VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers

VMware Smart Assurance 10.0.0

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

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

Contents

1 Overview 6

- Product contents 6
- Product and version compatibility 9
- Installation tasks overview 10
- Upgrade tasks overview 11
- Migration tasks overview 11
- Uninstallation tasks overview 12

2 Performing an Installation 13

- Installation overview 13
- Installation prerequisites 14
- Install the product 14
- Support for FIPS 140-2 for Smart Assurance products 17
- Next steps 20

3 Performing an Installation in Docker Container 21

- Installation overview 21
- Installation prerequisites 21
- Creating and starting Docker image 22
- Operations on Docker container 22
- Performing Smarts upgrade inside Docker 24

4 NAS Installation and Startup 25

- Overview 25
- Installing and starting the HTTPS Adapter service 26

5 Performing an Upgrade 29

- Upgrade installation overview 29
- Upgrade installation prerequisites 31
- Upgrade the product 31
- Upgrading Smart Assurance products in FIPS mode 35
- Next steps 35

6 Performing a Migration 36

- Migration overview 36
- Install and migrate on the same host 37
- Install and migrate on a different host 40
- Post-migration tasks 42

7 Migration Utilities 45

Customization migration utility overview 45

sm_migrate function 48

Customization migration procedures 49

Perform a rollback 53

Custom file migration use cases 53

Three-way merge utility 57

Automatically migrate topology for IP Manager using RPS utility 59

Deployment utility overview 61

8 Verifying the Installation 65

Check the version number 65

Start services 66

Start programs 67

Service and program startup options 68

Start Smarts NOTIF 69

Verify the product status 71

Verify the FIPS 140 mode status 71

Collect system information 73

Configuration Scanner Tool 77

9 Performing an Uninstallation 79

Before uninstallation 79

Uninstall VMware Smart Assurance products 82

10 The sm_edit utility 84

sm_edit 84

sm_edit example 85

11 Manually Installing Services 86

Overview 86

Broker services 87

Services for the IP Manager 87

Services for the Service Assurance Manager 89

Services for the MPLS Management Suite 94

Services for the Server Manager 96

Services for the Network Protocol Management Suite installation 96

12 Procedures for CD/DVD-ROMs 99

Mounting a CD/DVD-ROM on UNIX systems 99

13 Using the MPLS server_config Utility 101

Use the server_config.pl script to change domain names 101

14 Configuration Scanner tool Sample Output 105

Files created by Configuration Scanner tool 105

Sample outputs 106

Overview

1

This chapter includes the following topics:

- Product contents
- Product and version compatibility
- Installation tasks overview
- Upgrade tasks overview
- Migration tasks overview
- Uninstallation tasks overview

Product contents

This document provides installation, upgrade, migration, and uninstallation procedures for:

- VMware Smart Assurance Service Assurance Manager
- VMware Smart Assurance IP Manager
- VMware Smart Assurance MPLS Management Suite
- VMware Smart Assurance Server Manager
- VMware Smart Assurance Network Protocol Management Suite

  The VMware Smart Assurance Service Assurance Manager includes the following products:

- Service Assurance Manager

  The Service Assurance Manager product includes the following components:

  - Global Manager
  - VMware Smart Assurance Broker
  - VMware Smart Assurance MBIM — Maintenance and Business Impact Manager Server
  - Generic notification adapters such as Log File, SNMP Trap, Script, and email
  - EMC Data Access API
    - Smarts Foundation EMC Data Access API (Smarts EDAA)

  - Alert EMC Data Access API (EDAA)
  - VMware Smart Assurance Data Web Applications (Tomcat)
  - VMware Smart Assurance Notification Exchange (Rabbit MQ)
  - VMware Smart Assurance Notification Cache (ElasticSearch)

  Note Some components, such as Business Impact Manager, require licensing.

- Global Console

  The Global Console product is the graphical interface for all VMware Smart Assurance products.

  Global Console functionality can also be deployed as a Web Console or a Business Dashboard.

- Adapter Platform

  The SAM Adapter Platform product provides functionality to import and normalize topology and events from outside the VMware Smart Assurance domain.

- Syslog Adapter

  The Syslog Adapter product reads and processes system log (Syslog) messages. It requires the SAM Adapter Platform.

- Smarts Notification Module

  The Smarts Notification Module (NOTIF) augments VMware Smart Assurance solutions with event management features that are configured through a graphical user interface (the Smarts NOTIF Editor). Smarts NOTIF enables the user to easily optimize the flow of events and notifications sent through any VMware Smart Assurance system. Smarts NOTIF can be installed on either the SAM server or Adapter Platform server, or both. The internal event and notification processing features of the standard SAM Adapter Platform are replaced by Smarts NOTIF.

  Note Smarts NOTIF functionality and architecture is discussed in the *VMware Smart Assurance Notification Module User Guide*.

- Smarts Notification Module Cisco Syslog Processing Adapter

  The Smarts Notification Module Cisco Syslog Processing Adapter (referred to as the Smarts NOTIF Cisco Syslog Adapter) replaces the log file processing features of the standard Syslog Adapter. The Smarts NOTIF Cisco Syslog Adapter processes the log file information into useful notifications with or without the use of ASL scripts.

  Note The *VMware Smart Assurance Notification Module Cisco Syslog Processing Adapter Installation and User Guide* provides additional information on this adapter.

- SNMP Trap Adapter

  The SNMP Trap Adapter product reads SNMP traps and forwards traps to any VMware Smart Assurance application. It requires the SAM Adapter Platform.

- XML Adapter

  The XML Adapter product imports and exports topology from any VMware Smart Assurance application.

  The VMware Smart Assurance IP Manager includes the following products:

- IP Availability Manager
- IP Performance Manager
- IP Server Performance Manager
- IP Availability Manager Extension for NAS

  The VMware Smart Assurance MPLS Management Suite includes the following products:

- VMware Smart Assurance MPLS Manager is composed of three servers:
  - MPLS Topology Server
  - MPLS Monitoring Server
  - MPLS Analysis Server
- MPLS VPN-Tagging Server

  The VMware Smart Assurance Network Protocol Management Suite includes the following products:

- VMware Smart Assurance Network Protocol Manager for BGP
- VMware Smart Assurance Network Protocol Manager for EIGRP
- VMware Smart Assurance Network Protocol Manager for IS-IS
- VMware Smart Assurance Network Protocol Manager for OSPF

  The VMware Smart Assurance Server Manager includes the Server Manager software.

Installation directory structure

The installation directory structure is shown in Installation directory structure. All VMware Smart Assurance products use the same basic installation directory structure.

In Installation directory structure, notice that:

- BASEDIR, which is not an environment variable, is used in documentation to represent the top-level directory structure of an VMware Smart Assurance product software installation.

  For UNIX, this location is /opt/InCharge/*<product>*.

  BASEDIR represents:

  - For MPLS Management Suite —*<installation_root_directory>/MPLS*
  - For IP Manager — *<installation_root_directory>/IP*
  - For Service Assurance Manager — *<installation_root_directory>/SAM*
  - For Server Manager — *<installation_root_directory>/ESM*

- For Network Protocol Management Suite — *<installation_root_directory>/NPM*

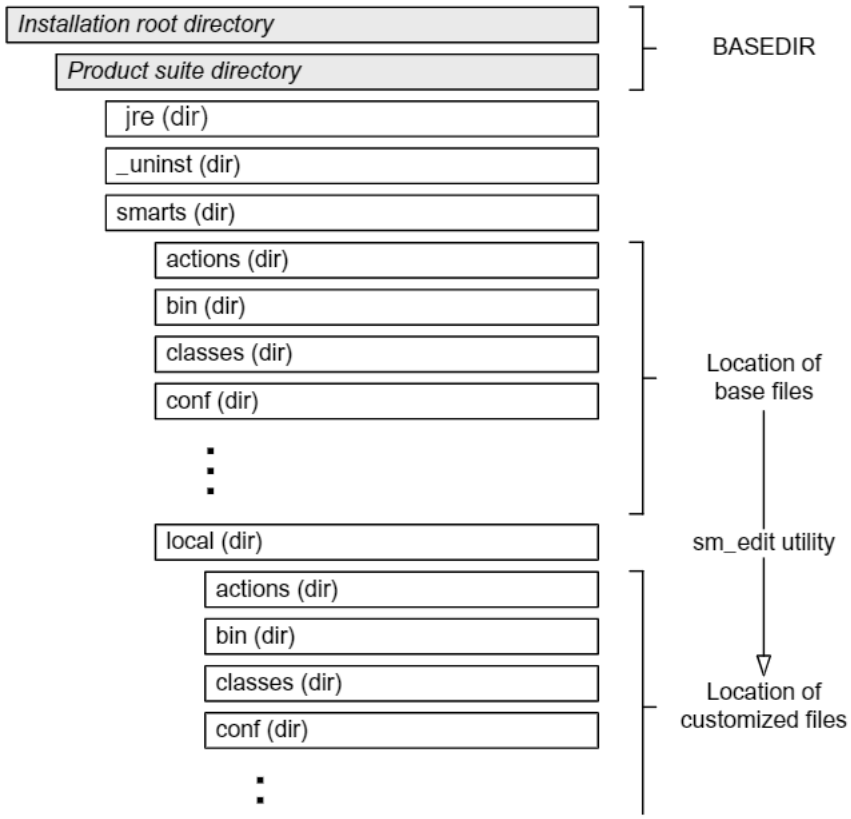
  By default, VMware Smart Assurance software is installed to BASEDIR/smarts.

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

- The VMware Smart Assurance sm_edit utility ensures that modified files are always saved to the appropriate local area and that base (original) copies of the files remain unchanged. Chapter 10 The sm_edit utility provides additional information.

  The VMware Smart Assurance System Administration Guide provides detailed information about the directory structure for VMware Smart Assurance software and the sm_edit utility.

  Figure 1-1.



Product and version compatibility

The *VMware Smart Assurance Support Matrix* provides information about the products and the compatible versions of the VMware Smart Assurance products.

Installation tasks overview

To install VMware Smart Assurance Service Assurance Manager, IP Manager, MPLS Management Suite, Server Manager, or the Network Protocol Management Suite, you need to meet the requirements or perform the tasks that are listed in Installation requirements and tasks.

Note To install additional components to an existing installation, you can perform an installation or an upgrade.

Before you install	
The Broker license host should be installed, configured, and operating.	VMware Smart Assurance System Administration Guide
The Global Console, Global Manager, and Service Assurance products should be installed, configured, and licensed.	*VMware Smart Assurance Installation Guide*
IP Manager should be installed, configured, and licensed. After IP Manager is installed, you can install or upgrade other Smarts products.	*VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM.*
Review the important release issues for the product being installed.	*VMware Smart Assurance Release Note*
Determine if the products are supported on your platform.	*VMware Smart Assurance Support Matrix*
Review the patch requirements for your operating system.	*VMware Smart Assurance Support Matrix*
Determine if your system meets the hardware requirements.	*VMware Smart Assurance Support Matrix*
Installation method	
Install the product.	Select one of the following installation methods: ■ Install using CLI mode ■ Install using Unattended mode
After you install	
If your product is part of a deployment that requires the Federal Information Processing Standard (FIPS) Publication 140-2, a U.S. government computer security standard governing cryptographic modules, perform the procedure to enable products in FIPS mode.	Support for FIPS 140-2 for Smart Assurance products
If you installed the products as services, start them for the first time.	■ Starting services on UNIX ■ Start programs
Verify the current state of the products and the Broker.	Verify the product status
Optional task: After modifying your configuration files on one installation, you can use the deployment utility to create a deployment package of your configuration changes and deploy the package on other installations.	*Deployment utility overview*

Upgrade tasks overview

To upgrade, you need to meet the requirements or perform the tasks that are listed in Upgrade installation requirements and tasks.

Before you upgrade	
Review the release notes for important issues.	*VMware Smart Assurance Release Note*
Determine if the products are supported for your platform.	*VMware Smart Assurance Support Matrix*
Determine if your system meets the hardware requirements.	*VMware Smart Assurance Support Matrix*
Upgrade installation	
Upgrade the products in the following order: 1 Top-most SAM server 2 An Aggregation SAM server if it is a hierarchical SAM deployment. 3 IP Manager. 4 Any order: Server Manager, MPLS Manager, and Network Protocol Manager.	■ For VMware Smart Assurance products: Chapter 5 Performing an Upgrade
After you install	
Evaluate your custom code and review the tools for restoring user customization.	Custom file migration use cases
If your product is part of a deployment that requires the Federal Information Processing Standard (FIPS) Publication 140-2, a U.S. government computer security standard governing cryptographic modules, perform the procedure to upgrade products in FIPS mode.	Upgrading Smart Assurance products in FIPS mode
If you installed the products as services, start them for the first time.	■ Starting services on UNIX ■ Start programs
Verify the current state of the products and the Broker.	Verify the product status
(Optional) After performing an upgrade and modifying your configuration files on one installation, you can use the deployment utility to create a deployment package of your configuration changes and deploy the package on other installations. After deploying the package on other installations, you do not have to run the migrate utility to merge your customizations.	*"Deployment utility overview" on page 97*

Migration tasks overview

To migrate to Version 10.0.0, you need to meet the requirements or perform the tasks that are listed in Migration requirements and tasks.

Before you migrate	
Review the release notes for important issues.	*VMware Smart Assurance Release Note*

Determine if the products are supported for your platform.	*VMware Smart Assurance Support Matrix*
Determine if your system meets the hardware requirements.	*VMware Smart Assurance Support Matrix*
Installation and migration	
Perform the migration in the following order: 1 Top-most SAM server 2 An Aggregation SAM server if it is a hierarchical SAM deployment. 3 IP Manager. 4 Any order: Server Manager, MPLS Manager, and Network Protocol Manager.	■ For VMware Smart Assurance products: Chapter 6 Performing a Migration.
After you install	
Evaluate your custom code and review the tools for restoring user customization.	Custom file migration use cases
If you installed the products as services, start them for the first time.	■ Starting services on UNIX ■ Start programs
Verify the current state of the products and the Broker.	Verify the product status
(Optional) After performing a migration and modifying your configuration files on one installation, you can use the deployment utility to create a deployment package of your configuration changes and deploy the package on other installations. After deploying the package on other installations, you do not have to run the migrate utility to merge your customizations.	*"Deployment utility overview" on page 97*

Uninstallation tasks overview

To uninstall the product, you need to meet the requirements or perform the tasks that are listed in Uninstallation requirements and tasks.

Table 1-4. Uninstallation requirements and tasks

Before you uninstall	
Review uninstall prerequisites.	Chapter 9 Performing an Uninstallation
Uninstallation	
Uninstall the product.	■ "Uninstall using Wizard mode" on page 125 ■ UNIX only, Uninstall using CLI mode ■ Uninstall using Unattended mode

Performing an Installation

2

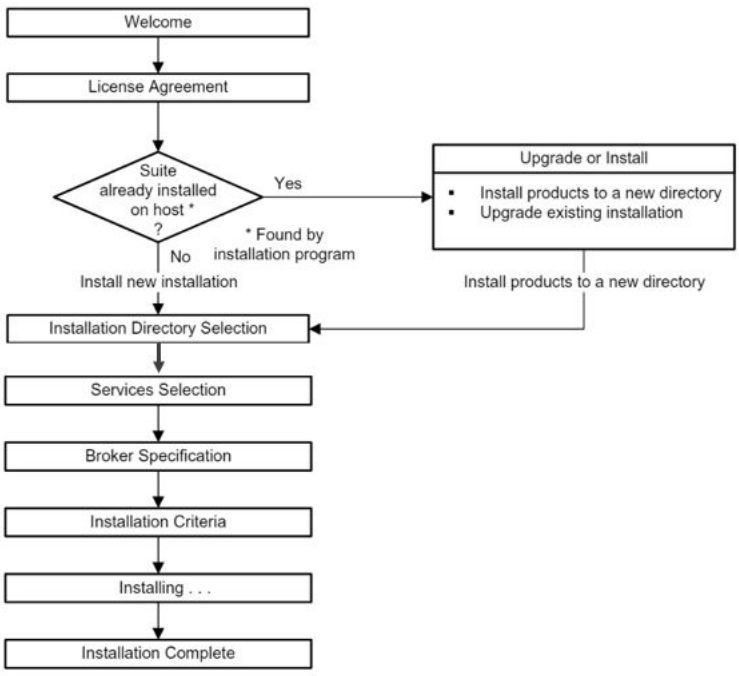
This chapter includes the following topics:

- Installation overview
- Installation prerequisites
- Install the product
- Support for FIPS 140-2 for Smart Assurance products
- Next steps

Installation overview

The installation flow is shown in New installation flowchart. A new installation installs a new version of a product on a host system that either has no software installed or has a previous version of the software installed. Chapter 5 Performing an Upgrade provides instructions to install an upgrade installation.

Figure 2-1. New installation flowchart



Installation prerequisites

Fulfill the following prerequisites before starting the installation:

- Ensure that you have superuser (User ID 0) or administrative privileges on the target host. The installation program will halt if you do not have the appropriate privileges.
- Ensure that the required operating system patches have been installed. Clicking **More Information** during the installation process will launch the System Information window and the Pass/Fail status of the operating system patches. The *VMware Smart Assurance Support Matrix* provides information on operating system patches.
- Determine the location of the VMware Smart Assurance Broker.

  You must specify the location of the Broker during a new installation of VMware Smart Assurance software. Typically, this location is chosen during the design of the VMware Smart Assurance software deployment and before any installation begins. Consult with your deployment planner or check the build guide that documents your deployment to determine the name of the host where the Broker was installed and the port that the Broker uses.

  If the location is the same host where you are installing this product, the installation program will automatically install the Broker if it is not already on the host.
- (Service Assurance Manager only) Decide whether your operators will use the Service Assurance Manager Notification Console (classic SAM functionality).

Install the product

You acquire the software for the VMware Smart Assurance Service Assurance Manager, VMware Smart Assurance IP Manager, VMware Smart Assurance MPLS Management Suite, VMware Smart Assurance Server Manager, and VMware Smart Assurance Network Protocol Management Suite in one of two ways:

- From the installation CD/DVD-ROM.

  Insert the CD/DVD-ROM into the optical drive of the host system. Chapter 12 Procedures for CD/DVD-ROMs describes how to access the optical drive for various operating systems.

  When you insert the installation CD/DVD, several minutes might pass between the InstallShield preparation screen and the VMware Smart Assurance splash screen/installation dialog boxes. Be patient. Do not eject/reinsert the CD/DVD to start a second install process.
- From the VMware online support website.

  Go to the VMware online support website and download the installation file that is specific to your platform.

  You install each product in one of three ways: Wizard mode, CLI mode, or Unattended mode.

Install using CLI mode

CLI mode provides a text-based method for invoking the installation program. This mode is intended for UNIX platforms with non-graphics consoles. The CLI mode follows the same process flow as the Wizard mode but uses text rather than graphics.

Running CLI mode

Table 2-1. Setup command syntax for CLI mode

Product	Operating system	Executable
Service Assurance Manager Server	Linux	./setup-SAM-10_0_0_0-linux64.bin
Service Assurance Manager Console	Linux	./setup-CONSOLE-10_0_0_0-linux.bin
IP Manager	Linux	./setup-IP-10_0_0_0-linux64.bin
MPLS Management Suite	Linux	./setup-MPLS-10_0_0_0-linux64.bin
Server Manager	Linux	./setup-ESM-10_0_0_0-linux64.bin
Network Protocol Management Suite	Linux	./setup-NPM-10_0_0_0-linux64.bin

User selections and navigation in CLI mode

During the installation and uninstallation processes, you are prompted with a series of steps and menus:

- For prompts, accept the default value or select another choice. The default values are indicated in brackets. To accept the default value, press **Enter**. To reply “yes,” enter **y** or **Y**; to reply “no,” enter **n** or **N**. Do not press **Delete** because doing so will cause the process to terminate with an error message.
- For selections in menus, accept the default selections or type the number of the item and press **Enter**.

  If you incorrectly type an entry, press **back** to repeat the prompt and select the correct value. Arrow keys and the Backspace key are not supported.

If your product is part of a deployment that requires the Federal Information Processing Standard (FIPS) Publication 140-2, a U.S. government computer security standard governing cryptographic modules, follow the instructions in Support for FIPS 140-2 for Smart Assurance products.

Next steps provides post-installation tasks.

Install using Unattended mode

Unattended mode reads the selections and settings for the installation from a user-modifiable response file, which enables you to easily duplicate the installation on many computer systems. Manual intervention is not necessary after you execute the setup command.

The response file, named <product>-response.txt, is located on the CD/DVD-ROM in the /utils directory. The file provides instructions and examples of command line options that are passed to the installation program in Unattended mode. The command line options are organized by process flow, which is almost identical to that of Wizard mode or CLI mode.

Note For instructions on installing the Service Assurance Manager Server in Unattended mode, complete the steps in the following section. To install other Service Assurance Manager products after Server install, refer to "Installing the Service Assurance Manager Console, or the Smarts NOTIF Editor, or both" on page 32.

Modifying the response file

To modify the response file:

1 Copy the response file from the CD/DVD's /utils directory to a directory on your host, for example, to the /tmp directory.

2 Using a text editor, modify the values for the command line options in the response file:

3 Specify the target directory.

4 Select a directory for the process log file.

5 Select the products to install. Ensure that the property value for the product is set to **true**.

6 Select the products to start as services. Ensure that the property value for the product is set to **true**.

7 Specify the location of the Broker. By default, the location is set to localhost at port 426.

8 Save the file.

Running Unattended mode

To start the Unattended mode, invoke the setup command with the **-**options command-line option, followed by the full path to the response file as described in Setup command syntax for Unattended mode.

Table 2-2. Setup command syntax for Unattended mode

Product	Operating system	Executable
Service Assurance Manager Server	Linux	./setup-SAM-10_0_0_0-linux64.bin -i silent -f <path>/<product>-response.txt
Service Assurance Manager Console	Linux	./setup-CONSOLE-10_0_0_0-linux64.bin -i silent -f <path>/<product>-response.txt
IP Manager	Linux	./setup-IP-10_0_0_0-linux64.bin -i silent -f <path>/<product>-response.txt
MPLS Management Suite	Linux	./setup-MPLS-10_0_0_0-linux64.bin -i silent -f <path>/<product>-response.txt
Server Manager	Linux	./setup-ESM-10_0_0_0-linux64.bin -i silent -f <path>/<product>-response.txt

Table 2-2. Setup command syntax for Unattended mode (Continued)

Product	Operating system	Executable
Network Protocol Management Suite	Linux	./setup-NPM-10_0_0_0-linux64.bin -i silent -f <path>/<product>-response.txt
where <*path*> is the fully qualified path to the response file and <*product*> is the product name, for example, IP_NETWORK_SUITE, MPLS_SUITE, or SAM_SUITE.		

For example for MPLS Management Suite, to start the Unattended mode of installation on Linux when the response file is located in /opt/home, enter:

```
./
setup-MPLS-10_0_0_0-linux64.bin
 -i silent -f <path>/<product>-response.txt
```

If your product is part of a deployment that requires the Federal Information Processing Standard (FIPS) Publication 140-2, a U.S. government computer security standard governing cryptographic modules, follow the instructions in Support for FIPS 140-2 for Smart Assurance products.

