MICRO FOCUS

Application Performance Management

Software Version: 9.50

APM Upgrade Guide

Document Release Date: May 2018

Software Release Date: May 2018

Legal notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted rights legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright notice

Trademark notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD, the AMD Arrow symbol and ATI are trademarks of Advanced Micro Devices, Inc.

Citrix® and XenDesktop® are registered trademarks of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

iPad® and iPhone® are trademarks of Apple Inc.

Java is a registered trademark of Oracle and/or its affiliates.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, Lync®, Windows NT®, Windows® XP, Windows Vista® and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NVIDIA® is a trademark and/or registered trademark of NVIDIA Corporation in the U.S. and other countries.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SAP® is the trademark or registered trademark of SAP SE in Germany and in several other countries.

UNIX® is a registered trademark of The Open Group.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To verify you are using the most recent edition of a document, go to https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.

To check for recent software patches, go to https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=patches?keyword=.

This site requires that you register for a Passport and sign in. To register for a Passport ID, go to https://cf.passport.softwaregrp.com/hppcf/login.do.

Or click the **Register** link at the top of the Software Support page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your sales representative for details.

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To verify you are using the most recent edition of a document, go to https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=online help.

This site requires that you register for a Passport and sign in. To register for a Passport ID, go to https://cf.passport.softwaregrp.com/hppcf/login.do.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your sales representative for details.

For information and details about the products, services, and support that offers, contact your Client Director.

Support

Visit the Software Support Online web site at https://softwaresupport.softwaregrp.com/.

This web site provides contact information and details about the products, services, and support that offers.

online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Manage software licenses
- Download new versions of software or software patches
- Access product documentation
- Manage support contracts
- Look up support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require you to register as a Passport user and sign in. Many also require a support contract.

To register for a Passport ID, go to https://cf.passport.softwaregrp.com/hppcf/login.do.

Visit the Software Support Online web site at https://softwaresupport.softwaregrp.com/.

This web site provides contact information and details about the products, services, and support that offers.

online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Manage software licenses
- Download software
- Access product documentation
- Manage support contracts
- Look up support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require you to register as a Passport user and sign in. Many also require a support contract.

To register for a Passport ID, go to https://softwaresupport.softwaregrp.com/.

To check for recent updates or to verify that you are using the most recent edition of a document, contact your Client Director.

Contents

Introduction

Welcome to the APM Upgrade Guide. This guide provides a detailed workflow for how to upgrade from APM 9.40 to APM 9.50 and from 9.30 to 9.50.

NOTE:

- If you have an earlier version of BSM, you must upgrade your existing version to APM 9.40 with the latest patch and then upgrade to APM 9.50. See the APM Upgrade Guide - BSM 9.25 or 9.26 to APM 9.30 (https://softwaresupport.hpe.com/km/KM02225469).
- If you have an earlier version of BSM, you must upgrade your existing version to APM 9.30 with the latest patch and then upgrade to APM 9.50. See the APM Upgrade Guide - BSM 9.25 or 9.26 to APM 9.30 (https://softwaresupport.hpe.com/km/KM02225469).
- If you have a RUM data collector, when upgrading APM, RUM persists the data samples to send to APM. Persistency is limited by the amount of unsent sample data and by time. To increase the amount of unsent sample data, see Configuring the Amount of Unsent Sample Data to Store in RUM in the Real User Monitor Administration Guide.

How This Guide is Organized

This book is divided into the following parts:

- Part 1 contains the workflow for upgrading using the direct method
- Part 2 contains the workflow for upgrading using the staging method
- Part 3, the appendix, contains reference information that applies to both the staging and upgrade workflows

You should select either the staging or direct workflow. Whichever workflow is chosen should be read and executed in chronological order where relevant.

Staging vs. Direct Upgrade Overview

There are two possible methods for upgrading from APM 9.40 to APM 9.50.

Using a **staging** environment to upgrade to APM refers to installing the new software on different machines and database schemas (referred to as the staging environment) to allow the original servers to continue functioning while the upgrade is in process. The original machines are referred to as the production environment. This minimizes downtime and allows you to ensure that the new servers are functioning as required before disconnecting the original servers.

When upgrading using a staging environment, APM 9.40 is installed on the staging servers. Staging mode begins when both production and staging servers are installed. During staging mode, metric data is transferred from the production server to the staging server using the Staging Data Replicator (SDR).

Only changes to the database are transferred during staging mode, configuration changes made to the production server are not transferred.

