

VMware Smart Assurance Version 10.0.0.2 Cumulative Patch Readme

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	Revision history	5
	Scope	5
2	Patch description	6
	Installation directory	6
	Installation overview	6
	Patch Upgrade Procedure for Version 10.0.0.1	7
	Install a new patch over an older patch	8
	Upgrade DCF Collectors After Applying Patch	8
	Patch installation files	9
3	Enhancements and changes	10
	General enhancements and changes	10
	Enhancements and changes in IP	10
	Enhancements and changes in SAM	10
	Enhancements and changes in MPLS	10
	Enhancements and changes in NPM	10
	Enhancements and changes in ESM	10
	New configuration flags	11
4	Known problems and limitations	14
	General Known problems and limitations	14
	Known problems and limitations in IP	14
	Known problems and limitations in SAM	14
	Known problems and limitations in MPLS	14
	Known problems and limitations in NPM	14
	Known problems and limitations in ESM	14
5	Number of fixed defects and certified devices	16
6	Fixed Defects	17
	Fixed Foundation defects	17
	Fixed IP specific defects	17
	Fixed SAM specific defects	17
	Fixed MPLS specific defects	18
	Fixed NPM specific defects	18
	Fixed ESM specific defects	18

7	Certified devices	19
	Simple certifications	19
	Complex certifications	23
	Certification impact	25
8	Environment and system requirements	32
	Supported operating systems and version number details	32
9	Installation	33
	Apply patch using CLI mode	33
	Run CLI mode	33
	User selections and navigation in CLI mode	33
	Apply patch using Unattended (Silent) mode	35
	Apply DCF Patch using CLI Mode	35
	Apply DCF Patch using Unattended (Silent) Mode	36
10	Log files	38
	Install log	38
	Merged files Log	38
11	Reconcile user-modifiable files	39
	Review the results of the reconciliation process	39
	Resolve issues in conflict files	39
12	Uninstallation	41
	Before uninstallation	41
	Roll back to a previous patch	41
	Uninstall Patch Using the Uninstaller Program	41
	Uninstall Patch Using Unattended (Silent) Mode	42
	Uninstall DCF Patch using CLI Mode	42
	Uninstall DCF Patch Using Unattended (Silent) Mode	43
13	Troubleshooting and getting help	44

Revision history

This section presents the revision history of this document.

Revision history

Revision	Release Date	Description
01	July 2019	Release of VMware Smart Assurance Version 10.0.0 Patch 1 Readme.
02	Aug 2019	Release of VMware Smart Assurance Version 10.0.0 Patch 2 Readme.

Scope

This section presents the product scope for this patch release.

Products released in this patch

Patch Release	Release date	Product (s) released in this patch
VMware Smart Assurance Version 10.0.0 Patch 1	July 2019	ESM and DCF
VMware Smart Assurance Version 10.0.0 Patch 2	Aug 2019	IP

Patch description

A patch provides one or more fixes to an VMware Smart Assurance product. A patch can only be applied to the specific major or minor release and Service Pack of the particular product for which it is intended, this is called the product's baseline.

Note All VMware Smart Assurance 10.0.0.x products will not be released for every patch release. A patch may apply only to a subset of products, for example, the next patch release may be only for SAM and IP. Also, if the latest patch version for all products is 1 and Patch 2 is only for SAM and IP, the next patch number irrespective of which product is released will be Patch 3. Details for this product are kept in a separate Patch Readme.

This chapter includes the following topics:

- [Installation directory](#)
- [Installation overview](#)
- [Patch Upgrade Procedure for Version 10.0.0.1](#)
- [Install a new patch over an older patch](#)
- [Upgrade DCF Collectors After Applying Patch](#)
- [Patch installation files](#)

Installation directory

In this document, the term <BASEDIR> represents the location where Smarts software is installed.

For UNIX, the default location is: /opt/InCharge/<productsuite>.

The <productsuite> represents the Smarts product suite to which the product belongs.

Optionally, you can specify the root of <BASEDIR> to be something other than /opt/InCharge (on UNIX) but you cannot change the name of the <productsuite> that is part of the <BASEDIR>.

The *System Administration Guide* provides additional information about the directory structure of Smarts software.

Installation overview

A patch installs files to the <BASEDIR>/smarts/local directory of the product. The Installation software performs the following actions:

Backs up all files that are being replaced or merged.

Merges changes from your current, user-modifiable configuration files into the new versions of the files from the patch.

Displays complete summary at the end of patch installation.

Displays the location of a log file that lists the results of merging the files.

Note If the original product was installed on one computer and then was copied to another computer, the patch cannot be applied to the copied installation. You must apply the patch to the computer with the original installation, and then the results can be copied to another computer.

Patch Upgrade Procedure for Version 10.0.0.1

This section describes the patch upgrade steps for version 10.0.0.1.

Prerequisites

If VCO is already existing in the topology, execute the following command to find all the VeloCloud instances:

```
<BASEDIR>/smarts/bin/dmctl -s <ESM-DOMAIN-NAME> invoke  
ICF_PersistentDataSet::VCOTopologyCollectorInstanceIds get
```

Procedure

- 1 Stop ESM server.
Refer [VMware Smart Assurance Server Manager User and Configuration Guide](#).
- 2 Install DCF patch.
Refer [Apply DCF Patch using CLI Mode](#) section.
- 3 If VeloCloud collector instances are already existing in DCF, update the instances and recreate Kafka topics.
To update the instances and recreate Kafka topics, refer [Upgrade DCF Collectors After Applying Patch](#) section.
- 4 Install ESM patch.
Refer [Apply patch using CLI mode](#) section.
- 5 Add new params related to VeloCloud in <BASEDIR>/smarts/local/conf/esm-param.conf file.
Refer [New configuration flags](#) section.
- 6 Start ESM server.
Refer [VMware Smart Assurance Server Manager User and Configuration Guide](#).

Install a new patch over an older patch

Patches are cumulative; each successive patch includes all of the fixes from any previous patches. As a result, a newer patch can be installed on top of an older patch. The patch number, which increments itself for each successive patch, indicates the version. A patch with higher version number can be installed over a patch with a lower version number.

The Installation software checks the version of the installed product and the version to be installed at the beginning of its process. It will not allow an older version to be installed on top of a newer version.

Upgrade DCF Collectors After Applying Patch

To upgrade DCF collectors after applying a patch:

Procedure

1 Upgrade VeloCloud discovery and monitoring collector instances in DCF.

- a To update the VeloCloud collector instance and to answer the prompts by giving default values while performing update, run the command:

```
<DCF_INSTALL_DIRECTORY>/bin/manage-modules.sh update velocloud-sdwan-collect
<instance-id>
```

Refer *Prerequisite* section of [Patch Upgrade Procedure for Version 10.0.0.1](#) to find all the VeloCloud instance ids.

- b After update stop the VeloCloud collector instance using the command:

```
<DCF_INSTALL_DIRECTORY>/bin/manage-modules.sh service stop collector-manager
<instance-id>
```

To find all the VeloCloud instance ids refer the *Prerequisite* section of [Patch Upgrade Procedure for Version 10.0.0.1](#).