Next steps provides post-installation tasks.

Note SAM and SAM-Console Custom feature is removed. Now, all the features are available as a complete installation in both fresh installation and upgrade from older products.

Support for FIPS 140-2 for Smart Assurance products

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard governing cryptographic modules. FIPS 140 is required for any software purchased by the U.S government and U.S military. This release specifically addresses U.S Government accounts which require FIPS 140 compliance.

A configuration parameter, *SM_FIPS140*, has been introduced for FIPS 140 in the runcmd_env.sh file. The SAM or VMware Smart Assurance administrator can enable or disable this parameter as required. The default value of this parameter is *FALSE*.

FIPS 140 mode allows you to use SNMP V1, SNMPV2C, SNMP V3, with SHA and AES 128 protocols. FIPS 140 does not support the DES privacy protocol or the MD5 authentication protocol. When you discover an SNMPv3 device, you need to select the option “V3” in the “Add Agent” window. The “Authentication Protocol” option lists only SHA and not MD5, and the “Privacy Protocol” option lists only AES and not DES. This is because MD5 and DES are not supported in FIPS 140 mode. When you discover SNMPv3 devices with MD5 and DES protocol as seed, the devices go to the Pending List and display as “Invalid” or “Unsupported SNMP V3 protocol.”

Note FIPS 140 mode cannot be enabled or disabled after a server is started. FIPS 140-enabled Domain Managers such as MPLS Management Suite, IP Manager, Service Assurance Manager, and Server Manager can work only with the SAM Global Console 9.x or later for FIPS 140-2 mode.

A non-FIPS 140 mode Broker will not be able to communicate with a FIPS 140-enabled Manager (IP server, SAM server, or Domain Manager). Trying to establish such a connection will result in the enabled Manager going into a DEAD state after couple of minutes. Communication should always happen between FIPS 140-enabled Brokers and Managers.

Inter-domain and FIPS 140 Broker communication happens only when the Broker, Managers, and the SAM Console are all in FIPS 140 mode, else the application will not be operational.

This section covers the following scenarios for FIPS 140:

- Enabling FIPS 140 mode on a new installation
- Disabling FIPS 140 mode
- Verify the FIPS 140 mode status

Enabling FIPS 140 mode on a new installation

When you install a 10.0.0 product, FIPS 140 is not enabled by default. You must enable FIPS 140 on a clean installation or an upgrade, before the servers are started, using the following procedure:

1 Back up the *imk.dat*, *brokerConnect.conf*, *serverConnect.conf* and *clientConnect.conf* files from the existing installation. These files are located in the *BASEDIR/local/conf* folder.

Note The backup is necessary in case you need to disable FIPS 140 mode and remove FIPS 140-2 encryption.

2 Run the following command at the command line prompt:

```
sm_rebond --upgrade --basedir=<
BASEDIR
>/smarts

sm_rebond --upgrade --basedir=C:\InCharge\SAM\smarts
```

3 When prompted, type a password to regenerate the *imk.dat* file. The default password is *Not a secret*.

4 Set the value for the parameter **SM_FIPS140** to **TRUE** in the *runcmd_env.sh* file. The file is located under the *BASEDIR/smarts/local/conf* directory.

Enabling FIPS 140 mode on SAM Web Console

1 Perform steps 1 - 3 as described in the section, Enabling FIPS 140 mode on a new installation.

2 Go to the <BASEDIR>/smarts/jre/lib/security folder, and in the java.security file, change:

“sun.security.rsa.SunRsaSign” to “com.rsa.jsafe.provider.JsafeJCE” and “com.sun.net.ssl.internal.ssl.Provider” to “com.rsa.jsse.JsseProvider.”

3 Set the value for the parameter SM_FIPS140 to TRUE in the runcmd_env.sh file. This file is located under the <BASEDIR>/CONSOLE/smarts/local/conf folder of your Global Console installation.

4 or

5 Use "-Dcom.smarts.fips_mode=true" as a command line parameter for the sm_gui command.

Enabling FIPS 140 mode on SAM Dashboard

1 Perform steps 1 - 3 as described in the section, Enabling FIPS 140 mode on a new installation.

2 Set the value for the com.smarts.fips_mode to TRUE in the corresponding webconsole.properties file (located under <BASEDIR>/InCharge/CONSOLE/smarts/tomcat/webapps/webconsole folder)

3 or

4 dashboard.properties file (located under <BASEDIR>/InCharge/CONSOLE/smarts/tomcat/webapps/templates).

5 Set the value for the parameter SM_FIPS140 to TRUE in the runcmd_env.sh file. This file is located under the <BASEDIR>/CONSOLE/smarts/local/conf folder of your Global Console installation.

6 or

7 Use "-Dcom.smarts.fips_mode=true" as a command line parameter for the sm_gui command.

Enabling FIPS 140 mode on SAM NOTIF

1 Perform steps 1 - 3 as described in the section, Enabling FIPS 140 mode on a new installation.

2 Go to the <BASEDIR>/CONSOLE/smarts/notif/editor/ or the <BASEDIR>/SAM/smarts/notif/editor folder, and edit the NotifGui.bat/NotifGui.sh file to replace the string, “com.netmg.notif.gui.NotifApplication” with “-Dcom.smarts.fips_mode=true com.netmg.notif.gui.NotifApplication.”

3 Set the value for the parameter SM_FIPS140 to TRUE in the runcmd_env.sh file. This file is located under the <BASEDIR>/CONSOLE/smarts/local/conf folder of your Global Console installation.

4 or

5 Use "-Dcom.smarts.fips_mode=true" as a command line parameter for the sm_gui command.

Note If you install the servers as a service on Linux platforms, the services will start automatically after you issue the sm_rebond command. First stop the services, modify SM_FIPS140=TRUE in the runcmd_env.sh file, and then manually start the services.

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

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

This message is generated because FIPS 140 requires secure communication, which can be achieved using SSL. If this certificate is not available, the SAM Manager generates a self-signed certificate. This message is benign in nature and does not impact functionality.

Disabling FIPS 140 mode

To disable FIPS 140:

1 Replace the *imk.dat*, *brokerConnect.conf*, *serverConnect.conf* and *clientConnect.conf* files in the *BASEDIR/local/conf* folder, with the copies saved from prior to "Enabling FIPS 140 mode on a new installation". If you do not have a copy of these files saved, contact Technical Support.

2 Set the value for the **SM_FIPS140** parameter to **FALSE** in the *runcmd_env.sh* file. This file is located under *BASEDIR/smarts/local/conf/runcmd_env.sh.*

3 Restart all processes, such as the Broker, Domain Managers, SAM Global Manager, and Global Console.

Note RPS files started under FIPS mode cannot be re-used in non-FIPS mode. Domains will need to be started either from scratch or pre-FIPS RPS files can be used in cases where topologies have not changed. Restoring from older RPS files may not be productive as it will not contain any recent topology.

Next steps

Perform the following tasks:

- Chapter 6 Performing a Migration describes additional tasks if you are migrating from a previous version of the product.
- Chapter 8 Verifying the Installation describes tasks for verifying the proper installation of the software and starting services.

Performing an Installation in Docker Container

3

This chapter includes the following topics:

- Installation overview
- Installation prerequisites
- Creating and starting Docker image
- Operations on Docker container
- Performing Smarts upgrade inside Docker

Installation overview

Docker is a tool for packaging and shipping applications. Based on the idea of a shipping container, it provides a standardized way for administrators to create lightweight images, or collections of images, for each element of an application, and then easily and quickly deploy the image.

Since the image is standardized, it can be uniformly deployed in development or production environment.

Note You can install the Smarts applications in docker container only on the Linux platform. The Docker script is written with the CentOS as the base operating system. VMware supports separate (explicit) Docker containers for each product, so individual Docker scripts are written such that, on execution only the respective product gets installed.

Installation prerequisites

Fulfill the following prerequisites before starting the docker installation:

- Ensure that you have docker installed on your system.
- The response file, named <product>-response.txt and docker script file, are located in the ISO file in the /utils directory.
- The binary files are located in the ISO file in the /suite directory.
- Docker script includes few basic OS utilities that are required to execute the Smarts product functionality. Utilities like Telnet and SSH are required for CLI discovery process. Any additional utilities which is required for specific requirement, can be installed using “yum” inside container.

- Ensure that you placed the following mentioned files in any folder on your system:

Table 3-1. Files needed to install Smarts application in docker container.

Setup File	Response File	Docker File
setup-IP-10_0_0_0-linux64.bin	IP_NETWORK_SUITE-response.txt	IP_NETWORK_SUITE-Dockerfile.txt
setup-SAM-10_0_0_0-linux64.bin	SAM_SUITE-response.txt	SAM_SUITE-Dockerfile.txt
setup-CONSOLE-10_0_0_0-linux.bin	SAM_CONSOLE_SUITE-response.txt	SAM_CONSOLE_SUITE-Dockerfile.txt
setup-ESM-10_0_0_0-linux64.bin	ESM_SUITE-response.txt	ESM_SUITE-Dockerfile.txt
setup-MPLS-10_0_0_0-linux64.bin	MPLS_SUITE-response.txt	MPLS_SUITE-Dockerfile.txt
setup-NPM-10_0_0_0-linux64.bin	NPM_SUITE-response.txt	NPM_SUITE-Dockerfile.txt

Note The docker file creates the docker image with the help of above files mentioned in the table. In order to disable EDAA mode and change to the broker host, edit <product>-response.txt. Install using Unattended mode provides more information on installing the product using Unattended mode.

Creating and starting Docker image

You can create and start docker image for the VMware Smart Assurance Service Assurance Manager, VMware Smart Assurance IP Manager, VMware Smart Assurance MPLS Management Suite, VMware Smart Assurance Server Manager, and
VMware Smart Assurance Network Protocol Management Suite by using the following steps:

1 Run the following command, to build the docker image:

```
docker build -t <image-name> -f <docker file name> ./
```

2 Run the following command, to start the docker container in the host mode:

```
docker run -it --net=host --name <container name>  <docker-image-name>
```

3 Start the "ic-serviced" so that services can be created:

```
/etc/init.d/ic-serviced start
```

4 Start your servers with your environment specific options.

Operations on Docker container

You can perform various operations on docker container like add, remove, stop, and list the docker container or docker image in the system. The docker commands used in this chapter are docker specific and do not have any dependencies on Smarts product.

Note In docker there is nothing called uninstallation, you just need to remove the container and the image file from the system.

To remove the docker containers and the image files, you need to perform the following series of task:

1 Search for the list of container present on your system, run the following command to list the containers:

```
#docker ps –a
```

2 Run one of the following command, to attach the existing container (if any):

```
#docker attach <container ID>
or,
#docker attach <container name>
```

3 To stop the docker, run the following command:

- Invoke the following command, to stop all the containers running on your machine:

```
#docker stop $(docker ps –a –q)
#docker stop <container ID>
or,
#docker stop <container name>
```

4 To remove the container, run the following command:

- Invoke the following command, to remove all the containers on your machine:

```
#docker rm $(docker ps –a –q)
#docker rm <container ID>
or,
#docker rm<container name>
```

5 Search for the list of docker images present on your system, run the following command to list the docker image:

```
#docker images ––all
```

6 Invoke one of the following command, to remove the image:

```
#docker rmi <ImageID>
or,
#docker rmi <Image Name>
```

7 Invoke one of the following command in the Docker container to exit or stop the container:

```
#exit
Ctrl + C
Ctrl + \
```

Performing Smarts upgrade inside Docker

You can upgrade the VMware Smart Assurance Service Assurance Manager, VMware Smart Assurance IP Manager, VMware Smart Assurance MPLS Management Suite, VMware Smart Assurance Server Manager, and VMware Smart Assurance Network Protocol Management Suite in docker, by using the following steps:

1 Invoke the following command, to copy the build inside the docker container:

```
docker cp <build file> <container name>:<Path inside docker container>
```

2 Run the following command, to login to the docker container:

```
docker exec –it <container name> bash
```

3 To perform upgrade on the Linux platform, refer to Chapter 5 Performing an Upgrade.

Note The regular upgrade procedure needs to be followed once the files are copied inside the docker. An upgrade installation needs to triggered inside the docker.

NAS Installation and Startup

4

This chapter includes the following topics:

- Overview
- Installing and starting the HTTPS Adapter service

Overview

The NAS Extension is installed with the IP Availability Manager. After installation, the IP Availability Manager can discover NAS devices, and perform root cause and impact analysis on these devices.

Configuring the NAS Extension involves the tasks summarized in Steps for configuring the NAS Extension.

Table 4-1. Steps for configuring the NAS Extension

	Reference
If necessary, configure the HTTPS Adapter to support access to the managed Celerra devices.	For information about this requirement, refer to the “Configuring Control Station usernames and passwords” chapter in the VMware Smart Assurance IP Manager User Guide.
If necessary, configure external Control Station and Data Mover IP addresses.	For information about this requirement, refer to the “Configuring Control Station and Data Mover IP addresses” chapter in the VMware Smart Assurance IP Manager User Guide , which also refers you to the appropriate VMware documentation, if needed.
Install the HTTPS Adapter as a service and start the service.	*“Installing and starting the HTTPS Adapter service” on page 46*.
Start the IP Availability Manager.	*VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers*
Start the Global Manager.	VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers. For configuration information, refer to the VMware Smart Assurance Service Assurance Manager Configuration Guide.
Start the Global Console.	VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers.

Installing and starting the HTTPS Adapter service

The NAS Extension software includes an adapter process (the HTTPS Adapter), which probes the Celerra devices using the HTTPS/XML probe to obtain internal topology information. While the installation of this adapter is automatic, you must install the service and start it manually. Install the HTTPS Adapter as a service and start the service manually, as described next for UNIX.

Once started, the HTTPS Adapter registers with the Broker. The VMware Smart Assurance System Administration Guide provides more information about starting services.

UNIX:

To install the HTTPS Adapter as a service on UNIX, issue the following command:

```
# sm_service install --force --unmanaged --startmode=manual \
'--name=<service_name>' \
'--description=<Smarts description>' \
'BASEDIR/smarts/bin/sm_adapter_java'
'--name=<HTTPS_Adapter_Name>' \
'--output=<HTTPS_Adapter_Name>.log' \
'-J' \
'nas_probe.jar'
```

You can also specify the Broker and Port, if the IP Availability Manager with NAS Extension is registered with a Broker and Port other than the default, **localhost:426**. To do this, add the following arguments to the end of the command:

```
--broker=<IP Address or Hostname>:<Port Number>
```

To start the service, type the following command:

```
# BASEDIR/smarts/bin/sm_service start
         <service_name>
```

To stop the service, issue the following command:

```
# BASEDIR/smarts/bin/sm_service stop
         <service_name>
```

Running HTTPs adapter in FIPS mode

The NAS subsystem was changed to provide FIPS 140 support. Hence you need to download additional JAR (Java Archive) files, else errors are seen in the NAS log when you run NAS discovery.

Example

```
NAS Log Error Snippet:
MAIN_MSG-*-STDFD_OUT-stdout: javax.net.ssl.SSLException: java.security.InvalidKeyException: Illegal
key size
[June 17, 2011 6:37:49 PM GMT+05:30 +227ms] t@1084229984 platform
MAIN_MSG-*-STDFD_OUT-stdout:
at com.rsa.sslj.x.aJ.b(Unknown Source)
at com.rsa.sslj.x.aJ.a(Unknown Source)
at com.rsa.sslj.x.aJ.b(Unknown Source)
at com.rsa.sslj.x.aU.d(Unknown Source)
at com.rsa.sslj.x.aU.a(Unknown Source)
at com.rsa.sslj.x.aU.h(Unknown Source)
at com.rsa.sslj.x.cI.startHandshake(Unknown Source)
at com.smarts.nas_probe.ControlStationInterface.getSSLSocket(ControlStationInterface.java:314)
at com.smarts.nas_probe.ControlStationInterface.post(ControlStationInterface.java:75)
at com.smarts.nas_probe.ControlStationInterface.getReply(ControlStationInterface.java:58)
at com.smarts.nas_probe.XMP.NasXML(XMP.java:25)
Caused by: com.rsa.sslj.x.ax: java.security.InvalidKeyException: Illegal key size
at com.rsa.sslj.x.aJ.b(Unknown Source)
at com.rsa.sslj.x.cR.k(Unknown Source)
at com.rsa.sslj.x.t.f(Unknown Source)
at com.rsa.sslj.x.t$a.run(Unknown Source)
at com.rsa.sslj.x.aJ$a$a.run(Unknown Source)
at java.security.AccessController.doPrivileged(Native Method)
at com.rsa.sslj.x.aJ$a.run(Unknown Source)
... 7 more
[June 17, 2011 6:37:49 PM GMT+05:30 +229ms] t@1084229984 platform
MAIN_MSG-*-STDFD_OUT-stdout: e
Caused by: java.security.InvalidKeyException: Illegal key size
at javax.crypto.Cipher.a(DashoA13*..)
at javax.crypto.Cipher.init(DashoA13*..)
at javax.crypto.Cipher.init(DashoA13*..)
at com.rsa.sslj.x.Y.<init>(Unknown Source)
......
```

With BSAFE SSL-J, some of the FIPS 140 cryptographic algorithms require Unlimited Strength Jurisdiction Policy Files.

Unlimited Strength Jurisdiction Policy JAR Files for NAS discovery

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

1. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8 from the Oracle website.
2. Extract the local_policy.jar and US_export_policy.jar files from the downloaded zip file.
3. Go to the smarts/jre/lib/security directory and then back up the existing policy files in this path.

4 Overwrite the local_policy.jar and US_export_policy.jar files to the smarts/jre/lib/security directory.

Note If you want to switch back from FIPS mode to non-FIPS mode, reset SM_FIPS140 to FALSE. You do not need to remove the Unlimited Strength Jurisdiction Policy Files.

Performing an Upgrade

5

This chapter includes the following topics:

- Upgrade installation overview
- Upgrade installation prerequisites
- Upgrade the product
- Upgrading Smart Assurance products in FIPS mode
- Next steps

Upgrade installation overview

This chapter describes how to perform an upgrade installation for the IP Manager, Service Assurance Manager, MPLS Management Suite, Server Manager, and Network Protocol Manager. An upgrade installation applies a new version of software to an existing version in the same directory on the same host. An “upgrade installation” is also known as an “in-place upgrade.” During an upgrade installation, new product services are not available to install, unless you select additional products during the upgrade procedure.

You can upgrade the versions of software listed in the VMware Smart Assurance SAM, IP, ESM, MPLS, and NPM Managers Support Matrix to Version 10.0 using the in-place upgrade instructions provided in this chapter.

The upgrade installation flow is shown in Upgrade installation flowchart.

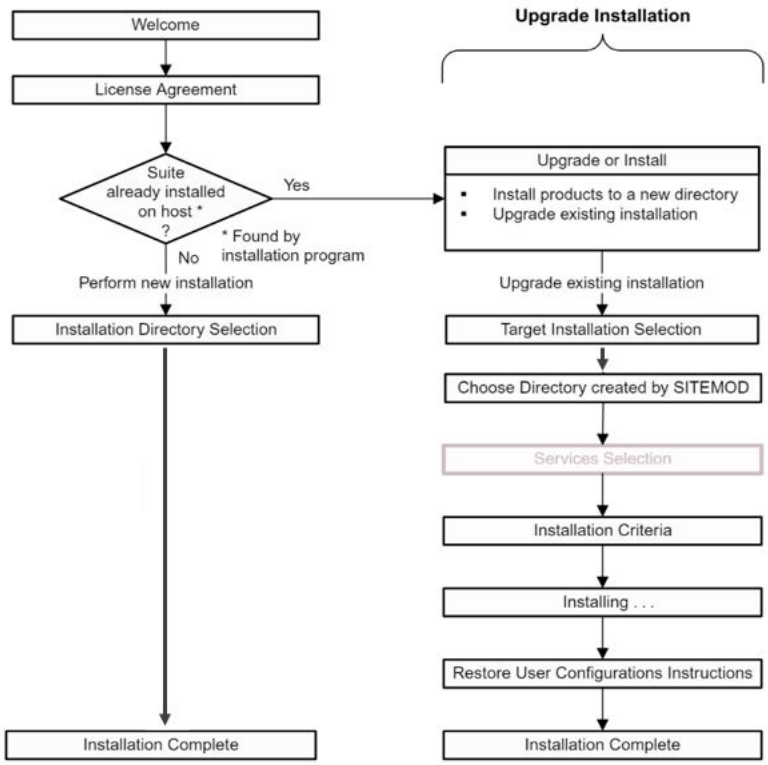
1 Start with the top-most SAM server.

2 An Aggregation SAM server if it is a hierarchical SAM deployment.

3 IP Manager.

4 Any order: Server Manager, MPLS Manager and Network Protocol Manager.

Figure 5-1. Upgrade installation flowchart



Installer tasks

During an upgrade installation, the installation program performs the following tasks:

1 All the smarts services needs to be stopped before upgrade or new installation. Use sm_service command to stop the services manually.

   ./sm_service stop <SERVICE NAME>

2 Creates a backup copy of your customizations in the <BASEDIR>/smarts/.migrate.bkp.<version> directory.

3 Removes the patch, if any, from the existing installation.

4 Installs the software.

5 Prompts you to merge your customizations files in the BASEDIR>/smarts/.migrate.bkp.<version> directory to the BASEDIR/smarts/local directory.

Note If the broker is running on the host with a IP Manager, then it will have to be stopped during an upgrade. The broker has to be stopped to prevent the impact on all the other applications running on the system.

Installer-called utilities

The installation program invokes the sm_migrate utility to backup the existing user-customized files and base files. It also presents the sm_migrate command to be run after the 10.0.0 installation to complete a three-way merge of the following sets of files:

- Existing user-customized files in the <BASEDIR>/smarts/.migrate.bkp.<version> directory.
- Existing base files in the <BASEDIR>/smarts/.migrate.bkp.<version> directory.
- 10.0.0 base files in the BASEDIR/smarts directory

  The sm_migrate utility invokes another utility, the sm_merge utility, for each of the files that requires a three-way merge. Chapter 7 Migration Utilities explains how the sm_migrate and sm_merge utilities work.

Upgrade installation prerequisites

Fulfill the following prerequisites before starting the upgrade installation:

- Ensure that you have superuser (User ID 0) or administrative privileges on the target host. The installation program will halt if you do not have the appropriate privileges.
- Ensure that the required operating system patches have been installed. Clicking **More Information** during the installation process will launch the System Information window and the Pass/Fail status of the operating system patches. The *VMware Smart Assurance Support Matrix* provides information on operating system patches.
- Remove all the unused files in the /local directory. The unused files will also include RPS files and custom files created by you. The upgrade process uses the sm_migrate utility that creates a backup of all the files in the local directory and copies them back to local directory after the upgrade. RPS and custom files can be large, and may slow down the process.
- Disk space requirement—During an upgrade installation, the installer creates a backup of files in actions, conf, model, repos, rules, script directories. Ensure that you have disk space of twice the size of these directories available on the system. After the upgrade and verifying the installation, you can archive or remove the backup directories. This requirement is in addition to the minimum disc requirement outlined for each product in the *VMware Smart Assurance Support Matrix*.

