existence. If it is not present, SNMP errors are displayed in the log file.

There is currently no resolution. These errors do not cause any impact on the functionality.

# CHAPTER 4

## Server Manager (ESM)

This chapter includes the following topics:

- [Server Manager overview](#) ..... 154
- [New features and changes in Server Manager](#) ..... 155
- [Fixed Issues in Server Manager](#) ..... 155
- [Known problems in Server Manager](#) ..... 167

## Server Manager overview

Server Manager works in conjunction with the IP Manager and the Service Assurance Manager to discover, monitor, and analyze the availability and performance of many hardware and software elements.

The *EMC Smarts Server Manager User and Configuration Guide* provides a complete list of the hardware and software elements, including Storage Area Network elements and VMware® virtual products.

## Server Manager discovery and monitoring

The Server Manager imports initial topology from the IP Availability Manager. After the topology is imported, the Server Manager discovers domain-specific entities relating to the licensed features and creates additional topology objects for those features.

For example, for the VMware feature, the Server Manager topology includes VMware entities such as the VMware ESX server and virtual machines.

After discovery and topology creation, the Server Manager reconnects with the IP Availability Manager from which it discovered the topology. It then places the IP addresses of the virtual machines it discovered on the Pending List of the IP Availability Manager. This ensures that every virtual machine is discovered as a separate entity.

The Server Manager performs domain-specific monitoring that varies depending on the feature being monitored. For example,

- For the VMware feature, the Server Manager uses vCenter API.
- For the Software-Defined Networks feature, the Server Manager uses RESTful web services API.
- For the Microsoft Hyper-V feature, the Server Manager uses Microsoft Windows Management Instrumentation (MS WMI).
- For the KVM hypervisor management, the Server Manager uses OpenStack NOVA API and RESTful web services API.
- For the Microsoft Cluster feature, the Server Manager uses Microsoft Windows Management Instrumentation (MS WMI).
- For Host performance monitoring, the Server Manager uses SNMP and WMI.
- For the F5 BIG-IP, the Server Manager uses SNMP.
- For Storage Area Network monitoring and discovery, ESM has been integrated with EMC M&R to derive storage array and SAN related topology data. This information is exposed through the EMC M&R Web Interface API.
- For Process Monitoring, the Server Manager uses SNMP and WMI.
- For the Atmos feature, the Server Manager uses SNMP.

In addition, the Server Manager subscribes to IP Availability Manager events such as Host Unresponsive and uses them to perform cross-domain root-cause and impact analysis. The Server Manager correlates the effect of problems with the physical host systems on the virtual entities for that feature .

## New features and changes in Server Manager

There are no new 9.6 features for Server Manager.

## Fixed Issues in Server Manager

Here are the fixed issues for Server Manager.

**Table 23** Fixed issues in Server Manager (ESM)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-9796 SR 88896838	The F5 Loadbalancer Pool events is not generated post ESM 9.4.2 patch 12 implementation.	There is no need to update OS version again by HostResources MIB-2 data, as the OS version for F5 specific device is getting updated in the containment driver itself.	9.4.2	9.5.1
IS-9074 SR 07880320	There is a lack of CPU FileSystem memory (and other features) for managed hosts on ESM Topology.	The user can create WMI credential using hostname or FQDN or IP address in host field, and perform the discovery.	9.4.1	9.5
IS-9097 SR 07864248	The PrimaryOwnerContact attribute is not populated with data.	The PrimaryOwnerContact attribute has been populated in ESM on host entities.	9.4.1.X	9.5
IS-7476 SR 5162222	ESM and IP are reporting some virtual machines on the vCenter: some virtual machines on the vCenter are properly reported as virtual, and whereas some are reported as physical servers.	Cluster names are reused across different data centers which have been fixed now.	9.4.1	9.5
IS-8183 SR 06228280	Event correlation does not work for VirtualMachine class.	Code has been modified as follows: 1. If the host (HostType = VIRTUAL and member of Partition) in IP	9.4	9.5

**Table 23** Fixed issues in Server Manager (ESM) (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		<p>becomes unresponsive, the VM in ESM which virtualizes the host would generate “Virtual Machine Down” event.</p> <p>2. If the host (HostType = VIRTUAL and member of Partition) in IP becomes unresponsive and the partition to which it belongs is Down, then the VM in ESM which virtualizes the host would clear the “Virtual Machine Down” event.</p> <p>3. If the switch is down, the ESX host and VM hosts become unresponsive in IP. However, the VM down is not generated from ESM. The impact of Switch Down would not display that VM has been impacted. This is as per the existing design.</p>		
IS-8267 SR 06728433	<p>Getting wrong application count and unable to monitor the application, which is incorrectly marked as duplicate. Also, the following issues occur:</p> <ul style="list-style-type: none"> <li>• Applications are getting created on ICMPONLY hosts.</li> </ul>	<p>Process Name rather than using regex pattern matching (glob).</p> <p>Following is the resolution for the issues:</p> <ul style="list-style-type: none"> <li>• In order to remove the application from the</li> </ul>	9.4.2.2	9.5

**Table 23** Fixed issues in Server Manager (ESM) (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	<ul style="list-style-type: none"> <li>• On loading the process data (APP-XXX.txt) files, the applications are getting removed on discoverAll/discovery/sync.</li> <li>• On upgrade, the template name and relationship is not retained to the application.</li> <li>• Also, many unwanted processes, which are part of SNMP host data, are getting recreated on the ICMPONLY host, which results into many processes on the topology.</li> </ul>	<p>ICMPONLY host, CleanRougeApplications flag is introduced in the esm-param.conf file, and the same is used in esm-post to remove the rouge applications.</p> <ul style="list-style-type: none"> <li>• 9.4.1 did not have the templateRow present in the process data files(txt), and on upgrade, the templateRow value changes to 0, which was causing the applications to be removed from the host, on loading of process data files.</li> <li>• The templateName was getting overwritten to empty incase if user loads the process data files from while upgrading. So, in order to retain the process templateName, the templateName is being read, while processing the host monitor config file.</li> <li>• The Application::remove() code is added to clean the ESM_ProcessMonitoring_Setting of the host, in case if the application is removed and the same does not get reused during</li> </ul>		

**Table 23** Fixed issues in Server Manager (ESM) (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		discovery or monitoring.		
IS-8397 SR 06228280	Event correlation does not work for VirtualMachine class.	Code has been modified to fix this issue.	9.4	9.5
IS-8303 SR 84196536, 6546943	ESM shows applications against ICMPONLY hosts with no SNMP or WMI access.	Model has been modified to create processData based on thread ID and the host name unlike the earlier way of creating it using just the thread-id. With the earlier approach, it was possible that the same thread ID in future process an ICMP host and hence it may create same processes for the ICMP host which belong to SNMP host. Now with this fix, process Data is created with UcsName along with the threadId.	9.4.1.X	9.5
IS-8207 SR 5703542	The Smarts Server Manager displays IncompleteNetworkConfiguration alarm for sfda18-dc1-bcs and sfda18-dac1-bcs.	Code has been added to provide support for vNIC type E1000e and create relationship with vSwitch.	9.4.1.X	9.5
IS-8007 SR 83051280	Receiving notifications of high utilization on processor groups that cannot be matched by scripts to the parent host objects. This disrupts the process where tickets are automatically opened and emails are sent to the user.	The fix is to clean up the ESM topology that has orphan processor/memory groups. Also, the processor/memory group that is already being exported from IP domain is to be deleted if the same are getting created in ESM domain by setting the EnableCPUFilesystemMemoryDiscovery to TRUE.	9.4.1	9.5
IS-8267 06728433	Following problems were observed when the user upgraded ESM	1. In order to remove the application from the ICMPONLY host,	9.4.2.2	9.5

**Table 23** Fixed issues in Server Manager (ESM) (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	<p>from 9.4.1 to 9.4.2.2 version. This can be true in case if user upgrades from any other version to 9.4.2.2.</p> <ol style="list-style-type: none"> <li>1. Applications were getting created on ICMPONLY hosts.</li> <li>2. After loading the application data (APP-<code>&lt;hostname&gt;.txt</code>) files, the existing applications were removed on <code>discoverAll/discovery/sync</code>.</li> <li>3. After upgrade, the template names and the relationship to associated templates were not retained on the applications which were created on the hosts via the application templates.</li> <li>4. Unwanted processes part of SNMP host were getting recreated on the ICMPONLY host which resulted in to many application missing events on the topology.</li> </ol>	<p>the CleanRougeApplications flag is introduced in the <code>esm-param.conf</code> file. You can find the <code>esm-param.conf</code> file under <code>\$SM_HOME/local/conf/esm</code> folder.</p> <ol style="list-style-type: none"> <li>2. The version 9.4.1 did not have the <code>templateRow</code> present in the process data files (<code>txt</code>). And, on upgrade, the <code>templateRow</code> value changes to 0 which was causing the applications to be removed from the host on loading of process data files.</li> <li>3. The <code>templateName</code> was getting overwritten to empty in case if user loads the process data files from while upgrading. So in order to retain the process <code>templateName</code>, the <code>templateName</code> is being read while processing the host monitor config file.</li> <li>4. The <code>Application::remove()</code> code is added to clean the <code>ESM_ProcessMonitoring_Setting</code> of the host in case if the application is removed and the same does not get reused during discovery or monitoring.</li> </ol>		
IS-7726 SR 5703542	Smarts Server Manager displays IncompleteNetworkConfiguration alarm for <code>sfda18-dc1-bcs</code> and <code>sfda18-dac1-bcs</code> .	Code has been added to provide support for vNIC type E1000e and create relationship with vSwitch.	9.3.0.X	9.5

**Table 23** Fixed issues in Server Manager (ESM) (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-7543 SR 83051280	Receiving notifications of high utilization on processor groups that cannot be matched by scripts to the parent host objects. This disrupts the process where tickets are automatically opened and e-mails are sent to the user.	The fix is to clean up the ESM topology that has orphan processor/memory groups. Also, the processor/memory group that is already being exported from IP domain is deleted if the same are getting created in ESM domain by setting the EnableCPUFilesystemMemoryDiscovery to TRUE.	9.4.1	9.5
IS-6879 SR 79710496	ESM does not synchronize with remnants of HBA devices when removed from AM PM domains.	Code has been modified for removing the VMKernelPort and ScsiLun instances. The code changes invokes delete function on the vcenter and its components instead of removing in order to remove the associated components.	9.4.1.1	9.5
IS-4969 SR 74743550	If hrSWRunPath 1.3.6.1.2.1.25.4.2.1.4 OID can be used instead of an exe path.	In order to fix this issue, the user was advised to upgrade to 9.4.1.4 build 6.	9.4.0.X	9.5
IS-4917 SR 74564452	ESM displays processes in the process monitor differently on the same host when comparing the NetSNMP 5.1 Agent version the Sysedge Agent.	For application monitoring, the process path has been included in right manner while comparing the existing application record with current application data fetched from host. The inclusion of path with application name was corrected when using full path is enabled.	9.3.0.x	9.5
IS-5115 SR 75128240	The nbcssc process is not created in configure process monitoring.	Issue :In case if the SNMP Agent returns an empty(null) name for an index for the OID	9.4.0.X	9.5

**Table 23** Fixed issues in Server Manager (ESM) (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		<p>hrSWRunName, then upon creating the process monitoring template, ESM does not show the process next to the index which is empty.</p> <p>This also, does not apply even if user manually creates a template.</p> <p>Solution: If present then null values are being checked and handled while queying for applications on the host.</p>		
IS-6942 SR 73066448	On discover, ESM hangs.	The "F5-BigIP-NULL-Selector" no longer throws any ASL error and the hang must not occur anymore.	9.3.0.0	9.5
Fixed problems in ESM 9.4.2				
SND-2647, IS-5001	SNMP v3 discovery does not work in Server Manager.			9.4.2
SND-2792, SND-2693	Applying the template when "Full Path" is enabled doesn't work.			9.4.2
SND-2664, SND-2793, SND-2821, SND-2822	Multiple application templates with subsets of processes cannot be applied to a Windows host.			9.4.2
IS-5089 SR 75128240	nbcssc process is not created on Configure Process Monitoring. In case if the SNMP Agent returns an empty(null) name for an index for the OID hrSWRunName, then while creating the process monitoring template, ESM does	If present, then null values are being handled while creating and while discovering on the host.	9.4.0.X	9.4.2

**Table 23** Fixed issues in Server Manager (ESM) (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	<p>not show the process next to the index which is empty.</p> <p>This also does not apply even if user manually creates a template.</p>			
IS-4497 SR 73066448	ESM hanging on discovery.	The bug is that the null.asl does not seem to have the DEFAULT rule to catch the asl front end exception which triggered the asl error as what being reported.	9.3.0.X	9.4.2
IS-6879 SR 79710496	<p>ESM not syncing out remnant HBA devices when removed from AM PM domains.</p> <p>Due to discovery exception like read timeout, the relationships were not created between the vCenter components.</p> <p>This results in stale instances in some scenarios.</p>	The stale instances which are not part of any vCenter are removed during ESM post processing.	9.4.1.X	9.4.2
IS-3819	<p>Null Pointer exception occurs during device discovery.</p> <p>Following Java NULL pointer exceptions occur while discovering VMAX, VNX, Brocade and Cisco MDS switch data.</p> <pre data-bbox="397 1608 652 1923"> [March 4, 2015 6:22:01 AM EST +544ms] t@4388 platform MAIN_MSG-**- STDFD_ERR-stderr: java.lang.NullPoint erException [March 4, 2015 6:22:01 AM EST +544ms] t@4388 platform MAIN_MSG-**- </pre>	<p>This fix handles the exceptions when EMC M&amp;R sends any invalid data.</p> <p>Modified file:</p> <p>classes/ esm_vcenter.jar</p>	9.4	9.4.1