2 Delete and recreate the VeloCloud discovery and monitoring topics following these steps:

- a Ensure <KAFKA_HOME>/config/server.properties file has "delete.topic.enable=true"

- b Execute the following commands:

```
export KAFKA_OPTS="-Djava.security.auth.login.config=<KAFKA_HOME>/config/
zookeeper_jaas.conf"
```

```
<KAFKA_HOME>/bin/kafka-topics.sh --zookeeper
<KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181
<KAFKA_CLUSTER_HOST3_IPADDRESS>:2181 --delete --topic <discovery topic name>
```

- c Wait for one minute.

- d Run the command:

```
<KAFKA_HOME>/bin/kafka-topics.sh --zookeeper
<KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181
<KAFKA_CLUSTER_HOST3_IPADDRESS>:2181 --delete --topic <monitoring topic name>
```

e Wait for one minute.

f Execute the following command to ensure the successful deletion of the topics mentioned in steps b and d. The command does not list any topic if the deletion is successful.

```
<KAFKA_HOME>/bin/kafka-topics.sh --zookeeper
<KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181
<KAFKA_CLUSTER_HOST3_IPADDRESS>:2181 --list
```

g Execute the command:

```
export KAFKA_OPTS="-Djava.security.auth.login.config=<KAFKA_HOME>/config/
kafka_server_jaas.conf"
```

h Run the command:

```
<KAFKA_HOME>/bin/kafka-topics.sh --create --zookeeper
<KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181
<KAFKA_CLUSTER_HOST3_IPADDRESS>:2181 --replication-factor 3 --partitions 1 --
topic <Discovery Topic Name>
```

- The value for --replication-factor must be equal to number of nodes in the cluster.
- At present, only 1 partition is supported per topic.

i Wait for 30 seconds.

j Execute the command:

```
<KAFKA_HOME>/bin/kafka-topics.sh --create --zookeeper
<KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181
<KAFKA_CLUSTER_HOST3_IPADDRESS>:2181 --replication-factor 3 --partitions 1 --
<topic <Monitoring Topic Name>
```

- The value for --replication-factor should be equal to number of nodes in the cluster.
- At present, only 1 partition is supported per topic.

k Wait for 30 seconds.

Patch installation files

Install the patch on each host where the Smarts product is running.

Binary details for this release are:

- IP:
 - setup-IP-linux-10_0_0_2-20190807-64BIT.bin

Enhancements and changes

This chapter includes the following topics:

- [General enhancements and changes](#)
- [Enhancements and changes in IP](#)
- [Enhancements and changes in SAM](#)
- [Enhancements and changes in MPLS](#)
- [Enhancements and changes in NPM](#)
- [Enhancements and changes in ESM](#)
- [New configuration flags](#)

General enhancements and changes

Enhancements and changes in IP

This patch release does not contain any enhancement and changes.

Enhancements and changes in SAM

This patch release does not contain any enhancement and changes.

Enhancements and changes in MPLS

This patch release does not contain any enhancement and changes.

Enhancements and changes in NPM

This patch release does not contain any enhancement and changes.

Enhancements and changes in ESM

This Patch release introduces:

- Support for VeloCloud MSP user type.
- Enterprise filtering for operator and MSP users.

New configuration flags

This chapters helps you to configure new flags.

New parameters has been introduced with this patch release in ESM

Table *Parameters and Descriptions* illustrates about the new parameters and their descriptions in ESM file.

Table 3-1. Parameters and Descriptions

Parameters	Descriptions
VCO_USERTYPE-<Orchestrator_host_IP_address> operator MSP	<p>Defines the VeloCloud usertype.</p> <p>Note Usertype is a mandatory parameter and it can either be "operator" or "MSP".</p>
VCO_ENTERPRISE_FILTER- <Orchestrator_host_IP_address> <REGEX FILTER>	<p>Defines the RegEx pattern for list of enterprises in the VeloCloud that ESM needs to discover and monitor.</p> <p>The regex pattern must confirm to patterns defined in java.util.regex documentation. This is an optional parameter.</p> <p>Default filter is .* (i.e discover all enterprises that belong to a specific user)</p> <p>For example, if ESM needs to discover two Tenants, "A" and "B", then the parameter can be defined as "A B".</p> <p>VCO_ENTERPRISE_FILTER- <Orchestrator_host_IP_address> A B</p>

Parameters	Descriptions
VCO_HTTP_RESPONSE_TIMEOUT– <Orchestrator_host_IP_address> <Time in Seconds>	Defines the http timeout for response in seconds for VeloCloud discovery and monitoring collector while fetching Topology using REST API. This is an optional parameter. Default value is 120 seconds.
VCO_DISCOVERY_TIMEOUT– <Orchestrator_host_IP_address> <Time in Seconds>	Defines the discovery collector timeout in seconds for VeloCloud discovery. This is an optional parameter. Default value is 3600 seconds.

Note The following parameters need to be modified in `esm-param.conf` file to discover a Topology having around 3500 Vedges, the parameters need to be modified in `esm-param-conf` file based on customer deployment:

- `MessagePollTimeoutPeriodInSeconds--<kafka_IP_Address> 2400`

When the latency between orchestrator and the DCF collector is higher this flag needs to be set to a higher value. This flag dictate the timeout value for the ESM to wait for messages from kafka. If the timeout expires then the discovery is stopped abruptly.

- `VCO_HTTP_RESPONSE_TIMEOUT--<Orchestrator IP> 220`

This the timeout value for the http request that the DCF collector sends to the orchestrator. While configuring this value the processing time of the orchestrator must also be considered into account as some of the REST API take longer time to return.

- `VCO_DISCOVERY_TIMEOUT--<Orchestrator IP> 18000`

This parameter value need to be increased based on the topology size. This is the maximum time in seconds that the collector is let to run before abruptly stopping the collector. This is a safeguard measure to prevent the collector to be keep running under a false condition.

Configuration Flags in IP Certification

- **EnableMXVirtualRouterDiscovery:** This flag must be enabled for Juniper MX480 virtual router discovery.

```
# EnableMXVirtualRouterDiscovery (Enables or disables the discovery of Juniper MX Series Virtual Router):
#
#           A value of TRUE enables the discovery of Juniper MX Series Virtual Router.
#           A value of FALSE disables the discovery of Juniper MX Series Virtual Router.
#
# Default Value = FALSE
EnableMXVirtualRouterDiscovery FALSE
```

- **MXLogicalCommunityOnly:** This flag must be enabled for virtual router community string.

```
# MXLogicalCommunityOnly - Add SysOID to allow selective logical router default community string format without main router community string.
```

```
# Example: if logical/default@XXXXX ( Here XXXXX is main router community string ) is actual  
string for logical router, then we need to configure only logical string format like logical/  
default  
MXLogicalCommunityOnly.1.3.6.1.4.1.2636.1.1.1.2.25 logical/default
```

Known problems and limitations

This chapter includes the following topics:

- [General Known problems and limitations](#)
- [Known problems and limitations in IP](#)
- [Known problems and limitations in SAM](#)
- [Known problems and limitations in MPLS](#)
- [Known problems and limitations in NPM](#)
- [Known problems and limitations in ESM](#)

General Known problems and limitations

Known problems and limitations in IP

This patch release does not include any known issues.

Known problems and limitations in SAM

This patch release does not include any known issues.

Known problems and limitations in MPLS

This patch release does not include any known issues.

Known problems and limitations in NPM

This patch release does not include any known issues.

Known problems and limitations in ESM

VeloCloud known problems and limitations

Issue Summary: The password for DCC and Kafka cannot be “changeme”.

Description: When the password is "changeme", discovery for the VeloCloud orchestrator fails.