NOTE:

- If your source and target environments are not running the same operating systems, you must upgrade using the staging method.
- If you are upgrading to APM 9.50 and are running Red Hat Enterprise Linux 5.x, upgrade your operating system to Red Hat Enterprise Linux 6.x or 7.x and then perform the upgrade if you plan to use the Direct method.
- Scheduled reports are not sent from the staging servers while in staging mode. For more details, see Troubleshooting the Upgrade Process, on page 100.
- All APM machines in the staging environment must be set to the same time zone as the source environment. Incompatible time zone settings can lead to inaccuracies in reporting historical data.

Upgrading **directly** refers to installing the new version on the same/new servers and database schemas as the original version. This can only be performed after uninstalling the original version and therefore results in greater downtime.

NOTE:

- You must upgrade using a staging environment if you are switching operating systems. In APM 9.50, Windows Server 2003 is no longer supported. Users with Windows Server 2003 have to perform a staging upgrade to a supported operating system.

- If you are using the staging upgrade option (from BSM 9.25/6) with the standalone SDR, you need to use the 9.30 SDR. You can also use the 9.30 SDR to send the samples from BSM 9.25/6 to the staging APM 9.30.

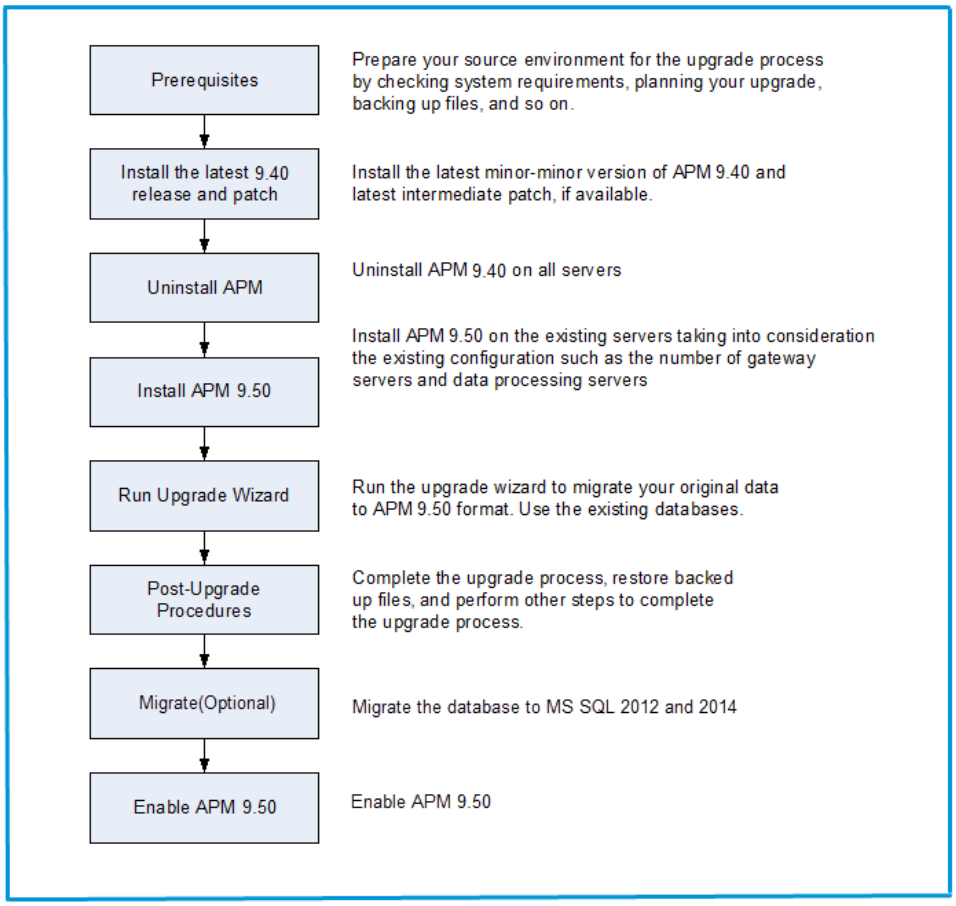
  When you will upgrade the staging APM 9.40 directly to APM 9.50, you can use the same 9.40 SDR to send samples to APM 9.50.

Part 1: Direct Upgrade

This section contains the workflow for upgrading APM using the direct method.

Chapter 1: Overview of APM 9.40 to APM 9.50 Direct Upgrade

The upgrade from APM 9.40 to APM 9.50 involves a number of milestones. The following diagram shows the major steps and how they affect your environment.