**Table 23** Fixed issues in Server Manager (ESM) (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	<pre>STDFD_ERR-stderr:     at com.smarts.w4n.w4nD ataSource.w4nXMLMan agement.XMLDataMgrI mplement.getAllElem entsName(XMLDataMgr Implement.java:49)     at com.smarts.w4n.disc covery.storage.Stora geDiscovery.startDi scovery(StorageDisc covery.java:70)     at com.smarts.w4n.disc covery.common.W4NDi scoveryManager.start SolutionPackDiscove ry(W4NDiscoveryMana ger.java:117)     at com.smarts.w4n.disc covery.common.W4NDi scoveryManager.initi ateDiscovery(W4NDi scoveryManager.java: 96)     at com.smarts.w4n.disc covery.common.W4NDi scoveryProbe.invoke( W4NDiscoveryProbe.j ava:134)     at com.smarts.java_pro be.ProbeRunner.invo ke(ProbeRunner.java :69)</pre>			
SND-1535	ProcessPerformanceM onitoring is not happening for WMI devices.		9.3	9.4.1
SND-2204	<p>For Brocade Fabric, some of the relationships are not created in ESM integration with M&amp;R 6.5 and vCenter discovered:</p> <ul style="list-style-type: none"> <li>• MemberPort</li> <li>• MemberPortLink</li> <li>• TraversedBy</li> </ul> <p>In case of ESM and M&amp;R integration, the following relationships may</p>	Addressed the logic issue and now the relationship is created. Modified file: classes/esm_vcenter.jar	9.4	9.4.1

**Table 23** Fixed issues in Server Manager (ESM) (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	<p>not be discovered for Brocade Fabric:</p> <ul style="list-style-type: none"> <li>• MemberPort</li> <li>• MemberPortLink</li> <li>• TraversedBy</li> </ul>			
IS-4207 SR 71810916	Smarts ESM is generating log errors with regards to Variable 'VMWareClusters' has not been assigned a value.		9.3.0.X	9.4.1
Fixed problems in ESM 9.4 and 9.3				
IS-2366 IS-2592 SR 67940014 SR 69043310	ESM Topology Not Cleaned Up After ESX Removal.	<p>The cleanup of ESX host is handled properly. However, the ScsiLuns will stay in the topology as it can still be there in case if they are discovered through Array.</p> <p>Modified file:</p> <p>local/rules/esm/esm-post.asl</p>	9.2.1.0	9.4
IS-2838 69573044	F5 Pools are not discovered and monitored properly.	<p>IPv4z type IP addresses were not parsed according to new standards. As a result, some of the pool members were not created. The code has been enhanced to parse IPv4z IP address and create the pool members.</p> <p>Modified files:</p> <ul style="list-style-type: none"> <li>• rules/f5/ic-f5_esm-pools.asl</li> <li>• conf/esm/ DISCOVERY_f5_ESM.import</li> </ul>		9.4
IS-1878	The ESM Domain is in perpetual discovery.	The root cause of this issue is that Exchange has a huge IP topology that changes	9.4	9.4

**Table 23** Fixed issues in Server Manager (ESM) (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		<p>frequently. The ESM server does a topology sync with IP whenever IP changes.</p> <p>The problem is that because of the huge topology and frequent IP topology changes we are never able to completely finish discovery without starting a new dxa sync with IP which initiates another full discovery.</p> <p>To address this issue, changes were made to ESM dxa discovery to implement incremental discovery.</p> <p>Configuration change is also needed at the customer site.</p>		
IS-1877	The ESM Domain freezes during Discovery	<p>Since the discovery is multi-threaded, some situation arises during discovery that some threads are waiting on a mutex that is being locked from another thread. If an exception occurs and the mutex is not released, this creates a thread deadlock situation.</p> <p>Changes were made to WMI discovery drivers to handle this.</p>	9.4	9.4
IS-1689	Create new service process for WMI accessor and poller	<p>Exchange has more than 12000 objects being polled during WMI Polling. Since Process Monitoring polling instrumentation is created after the cpu/memory/filesystem/disks/interface etc, it has a lower priority. As a result, the process</p>	9.4	9.4

**Table 23** Fixed issues in Server Manager (ESM) (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		<p>monitoring polling is happening after the polling for the above mentioned objects and it could take hours sometimes before we actually run WMI Process Monitoring. This is unacceptable. To address this issue, we have decided to separate the service process monitoring polling from the other WMI polling by creating a separate Accessor and Poller just or WMI Process Monitoring.</p>		
SND-1465 IS-2026	Process monitoring FALSE DOWN event in ESM.		9.4	9.4
610536 SR 58543552	Disk Failure alarm not being reported	Dell Disk event computation was incorrect and has been corrected to fix the issue.	9.2.2	9.3
653152 SR 58207364	F5 Load balancers running v11 are not being monitored.	AM and PM entities are now getting discovered and monitored for F5 Loadbalancers with version 11.	9.1	9.3
653924 SR 60887814	False VSwitchofLostConnection alert generated on non ESXi servers (those have only ServiceConsolePort)	Prior to 9.3, ESM was generating alerts even if the KernelConsolePort is not available on the ESX. The 9.3 Model has been modified to handle the case and to generate alerts only if KernelConsolePort is available and is down.	9.2.1.4	9.3
654348 SR 61815176	The VMVirtualizes relationship is not updated for a VirtualMachine when it	The post processor in ESM has been addressed to update the VMVirtualizes/ VirtualizedByVM	9.2.2	9.3

**Table 23** Fixed issues in Server Manager (ESM) (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	has multiple IP addresses configured.	relationship between Hosts and VirtualMachines even if the VirtualMachine has multiple IP addresses associated with it		

## Known problems in Server Manager

These problems affect Server Manager.

### Error occurs while adding HTTPS credentials of M&R

If the HTTPS credential addition of M&R fails with the following error in the log, then the following resolution steps need to be followed:

```
[May 17, 2018 7:03:37 AM EDT +360ms] t@3544 platform
MAIN_MSG--*--STDFD OUT-stdout: APGTests::LoginTest: caught exception:
javax.xml.ws.WebServiceException: Failed to access the WSDL at:
https://10.247.62.115:58443/APG-WS/wsapi/db?wsdl. It failed with:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to
find valid certification path to requested target.
```

SND-6640

#### Resolution

The following steps need to be performed to successfully add the credentials:

1. Download the certificate:

```
echo -n | openssl s_client -connect <M&R
IP>:58443 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
> /tmp/W4net.cer
```

2. Import the certificate:

```
keytool -import -storepass changeit -noprompt
-alias w4netcert -keystore <BaseDir of ESM
Install>/smarts/jre/lib/security/cacerts -trustcacerts -file
/tmp/W4net.cer
```

### ASL errors appear in SAM logs due to ScaleIO StorageClientService Disconnected event

ASL errors appear in SAM logs when StorageClientDisconnected Event is generated and HostedBy relationship is not present for StorageClientService.

SND-5673

**Resolution**

Discover StorageClientService as a Host in IP Server. This results in StroageClientService HostedBy relationship with Host hence ASL errors does not appear in the SAM logs.

**Restore Defaults option in P&T is not working for DisablePollingList text box where user can specify the classnames**

Whenever user provides classname for DisablePollingList text box in the following path: ScaleIO Polling Groups > ScaleIO Storage Provider > settings > Storage Provider Polling, and apply it, then click on Resotre Defaults options, the provided classname in the DisablePollingList text box is not getting cleared.

SND-5692

**Resolution**

Whenever user provides classname for DisablePollingList text box, to clear the entry in the textbox, the user needs to manually delete the contents in the text box.

**ScaleIO Host instance Discovery Method attribute shows wrong value as SNMP\_Discovery in ESM server**

When user starts the IP and ESM server, and discovers the ScaleIO host instance. The DiscoveryMethod attribute displays wrong value as SNMP\_DISCOVERY instead of SCALEIO\_DISCOVERY in ESM.

SND-5691

**Resolution**

No functionality is impacted by this issue. This issue is inconsistent and there is currently no resolution, and can be ignored.

**Any change in OpenStack credentials requires a rediscovery to be triggered in ESM Server**

In the ESM Server, any change in OpenStack credentials requires a rediscovery that needs to be triggered.

SND-5638

**Resolution**

Rediscover the OpenStack host in the ESM server.

**Manually configured Process Monitoring applications are not getting listed in ESM Server post upgrade and migrate**

After upgrading from lower versions of ESM to 9.5, the process monitoring applications which were created manually earlier (before upgrade) are not getting listed.

SND-5667

**Resolution**

There is an additional step which is required to be performed post upgrade in order to list all the manually configured applications. Perform the following procedure:

1. Take the backup of all the files with the format "APP-\*.txt", in <ESM-BaseDir>/smarts/local/conf/esm.
2. Perform the upgrade process.
3. Start the ESM Server and wait for discovery to complete.
4. Copy the previously backed up files from Step 1 and place it in the newly upgraded/migrated path <ESM-BaseDir>/smarts/local/conf/esm.
5. Attach the ESM Server to the SAM Console.
6. Right click on the ESM Server and select the option "Load all ESM host monitoring data from backup".
7. Trigger Discover all in ESM Server.
8. Verify that all the manually configured process before upgrade/migrate are getting listed in ESM Domain Manager.

## Two RCA (Cable Down and Interface Down) are generated when cable between the Host and the Switch goes down

In ESM 9.5, discover any Host and Switch which has cable connection. When the cable connection is down, two RCA are getting generated.

SND-5557

### Resolution

There is no resolution.

## Wrong credentials are updated in ESM

When user enters the wrong credential for existing userID by using "Apply Credential with testing" option, the wrong credentials are updated in the ESM. This behavior is also observed in the Vcenter and in the ScaleIO.

SND-5522

### Resolution

In case the credentials are changed, user can delete the credentials and re-enter.

## ESM logs are getting dumped with "WMI-Configuration does not exist" messages

In ESM 9.4.2, when the ESM server is started with the `--clean-topology` option, the following messages appear in the log files:

```
WMI-Configuration does not exist
```

SND-3901

### Resolution

There is no impact to functionality. The workaround is to restart the ESM server service. The *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers* provides information about starting services.

## Duplicate entries are created for process monitoring on a Windows host

Duplicate entries for EMC Smarts processes are created after a new filter is added for process monitoring and rediscovery is performed.

SND-2578

**Resolution**

There is no resolution.

## **Inconsistent EMC M&R name in the 9.4 Global Console**

When the 9.4 Domain Manager Administration Console is attached to the 9.4 or 9.3 Server Manager, EMC M&R appears as a choice in the Configure ESM Credentials window.

In the Polling and Thresholds Console, the W4NServer Polling Group and W4NServer Polling setting appear.

SND-1718

**Resolution**

No functionality is impacted because of this difference in the naming convention. The term EMC M&R replaces Watch4net or W4N.

## **Cable not created properly between master Xen server and Switch**

Cable not created properly.

SND-1604

**Resolution**

Add Xen VM MAC address range used during vm configuration to `tpmgr-param.conf` file. For example, `VirtualMACPattern 00-00-0C-07-AC-|00-00-5E-00-01-|<Xen-VM-Mac-Addr-Range>`

## **Deleting Xen Host and performing Discover All in IP server or ESM server does not remove associated Hypervisor instance**

In VMware, VCenter objects are deleted when a corresponding host is deleted in IP AM-PM server.

In Hypervisor hostby relationship, for both vendors, only Host is deleted and Hypervisor instance is retained as it is in ESM.

SND-1098

**Resolution**

Delete Hypervisor manually or delete using a script in ESM.

## **Unmanaging Xen Hypervisor instance does not unmanage its CPU, Memory, and VM instances**

Unmanaging Xen Hypervisor instance does not unmanage its CPU, Memory, and VM instances

SND-1039

**Resolution**

Unmanage each entity as a workaround.

## NSX discovery does not work in ESM server when server credentials are provided as hostnames

To observe the issue, start IP Manager and the ESM server. Enter the NVP and Openstack credentials as hostnames.

After discovery in IP, ESM does not discover the NSX component.

SND-479

### Resolution

Enter the credentials with the IP addresses.

## Veritas Clusters are not supported

Server Manager 9.3 does not support Veritas Clusters in the cluster management feature.

### Resolution

There is no resolution. This issue will be addressed in a future release.

## Bulk credential configuration for WMI Access is deprecated

Server Manager 9.3 no longer supports bulk credential configuration for Microsoft Windows Management Instrumentation.

### Resolution

There is no resolution.

## Credentials to vCenter may fail in ESM server if legacy MD2 encryption is in use on the vCenter server

ESM 9.3 uses JRE7 and connectivity to vCenter is failing.