Upgrade the product

You upgrade each product in one of three ways: CLI mode or Unattended mode.

Perform the following tasks:

1. Review the important release issues found in your product-specific release notes.
2. On the host where the target existing installation resides, log in as superuser (User ID 0) or administrator.
3. Mount the CD/DVD-ROM. Chapter 12 Procedures for CD/DVD-ROMs provides more information.

4 Choose CLI mode (UNIX only), or Unattended mode. The **setup** commands for invoking CLI mode and Unattended mode are listed in Upgrade the product, Upgrade the product, and Upgrade the product.

- In CLI mode, make the following additional selections:
  - In the **Upgrade or Install** screen, select **Upgrade existing suite** and click **Next** or enter [**1**].
    - In the **Target Installation Selection** screen (in which an existing product is selected unless the product was previously installed to more than one directory, in which case you will see multiple choices), select a target installation directory and click **Next** or enter [**1**].
    - In the **Choose Products** screen, all of the existing products are selected to be upgraded. You can select additional products to add to the installation.
    - Specify any additional local directories created using SM_SITEMOD. Click **Next** or enter [**1**].
  - In Unattended mode, specify the following additional options in the response file (<product>-response.txt). All previously installed products must have their product options set to “true” in the response file.
    - Uncomment the **-INSTALL_TYPE.INSTALL_CHOICE** option.
    - Uncomment the **-SITEMOD_BEAN.SITEMODS_VAR** option, and provide one or more directory locations to perform an upgrade. You can provide the name of the directories, or the directory name with absolute path.

      For example, on Linux:

      SITEMOD_BEAN.SITEMODS_VAR=local-1:/opt/InCharge/SAM/smarts/Local-2

      :local-3

      Note For specifying directory separators, use : on Linux.
    - Uncomment the **MERGE_OPTION_UPGRADE.MERGE_CHOICE=MERGE** option to perform the merge.
    - Uncomment the **<** *product* **>.installLocation** option and set its property value to the installation directory of the target installation.

5 The installation program displays the **Directories created using SM_SITEMOD** screen which allows you to back up local directories that were created with SM_SITEMOD. If you used SM_SITEMOD to create local directories, enter a list of local directories. Click **Next** or enter [**1**].

The installation program then runs the sm_migrate utility to create a backup file of the user-customized files and base files in the existing installation. The backup file, named .migrate.bkp.<version>, is saved to the BASEDIR/smarts directory.

6 The installation program removes the patch, if any, from the existing installation and installs the software.

7 After the installation, the installation program shows the **Restore User Configurations Instructions** screen, which presents the sm_migrate command for restoring the old user-customizations in the .migrate.bkp.<version> backup file to the BASEDIR/smarts/local directory. The screen provides two options:

   a **Yes, merge the files** - Select this option if you want the utility to automatically merge the files modified by you.

   b **No, I will merge them later** - Select this option if you want to manually merge the files modified by you.

   Click **Next** or enter [**1**] to view the **Installation Summary**.

   Note For Service Assurance Manager, the upgrade process inserts the _edaa user entry into the security configuration file serverConnect.conf and the runcmd_env.sh file. The upgrade process does not modify the clientConnect.conf, brokerConnect.conf, and imk.dat files. The upgrade process does not insert the _edaa user entry into the files of Domain Managers.

   For Domain Managers, copying the security configuration files clientConnect.conf, serverConnect.conf, brokerConnect.conf, runcmd_env.sh, and imk.dat is not supported in an upgrade installation. You can manually copy the security configuration files using sm_migrate utility as described in Restoring customizations after an upgrade installation.

8 The **Installation Summary** shows informational messages such as successful confirmations, error messages, and warnings. Investigate any errors or warnings.

   If **Next** appears, your system needs to be rebooted because one or both of the following tasks are pending on the system:

   - A system-protected file was replaced during the installation and requires a restart.
   - A pending restart was triggered by another application or by an operating system patch installation.

     Click **Next** or enter [**1**] and then reboot your system. Otherwise, click **Finish** or enter [**1**] to exit the installation.

     The installation program writes an install log file to the BASEDIR/smarts/setup/logs directory, unless the installation fails at the very start, in which case the installation program writes the log file to the /tmp directory. The log file is a text file with the naming convention Install.<product>.<productversionNumber>.log.

9 Evaluate your custom code. Review the Custom file migration use cases. The sm_migrate utility migrated all user-customized files from the existing installation to the BASEDIR/smarts/local directory in the 10.0.0 installation. Review the output of the sm_migrate utility and evaluate if you would like to keep the user-customized files in the new installation.

   Configuration migration process logs provides more information on the log files that are created after the migration of user-customized files.

10 Depending on your deployment, ensure that the *BASEDIR/smarts/local/conf/runcmd_env.sh* file includes the environment variables, SM_TLS_PROTOCOLS and SM_ALLOW_LEGACY_CRYPTO.

   Use SM_TLS_PROTOCOLS set to the +TLSv1.1 value only if you need to interoperate with Smarts products based on Foundation 9.0.0.0 Build 1345 through 9.2.x.

   Use SM_ALLOW_LEGACY_CRYPTO set to TRUE only if you need to interoperate with Smarts products based on Foundation versions prior to 9.0.0.0 Build 1345.

   Check the version number provides the sm_server **--**version command to determine the Foundation (DMT) version.

   To ensure that the runcmd_env.sh file includes the environment variables:

   a Go to the *BASEDIR/smarts/bin* directory and enter this command to open the runcmd_env.sh file:

```
sm_edit conf/runcmd_env.sh
```

   b Search for the environment variables. If they do not exist, add one or both depending on your deployment:

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

   c Save and close the file.

11 Optional for IP Manager, run the repository file migration utility (**sm_migraterps**) to make the repository file compatible with the newer 10.0.0 version of the software as described in Automatically migrate topology for IP Manager using RPS utility.

12 If your product is part of a deployment that requires the Federal Information Processing Standard (FIPS) Publication 140-2, a U.S. government computer security standard governing cryptographic modules, follow the instructions in Upgrading Smart Assurance products in FIPS mode.

13 If you installed the products as services, start the services. Starting services on UNIX provides more information.

14 Verify the current state of the products and Broker. Verify the product status provides more information.

15 Initiate a discovery. Consult the discovery guide or user guide for your product for more information on this procedure.

16 For Server Manager,

   a In the Domain Manager Administration Console, right-click on the ESM server (INCHARGE-ESM, by default) in the left pane and select the **Load All ESM Host monitoring data from Backup** option.

   b Perform a discovery (**Topology > Discover All**) from the ESM server.

      All of the applications that were configured prior to the upgrade are restored and Server Manager starts to monitor those applications.

Upgrading Smart Assurance products in FIPS mode

Note Upgrading in FIPS mode is not available for Server Manager.

10.0.0 products do not use a Federal Information Processing Standard (FIPS 140-2) approved encryption algorithm to protect the imk.dat file. By default, the 10.0.0 imk.dat file uses MD5, which is not a FIPS-approved algorithm. Hence, while upgrading from previous versions of products to Version 10.0.0, the imk.dat file needs to be regenerated in order to run in the FIPS mode.

In order to convert an existing installation to FIPS, use the sm_rebond (in non-FIPS mode) first to get everything re-encoded in a FIPS compatible way. The steps are as follows:

1 Run the following command at the command line prompt:

```
sm_rebond --upgrade --basedir=<
BASEDIR
>/smarts
sm_rebond --upgrade --basedir=C:\InCharge\SAM\smarts
```

2 When prompted, type a password to regenerate the imk.dat file. The default password is *Not a secret*.

3 Set the value for the parameter **SM_FIPS140** to **TRUE** in the *runcmd_env.sh* file. The file is located under the *BASEDIR/smarts/local/conf* directory.

Next steps

Chapter 8 Verifying the Installation describes tasks for verifying the proper installation of the software and starting services.

Performing a Migration

6

This chapter includes the following topics:

- Migration overview
- Install and migrate on the same host
- Install and migrate on a different host
- Post-migration tasks

Migration overview

Consult the VMware Smart Assurance SAM, IP, ESM, MPLS, and NPM Managers Support Matrix for software versions that require a manual migration to the latest version.

Two methods are available:

- Install and migrate on the same host
- Install and migrate on a different host

  After the installation, run the sm_migrate utility to backup the user-customized files in the previous version and migrate the files to the new version. Chapter 7 Migration Utilities explains how the sm_migrate utility works.

  Disk space requirement—During a migration, the sm_migrate creates a backup of files in actions, conf, model, repos, rules, script directories. Ensure that you have disk space of four times the size of these directories available on the system. After the migration and verifying the installation, you can archive or remove the backup directories. This requirement is in addition to the minimum disk requirement outlined for each product in the
  VMware Smart Assurance SAM, IP, ESM, MPLS, and NPM Managers Support Matrix.

  Server name requirement for migration—To preserve notification history and the original Source attributes of notifications in the Service Assurance Manager, the server names of underlying Domain Managers should remain the same. This way at the end of the migration of all Smarts Domain Managers, the SAM server can correctly associate the pre-existing topology and notifications with the topology and events coming from migrated Domain Managers. For example, if the Server Manager has a server name INCHARGE-ESM, do not change it to a different name for the latest release.

Make sure that you read *Install and migrate on the same host* and *Install and migrate on a different host* in their *entirety before proceeding*.

Note Remove all the unused files in the /local directory. The unused files will also include RPS files and custom files created by you. The sm_migrate utility creates a backup of all the files in the local directory and copies them back to local directory. RPS and custom files can be large, and may slow down the process.

Install and migrate on the same host

To migrate from a previous version of a product to the new, current version on the same host, you must:

1. Install the product and specify an installation directory that is different from the one that is used for the previous installation.
2. Stop the old services for the previous version, if necessary.

   For UNIX, keep the service daemon (the sm_serviced component) running. If sm_serviced is stopped, all VMware Smart Assurance products will stop and will need to be restarted.

   For most cases, the installation program detects and stops all services, scheduled jobs, and processes that use programs or libraries that are running from the existing installation.

   It also stops the service daemon, sm_serviced, if it is running.
3. Migrate user-customized files from the previous installation to the new installation.
4. Reuse the customized Polling and Thresholds settings from the old repository.

   Detailed instructions are described in Migration procedure for the same host.

   For a test lab environment, since the two installations are on the same host, you can run both installations in parallel. For parallel installations, both installations connect to the same Broker and Global Manager, as long as the old and new product service and sm_server names are unique. In this case, you will need to rename the service and sm_server for the previous product version. Managers registered with the same Broker must have unique names.

   For a production environment, VMware, Inc. recommends that you decommission the previous version of product.
5. Start with the top-most SAM server.
6. An Aggregation SAM server if it is a hierarchical SAM deployment.
7. IP Manager.
8. Any order: Server Manager, MPLS Manager, and Network Protocol Manager.

Migration procedure for the same host

To migrate the previous version of the product to the new version on the same host, perform the following tasks:

1. Review the important release issues for the product, as described in the VMware Smart Assurance IP Manager Release Notes.
2. Determine that the products that you are installing are supported for your platform. The VMware Smart Assurance SAM, IP, ESM, MPLS, and NPM Managers Support Matrix provides more information.
3. Determine if the host has enough disk space and memory to accommodate so both versions of the product can co-exist. The VMware Smart Assurance SAM, IP, ESM, MPLS, and NPM Managers Support Matrix provides more information.
4. Mount the CD/DVD-ROM on the host as described in Chapter 12 Procedures for CD/DVD-ROMs
5. Uninstall any temporary test patches (TTPs), if they exist, in your old installation.

   If a TTP has been installed on a Service Pack, you must first uninstall the TTP. Otherwise, the TTP files will be treated as files modified by you and copied to the local directory in the new installation area.
6. Install the new version of the product on the same host as described in Chapter 2 Performing an Installation
   - Specify an installation directory that is different from the old installation directory so both versions of the product can co-exist.
     - Install products as services. These services overwrite the old stopped services.

       Note If you need to continue to run the previous versions of the products, manually install services for them with unique names and start them.

       The installation program installs the software.
7. Run the sm_migrate utility to copy user-customized files from the previous installation to the new installation. Migrating customizations on the same host provides instructions.

   Note Run the sm_migrate utility immediately after the installation and before you start any services or modify any files in the new installation. The sm_migrate utility will not merge any files from the previous installation local directory, if the same files are present in the new installation BASEDIR/smarts/local directory.
8. Evaluate your security settings. Migration of security configuration files provides more information.
9. Evaluate the environment variables in the old runcmd_env.sh file. Migration of security configuration files provides more information.

10 Evaluate your custom code. Review the Custom file migration use cases to plan your post-migration steps. The sm_migrate utility migrated all user-customized files from the previous installation to the BASEDIR/smarts/local directory in the new installation. It also made a backup copy of the files under the BASEDIR/smarts/.migrate.bkp.x.x directory (for example, .migrate.bkp.2.0.0.0). Review the output of the sm_migrate utility and evaluate if you would like to keep the user-customized files in the new installation.

11 Depending on your deployment, ensure that the *BASEDIR/smarts/local/conf/runcmd_env.sh* file includes the environment variables, SM_TLS_PROTOCOLS and SM_ALLOW_LEGACY_CRYPTO.

   Use SM_TLS_PROTOCOLS set to the +TLSv1.1 value only if you need to interoperate with Smarts products based on Foundation 9.0.0.0 Build 1345 through 9.2.x.

   Use SM_ALLOW_LEGACY_CRYPTO set to TRUE only if you need to interoperate with Smarts products based on Foundation versions prior to 9.0.0.0 Build 1345.

   Check the version number provides the sm_server **--**version command to determine the Foundation (DMT) version.

   a Go to the *BASEDIR/smarts/bin* directory and enter this command to open the runcmd_env.sh file:

   ```
   sm_edit conf/runcmd_env.sh
   ```

   b Search for the environment variables. If they do not exist, add one or both depending on your deployment:

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

   c Save and close the file.

12 Rename the repository file before reusing it.

   a Locate the existing repository file that was copied to the BASEDIR/smarts/local/repos/icf directory in the new 10.0.0 installation.

   b Rename the repository file by removing the version number extension. For example, the repository file INCHARGE-MPLS-ANALYSIS.rps.3.1.0.2 should be renamed to INCHARGE-MPLS-ANALYSIS.rps without the version number extension.

13 Optional for IP Manager, run the repository file migration utility (**sm_migraterps**) to make the repository file compatible with the newer 10.0.0 version of the software as described in Automatically migrate topology for IP Manager using RPS utility.

14 If you installed the products as services, start them for the first time. Starting services on UNIX provide more information.

15 Verify the current state of the products and Broker. Verify the product status provides more information.

16 For Server Manager,

   a In the Domain Manager Administration Console, right-click on the ESM server (INCHARGE-ESM, by default) in the left pane and select the **Load All ESM Host monitoring data from Backup** option.

   b Perform a discovery (**Topology > Discover All**) from the ESM server.

   All of the applications that were configured prior to the migration are restored and Server Manager starts to monitor those applications.

17 Decommission the previous version of the products. For instructions, refer to the uninstallation chapter in the installation guide for the previous software version.

Install and migrate on a different host

If you want to run the new version of the 10.0.0 product before decommissioning the previous version, you must:

1 Install the new version of the 10.0.0 product on a different host.

2 Migrate any customized configuration file changes to the new installation.

   Detailed instructions are described in Migration procedure for a different host.

   Since the two installations are on different hosts, you can run both installations in parallel. You have the option of:

   - Having both installations connect to the same Global Manager and Broker.

     Managers registered with the same Broker must have unique names. In this scenario, stop and rename the services for the previous version and, when you install the 10.0.0 product, the installation program will use the default server names.

   - Having multiple instances of the Global Manager and Broker with each instance assigned to a different version of the product.

     For a production environment, VMware, Inc. recommends that you decommission the previous version of product.

3 Start with the top-most SAM server.

4 An Aggregation SAM server if it is a hierarchical SAM deployment.

5 IP Manager.

6 Any order: Server Manager, MPLS Manager, and Network Protocol Manager.

Migration procedure for a different host

To migrate the previous version of the product to the new version on a different host, satisfy or perform the following tasks:

1 Review the important release issues for the 10.0.0 product, as described in the VMware Smart Assurance IP Manager Release Notes.

2 Determine that the products that you are installing are supported for your platform. The VMware Smart Assurance SAM, IP, ESM, MPLS, and NPM Managers Support Matrix provides more information.

3 Determine if the host has enough disk space and memory to accommodate so both versions of the product can co-exist. The VMware Smart Assurance SAM, IP, ESM, MPLS, and NPM Managers Support Matrix provides more information.

4 Mount the CD/DVD-ROM on the host as described in Chapter 12 Procedures for CD/DVD-ROMs

5 Uninstall any temporary test patches (TTPs), if they exist, in your old installation.

   If a TTP has been installed on a Service Pack, you must first uninstall the TTP. Otherwise, the TTP files will be treated as files modified by you and copied to the local directory in the new installation area.

6 Install the new version of the product on the different host as described in Chapter 2 Performing an Installation

   The installation program installs the 10.0.0 software.

7 Run the sm_migrate utility to copy user-customized files from the previous installation to the new 10.0.0 installation. Migrating customizations to a different host provides instructions.

   Note Run the sm_migrate utility immediately after the installation and before you start any services or modify any files in the new installation. The sm_migrate utility will not merge any files from the previous installation local directory, if the same files are present in the new installation BASEDIR/smarts/local directory.

8 Evaluate your security settings. Migration of security configuration files provides more information.

9 Evaluate the environment variables in the old runcmd_env.sh file. Migration of security configuration files provides more information.

10 Evaluate your custom code. Review the Custom file migration use cases to plan your post-migration steps. The sm_migrate utility migrated all user-customized files from the previous installation to the BASEDIR/smarts/local directory in the new installation. It also made a backup copy of the files under the BASEDIR/smarts/.migrate.bkp.x.x directory (for example, .migrate.bkp.2.0.0.0). Review the output of the sm_migrate utility and evaluate if you would like to keep the user-customized files in the new installation.

11 Depending on your deployment, ensure that the *BASEDIR/smarts/local/conf/runcmd_env.sh* file includes the environment variables, SM_TLS_PROTOCOLS and SM_ALLOW_LEGACY_CRYPTO.

   Use SM_TLS_PROTOCOLS set to the +TLSv1.1 value only if you need to interoperate with Smarts products based on Foundation 9.0.0.0 Build 1345 through 9.2.x.

   Use SM_ALLOW_LEGACY_CRYPTO set to TRUE only if you need to interoperate with Smarts products based on Foundation versions prior to 9.0.0.0 Build 1345.

Check the version number provides the sm_server **--**version command to determine the Foundation (DMT) version.

a Go to the *BASEDIR/smarts/bin* directory and enter this command to open the runcmd_env.sh file:

```
sm_edit conf/runcmd_env.sh
```

b Search for the environment variables. If they do not exist, add one or both depending on your deployment:

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

c Save and close the file.

12 Rename the repository file before reusing it.

a Locate the existing repository file that was copied to the BASEDIR/smarts/local/repos/icf directory in the new 10.0.0 installation.

b Rename the repository file by removing the version number extension. For example, the repository file INCHARGE-MPLS-ANALYSIS.rps.3.1.0.2 should be renamed to INCHARGE-MPLS-ANALYSIS.rps without the version number extension.

13 Optional for IP Manager, run the repository file migration utility (**sm_migraterps**) to make the repository file compatible with the newer 10.0.0 version of the software as described in Automatically migrate topology for IP Manager using RPS utility.

14 If you installed the products as services, start them for the first time. Starting services on UNIX provide more information.

15 Verify the current state of the products and Broker. Verify the product status provides more information.

16 For Server Manager,

a In the Domain Manager Administration Console, right-click on the ESM server (INCHARGE-ESM, by default) in the left pane and select the **Load All ESM Host monitoring data from Backup** option.

b Perform a discovery (**Topology > Discover All**) from the ESM server.

All of the applications that were configured prior to the migration are restored and Server Manager starts to monitor those applications.

17 Decommission the previous version of the products. For instructions, refer to the uninstallation chapter in the installation guide for the previous software version.

Post-migration tasks

Perform these tasks after the data migration steps are complete:

1 Rename the repository file

2 Ensure that the Broker host:port is updated in the runcmd_env.sh files

3 Remove the old out-of-date service entries

4 Change the secret phrase to match rest of deployment

5 Uninstall the old software

Rename the repository file

For a same host or different host migration, the old repository file is copied to the BASEDIR/smarts/local/repos/icf directory in the 10.0.0 installation. Because the repository file has a version number extension (for example, .2.0 extension), rename the repository file without the .2.0 extension before using it.

As further information, regardless of whether the old installation is on a UNIX system, sm_migrate saves the old repository file and all other customization files in DOS format. If the new installation is on a UNIX system, sm_migrate automatically converts the repository file and all other customization files to UNIX format.

Ensure that the Broker host:port is updated in the runcmd_env.sh files

If you are installing the 10.0.0 Broker during the installation to a location that is different from where the Broker for the previous installation resides, for each server that is registered with the Broker, you need to use the sm_edit utility to edit the SM_BROKER_DEFAULT variable in the runcmd_env.sh file in each of those server's BASEDIR/smarts/local/conf directory with the hostname (and port) of the host system that is running the Broker:

If the Broker host is resolved using a DNS name, this step is not necessary. It is recommended not to use Name Server Caching Daemon (NSCD) to cache DNS lookups (the host's database) in Linux.

1 Run BASEDIR/smarts/bin/sm_service show --cmdline (UNIX).

2 For each service that you have installed, you will see output similar to the following:

```
sm_service install --force --name=ic-broker
--description="VMware Broker" --env=SM_CLIENTCONNECT=brokerConnect.conf --startmode=runonce
C:\InCharge\IP\smarts\bin\brstart.exe --port=426 --
restore=C:\InCharge\IP\smarts/local/repos/broker/broker.rps --output
```

Remove the old out-of-date service entries

Use the following command to remove all old services that are going to be replaced by the 10.0.0 product:

```
<BASEDIR>
/smarts/bin/sm_service remove
<service name>
```

For UNIX, you need to point the product to the new 10.0.0 services that will be installed. Do this by making a copy of /etc/init.d/ic-serviced, change the SMHOME variable to point to the 10.0.0 services, and place it in the 10.0.0 /etc/init.d directory.

Change the secret phrase to match rest of deployment

If the rest of the deployment uses a different site secret, and assuming that you want to employ secure communications between the component applications in the deployment, you need to change the site secret of this installation to match the rest of deployment. You do so by using the deployment's site secret to recreate and encrypt the clientConnect.conf, serverConnect.conf, brokerConnect.conf, and .imk.dat files in the BASEDIR/smarts/local/conf directory of this installation.

Use the sm_rebond command to encrypt the files. For example, from the BASEDIR/smarts/bin directory, enter:

```
sm_rebond --basedir=/opt/InCharge/IP/smarts
```

The *VMware Smart Assurance System Administration Guide* provides complete information about the security files and encryption.