Chapter 2: Prerequisites

Perform all steps specified in this chapter before continuing with the upgrade process.

General Prerequisites

Perform the following steps where relevant before continuing with the upgrade process.

1. ## Create deployment plan

   Create a complete deployment plan including the required software, hardware, and components. For details, see the APM Getting Started Guide and the APM System Requirements and Support Matrixes. You can access these documents from the Software Support site (https://softwaresupport.softwaregrp.com).

2. ## Create upgrade plan

   Create an upgrade plan, including such items as whether you will be performing a staging or direct upgrade, estimated down time, and so on.

   Database Administrator. During the upgrade process, the services of your Database Administrator may be required.

   Multiple servers. If you are upgrading multiple APM servers, perform the upgrade procedure on only one Gateway and one Data Processing server. When the upgrade process is complete, install any additional servers and connect them to the database schemas using Configuration Wizard as described in the APM Installation Guide.

3. ## Allocate additional disk space.

   The database replication requires 1.5 times the amount of disk space in your original (production) database. If you want to save original data by selecting this option in the upgrade wizard, you will need two times the amount of disk space in your original database.

4. ## Order and register licenses

   Order licenses with a sales representative based on your deployment plan. Register your copy of APM to gain access to technical support and information on all products. You will also be eligible

for updates and upgrades. You can register your copy of APM on the Support site https://softwaresupport.softwaregrp.com.

5. Set up database server

NOTE:
You cannot change the database type during the upgrade if you want to keep your configuration and runtime data. For example, if you currently run Oracle, you must also use Oracle with the new APM environment.

Verify that your database has the following settings:

- Oracle: The Oracle Partitioning option must be enabled. Make sure that the parameter **RECYCLEBIN** is set to **Off**, as specified in the APM Database Guide.

For information about setting up your database server, see the APM Database Guide.

6. Migrate manual changes to conf directory

If you made changes to any files in the **<HPE APM root directory>\WebServer\conf** directory, back up the changed files and, after the upgrade, reapply the changes to the new files (**do not copy the old files on top of the new ones**).

7. Back up database schema (recommended)

We recommend backing up database schemas as close as possible to the upgrade procedure.

8. Delete obsolete database schemas (optional)

Delete BPI, Events, and RTSM History database schemas since they are no longer used in APM 9.50

9. Disable RTSM integrations (optional)

If integrations are configured in the RTSM Integration Studio (for example, topology synchronization integrations between central UCMDB and RTSM), after upgrading, the Data Flow Probe will run population jobs immediately for active integration points, even if the integration is not scheduled. If you do not want the integration to run, disable the integration before running the upgrade from APM 9.40.

10. Back up files

Back up the following files from your original APM servers:

- **<Gateway Server root directory>\AppServer\webapps\site.war\openapi\excels directory**
- **<Data Processing Server root directory>\BLE\rules\<custom rules jar> file(s)**

- **<Gateway Server root directory>\JRE\lib\security\cacerts**
- **<Gateway Server root directory>\JRE64\lib\security\cacerts**
- **<Data Processing Server root directory>\BLE\rules\groovy\rules\ file(s)**

11. Back up your license folder

    - **On Windows:** <HPE APM root directory>\conf\license
    - **On Linux:** /opt/HP/BSM/conf/license

12. Copy customized Java database connectivity properties (jdbc) - Oracle RAC (optional)

    When upgrading, the custom modifications you made in the **jdbc.drivers.properties** file are overwritten. If you configured APM with an Oracle RAC database, and if you have custom modifications in the jdbc.drivers.properties file:

    Create a new file in **<HPE APM root directory>/conf** called **jdbc.drivers.extension<number>.<name>.properties** and copy only the custom properties from jdbc.drivers.properties to this file before performing the upgrade.

    For example, before upgrading, copy this string: **ddoracle.url=jdbc:mercury:oracle:TNSNamesFile=<HOME_APM>\\conf\\bac-tnsnames.ora;TNSServerName=${sid}** from the **jdbc.drivers.properties** file to the **<HOME_APM>/conf/jdbc.drivers.extension1.RAC.properties** file.

    After upgrading, the **jdbc.drivers.extension1.RAC.properties** file is not overwritten so all the custom properties are saved this file is used by APM.

    If there are multiple custom files in the **<HPE APM root directory>/conf/** directory with the same property name, APM uses the one with the latest extension number.