Workaround: Need to change the password for DCC and Kafka from "changeme".

Issue Summary: The name for the Orchestrator host instance in IP domain must be the IP address of the Orchestrator.

Description: Orchestrator host instance in IP domain must not be a DNS resolved name or anything other than the IP address. If it is, then the discovery for the VeloCloud orchestrator fails in the ESM server.

Workaround: If the name resolve to the DNS name then either use USESEEDNAME option to resolve the name or create the Orchestrator host using the below dmctl commands:

```
1 create Host::
2 create SNMPAgent::SNMPAgent-<ip address>
3 create IP::IP-<ip address>
4 insert Host::::HostsServices SNMPAgent::SNMPAgent-<ip address>
5 insert Host::::HostsAccessPoints IP::IP-<ip address>
6 put SNMPAgent::SNMPAgent-<ip address>::AgentAddress <ip address>
7 get SNMPAgent::SNMPAgent-<ip address>::LayeredOver
8 insert SNMPAgent::SNMPAgent-<ip address>::LayeredOver IP::IP-<ip address>
```

Issue Summary: Only one Kafka partition is supported for the Kafka topic that is used for discovery..

Description: Only one Kafka partition is supported for the Kafka topic that is used for discovery.

Workaround: No workaround available.

Number of fixed defects and certified devices

5

This section lists the number of defects fixed and devices certified (new and updated) for this patch.

Number of fixed defects and certified devices:

Product	Number of fixed defects	Number of new certifications	Number of updated certifications	Patch release
DMT	0	0	0	NA
IP	0	44	6	10.0.0.2
SAM	0	0	0	NA
NPM	0	0	0	NA
ESM	0	0	0	NA
MPLS	0	0	0	NA

Fixed Defects

This chapter includes the following topics:

- [Fixed Foundation defects](#)
- [Fixed IP specific defects](#)
- [Fixed SAM specific defects](#)
- [Fixed MPLS specific defects](#)
- [Fixed NPM specific defects](#)
- [Fixed ESM specific defects](#)

Fixed Foundation defects

Fixed Foundation defects applicable for all products

CQ/JIRA or SR Ticket Number	Symptom	Description of Fix	Modified Files (all files in <BASEDIR>/smarts/local/)	Patch Release
NA	NA	NA	NA	NA

Fixed IP specific defects

CQ/JIRA or SR Ticket Number	Symptom	Description of Fix	Modified Files (all files in <BASEDIR>/smarts/local/)	Patch Release
		The Fixed Foundation defects table lists issues fixed in the patch.		
NA	NA	NA	NA	NA

Fixed SAM specific defects

CQ/JIRA or SR Ticket Number	Symptom	Description of Fix	Modified Files (all files in <BASEDIR>/smarts/local/)	Patch Release
		The Fixed Foundation defects table lists issues fixed in the patch.		
NA	NA	NA	NA	NA

Fixed MPLS specific defects

CQ/JIRA or SR Ticket Number	Symptom	Description of Fix	Modified Files (all files in <BASEDIR>/smarts/local/)	Patch Release
		The Fixed Foundation defects table lists issues fixed in the patch.		
NA	NA	NA	NA	NA

Fixed NPM specific defects

CQ/JIRA or SR Ticket Number	Symptom	Description of Fix	Modified Files (all files in <BASEDIR>/smarts/local/)	Patch Release
		The Fixed Foundation defects table lists issues fixed in the patch.		
NA	NA	NA	NA	NA

Fixed ESM specific defects

CQ/JIRA or SR Ticket Number	Symptom	Description of Fix	Modified Files (all files in <BASEDIR>/smarts/local/)	Patch Release
		The Fixed Foundation defects table lists issues fixed in the patch.		
NA	NA	NA	NA	NA

Certified devices

This section describes the devices certified and the certification impact in this patch:

This chapter includes the following topics:

- [Simple certifications](#)
- [Complex certifications](#)
- [Certification impact](#)

Simple certifications

Simple certification involves only in configure file changes and the qualification of new OID in the currently existing driver. This section describes the devices certified in this patch.

Simple devices certified in the patch:

SR /TASC Number	Vendor Name	Description	Patch Release
SASS-13510 /304922	Arista	Certified the following components for the DCS-7280QR-C36-M Switch (System OID : .1.3.6.1.4.1.30065.1.3011.7280.3101.2878.36.972): Memory, Port, Processor, and VLAN.	10.0.0.2
SASS-13484 /304910	Cisco	Certified the following components for the ciscoC1111X8P Router (System OID : .1.3.6.1.4.1.9.1.2668): Card, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor, and VLAN.	10.0.0.2
SASS-13482 /304908	Symmetricom	Certified the following components for the SyncServer S600 Host (System OID : .1.3.6.1.4.1.9070.1.2.5.7.4): Host.	10.0.0.2
SASS-13431 /304905	Juniper	Certified the following components for the QFX1000260C Switch (System OID : .1.3.6.1.4.1.2636.1.1.1.4.82.19): Card, Fan, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor, and VLAN.	10.0.0.2
SASS-13430 /304904	Juniper	Certified the following components for the EX9253 Switch (System OID : .1.3.6.1.4.1.2636.1.1.1.2.156): Card,CardRedundancyGroup, Fan, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor, and VLAN.	10.0.0.2

SASS-13428 /304903	Juniper	Certified the following components for the EX9251 Switch (System OID : .1.3.6.1.4.1.2636.1.1.1.2.151): Card, Fan, Interface, Port, VLAN, Memory, Processor, PowerSupply, and Temperature Sensor.	10.0.0.2
SASS-13553 /304902	Juniper	Certified the following components for the EX4650 Switch (System OID : .1.3.6.1.4.1.2636.1.1.1.4.508.1): Card, Fan, Interface, Memory, Processor, Port, PowerSupply, Temperature Sensor, VLAN, and Virtual Chassis.	10.0.0.2
SASS-13475 /304900	Pan	Certified the following components for the PanM-200 Firewall (System OID : .1.3.6.1.4.1.25461.2.3.40): Interface, Memory, and Processor.	10.0.0.2
SASS-13476 /304899	Cisco	Certified the following components for the ciscoC11114P Router (System OID : .1.3.6.1.4.1.9.1.2505): Card, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor and VLAN.	10.0.0.2
SASS-13343 /304896	F5 Networks	Certified the following components for the BIG-IP i11800 LoadBalancer (System OID : .1.3.6.1.4.1.3375.2.1.3.4.122): AggregatePort, Disk, Fan, FileSystem, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor, and VLAN.	10.0.0.2
SASS-13461 /304895	Cisco	Certified the following components for the ciscoCatWSC2960L8TSL Switch (System OID : .1.3.6.1.4.1.9.1.2360): Fan, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor, and VLAN.	10.0.0.2
SASS-13455 /304893	Cisco	Certified the following components for the ciscoC11174P Router (System OID : .1.3.6.1.4.1.9.1.2520): Card, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor, and VLAN.	10.0.0.2
SASS-13440 /304889	Aruba	Certified the following components for the Aruba JL261A 2930F-24G-PoE+-4SFP Switch (System OID : .1.3.6.1.4.1.11.2.3.7.11.181.24): Fan, Interface, Memory, Port, PowerSupply, Processor, and VLAN.	10.0.0.2
SASS-13319 /304888	Aruba	Certified the following components for the Aruba JL076A 3810M-40G-8SR-PoE+-1-slot Switch (System OID : .1.3.6.1.4.1.11.2.3.7.11.174.6): AggregatePort, Fan, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor, and VLAN.	10.0.0.2