Uninstall the old software

If the new version of the product is functioning properly, all data has been migrated to the new version, and all services are functioning properly, you should uninstall the previous version of the product.

Uninstalling the previous version of the product will prevent conflicts if the previous version is started by mistake while 10.0.0 is running. Chapter 9 Performing an Uninstallation provides more information.

Uninstall will display errors if services were installed by the installation program when the old version was installed, but were removed manually in a later step. The uninstall process will display errors because it will not find the services when it tries to remove them.

Migration Utilities

7

This chapter includes the following topics:

- Customization migration utility overview
- sm_migrate function
- Customization migration procedures
- Perform a rollback
- Custom file migration use cases
- Three-way merge utility
- Automatically migrate topology for IP Manager using RPS utility
- Deployment utility overview

Customization migration utility overview

The sm_migrate utility is used to migrate user-customized files from an old installation to a new installation, where the old installation and the new installation are in different installation directories or, for an upgrade installation, in the same installation directory. User-customized files include user-modified files (using sm_edit), user-introduced files, and the repository file.

Note If TTPs (Temporary Test Patch) are installed on a previous installation of SAM, you must first uninstall the TTP and then run the utility. Else, TTP files will be treated as files modified by you and copied to the local directory in the new installation area.

When migrating a customized file from an old installation to a new installation, if a file with the same name exists in the local directory of the new installation, the Customization Migration Utility does not modify or overwrite it. The utility skips all such files being considered for merging. For files being considered to be copied-over, the utility migrates the files with the old version number appended to the file name.

sm_migrate modes of operation

The sm_migrate has seven command-line options:

- --old (or -o)

- --new (or -n)
- --archive (or -a)
- --upgrade (or -u)
- --rollback (or -r)
- --silent (or -s)
- --sitemod (or -l)
- --help (or -h)

  These command-line options can be used in pairs in the command line to achieve eight different modes of operation described below.

SAME HOST MODE

This mode is used when the new installation and the old installation are on the same host, in two separate locations. In this mode, sm_migrate migrates all customizations (non-binary files that have been modified or introduced by you in the old installation) from the old installation to a new installation.

Note All files that were modified or newly introduced in the old installation must be present only under the BASEDIR/smarts/ directory.

When you use the --sitemod option, the migration utility will migrate all customized old files for all user created locals.

DIFFERENT HOST - OLD MODE

This mode is used when the new installation and the old installation are on different hosts. In this mode, sm_migrate backs up and creates tar or a zip archive (file) of the customizations in the old installation. The tar or zip file resides in the location specified by you while executing the utility.

Note To run the utility from an older version of a Smarts product that does not have the migration utility, you must copy the sm_migrate.pl script and certain Perl files (packaged in migratePerlPkg.zip file) and place them in the appropriate locations. The sm_migrate.pl must be placed in the bin directory and the Perl package must be placed under the BASEDIR/smarts/local folder and extracted there.

When you use the --sitemod option, the migration utility will migrate all customized old files for all user created locals.

After running DIFF_HOST_OLD mode and before running DIFF_HOST_NEW mode, you must manually move the tar or zip archive from the old host to the new host, preferably under the smarts directory of your new installation.

DIFFERENT HOST - NEW MODE

This mode is also used when the new installation and the old installation are on different hosts. In this mode, sm_migrate migrates the customizations from the tar or zip archive that was created in the old installation to the local directory under the new installation and attempts to merge the files from your new installation with the files present in the backup archive wherever applicable, and places them in your new local directory.

UPGRADE MODE

This mode is used during an in-place upgrade, where the installer creates a backup of the files modified or newly introduced by you in the old installation into a .migrate.bkp.<old_version> backup directory and merges them into a new installation. This mode has been designed for the installer, but can be invoked by you too.

Note This mode must not be invoked by you if there are multiple .migrate.bkp.<version> directories under the <BASEDIR/smarts directory.

ROLLBACK MODE

In any execution of the migration utility, before the utility migrates your customizations from the backup directory to your new installation, it creates a backup of certain files in your current new local and stores it in a .rollback_<version_timestamp> directory. Also, it records the version and timestamp before any migration.

The rollback option allows you to reverse the changes made by the migration utility by restoring the local version in your new installations using files from the .rollback_<version_timestamp> directory. Rollback will contain only those locals which are part of migration.

Note In some scenarios, if a file is copied to the new installation with .<old_version> extension, then this file is not deleted when a rollback is performed.

The rollback action is restricted only to rollback points that were recorded in your current version. For example if you upgrade from 9.4.0.0 to 9.5.0.0, and then install a patch (for example, 9.5.0.1), the rollback utility will not allow you to rollback to your 9.5.0.0 local version. You have to manually uninstall the patch in order to rollback to 9.5.0.0.

Note You can use the rollback option only after an in-place upgrade or if you have previously run the migration utility either in the SAME_HOST, DIFFERENT_HOST or UPGRADE_NEW modes.

Perform a rollback on page 90 describes the procedure for carrying out a rollback.

sm_migrate function

The customization migration utility is capable of four major functions, which include:

- Copying all non-binary files from the <BASEDIR>/smarts/local folder that have been modified or introduced by you in the previous version of the product into the appropriate backup directories under the <BASEDIR>/smarts directory of the new installation. Details of backup folders created by sm_migrate utility provides details on the backup directories created by the utility during the migration and upgrade process.

Table 7-1. Details of backup folders created by sm_migrate utility

Scenario	Name and location of backup folders under <BASEDIR>/smarts
Migration on same host	.migrate.bkp.<old_version>, .rollback_<version_timestamp>
Migration on different host old mode	user-defined tar or zip file name,
Migration on different host new mode	.rollback_<version_timestamp>, .migrate.bkp.<old_version>
Upgrade	.migrate.bkp.<old_version>, .rollback_<version_timestamp>

For files that have been modified by you, the utility also creates a copy of the base files from the <**BASEDIR**>/smarts folder. These files are backed up into .migrate.bkp.<old_version> directory. The original and the local versions of the files from the old installation will be needed when the utility attempts to merge your changes with the new installation files.

Under the smarts/.migrate.bkp.<old_version> and backup.tar or backup.zip directory you can find files with the following extensions:

- .custom - files from the <**BASEDIR**>/smarts/local folder introduced by you and are not part of the default installation
  - .local - files from the <**BASEDIR**>/smarts/local folder that are part of the default installation and have been modified from their original version, using sm_edit.
  - .base - the <**BASEDIR**>/smarts version of these files with .local extension

    Custom file migration use cases provide details.
- Copying the cacert.sso certificate file from <**BASEDIR**>/smarts/jre/lib/security directory into the .migrate.bkp.<old_version>/jre/lib/security directory to retain the certificate file.
- Copying all files you have added into the <**BASEDIR**>/smarts/local folder of the new installation. This allows for an easy and automatic migration of all customer files to the new installation, so that no manual step is required for moving the files from the backup directory.

  Note All files, customized or newly introduced in the existing installation, must be present under the <**BASEDIR**>/smarts/ folder only. The utility also copies the RPS files found in the old_local.

- Merging .asl, .import, .conf, .xml, .pl, .sh and .cmd files modified by you into the new installation. The utility first backs up the corresponding files from the old_base, and then migrates the files from .migrate.bkp.<old_version> backup directory to the new installation.

  Note This is an optional function and you may skip it.

  In order to merge the configurations from the existing installation into the new installation, the utility uses files from:

  - Original base installation (previous installation with <file_name>.base extension)
  - Local directory of the previous installation (files you have modified with a <file_name>.local extension)
  - New installation (with <file_name> extension)

    The files to be merged are put in the new_local after performing a three-way merge between the two files in the backup directory and the corresponding file in the new base.

- Rolling back changes made by the sm_migrate utility in your current installation. It creates a backup of the new_local, and allows you to rollback to multiple stages of backup, as long as the changes were carried out in your current version. The backup consists of all .conf, .import, .asl, .mdl, .xml, .template, .sh, .conflict, .automerge, .cmd, .dat, and .bat files found in the new_local.

  Note Soft links created for product related files in the UNIX environment are not handled by sm_migrate utility.

Customization migration procedures

Run the sm_migrate utility immediately after the installation and before you start any services or modify any files in the new installation. Back up the BASEDIR/smarts/local directory in the new installation before you run sm_migrate.

Note When you run the sm_migrate utility, ensure that you run only one instance of sm_migrate utility.

Migrating customizations on the same host

Use the following steps to migrate customizations on the same host:

1. Go to the BASEDIR/smarts/bin directory of the new installation and type the following command on one line to invoke the sm_migrate utility:

```
sm_perl sm_migrate.pl --old=<BASEDIR>/smarts (old installation) --new=<BASEDIR>/smarts (new
installation) --sitemod=<BASEDIR>/smarts/local;local1
```

IP Manager

```
c:\InCharge93\IP\smarts\bin>sm_perl sm_migrate.pl
--old=c:\Incharge93\IP\smarts --new=c:\Incharge94\IP\smarts --sitemod=c:\Incharge94\IP\smarts\local1;
c:\Incharge94\IP\smarts\local2
```

Service Assurance Manager

```
c:\InCharge\SAM\smarts\bin>sm_perl sm_migrate.pl
```

MPLS Management Suite

```
c:\InCharge93\MPLS\smarts\bin>sm_perl sm_migrate.pl
--old=c:\Incharge93\MPLS\smarts --new=c:\Incharge94\MPLS\smarts --
sitemod=c:\Incharge94\MPLS\smarts\local1; c:\Incharge94\MPLS\smarts\local2
```

Server Manager

```
c:\InCharge\ESM\smarts\bin>sm_perl sm_migrate.pl
--old=c:\Incharge\ESM\smarts --new=c:\Incharge\ESM\smarts --sitemod=c:\Incharge94\ESM\smarts\local1;
c:\Incharge94\ESM\smarts\local2
```

Network Protocol Management Suite

```
c:\InCharge\NPM\smarts\bin>sm_perl sm_migrate.pl
--old=c:\Incharge\NPM\smarts --new=c:\Incharge\NPM\smarts --sitemod=c:\Incharge94\NPM\smarts\local1;
c:\Incharge94\NPM\smarts\local2
```

Migrating customizations to a different host

Use the following steps to migrate customizations on remote hosts:

1. Prepare to archive the customizations made in the old installation into a tar or zip archive by copying the following files:
   - **Perl packages**: Copy migrateperlpkg.zip from the BASEDIR/smarts/perl directory in the new installation to the BASEDIR/smarts/local directory of the old installation. For Linux and CentOS, use the unzip migrateperlpkg.zip command.
     - **sm_migrate.pl utility**: Copy this file from the BASEDIR/smarts/bin directory of the new installation to the BASEDIR/smarts/bin directory of your old installation.
2. Go to the BASEDIR/smarts/bin directory of your old installation and enter the following command on one line to generate an archive of the customizations:

```
sm_perl sm_migrate.pl --old=<BASEDIR>/smarts (old installation) --archive=<BASEDIR>/smarts/<tar or
zip file to contain customizations> ----sitemod==<BASEDIR>\smarts\local1; =<BASEDIR>\smarts\local2
```

IP Manager

```
c:\InCharge93\IP\smarts\bin>sm_perl sm_migrate.pl --old=c:\InCharge93\IP\smarts --
archive=c:\InCharge93\IP\smarts\backup.zip --sitemod=c:\InCharge93\IP\smarts\local1;c:\InCharge93\IP\
smarts\local2
```

Service Assurance Manager

```
c:\InCharge\SAM\smarts\bin>sm_perl sm_migrate.pl --old=c:\InCharge\SAM\smarts --
archive=c:\InCharge\SAM\smarts\backup.tar --sitemod=c:\InCharge\SAM\smarts\local1;c:\InCharge\SAM\
smarts\local2
```

MPLS Management Suite

```
c:\InCharge93\MPLS\smarts\bin>sm_perl sm_migrate.pl --old=c:\InCharge93\MPLS\smarts --
archive=c:\InCharge93\MPLS\smarts\backup.zip --
sitemod=c:\InCharge93\MPLS\smarts\local1;c:\InCharge93\MPLS\
smarts\local2
```

Server Manager

```
c:\InCharge\ESM\smarts\bin>sm_perl sm_migrate.pl --old=c:\InCharge\ESM\smarts --
archive=c:\InCharge\ESM\smarts\backup.tar --
sitemod=c:\InCharge\ESM\smarts\local1;c:\InCharge\ESM\smarts\
local2
```

Network Protocol Management Suite

```
c:\InCharge\NPM\smarts\bin>sm_perl sm_migrate.pl --old=c:\InCharge\NPM\smarts --
archive=c:\InCharge\NPM\smarts\backup.tar --sitemod=c:\InCharge\NPM\smarts\local1;c:\InCharge\NPM\
smarts\local2
```

IP Manager

```
c:\InCharge93\IP\smarts\bin>sm_perl sm_migrate.pl --archive=c:\InCharge93\IP\smarts\backup.zip --
new=c:\InCharge93\IP\smarts
```

Service Assurance Manager

```
c:\InCharge\SAM\smarts\bin>sm_perl sm_migrate.pl --archive=c:\InCharge\SAM\smarts\backup.tar --
new=c:\InCharge\SAM\smarts
```

MPLS Management Suite

```
c:\InCharge93\MPLS\smarts\bin>sm_perl sm_migrate.pl --archive=c:\InCharge93\MPLS\smarts\backup.zip --
new=c:\InCharge93\MPLS\smarts
```

Server Manager

```
c:\InCharge\ESM\smarts\bin>sm_perl sm_migrate.pl --archive=c:\InCharge\ESM\smarts\backup.tar --
new=c:\InCharge\ESM\smarts
```

Network Protocol Management Suite

```
c:\InCharge\NPM\smarts\bin>sm_perl sm_migrate.pl --archive=c:\InCharge\NPM\smarts\backup.tar --
new=c:\InCharge\NPM\smarts
```

Restoring customizations after an upgrade installation

During an upgrade, the installer creates a backup of your customizations and places them in the <BASEDIR>/smarts/.migrate.bkp.<version> directory.

If during the installation you choose to skip migrating the files back into your new local directory, you may either manually migrate or merge the files into your new local installation directory or run the sm_migrate utility in the UPGRADE mode to perform this action.

Use the following steps to run the **sm_migrate** utility:

1 Go to the <**BASEDIR**>/smarts/bin folder.

2 Type the following command to migrate the backup directory to the new installation:

```
./sm_perl sm_migrate.pl
--new=<new installation location up to and including smarts> --upgrade --silent
c:\InCharge\SAM\smarts\bin>sm_perl sm_migrate.pl
--new=c:\InCharge\SAM\smarts --upgrade
```

3 Press **y** or any other key to start the file merge utility (sm_merge utility), and then press **Enter**. The utility is invoked individually for each of the files that may require a three-way merge. Three-way merge utility provides details. Once the utility completes merging the files, a message is displayed indicating successful completion of the process.

   or

   Press **n** to skip the invocation of the file merge utility.

   Note You may use an additional --silent option to avoid this prompt. In which case, by default, the utility will attempt the three-way merge.

4 Press **y** or any other key to copy security configuration files, and then press **Enter**. This will copy the security configuration files from .migrate.bkp.<version>/conf to local/conf of the new installation.

   or

   Press **n** to skip the copying of security configuration files.

5 Review the files (merged, auto-merged and .conflict) after the migration is over. Take appropriate actions as mentioned in the 'User Action' column in Custom file migration use cases.

Perform a rollback

Use the following steps to rollback changes made by the sm_migrate utility:

1 Go to the <**BASEDIR**>/smarts/bin folder of your new installation, and type the following command to rollback the changes made by sm_migrate utility to your new installation:

```
./sm_perl sm_migrate.pl --new=<new_installation location _upto_and including smarts> --rollback [--
silent]
c:\InCharge\SAM\smarts\bin>sm_perl sm_migrate.pl
--new=c:\InCharge\SAM\smarts --rollback
```

Custom file migration use cases

The use cases for custom file migration and resulting backup and merge activities are described in Custom file migration use cases .

Note <file_name> with no extension represents a base file that is present under the BASEDIR/smarts directory of the new installation.

Table 7-2. Custom file migration use cases

Use case	Backup action	Merge Action	
Old installation	**New installation: BASEDIR/smarts/.migrate.bkp.<version>**	**New_installation:BASEDIR/smarts/local**	**User action**
There is a local copy of a file, and changes were introduced by you. The file is also used in the new base installation.	Back up the base and the local copies of the file. The base copy is backed up with “base” extension, as <file_name>.base. The local copy will be backed up with “local” extension, as <file_name>.local. Local name will be customized name of local. For example: <file_name>.local123.	Run sm_merge for: ■ <file_name>.base ■ <file_name>.local ■ <file_name> **Merge Outcome:** ■ Changes made by you are merged into the new file and placed in <New_installation>/smarts/local/<file_name>.conf ■ If the changes made by you could not be merged without a conflict, a .conflict file is generated and placed in <New_installation>/smarts/local/<file_name>.conflict	■ Because the three-way merge utility works at a string level and not at a code level for files such as .asl, .xml, .cmd, and .sh, the merge result of these files is appended with .automerge extension. Review the files, and if the changes are acceptable, save the file without .automerge extension. ■ Files with .import and .conf extension are not appended with an automerge extension on successful merge. ■ For conflict files, review the conflict file, manually resolve the conflict, and save the file without a .conflict extension.
There is a file in old base, old local and the same file exists in new base.	No backup action.	No merge.	No user action required.
There is a file in old base and the same file exists in new base.	No backup action.	No merge.	No user action required.
The local copy of the file that was introduced by a patch and later modified by you. The file exists in the new base, but does not exist in the old base.	Back up the local copy of the file. The local copy will be backed up with “local” extension, as <file_name>.local. Local name will be customized name of local. For example: <file_name>.local123.	sm_merge utility will compare <file_name>.local and <file_name>. **Merge Outcome:** <file_name>.conflict	Review the conflict file, manually resolve the conflict and save the file without a .conflict extension.

Table 7-2. Custom file migration use cases (Continued)

Use case	Backup action	Merge Action	
Old installation	**New installation: BASEDIR/smarts/.migrate.bkp.<version>**	**New_installation:BASEDIR/smarts/local**	**User action**
There is a local copy of the file, and changes were introduced by you, but the file is no longer used in the new release.	Backup the base and the local copies of the file. The base copy is backed up with “base” extension, as <file_name>.base. The local copy will be backed up with “local” extension, as <file_name>.local. Local name will be customized name of local. For example: <file_name>.local123.	No merge	The files remain in the backup directory. Determine if the customization is still relevant to the new installation.
The local copy of the file was introduced by a patch, and changes were made by you. The file does not exist in either the new or old base.	Backup the local copy of the file. The local copy will be backed up with “local” extension, as <file_name>.local. Local name will be customized name of local. For example: <file_name>.local123.	No merge	Determine if the customization is still relevant to the new installation.
There is a local copy of the file, and changes were made by you. The file is also used in the new version, and there is already a local copy of the file in the new local.	Backup the local copy of the file. The local copy will be backed up with “local” extension, as <file_name>.local. Local name will be customized name of local. For example: <file_name>.local123.	No merge	The sm_merge gives precedence to the files in new_local. No changes will be made to the files that are already under new_local. Key exceptions to the rule are covered in the Migration of security configuration files.
There is a local copy of the file, and custom code was introduced by you. This code does not exist in either the old or the new base.	Back up the local copy of the file. The local copy will be backed up with “custom” extension, as <file_name>.custom.	No merge. Copy the files (without the .custom extension) from New Installation: BASEDIR/smarts/.migrate.bkp.<version> to New installation: BASEDIR/smarts/local	Determine whether these custom files are still needed in your new installation.

Table 7-2. Custom file migration use cases (Continued)

Use case	Backup action	Merge Action	
Old installation	**New installation: BASEDIR/smarts/.migrate.bkp.<version>**	**New_installation:BASEDIR/smarts/local**	**User action**
There is a local copy of the file, and custom code was introduced by you. This file is also used in the new base.	Back up the local copy of the file. The local copy will be backed up with “custom” extension, as <file_name>.custom.	No merge. Copy the files (without the .custom extension) from New Installation: BASEDIR/smarts/.migrate.bkp.<version> to New installation: BASEDIR/smarts/local The file is copied with .<old_version> extension.	Determine whether these custom files are still needed in your new installation.
There is a local copy of the file, and changes were made by you. The file is also used in the new version, and there is already a local copy of the file in the new local introduced by a patch.	Back up the base and the local copies of the file. The base copy is backed up with “base” extension, as <file_name>.base. The local copy will be backed up with “local” extension, as <file_name>.local. Local name will be customized name of local. For example: <file_name>.local123.	Run sm_merge for: ■ <file_name>.base ■ <file_name>.local ■ <file_name> **Merge Outcome:** ■ Changes made by you are merged into the new file and placed in <New_installation>/smarts/local/<file_name>.conf ■ If the changes made by you could not be merged without a conflict, a .conflict file is generated and placed in <New_installation>/smarts/local/<file_name>.conflict	■ Because the three-way merge utility works at a string level and not at a code level for files such as .asl, .xml, .cmd, and .sh, the merge result of these files is appended with .automerge extension. Review the files, and if the changes are acceptable, save the file without .automerge extension. ■ Files with .import and .conf extension are not appended with an automerge extension on successful merge. ■ For conflict files, review the conflict file, manually resolve the conflict, and save the file without a .conflict extension.

Migration of security configuration files

The sm_migrate utility prompts you for copying the security configuration files serverConnect.conf, clientConnect.conf, brokerConnect.conf, runcmd_env.sh and imk.dat. You can either choose to copy these files into the local directory of the new installation or configure these files later, manually.

If you choose to copy and have changed the site secret in your previous installation, you need to run the sm_rebond command to encrypt the files. For example:

```
./sm_rebond --basedir=C:\InCharge\IP\smarts
```

After copying the files, the data in the old runcmd_env.sh file is appended to the new runcmd_env.sh file and the new 10.0.0 version data is commented.

Note Migration of security configuration files is not supported on cross platforms.

Migration of dynamic model files

The dynamic model files (files with .mdl and .ldm extension) are backed up in the .migrate.bkp.<version> directory. These files are not considered by sm_migrate utility for merging. Remove the .ldm file from the local directory of the new installation. Recompile the .mdl file before it is used in the new installation. A new .ldm file will be generated once you recompile the .mdl file.

The VMware Smart Assurance Dynamic Modeling Tutorial explains the concepts and methods of dynamic modeling.

Three-way merge utility

The three-way merge utility, sm_merge, helps incorporate configuration changes (made in the .conf, .import .asl, .xml, .pl, .sh, and .cmd files) from an old installation into a new installation of a product. The utility performs a three-way merge on each of the files that you have modified.

The utility uses <file_name>.base, <file_name>.local, and <file_name>, and finds the largest sequence of lines that is common to all three files (this sequence need not necessarily be continuous lines). This largest sequence of lines is called the Longest Common Subsequence (LCS). Then, for each of the three files, it finds groups of lines in between two consecutive lines in the LCS. These groups are referred to as “content blocks.” The utility compares these content blocks to decide on merge as given in Three-way merge utility.