13. Disable APM-Operations Bridge Manager (OBM ex OMi) integration

    If OBM Integration is enabled, disable it by clearing the OBM URL before upgrading.

    a. Check whether the OBM integration is enabled in the JBoss JMX console:

       OMi-Integration > OMi-Integration:service=Settings > boolean isIntegrationEnabled for customer 1

    b. If the OBM integration is enabled:

       i. Issue **DELETE REST** call to URL: **http://<APM_HOST>/topaz/omi/integration/customer/1/settings/url** to delete the OBM URL setting.

       ii. In APM, locate the names of the CI Status Alerts that need to be deleted:

       Admin > Platform > Infrastructure Settings > Foundations > OMi Integration > OMi Integration - Statuses Synchronization

iii. In APM, select **Admin > Service Health > CI Status Alerts** and locate and delete the required alerts.

iv. On the OBM side, delete the APM Connected Server:

OMi > Administration > Setup and Maintenance > Connected Servers

NOTE:
After completing the upgrade, you will need to perform the integration again. See the OBM Integration Guide for instructions.

Installation Prerequisites - Windows

Note the following before installing APM servers on a Windows platform:

- It is recommended that you install APM servers to a drive with at least 40 GB of free disk space. For more details on server system requirements, see the APM System Requirements and Support Matrixes.
- If APM servers, including the database servers, are installed on multiple network segments, it is highly recommended that the number of hops and the latency between the servers be minimal. Network-induced latency may cause adverse affects to the APM application and can result in performance and stability issues. We recommend the network latency should be no more than 5 milliseconds, regardless of the number of hops. For more information, contact Support.
- APM servers must be installed on dedicated machines and must not run other applications. Certain APM components can coexist on APM servers. For details on coexistence support, see the APM System Requirements and Support Matrixes.
- If you plan to use the IIS web server, install it prior to APM installation and enable it after the installation is completed. For more information, see Working with the IIS Web Server, on page 73.
- APM servers must not be installed on a drive that is mapped to a local or network resource.
- Due to certain web browser limitations, the names of server machines running the Gateway Server must consist only of alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and periods (.). For example, if the names of the machines running the Gateway Server contain underscores, it may not be possible to log into the APM site when using Microsoft Internet Explorer 7.0 or later.
- During APM server installation, you can specify a different path for the APM directory (default is **C:\HPBSM**), but note that the full path to the directory must not contain spaces, cannot contain more than 15 characters, and should end with **BSM**.
- The installation directory name should consist of only alphanumeric characters (a-z, A-Z, 2-9).

  NOTE:
  You cannot use 0 or 1 in the installation directory name

- User Access Control (UAC) must be disabled before installing APM. UAC is enabled by default in

some version of Windows Server. To manually disable UAC run the following command:

C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f

C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v ConsentPromptBehaviorAdmin /t REG_DWORD /d 0 /f

- If you plan to run APM servers on a hardened platform (including using HTTPS protocol), review the hardening procedures described in the APM Hardening Guide.
- If you do not have a profile database on your source environment, please add one before starting the upgrade. The database should be marked as the default profile database. Most users already have a profile database.
- You must have administrator privileges to install APM on the server machine.
- In the APM cluster, open port 21212 on the Data Processing Server.

  NOTE:
  During installation, the value of the Windows Registry key HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ReservedPorts is updated to include the following port ranges required by APM: 1098-1099, 2506-2507, 8009-8009, 29000-29000, 4444-4444, 8083-8083, 8093-8093.

  These port ranges are not removed from the registry key at APM uninstall. You should remove the ports from the registry key manually after uninstalling APM if they are no longer needed by any other application.

Installation Prerequisites - Linux

Note the following before installing APM servers on a Linux platform:

- It is recommended that you install APM servers to a drive with at least 40 GB of free disk space. The /tmp directory should have at least 2.5 GB of free disk space. You can change the /tmp directory by running the following command:

  ```
  export IATEMPDIR=/new/tmp/dir
  ```

  ```
  export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp/dir
  ```

  where `/new/tmp/dir` is the new /tmp directory

  For more details on server system requirements, see the APM System Requirements and Support Matrixes.
- If APM servers, including the database servers, are installed on multiple network segments, it is highly recommended that the number of hops and the latency between the servers be minimal.

Network-induced latency may cause adverse affects to the APM application and can result in performance and stability issues. We recommend the network latency should be no more than 5 milliseconds, regardless of the number of hops. For more information, contact Support.