SASS-13352 /304886	Arista	Certified the following components for the DCS-7050SX3-48YC8 Switch (System OID : .1.3.6.1.4.1.30065.1.3011.7050.3741.3.48.1654.8): Interface, Memory, Port, Processor, and VLAN.	10.0.0.2
SASS-13353 /304881	Arista	Certified the following components for the DCS-7050SX2-72Q Switch (System OID : .1.3.6.1.4.1.30065.1.3011.7050.3741.2.72.2512): Interface, Memory, Port, Processor, and VLAN.	10.0.0.2
SASS-13354 /304880	Arista	Certified the following components for the DCS-7280CR2A-60 Switch (System OID : .1.3.6.1.4.1.30065.1.3011.7280.2727.2.364.8.60): Interface, Memory, Port, Processor, and VLAN.	10.0.0.2
SASS-13322 /304876	Arista	Certified the following components for the DCS-7060CX2-32S Switch (System OID : .1.3.6.1.4.1.30065.1.3011.7060.2733.2.32.3282): Interface, Memory, Port, Processor, and VLAN.	10.0.0.2
SASS-13327 /304875	F5 Networks	Certified the following components for the BIG-IP-I7800D LoadBalancer (System OID : .1.3.6.1.4.1.3375.2.1.3.4.130): Disk, Fan, Filesystem, Interface, Memory, Port, Power supply, Processor, and Temperature Sensor.	10.0.0.2
SASS-13320 /304874	Arista	Certified the following components for the DCS-7050CX3-32S Switch (System OID : .1.3.6.1.4.1.30065.1.3011.7050.2733.3.32.3282): Interface, Memory, Port, Processor, and VLAN.	10.0.0.2
SASS-13321 /304872	Opengear	Certified the following components for the ogACM70045 TerminalServer (System OID : .1.3.6.1.4.1.25049.1.91): Interface and Memory.	10.0.0.2
SASS-13551 /304866	HP	Certified the following components for the HP-ProCurve-J9310A Switch (System OID : .1.3.6.1.4.1.11.2.3.7.11.114): Fan, Interface, Memory, Processor, Port, PowerSupply, Temperature Sensor, and VLAN.	10.0.0.2
SASS-13549 /304864	HP	Certified the following components for the HP-ProCurve-J9311A Switch (System OID : .1.3.6.1.4.1.11.2.3.7.11.115): Fan, Interface, Memory, Processor, Port, PowerSupply, Temperature Sensor, and VLAN.	10.0.0.2
SASS-13285 /304863	Datadomain	Certified the following components for the emcDD690 Host (System OID : .1.3.6.1.4.1.19746.3.1.0): FileSystem, Interface,Memory, MemoryGroup, Processor, and ProcessorGroup.	10.0.0.2

SASS-13292 /304848	Cisco	Certified the following components for the ciscoC385012XS Switch (System OID : .1.3.6.1.4.1.9.1.2162): Fan, Interface, Memory, PowerSupply, Processor, TemperatureSensor, and VLAN.	10.0.0.2
SASS-13291 /304847	Cisco	Certified the following components for the catwsC3560CX8ptS Switch (System OID : 1.3.6.1.4.1.9.1.2130): Card, Fan, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor, and VLAN.	10.0.0.2
SASS-13526 /304834	Cisco	Certified the following components for the SG300-28 Switch (System OID : 1.3.6.1.4.1.9.6.1.83.28.1): Interface, Port, Processor, and VLAN.	10.0.0.2
SASS-13381 /304830	Apcon	Certified the following components for the ACI-4040 Switch (System OID : 1.3.6.1.4.1.10830.3.2): Interfaces, Memory, Processor, and FileSystem.	10.0.0.2
SASS-13426 /304828	Juniper	Certified the following components for the EX3400-48P Switch (System OID : 1.3.6.1.4.1.2636.1.1.1.4.131.4): Card, Card Redundancy Group, VCCRE Card Redundancy Group, Fan, Interface, Port, VLAN, Memory, Processor, PowerSupply, and Temperature Sensor.	10.0.0.2
SASS-13275 /304823	Checkpoint	Certified the following components for the CheckPoint5400 Firewall (System OID : 1.3.6.1.4.1.2620.1.6.123.1.67): Fan, FileSystem, Interface, Memory, Processor, TemperatureSensor, and VoltageSensor.	10.0.0.2
SASS-13274 /304822	Pulsesecure	Certified the following components for the ivePSA7000f Firewall(System OID : 1.3.6.1.4.1.12532.256.4.1): Disk, Interface, Memory, and Processor.	10.0.0.2
SASS-13233 /304817	Cisco	Certified the following components for the Cisco VCS Host (System OID : 1.3.6.1.4.1.5596.130.6.4.1): FileSystem, Interface, Memory, MemoryGroup, Port, Processor, ProcessorGroup, and TemperatureSenosr.	10.0.0.2
SASS-13479 /304784	Arista	Certified the following components for the DCS-7280CR2K-30-F Switch (System OID : 1.3.6.1.4.1.30065.1.3011.7280.2727.2.202.30): Interface, Port, Memory, Processor, and VLAN.	10.0.0.2

SASS-13491 /304781	Cisco	Certified the following components for the ciscoUCSC460M4Rackserver Host (System OID : 1.3.6.1.4.1.9.1.1817): Card, Disk, Fan, Interface, Memory, MemoryGroup, PowerSupply, TemperatureSensor, and VoltageSensor.	10.0.0.2
SASS-13535 /304780	Cisco	Certified the following components for the ciscoUcsC260 Host (System OID : 1.3.6.1.4.1.9.1.1516): Card, Disk, Fan, Interface, Memory, MemoryGroup, PowerSupply, TemperatureSensor, and VoltageSensor.	10.0.0.2
SASS-13152 /304778	Dell	Certified the following components for the PowerEdge R330 Host (System OID : 1.3.6.1.4.1.21343.3.2.24): Fan, Interface, Memory, MemoryGroup, Processor, ProcessorGroup, FileSystem, PowerSupply, TemperatureSensor, and VoltageSensor.	10.0.0.2
SASS-13269 /304769	Cisco	Certified the following components for the cevChassisN77c7702 Switch (System OID : 1.3.6.1.4.1.9.12.3.1.3.1648): Card, Fan, Memory, Port, PowerSupply, Processor, TemperatureSensor, and VLAN.	10.0.0.2
SASS-13434 /304833	Draytek	Certified the following components for the Vigor 2860 Router (System OID : 1.3.6.1.4.1.7367): Interface.	10.0.0.2
SASS-13355 /304878	Audiocodes	Certified the following components for the MEDIANT800C Mediagateway(System OID : 1.3.6.1.4.1.5003.8.1.1.72): Card, Interface, Memory, and Processor	10.0.0.2

Complex certifications

Complex certifications involve recertification, new device certifications, and involve new driver creations or multiple file changes. This section describes the devices certified in this patch.