Use cases for content block comparison

The scenarios for comparison of content blocks during the three-way merge process are described in Content block comparison use cases. In this table, X, Y, and Z represent the content blocks, one from each of the three files.

Table 7-3. Content block comparison use cases

Scenario	Content block comparison	Result

XYY
■ Content block in the <file_name>.base looks like X
■ Content block in <file_name>.local looks like Y
■ Content block in the <file_name> looks like Y
	The following content blocks are picked up:
	■ Content block in <file_name>.base = X
	`AllowPrivateIPAsName FALSE`
	■ Content block in <files_name>.local = Y
	`AllowPrivateIPAsName TRUE`
	■ Content block in <file_name> = Y
	`AllowPrivateIPAsName TRUE`
		Result: Y
		Since the <file_name>.local version and the <file_name> version of the content blocks match, the Y version is picked.

XYX
■ Content block in the <file_name>.base looks like X
■ Content block in the <file_name>.local looks like Y
■ Content block in <file_name> looks like X
	The following content blocks are picked up:
	■ Content block in <file_name>.base = X
	`ERXIfExcludeSysPattern router*`
	■ Content block in <files_name>.local = Y
	`ERXIfExcludeSysPattern *`
	■ Content block in <file_name> = X
	`ERXIfExcludeSysPattern router*`
		Result : Y
		This is the case where the file modified by you (Y) is preserved and is written to new_local.

X Y Z
■ Content block in the <file_name>.base looks like X
■ Content block in the <file_name>.local looks like Y
■ Content block in the <file_name> looks like Z. This is the case where a .conflict file is created.
	The following blocks sections are picked up:
	■ Content block in <file_name>.base = X
	`#Enable/Disable discovery of VLANs`
	`PropagateVRIfAlias  FALSE`
	■ Content block in <files_name>.local = Y
	`#Enable/Disable discovery of Router`
	`PropagateVRIfAlias  TRUE`
	■ Content block in <file_name> = Z
	`#Enable/Disable discovery of Multicast # New install changes`
	`PropagateVRIfAlias  FALSE`
		Result: Conflict
		All three content blocks will be written into a .conflict file.

During this process, modifications done on each of the files in the old installation are merged into the new installation. The utility identifies the files to be copied and copies them into a predefined new directory in the new installation with an appropriate suffix. Use cases for content block comparison provides details on the files which will be copied:

The utility performs the following functions:

- Automated analysis of the differences between any two files (for example, File A and File B), while also considering the parent file.
- Incorporates the changes done to the parent file in File A and File B, and automatically merges the two changes. This type of merge is used in revision control systems.
- It maintains a record of the conflicts encountered during the merge process in a .conflict file.

  In case the utility is unable to merge the files due to some conflict, it creates a .conflict file for each file. The .conflict file provides details of the files which were not completely merged by the three-way utility. Each conflicting instance is recorded in the .conflict file. You can review the .conflict files to spot the conflicts, and manually resolve the differences.

Configuration migration process logs

Log file and description lists the logs files that are created for the modified customization migration process. These files are available under the BASEDIR/smarts/setup/logs directory.

Table 7-4. Log file and description

Log file name	Description
Config_migration_copy.log	Logs information about files that were modified during the previous installation, and those which were backed up in the new installation.
Config_migration_merge.log	Logs information about the files on which three-way merge was performed. It also mentions whether the merge process was successful or if any conflicts arose during the process.
<file_name>.conf.MergeLog <file_name>.asl.MergeLog <file_name>.import.MergeLog <file_name>.xml.MergeLog <file_name>.sh.MergeLog <file_name>.cmd.MergeLog	For each type of file (.conf, .import .asl, .xml, .sh, and .cmd) merge logs are created. These logs record the lines which the three-way merge process copied from the previous installation, lines which were retained as-is, and those where conflicts were observed.

Automatically migrate topology for IP Manager using RPS utility

The repository file (RPS) migration utility (**sm_migraterps**) automatically converts the RPS file created by the previous version of the software to an RPS file compatible with the newer version of the software. For example, you can use the utility to automatically convert the IP 9.4.0.0 RPS file into a compatible version of IP Manager 9.5. This tool allows the administrator to quickly migrate the product without going through a rediscovery of the entire topology.

The RPS migration utility supports migration from IP Manager 9.x.x versions to IP Manager 9.5.x and later.

If you are migrating from IP Manager 9.4.x, running the RPS migration utility is optional. For example, if you have an IP Manager 9.4 repository file that includes virtual switch systems in the topology, use the sm_migraterps utility to remove VirtualSwitchSystemLink and make the repository compatible for IP Manager 10.0.0.

This section covers the following:

- Functions of RPS migration utility
- Running RPS migration utility

Functions of RPS migration utility

The utility performs the following functions:

- Creates a temporary and a backup copy of the RPS file to be migrated. On successful migration, the backup file is deleted. The tool then renames the temporary file as the new RPS and, the original RPS file as the backup file with a .v70 suffix.
- Checks for the existence of the source RPS file. Users must ensure that they are using a valid source RPS file.

Running RPS migration utility

Note It is recommended to run the RPS migration utility only once. A second run will overwrite the older backup file.

To run the RPS migration utility:

1 Go to the <**BASEDIR**>/smarts/bin folder.

2 Copy the previous version of the RPS file to the <**BASEDIR**>/smarts/bin folder.

3 Type the following command:

```
sm_migraterps <rps_file> --trace <logfilename>
```

4 Copy the migrated RPS file into the < **BASEDIR** *>/smarts/local/repos/icf* folder.

5 Use the *--ignore-restore-errors* option in the sm_service command to start the IP Manager with the migrated repository file. Otherwise, the IP Manager may generate errors and may not start up with the migrated repository file.

6 Initiate a full discovery (Discover All). Consult the discovery guide or user guide for your product for more information on this procedure.

Note A full discovery is required for the new version features and changes to take effect.

Deployment utility overview

The Deployment Utility allows you to deploy customizations and configuration changes from an existing installation to another installation on the same version of a product. The deployment can be carried out on the same host or between two different hosts running the same operating system.

The utility is useful if you have to apply the same configurations on multiple installations of a product. Use the utility if you have:

- Multiple new installation running on the same or multiple hosts that will need to share the same configuration and customizations.
- Multiple installations on the same or multiple hosts that are upgraded and will share the same configuration and customizations.

  In both cases, you will need to start with one installation where you make all your modifications to configuration files, <BASEDIR>/smarts/local files and, create and compile dynamic models. Then, run the sm_deploy utility to create a package that contains your modifications. Use the sm_deploy utility to apply the files collected from the first installation to the rest of your installations.

  The Deployment Utility performs the following three functions:

- Create a package
- Deploy the package
- Rollback

Create a package

The utility enables you to create a deployment package which consists of all the customizations made to files in an installation. In SAM, by specifying a broker and server information when you run the utility, you can collect configuration settings from RPS into the package.

Deploy the package

The utility enables you to deploy a previously collected deployment package into other installations of the same product running on the same version and operating system as the original installation. If you have collected configuration settings from SAM RPS, the configurations will be available in the file, *<SAM_server>.xml* under *local/conf/ics* directory.

Rollback

Before deploying the package into an installation, the utility creates a rollback directory containing the backup copy of files from the current installation which will be used incase of a rollback action. You can rollback your configuration to that in your rollback directory, only if the version of your current installation is the same as the version of the installation when the rollback directory was created.

Note Soft links created for product related files in the UNIX environment are not handled by sm_deploy utility.

Running the Deployment utility

To run the Deployment utility, go to <BASEDIR>/smarts/bin directory and type the following command:

```
./sm_perl sm_deploy.pl <options>
```

where, <*options*> refers to the options specified in the section,sm_deploy modes of operation.To run the utility from an older version of a Smarts product that does not have the migration utility, you must copy the sm_deploy.pl script and certain Perl files (packaged in migratePerlPkg.zip file) and place them in the appropriate locations. The sm_deploy.pl must be placed in the bin directory and the Perl package must be placed under the BASEDIR/smarts/local folder and extracted there.

sm_deploy modes of operation

The sm_deploy has the following command-line options:

- --install=<dir> – To install the utility.
- --create=<file> – To create the deployment package.
- --deploy=<file> – To deploy the package.
- --rollback – To rollback the configuration changes.
- --broker – The broker to which the SAM server is attached. Use this option to collect configuration settings from SAM RPS.
- --server – The SAM server whose configuration settings from RPS are to be collected.
- --clean – To clean the files in the local directory.
- --silent
- --sitemod – To specify customer specific local directories.
- --help

  The deployment utility must be used with at least one of these options.

  Note If you want to run this utility from older versions of VMware Smart Assurance products, you must copy the sm_migrate.pl script, sm_deploy.pl script and, the Perl files packaged in a .zip file from the 10.0.0 installation to the corresponding locations in the old installation.

To create a deployment package

1 Go to the <BASEDIR>/smarts/bin folder of your target installation, and type the following command:

```
./sm_perl sm_deploy.pl --install=<BASEDIR>/smarts --create=<archive-name.tar> --
sitemod==<BASEDIR>/smarts/local
```

2 The utility identifies the files with customizations from the local directory under <BASEDIR>/smarts directory of the installation that need to be copied to the deployment package. Local directory can be local1, local2.

3 The utility copies the files from the local directory to the deployment backup directory *.deploy.bkp<pdt>.<version>* under <BASEDIR>/smarts, archives these files to a specified archive file and then deletes the backup directory.

Manage RPS file settings across multiple installations

The method of extracting the configuration settings from an RPS file into the deployment package varies between SAM and IP Managers.

For SAM, use the deployment utility to extract the configuration settings from the RPS file.

Go to the <BASEDIR>/smarts/bin folder of your target installation, and type the following command:

```
./sm_perl sm_deploy.pl --install=<BASEDIR>/smarts --create=<archive-name.tar> --broker=<host:port> --
server=<SAM_server>
```

This can be a convenient way to deploy the configurations of aggregate SAM domain since they often share the same configuration.

For IP, use the *sm_settings.pl* script of the *IP-Configuration Manager* tool to export the Polling and Threshold groups from an existing domain and import them into the IP-Configuration Manager to be deployed further on other domains.

For more information on loading settings into IP-Configuration Manager, refer to the *VMware Smart Assurance Smarts IP Manager User Guide*.

For Network Protocol Manager, MPLS Manager, and Server Manager, the configuration settings from an RPS file must be manually configured in all other installations of these products.

To deploy the package

1 Go to the <BASEDIR>/smarts/bin folder of your target installation, and type the following command:

```
./sm_perl sm_deploy.pl --install=<TargetBASEDIR>/smarts --deploy=<archive-name.tar>
```

2 Creates a rollback directory with the backup of files from the target installation which will be used incase of a rollback action. Rollback will contain local folders which are part of the deployment package.

3 Copies all the files from the deployment package to the local directory of the target installation.

4 Overwrites the files that are part of both, the deployment package and the local directory of the target installation.

5 If the *--clean* option is specified, the files in the local directory of the target installation that are not part of the deployment package are deleted.

   Or

   If *--clean* option is not specified, the files in the local directory of the target installation that are not part of the deployment package are retained.

   To deploy the SAM RPS settings,

   - Manually import the *<SAM_server>.xml* file from local/conf/ics directory to the directory in the target installation by typing the following sm_config command:

     ```
     ./sm_config --server=<SAM_server> import --force <SAM_server>.xml
     ```

To Rollback

1 Go to the <BASEDIR>/smarts/bin folder of your target installation, and type the following command:

```
./sm_perl sm_deploy.pl --install=<TargetBASEDIR>/smarts --rollback
```

2 Copies the files from the local directory of the installation whose rollback directory you choose to rollback to, into the corresponding location in your current installation.

Note If your current directory is a rollback directory location, it will not be displayed in the list of rollback directory locations to which you can rollback.

Verifying the Installation

8

This chapter includes the following topics:

- Check the version number
- Start services
- Start programs
- Service and program startup options
- Start Smarts NOTIF
- Verify the product status
- Verify the FIPS 140 mode status
- Collect system information
- Configuration Scanner Tool

Check the version number

When you run a utility to report the version number of the software, you will see both the version number for the product as well as the version number for the underlying foundation software. These two version numbers might differ.

To verify the version number, enter the following command from the <BASEDIR>/smarts/bin directory:

```
sm_server --version
```

This command should return the following information:

- Operating system (OS) name on which the product is running and the OS version identifier.
- Version number of the product.
- **Version number of the foundation (DMT)** code, foundation build number, the date and time that the build was made as well as whether you have installed a 64-bit version of the software. If you installed the 64-bit version, you will see a “/64” after the foundation and the product version number.

The “sm_server --version” output is the following:

```
Operating System <Identifier>
<product>: V<Number>(<InternalBuild>), <Date>
Copyright 2019, VMware Inc – Build <Build>
Foundation V<Number>(<InternalBuild>), <Date>
Copyright 1995–2018, VMware – Build <Build>
```

For example, for IP Manager, the output might look similar to:

```
linux_rhAS50-x86-64/206320000
IP_NETWORK_SUITE: V10.0.0.0(174350), 22-Jan-2019 02:00:03 Copyright 2019, VMware Inc – Build 4
Foundation V10.0.0.0(174262), 18-Jan-2019 10:24:40 Copyright 2019, VMware Inc – Build 1
```

The product version number is displayed during the Wizard mode installation on the InstallShield screen.

Be aware that product versions vary and do not always match the software foundation version number. For example, if you select the *About* from the *Help* menu in the Global Console, you may see a different number.

Start services

VMware, Inc. recommends installing VMware Smart Assurance products as services. If you installed the products as services, you must start them for the first time. These services start automatically upon system reboot.

Note Start the Broker service first if it is not running.

Starting services on UNIX

Verify the status of the service daemon before starting a service.

Verifying the status of the service daemon

Use the ic-serviced command to check the status of the service daemon. The path to the ic-serviced command varies by operating system.

CentOS

On CentOS systems, enter the following command to verify the status of the service daemon:

```
/etc/init.d/ic-serviced status
```

If the sm_serviced process does not respond, the process is not running. Start the service by entering the command:

```
/etc/init.d/ic-serviced start
```

Linux

On Linux systems, enter the following command to verify the status of the service daemon:

```
/etc/init.d/ic-serviced status
```

If the sm_serviced process does not respond, the process is not running. Start the service by entering the command:

```
/etc/init.d/ic-serviced start
```

Starting services

To start or stop an VMware Smart Assurance service, use the sm_service utility. Type the command from the BASEDIR/smarts/bin directory:

```
sm_service start
<service_name> [<service_name> ...]
```

where *<service_name>* is each service you need to start. Starting services provides a list of service names.

Start programs

You can start VMware Smart Assurance programs from the terminal when the program is not intended to be long-running or to perform testing. VMware, Inc. does not recommend using this method in a production environment.

The VMware Smart Assurance System Administration Guide provides a complete description of the command syntax.

To start a program, type the command with the appropriate options on one line.

- For UNIX, invoke the command from the BASEDIR/smarts/bin directory. Prefix the command with ./ (a period followed by a forward slash).

Starting the VMware Smart Assurance Broker

```
./brstart --port=426 --output
```

Starting a Manager

```
t ./sm_server --name=<server_name>
--config=<config_directory>
--port=0
--ignore-restore-errors
--output s
```

For UNIX, to run the program in the background, use the daemon option.

Note Service Assurance Manager Console crashes when running commands on a Linux platform since the FIPS library fails to load. SELinux prevents the shared libraries, libcryptocme2.so and libccme_base.so from loading because of the existence of text relocation in the library.

The following workarounds are available to avoid the SAM Console crash:

1 Run the following commands to change the file context for the shared libraries, libcryptocme2.so and libccme_base.so to **textrel_shlib_t**:

```
chcon -t textrel_shlib_t libcryptocme2.so
chcon -t textrel_shlib_t libccme_base.so
```

2 Set the parameter **setenforce** to 0 to run SELinux in permissive mode.

3 Navigate to Edit */etc/selinux/config* and set the parameter **SELINUX** to **Disabled**.

Service and program startup options

Default service names, server names, and configuration directories lists service names, server names, and configuration directories for VMware Smart Assurance products.

Table 8-1. Default service names, server names, and configuration directories

Product	Service name	Server name	Config directory
Broker	ic-broker	Not applicable	Not applicable
IP Manager			
IP Availability Manager	ic-am-server	INCHARGE-AM	icf
IP Performance Manager	ic-pm-server	INCHARGE-PM	icf
IP Availability and Performance Manager	ic-am-pm-server	INCHARGE-AM-PM	icf
Service Assurance Manager			
Service Assurance Manager Server	ic-sam-server	INCHARGE-SA	ics
Service Assurance Manager Adapter Platform Server	ic-icoi-server	INCHARGE-OI	icoi
SNMP Trap Adapter	ic-trapd-receiver	TRAP-INCHARGE-OI	icoi
Syslog Adapter	ic-syslog-adapter	SYSLOG-INCHARGE-OI	Not applicable

Table 8-1. Default service names, server names, and configuration directories (Continued)

Product	Service name	Server name	Config directory
Business Impact Manager	MBIM	INCHARGE-MBIM	bim
MPLS Management Suite			
MPLS Analysis Server	ic-mpls-analysis	INCHARGE-MPLS-ANALYSIS	mpls-a
MPLS Monitoring Server	ic-mpls-monitoring	INCHARGE-MPLS-MONITORING	mpls-m
MPLS Topology Server	ic-mpls-topology	INCHARGE-MPLS-TOPOLOGY	mpls-t
MPLS VPN-Tagging Server	ic-vpn-tagging	VPN-TAGGING	vpn-tagging
Server Manager			
Server Manager	ic-esm-server	INCHARGE-ESM	esm
Network Protocol Management Suite products			
Network Protocol Manager for BGP	ic-npm-bgp-server	INCHARGE-BGP	conf/bgp
Network Protocol Manager for EIGRP	ic-npm-eigrp-server	INCHARGE-EIGRP	conf/eigrp
Network Protocol Manager for IS-IS	ic-npm-isis-server	INCHARGE-ISIS	conf/isis
Network Protocol Manager for OSPF	ic-npm-ospf-server	INCHARGE-OSPF	conf/ospf

- Chapter 11 Manually Installing Services provides the default service and program parameters that are used for the service install commands.
- The VMware Smart Assurance System Administration Guide provides information in regard to the sm_server, sm_adapter, and sm_trapd programs.

Start Smarts NOTIF

To start Smarts NOTIF:

1 Set an environment variable in the **BASEDIR** directory path to ensure that Java can be successfully started for Smarts NOTIF. In **BASEDIR**/smarts/local/conf/**runcmd_env.sh**, add the following line:

```
SM_JAVA_ENABLED=YES
```

2 Configure the SNMP Trap Adapter to use the Notif-trap_mgr_parse.asl script instead of the default trap_mgr_parse.asl script so that Smarts NOTIF processes SNMP traps. For example:

```
./sm_service install --force --unmanaged --startmode=runonce \
'--name=ic-notif-trap' \
'--description=Notif Trap Receiver' \
'/opt/InCharge/SAM/smarts/bin/sm_trapd' \
'--name=NOTIF-TRAP' \
'--server=INCHARGE-OI' \
'--output' \
'--config=icoi' \
'--port=1162' \
'--model=sm_actions' \
'--rules=icoi-trapd/Notif-trap_mgr_parse.asl'
```

3 Configure the Syslog Adapter to use the Notif-SysLog_mgr.asl script instead of the default SysLog_mgr.asl script in order for Smarts NOTIF to process Cisco system log files.

For example:

```
./sm_service install --force --unmanaged --startmode=runonce \
'--name=ic-notif-syslog' \
'--description=Notif Syslog Adapter' \
'/opt/InCharge/SAM/smarts/bin/sm_adapter' \
'--name=NOTIF-SYSLOG' \
'--server=INCHARGE-OI' \
'--output' \
'--config=icoi' \
'--port=1162' \
'--model=sm_actions' \
'--model=sm_system'\
'--rules=icoi-syslog/Notif-SysLog_mgr.asl'\
'--tail=/opt/InCharge/SAM/smarts/local/logs/sample.txt'
```

4 Launch the Smarts NOTIF Editor by selecting **Start** > **Programs** > **InCharge** > **Smarts NOTIF Editor**.

Note You can also launch the editor by double-clicking the **NotifGui.sh** file (for UNIX systems) in the BASEDIR/smarts/notif/editor directory.

5 Use the Smarts NOTIF Editor to connect to the running SAM server or Adapter Platform server. Select **Remote** > **Edit a server's settings** in the Smarts NOTIF Editor. The **Connect to a Server** dialog box appears, showing the list of available Adapter Platform and SAM server connections.

6 Choose a server from the list of available server connections in the **Connect to a Server** dialog box and click **OK**.

If server connections are not displayed, perform the following to populate the list of server connections:

7 Click **More** in the **Connect to a Server** dialog box. The **Manage Connections** dialog box appears where you can add server connections.

8 Click **Add** in the **Manage Connections** dialog box. The **Input** dialog box appears.

9 Enter a connection reference name (for example, “Remote Smarts NOTIF OI server”) in the **Input** dialog box and click **OK**.

10 Fill in the new connection record in the right pane of the **Manage Connections** dialog box.

11 Click **OK** to save the connection setup.

The **Remote Server Settings** dialog box appears that shows the server's current settings.

12 Select the **Activate Smarts NOTIF** checkbox, and then click **OK**.

Note You can also change other server settings in the **Remote Server Settings** dialog box if necessary.

13 Restart your SAM server or Adapter Platform server.

Note Server setting changes made in the Smarts NOTIF Editor **Remote Server Settings** dialog box are persistent. When you change server settings in the **Remote Server Settings** dialog box and click **OK**, the changes are saved to the **Notif_Settings.import** file that is generated and saved to the **BASEDIR**/smarts/local/conf/<*icoi* or *ics*> directory in the Adapter Platform or SAM server where Smarts NOTIF is running. Server setting changes made in the Smarts NOTIF Editor are preserved even if the repository is deleted. For example, if the repository is erased because you used the **--norestore** option for server startup, the server uses the last saved settings from the Smarts NOTIF Editor saved in **BASEDIR**/smarts/local/conf/<*icoi* or *ics*>/**Notif_Settings.import**.

The VMware Smart Assurance Notification Module User Guide includes information on how to use the Smarts NOTIF Editor.

Verify the product status

You can determine the current state of the products that register with the Broker by typing the following command from the BASEDIR/smarts/bin directory:

```
./brcontrol
```

This command displays a list of VMware Smart Assurance Managers and adapters that are registered with the Broker, their states (RUNNING, DEAD, UNKNOWN), process IDs, port numbers, and the last time that their states changed.

Also check any log files for the products. Typically, these log files are in BASEDIR/smarts/local/logs.

Note More than one log file may be generated due to changes in the foundation code that supports internationalization. The VMware Smart Assurance System Administration Guide provides additional information on log files.