- APM servers must be installed on dedicated machines and must not run other applications. Certain APM components can coexist on APM servers. For details on coexistence support, see the the APM System Requirements and Support Matrixes.
- Before installing APM on a Linux machine, make sure that SELinux does not block it. You can do this by either disabling SELinux, or configuring it to enable java 32-bit to run.

  To disable SELinux, open the **/etc/selinux/config** file, set the value of **SELINUX=disabled**, and reboot the machine.

  On systems with SELinux disabled, the `SELINUX=disabled` option is configured in **/etc/selinux/config**:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

  Also, the `getenforce` command returns **Disabled**:

```
~]$ getenforce
Disabled
```

  To confirm that the aforementioned packages are installed, use the rpm utility:

```
~]$ rpm -qa | grep selinux
selinux-policy-3.12.1-136.el7.noarch
libselinux-2.2.2-4.el7.x86_64
selinux-policy-targeted-3.12.1-136.el7.noarch
libselinux-utils-2.2.2-4.el7.x86_64
libselinux-python-2.2.2-4.el7.x86_64
```

```
~]$ rpm -qa | grep policycoreutils
policycoreutils-2.2.5-6.el7.x86_64
policycoreutils-python-2.2.5-6.el7.x86_64
```

```
~]$ rpm -qa | grep setroubleshoot
setroubleshoot-server-3.2.17-2.el7.x86_64
setroubleshoot-3.2.17-2.el7.x86_64
setroubleshoot-plugins-3.0.58-2.el7.noarch
```

Before SELinux is enabled, each file on the file system must be labeled with an SELinux context. Before this happens, confined domains may be denied access, preventing your system from booting correctly.

To prevent this, configure `SELINUX=permissive` in the **/etc/selinux/config file**:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

As a root user, restart the system. During the next boot, file systems are labeled. The label process labels all files with an SELinux context:

```
~]# reboot
```

In permissive mode, SELinux policy is not enforced, but denials are logged for actions that would have been denied if running in enforcing mode.

Before changing to enforcing mode, as a root user, run the following command to confirm that SELinux did not deny actions during the last boot. If SELinux did not deny actions during the last boot, this command does not return any output.

```
~]# grep "SELinux is preventing" /var/log/messages
```

If there were no denial messages in the **/var/log/messages** file, configure `SELINUX=enforcing` in **/etc/selinux/config**:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Reboot your system. After reboot, confirm that `getenforce` returns **Enforcing**:

```
~]$ getenforce
Enforcing
```

```
~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
```

```
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
```

- To configure SELinux to enable java 32-bit to run, execute the command **setsebool –P allow_ execmod on**.
- APM servers must not be installed on a drive that is mapped to a network resource.
- Due to certain Web browser limitations, the names of server machines running the Gateway Server must only consist of alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and periods (.). For example, if the names of the machines running the Gateway Server contain underscores, it may not be possible to log in to the APM site. To access the APM site in this case, use the machine's IP address instead of the machine name containing the underscore.
- If you plan to run APM servers on a hardened platform (including using HTTPS protocol), review the hardening procedures described in the APM Hardening Guide.
- You must be a root user to install APM on the server machine.
- The **DISPLAY** environment variable must be properly configured on the APM server machine. The machine from which you are installing must be running an X-Server as the upgrade process cannot be performed silently.
- If you do not have a profile database on your source environment, please add one before starting the upgrade. The database should be marked as the default profile database. Most users already have a profile database.
- In the APM cluster, open port 21212 on the Data Processing Server.
- To install APM 9.50 on Oracle Linux (OEL) or Red Hat Enterprise Linux operating systems supported 6.x and 7.x versions, the following RPM packages must be installed in the machine:

◦ glibc	◦ libXext
◦ glibc-common	◦ libXtst
◦ nss-softokn-freebl	◦ compat-libstdc++-33
◦ libXau	◦ libXrender
◦ libxcb	◦ libgcc
◦ libX11	◦ openssl1.0.2g
	◦ rpm-devel

The installer attempts to install or update these packages.