This issue is due to the use of legacy MD2 encryption on the vCenter server side. Java version 7 has disabled MD2 on the client side due to identified security risks.

CQ 615855

### Resolution

There are two choices:

1. Upgrade the encryption algorithm which vCenter uses from the legacy MD2/MD5 encryption to RSA SHA1.
2. Edit the file, `/smarts/jre/lib/security`.
  - a. Search for the following text within the file:  
`jdk.certpath.disabledAlgorithms`
  - b. Comment out this line so it looks like this: `#`  
`jdk.certpath.disabledAlgorithms`
  - c. Save and close the file.
  - d. Restart the ESM server.

## Port and disk data is not synchronized for EMC M&R reports

In EMC M&R reports and views, the Server Manager data about the status of ports and disks may not be current.

Even though EMC M&R polls the device every five minutes, it may take one hour to update the reports and views. The same status is updated in the Server Manager without delay based on the polling interval in the Server Manager configuration.

CQ 654499

### Resolution

There is no resolution at this time.

## SNMP error messages in log files are not suppressed

SNMP error messages are flooding the log files when the SNMP Adapter (SNMPAdapter.c program) finds problems in received packets.

For example:

```
SNMP-E-AGENTERRORSTATS-Below message for SNMP agent at
'<ip_address:port>', was suppressed 0 times since The Epoch
```

CQ 616338

### Resolution

Use the `dmctl` command to increase the value for the `snmpLoggingThreshold` attribute in the `SM_System` class during runtime. This high-level setting is a throttling mechanism. Within the specified time period, only one error message is logged. By default, the value is 30 minutes. The acceptable value can range from 30 minutes to 1440 minutes (24 hours).

1. For example, log in to the Global Manager (INCHARGE-SA) with the `dmctl` command from `BASEDIR/smarts/bin` directory:

```
[root@<host> bin]# ./dmctl -b localhost:3333 -s INCHARGE-SA
Server INCHARGE-SA User: admin
admin's Password: XXXXXXXXXXXX
Domain Manager Control Program (V9.3.0.0) -- Type 'help' for a
list of commands.
Attached to 'INCHARGE-SA'
```

2. Locate the `SM_System` class attributes. Type: `dmctl> geti SM_System SM-System`
3. View the `SM_System` class attributes. Type: `dmctl> get SM_System::SM-System`

The result looks like:

```
Properties of SM_System::SM-System:
  CreationClassName = SM_System
  FIPS = FALSE
  Name = SM-System
  ServiceName =
  UseLowResTimer = FALSE
  brokerName = itops-qa-108.lss.emc.com:3333
  errLevel = Warning
  homedir = /opt/umesh/SAM_922/SAM/smarts
```

```

hostname = itops-qa-108.lss.emc.com
lockCheckAction = NONE
lockCheckActionCrash = 0
lockCheckActionNone = 0
lockCheckActionStacktrace = 0
lockCheckCycle = 60
lockCheckPeriod = 300
logLevel = Error
now = 1399446392
nowString = May 7, 2014 3:06:33 AM EDT
pid = 30257
serverName = INCHARGE-SA
serverPort = 0
snmpLoggingThreshold = 30
traceLevel = Fatal
uptime = 420532
uptimeString = 4 20:48:53

```

4. Increase the `snmpLoggingThreshold` attribute value. For example, set it to 300 minutes. Type: `dmctl> put SM_System::SM-System::snmpLoggingThreshold 300`

5. Verify the modified value. Type: `dmctl> get SM_System::SM-System`  
The result looks like:

```

Properties of SM_System::SM-System:
CreationClassName = SM_System
FIPS = FALSE
Name = SM-System
ServiceName =
UseLowResTimer = FALSE
brokerName = itops-qa-108.lss.emc.com:3333
errLevel = Warning
homedir = /opt/umesh/SAM_922/SAM/smarts
hostname = itops-qa-108.lss.emc.com
lockCheckAction = NONE
lockCheckActionCrash = 0
lockCheckActionNone = 0
lockCheckActionStacktrace = 0
lockCheckCycle = 60
lockCheckPeriod = 300
logLevel = Error
now = 1399446907
nowString = May 7, 2014 3:15:07 AM EDT
pid = 30257
serverName = INCHARGE-SA
serverPort = 0
snmpLoggingThreshold = 300
traceLevel = Fatal
uptime = 421047
uptimeString = 4 20:57:27

```

## VMAX and VNX RAID Group monitoring occurs in EMC M&R for only specific RAIDGROUP types

The Server Manager monitors every type of RAIDGROUP except for RAID groups that have unknown values for the `PoolName` and `PoolType` attributes.

EMC M&R monitoring of RAID groups occurs only when specific conditions are satisfied.

**Table 24** Conditions for EMC M&R monitoring of RAIDGROUP

RaidGroup Type	Status	FreeCapacity	ESM PoolName attribute value	EMC M&R Monitoring
VNX				
RAID Group	NO	YES	RAID Group	Status is not polled
PoolType attribute is Storage Pool	YES	YES	Storage Pool	YES
VMAX				
Disk Group	NO	NO	Unknown	Not Instrumented
PoolType attribute is Thin Pool	YES	YES	Storage Pool	YES, Instrumented/monitored

CQ 654254

**Resolution**

There is no resolution.

To troubleshoot, set the *EnableWANRAIDGroupMonitoringDebug* flag in the Server Manager to log messages for the EMC M&R RAIDGroup monitoring. Do a reconfiguration in Server Manager to make the setting effective. The *EMC Smarts Server Manager User and Configuration Guide* provides more troubleshooting information.

## Sticky applications are difficult to remove

After you modified an existing user-defined application template and removed some processes from the template, processes that you wanted to remove are still in the topology and associated with the host.

This issue occurs when you perform a rediscovery with **Topology > Discover All** in Server Manager.

CQ 616539

**Resolution**

Use one of these two resolutions:

- From the Domain Manager Administration Console
  1. Open the discovery filter for the application template in the Application Filters tab.
  2. Select the checkbox for Sticky Applications to remove the checkmark
  3. Click **Apply** to save the filter.
  4. Perform a rediscovery by selecting **TopologyDiscover All** in Server Manager to remove the processes from the topology and the host.
- From the Domain Manager Administration Console

1. Select `Configure Process Monitoring` and uncheck the processes that are no longer needed.
2. Modify the filter.
3. Rediscover the affected Host.
4. Click on a `Host` instance and navigate to `Host Services > SNMPAgent` in the tree.
5. Right-click on the `SNMPAgent` instance and select `Rediscover`.

## Duplicate FibreChannelSwitch instances appear in the topology

Duplicate FibreChannelSwitch instances appear in the Topology Browser attached to the Global Manager.

CQ 651410

### Resolution

The FibreChannelSwitch consolidation logic in Service Assurance Manager depends on the IPAddress attribute in the FibreChannelSwitch object in the Server Manager. If this attribute is not present or is incorrect, then duplicate instances are created because Service Assurance Manager is receiving instances from IP Manager and Server Manager with different IPAddress attribute information.

Use the Domain Manager Administration Console to examine the FibreChannelSwitch object in the Server Manager. Verify if the IPAddress attribute is present or if the value matches the corresponding value from the IP Manager. Correct the value if necessary and perform a rediscovery (Topology > Discover All) in Server Manager.

## Name of the Virtual Machine did not update from the ESM server

After a VM is renamed, the reconfigured VM event was triggered in the vCenter. But the ESM server did not show the new VM's name after polling.

CQ 609502

### Resolution

Rediscover the vCenter by performing a Discovery All from the ESM server.

## Synchronization issue between ESM server and network configuration

CQ 576667

ESM topology does not get updated and notifications in Global Console are not cleared when vCenter fails to generate events indicating the resolution of that condition. However, the notifications get cleared after rediscovery.

CQ 576651, CQ 576661, CQ 576637

### Related issues

When vCenter configuration options are changed, those changes are not detected until DiscoverAll is done.

Even after VMWareESX::Down clears VMwareDatastore::ConnectivityDown alerts, its impacts remain as active notifications. The other notifications that remain active are:

- VMWareESX::HostLostConnectionToAtLeastOneDatastore
- VMwareCluster::AutoVMotionCapabilityImpaired
- VMwareDatastore::NoAccess

When an ESX server is shutdown, the local datastore does not come up for very long. There is no associated event from vCenter and an immediate ESM DiscoverAll does not correct the situation.

## Isolated event generated when vCenter physical connections get disconnected

If the physical connections of a vCenter get disconnected, an isolated event `Interface::InterfaceLostConnection` is generated from the ESM Server, along with the expected events `Host::Down` and `Host::Unresponsive`.

CQ 577351

### Resolution

The isolated event `InterfaceLostConnection` will get cleared when `Host::Down` and `Host::Unresponsive` events clear.

## ESX server in the vCenter gets duplicated

Each ESX server in the vCenter gets duplicated with one having the vCenter with the IP as part of its name, and the other containing the vCenter DNS name.

This issue occurs after rediscovery of the ESX server. For example, if the vCenter is discovered as IP address 10.9.125.111 and the credentials for this vCenter use the DNS name of the vCenter, then ESM discovery of this vCenter will not occur.

CQ 576591 / CQ 575476

### Resolution

For ESM discovery of the vCenter to occur, use any one of the following combination:

- Either the IP address for the vCenter name in the topology and the credentials
- Or, the DNS name in the topology and the credentials

---

### Note

The name of the vCenter used for credentials must match the discovered instance name.

---

## JVM fails due to letter case mismatch of SM\_HOME and SM\_JAVAHOME

If the letter case of `SM_HOME` and `SM_JAVAHOME` values in Windows do not match, JVM fails to start and the vCenter credential check fails.

CQ 593531 / CQ 592473

### Resolution

In `runcmd_env.sh`, edit the value of `SM_HOME` or `SM_JAVAHOME` so that the letter case of `SM_JAVAHOME` and `SM_HOME` values are same.

## Installation/uninstallation issues

The following issues relate to the install or uninstall process.

### Server log errors encountered after 9.3 ESM upgrade from Version 9.x

After you upgrade a Server Manager from Version 9.x to Version 9.3 and start the Server Manager, the following error messages appear in the Server Manager log file.

The Server Manager log file is located in the `opt/InCharge/ESM/smarts/local/logs` directory.

```
[April 14, 2014 1:49:25 AM EDT +443ms] t@1148692800 InCharge Framework
MR-W-CLASS_NOTDEFINED-Class: 'ServiceProcess_Template_Setting' is no
longer defined in repos.
[April 14, 2014 1:49:25 AM EDT +444ms] t@1148692800 InCharge Framework
MR-W-CLASS_NOTDEFINED-Class: 'WMI_ThresholdSetting' is no longer
defined in repos.
[April 14, 2014 1:49:25 AM EDT +447ms] t@1148692800 InCharge Framework
MR-W-ATTRIBUTE_NOTDEFINED-'ESM_ProcessMonitoring_Setting::Type':
Attribute is no longer defined by class.
[April 14, 2014 1:49:25 AM EDT +447ms] t@1148692800 InCharge Framework
MR-W-
ATTRIBUTE_NOTDEFINED-'ESM_ProcessMonitoring_Setting::ParentSettingSele
ctors': Attribute is no longer defined by class.
[April 14, 2014 1:49:25 AM EDT +447ms] t@1148692800 InCharge Framework
MR-W-ATTRIBUTE_MISMATCH-'ESM_ProcessMonitoring_Setting::procTable':
Attribute was 'Struct_Set 11'. Now is 'Struct_Set 13'
[April 14, 2014 1:49:25 AM EDT +456ms] t@1148692800 InCharge Framework
ICF_MSG-*-ICF_RESTOREFINISH-PersistenceManager: restore finished
[April 14, 2014 1:49:25 AM EDT +457ms] t@1148692800 InCharge Framework
ICFM-E-ICF_EINIT-While initializing the InCharge application
ICF-ERESTOREREPOS-While attempting to restore topology from
file /opt/InCharge/ESM/smarts/local/repos/icf/INCHARGE-ESM.rps
MR-CANTCREATE_INSTANCE-'ServiceProcess_Template_Setting::SET-CFG-ESM
Process Monitoring Template/Process Monitoring Template/
ServiceProcess_Template_Setting' could not be created. ; in file "/
work/tancurrent/DMT-9.3.0.0/93/smarts/repos/mr/dyn_acc.c" at line 2958
MR-CLASS_NOT_FOUND-Class of given name
'ServiceProcess_Template_Setting' not found; in file "/work/
tancurrent/DMT-9.3.0.0/93/smarts/repos/mr/dyn_acc.c" at line 1746
```

CQ 611341

### Resolution

The error messages are benign in nature. They do not cause any impact on the functionality and can be ignored.

To suppress these messages, install the service for the Server Manager manually with the `--ignore-restore-errors` option and start the service. Consult the *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers* for instructions.

## ESM server generates shutdown core dump messages after unattended mode upgrade on Linux

On Linux, a 9.3 ESM server generates shutdown core dump messages after completing an upgrade in unattended (silent) mode.

SND-2691

### Resolution

The error messages are benign in nature. They do not cause any impact on the functionality and can be ignored.