If only one log file per server is desired, use sm_edit to update the BASEDIR/smarts/local/conf/runcmd_env.sh file. To get a single log file, set the following environment variables:

```
export SM_LOCALE=en_US (or appropriate locale code)
export SM_ENCODING_OUTPUT=UTF-8
```

Verify the FIPS 140 mode status

To verify if the installation is running in FIPS-140 mode, run the following command in the dmctl mode:

```
get SM_System::SM-System::FIPS
```

The value for this parameter must be TRUE.

You can also check for the status of FIPS 140 in the log files in the BASEDIR/smarts/local/logs directory. When the Broker and server start in FIPS 140 mode, a message similar to the following one is written to the Broker and server log files:

```
RSA BSAFE: MES 3.2.4 26-May-2012/64(0), FIPS: RSA BSAFE Crypto-C Micro Edition FIPS 140-2 Module
3.0.0.0/64(0), May 31 2008 13:19:56
```

Common issues

Domain registers with the broker, but appears DEAD after a few minutes

The domain is in FIPS 140 mode but the broker is not.

Domain is not able to register with the broker

The Broker is in FIPS 140 mode but the domain is not.

Broker or Domain log entry

```
CI-N-EWHILE-While executing function "queue_work”CI-EFLOWID-For flow CI_FlowTCP_U [Flow in
negotiations Accepted physical flow] PHYSICAL @0x0000000000a38db  . *:v4:44445 KS N/A, KR N/A  . Open
fd=10, conn August 17, 2011 3:27:43 PM EDT, disc N/A,  . 127.0.0.1:44445 -> 127.0.0.1:58347, tmo 0
00:00:15 N/S 1/0 CI-EWHILE-While executing function ""CI_FlowTLS_U::handshake”” CI-BSAFE-error:
1407609C:SSLroutines:SSL23_GET_CLIENT_HELLO:http request: ; in file "s23_srvr.c" at line 746
```

The entry might also appear as: *SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol*.

This may be because the Domain (or Broker) is in FIPS 140 mode but the client is not. It may also be that the client is a non-Smarts client (for example a load balancer’s HTTP check). In that case, switch the load balancer to HTTPS check.

Client error

```
CI-E-EWHILE-While executing function ""CI_FlowTLS_U::handshake””CI-BSAFE-error:1408F10B:SSL
routines:SSL3_GET_RECORD:wrong version number: ; in file "s3_pkt.c" at line 553CI-TLSPE-TLS protocol
error
```

This may be because the Domain or Broker is not FIPS 140 capable but the client is operating in FIPS 140 mode.

Log errors

```
[July 11, 2011 5:09:41 PM EDT +385ms] t@31 PollingQueue #8CI-E-EDECRYPT-Cannot decrypt.CI-EDECRYPT-
Cannot decrypt.[July 11, 2011 5:09:41 PM EDT +386ms] t@31 PollingQueue #8IA-E-ERROR_EXECUTING_ACTION-
Error executing action MA-PerlScript-sihou513a.CI-EDECRYPT-Cannot decrypt.
```

This may be because the lmk.dat version or the password does not match between domains. Ensure that the password and the version matches across all installs that inter operate.

Error on startup of domain or other tools

```
[August 8, 2011 8:29:07 PM EDT +466ms] t@3916876800 <Primary Thread>CI-F-EBLACKSTRING_CONTEXT-While
creating the contextCRPT-CRYPTO_MD5_INIT_FAILED-Failed to initialize the context for MD5 algorithm
```

This may be because you are trying to use a v1 imk.dat file in FIPS 140 mode. Ensure that you use v2.1 for FIPS 140 compatibility.

Collect system information

The sm_getinfo utility is used to collect data for troubleshooting VMware Smart Assurance Manager (server) problems. The utility backs up the current configuration for a server by creating a tar archive of all files and user customizations that are essential to troubleshooting the server. Customers then email the tar archive to VMware Customer Support for problem resolution.

sm_getinfo files

The sm_getinfo utility, which is supported on CentOS, and Linux, creates four types of files in the installation directory area from which it is invoked. The files are shown described in Files created by the sm_getinfo utility.

Table 8-2. Files created by the sm_getinfo utility

Filename	Description
Files in BASEDIR/smarts/local/logs directory	
sm_getinfo<date>.tar.gz Example:sm_getinfo26Mar2012-015952.tar.gz	A compressed tar archive in which the sm_getinfo utility stores a server 's log files, repository files, core files (CentOS, Linux) , user-modified files (using sm_edit), user-introduced files, and system environment information. The actual content of the tar archive depends on the user-specified options on the sm_getinfo invocation command line. The name of the tar archive includes the date when the tar archive was created.
MANIFEST	A text file that lists all of the files that the sm_getinfo utility includes in the tar archive.
Files in BASEDIR/smarts/local/logs/smgetinfo_files directory	

Table 8-2. Files created by the sm_getinfo utility (Continued)

Filename	Description
smgetinfo-versions.log.<date> Example:smgetinfo-versions.log.26Mar2012-020004 Example of other files in smgetinfo_files:TTP-Installed-versions.log.26Mar2012-020005	A log file in which the sm_getinfo utility writes information about a server's log file or repository file that is larger than 700 megabytes (MB). The sm_getinfo utility does not include any log or repository file in a server's tar archive that exceeds 700 MB. In addition, sm_getinfo writes system information to the log file. The name of the log file includes the date when the log file was created.
Final_sm_getinfo<timestamp>.tar Example:Final_sm_getinfo20Sep2012-005855.tar	The -k or --smconfigscan command invokes the Configuration Scanner tool, and generates the Final_getinfo-<timestamp>.tar, along with other Configuration Scanner tool-related files. **Note** If the sm_getinfo utility is run without the -k or --smconfigscan command, a getinfo-<timestamp>.tar output file will be generated without Final_ appended to the output. This implies that you will be running the sm_getinfo tool as usual.

sm_getinfo command-line syntax

You run the sm_getinfo utility from the BASEDIR/smarts/bin directory. The options that you specify on the invocation command line determine which files are included in the sm_getinfo-created tar archive.

Here is the command line syntax for sm_getinfo:

```
sm_perl sm_getinfo.pl
| --server <server name> --pid <server process ID>
| --broker <location>
| --log [<number of latest logs>]
| --nolog
| --repos [--latest]
| --norps
| --core
| --all
| --version
| --help
| --smmonitor "<sm_monitor options>"
| --flush
| --smconfigscan
```

where:

- <> Angle brackets are user-supplied parameter values (variables).
- [ ] Square brackets are optional entries.
- | Vertical bar symbols are alternate selections.

The command-line options are described in Command-line options for the sm_getinfo utility .

Table 8-3. Command-line options for the sm_getinfo utility

Option	Description
--server <server name> --pid <server process ID> | -s <server name> -p <server process ID>	Specifies the VMware Smart Assurance server name and PID against which the sm_getinfo utility will collect information. To dump a core file for a running server on CentOS or Linux, the pid option must be provided. Also, the server name is used to invoke the sm_monitor tool.
--broker <location> | -b <location>	Specifies an alternate broker location as host:port.
--pid <pid> | -p <pid>	PID of Domain Manager used to run gcore.
--log [<number of latest logs>] | -l [<number of latest logs>]	For each VMware Smart Assurance server, collects and stores a user-specified number of latest logs or all generated log files that are in the BASEDIR/smarts/local/logs directory. Note that whenever collecting a log, the related .audit and .archive files should be collected as well. If a server name is specified, only the files that correspond to the server will be collected. To avoid generating a too-large tar archive (too large to email), any log file that is larger than 700 MB will be excluded and its information will be logged in smgetinfo-versions.log<date>.
--nolog | -g	Excludes log files when collecting local files. This option and --log are mutually exclusive.
--repos [--latest] | -r [-t]	For each VMware Smart Assurance server, collects and stores the latest repository file or all repository files. If a server name is specified, only the file corresponding to the server will be collected. Any repository file that is larger than 700 MB will be excluded and its information will be logged in smgetinfo-versions.log<date>.
--norps | -n	Excludes repository files when collecting local files. This option and --repos are mutually exclusive.
--core | -c	Collects and stores the core files (CentOS, Linux) that are generated by the VMware Smart Assurance software, and the corresponding logs.
--all | -a	All data and files in BASEDIR/smarts/local and BASEDIR/smarts/setup directories will be collected and stored. If --all option is specified, the other options will be ignored except --server and --pid.
--version | -v	Print version information and exit.
--help | -h	Print usage information and exit.
--smmonitor “<sm_monitor options>” | -m “<sm_monitor options>”	Specifies the options for running sm_monitor, which will override the default options “-m run-all -z.” Approximately two cycles are run to collect the required information. The collected information is output to the BASEDIR/smarts/local/logs/SM-Monitor-<server name> directory.
--flush | -f	Force a flush. Needed when the sm_getinfo utility is invoked from a remote host.
--smconfigscan | -k **Note** This option is available for IP Manager only.	Invokes the configuration scanner tool to provide a snapshot of all the customizations introduced by you in your current installation. *“Configuration Scanner Tool” on page 116* provides more information on how to use the tool.

sm_getinfo invocation examples

To gather the five latest logs, enter:

```
sm_perl sm_getinfo.pl  --logs 5
```

To gather the latest repository data and core files, enter:

```
sm_perl sm_getinfo.pl  --repos --latest --core
```

To gather the entire BASEDIR/smarts/local directory, enter:

```
sm_perl sm_getinfo.pl  --all
```

To invoke sm_monitor, enter:

On Linux:

```
sm_perl sm_getinfo.pl -s
<server name>
-m "-m correlation -z"
sm_perl sm_getinfo.pl -s
<server name>
  -m "-m mem"
```

sm_getinfo data collection

If no command-line option is specified, the sm_getinfo utility will store the following information in the tar archive:

- For each server, the latest server log file in BASEDIR/smarts/local/logs and the related .audit and .archive files in BASEDIR/smarts/local/logs. If a server name is specified, only the files that correspond to the server will be collected. To avoid generating a too-large tar archive (too large to email), any log file that is larger than 700 MB will be excluded and its information will be logged in smgetinfo-versions.log<date>.
- For each server, the latest repository file in BASEDIR/smarts/local/repos. If a server name is specified, only the repository file for the server will be archived. Any repository file that is larger than 700 MB will be excluded and its information will be logged in smgetinfo-versions.log<date>.
- The local files that are not in the BASEDIR/smarts/local/logs and repos directories and changed since last temporary test patch (TTP) and patch.
- The new local files that are not in the BASEDIR/smarts/local/logs and repos directories and were added since the last TTP and patch.

- All local files except the files in logs and repos directories if no TTP or patch is installed.
- All files in the BASEDIR/smarts/setup/info and BASEDIR/smarts/setup/logs directories.
- Core files (UNIX) that are generated by the VMware Smart Assurance software, and the corresponding server log files. On Linux, some library (lib) files that are related to the cores are also collected.
- VMware Smart Assurance TTP or patch version information. Additionally, it verifies MD5 checksum for the installed TTP files and the files that are listed in manifest.md5 in the BASEDIR/smarts/setup/info directory.
- The data collected by sm_monitor. If a server name is specified, only the files that correspond to the server will be collected.
- The data generated by the VMware Smart Assurance Health Monitor (SHM).
- System environment information.

Configuration Scanner Tool

Note This tool is available only for IP Manager.

The Configuration Scanner tool scans for configuration changes in your current installation. It scans for customizations with regard to the following:

- **Polling and threshold settings:** The tool presents the non-default values and settings. That is, the tool generates a list of polling settings and threshold parameters that have changed from their default values, along with details of all the groups they are associated with. The output also includes tagging settings. In case of CLI settings, the tool collects and displays the username and the associated matching criteria.
- **Configuration files:** The tool generates a list of files that have changed from the default installation. The tool scans the files in the SM_SITEMOD and base installation and does a two-way difference analysis to figure out what files have changed, and displays the list of files, flagged appropriately as modified or added. For discovery.conf, name-resolver.conf and tpmgr-param.conf files, the tool parses through the content and presents the difference at an attribute->value pair level.

  Note The clientConnect.conf, serverConnect.conf, brokerConnect.conf, .imk.dat files and the l10n classes and Perl directories are excluded from the scan.

  The tool ignores service pack and patch files that are not modified by you.

Running the Configuration Scanner tool from the sm_getinfo utility

To run the Configuration Scanner tool:

1 Go to the <**BASEDIR**>/smarts/bin folder.

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

For UNIX, this location is: /opt/InCharge/<*product*>.

On UNIX operating systems, IP Availability Manager is, by default, installed to: /opt/InCharge/IP/smarts. Optionally, you can specify the root of **BASEDIR** to be something different, but you cannot change the <*product*> location under the root directory.

2 Type the following command:

```
                sm_perl sm_getinfo <options> -k (or --smconfigscan)
sm_perl sm_getinfo --broker=localhost:5086 --server=INCHARGE-AM --smconfigscan
or
sm_perl sm_getinfo -b localhost:5086 -s pserver --smconfigscan
```

Performing an Uninstallation

9

This chapter includes the following topics:

- Before uninstallation
- Uninstall VMware Smart Assurance products

Before uninstallation

You should complete the following tasks before uninstalling the product:

- Remove manually installed services
- Determine order for removing products (UNIX only)
- Detect and stop programs

Remove manually installed services

Services that you manually installed with sm_service command are not removed by the uninstallation program. You must remove these services manually before uninstalling the product software.

To remove a service, invoke sm_service from the BASEDIR/smarts/bin directory:

1 Use sm_service to list installed services.

```
sm_service show
```

2 Remove the manually installed service.

```
sm_service remove ic-
<service name>
```

Determine order for removing products (UNIX only)

When uninstalling VMware Smart Assurance products from the same server, the product that was installed first must be uninstalled last. During the installation of the first product, the VMware Smart Assurance Service Database is created and the other products subsequently access it. Uninstalling the product installed first will also uninstall the Service Database that will disable the sm_service command for those products, prevent their proper operation and uninstallation.

You can determine what product software was installed first by performing this check:

1 Use a text editor to open the **ic-serviced** script.
   - For CentOS, **ic-serviced** is located in the /etc/init.d directory
     - For Linux, **ic-serviced** is located in the /etc/init.d directory
2 Find the value of the SMHOME variable.

   The value of SMHOME indicates which product was installed first.

Detect and stop programs

Before upgrading or uninstalling your product, you must stop all VMware Smart Assurance services, VMware Smart Assurance scheduledjobs, and any other process that uses programs or libraries running from the VMware Smart Assurance product.

Detecting programs

The sm_plist utility identifies all VMware Smart Assurance programs that are running for any product on your machine. You can use the sm_plist utility whenever you need to identify VMware Smart Assurance programs that are running (for example, before applying a service pack or patch and uninstalling the product software).

To use the utility, invoke itfrom the BASEDIR/smarts/script directory. The utility displays active programs in a window:

1 Go to the BASEDIR/smarts/script directory.
2 Start the sm_plist utility:

   On UNIX, enter

```
./sm_plist.sh
<BASEDIR2>
cscript sm_plist.vbs
<BASEDIR2>
```

Stopping active programs (UNIX)

To stop active VMware Smart Assurance programs (UNIX):

1 Stop active VMware Smart Assurance services using the sm_service utility from BASEDIR/smarts/bin:

```
./sm_service stop --all
```

2 Determine if any VMware Smart Assurance services are still running by using the brcontrol utility from BASEDIR/smarts/bin:

```
./brcontrol -b
<host>:<port>
```

Table 9-1. Next steps for detecting and stopping programs

The Broker is on the . . .	And this displays . . .	Do this . . .
Same host	"Error attaching to Broker" message	The Broker is not running. Go to step 4 .
	List of servers registered with the Broker	■ The Broker or service daemon did not shut down. ■ If any servers are still running on the host, these did not shut down. Go to step 3 .
Different host	List of servers registered with the Broker	■ If any servers are still running on the host where you will install the VMware Smart Assurance software, these did not shut down. Go to step 3 .

1 Stop any VMware Smart Assurance server that is still running. If the Broker is on the host, stop the local Broker:

- To stop any server that is still running, use the dmquit utility from BASEDIR/smarts/bin:

```
./dmquit --server=<server name>
 -b
<host>:<port>
./brquit --broker=localhost:
<port>
```

2 Determine if any other VMware Smart Assurance processes are still running and shut the processes down:

   - Detect the processes using the following command:

```
ps –ef | grep “sm_”
kill
<pid>
```

Uninstall VMware Smart Assurance products

VMware Smart Assurance product software uses the InstallShield program to install and uninstall products. For UNIX, you invoke the uninstallation program from the system prompt. Failure to use the appropriate method will result in an unstable system and/or inconsistent product directories.

Note Do not manually delete the installed product directories. Before uninstallation, you must stop all the Smarts services.

Also, if you plan to reinstall the product, save all of the customized files that are in the BASEDIR/smarts/local directory before performing the uninstallation. *The uninstallation program will remove all of the files and directories in the BASEDIR/smarts directory, and then remove the smarts directory.*

Uninstall using CLI mode

To uninstall an VMware Smart Assurance product or product:

1 Go to the BASEDIR/_uninst directory and enter the following command:

```
./uninstaller
```

   During the uninstallation processes, you are prompted with a series of steps and menus. You can either accept the default value or select another choice. The default values are indicated in brackets or as predefined selections (checkmarks) in menus. To accept the default value, press **Enter**.

   When replying to a prompt, you can either accept the default value or select another choice.

   To reply yes, enter **Y**

   To reply no, enter **N**.

   Do not press **Delete**; doing so will cause the process to terminate with an error message. For selections in menus, you can accept default selections or type the number of the item and press **Enter**.

   If you incorrectly type an entry, type **back** to repeat the prompt and select the correct value. Arrow keys and the backspace key are not supported.

2 Press **Enter** to continue.

3 Upon completion, the uninstallation program will remove all of the files and directories in the BASEDIR/smarts directory, and then remove the smarts directory.

   The uninstallation program will also write an uninstall log file to the BASEDIR directory, unless the uninstallation fails at the very start, in which case the installation program will write the log file to the /tmp directory. The log file is a text file with the naming convention Uninstall.<product>.<productversionNumber>.log.

Uninstall using Unattended mode

The Unattended mode enables you to automate the removal of the VMware Smart Assurance products.

1 Invoke the uninstallation program with appropriate options for the operating system:

2 On UNIX systems, go to the BASEDIR/_uninst directory and enter the following command:

```
uninstaller -i silent
```

3 Upon completion, the uninstallation program will remove all of the files and directories in the BASEDIR/smarts directory, and then remove the smarts directory.

   The uninstallation program will also write an uninstall log file to the BASEDIR directory, unless the uninstallation fails at the very start, in which case the installation program will write the log file to the /tmp directory. A non-zero status indicates a failure. The log file is a text file with the naming convention Uninstall.<product>.<productversionNumber>.log.

The sm_edit utility

10

This chapter includes the following topics:

- sm_edit
- sm_edit example

sm_edit

As part of the VMware Smart Assurance deployment and configuration process, you need to modify certain files. User modifiable files include configuration files, rule set files, templates, and seed files that contain encrypted passwords. Original versions of these files are installed into appropriate subdirectories under the BASEDIR/smarts/ directory.

The original versions of files should not be altered. If a file must be modified, a new version should be created and then stored as a local copy of the file in BASEDIR/smarts/local or one of its subdirectories.

When VMware Smart Assurance software requires one of these files, it is designed to first search for a modified file in BASEDIR/smarts/local or one of its subdirectories. If a modified version of a file is not found in the local area, VMware Smart Assurance software then searches corresponding BASEDIR/smarts directories for the original version of the file.

To ease file editing and storage, VMware, Inc. provides the sm_edit utility with the every VMware Smart Assurance product. When invoked, sm_edit opens the specified file in a text editor. This utility ensures that modified files are always saved to the appropriate local area and that non-local copies of all files remain unchanged. If an appropriate subdirectory does not exist for the file you are modifying, sm_edit creates the appropriate subdirectory before saving the modified file to that location. For files with header information set for encryption, sm_edit encrypts certain fields in the file. In addition, sm_edit preserves the file permissions of modified files, which helps ensure that important configuration files are not altered by unauthorized users.

The VMware Smart Assurance System Administration Guide provides instructions on how to configure the utility to use a specific editor.

sm_edit example

To use sm_edit from the command line, specify the file name and include the subdirectory under BASEDIR/smarts/local where the file resides. For example, to edit the trapd.conf, enter the following command from the BASEDIR/smarts/bin directory:

```
sm_edit conf/trapd/trapd.conf
```

In this example, sm_edit searches in the BASEDIR/smarts/local/conf/trapd directory for the trapd.conf file. If it finds the trapd.conf file, it opens the file in a text editor. If sm_edit does not find the trapd.conf file in the BASEDIR/smarts/local/conf/trapd directory, it creates a local copy of the trapd.conf file and writes it to the BASEDIR/smarts/local/conf/trapd directory.

The VMware Smart Assurance System Administration Guide provides additional information about the sm_edit utility.

Manually Installing Services

11

This chapter includes the following topics:

- Overview
- Broker services
- Services for the IP Manager
- Services for the Service Assurance Manager
- Services for the MPLS Management Suite
- Services for the Server Manager
- Services for the Network Protocol Management Suite installation

Overview

If you did not install services when you installed the VMware Smart Assurance products, you may install services manually. Services are programs that, once started, are generally intended to run continuously. Components installed as services start automatically upon system reboot; those not installed as services (manual processes or disabled processes) require that you issue commands to start and stop them as necessary.

VMware, Inc. recommends that VMware Smart Assurance products be installed as services whenever possible. Typical reasons to install products as services include the following conditions:

- (IP Manager only) There is a need to install services for a single product instead of the combined IP Availability Manager and IP Performance Manager products (for example, IP Availability Manager alone or IP Performance Manager alone). Selection of bootstrap files when installing services provides more information.
- During installation of the product software, you chose to start product components manually and now want to run the components as services.

- Multiple instances of a single product component running as a service are required. During installation, you can install only a single instance of a product component as a service.

  To manually install a product as a service, use the sm_service installcommand with the appropriate set of options.

  The VMware Smart Assurance System Administration Guide provides a complete description of the command syntax.

Selection of bootstrap files when installing services

When you install IP Manager 10.0.0 with all services selected, both IP Availability Manager and IP Performance Manager services are installed. The default configuration file, bootstrap.conf, is used by the IP Manager 10.0.0 installer.

If your deployment supports only IP Availability Manager or IP Performance Manager, you must manually install these services for the IP Manager(s) using a bootstrap file different from bootstrap.conf.

Broker services

This section provides the default UNIX commands that are used to install the service manually for the Broker. Type the command on one line.

UNIX

```
t BASEDIR/smarts/bin/sm_service install
--force
--name=ic-broker
“--description= VMware Smart Assurance
         Broker”
--env=SM_CLIENTCONNECT=brokerConnect.conf
--startmode=runonce
BASEDIR/smarts/bin/brstart
--port=426
--output
--restore=BASEDIR/smarts/local/repos/ broker/broker.rps s
```

Services for the IP Manager

Here are the UNIX commands used to install services manually for the underlying servers in the IP Manager.