If the installation of one of the above packages fails:

1. Click **Cancel** to stop the installation.
2. Refer the problem to your system administrator.
3. When the problematic package is fixed, re-run the installation

NOTE:
If the installer fails to install **compat-libstdc++-33**, manually download the following RPM packages:

- **compat-libstdc++-33.i686**
- **compat-libstdc++-33.x86_64**

If the Yum Linux upgrade service is not functional on your machine, you will need to download and install the necessary RPM packages manually by running the following command:

yum install -y openssl1.0.2g glibc.i686 glibc-common.i686 nss-softokn-freebl.i686 libXau.i686 libxcb.i686 libX11.i686 libXext.i686 libXtst.i686 compat-libstdc++-33.i686 libXrender.i686 libgcc.i686 rpm-devel

NOTE:
The version of these packages changes from system to system. You can download the packages from any RPM repository site that matches your system specifications. The following RPM search tool can assist you in this task (http://rpm.pbone.net/).

To determine the package version you need to download:

- Run the following command in a terminal window:

  rpm –qa ${PACKAGE_NAME} (ex: rpm -qa glibc)

  The command will return the following text:

  ```
  # rpm -qa glibc
  glibc-2.12-1.132.el6.x86_64
  ```

  This text indicates the package version required for your machine.

  For example, in this case you would need to download the i686 architecture package with the same version - glibc-2.12-1.132.el6.i686 – and install it manually.

Chapter 3: Uninstall APM

Disable APM on all servers by selecting **Start > Programs > Application Performance Managemen > Administration > Disable Application Performance Managemen**.

Back up your license folder. Your license folder is located in:

- Windows: **<HPE APM root directory>\conf\license**
- Linux: **/opt/HP/BSM/conf/license**

Uninstall APM on all servers using one of the following procedures:

Uninstalling APM servers in a Windows environment

To completely uninstall Application Performance Management servers in a Windows environment:

1. Uninstall APM via the Windows user interface or silently.
   a. Uninstall APM Using the Windows user interface:
      i. On the machine from which you are uninstalling Application Performance Management, select **Start > Control Panel > Programs and Features**. Select **Application Performance Management**.
      ii. Click **Uninstall**, wait for the APM uninstall script to remove any present updates, and follow the on-screen instructions when prompted.

      NOTE:
      In some cases, this process may take a long time (more than 30 minutes).

      iii. If the **Show Updates** check box is selected, all the updates installed over APM are displayed. When APM is removed, all updates are also removed.
   b. Uninstall APM silently:
      i. Stop all APM servers.
      ii. Run the command **<HPE APM root directory>\installation\bin\uninstall.bat -i silent**
2. Restart the server machine.
3. If you are running APM with Microsoft IIS, open the IIS Internet Services Manager and check the following:
   a. Under the **Default Web Site**, check that the following virtual directories have been removed and remove them if they still appear:

- bpi
- bsm
- ext
- HPBSM
- jakarta
- mam_images
- mercuryam
- odb
- topaz
- tvb
- ucmdb-ui
- uim

b. Right-click the server machine name in the tree, and select **Properties**. In the Properties dialog box, with **WWW Service** displayed in the Master Properties list, click **Edit**. Select the **ISAPI Filters** tab. If the **jakartaFilter** filter still appears, remove it.

NOTE:
If you plan to uninstall APM and then reinstall it to a different directory on the server machine, there is no need to remove the **jakartaFilter** filter. However, you will need to update the path for the filter. For details, see After uninstalling APM and reinstalling to a different directory, APM does not work, on page 95.

Uninstalling APM servers in a Linux environment

1. Log in to the server as user **root**.
2. To access the uninstall program, type: **cd /opt/HP/BSM/installation/bin**
3. Stop all APM servers.
4. Run the following script to uninstall in UI mode: **./uninstall.sh**. To perform this step in silent mode, use the command **./uninstall.sh -i silent**.
5. The APM uninstall program begins. Follow the on-screen instructions. When the uninstall program is complete, a success message is displayed.
6. Click **Finish**.
7. Check the **HPBsm_<version>_HPOvInstaller.txt** log file located in the **/tmp** directory for errors. Previous installation files can be found in the **/tmp/HPOvInstaller/HPBsm_<version>** directory.

NOTE:
If you encounter problems during the uninstall procedure, contact Support.

Migrate Database to MS SQL 2012 and MS SQL 2014 (optional)

If you would like to use either MS SQL 2012 or MS SQL 2014, migrate your database to a new MS SQL 2012 or MS SQL 2014 database. For details, see the MS SQL documentation.

Chapter 4: Install APM 9.50

Install APM 9.50 on a set of APM servers. This set can be either one Gateway Server and one Data Processing Server or a single one-machine server. In the first case, run the wizards on the Data Processing Server first. The wizard will direct you as to when to begin installation on the Gateway Server.