# CHAPTER 5

## Multi-Protocol Label Switching Manager (MPLS)

This chapter includes the following topics:

- [Multi-Protocol Label Switching Manager overview](#) .....180
- [New features and changes in MPLS Manager](#) ..... 180
- [Fixed Issues in MPLS Manager](#) ..... 180
- [Known Problems in MPLS Manager](#) ..... 181

## Multi-Protocol Label Switching Manager overview

MPLS Manager monitors and analyzes Multi-Protocol Label Switching (MPLS) networks and provider-provisioned virtual private networks (VPNs) that are configured and provisioned over MPLS networks

## New features and changes in MPLS Manager

There are no new features in 9.6 release for MPLS Manager.

## Fixed Issues in MPLS Manager

Here are the fixed issues for MPLS Manager.

**Table 25** Fixed issues in MPLS Manager

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-9827 SR 08600633	The ingress LSP does not discover on Juniper ptx router.	The generic OID . 1.3.6.1.2.1.1.1 has been used to Juniper OS version.	9.4.2.X	9.5.1
IS-10434 SR 09597178	In MPLS 9.4.X, the LSPHops objects are not discovered.	The model function has been modified to create LSPHOP objects.	9.4.2.X	9.5.1
IS-8376 SR 85478892	FALSE MTUMismatch alert appears because the IOS device do not add Layer 2 header in MTU.	The dxa, model files, and ASL files has been modified to add correct Layer 2 header size to the MTU on IOS devices before comparing.	9.4	9.5
IS-8226 SR 6628250	Parsing issue occurs when the SNMP agent returns empty VRF name.	The asl file has been modified to handle and ignore the empty VRF name.	9.4.2.X	9.5
IS-5652 76827676	Performance issue occurs.	A check has been introduced to check if the in and out ports in routing table are same to terminate the	9.4.0.X	9.5

**Table 25** Fixed issues in MPLS Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		while loop so that MPLS server does not go into infinite loop		
Fixed problems in 9.4.2				
IS-5409 SR 76827676	Performance issue about memory used by the MPLS topology server.	A condition/ check has been introduced to avoid a looping problem during routing table entry traversal and this in turn fixed the MPLS crash issue.	9.4.0.x	9.4.2

## Known Problems in MPLS Manager

The following issues apply to MPLS Manager, and to the functionality that is provided by the IP Availability Manager and Global Manager applications in an MPLS Manager deployment.

### ASL errors appear in the MPLS Manager log file during discovery

The following ASL errors appear in the MPLS Manager log file during discovery:

```
ASL-W-EERROR RULE SOURCE-While executing rule set '/opt/InCharge/
MPLS/smarts/rules/mpls-tma/ic-mpls-ldp-juniper-mpls-ldp-mib.asl'
ASL-EERROR ACTION-While executing action at:
ASL-CALL_STACK_RULE- RuleName: POST_PROCESS, Line: 248
ASL-CALL_STACK_RULE- RuleName: EOF, Line: 291
ASL-EERROR INVOKE-While attempting to invoke operation
'getInterface' of object 'IP::IP-146.172.96.19'
MR2-MR_WHILE_OPERATION_INVOKE-While invoking operation getInterface
in object 'IP::IP-146.172.96.19'
MR-OP_THREW-Calling operation getInterface: caught CI_Exception; in
file "MSI_Topology.c" at line 31986
MR-EINTERNAL-REPOS Internal Error; in file "MSI_Topology.c" at line
31957
MR-NON_SINGLETON_SET-Set operation produced a set which is not a
singleton
```

SND-2609

#### Resolution

There is no resolution.

## EMC Smarts Adapter for Cisco ISC is listed in the Uninstallation dialog box

In the Uninstallation dialog box, the ISC Adapter is still listed as a feature.

CQ 653588

### Resolution

There is no resolution for this issue.

## SSH - CLI discovery was not happening on Windows platform

SSH was not working on Windows platform because the Net SSH with Cisco devices accept only one command per session. Hence SSH could not be supported on Windows platform.

CQ 644822

### Resolution

There is no resolution for this issue.

## sm\_stats --show-dm-processes throw an ASL error

sm\_stats --show-dm-processes throws an ASL error.

### Example

```
st:4244 --show-dm-processes
discovery/ic-stats.asl: Last Consistency Phase One Update = 0
discovery/ic-stats.asl: Last Offline Consistency Update = 0
discovery/ic-stats.asl: Last Consistency Update = 0
discovery/ic-stats.asl:
discovery/ic-stats.asl: Last Offline Codebook Computation = 0
discovery/ic-stats.asl: Last Codebook Computation = 0
discovery/ic-stats.asl:
discovery/ic-stats.asl: Last Correlation = 0
discovery/ic-stats.asl:
discovery/ic-stats.asl: codebookRadius = -1
discovery/ic-stats.asl: correlationInterval = 30
discovery/ic-stats.asl: correlationRadius = 4
---
---
---ASL-W-E-R-R-O-R R-U-L-E _S-O-U-R-C-E-While executing rule set 'C:
\InCharge921\MPLS\smarts\rul
es\discovery\ic-stats.asl'
ASL-E-R-R-O-R _A-C-T-I-O-N-While executing action at:
ASL-C-A-L-L _S-T-A-C-K _R-U-L-E- RuleName: SNMP_ACCESSOR_INTERFACE, Line: 1332
ASL-C-A-L-L _S-T-A-C-K _R-U-L-E- RuleName: SHOW_DM_PROCESSES, Line: 1209
ASL-C-A-L-L _S-T-A-C-K _R-U-L-E- RuleName: START, Line: 120
ASL-E-R-R-O-R _U-N-D-E-F-I-N-E-D _T-A-B-L-E _K-E-Y _A-C-C-E-S-S to access undefined
key '0' in t
able '...'
ASL-B-A-D _H-A-S-H _T-A-B-L-E _I-N-D-E-X-The index '0' is out of bounds
```

### Resolution

For polling, <MPLS-MONITORING> server is used. Errors may appear if the command is executed against the TOPOLOGY server since the class, SNMP\_ACCESSOR\_INTERFACE, is not part of topology but of monitoring.

Run the sm\_stats command with the MONITORING server for show-dm-process. (Provide the monitoring server name instead of the topology server.)

## Remote ping server tools are available to unintended object types

In the Notification Log Console, the remote ping server tools should be available only to MPLS router, switch, or VRF objects.

Remote ping server tools are not only available to these object types, but are also available to other object types.

CQ 214132

### Resolution

In the Notification Log Console, invoke the remote ping server tools only for MPLS router, switch, or VRF objects.

## MPLS VPN maps do not increment and decrement hops

The Increment Hops and Decrement Hops options do not work for MPLS VPN maps, even though expandable nodes appear in the maps. An expandable node is marked with a plus (+) sign.

CQ 236322

### Resolution

In an MPLS VPN map, select the expandable node that you wish to expand and use the "Expand Map Element" option in the Global Console. To select multiple expandable nodes, select the nodes while holding down the Ctrl key.

## Unable to unmanage LSP objects

When you right click an LSP object in the topology tree of a Global Console that is attached to the MPLS Topology Server, the Unmanage option does not appear in the pop-up menu.

You cannot unmanage an LSP object.

CQ 303190

### Resolution

No resolution is available at this time.

## Error if special characters are included in a server's name in the startup command line

In a startup command line for an MPLS Manager component server, you cannot include special characters in the server's name unless you enclose the whole name in double quotation marks.

CQ 304721

### Resolution

For any server's name that includes special characters, enclose the whole name in double quotation marks. For example: `/opt/InCharge/MPLS/smarts/bin> ./sm_server -n "ICMMS*() []MPLS-TOPOLOGY" -c mpls-t --output --daemon --norestore`

## Unable to determine which IP belongs to a logical router

Logical routers are not supported by MPLS Manager, though physical routers that host logical routers are supported.

Because no LSPID information is available for a logical router in the host router's MIB, MPLS Manager has no way of knowing for certain which IP belongs to which logical router. MPLS Manager selects the first /32 loopback address in the SNMP Agent as the LSPID. Accordingly, MPLS Manager might choose the wrong LSPID for an LSP that ends at a logical router.

CQ 330885

### Resolution

No resolution is available at this time.

## Discovery settings are not preserved in the MPLS Topology Server's repository file

Not all discovery settings are restored from the MPLS Topology Server's repository file when the server is restarted, including the settings for scheduled full discovery and scheduled pending discovery.

These settings are available on the Discovery tab of a Domain Manager Administration Console that is attached to the MPLS Topology Server:

- Scheduled full discovery is available through the "Enable Full Discovery" checkbox.
  - Scheduled pending discovery is available through the "Enable Discovery Pending" checkbox.
- Other discovery settings that might be missing are the "lastUpdated" times for various discovery probes (discover-all, pending). These settings are reset to a default value.

CQ 359342

### Resolution

To run the discover-all probe in the MPLS Topology Server, configure scheduled full discovery, or invoke a manual full discovery, at one or more of the source IP Availability Managers. Doing so will trigger full discovery in the MPLS Topology Server.

To run the pending probe in the MPLS Topology Server, reconfigure scheduled pending discovery, or invoke a manual pending discovery, at the MPLS Topology Server.

## Service for the MPLS VPN-Tagging Server should not include `--subscribe`

When installing the MPLS VPN-Tagging Server as a service, the service for the server includes the `--subscribe` option. The service should not include the `--subscribe` option.

CQ 360247

### Resolution

As a workaround, edit the service for the MPLS VPN-Tagging Server and remove the `--subscribe` option.

## Device Certification tab appears on the Polling and Thresholds Console

When the MPLS Topology Server is first started, and assuming a valid EMC Smarts Adapter for Alcatel-Lucent 5620 SAM EMS (the Adapter) license is present, the Certification and Polling tabs appears in the Polling and Thresholds Console, when only the Polling tab should appear.

CQ 378805

### Resolution

No resolution is available at this time. Processing between the Adapter and MPLS Manager requires the exchange of parameters that, in the current MPLS Manager architecture, can only be accomplished when the Certification tab is enabled.

## Not all LdpProtocolEndpoints and LdpAdjacencies are discovered for Cisco IOS devices

MPLS Manager uses the MPLS-LDP-MIB to discover targeted and non-targeted LDP sessions on Cisco IOS devices. MPLS Manager sometimes obtains incomplete MIB information about LDP sessions from the Cisco IOS devices.

As a result, MPLS Manager sometimes does not discover all the LdpProtocolEndpoint and LdpAdjacency instances for the LDP sessions that are implemented on the managed Cisco IOS devices.

This issue affects MPLS Manager's ability to discover LSP sessions that are built on Cisco IOS devices.

CQ 463493

### Resolution

No resolution is available at this time.

## BGPProtocolEndpoint is not discovered on Cisco routers if BGP is enabled only on VRF

On a Cisco router, if BGP is enabled on a VRF but not enabled globally, MPLS Manager does not discover the BGPProtocolEndpoint that is associated with the VRF.

This behavior occurs because the BGPPeerTable (.1.3.6.1.2.1.15.3) on a Cisco router is not populated due to Cisco bug CSCso90107.

This causes these problems:

- IP Availability Manager does not identify the router as a BGP-enabled device.
- MPLS Manager does not import the router from IP Availability Manager and thus does not discover the BGPProtocolEndpoint.

This issue impacts BGPSession discovery: MPLS Manager creates a one-way adjacency (half link) to the Cisco router instead of a two-way adjacency (full link), even though the Cisco router and the router to which the BGPSession connects are both in IP Availability Manager's repository. This issue impacts Network Protocol Manager for BGP in the same way: Network Protocol Manager for BGP creates a half link to the Cisco router instead of a full link.

CQ 502060

**Resolution**

Contact Cisco Support to obtain the correct patch for your device. After this upgrade, the BGPPeerTable should be populated for the device where BGP is enabled at the VRF level.

## **Changes in RemoteAS value are not updated in the MPLS Topology Server**

The BGPProtocolEndpoint's RemoteAS attribute is updated in the MPLS Topology Server only during discovery.

In Network Protocol Manager for BGP, this value is instrumented and therefore is updated more frequently.

CQ 502542

**Resolution**

When a BGPProtocolEndpoint RemoteASMismatch notification is generated by MPLS Manager, refer to Network Protocol Manager for BGP for the correct value of RemoteAS and ignore the value in the MPLS Topology Server.

## **Discover All in IP Availability Manager is not triggering discovery in BGP Manager**

The Discover All action in IP Availability Manager is not triggering discovery in Network Protocol Manager for BGP, which leads to inconsistencies in the reported BGP topology between the MPLS and BGP Managers.

CQ 502740

**Resolution**

Perform a Discover All in Network Protocol Manager for BGP each time Discover All or rediscovery is triggered in IP Availability Manager. Otherwise, topology inconsistencies will occur between the MPLS and BGP Managers.

## **BGP object monitoring is disabled if the BGP Manager shuts down**

The MPLS Monitoring Server is not able to monitor a BGP object's status attributes in the source Network Protocol Manager for BGP when either of the following occurs:

- The BGP object is not discovered by Network Protocol Manager for BGP.
  - Network Protocol Manager for BGP shuts down or is not found by the MPLS Topology Server.
- In addition, the status attributes are not repopulated in the MPLS Monitoring Server when either of the following occurs:

- The BGP object is discovered later by Network Protocol Manager for BGP.
- Network Protocol Manager for BGP starts up again.