Description of complex devices certified in the patch

SR /TASC Number	Vendor Name	Description	Patch Release
SASS-13293 /304851	Cisco	Certified the following components for the catwsC2960CX8tcL Switch (System OID : 1.3.6.1.4.1.9.1.2137): Card, Fan, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor, and VLAN.	10.0.0.2

SASS-13317 /304850	Brocade	Certified the following components for the DS-5300B FiberChannelSwitch (System OID : .1.3.6.1.4.1.1588.2.1.1.64): Card, Fan, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor, and VoltageSensor.	10.0.0.2
SASS-13315 /304849	Brocade	Certified the following components for the SilkwormSeries FiberChannelSwitch (System OID : .1.3.6.1.4.1.1588.2.1.1.1): Card, Fan, Port, PowerSupply , and TemperatureSensor.	10.0.0.2
SASS-13301 /304854	Cisco	Certified the following components for the ciscoWsC2960P48TcS Switch (System OID : .1.3.6.1.4.1.9.1.1756): Card, Fan, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor, and VLAN.	10.0.0.2
SASS-13289 /304846	Cisco	Certified the following components for the ciscoAIRAP1702 Switch (System OID : .1.3.6.1.4.1.9.1.2129): Interface, Memory, Port, and Processor.	10.0.0.2
SASS-13288 /304845	Cisco	Certified the following components for the ciscoAIRAP2702 Switch (System OID : .1.3.6.1.4.1.9.1.1938): Interface, Memory, Port, and Processor.	10.0.0.2
SASS-13270 /304826	Cisco	Certified the following components for the Cisco9500FixedSwitchStack Switch (System OID : .1.3.6.1.4.1.9.1.2593): Card,CardRedundancyGroup, Fan, Interface, Memory, Port, PowerSupply, Processor, TemperatureSensor, VoltageSensor, and VLAN.	10.0.0.2
SASS-13569 /304774	Libert	Certified the following components for the liebertGlobalProducts Host (System OID : .1.3.6.1.4.1.476.1.42): Interface, TemperatureSensor, and VoltageSensor.	10.0.0.2
SASS-13286 /304861	Juniper	Certified the following components for the SRX550 Router (System OID : .1.3.6.1.4.1.2636.1.1.1.2.86): Card, Disk, Fan, Interface, Memory, Processor, Powersupply, and Temperaturesensor.	10.0.0.2
SASS-13294 /304890	Arista	Certified the following components for the DCS-7150S-24 Switch (System OID : .1.3.6.1.4.1.30065.1.3011.7150.3282.24): Port, Interface, Memory, and Processor.	10.0.0.2
SASS-13178 /304779	Juniper	Certified the following components for the MX480 Router (System OID : .1.3.6.1.4.1.2636.1.1.1.2.25): Card, CardRedundancyGroup, Fan, Interface, Memory, Processor, Powersupply, Router, and Temperaturesensor.	10.0.0.2

Certification impact

This section lists the impacted drivers and SysOIDs as a result of certification changes.

Certification impact

SR/TASC Number	Impacted drivers	Impacted SysOIDs	Patch Release
304826	HEALTH = Cisco-Router-CRS-EntSensor	.1.3.6.1.4.1.9.1.348 .1.3.6.1.4.1.9.1.925 .1.3.6.1.4.1.9.1.822 .1.3.6.1.4.1.9.1.1116 .1.3.6.1.4.1.9.1.610 .1.3.6.1.4.1.9.1.2068 .1.3.6.1.4.1.9.1.2093 .1.3.6.1.4.1.9.1.1861 .1.3.6.1.4.1.9.1.2157 .1.3.6.1.4.1.9.1.1935 .1.3.6.1.4.1.9.1.2101 .1.3.6.1.4.1.9.1.2143 .1.3.6.1.4.1.9.1.2155 .1.3.6.1.4.1.9.1.2102 .1.3.6.1.4.1.9.1.2593 .1.3.6.1.4.1.9.1.2520 .1.3.6.1.4.1.9.1.2505 .1.3.6.1.4.1.9.1.2668	10.0.0.2

304845	HEALTH = Cisco-Router	.1.3.6.1.4.1.9.1.497 .1.3.6.1.4.1.9.1.1040 .1.3.6.1.4.1.9.1.847 .1.3.6.1.4.1.9.1.1745 .1.3.6.1.4.1.9.1.1747 .1.3.6.1.4.1.9.1.1824 .1.3.6.1.4.1.9.1.2382 .1.3.6.1.4.1.9.1.1770 .1.3.6.1.4.1.9.1.1875 .1.3.6.1.4.1.9.1.1828 .1.3.6.1.4.1.9.1.1420 .1.3.6.1.4.1.9.1.1856 .1.3.6.1.4.1.9.1.848 .1.3.6.1.4.1.9.1.2309 .1.3.6.1.4.1.9.1.1853 .1.3.6.1.4.1.9.1.842 .1.3.6.1.4.1.9.1.2050 .1.3.6.1.4.1.9.1.2060 .1.3.6.1.4.1.9.1.1857 .1.3.6.1.4.1.9.1.1767 .1.3.6.1.4.1.9.1.2494 .1.3.6.1.4.1.9.1.1882 .1.3.6.1.4.1.9.1.2059 .1.3.6.1.4.1.9.1.1557 .1.3.6.1.4.1.9.1.1938 .1.3.6.1.4.1.9.1.2129	10.0.0.2
--------	-----------------------	--	----------

304849	HEALTH = Brocade-Switch Environment = BrocadeEnvMon:DeviceID	<p>.1.3.6.1.4.1.1588.2.1.1.1 .1.3.6.1.4.1.1588.2.1.1.18 .1.3.6.1.4.1.1588.2.1.1.55 .1.3.6.1.4.1.1588.2.1.1.55 .1.3.6.1.4.1.1588.2.1.1.10 .1.3.6.1.4.1.1588.2.1.1.32 .1.3.6.1.4.1.1588.2.1.1.58 .1.3.6.1.4.1.1588.2.1.1.42 .1.3.6.1.4.1.1588.2.1.1.43 .1.3.6.1.4.1.1588.2.1.1.72 .1.3.6.1.4.1.1588.2.1.3 .1.3.6.1.4.1.1588.2.1.1.71 .1.3.6.1.4.1.1588.2.1.1.1.62 .1.3.6.1.4.1.1588.2.1.1.34 .1.3.6.1.4.1.1588.2.1.1.26 .1.3.6.1.4.1.1588.2.1.1.44 .1.3.6.1.4.1.1588.2.1.1.118 .1.3.6.1.4.1.1588.2.1.1.64 .1.3.6.1.4.1.1588.2.1.1.46 .1.3.6.1.4.1.1588.2.1.1.109 .1.3.6.1.4.1.1588.2.1.1.83 .1.3.6.1.4.1.1588.2.1.1.76 .1.3.6.1.4.1.1588.2.1.1.67 .1.3.6.1.4.1.1588.2.1.1.1.77 .1.3.6.1.4.1.1588.2.1.1.121 .1.3.6.1.4.1.1588.2.1.1.120 .1.3.6.1.4.1.1588.2.1.1.62 .1.3.6.1.4.1.1588.2.1.1.92 .1.3.6.1.4.1.1588.2.1.1.66 .1.3.6.1.4.1.1588.3.3.1.1001 .1.3.6.1.4.1.1588.3.3.1.1000 .1.3.6.1.4.1.1588.3.3.1.131 .1.3.6.1.4.1.1588.2.1.1.77 .1.3.6.1.4.1.1588.2.1.1.165 .1.3.6.1.4.1.1588.2.1.1.166 .1.3.6.1.4.1.1588.2.1.1.133 .1.3.6.1.4.1.1588.3.3.1.164 .1.3.6.1.4.1.1588.2.1.1.129 .1.3.6.1.4.1.1588.2.1.1.148 .1.3.6.1.4.1.1588.3.3.1.151 .1.3.6.1.4.1.1588.2.1.1.162</p>	10.0.0.2
--------	---	--	----------