NOTE:

- Do not install additional servers at this time, you can install them towards the end of the workflow.
- You must install APM using a user with root (Linux) or administrative privileges (Windows). If necessary in case Windows OS, switch the user which has administrative privileges that is being used to install and enable APM.
- Run the installation and post-installation wizards. Do not run the upgrade wizard yet. Exit the wizard on the last screen of the post-installation wizard without continuing.

Download the software

1. Go to the Software Support web site (https://softwaresupport.softwaregrp.com) and sign in using your Passport.
2. Click **Product Information > Downloads**.
3. Click **Select an SAID** and select **application performance management (bac)** from the Products list.

   or

   Click **Directly enter an SAID** and enter your SAID.
4. Accept the terms and conditions.
5. Click **View available products**.
6. In the Show a single category/product center drop down list, select **Application Performance Management**.
7. Select **Application Performance Managemen version 9.50** in the language you require (for example, Application Performance Management version 9.50 English Software E-Media).
8. Click **Get software updates**.
9. Click **Get Software** for your selected product.
10. Confirm that your product is selected in the Product name field.

11. From the Downloads field, select the required download:
    - **Application Performance Managemen 9.50 Windows Setup (APM_9.50_Windows_ Setup.zip)**
    - **Application Performance Managemen 9.50 Linux Setup (APM_9.50_Linux_Setup.zip)**
12. Click **Download**.
13. Unzip the file and run the installation program.

Run Installation and Post Installation Wizards

- Installing APM on a Windows Platform, on page 72
- Installing APM on a Linux Platform, on page 81
- Installing APM Silently, on page 85

If there is a patch available, Go to the Software Support web site (https://softwaresupport.softwaregrp.com) and download the required patch.

Alternatively, you may run the Installation and Post-Installation wizards in silent mode. However, silent mode is not supported for the Upgrade Wizards. For details, see Installing APM Silently.

Chapter 5: Run 9.50 Upgrade Wizard

You should only have one set of 9.50 servers installed at this time. Do not run the Upgrade Wizard on more than one set of 9.50 servers.

You can launch the Upgrade Wizard from the Post-Install Wizard by choosing the following option:

- Upgrade. Continue with the upgrade from APM 9.40 with latest intermediate patch

If you can choose **Exit. Complete the upgrade or installation process at a later time.** you will need to run the Upgrade Wizard manually.

The upgrade wizard can be found on all Gateway, Data Processing, and One-machine servers in the following locations:

- **Windows:**
  - If you want to upgrade from 9.30 to 9.50 version, select the upgrade wizard from the following location:

  <HPE APM root directory>\bin\upgrade_wizard_run_from930.bat
  - If you want to upgrade from 9.40 to 9.50 version, select the upgrade wizard from the following location:

  <HPE APM root directory>\bin\upgrade_wizard_run_from940.bat
- **Linux:**
  - If you want to upgrade from 9.30 to 9.50 version, select the upgrade wizard from the following location:

  /opt/HP/BSM/bin/upgrade_wizard_run_from930.sh
  - If you want to upgrade from 9.40 to 9.50 version, select the upgrade wizard from the following location:

  /opt/HP/BSM/bin/upgrade_wizard_run_from940.sh

For details about the upgrade wizard, see Upgrade Wizard, on page 88.

Chapter 6: Post-Upgrade Procedures

Perform these tasks to complete the upgrade process:

General Post-Upgrade Procedures

Perform these tasks to complete the upgrade process:

Upgrading Customized Service Health KPIs

In APM, the internal format of the KPI parameter “KPI is critical if” was changed. As a result, this value may be incorrect following upgrade, if you have created or customized KPIs.

NOTE:
APM must be running to perform this step.

To fix this, perform the following:

1. Access the JMX console on the Gateway Server via http://<Gateway Server name>:29000/ and enter your user name and password.
2. Click **service=repositories_manager** in the Topaz section.
3. Locate the **upgradeCriticalIf()** and input **1** as the customer ID in the parameter field.
4. Click **Invoke**.

Delete temporary internet files

When logging into APM for the first time after upgrading, delete the browser's temporary Internet files. This should be done on each browser that accesses APM.

Disable firewall between APM Gateway and Data Processing servers

In general, placing firewalls between APM servers is not supported. If an operating system firewall is active on any APM server machine (GW or DPS), a channel must be left open to allow all traffic between all APM Gateway and DPS servers.

Additionally, to enable APM users and data collectors to communicate with the APM Gateway servers, you must leave open the relevant ports depending on your APM configuration. The required ports are typically 443 or 80. For details, see "Port Usage" in the APM Platform Administration Guide.