IP Availability Manager -only server

UNIX

```
t /opt/InCharge/IP/smarts/bin/sm_service install
--force
--name=ic-am-server
“--description= VMware Smart Assurance IP Availability Manager Server”
--startmode=runonce
/opt/InCharge/IP/smarts/bin/sm_server
--name=INCHARGE-AM
--config=icf
--bootstrap=bootstrap-am.conf
--port=0
--subscribe=default
--ignore-restore-errors
--outputs
```

IP Performance Manager -only Server

UNIX

```
t /opt/InCharge/IP/smarts/bin/sm_service install
--force
--name=ic-pm-server
“--description= VMware Smart Assurance IP Performance Manager Server”
--startmode=runonce
/opt/InCharge/IP/smarts/bin/sm_server
--name=INCHARGE-PM
--config=icf
--bootstrap=bootstrap-pm.conf
--port=0
--subscribe=default
--ignore-restore-errors
--outputs
```

IP Availability and Performance Manager Server

UNIX

```
t /opt/InCharge/IP/smarts/bin/sm_service install
--force
--name=ic-am-pm-server
“--description= VMware Smart Assurance IP Availability Manager and Performance Manager Server”
--startmode=runonce
/opt/InCharge/IP/smarts/bin/sm_server
--name=INCHARGE-AM-PM
--config=icf
--bootstrap=bootstrap-am-pm.conf
```

```
--port=0
--subscribe=default
--ignore-restore-errors
--outputs
```

IP Configuration Manager

UNIX

```
/opt/InCharge/IP/smarts/bin/sm_service install
--force
--name=ic-ip-configuration
"--description=VMware Smarts IP Configuration Manager"
--startmode=runonce
/opt/InCharge/IP/smarts/bin/sm_server
--name=INCHARGE-CM
--config=icf-c
--bootstrap=bootstrap.conf
--port=0
--subscribe=default
--ignore-restore-errors
--nodx
--output
```

Services for the Service Assurance Manager

This section provides default service parameters for the VMware Smart Assurance Service Assurance Manager.

VMware Smart Assurance Broker

UNIX

```
t/opt/InCharge/SAM/smarts/bin/sm_service install
 --force
 --startmode=runonce
 --name=ic-broker
 --description="VMware Smarts Broker"
 --env=SM_CLIENTCONNECT=brokerConnect.conf
/opt/InCharge/SAM/smarts/bin/brstart
--port=426
 --restore=/opt/InCharge/SAM/smarts/local/repos/broker/broker.rps
 --outputs
```

Service Assurance Manager (Presentation SAM server)

UNIX

```
/opt/InCharge/SAM/smarts/bin/sm_service install
--force
--unmanaged
--startmode=runonce
--name=ic-sam-server-pres
--description="VMware Smarts Service Assurance Manager Server (notification cache publishing)"
/opt/InCharge/SAM/smarts/bin/sm_server
-n INCHARGE-SA-PRES
--config=ics
--port=0
--edaa=sam-presentation/2.0
--bootstrap=bootstrap-amqp.conf
--ignore-restore-errors
--output
```

Service Assurance Manager (Global Manager)

UNIX

```
t/opt/InCharge/SAM/smarts/bin/sm_service install
 --force
 --unmanaged
 --name=ic-sam-server
 --startmode=runonce
 --description="VMware Smarts Service Assurance Manager
  Server"
 /opt/InCharge/SAM/smarts/bin/sm_server
 --name=INCHARGE-SA
 --config=ics
 --port=0
 --ignore-restore-errors
 --outputs
```

Business Impact Manager server

UNIX

```
t/opt/InCharge/SAM/smarts/bin/sm_service install
--startmode=runonce
--name=MBIM
--description="VMware Smarts MBIM - Maintenance and Business Impact Manager Server"
/opt/InCharge/SAM/smarts/bin/sm_server
--name=INCHARGE-MBIM
```

```
--config=bim
--port=0
--ignore-restore-errors
--outputs
```

Adapter Platform

UNIX

```
t /opt/InCharge/SAM/smarts/bin/sm_service install
 --force
 --unmanaged
 --name=ic-icoi-server
 --startmode=runonce
 --description="VMware Smarts SAM Adapter Platform Server"
 /opt/InCharge/SAM/smarts/bin/sm_server
 --name=INCHARGE-OI
 --config=icoi
 --port=0
 --ignore-restore-errors
 --outputs
```

Business Dashboard

UNIX

```
t/opt/InCharge/CONSOLE/smarts/bin/sm_service install
 --force
 --unmanaged
 --name=ic-business-dashboard
 --startmode=runonce
 --description="VMware Smarts Servlet Engine"
 /opt/InCharge/CONSOLE/smarts/bin/sm_tomcat
 --output
 starts
```

Syslog Adapter

Before you configure the Syslog Adapter, identify the location of the SYSFILE you want the adapter to tail and parse and ensure that sm_service install command line for the ic-syslog-adapter identifies this location. The *VMware Smart Assurance Service Assurance Manager Adapter Platform User Guide* provides more information on configuring the Syslog Adapter.

UNIX

```
t /opt/InCharge/SAM/smarts/bin/sm_service install
 --force
 --unmanaged
 --name=ic-syslog-adapter
 --startmode=runonce
 --description="VMware Smarts Syslog Adapter"
 /opt/InCharge/SAM/smarts/bin/sm_adapter
 --name=SYSLOG-INCHARGE-OI
 --rserver=INCHARGE-OI
 --tail=/var/log/syslog
 --model=sm_system
 --model=sm_actions
 --output icoi-syslog/syslog_mgr.asls
```

SNMP Trap Adapter

UNIX

```
t /opt/InCharge/SAM/smarts/bin/sm_service install
 --force
 --unmanaged
 --name=ic-trapd-receiver
 --startmode=runonce
 --description="VMware Smarts SNMP Trap Adapter"
 /opt/InCharge/SAM/smarts/bin/sm_trapd
 --name=TRAP-INCHARGE-OI
 --server=INCHARGE-OI
 --config=icoi
 --port=162
 --seed=seedfile
 --model=sm_actions
 --output
 --rules=icoi-trapd/trap_mgr_parse.asls
```

Notif trap Adapter

UNIX

```
t /opt/InCharge/SAM/smarts/bin/sm_service install --force -unmanaged
--startmode=runonce
--name=ic-notif-trapd-receiver
--description="VMware Smarts NOTIF SNMP Trap Adapter"
/opt/InCharge/SAM/smarts/bin/sm_trapd
--name=NOTIF-TRAP-INCHARGE-OI
--server=INCHARGE-OI
--config=icoi
--port=162
```

```
--model=sm_actions
--rules=icoi-trapd/Notif-trap_mgr_parse.asl
--seed=seedfile
--outputs
```

Notif syslog adapter

UNIX

```
t /opt/InCharge/SAM/smarts/bin/sm_service install --force --unmanaged
--startmode=runonce
--name=ic-notif-syslog-adapter
--description="VMware Smarts Syslog Adapter"
/opt/InCharge/SAM/smarts/bin/sm_adapter
--name=NOTIF-SYSLOG-INCHARGE-OI
--rserver=INCHARGE-OI
--tail=/var/log/syslog
--model=sm_system
--model=sm_actions
--output icoi-syslog/Notif-SysLog_mgr.asls
```

Smarts Data Web Applications (Tomcat)

UNIX

```
/opt/InCharge/SAM/smarts/bin/sm_service install --force  --unmanaged  --startmode=runonce
--name=smarts-tomcat
--description="VMware Smarts Data Web Applications (Tomcat)"
/opt/InCharge/SAM/smarts/bin/sm_tomcat
--ignoreme
```

Smarts Notification Exchange (Rabbit MQ)

UNIX

```
/opt/InCharge/SAM/smarts/bin/sm_service install --force
--unmanaged  --startmode=runonce
--name=smarts-rabbitmq
--description="VMware Smarts Notification Exchange (Rabbit MQ)"
/opt/InCharge/SAM/smarts/bin/sm_rabbitmq
--ignoreme
```

Smarts Notification Cache (ElasticSearch)

UNIX

```
/opt/InCharge/SAM/smarts/bin/sm_service install --force
--unmanaged  --startmode=runonce
--name=smarts-elasticsearch
--description="VMware Smarts Notification Cache (ElasticSearch)"
/opt/InCharge/SAM/smarts/bin/sm_elasticsearch
--ignoreme
```

Services for the MPLS Management Suite

This section provides the default UNIX commands that are used to install services manually for the MPLS Management Suite. Type the command on one line.

For the MPLS Management Suite, when you install the services manually, if you specify custom service and server names instead of the default names listed in Services for the MPLS Manager, you must run a script next. Running the script is required so that proper domain communication can be established. Chapter 13 Using the MPLS server_config Utility provides information about the script.

MPLS Topology Server

When you start the MPLS Manager for the first time (and only the first time) after migrating from the previous version to the new version, you must start the MPLS Topology Server with the --ignore-restore-errors option.

UNIX

```
t /opt/InCharge/MPLS/smarts/bin/sm_service install
--force
--unmanaged
--startmode=runonce
--name=ic-mpls-topology
--description="VMware Smart Assurance
         MPLS Topology Server"
/opt/InCharge/MPLS/smarts/bin/sm_server
--name=INCHARGE-MPLS-TOPOLOGY
--config=mpls-t
--ignore-restore-errors
--outputs
```

MPLS Monitoring Server

UNIX

```
t/opt/InCharge/MPLS/smarts/bin/sm_service install
--force
--unmanaged
--startmode=runonce
--name=ic-mpls-monitoring
--description="VMware Smart Assurance
         MPLS Monitoring Server"
/opt/InCharge/MPLS/smarts/bin/sm_server
--name=INCHARGE-MPLS-MONITORING
--config=mpls-m
--ignore-restore-errors
--outputs
```

MPLS Analysis Server

UNIX

```
t /opt/InCharge/MPLS/smarts/bin/sm_service install
--force
--unmanaged
--startmode=runonce
--name=ic-mpls-analysis
--description="VMware Smart Assurance
         MPLS Analysis Server"
/opt/InCharge/MPLS/smarts/bin/sm_server
--name=INCHARGE-MPLS-ANALYSIS
--config=mpls-a
--ignore-restore-errors
--outputs
```

MPLS VPN-Tagging Server

UNIX

```
t /opt/InCharge/MPLS/smarts/bin/sm_service install
--force
--unmanaged
--startmode=runonce
--name=ic-vpn-tagging
--description="VMware Smart Assurance
         MPLS VPN-Tagging Server"
/opt/InCharge/MPLS/smarts/bin/sm_server
--name=VPN-TAGGING
--config=vpn-tagging
--ignore-restore-errors
--outputs
```

Services for the Server Manager

This section provides the default UNIX commands that are used to install the service manually for the VMware Smart Assurance Server Manager. Type the command on one line.

Server Manager

UNIX

```
t opt/InCharge/ESM/smarts/bin/sm_service install
 --force
 --unmanaged
 --name=ic-esm-server
 --description="VMware Smarts Server Manager (ESM)"
 --startmode=runonce
 opt/InCharge/ESM/smarts/bin/sm_server
 --name=INCHARGE-ESM
 --config=esm
 --subscribe=default
 --output
--ignore-restore-errorss
```

Services for the Network Protocol Management Suite installation

This section provides the default UNIX commands that are used to install services manually for the Network Protocol Management Suite. Type the command on one line.

Network Protocol Manager for BGP

UNIX (IPv6 and IPv4 mode)

```
/opt/InCharge/NPM/smarts/bin/sm_service install
--force
--name=ic-npm-bgp-server
--description="VMware Smarts NPM for BGP Server"
--startmode=runonce
/opt/InCharge/NPM/smarts/bin/sm_server
--name=INCHARGE-BGP
--config=bgp
--port=0
--subscribe=default
--output
```

UNIX (IPv4 mode only)

```
/opt/InCharge/NPM/smarts/bin/sm_service install
--force
--name=ic-npm-bgp-server
--description="VMware Smarts NPM for BGP Server"
--startmode=runonce
/opt/InCharge/NPM/smarts/bin/sm_server
--name=INCHARGE-BGP
--config=bgp
--port=0
--bootstrap=bootstrap-ipv4.conf
--subscribe=default
--output
```

Network Protocol Manager for EIGRP

UNIX

```
/opt/InCharge/NPM/smarts/bin/sm_service install
--force
--name=ic-npm-eigrp-server
--description="VMware Smarts NPM for EIGRP Server"
--startmode=runonce
/opt/InCharge/NPM/smarts/bin/sm_server
--name=INCHARGE-EIGRP
--config=eigrp
--port=0
--subscribe=default
--ignore-restore-errors
--output
```

Network Protocol Manager for IS-IS

UNIX (IPv6 and IPv4 mode)

```
/opt/InCharge/NPM/smarts/bin/sm_service install
--force
--name=ic-npm-isis-server
--description="VMware Smarts NPM for ISIS Server"
--startmode=runonce
/opt/InCharge/NPM/smarts/bin/sm_server
--name=INCHARGE-ISIS
--config=isis
--port=0
--subscribe=default
--output
```

UNIX (IPv4 mode only)

```
/opt/InCharge/NPM/smarts/bin/sm_service install
--force
--name=ic-npm-isis-server
--description="VMware Smarts NPM for ISIS Server"
--startmode=runonce
/opt/InCharge/NPM/smarts/bin/sm_server
--name=INCHARGE-ISIS
--config=isis
--port=0
--bootstrap=bootstrap-ipv4.conf
--subscribe=default
--output
```

Network Protocol Manager for OSPF

UNIX (IPv6 and IPv4 mode)

```
/opt/InCharge/NPM/smarts/bin/sm_service install
--force
--name=ic-npm-ospf-server
--description="VMware Smarts NPM for OSPF Server"
--startmode=runonce
/opt/InCharge/NPM/smarts/bin/sm_server
--name=INCHARGE-OSPF
--config=ospf
--port=0
--subscribe=default
--output
```

UNIX (IPv4 mode only)

```
/opt/InCharge/NPM/smarts/bin/sm_service install
--force
--name=ic-npm-OSPF-server
--description="VMware Smarts NPM for OSPF Server"
--startmode=runonce
/opt/InCharge/NPM/smarts/bin/sm_server
--name=INCHARGE-OSPF
--config=ospf
--port=0
--bootstrap=bootstrap-ipv4.conf
--subscribe=default
--output
```

Procedures for CD/DVD-ROMs 12

Mounting a CD/DVD-ROM on UNIX systems

Use the following procedure to find the instructions appropriate for your operating system:

1 Insert the CD/DVD-ROM into the optical drive.

2 If the CD/DVD-ROM is automatically mounted, continue to step 3 . Otherwise, select the appropriate mount command as shown in Mounting the CD/DVD-ROM for UNIX operating systems.

Table 12-1. Mounting the CD/DVD-ROM for UNIX operating systems

Operating system	Commands and examples

CentOS	`# mount –o ro –F hsfs <device> /mnt`
	Example:
	`# mount –o ro –F hsfs /dev/dsk/c0t6d0s0 /mnt`

HP-UX	`mount –ocdcase –o ro –F cdfs <DEVICE> /mnt/cdrom` `mount –ocdcase –o ro –F cdfs /dev/cdrom /mnt/cdrom`

Linux	`# mount <device>`
	Example:
	`# mount /dev/cdrom /mnt/cdrom`

where *<device>* is the mount point for the optical drive.	

1 Change to the CD/DVD-ROM directory by typing the appropriate command from Changing to the CD/DVD-ROM directory in UNIX operating systems.

Table 12-2. Changing to the CD/DVD-ROM directory in UNIX operating systems

Operating system	Command

CentOS	If Volume Manager (VM) is running:
	`# cd /cdrom/<os>/<product>_SUITE/suite`
	If VM is not running:
	`# cd /mnt/suite`

HP-UX	`# cd /mnt/cdrom/suite`

Linux	If Automount is running:
	`# cd /cdrom/<os>/<product>_SUITE/suite`
	If Automount is not running:
	`# cd /mnt/cdrom/suite`

where: *<os>* is the operating system, for example, CentOS_64, linux_64, or winnt_64. *<product>* is the product software, for example, IP or MPLS.	

Using the MPLS server_config Utility

13

Use the server_config.pl script to change domain names

Purpose

When installed and unless the default domain name is changed during installation, MPLS Manager is configured with the default domain group name of INCHARGE-MPLS.

From this default domain group name, the three MPLS Manager server names are constructed by appending the function specific suffix to the default domain group name:

- INCHARGE-MPLS-TOPOLOGY
- INCHARGE-MPLS-MONITORING
- INCHARGE-MPLS-ANALYSIS

Note TOPOLOGY, MONITORING, and ANALYSIS are always appended to the Domain Group name to generate the three MPLS Manager domain managers.

A script (*server_config.pl*) is provided to make it easier to define server names, to update names, and populate the domain names changes to the default configurations files. Once updated, these new domain names are used by the TOPOLOGY, MONITORING and ANALYSIS servers.

Run the script

After the different servers have been installed with the default domain manager's names, you can use the server_config script to customize the domain managers' names.

The MPLS Manager post installation script uses the *sm_perl* command from either the MPLS BASEDIR/smarts/bin directory or from the location where the *server_config.pl* post installation script is located.

From the Perl /bin directory

Invoke the post installation script from the directory where the MPLS Manager post installation script is located.

```
sm_perl server_config.pl –o <OldGroupName> –n <NewGroupName> –b <BASEDIR>
```

From the MPLS installation directory

Invoke the post installation script from the directory where Perl is installed.

```
   ./sm_perl <BASEDIR>/smarts/script/mpls–tma/server_config.pl –o <OldGroupName> –n
<NewGroupName> –b <BASEDIR>
```

Invoke the command line script *server_config.pl* options from the *BASEDIR/smarts/bin/* directory as follows:

- Install services with default name if they have not been installed previously (see Example).

  server_config.pl -i -o <OldGroupName> -n<NewGroupName> -b<BASEDIR>

- Rename services that have been installed previously (see Example).

  server_config.pl -o <OldGroupName> -n<NewGroupName> -b<BASEDIR>

- Generate a list of services that have been installed previously (see Example).

  server_config.pl -s -b <BASEDIR>

- Display information on how to run the script with examples (see Example).

  server_config.pl -h

Example 1

```
server_config.pl –i –o “INCHARGE–MPLS” –n “HQ–MPLS” –b opt/InCharge/MPLS/smarts/
```

Example 2

```
server_config.pl –o “INCHARGE–MPLS” –n “HQ–MPLS” –b opt/InCharge/MPLS/smarts/
```

Example 3

```
server_config.pl –s –b opt/InCharge/MPLS/smarts/
```

Example 4

```
server_config.pl –h
```

Script options

Following are the required and optional command line script parameters:

Note Avoid using the following special characters when entering text strings for <OldGroupName> and <NewGroupName>: $ / \

Table 13-1. server_config.pl script command line options

Option	Purpose
--install-service or -i	Indicates that the service needs to be installed. ■ This parameter must be used with the --old-group, --new-group, and --basedir parameters. ■ If the services are not installed, they are installed. ■ If services are already installed, they are uninstalled and reinstalled with the NewGroupName.
--old-group="<OldGroupName>" or -o "<OldGroupName>"	A required value that specifies the old group name to be changed. ■ You must include the OldGroupName variable string in double quotes. ■ This parameter must be used with the --new-group and --basedir parameters. ■ If services are running, will terminate without doing anything.
--new-group="<NewGroupName>" or -n "<NewGroupName>"	A required value that specifies the new group name. ■ You must include the NewGroupName variable string in double quotes. ■ This parameter must be used with the --old-group and --basedir parameters. ■ If services are running, will terminate without doing anything.
--basedir=<BASEDIR> or -b <BASEDIR>	A required value which specifies the installation base directory. ■ This parameter must be used with the --old-group and --new-group parameters. ■ If services are running, will terminate without doing anything.
--show or -s	Indicates that you want to see the current group names, services and Domain Manager names. ■ With this option, no changes are made to either the service or the configuration file. ■ This parameter must be used with the --basedir parameter.
--help or -h	--help or -h shows command line parameters and examples. This parameter is used alone.

Note The order of the parameters is not important.

Always include the BASEDIR of the installed services in the command line. The only instances where you do not have to include it is when using the Help (-h) option.

Following are the steps that the script performs once invoked:

1 If the local directory *BASEDIR/smarts/local/conf/mpls-tma* does not already exist, it is created and a copy of the original mpls-tma.conf file from the *BASEDIR/smarts/conf/mpls-tma* directory is copied to it.

2 If a service corresponding to the <OldGroupName> is installed, the following process is initiated:

3 If the service is running and the user command line argument is not -s or --show, the script displays an error message and exits. You must stop the services before you can rename them.

4 If the service is not running and the Service Daemon is running, then the script uninstalls the service for the current <OldGroupName>, installs the service for the <NewGroupName>, then continues to step 4.

5 If the service is not running and the Service Daemon is not running, then the script displays a warning that there is potential for mismatch, uninstalls the service for the current <OldGroupName>, installs the service for the <NewGroupName>, then continues to step 4.

6 If a service corresponding to the <OldGroupName> is not installed, the following process is initiated:

7 If the installation option (--i or -install-service) is not specified, the scripts does not install the service.

8 If the installation option (--i or -install-service) is specified and if the Service Daemon is running, the script installs the service corresponding to the <NewGroupName>.

9 If the installation option (--i or -install-service) is specified and if the Service Daemon is not running, the script warns you that you must start it and exits without further action.

10 After step 2 or step 3 are performed, the script copies the previous local configuration file to a backup file named .<OldGroupName><.bak>

11 The script then replaces the <OldGroupName> with <NewGroupName> in *BASEDIR/smarts/local/conf/mpls-tma/mpls-tma.conf* and terminates.

Configuration Scanner tool Sample Output

14

This chapter includes the following topics:

- Files created by Configuration Scanner tool
- Sample outputs

Files created by Configuration Scanner tool

The following files are created by the tool:

- sm_configscan_report-<time_stamp>.txt: This is the report file created by the Configuration Scanner tool. This file contains:
  - List of files installed by the TTP, if any
  - List of files introduced by the user
  - Modifications made to the discovery.conf, tpmgr-param.conf and name-resolver.conf files
  - List of file differences for each modified file
  - List of modifications found in the server

    Report when server is specified and Report when server is not specified provides sample outputs.
- sm_configscan-<time_stamp>.tar: This tar file contains the following:
  - A copy of the Configuration Scanner report file
  - sm_configscanner.log
  - A copy of runcmd_env.sh
  - ConfigScanAdapter.log
  - PnTallOutput.txt: lists all the settings found on the server
  - A directory containing the DIFF files for each modified files

    The output files for the configuration scanner tool is available under the

    <**BASEDIR**>/smarts/local/logs/Final_sm_getinfo<timesatamp>.tar file.