304851	HEALTH = Cisco-Stack	.1.3.6.1.4.1.9.1.1757 .1.3.6.1.4.1.9.1.1805 .1.3.6.1.4.1.9.1.1699 .1.3.6.1.4.1.9.1.1765 .1.3.6.1.4.1.9.1.2133 .1.3.6.1.4.1.9.1.1703 .1.3.6.1.4.1.9.1.2131 .1.3.6.1.4.1.9.1.2135 .1.3.6.1.4.1.9.1.1750 .1.3.6.1.4.1.9.1.1754 .1.3.6.1.4.1.9.1.1753 .1.3.6.1.4.1.9.1.2136 .1.3.6.1.4.1.9.1.2137 .1.3.6.1.4.1.9.1.2363 .1.3.6.1.4.1.9.1.2361 .1.3.6.1.4.1.9.1.2369 .1.3.6.1.4.1.9.1.2233 .1.3.6.1.4.1.9.1.2365 .1.3.6.1.4.1.9.1.1756 .1.3.6.1.4.1.9.1.2360	10.0.0.2
304774	HEALTH = Liebert Environment = LiebertEnvMon:DeviceID	.1.3.6.1.4.1.476.1.42	10.0.0.2

304890	CONT = Arista-Switch	<p>.1.3.6.1.4.1.30065.1.3011.7508</p> <p>.1.3.6.1.4.1.30065.1.3011.7148.374 1</p> <p>.1.3.6.1.4.1.30065.1.3011.7124.328 2</p> <p>.1.3.6.1.4.1.30065.1.3011.7124.374 1</p> <p>.1.3.6.1.4.1.30065.1.3011.7504</p> <p>.1.3.6.1.4.1.30065.1.3011.7050.328 2.64</p> <p>.1.3.6.1.4.1.30065.1.3011.7050.328 2.52</p> <p>.1.3.6.1.4.1.30065.1.3011.7050.427. 64</p> <p>.1.3.6.1.4.1.30065.1.3011.7150.328 2.24</p> <p>.1.3.6.1.4.1.30065.1.3011.7150.328 2.64.2745</p> <p>.1.3.6.1.4.1.30065.1.3011.7150.328 2.52.2745</p> <p>.1.3.6.1.4.1.30065.1.3011.7050.251 2.16</p> <p>.1.3.6.1.4.1.30065.1.3011.7010.427. 48</p> <p>.1.3.6.1.4.1.30065.1.3011.7280.371 4.64</p> <p>.1.3.6.1.4.1.30065.1.3011.7050.374 1.128</p> <p>.1.3.6.1.4.1.30065.1.3011.7250.309 5.64</p> <p>.1.3.6.1.4.1.30065.1.3011.7260.309 5.64</p> <p>.1.3.6.1.4.1.30065.1.3011.7048.427. 3648</p> <p>.1.3.6.1.4.1.30065.1.3011.7050.195 8.64</p> <p>.1.3.6.1.4.1.30065.1.3011.7050.374 1.64</p> <p>.1.3.6.1.4.1.30065.1.3011.7050.309 5.32</p> <p>.1.3.6.1.4.1.30065.1.3011.7280.310 1.2878.36</p> <p>.1.3.6.1.4.1.30065.1.3011.7150.328 2.24.2745.761</p> <p>.1.3.6.1.4.1.30065.1.3011.7280.373 5.2.3648.48.1654.6</p> <p>.1.3.6.1.4.1.30065.1.3011.7504.135 9</p> <p>.1.3.6.1.4.1.30065.1.3011.7280.373 5.48.2878.6</p>	10.0.0.2
--------	----------------------	--	----------

.1.3.6.1.4.1.30065.1.3011.7050.374
1.72.2512
.1.3.6.1.4.1.30065.1.3011.7050.195
8.72.2512
.1.3.6.1.4.1.30065.1.3011.7160.32.2
726
.1.3.6.1.4.1.30065.1.3011.7124.374
1.761
.1.3.6.1.4.1.30065.1.3011.7512.135
9
.1.3.6.1.4.1.30065.1.3011.7280.312.
48.2878.6
.1.3.6.1.4.1.30065.1.3011.7280.134
7.48.2878.6
.1.3.6.1.4.1.30065.1.3011.7160.48.1
981.6
.1.3.6.1.4.1.30065.1.3011.7160.48.1
654.6
.1.3.6.1.4.1.30065.1.3011.7050.309
5.32.3282
.1.3.6.1.4.1.30065.1.3011.7280.265
5.2878.36.3282.972
.1.3.6.1.4.1.30065.1.3011.7280.272
7.48
.1.3.6.1.4.1.30065.1.3011.7280.397
7.48.2878.6
.1.3.6.1.4.1.30065.1.3011.7050.374
1.3.48.1654.12
.1.3.6.1.4.1.30065.1.3011.7516.135
9
.1.3.6.1.4.1.30065.1.3011.7280.272
7.2.202.30
.1.3.6.1.4.1.30065.1.3011.7280.310
1.2878.36.972
.1.3.6.1.4.1.30065.1.3011.7050.374
1.3.48.1654.8
.1.3.6.1.4.1.30065.1.3011.7050.374
1.2.72.2512
.1.3.6.1.4.1.30065.1.3011.7280.272
7.2.3648.60
.1.3.6.1.4.1.30065.1.3011.7060.273
3.2.32.3282
.1.3.6.1.4.1.30065.1.3011.7050.273
3.3.32.3282

304861	HOSTRESRCS = MIB2-Disk-FS	.1.3.6.1.4.1.9.1.652 .1.3.6.1.4.1.2636.1.1.1.2.26 .1.3.6.1.4.1.2636.1.1.1.2.28 .1.3.6.1.4.1.2636.1.1.1.2.36 .1.3.6.1.4.1.2636.1.1.1.2.35 .1.3.6.1.4.1.2636.1.1.1.2.34 .1.3.6.1.4.1.2636.1.1.1.2.40 .1.3.6.1.4.1.2636.1.1.1.2.39 .1.3.6.1.4.1.2636.1.1.1.2.41 .1.3.6.1.4.1.2636.1.1.1.2.49 .1.3.6.1.4.1.2636.1.1.1.2.64 .1.3.6.1.4.1.2636.1.1.1.2.58 .1.3.6.1.4.1.2636.1.1.1.2.86 .1.3.6.1.4.1.2636.1.1.1.2.136 .1.3.6.1.4.1.2636.1.1.1.2.129 .1.3.6.1.4.1.2636.1.1.1.2.134 .1.3.6.1.4.1.2636.1.1.1.2.133 .1.3.6.1.4.1.2636.1.1.1.2.143	10.0.0.2
304779	VROUTER = MX-Series	.1.3.6.1.4.1.2636.1.1.1.2.25	10.0.0.2

Environment and system requirements



This section lists the supported operating systems and describes how to verify the version number.