CQ 502937

**Resolution**

Perform a full discovery in the MPLS Topology Server in order to repopulate the status attributes.

## MPLS server tools cannot be imported by using the Import XML Configuration server tool

The MPLS remote ping and LSP ping server tools cannot be imported by using the Import XML Configuration server tool in the Topology Browser Console.

CQ 503097

### Resolution

This problem occurs because the server tool scripts point to .sh files instead of .cmd files. Either use the sm\_config utility to load the XML files or modify the “Import XML Configuration” and “Import XML Domain Configuration” server tools in the Global Manager Admin Console to point to the .cmd scripts.

Here are examples for using the sm\_config utility to load the XML definition or configuration files:

- To load the XML definition file for the LSP ping server tool:  
Go to the BASEDIR/smarts/bin directory in the Global Manager installation area and enter the following command on one line: `sm_config -s <Global Manager instance name> import --force lsp-ping-action.xml`  
  
For example, for LSP ping, enter the following: `sm_config -s INCHARGE-SA import --force lsp-ping-action.xml`
- To load the XML definition file for the remote ping server tool, enter the following:  
`sm_config -s INCHARGE-SA import --force mpls-action-config.xml`  
The *EMC Smarts Service Assurance Manager Configuration Guide* provides more information.

## Cannot monitor the status of TE LSPs on Cisco IOX devices

For Cisco IOS XR devices, MPLS Manager uses the MPLS-TE-STD-MIB to discover and monitor TE tunnel objects, and uses CLI to associate the primary TE LSPs with their backup/secondary TE LSPs.

Because of what appears to be an SNMP-agent bug on Cisco IOS XR devices, MPLS Manager cannot obtain status for the TE LSPs from the Cisco IOS XR devices.

Because the response from the SNMP agent is in violation of the SNMP protocol, MPLS Manager ignores the response and thus fails to obtain a value for the mplsTunnelOperStatus MIB object. When no status is obtained for this MIB object, MPLS Manager sets the LSP status to unknown.

This issue affects MPLS Manager’s ability to monitor the status of TE LSPs that are built on Cisco IOS XR devices.

CQ 515819

### Resolution

No resolution is available at this time. This issue pertains to Cisco TAC case CSCsz85420: No SNMP response when polling CRS-1.

## LSP ping requests on Cisco devices return a “QQQQQ” status

When executing LSP ping requests on Cisco devices, a return of “QQQQQ” indicates that the source device on which the LSP request is invoked could not send an echo request packet on the LSP to the destination device.

The reason for the failure could be one of many, including an incorrect value for the LSPId attribute of the LSP object.

---

### Note

LSP ping is applicable to LDP-signaled LSPs but not to RSVP-signaled LSPs. By default, MPLS Manager uses SNMP to discover Cisco LSPs, and if that discovery fails, uses CLI to discover Cisco LSPs. The advantage of SNMP-discovered LSPs is that MPLS Manager can better correlate the LSPs with the SNMP-discovered L2VPNs and the SNMP-discovered PseudoWires.

The disadvantage of SNMP-discovered LSPs is that the LSP-ID information for the LSPs is not available through SNMP discovery (but is available through CLI discovery). In an attempt to derive the LSP-ID for an SNMP-discovered LSP, MPLS Manager populates the LSPId attribute of the LSP object with the loopback IP address of the LSP’s destination device, which is not always the correct LSP-ID for the LSP.

An incorrect LSP-ID for an LSP will cause an LSP ping request on the LSP to fail.

CQ 556471

---

### Resolution

No resolution is available at this time. EMC continues to investigate this issue.

As a workaround:

1. To skip the SNMP discovery of Cisco LSPs, use the `sm_edit` utility to open the `mpls.conf` file and set the `LsRMIBUseFilter` parameter to `""`. For example, `LsRMIBUseFilter=""`
2. Restart MPLS Manager to initiate a full discover. MPLS Manager reads the `mpls.conf` file and uses CLI to rediscover the Cisco LSPs and assign correct LSP-IDs to the LSPs.
3. Execute LSP ping on the Cisco LSPs.

## MPLS Manager is generating false PseudoWire::Impacted events

MPLS Manager is generating PseudoWire::Impacted events for underlying Interfaces that MPLS Manager perceives to be disabled but are, in fact, operational (up).

Either MPLS Manager is receiving false Interface topology from its IP Availability Manager sources or MPLS Manager is constructing a false path from the Interface objects to the PseudoWire objects.

Here is the path that MPLS Manager constructs between a PseudoWire object and an underlying Interface object: **Pseudowire > LayeredOver > LdpAdjacency > LDPProtocolEndpoint > LayeredOver > Interface**

This results in **Pseudowire > LayeredOver > LdpAdjacency > LayeredOver > Interface**

From the LayeredOver relationships, the PseudoWire becomes impaired by the disabled Interface.

The actual declaration that the PseudoWire is impacted by the underlying disabled Interface is completed by the Global Manager. First, the Global Manager examines the following problems and events to learn the explanation chain:

- The Interface::Disabled problem that is exported by IP Availability Manager to the Global Manager and MPLS Manager.
- The Interface::Disabled problem that is exported by MPLS Manager to the Global Manager.
- The PseudoWire::Impacted event that is exported by MPLS Manager to the Global Manager.

Then, the Global Manager combines the Interface::Disabled problems from IP Availability Manager and MPLS Manager to form one notification that has two sources. And lastly, the Global Manager associates the PseudoWire::Impacted event notification as an impact of the Interface::Disabled problem notification.

CQ 566989

#### **Resolution**

No resolution is available at this time.

## **VRF LSP Ping All does not work as intended**

When viewing a notification by using the VRF LSP Ping All server tool, you see LSP Ping is not applicable to the VRF-GOLD/dev-Vpls9: no lsp is found, however the VRF has LSPs.

CQ 581704

#### **Resolution**

No user action is required. The software is working as designed. The relationship between LSP and VRF has been removed in order to support multicast. LSP ping functionality through the VRF notification is redundant because VRF and LSP do not impact each other.

## **LSP map is displayed when selecting LSP Hops map for a VPN object**

In the Map Console, when right-clicking a VPN object and selecting LSP Hops in the pop-up menu, the LSP map is displayed instead of the LSP Hops map.

The LSP map shows the originating (source) and terminating (destination) devices for the LayeredOver LSPs, whereas the LSP Hops map not only shows the originating and terminating devices for the LSPs but also shows all of the transit devices for the LSPs.

CQ 576830

#### **Resolution**

This issue will be addressed in a future release. As a workaround, in the opened topology map for a VPN object, right-click each LSP and select **LSP Hops** in the pop-up menu to view the LSP hops for the LSP.



# CHAPTER 6

## Network Protocol Manager (NPM)

This chapter includes the following topics:

- [Network Protocol Manager overview](#)..... 192
- [New features and changes in Network Protocol Manager](#)..... 192
- [Fixed Issues in Network Protocol Manager](#)..... 193
- [Known Problems in Network Protocol Manager](#).....201

## Network Protocol Manager overview

The Network Protocol Manager discovers and monitors devices that are running any of the following routing-protocol services:

- Border Gateway Protocol (BGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Intermediate System to Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)

The Network Protocol Manager consists of the following components:

- Network Protocol Manager for BGP
- Network Protocol Manager for EIGRP
- Network Protocol Manager for IS-IS
- Network Protocol Manager for OSPF

Separate instances of Network Protocol Manager are required to manage the availability of each routing protocol: one each for BGP, EIGRP, IS-IS, and OSPF.

## New features and changes in Network Protocol Manager

Here are new features and changes for version 9.6:

- Smarts NPM BGP is enhanced to support 32-bit AS number.

---

### Note

When the autonomous system is beyond the range that is 2147483647, NPM is discovered with incomplete Topology.

---

## Configuring the monitoring of VRF based EIGRP sessions

For Network Protocol Manager for EIGRP, you can configure the monitoring of VRF based EIGRP sessions.

To configure the monitoring of VRF based EIGRP sessions, set the following parameters to TRUE for your EIGRP-Adapter\_Manager instance.

### Procedure

1. Use `sm_edit` to open the `<BASEDIR>/smarts/local/integration/eigrp/ic-eigrp-instrument.pl` file.
2. Change the default values from False to True (1) for the following:

```
my $vrfFlag = 1;
my $pagingFlag = 1;
```

- The `$vrfFlag` parameter is the `VRFEnabled` attribute which enables you to monitor the VRF based EIGRP sessions.
- The `$pagingFlag` parameter is the `PagingEnabled` attribute which enables paging if you know the device output performance is going to be large.

3. Save and exit the file. You do not have to restart the Network Configuration Manager.

## Enabling OSPF STUB area discovery

For Network Protocol Manager for OSPF, you can configure whether multiple STUB areas with the same area identifier (ID) are uniquely identified during the discovery process.

When the `EnableOSPFStubAreaDiscovery` parameter is set to `TRUE`, each connected device in the stub area is discovered and a separate stub area for each group of connected devices is created. The stub area is uniquely identified by an Integer stub area ID.

---

### Note

This feature does not probe any additional information via CLI/SNMP from the device.

---

### Procedure

1. From the `<BASEDIR>/smarts/bin` directory, open the `ospf.conf` file. For example in Linux, type this command:

```
sm_edit /opt/InCharge/NPM/smarts/conf/ospf/ospf.conf
```

2. Set `EnableOSPFStubAreaDiscovery = TRUE`.
3. Save and exit the file.
4. Restart the Network Protocol Manager for OSPF by typing from the `BASEDIR/smarts/bin` directory:

```
sm_service stop ic-npm-ospf-server
sm_service start ic-npm-ospf-server
```

5. Perform a full discovery (Discover All).

Consult the *EMC Smarts Network Protocol Manager Discovery Guide* for complete discovery information.

## Fixed Issues in Network Protocol Manager

Here are the fixed issues for Network Protocol Manager.

**Table 26** Fixed issues in Network Protocol Manager

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-11430 SR 10988121	BGP creates tagged/ untagged bgp endpoint. The instance name toggles between	Code has been modified so that an MSI_Manager flag <code>DisableBGPTagging</code> disables the	9.4.2	9.6

**Table 26** Fixed issues in Network Protocol Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
	discoveries from tagged and untagged and vice versa.	use of IP tags in the naming of BGPProtocolEndpoint, which in turn removes the tag in the BGPSession name.		
IS-11066 SR 10473520	The ISIS Neighbor is down between two devices, however, the user did not receive any alert for the same in Smarts.	The modified rules have been added to handle the cleanup topology properly.	9.4.1.X	9.5.1
IS-8763 SR 07448078	The BGP session Down alert is cleared falsely.	The device was deleting the SNMP MIB entries of BGP peer state and recreating repeatedly. When the SNMP instrumentation gets error, it was causing the alert to clear. The model code has been modified to handle the SNMP error.	9.4.2	9.5.1
IS-10202 SR 89801544	The OSPF object exists, even if the device is deleted in the IP.	The ASL rules have been added to cleanup topology.	9.4.2	9.5.1
IS-8861 SR 86814428	The OSPF alerts are not generated when an interface goes down.	The referred interface on the device is Aggregate interface, however there was no support of Aggregate interface in OSPF. The Aggregate	9.4.1	9.5.1

**Table 26** Fixed issues in Network Protocol Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
		interface support has been added on OSPF.		
IS-9490 SR 08067260	The OSPF traps are not created as notifications.	The AS rule has been modified to process the trap.	9.4	9.5.1
IS-8485	The Aggregate interfaces were not supported for the ISIS.	Current NPM implementation does not have support for the class Aggregate interface. A new class Aggregate interface has been added into NPM.	9.4.2	9.5.1
IS-9824 SR 07732078	The multiple invalid BGP Session Down notifications occur from a BGP connection.	The false BGP alerts occur due to SNMP errors. The model code has been modified to handle SNMP errors in instrumentation.	9.4.2	9.5.1
IS-9826 SR 08779211	The false BGP notifications occur.	The false BGP notifications occur because the extra unused BGP autonomous system objects cause to break post processing and incomplete topology creation. The ASL rule has been added to clean up the extra unused BGP autonomous system objects in discovery.	9.4.2.X	9.5.1
IS-8376 SR 85478892	FALSE MTUMisMatch alert appears because the IOS	The dxa, model files, and ASL files have been modified to add	9.4	9.5

**Table 26** Fixed issues in Network Protocol Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	device do not add Layer 2 header in MTU.	correct Layer 2 header size to the MTU on IOS devices before comparing.		
IS-8226 SR 6628250	Parsing issue occurs when the SNMP agent returns empty VRF name.	The asl file has been modified to handle and ignore the empty VRF name.	9.4.2.X	9.5
IS-8336 SR 82414920	The OSPF interface events are not generated at endpoint.	Changes has been done to handle SNMP error conditions properly. Like in this case, snmp oid poll throws errors when the interfaces is disabled and NPM generates unnecessary alarm based on this error condition. Same has been handled with this fix.	9.4.0.11	9.5
ER 505 SR 81639594, 83457748	VRF BGP/OSPF sessions are not discovered and monitored.	In order to enable this feature, set the VRFEnabled flag to TRUE (by default it is FALSE) for BGP and OSPF in the respective files given below:  BGP : <smarts>/conf/bgp/bgp.conf  OSPF : <smarts>/conf/ospf/ospf.conf  Also, In GUI VRFEnabled attribute is introduced in		9.5