Sample outputs

This section provides sample outputs for the following:

- Running Configuration Scanner tool with server name
- Report when server is specified
- Running Configuration Scanner tool without server name
- Report when server is not specified

Running Configuration Scanner tool with server name

You can run the tool by specifying a running server in the command line. In this scenario, the tool scans for changes you have made in the values of both the polling and threshold settings and configuration files. A sample output is provided:

```
C:\InCharge\IP\smarts\bin>sm_perl sm_getinfo -s INCHARGE-AMPM -k
Executing sm_configscan ...
================================================================sm_monitor about to run!
Please enter the correct credentials in clientConnect.conf
Or be prepared to enter the credentials below:
================================================================Getting hardware Info...
Getting AMPM show-dm-process info...
MAIN-N-Closing this log file at August 28, 2012 4:02:24 AM EDT; continuing in
C:\InCharge\IP\smarts\local\logs\AMPM-show-dm-proc-28Aug2012-040223_en_US_UTF-8.log
Getting AMPM stacktrace info...
Exiting eval via last at C:/InCharge/IP/smarts/bin//sm_monitor.pl line 180.
Getting AMPM queues info...
Getting AMPM subscriptions info...
Getting AMPM threads info...
Getting AMPM flows info...
Getting AMPM clients info...
Getting netstat info...
Getting tasklist info...
Getting log file...
Getting rps files...
Getting Monitor...
Getting Accessor Ping...
Getting Accessor Poll...
Getting Problems...
Getting instrumentation for IP...
MAIN-N-Closing this log file at August 28, 2012 4:05:13 AM EDT; continuing in
C:\InCharge\IP\smarts\local\logs\AMPM-instrumentation-28Aug2012-040223_en_US_UTF-8.log
Deleting files: C:\InCharge\IP\smarts\local\logs\smgetinfo_files\*smgetinfo-versions.log*
Getting the Smarts server version ...
Getting the Executable versions ...
Getting the Local lib versions ...
Getting the lib versions ...
Getting the list of installed TTPs ...
No TTPs currently installed
No patches currently installed.
```

```
Archiving the files...
Writing to sm_getinfo28Aug2012-040132.tar.zip ...
... Done writing to Final_sm_getinfo28Aug2012-040132.tar.zip
Please send the file: C:\InCharge\IP\smarts\local\logs\Final_sm_getinfo28Aug2012-040132.tar.zip to
VMware Support
```

Report when server is specified

The following is the sample of the report when the tool is run specifying a running server in the command line:

```
Version: IP.9.1.0.0
These files have been modified in the installation:
=====================================================
C:/InCharge/IP/smarts/local/conf/discovery/discovery.conf
C:/InCharge/IP/smarts/local/conf/discovery/name-resolver.conf
C:/InCharge/IP/smarts/local/conf/discovery/oid2type_Cisco.conf
C:/InCharge/IP/smarts/local/conf/discovery/oid2type_Misc.conf
C:/InCharge/IP/smarts/local/conf/discovery/tpmgr-param.conf
These files have been introduced in the installation:
=====================================================
C:/InCharge/IP/smarts/local/repos/icf/INCHARGE-AMPM.rps
C:/InCharge/IP/smarts/local/repos/icf/INCHARGE-AMPM.rps.bak
Server Name: INCHARGE-AMPM
The following Polling and Threshold settings were modified in the installation:
=============================================================
POLLING::Polling Groups::5620 SAM Managed Systems::Connectivity Polling - External
Poller::InstrumentCards
  Current Value : TRUE
  Default Value : FALSE
POLLING::Polling Groups::ComputeFabric::Environment Polling::PollingInterval
  Current Value : 120
  Default Value : 240
POLLING::Polling Groups::ComputeFabric::Environment Polling::Retries
  Current Value : 4
  Default Value : 3
POLLING::Polling Groups::ComputeFabric::Connectivity Polling::PollingInterval
  Current Value : 30
  Default Value : 240
POLLING::Polling Groups::Routers::Environment Polling::PollingInterval
  Current Value : 30
  Default Value : 240
THRESHOLD::Interface Groups::1 Gb Ethernet::Ethernet Interface/Port Performance::BroadcastThreshold
  Current Value : 10
  Default Value : 15
The following changes were made to some special configuration files:
=============================================================
File: C:/InCharge/IP/smarts/local/conf/discovery/discovery.conf
  Attribute Name : MetroEthernetEnabled
    Current Value  : TRUE
    Default Value  : FALSE
    Comment        : Modified
  Attribute Name : defaultTimeout
```

```
      Current Value  : 2000
      Default Value  : 1000
      Comment        : Modified
    Attribute Name : defaultRetries
      Current Value  : 8
      Default Value  : 5
      Comment        : Modified
    Attribute Name : defaultSNMPAutoRetries
      Current Value  : 4
      Default Value  : 3
      Comment        : Modified
    Attribute Name : DiscoveryAddrPref
      Current Value  : "IPV4FIRST_IPV6NEXT"
      Default Value  : "IPV6FIRST_IPV4NEXT"
      Comment        : Modified
    Attribute Name : numberProbeThreads
      Current Value  : 15
      Default Value  : 10
      Comment        : Modified
    Attribute Name : LicenseThresholdPercentage
      Current Value  : 40
      Default Value  : 90
      Comment        : Modified
  File: C:/InCharge/IP/smarts/local/conf/discovery/name-resolver.conf
    Attribute Name : NameFormat
      Current Value  : "TM_USESEEDNAME"
      Default Value  : "TM_USEAUTONAME"
      Comment        : Modified
    Attribute Name : TM_USEAGENTADDRESS
      Current Value  : 3
      Default Value  : 4
      Comment        : Modified
    Attribute Name : TM_USEPRIVATEIP
      Current Value  : 4
      Default Value  : 3
      Comment        : Modified
  File: C:/InCharge/IP/smarts/local/conf/discovery/tpmgr-param.conf
    Attribute Name : maxOIDsPerPacketForASNMP
      Current Value  : 15
      Default Value  : 19
      Comment        : Modified
    Attribute Name : GetBulkPattern-.1.3.6.1.4.1.1872.1.15
      Current Value  : TRUE
      Default Value  :
      Comment        : Newly added
    Attribute Name : GetBulkRetriesOverrideRatio-.1.3.6.1.4.1.1872.1.15
      Current Value  : 1.5
      Default Value  :
      Comment        : Newly added
    Attribute Name : GetBulkTimeoutOverrideRatio-.1.3.6.1.4.1.1872.1.15
      Current Value  : 2.5
      Default Value  :
      Comment        : Newly added
    Attribute Name : IFTypePatternIFExt.1.3.6.1.4.1.119.1.3.13.4
      Current Value  :
```

```
    Default Value  : 39|53|1
    Comment        : Removed
  Attribute Name : IFTypePattern-SwitchPort.1.3.6.1.4.1.119.1.14.8
    Current Value  :
    Default Value  : 37
    Comment        : Removed
The following are two way text differences:
==========================================
<--- C:/InCharge/IP/smarts/conf/discovery/discovery.conf --->
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 54 to 54 >>>>>>>>>>>>>>
defaultRetries = 5
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 54 to 54 <<<<<<<<<<<<<<
defaultRetries = 8
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 61 to 61 >>>>>>>>>>>>>>
defaultTimeout = 1000
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 61 to 61 <<<<<<<<<<<<<<
defaultTimeout = 2000
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 82 to 82 >>>>>>>>>>>>>>
defaultSNMPAutoRetries = 3
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 82 to 82 <<<<<<<<<<<<<<
defaultSNMPAutoRetries = 4
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 97 to 97 >>>>>>>>>>>>>>
numberProbeThreads = 10
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 97 to 97 <<<<<<<<<<<<<<
numberProbeThreads = 15
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 280 to 280 >>>>>>>>>>>>>>
DiscoveryAddrPref =  "IPV6FIRST_IPV4NEXT"
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 280 to 280 <<<<<<<<<<<<<<
DiscoveryAddrPref =  "IPV4FIRST_IPV6NEXT"
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 287 to 287 >>>>>>>>>>>>>>
MetroEthernetEnabled = FALSE
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 287 to 287 <<<<<<<<<<<<<<
```

```
MetroEthernetEnabled = TRUE
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 290 to 290 >>>>>>>>>>>>>>
LicenseThresholdPercentage = 90
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 290 to 290 <<<<<<<<<<<<<<
LicenseThresholdPercentage = 40
<=============== End Difference ===============>
<------------------------------------------------>
<--- C:/InCharge/IP/smarts/conf/discovery/name-resolver.conf --->
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 19 to 18 >>>>>>>>>>>>>>
#NameFormat = "TM_USESEEDNAME"
NameFormat = "TM_USEAUTONAME"
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 18 to 19 <<<<<<<<<<<<<<
NameFormat = "TM_USESEEDNAME"
#NameFormat = "TM_USEAUTONAME"
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 30 to 29 >>>>>>>>>>>>>>
AutoNameOrder 3 TM_USEPRIVATEIP
AutoNameOrder 4 TM_USEAGENTADDRESS
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 29 to 30 <<<<<<<<<<<<<<
AutoNameOrder 3 TM_USEAGENTADDRESS
AutoNameOrder 4 TM_USEPRIVATEIP
<=============== End Difference ===============>
<------------------------------------------------>
<--C:/InCharge/IP/smarts/conf/discovery/oid2type_Cisco.conf ->
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 12369 to 12370 >>>>>>>>>>>>>>
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 12370 to 12384 <<<<<<<<<<<<<<
.1.3.6.1.4.1.9.1.916 {
TYPE = Firewall
VENDOR = Cisco
MODEL = ciscoASA5580sc
CERTIFICATION = CERTIFIED
CONT = Cisco-Entity
HEALTH = Cisco-Entity
INSTRUMENTATION:
CPU/Memory = CiscoRouter:DeviceID
Interface-Fault = MIB2
Interface-Performance = MIB2
}
<=============== End Difference ===============>
<------------------------------------------------>
<--C:/InCharge/IP/smarts/conf/discovery/oid2type_Misc.conf -->
<============== Start Difference ==============>
```

```
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 8816 to 8806 >>>>>>>>>>>>>>
.1.3.6.1.4.1.10734.1.3.8 {
TYPE = Firewall
VENDOR = TippingPoint
MODEL = TippingPointIPS
CERTIFICATION = CERTIFIED
CONT = MIB2-IfStack
INSTRUMENTATION:
Interface-Fault = MIB2
Interface-Performance     = MIB2
}
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 8806 to 8816 <<<<<<<<<<<<<<
#.1.3.6.1.4.1.10734.1.3.8 {
# TYPE = Firewall
# VENDOR = TippingPoint
# MODEL = TippingPointIPS
# CERTIFICATION = CERTIFIED
# CONT = MIB2-IfStack
#
#INSTRUMENTATION:
# Interface-Fault = MIB2
# Interface-Performance = MIB2
#}
<=============== End Difference ===============>
<------------------------------------------------------------>
<--C:/InCharge/IP/smarts/conf/discovery/tpmgr-param.conf --->
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 40 to 40 >>>>>>>>>>>>>>
IFTypePatternIFExt.1.3.6.1.4.1.119.1.3.13.4 39|53|1
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 40 to 40 <<<<<<<<<<<<<<
#IFTypePatternIFExt.1.3.6.1.4.1.119.1.3.13.4 39|53|1
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 125 to 125 >>>>>>>>>>>>>>
IFTypePattern-SwitchPort.1.3.6.1.4.1.119.1.14.8 37
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 125 to 125 <<<<<<<<<<<<<<
#IFTypePattern-SwitchPort.1.3.6.1.4.1.119.1.14.8 37
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 554 to 554 >>>>>>>>>>>>>>
#GetBulkPattern-.1.3.6.1.4.1.1872.1.15 TRUE
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 554 to 554 <<<<<<<<<<<<<<
GetBulkPattern-.1.3.6.1.4.1.1872.1.15 TRUE
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 565 to 565 >>>>>>>>>>>>>>
```

```
#GetBulkTimeoutOverrideRatio-.1.3.6.1.4.1.1872.1.15 2.5
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 565 to 565 <<<<<<<<<<<<<<
GetBulkTimeoutOverrideRatio-.1.3.6.1.4.1.1872.1.15 2.5
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 576 to 576 >>>>>>>>>>>>>>
#GetBulkRetriesOverrideRatio-.1.3.6.1.4.1.1872.1.15 1.5
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 576 to 576 <<<<<<<<<<<<<<
GetBulkRetriesOverrideRatio-.1.3.6.1.4.1.1872.1.15 1.5
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 582 to 582 >>>>>>>>>>>>>>
maxOIDsPerPacketForASNMP 19
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 582 to 582 <<<<<<<<<<<<<<
maxOIDsPerPacketForASNMP 15
<=============== End Difference ===============>
<------------------------------------------------>
```

Running Configuration Scanner tool without server name

You can run the tool without specifying a running server in the command line. In this scenario, the tool only scans for changes you made to the configuration files. A sample output is provided:

```
C:\InCharge\IP\smarts\bin>sm_perl sm_getinfo -k
Executing sm_configscan ...
Deleting files: C:\InCharge\IP\smarts\local\logs\smgetinfo_files\*smgetinfo-versions.log*
Getting the Smarts server version ...
Getting the Executable versions ...
Getting the Local lib versions ...
Getting the lib versions ...
Getting the list of installed TTPs ...
No TTPs currently installed
No patches currently installed.
Archiving the files...
Writing to sm_getinfo28Aug2012-044639.tar.zip ...
... Done writing to Final_sm_getinfo28Aug2012-044639.tar.zip
Please send the file: C:\InCharge\IP\smarts\local\logs\Final_sm_getinfo28Aug2012-044639.tar.zip to
VMware Support
```

Report when server is not specified

The following is the sample of the report when the tool is run without specifying a running server in the command line:

```
Version: IP.9.1.0.0
These files have been modified in the installation:
====================================================
C:/InCharge/IP/smarts/local/conf/discovery/discovery.conf
C:/InCharge/IP/smarts/local/conf/discovery/name-resolver.conf
C:/InCharge/IP/smarts/local/conf/discovery/oid2type_Cisco.conf
C:/InCharge/IP/smarts/local/conf/discovery/oid2type_Misc.conf
C:/InCharge/IP/smarts/local/conf/discovery/tpmgr-param.conf
These files have been introduced in the installation:
====================================================
C:/InCharge/IP/smarts/local/repos/icf/INCHARGE-AMPM.rps
C:/InCharge/IP/smarts/local/repos/icf/INCHARGE-AMPM.rps.bak
The following changes were made to some special configuration files:
=================================================================
File: C:/InCharge/IP/smarts/local/conf/discovery/discovery.conf
  Attribute Name : MetroEthernetEnabled
    Current Value  : TRUE
    Default Value  : FALSE
    Comment        : Modified
  Attribute Name : defaultTimeout
    Current Value  : 2000
    Default Value  : 1000
    Comment        : Modified
  Attribute Name : defaultRetries
    Current Value  : 8
    Default Value  : 5
    Comment        : Modified
  Attribute Name : defaultSNMPAutoRetries
    Current Value  : 4
    Default Value  : 3
    Comment        : Modified
  Attribute Name : DiscoveryAddrPref
    Current Value  : "IPV4FIRST_IPV6NEXT"
    Default Value  : "IPV6FIRST_IPV4NEXT"
    Comment        : Modified
  Attribute Name : numberProbeThreads
    Current Value  : 15
    Default Value  : 10
    Comment        : Modified
  Attribute Name : LicenseThresholdPercentage
    Current Value  : 40
    Default Value  : 90
    Comment        : Modified
File: C:/InCharge/IP/smarts/local/conf/discovery/name-resolver.conf
  Attribute Name : NameFormat
    Current Value  : "TM_USESEEDNAME"
    Default Value  : "TM_USEAUTONAME"
    Comment        : Modified
```

```
  Attribute Name : TM_USEAGENTADDRESS
    Current Value  : 3
    Default Value  : 4
    Comment        : Modified
  Attribute Name : TM_USEPRIVATEIP
    Current Value  : 4
    Default Value  : 3
    Comment        : Modified
File: C:/InCharge/IP/smarts/local/conf/discovery/tpmgr-param.conf
  Attribute Name : maxOIDsPerPacketForASNMP
    Current Value  : 15
    Default Value  : 19
    Comment        : Modified
  Attribute Name : GetBulkPattern-.1.3.6.1.4.1.1872.1.15
    Current Value  : TRUE
    Default Value  :
    Comment        : Newly added
  Attribute Name : GetBulkRetriesOverrideRatio-.1.3.6.1.4.1.1872.1.15
    Current Value  : 1.5
    Default Value  :
    Comment        : Newly added
  Attribute Name : GetBulkTimeoutOverrideRatio-.1.3.6.1.4.1.1872.1.15
    Current Value  : 2.5
    Default Value  :
    Comment        : Newly added
  Attribute Name : IFTypePatternIFExt.1.3.6.1.4.1.119.1.3.13.4
    Current Value  :
    Default Value  : 39|53|1
    Comment        : Removed
  Attribute Name : IFTypePattern-SwitchPort.1.3.6.1.4.1.119.1.14.8
    Current Value  :
    Default Value  : 37
    Comment        : Removed
The following are two way text differences:
==========================================
<--- C:/InCharge/IP/smarts/conf/discovery/discovery.conf --->
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 54 to 54 >>>>>>>>>>>>>>
defaultRetries = 5
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 54 to 54 <<<<<<<<<<<<<<
defaultRetries = 8
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 61 to 61 >>>>>>>>>>>>>>
defaultTimeout = 1000
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 61 to 61 <<<<<<<<<<<<<<
defaultTimeout = 2000
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 82 to 82 >>>>>>>>>>>>>>
```

```
defaultSNMPAutoRetries = 3
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 82 to 82 <<<<<<<<<<<<<<
defaultSNMPAutoRetries = 4
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 97 to 97 >>>>>>>>>>>>>>
numberProbeThreads = 10
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 97 to 97 <<<<<<<<<<<<<<
numberProbeThreads = 15
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 280 to 280 >>>>>>>>>>>>>>
DiscoveryAddrPref =  "IPV6FIRST_IPV4NEXT"
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 280 to 280 <<<<<<<<<<<<<<
DiscoveryAddrPref =  "IPV4FIRST_IPV6NEXT"
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 287 to 287 >>>>>>>>>>>>>>
MetroEthernetEnabled = FALSE
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 287 to 287 <<<<<<<<<<<<<<
MetroEthernetEnabled = TRUE
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 290 to 290 >>>>>>>>>>>>>>
LicenseThresholdPercentage = 90
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 290 to 290 <<<<<<<<<<<<<<
LicenseThresholdPercentage = 40
<=============== End Difference ===============>
<------------------------------------------------>
<--C:/InCharge/IP/smarts/conf/discovery/name-resolver.conf -->
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 19 to 18 >>>>>>>>>>>>>>
#NameFormat = "TM_USESEEDNAME"
NameFormat = "TM_USEAUTONAME"
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 18 to 19 <<<<<<<<<<<<<<
NameFormat = "TM_USESEEDNAME"
#NameFormat = "TM_USEAUTONAME"
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 30 to 29 >>>>>>>>>>>>>>
AutoNameOrder 3 TM_USEPRIVATEIP
AutoNameOrder 4 TM_USEAGENTADDRESS
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
```

```
<<<<<<<<<<<<<< From line: 29 to 30 <<<<<<<<<<<<<<
AutoNameOrder 3 TM_USEAGENTADDRESS
AutoNameOrder 4 TM_USEPRIVATEIP
<=============== End Difference ===============>
<------------------------------------------------>
<--C:/InCharge/IP/smarts/conf/discovery/oid2type_Cisco.conf-->
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 12369 to 12370 >>>>>>>>>>>>>>
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 12370 to 12384 <<<<<<<<<<<<<<
.1.3.6.1.4.1.9.1.916 {
TYPE = Firewall
VENDOR = Cisco
MODEL = ciscoASA5580sc
CERTIFICATION = CERTIFIED
CONT = Cisco-Entity
HEALTH = Cisco-Entity
INSTRUMENTATION:
CPU/Memory = CiscoRouter:DeviceID
Interface-Fault = MIB2
Interface-Performance = MIB2
}
<=============== End Difference ===============>
<------------------------------------------------>
<--C:/InCharge/IP/smarts/conf/discovery/oid2type_Misc.conf -->
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 8816 to 8806 >>>>>>>>>>>>>>
.1.3.6.1.4.1.10734.1.3.8 {
TYPE = Firewall
VENDOR = TippingPoint
MODEL = TippingPointIPS
CERTIFICATION = CERTIFIED
CONT = MIB2-IfStack
INSTRUMENTATION:
Interface-Fault           = MIB2
Interface-Performance     = MIB2
}
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 8806 to 8816 <<<<<<<<<<<<<<
#.1.3.6.1.4.1.10734.1.3.8 {
# TYPE = Firewall
# VENDOR = TippingPoint
# MODEL = TippingPointIPS
# CERTIFICATION = CERTIFIED
# CONT = MIB2-IfStack
#
#INSTRUMENTATION:
# Interface-Fault           = MIB2
# Interface-Performance     = MIB2
#}
<=============== End Difference ===============>
<------------------------------------------------>
<--C:/InCharge/IP/smarts/conf/discovery/tpmgr-param.conf --->
```

```
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 40 to 40 >>>>>>>>>>>>>>
IFTypePatternIFExt.1.3.6.1.4.1.119.1.3.13.4 39|53|1
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 40 to 40 <<<<<<<<<<<<<<
#IFTypePatternIFExt.1.3.6.1.4.1.119.1.3.13.4 39|53|1
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 125 to 125 >>>>>>>>>>>>>>
IFTypePattern-SwitchPort.1.3.6.1.4.1.119.1.14.8 37
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 125 to 125 <<<<<<<<<<<<<<
#IFTypePattern-SwitchPort.1.3.6.1.4.1.119.1.14.8 37
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 554 to 554 >>>>>>>>>>>>>>
#GetBulkPattern-.1.3.6.1.4.1.1872.1.15 TRUE
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 554 to 554 <<<<<<<<<<<<<<
GetBulkPattern-.1.3.6.1.4.1.1872.1.15 TRUE
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 565 to 565 >>>>>>>>>>>>>>
#GetBulkTimeoutOverrideRatio-.1.3.6.1.4.1.1872.1.15 2.5
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 565 to 565 <<<<<<<<<<<<<<
GetBulkTimeoutOverrideRatio-.1.3.6.1.4.1.1872.1.15 2.5
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 576 to 576 >>>>>>>>>>>>>>
#GetBulkRetriesOverrideRatio-.1.3.6.1.4.1.1872.1.15 1.5
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 576 to 576 <<<<<<<<<<<<<<
GetBulkRetriesOverrideRatio-.1.3.6.1.4.1.1872.1.15 1.5
<=============== End Difference ===============>
<============== Start Difference ==============>
>>>>>>>>>>>>>> Base File Contents >>>>>>>>>>>>>>
>>>>>>>>>>>>>> From line: 582 to 582 >>>>>>>>>>>>>>
maxOIDsPerPacketForASNMP 19
<<<<<<<<<<<<<< Local File Contents <<<<<<<<<<<<<<
<<<<<<<<<<<<<< From line: 582 to 582 <<<<<<<<<<<<<<
maxOIDsPerPacketForASNMP 15
<=============== End Difference ===============>
<------------------------------------------------>
```