This chapter includes the following topics:

- [Supported operating systems and version number details](#)

Supported operating systems and version number details

Supported operating systems and version number details

Product	Supported operating systems	Version number details
IP	Red Hat Enterprise Linux 7.1, 7.2, and 7.3–64 bit, CentOS 6.7, 6.8, and 6.9–64 bit, CentOS 7.1, 7.2, and 7.3–64 bit VMware® ESX Version 5.x,6.x	From <BASEDIR>/smarts/bin/, type the following command: ./sm_server --version (Linux) The following output is displayed: sm_server: linux_rhAS50-x86-64/301032700 IP_NETWORK_SUITE: V10.0.0.2(179090), 07-Aug-2019 15:27:22 Copyright 2019, VMware Inc - Build 119 Foundation V10.0.0.1(177047), 14-May-2019 12:35:58 Copyright 2019, VMware Inc - Build 1

Installation

This chapter includes the following topics:

- [Apply patch using CLI mode](#)
- [Apply patch using Unattended \(Silent\) mode](#)
- [Apply DCF Patch using CLI Mode](#)
- [Apply DCF Patch using Unattended \(Silent\) Mode](#)

Apply patch using CLI mode

CLI mode provides a text-based method for invoking the Installation software. This mode is intended for UNIX platforms with non-graphic (text-only) consoles. The CLI mode installation follows the same process as the wizard mode but displays text on the terminal screen and requires user responses on the keyboard.

Run CLI mode

- 1 Change directory to the directory where you typically store patches, for example, `./opt`.
- 2 Type the setup command listed in below table and then press **Enter**. Replace “xx” with the relevant product name, for example, ESM. For exact name, check the [Patch installation files](#) section.

Setup command syntax for CLI mode

Operating system	CLI setup command syntax
Linux	<code>./setup-XX-linux-10_0_0_2-20190807-64BIT.bin</code>

A welcome message with information about the installation appears.

Prerequisites

Stop all VMware Smart Assurance services and processes that use programs or libraries from the product being upgraded or installed before performing the installation.

User selections and navigation in CLI mode

During the patch installation process, at the end of each screen of text, you are prompted with a set of options. For example:

```
type 'back' - to go to the previous step
type 'quit' - to cancel anytime
```

- Select a choice by typing the text and pressing **Enter**.
- Accept the default choice, by pressing **Enter**.

Other screens have different choices. For example when the license agreement is displayed, the following prompt appears:

```
Press any key to continue to read license agreement or press '0' to advance to end.
```

At the end of the license agreement, the installation process displays the first of several menus.

```
Choose from the following (Y/N) options:
Y - to accept the terms of the license agreement.
N - not to accept the terms of the license agreement.
```

Type the desired selection and press **Enter**. In the case of the license agreement, you must accept the agreement by typing **Y** and pressing **Enter**.

The screen is displayed with an **Get User Input**. Choose the base location by entering the correct number.

For example, type **1** to choose the default location for installation and press **Enter**.

```
Get User Input
-----
1) /opt/InCharge 10.0.0.*
```

For example, if the product name is ESM and default install folder is /opt/InCharge, the installer displays :

```
VMware Smart Assurance Server Manager Suite will be installed in the following
location:

Product Name:
  ESM

Install Folder:
  /opt/InCharge
```

Press **Enter** to continue the installation.

Press **Enter** to exit the installer

When the patch installation is complete, reconcile the configuration files as described in [Chapter 11 Reconcile user-modifiable files](#).

Apply patch using Unattended (Silent) mode

Unattended mode installs the patch without user input or a response file. When invoking the install program, specify the location of the product suite to be patched.

In order to invoke an unattended installation of the patch, type the appropriate setup command from below table and then press **Enter**. Replace “xx” with the relevant product name, for example, ESM. For exact name, check the [Patch installation files](#) section.

Setup command syntax for unattended mode

Operating system Unattended setup command syntax

	<pre>setup-XX-linux-10_0_0_2-20190807-64BIT.bin -i silent -DrpProduct.installLocation=/opt/InCharge</pre>
Linux	<p>Where XX represents the product name.</p> <p>Note you must provide the correct base installation location. Here in the example, base10.0 build is installed inside /opt/InCharge</p>

once the installation is completed inside /tmp ** log file will be created with the summary.

When the patch installation is complete, reconcile the configuration files as described in [Chapter 11 Reconcile user-modifiable files](#).

Apply DCF Patch using CLI Mode

This section details about the installation procedure of DCF patch in Console Mode.

To install DCF Patch:

Prerequisites

- 1 Download the installer package `dcf-1.0.0.1-32.bin` from support.vmware.com.
- 2 Ensure to stop all programs before you start the installation.

Procedure

- 1 Type the command `./dcf-1.0.0.1-32.bin -i console` to run the installer in console based installer mode. Press **Enter** to continue.
License agreement prompt appears.
- 2 Press any key to continue to read license agreement or press '0' to advance to end. Type 'Y' and press **Enter** to accept the license agreement.

- Specify the directory to install DCF when installer prompts, or else press **Enter** to accept the default folder.

Default Install Folder: /opt/DCF

Note If the target directory already contains an existing DCF installation, then it upgrades (patch or full), else fresh installation takes place.

- Verify the following in the Pre-Installation Summary before moving ahead with the installation:

```
Product Name:
  DCF

Install Folder:
  /opt/DCF
```

- Press **Enter** to continue.

Installation complete message displays.

- Press **Enter** to exit the installer.

Apply DCF Patch using Unattended (Silent) Mode

This section illustrates the DCF patch installation in Unattended (Silent) mode that is patch installation without user input.

To start with an unattended installation of the DCF patch, type the below setup command and press **Enter**.

Setup command syntax for unattended mode when DCF base install location is /opt/DCF.

Operating system	Unattended setup command syntax
------------------	---------------------------------

Linux	<code>./dcf-1.0.0.1-32.bin -i silent</code>
-------	---

If the base install location is different from /opt/DCF, specify the location of the product suite to be patched in properties file.

For example, by adding DCF installation path as:

USER_INSTALL_DIR=/opt/DCF1 in "installer.properties" file.

Execute the command to create installer.properties file:

```
echo "USER_INSTALL_DIR=<DCF_Install_DIRECTORY>" > installer.properties
```

Provide path to the installer.properties file if it is not present in the dcf binary location and execute the following command for installation of DCF Patch:

```
./dcf-1.0.0.1-32.bin -i silent -f installer.properties
```

Note Ensure to update the `installer.properties` file with DCF 10.0.0 base directory `<DCF_Install_DIRECTORY>`, otherwise installation takes place at the new location causing two DCF instances.

Log files

Patch report and log file locations, lists the files that the Installation software creates during the install process.

Table 10-1. Patch report and log file locations

Name	Path	File Name
Install log	<BASEDIR>/smarts/setup/logs	Install.<product>_SUITE. <patchversion>.log
Merged files log	<BASEDIR>/smarts/setup/logs	merge-summary-<patch version>.log

Where <patch version> is the complete version number for the patch, for example, 10.0.0.2

Install log

The installer creates an Install log file listing all actions performed by the installation. You need not read this file unless you suspect an installation failure.

If the installation process fails, the log files are located in a temporary directory, for example /tmp or C:\temp. A non-zero status indicates a failure.

Merged files Log

This log lists the files in the BASEDIR/smarts/local directory structure that were merged. For each merged file, the log lists the location and name of the file. If any file cannot be merged due to conflicts, this is also noted. In addition, the log lists the name and location for unmerged versions of all user-modifiable files that are included in the patch.