**Table 26** Fixed issues in Network Protocol Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
		MSI_AdapterMa nager class.  Note: You must install IP 9.4.2 Patch 4 before using this feature.		
IS-6828 SR 80425716	BGP is shutting down abruptly (with core dump) due to FD growth.	Changes has been made to handle exception when a device with SNMP V3 does not have a username.	9.2.1.X	9.5
IS-7314 SR 04845027	BGP Peer sessions with Peer ID 0.0.0.0 were not being discovered.	Made a configurable feature to enable users to set flag DiscoverBGPSes sionWithout- PeerID to True in <smarts>/bgp/ bgp.conf file.	9.3.0.18	9.5
IS-7272 SR 81991444	BGP Session Flapping event was not being generated when trap received.	Code added to handle trap count for each trap received.	9.3.0.10	9.5
IS-7511 SR 82414920	The OSPF interface events are not generated at endpoint.	Changes has been done to handle SNMP error conditions properly. Like in this case, snmp oid poll will throw errors when the interfaces is disabled and NPM generates unnecessary alarm based on this error condition.	9.4.0.11	9.5
IS-6697 SR 79973134	The ISIS Manager does not create end	The History table has been implemented for ISIS interfaces.	9.4.1.X	9.5

**Table 26** Fixed issues in Network Protocol Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
	points for two CISCO devices.			
IS-7305 SR 80425716	BGP shuts down abruptly.	Added check to cleanup memory when SNMP v3 user name is missing	9.2.1.X	9.5
IS-5265 SR 75570446	EBGP session configured on IPv6 is not discovered.	Certified CISCO-BGP-4 and JUNIPER-BGP-4 MIBs to support SNMP	9.4.0.11	9.5
IS-5111 SR 74746918	ISIS Interface disabled alerts received when the device doesn't have any ISIS configuration.	Consolidated the history table for ISISInterface creation.	9.3.0.0	9.5
IS-5592 SR 75570446	EBGP session configured on IPv6 is not discovered.	Certified CISCO-BGP-4 and JUNIPER-BGP-4 MIBs to support SNMP discovery for IPv6.	9.4.0.11	9.5
IS-5429 SR 75856922	CLI access not found.	Fixed wrong setting key for instrumentation classes.	9.4.1	9.5
IS-7370 SR 81991444	When Smarts NPM BGP session IsFlapping is created, the notification is not created by single trap.	Two attributes are introduced in MSI_AdapterManager class. For EIGRP domain, these attributes are visible on EIGRP-Adapter-Manager instance.	9.3.0.10	9.5
Fixed problems in 9.4.2				
IS-6687, SR 72313228	VRF EIGRP sessions are not discovered and monitored.	Enhanced Network Configuration Manager to discover and monitor VRF	9.4.1	9.4.2

**Table 26** Fixed issues in Network Protocol Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
		<p>based EIGRP sessions.</p> <p>Modified files (all files in &lt;BASEDIR&gt;/smarts/local/) are:</p> <p>actions/eigrp/ic-eigrp-create.pl integration/eigrp/ic-eigrp-instrument.pl</p> <p>Modified the EIGRP-Adapter_Manager class to include two new attributes, PagingEnabled and VRFEnabled.</p>		
IS-6211, SR 72313228	Cisco ASA/PIX firewalls are not discovered and monitored for EIGRP.	<p>Enhanced Network Configuration Manager to discover and monitor Cisco ASA/PIX firewalls for EIGRP.</p> <p>Modified files (all files in &lt;BASEDIR&gt;/smarts/local/) are:</p> <p>actions/eigrp/ic-eigrp-create.pl integration/eigrp/ic-eigrp-instrument.pl</p>	9.4.0.X	9.4.2

**Table 26** Fixed issues in Network Protocol Manager (continued)

<b>CQ/SR/Issue number</b>	<b>Problem summary</b>	<b>Description of fix</b>	<b>Found in version</b>	<b>Fixed in version</b>
IS-5265 SR 75570446	EBGP session configured on IPv6 not discovered.	Implemented consolidated history table which resolved the issues between CLI and SNMP Discovery.	9.4.0.X	9.4.2
IS-5111 SR 74746918	ISISInterface Disabled alerts received when the device doesn't have any ISIS configuration.	Added GA_StringDictionary to handle ISIS Eps and interfaces history table which resolved handling of ISIS Eps and Interfaces.	9.3.0.X	9.4.2
IS-2561 SR 75517670	NPM domains cannot update the RPS file.	The domain manager boot code is modified to avoid inheriting the files to child process sm_authority.	9.2.2.x	9.4.2
SND-359	The IsIPv6 attribute is set to TRUE for instances of dual stack devices whose NeighborIpAddress is IPv4. For example, the ISISNeighborEndpoint instance with NeighborIpAddress IPv4 has the IsIPv6 attribute set to TRUE.	Changed the logic to identify the Ipv6 ISISNeighborEndpoint based on neighbor IP address type. Modified file:  <smarts>/rules/isis/ic-isis-ipv6.asl	9.3	9.4

## Known Problems in Network Protocol Manager

The following issues apply to Network Protocol Manager and to the functionality that is provided by the IP Availability Manager and Global Manager applications in a Network Protocol Manager deployment.

### Devices use incorrect access credentials from multiple IP Managers in NPM CLI discovery

For NPM CLI discovery, when the IP Availability Manager and the combined IP Availability and Performance Manager are both running, some devices from the IP Availability and Performance Manager use the device access credentials from the IP Availability Manager.

For example, in the NPM log file, the following error messages appear:

```
[Mon Dec 8 08:06:20 2014]
Encountered Problem on login to '10.9.7.5'.
  Perhaps the AccessId 'cisco' or the AccessCode is incorrect!
  Got Error: login failed: bad name or password at /opt/InCharge/NPM/
smarts/perl/5.16.2/SMARTS/CLI/Remote/Telnet.pm line 287
  at /opt/InCharge/NPM/smarts/perl/5.16.2/SMARTS/CLI/Discovery.pm line
350.
```

10.9.7.5 is a router discovered in AM-PM and it has to use AM-PM device access credentials, but the router uses the AM device access credential "cisco".

SND-1667

#### Resolution

The workaround is to create multiple CLI setting groups with criteria that is specific for the IP Manager. For example, to ensure access credentials of both AM and AM-PM servers are loaded into the NPM for BGP server, define a new CLI\_Access setting group in one of the IP Managers and use a different criteria. In this example, the IP Availability Manager uses the default setting and the combined IP Availability and Performance Manager uses a new group called "AMPM-matching criteria" that uses SNMP address.

### Errors appear in the Discovery Progress window for IPv6 devices

CLI discovery errors appear in the Discovery Progress window for IPv6 devices.

CQ 654440

#### Resolution

Perform a Discover All from the IP Availability Manager server after topology synchronization and the errors no longer appear.

### Unnecessary error message during startup of any Network Protocol Manager on Linux

During startup of any Network Protocol Manager that is running on Linux, the following error message is written to the log file.

```
CI-E-EWHILE-While executing function "doOpen"
```

CQ 422535

### **Resolution**

Ignore this message. No user action is required.

## **IP Manager populates SNMPAgents with incorrect attribute values**

An initial V3 discovery of an SNMPv3/v2c device was performed in the source IP Availability Manager, followed by a V2C discovery of the device in the source IP Availability Manager.

After the SNMPv3 discovery, the following attribute values were populated for the device's SNMPAgent:

- AuthProtocol=MD5 or SHA
- AuthPass = <encrypted authentication password>
- PrivProtocol=DES or AES
- PrivPass=<encrypted privacy password>
- SNMPVersion=V3

After the SNMPv2C discovery, the following attribute values were populated for the device's SNMPAgent:

- AuthProtocol=MD5 or SHA
- AuthPass = <encrypted authentication password>
- PrivProtocol=DES or AES
- PrivPass=<encrypted privacy password>
- SNMPVersion=V2C

The following attribute values were expected:

- AuthProtocol=<empty>
- AuthPass = <empty>
- PrivProtocol=<empty>
- PrivPass=<empty>
- SNMPVersion=V2C

CQ 421888

### **Resolution**

This issue is specific to IP Availability Manager. It will be fixed in a planned, upcoming patch or release.

## **Relationships are removed in Network Protocol Manager after tagging IPs in IP Availability Manager**

Relationships are removed after tagging IPs in IP Availability Manager.

CQ 574846

### **Resolution**

Delete the device that has tagging from the NPM topology, then do a discover all.

## **Network Protocol Manager for BGP issues**

These problems affect Network Protocol Manager for BGP.

## Limited notifications for Cisco BGP-enabled devices in IPv6 network

In Network Protocol Manager for BGP, the range of notifications for Cisco BGP-enabled devices in IPv6 network is limited.

This is because the discovery and monitoring mechanism of Cisco BGP-enabled devices is CLI-based and not based on SNMP polling and MIB values.

**Table 27** Notifications for Cisco BGP-enabled devices in IPv6 network

Managed objects	Notifications
BGPProtocolEndPoint	IBGPPeerMissing
BGPSession	Disconnected
	Down
BGPService	Down

CQ 577037

This section lists the Cisco IPv4 notifications that cannot be generated in IPv6.

- For BGPService in IPv6:
  - IPBGPeerMissing
  - IBGPPeerMissingEvent
  - RemoteAsMismatch
  - RemoteASMismatchEvent
  - RemoteSpeakerEvent
  - RemoteSpeakerNotConfigured
  - RemoteSystemNotRunningBGP
  - RemoteSystemNotRunningBGPEvent
- For BGPSession in IPv6:
  - Flapping
  - PreFixThresholdCrossed

## Unnecessary stack trace messages during startup/shutdown of BGP Manager on Windows

During startup and shutdown of a Network Protocol Manager for BGP that is running on Windows, stack trace messages are written to the log file.

CQ 422336

### Resolution

Ignore this message. No user action is required.

## Unnecessary error message during shutdown of BGP Manager

During shutdown of a Network Protocol Manager for BGP, multiple instances of the following error message are written to the log file:

```
WARNING ESRVTHEXCEPTION-Service thread closure for queue IA-Poller
polling
```

CQ 422535

### **Resolution**

Ignore this message. No user action is required.

## **Missing class in dynamic model causes BGP Manager to core dump on boot**

Network Protocol Manager for BGP core dumps on boot when a class defined in dynamic model does not exist.

CQ 495024

### **Resolution**

There is no workaround at this time.

## **BGPProtocolEndpoint is not discovered on Cisco routers if BGP is enabled only on VRF**

On a Cisco router, if BGP is enabled on a VRF but not enabled globally, Network Protocol Manager for BGP does not discover the BGPProtocolEndpoint that is associated with the VRF.

This behavior occurs because the BGPPeerTable (.1.3.6.1.2.1.15.3) on a Cisco router is not populated due to Cisco bug CSCso90107.

This causes these problems:

- IP Availability Manager does not identify the router as a BGP-enabled device.
- Network Protocol Manager for BGP does not import the router from IP Availability Manager and thus does not discover the BGPProtocolEndpoint.

This issue impacts BGPSession discovery: Network Protocol Manager for BGP creates a one-way adjacency (half link) to the Cisco router instead of a two-way adjacency (full link), even though the Cisco router and the router to which the BGPSession connects are both in IP Availability Manager's repository.

CQ 502060

### **Resolution**

Contact Cisco Support to obtain the correct patch for your device. After this upgrade, the BGPPeerTable should be populated for the device where BGP is enabled at the VRF level.

## **Network Protocol Manager for EIGRP issues**

These problems affect Network Protocol Manager for EIGRP.

### **Deleting a device in IP Availability Manager causes a rediscovery error in EIGRP Manager**

When a device is deleted in IP and the Discover All is issued in NPM, that device gets added to the pending list and keeps logging an error in NPM.

The error is:

```
ACC-E-OBJECT_NOT_CONNECTED-Object is not connected to the accessor
```

CQ 574847

### **Resolution**

Delete the device from the NPM topology before doing discover all or remove the device from the pending list after it is added.

## EIGRP Manager discovery drivers are accessing incorrect CLI credentials

When there is change in credentials for any device, NPM does not use the new credentials for discovery.

CQ 574848

### Resolution

Delete the device from NPM topology and do discover all. Or execute the following command from `BASEDIR/bin`:

```
./sm_adapter -s <Server name> --model=sm_msi --DelementName=SNMPAgent-
<dvice name> <Base Dir>/rules/eigrp/ic-eigrp-cisco.asl
```

## False alerts in EIGRP Domain Manager

Customers using SSH to monitor devices with Network Protocol Manager for EIGRP on Linux platform may experience false alerts due to slow responses from devices.

CQ 586499

### Resolution

EMC recommends using TELNET if possible.

When using TELNET, adjust the `read_timeout` and `get_timeout` values to avoid the alerts. For example, use `sm_edit` to change values in the `perl-cli.conf` file:

```
./sm_edit <BASEDIR>/smarts/conf/eigrp/perl-cli.conf
read_timeout=50
get_timeout=2
```

Save the file and exit.