For example, in case of ESM:

- Summary of merge operation can be found at location :

```
/opt/InCharge/ESM/smarts/setup/logs/merge-summary-10.0.0.2.log
```

- For more detail logs:

```
/opt/InCharge/ESM/smarts/setup/logs/detail-merge-10.0.0.2.log
```

If there were any conflict during the merge operation, the old local backup file will be saved as "File_Name.bkp" in its same location. These conflict files needs to be merged manually before starting the server.

Reconcile user-modifiable files

The Installation software is designed to preserve your changes to user-modifiable files when installing new versions of these files.

Existing changes to user-modifiable files are always automatically merged. All files are merged by default.

The Installation software also creates a backup of all the versions of the user-modifiable files to ensure that you will not lose any configuration data.

Note Ensure to resolve the merge conflict issues before starting the application.

This chapter includes the following topics:

- [Review the results of the reconciliation process](#)
- [Resolve issues in conflict files](#)

Review the results of the reconciliation process

The results of the reconciliation analysis performed during the installation and all actions taken are included in the merged files log located in <BASEDIR>/smarts/setup/logs. The name of the log file is

```
install.merge.<patch version>.log
```

Determine which files require action by reviewing the merged files log generated by the install process:

- 1 Using any editor, open and review the log:
<BASEDIR>/smarts/setup/log/Install.Merge.10.0.0.2.log.
- 2 Review the log:
 - a Resolve conflicts in files manually. See [Resolve issues in conflict files](#).
 - b During the installation, the entries that indicate file merges without conflicts that resulted in automerger files.

Resolve issues in conflict files

If a conflict occurs for any file in the same local directory of the file location, you can find the below files:

- One is the conflict file. For example, <filename>
- Another file is .bak.001. For example, <filename>.bak.001

Review the conflict files and resolve issues using the following procedure:

- 1 Open the user-modifiable file where the conflict occurs using `sm_edit`.
For example, the conflict file for `esm.param.conf` is named `esm-param.conf`.
- 2 Review and resolve the conflict manually.
- 3 Save and close the file.

To use patch introduced file (for example, `esm-param.conf`):

- 1 Rename the original conflict file. (For example, if the conflict file name is `esm-param.conf`, rename the file `esm-param.conf` to `esm-param.conf_old`).
- 2 Rename the `<filename>.bak.001` file to the original file name `<filename>` by removing `.bak.001` extension.
For example, if the patch file name is `esm-param.conf.bak.001`, rename it to the `esm-param.conf` to use the original file.
- 3 Save and close the file.

Note All the user-modifiable unmerged files before patch installation, are backed up in "`<BASEDIR>/<Product Name>/smarts`" location. By default, the backup directory is hidden.

Uninstallation

Uninstalling a patch removes all previously applied patches and returns the software to the baseline product version.

Note Root privileges are required to uninstall a patch.

Note Use either the uninstaller program to uninstall a patch. Failure to use one of these methods can result in an unstable system and/or inconsistent product directories.

This chapter includes the following topics:

- [Before uninstallation](#)
- [Roll back to a previous patch](#)
- [Uninstall Patch Using the Uninstaller Program](#)
- [Uninstall Patch Using Unattended \(Silent\) Mode](#)
- [Uninstall DCF Patch using CLI Mode](#)
- [Uninstall DCF Patch Using Unattended \(Silent\) Mode](#)

Before uninstallation

You must complete the following task before uninstalling the patch:

- Stop all VMware Smart Assurance services and processes that use programs or libraries from the product.

Roll back to a previous patch

If you want to revert to a previous patch, you must:

- Uninstall the currently installed patch to return to the baseline version.
- Reinstall the previous patch.

For example, to revert from Patch 2 to Patch 1, uninstall Patch 2, and then reinstall Patch 1.

Uninstall Patch Using the Uninstaller Program

Use the uninstaller program to uninstall a patch:

Note Do not to use the uninstaller program in the `_uninst` directory because it will remove the entire product.

- 1 Change the directory or use the file navigator to find the `_rpuninst` directory.
For Example: `/opt/InCharge/<Product>/_rpuninst` on UNIX systems.
- 2 Invoke the uninstaller program.
For example: `./uninstaller` on UNIX systems.
- 3 press **Enter** to continue the uninstallation.

Uninstall Patch Using Unattended (Silent) Mode

Use the uninstaller program to uninstall a patch:

Note Do not to use the uninstaller program in the `_uninst` directory because it will remove the entire product.

- 1 Change the directory or use the file navigator to find the `_rpuninst` directory.
For Example: `/opt/InCharge/<Product>/_rpuninst` on UNIX systems.
- 2 Execute the uninstaller program.
`./uninstaller -i silent` on UNIX systems.
- 3 press **Enter** to continue the uninstallation.

Uninstall DCF Patch using CLI Mode

This section describes about the uninstallation procedure of DCF Patch in CLI mode.

Note Uninstallation of DCF, uninstalls the base also. There is no separate patch installation.

Procedure

- 1 Browse the uninstaller in `/opt/DCF/Uninstaller`.
`/opt/DCF` is the location where DCF is installed.
- 2 Invoke the uninstallation operation using `./uninstall`.
Uninstaller prepares for DCF uninstallation.
- 3 Uninstaller displays the confirmation message to remove the features installed by InstallAnywhere. It does not remove files and folders created after the installation. Press **Enter** to continue.
Uninstallation completes.

Uninstall DCF Patch Using Unattended (Silent) Mode

This section illustrates how to uninstall DCF patch in Unattended (Silent) mode that is patch uninstallation without user input or a response file. Specify the base location where the product suite is installed to invoke the uninstallation.

To start with an unattended uninstallation of the DCF patch, type the appropriate setup command from below table and then press **Enter**.

Setup command syntax for unattended mode

Operating system Unattended setup command syntax

Linux	<code><BaseDCFloc>/Uninstaller/uninstall -i silent</code>
-------	---

Troubleshooting and getting help

13

VCO Discovery fails with Java Exception

If the VCO discovery fails with Java Exception and below message appears in ESM logs:

```
NV_MESSAGE-*--NV_GENERIC-MSG ERR : [Thread-3 DiscoveryManager]:Null message received from kafka. It may be due to not having any data with in 100 seconds.

[June 18, 2019 4:26:36 AM EDT +019ms] t@219129600 Discovery #4
NV_MESSAGE-*--NV_GENERIC-MSG ERR : [Thread-3 VcoDiscovery]:Exception in Discovery through DCF collector

[June 18, 2019 4:26:36 AM EDT +022ms] t@1259902720 platform
MAIN_MSG-*--STDFD_ERR-stderr: java.lang.Exception: Error while receiving data from the kafka topic

[June 18, 2019 4:26:36 AM EDT +022ms] t@1259902720 platform
MAIN_MSG-*--STDFD_ERR-stderr: at
com.emc.asd.stream.discovery.vco.DiscoveryManager.startDiscovery(DiscoveryManager.java:137)
at com.emc.asd.stream.discovery.vco.VcoDiscovery.invoke(VcoDiscovery.java:170)
at com.smarts.java_probe.ProbeRunner.invoke(ProbeRunner.java:69)
```

Workaround:

Below parameter need to be set if there is a network latency and ESM is unable to read data from Kafka within default value of 100 seconds. Due to which VCO is not discovered.

MessagePollTimeoutPeriodInSeconds-<kafka_IP> 1200" .

Getting help

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

Product information - For documentation, release notes, software updates, or for information about products, go to VMware Online Support at:

- <https://docs.vmware.com>
- <https://support.vmware.com>