If the alerts continue, you may need to increase both timeout values and evaluate the `EIGRPProtocolEndpoint PeerState` status.

---

### Note

You do not need to restart the Domain Manager or trigger full discovery after `perl-cli.conf` is updated.

---

## Network Protocol Manager for IS-IS issues

These problems affect Network Protocol Manager for IS-IS.

### ASL error in the IS-IS log file when starting a domain with an existing NPM RPS

When there are stale `ISISProtocolEndpoints` in the RPS, and creation of instrumentation objects fail, the following error messages are observed in the log.

```
ASL-W-ERROR_RULE_SOURCE-While executing rule set '/data/mensha/
9.2_GCD/NPM/smarts/rules/isis/settings.asl'
ASL-ERROR_ACTION-While executing action at:
ASL-CALL_STACK_RULE- RuleName:
INSTRUMENT SNMP AND ADD TO ACCESSOR, Line: 220
ASL-CALL_STACK_RULE- RuleName: START, Line: 93
ASL-ERROR_UNDEFINED_VARIABLE_ACCESS-Variable 'instrumentationObj'
has not been assigned a value
```

CQ 577896 / CQ 577888

### **Resolution**

These messages are observed because the Domain Manager could not create the instrumentation objects for stale endpoints. These messages are seen only during restart with a faulty RPS file.

These stale endpoints are removed during the first discovery. They do not have any impact on the functionality of the NPM server and can be ignored. All valid endpoints will be instrumented and monitored properly.

## **Network Protocol Manager for OSPF issues**

These problems affect Network Protocol Manager for OSPF.

### **Unable to disable CLI discovery in Network Protocol Manager for OSPF**

Disabling the `EnableOSPFPassiveInterfaceDiscovery` parameter in `BASEDIR/conf/ospf/ospf.conf` does not stop CLI discovery in Network Protocol Manager for OSPF.

CQ 635663

### **Resolution**

CLI discovery is enabled by default in Network Protocol Manager for OSPF to ensure passive interface discovery. If you disable the parameter setting for `EnableOSPFPassiveInterfaceDiscovery` in `BASEDIR/conf/ospf/ospf.conf`, you must perform a `DiscoverAll` in IP Availability Manager.

Performing the `DiscoverAll` action in IP Availability Manager triggers the `DiscoverAll` action in the Network Protocol Manager domain and will cause any runtime changes made in `BASEDIR/conf/ospf/ospf.conf` to take effect.

### **Jupiter/Sonet L3 sub-interfaces do not map correctly in OSPF**

Juniper L3 OSPF interfaces layered over Sonet L2 interfaces raise Interface Disabled alarms even when not disabled.

CQ 543063

### **Resolution**

This problem is due to a bug in the Juniper MIB. To work around this issue, give the sub-interface the same name as the L2 interface IP address.

# CHAPTER 7

## Optical Transport Manager (OTM)

This chapter includes the following topics:

- [Optical Transport Manager \(OTM\) overview](#) ..... 208
- [New features and changes in OTM](#) ..... 208
- [Fixed Issues in Optical Transport Manager](#) ..... 209
- [Known Problems in Optical Transport Manager](#) ..... 210

## Optical Transport Manager (OTM) overview

The EMC Smarts Optical Transport Manager provides root cause and impact analysis for services using optical transport networks.

The Optical Transport Manager includes the following components:

- Four domain managers that monitor optical networks:
  - SONET/SDH
  - WDM
  - Low Order SONET/SDH (also referred to as PDH)
  - Next Generation WDM, also called WDM-NG, used for monitoring WDM networks which are managed by TMF 864-compliant Element Management Systems  
The first three domain servers are split into two functional servers: Topology and Analysis. The WDM-NG server works with EMC M&R to collect data from EMS systems that support the TMF 864 interface. Both topology and analysis functions are combined in the WDM-NG server.
- XD Manager OTM to IP  
The XD Manager OTM to IP cross-correlates root-cause and impact analysis between a managed optical domain and the IP network.

The Optical Transport Management Suite works in conjunction with adapters to various Element Management Systems (EMS). A Topology adapter is used to discover inventory, and an Event adapter is used to capture notifications.

The following adapter is currently available from EMC:

- Optical Transport Management Suite Adapter for TMF 814. It supports:
  - Ciena LightWorks ON-Center EMS for Ciena CoreDirector networks
  - Cisco Transport Manager (CTM) EMS for Cisco ONS 15454 MSPP networks  
Custom-built adapter modules may be developed within the adapter frameworks provided for your specific devices and deployment situation.  
Monitoring of TMF 864-enabled Element Management Systems such as Coriant Intelligent Node Manager SR 6.0 SP2, using the SolutionPack for Optical Wavelength Services, the next generation WDM domain manager, and the SolutionPack for EMC Smarts.

## New features and changes in OTM

Here are the new features introduced with version 9.6.

### Support for addition of Card level events

Smarts Optical Transport Manager 9.6 supports additional Card level events to categorize between service affecting (SA) and non-service affecting (NSA) card failures.

### Foundation upgrade

The Optical domain managers and adapter have been migrated to the latest Foundation software. OTM now takes advantage of foundation features, for example,

secure client-server communication over the TLS protocol, internationalization support, FIPS support, and logging enhancements.

The EMC Data Access API (EDAA) is described in these documents:

- *Smarts Foundation EMC Data Access API (EDAA) Programmer Guide*
- *Service Assurance Suite Alert EMC Data Access API (EDAA) Programmer Guide*  
Other foundation features are described in the *EMC Smarts Foundation System Administration Guide*.

## New WDM Manager for Next Generation WDM Devices

The EMC Smarts Optical Transport Manager includes a new service, named Next Generation WDM Manager (WDM-NG).

This service can be used for discovery, monitoring and root cause analysis of next generation WDM networks. This domain manager uses a fresh topology model, which closely follows the TeleManagement Forum's MTOSI (Multi-Technology Operations Systems Interface) specification for representing Optical network components.

Please refer to the *EMC Smarts Optical Transport Manager User Guide* for information about the service architecture and notifications generated by the Next Generation WDM Manager.

The Next Generation WDM Manager can be deployed with these products:

- EMC Smarts Service Assurance Manager
- EMC M&R with the following SolutionPacks installed:
  - SolutionPack for Optical Wavelength Services
  - SolutionPack for EMC Smarts

## Fixed Issues in Optical Transport Manager

Here are the fixed issues for Optical Transport Manager.

**Table 28** Fixed issues in Optical Transport Manager

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-6078 SR 78092202	OutOtsPort, InOtsPort relationships for INLINE Amplifier Ports	Code logic has been enhanced to use upstream and downstream relationship to deduce a single root cause during fiber cut scenario in WDM network.	9.4.1.X	9.4.2
IS-3953 SR 70698404	Port events on various OTM Port classes lead to notifications being raised. Discrepancies in events/	Restricted port down for MuxInOchPort only if it is LOS ( isLosDetected).	5.1.0	9.4.1

**Table 28** Fixed issues in Optical Transport Manager (continued)

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	notifications for MuxInOchPort.			
IS-3951 SR 64979744	API makeLinkGroup usage: For multiple links, the API is not creating the LinkGroup instance.	Fixed the logic to choose the appropriate link group name, and if needed, append it with some number to make it unique. Also, a find link group API, findLinkGroupBy Links has been added to overcome the bottleneck of returning appropriate link group based on set of links provided.	5.1	9.4.1
IS-2763 SR 69424730	The TopologicalLink Down problem does not have the PTP LosEvent as its impact.	Code has been changed to include the LosEvent in the impact. Modified files: <ul style="list-style-type: none"> <li>• Windows: lib \sm_wdm_n g.so</li> <li>• Linux: lib/ libsm_wdm_ ng.so</li> </ul>	9.4	9.4

## Known Problems in Optical Transport Manager

These problems affect Optical Transport Manager.

## Autodiscovery is not automatically triggered after data collection in EMC M&R

When the SolutionPack for Optical Wavelength Services starts to collect data from the Element Management System (EMS), it should trigger autodiscovery in the OTM WDM NG server after the data collection is completed. This is not happening.

SND-1885

### Resolution

Perform the Discover All as a manual step from OTM WDM NG server.

## Monitoring attributes are greyed out when using WDM-NG domain manager

In the Next Generation WDM domain, the monitored attributes in all the classes do not get an initial value of FALSE, and appear greyed out in the console.

The attribute value changes to TRUE or FALSE only when the domain manager receives an event (notify or clear) for an alarm condition that is represented by the attribute.

SND-931, SND-1467

### Resolution

Until this is fixed, the (greyed out) attribute value should be viewed as a FALSE value. This is how the domain treats these values internally for Root Cause Analysis, and hence there is no functionality impact because of this.

## Spurious alarms occur during OTM-XD processing

Unwanted events such as HighOrder\_Circuit :: ServiceUnavailableEvent, ClientCircuit :: ServiceUnavailableEvent, FiberLink :: DownOrDegraded are created in the OTM-IP-XD servers.

These are spurious alarms showing as root cause notifications and do not have an Impact tab.

CQ 571223, CQ 502887

### Resolution

You can ignore these events.

## Root cause alarms show incorrect impact notifications

Under certain conditions, the Fiberlink LineFailure and Card CardDown root cause alarms display incorrect impact notifications.

This is an issue in impact analysis. However, the root cause alarms display correctly.

CQ 502750, CQ 502932

## Non-LCTPG CTP failure overwrites the LCTPG CTP failure in the UD2 field

When a non-LCTPG CTP failure occurs, the User Defined (UD) 2 field is overwritten by the non-LCTPG failure.

The Root Cause Analysis information is correct, but the UD2 field of CKT::ServiceUnavailable and TRAIL::TrailDown events are updated with the non-LCTPG CTP failure. Also CTP failure information which was part of the LCTPG ring is erased.

CQ 501483, CQ 525856

## **FORCE\_POST\_PROCESSING\_ERROR displays in the discovery window of SDH Topology server**

FORCE\_POST\_PROCESSING error appears in the pending elements list of the Discovery window.

After doing a "discover all," the discovery status is updated with the "last discovery completed" message but the FORCE\_POST\_PROCESSING\_ERROR remains visible.

CQ 501438 CQ 525857

## **Userdefined1 field is updated though Userdefined1 field is deprecated**

When PTP failure occurs, the Userdefined1 field is updated though support for the field has been deprecated.

CQ 531953

## **Error message when TMF 814 Adapter is started**

When the TMF 814 Adapter is installed as a service, the following error message is found in the log file when the adapter is started:

```
IC Framework - ASL-E-ERROR_NO_PROFILE-Profile PROFILE-default does not exist
```

CQ 502562, CQ 502982

### **Resolution**

This message occurs once and has no subsequent effect on adapter processing.

## **Extraneous Fiberlink alarms display in OTM-XD-WDM server**

Fiberlink alarms display during topology creation of the OTM-IP-XD-WDM server. These alarms are extraneous and should not appear.

CQ 534358

## **Router to Switch configuration topology is not uploaded in the OTM-IP-XD server**

A router to switch 1:N configuration stitch file does not create the topology in the OTM-IP-XD server. At this time, the router-switch configuration is not supported.

CQ 502708

## **ServiceAtRisk alarms event is not supported by cross-domain analysis**

When a Circuit:: ServiceAtRisk event occurs, the OTM-IP-XD manager does not do any analysis. At this time, the AtRisk functionality is not supported.

CQ 534104

## **No reference documentation for cross domain failure for mixed order IP using SDH and PDH**

Reference documentation is not available for cross domain failure for mixed order IP using SDH and PDH.

CQ 532205



# CHAPTER 8

## Voice over IP (VoIP) Availability Manager

This chapter includes the following topics:

- [Voice over IP \(VoIP\) Availability Manager overview](#) .....216
- [New features and changes in VoIP](#) ..... 216
- [Fixed Issues in VoIP Availability Manager](#) ..... 217
- [Known Problems in VoIP Availability Manager](#) ..... 218

## Voice over IP (VoIP) Availability Manager overview

The VoIP Availability Manager provides enterprises with availability, fault management, and performance visibility across their Voice over IP (VoIP) infrastructures.

This product provides multivendor support and a comprehensive VoIP management solution, and enables enterprises to perform IP phone management, service management, and voice mail management.

- EMC Smarts VoIP Availability Manager
  - EMC Smarts VoIP Enablement Pack for Avaya
  - EMC Smarts VoIP Enablement Pack for Cisco
  - EMC Smarts VoIP Enablement Pack for ACME
  - EMC Smarts VoIP Enablement Pack for AudioCodes

The EMC Enablement Packs are for use with the VoIP Availability Manager to discover and monitor vendor-specific elements in the VoIP environment. At least one Enablement Pack must be installed. In this document, the term “VoIP Availability Manager” represents the VoIP Availability Manager product and the enablement and integration pack products.

## New features and changes in VoIP

There are no new features in 9.6 release for VoIP.

### Changes in the procedure to start VoIP Availability Manager

The `--java` and `MaxHeapSize` options are no longer supported for the VoIP Availability Manager start command. Use the following syntax to start the VoIP Availability Manager:

```
./sm_server -b <BROKER> --name=<VoIP_Availability_Manager> --
config=voip --subscribe=default --ignore-restore-errors --output
```

`MaxHeapSize` is preconfigured to 4GB. However, you can modify the `MaxHeapSize` value. To do so, perform these steps:

#### Procedure

1. Open the `bootstrap.conf` file:

```
sm_edit /<BASEDIR>/VoIP/smarts/conf/voip/bootstrap.conf
```

2. Locate the following Line#41:

```
call SM-JVM-Interface add_prop "-Xmx4096m"
```

3. Edit the value `-Xmx4096m` according to your need. For example, `-Xmx1024m` for a maximum 1GB heap size.
4. Save the file.

## Changes in the VoIP Availability Manager service installation

During installation, the service command line that starts the VoIP Availability Manager has been updated to handle the deprecated options `--java` and `MaxHeapSize`.

Issue this command for Linux or CentOS:

```
/opt/InCharge/VoIP/smarts/bin/sm_service install
--force
--unmanaged
--startmode=runonce
--name=ic-voip-server
--description="EMC Smarts VoIP Availability Manager"
--env=SM_JAVA_ENABLED=YES
/opt/InCharge/VoIP/smarts/bin/sm_server
--name=VoIP-AM
--config=voip
--port=0
--subscribe=default
--ignore-restore-errors
--output
```

Issue this command for Windows:

```
C:\InCharge\VoIP\smarts\bin\sm_service.exe install
--force
--unmanaged
--startmode=runonce
--name=ic-voip-server
"--description=EMC Smarts VoIP Availability Manager"
"--env=SM_JAVA_ENABLED=YES"
C:\InCharge\VoIP\smarts\bin\sm_server.exe
"--name=VoIP-AM"
"--config=voip"
"--port=0"
"--subscribe=default"
"--ignore-restore-errors"
"--output"
```

## Fixed Issues in VoIP Availability Manager

Here are the fixed issues for VoIP.

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
IS-9604 SR 08476483	In VOIP, the Find System search option does not work.	Code has been added to create the ICIM_ObjectFactory object, and also, the findsystem call has been added.	9.4.2	9.5.1
IS-8836 SR 07459316	Smarts VoIP 9.4.2.9 fails to monitor CUCM 10.5 phones' status. The status is	The instrumentation soap.xml code has been modified to pick up the correct	9.4.2.9	9.5

CQ/SR/Issue number	Problem summary	Description of fix	Found in version	Fixed in version
	displayed as Unknown.	AXL port number from settings.		
IS-8193 SR 84304972	IPPhones status changes from REGISTERED to UNKNOWN.	Sometimes, Cisco CUCM does not recognize IP address as NodeName in Soap queries that results into monitoring of IPPhone failure. To resolve this, NodeName parameter is populated with AgentSysName, rather than IP address. This has been achieved by setting CallAgentDiscovered with the AgentSysName when there is a change in phone registration.	9.4.2	9.5
IS-8244 SR 85240044	Production VOIP service crashes.	Cleanup code has been added when socket bind fails.	9.3.0	9.5

## Known Problems in VoIP Availability Manager

These problems affect VoIP Availability Manager.

### SOAP credentials are not associated with CCM if multiple SOAP Access Groups are created

SOAP credentials are not associated with Cisco Call Managers (CCMs) in the first discovery, because the call managers were not discovered until the first discovery was completed.

CQ 653089

#### Resolution

A minimum of two discovery cycles are required to discover Cisco phones.

## IP Availability Manager instances are missing from the VoIP Availability Manager topology

Upon VoIP Availability Manager startup, the `--clean-topology` option does not load the `domain.conf` file automatically. As a result, the IP Manager instances like `INCHARGE-AM` are missing from the VoIP Availability Manager topology.

CQ 639648

### Resolution

The workaround is:

1. After starting the VoIP Availability Manager service, verify if the instances of the IP Manager (`INCHARGE-AM`, for example) are listed in the topology. Either:
  - a. In the **Domain Manager Administration Console** attached to the VoIP Availability Manager, expand the `InChargeDomain` class in the tree and look for the instances.
  - a. Log in to the VoIP Availability Manager with the `dmctl` command from `BASEDIR/smarts/bin` directory. Examine the `InChargeDomain` class attributes by typing: `./dmctl -s <VoIP-AM> geti InChargeDomain`
2. If IP Manager instances are not listed, type the following command from the VoIP Availability Manager `<BASEDIR>/smarts/bin` directory, `./sm_adapter -s <VoIP-AM> -f <BASEDIR>/smarts/local/conf/domain.conf <BASEDIR>/smarts/rules/import.asl`

---

### Note

In the command, `<BASEDIR>` represents the VoIP Availability Manager installation path.

---

## Error messages observed in the VoIP AM log file

If the VoIP server RPS has SNMP v3 devices and if you are migrating to VoIP 9.3 the following errors are seen in the log file:

```
ASL-W-E-R-R-O-R_R-U-L-E_SOURCE-While executing rule set '/data/xxx/9.3_GCD/VoIP/smarts/rules/voip/settings.asl'
ASL-E-R-R-O-R_A-C-T-I-O-N-While executing action at:
ASL-C-A-L-L_S-T-A-C-K_R-U-L-E-   RuleName: ADD_TO_ACCESSOR, Line: 981
ASL-C-A-L-L_S-T-A-C-K_R-U-L-E-   RuleName: START, Line: 100
ASL-E-R-R-O-R_I-N-S-E-R-T-While attempting to insert into property
'instance_instrumentations' of object 'MR_Object::SNMP-Poller'
ADSP-M-I-S-S-I-N-G_U-S-E-R-SNMP_access_info missing user name
```

CQ 603695 / CQ 577886

### Resolution

The errors are expected and are related to SNMPv3 devices monitoring because SMPv3 is not completely supported by VoIP AM.

**Table 29** Behavior of individual components

Components	V3 support	Comments
SNMP discovery	Yes	--

**Table 29** Behavior of individual components (continued)

Components	V3 support	Comments
SNMP monitoring (instrumentation)	No	--
SNMP Traps	No	Yes, if the trap exploder converts V3 traps to V2 traps. This behavior is same for IP-AM.
Pending list discovery	Yes	--

## ASL errors appear in VoIP Availability Manager log when the trap adapter port is in use

ASL errors appear in the VoIP Availability Manager log file when the trap receiver port is in use.

CQ 353791, CQ 353730

### Resolution

Check to see if some other process is using the same port number that is being used by the internal trap receiver. The port number is specified in `BASEDIR/smarts/conf/voip/voip.conf`.

## Inter-trunk data from VoIP Performance Manager GatewayService should be ignored

Inter-trunk data from VoIP Performance Manager GatewayService should be discarded and not used in H323Service data in VoIP Availability Manager topology.

CQ 353793, CQ 353759

### Resolution

Ignore this data.

## IsActive attribute of H248RegistrationSession does not synchronize correctly

IsActive attribute of H248RegistrationSession does not synchronize correctly between VoIP Availability Manager and the Global Manager.

CQ 353795, CQ 353700

### Resolution

Ignore the IsActive status in the Global Manager. It is reflected correctly in VoIP Availability Manager.

If Avaya client tools are being used, then you need to force synchronization between VoIP Availability Manager and the Global Manager. In this case, there are two methods to force synchronization:

- Using the `dmctl` command against VoIP Availability Manager to invoke the `ICF_TopologyManager::ICF-TopologyManager syncCompleted` method. For example, from the `BASEDIR/smarts/bin` directory in a VoIP Availability Manager installation area, enter: `dmctl -s <VoIP Availability Manager name> -b`

```
<Broker> invoke ICF_TopologyManager::ICF-TopologyManager
syncCompleted
```

- Delete the value for the syncCompletedAt attribute for the VoIP Performance Manager instance in the VoipPerformanceManager class of the VoIP Availability Manager topology. To do so, attach a Domain Manager Administration Console to VoIP Availability Manager, locate the VoIP Performance Manager instance in the VoipPerformanceManager class in the topology tree, and delete the value of syncCompletedAt in the right panel.

## H323Service call counts do not agree with VoIP Performance Manager values

The values of Cisco H.323 signaling service (H323Service) attributes, ActiveCalls and CallsInProgress, do not agree with the performance data from the VoIP Performance Manager.

The ActiveCalls and CallsInProgress values should be the sum of all values reported by each CallManager. Currently, the ActiveCalls and CallsInProgress attributes reflect the last value reported by the CallManager.

This issue only occurs if your VoIP Availability Manager deployment includes the Cisco Enablement Pack and the VoIP Performance Manager Integration Pack.

CQ 501119

### Resolution

No workaround exists for this issue.

## Misleading subscription change messages in VoIP Availability Manager log file

A misleading error change message appears repeatedly in the VoIP Availability Manager log file:

```
[February 1, 2012 6:22:45 PM GMT+05:30 +388ms] t@1350678848
SM_ProtocolEngine-10 unknown IC Console - V8.1.3.0
RSVI_MSG--SUB_CHG-Subscription change: purgeObserver client:
SM_SocketObserver-10 unknown IC Console - V8.1.3.0
```

CQ 634653

### Resolution

Ignore this message. No user action is required.

## VoIP Availability Manager Avaya-related issues

The following issues pertain to Avaya devices.

### ReducedRedundancy event does not have CausedBy tab for Avaya RedundancyGroups

When the StandBy or Active Avaya Media servers are shut down, a ReducedRedundancy event is displayed in the Global Manager Notification List for the ConvergedCallManagerRedundancyGroup, but it does not have a root cause associated with it.

CQ 351547, CQ 351362

### Resolution

Restart the Global Manager to resolve this issue.

## Gateway Service display in the VoIP Availability Manager is inaccurate

Data appearing in the GWStatus field might be inaccurate.

CQ 353819, CQ 353815

### **Resolution**

This issue will be addressed in a future release.

## Avaya IP phone correlation issue

In the Notification Log Console for the selected Port Down notification, the Notification Properties dialog box does not display an Impact tab listing the IPPhone Unregistered notification.

When an Avaya IP phone disconnects from the network, the following occurs:

- VoIP Availability Manager generates an IPPhone Unregistered event.
- IP Availability Manager generates a Switch or Port Down event.

CQ 503015

### **Resolution**

No workaround exists for this issue.

## IP phones that are registered to a standalone Avaya PBX are not being monitored

For Avaya phones that are registered to a standalone PBX, VoIP Availability Manager does not establish instrumentation for those phones and thus does not monitor them.

This issue pertains to the operating mode (standalone) of the PBX. VoIP Availability Manager is designed to monitor IP phones that are registered to redundancy-group Avaya PBXs, not to standalone Avaya PBXs. All mid-to-large-scale VoIP service providers use redundancy-group mode to ensure less downtime and higher longevity of production.

The current logic relies on ConvergedCallManagerRedundancyGroups to establish instrumentation for Avaya phones.

CQ 641221

### **Resolution**

The current logic will be changed in a future release so that the VoIP Availability Manager will instrument and monitor IP phones that are registered to either a redundancy-mode PBX or a standalone PBX.

## VoIP Availability Manager Cisco-related issues

The following issues pertain to Cisco devices.

### SNMP v2 does not discover Cisco Unified Communications Manager 9.x

In the 9.4.2 release, the VoIP Availability Manager does not discover Cisco devices managed by Cisco Unified Communications Manager (CUCM) 9.x.

Cisco devices have a bug where SNMP v2 times out. The IP Manager performs the initial discovery for the VoIP Availability Manager. Subsequently, the VoIP Availability Manager discovers VoIP-specific objects based on the topology initially imported from the IP Manager. As a result of the bug, IP Manager times out and CUCM does not discover the Cisco devices.

IS-7234

**Resolution**

The workaround is to configure the IP Manager to use SNMP v1 to perform the discovery. Modify the `discovery.conf` file before starting the IP Manager. To do so:

1. Use `sm_edit` to open the `BASEDIR/smarts/conf/discovery/discovery.conf` file in the IP Manager installation.
2. Edit the parameters as follows:
  - `SNMPGetBulkEnabled=FALSE`
  - `defaultTimeout = 20000`
  - `defaultSNMPAutoTimeout = 20000`
3. Save and exit the file.
4. Restart the IP Manager server if it is already started.

**Cisco Unity Express version 3.2 is not supported**

VoIP Availability Manager does not support Cisco Unity Express version 3.2. Cisco Unity Express version 3.2 has a bug in its SNMP object, `cueShutdownRequest`. The `cueShutdownRequest` SNMP object is always set to `TRUE` and does not update.

This issue affects VoIP Availability Manager's ability to monitor Cisco Unity Express 3.2, especially the re-registration of Cisco IP phones. The status might be reported incorrectly by VoIP Availability Manager due to the device bug.

**Resolution**

No resolution is available at this time. This issue has been submitted to Cisco Systems, Inc. as ticket CSCsw23007.

**Cisco Call Manager Express with the SRST mode enabled is not supported**

Cisco Survivable Remote Site Telephony (SRST) is a remote survivable site that is used by IP phones to register when Call Managers go down in the main site.

Typically, Cisco SRST can be implemented as:

- Call Manager configured with a standalone SRST.
- Call Manager configured with a Call Manager Express with SRST mode enabled. VoIP Availability Manager only supports the standalone SRST configuration. It does not support Cisco Call Manager Express (CCME) with the SRST mode enabled.