- ## Update Data Collectors

  See the System Requirements and Support Matrixes, available from **Help > Planning and Deployment** and the Updated Components section in the Business Service Management Release Notes to determine if you must upgrade your data collector to the latest supported version.

- ## Restore the following files from backup

  Restore the following files to the APM server:

  - <Gateway Server root directory>/AppServer/webapps/site.war/openapi/excels directory
  - <Data Processing Server root directory>/BLE/rules/<custom rules jar> file(s)
  - <Gateway Server root directory>/JRE/lib/security/cacerts
  - <Gateway Server root directory>/JRE64/lib/security/cacerts
  - <Data Processing Server root directory>\BLE\rules\groovy\rules\ file(s)

- ## Perform hardening procedures

  If your original environment was secured with SSL and you are upgrading using a staging environment, you need to repeat the hardening procedures described in the APM Hardening Guide.

  If your original environment was secured with SSL and you are upgrading directly, you need to repeat the following hardening procedures:

  1. If you had previously made changes to **<HPBSM root directory>\EJBContainer\server\mercury\deploy\jboss-web.deployer\server.xml** while performing hardening procedures on your system, repeat the “Securing JBOSS” procedure in the Hardening Guide after the patch installation on all relevant APM machines.
  2. If you had previously configured SSL on an IIS web server used by APM, you need to verify HTTPS port binding in IIS is set to the correct port (443).
  3. If you had previously configured SSL on the Apache web server used by APM, you may need to reapply the changes to httpd.conf and httpd-ssl.conf files as follows:
     - In **<HPE APM root directory>\WebServer\conf\httpd.conf**, uncomment the following two lines:

       LoadModule ssl_module modules/mod_ssl.so
       Include conf/extra/httpd-ssl.conf
     - In **<HPE APM root directory>\WebServer\conf\extra\httpd-ssl.conf**, specify paths to

SSLCertificateFile and **SSLCertificateKeyFile**

- Restart the APM Apache web service

Ensure all processes started properly

You can check to ensure that all processes started properly. For details, see "How to View the Status of Processes and Services" in the APM Platform Administration Guide.

Check installation log files

You can see the installation log file by clicking the **View log file** link at the bottom of the installer window.

In a Windows environment, this log file, along with additional log files for separate installation packages, is located in the **%temp%\..\MicroFocusOvInstaller\HPEApm_9.50** directory.

In a Linux environment, the logs files are located in the **/tmp/HPOvInstaller/HPEApm_<version>** directory.

The installer log file name is in the following format:

HPEApm_<VERSION>_<DATE>_ HPOvInstallerLog.html or **HPEApm_<VERSION>_ <DATE>_ HPOvInstallerLog.txt** (for example, HPEApm_9.50_2018.05.10_11_53_ MicroFocusOvInstallerLog.txt).

Individual installation package log file names are in the following format:

Package_<PACKAGE_TYPE>_HPEApm_<PACKAGE_NAME>_install.log (for example, Package_msi_HPEApm_BPMPkg_install.log).

NOTE:
If the server is rebooted, all files from the **tmp** folder are deleted automatically by default. Therefore, backup all log files after installing APM, before rebooting the server.

Restore APM service changes

If you manually configured different users to run APM services, these settings must be configured again. For details, see Changing APM Service Users , on page 90.

Install component setup files

The component setup files are used to install the components used by APM. The component setup files are not installed as part of the basic APM installation. They are located separately in the Web delivery package download area. You can upload them to the APM Downloads page. The component setup files can then be downloaded from APM and used when required. For details on working with the APM Downloads page, see "Downloads" in the APM Platform Administration Guide.

NOTE:

- The components on the Downloads page are updated for each major and minor release (for example, 9.00 and 9.20). To download updated components for minor minor releases and patches (for example, 9.26), go to the Software Support site (https://softwaresupport.softwaregrp.com).
- You can install a component by using the component's setup file directly from the network. For details on installing a component, refer to the individual documentation for the component you want to install. The relevant documentation is available from the Downloads page in APM after the component's setup files are copied to the Downloads page.

To install component setup files, copy the component setup files that you want available in the Downloads page from the appropriate directory in the release download area to the **<HPE APM root directory>\AppServer\webapps\site.war\admin\install** directory on the APM Gateway server. If required, create the **admin\install** directory structure.

Starting and Stopping APM

After completing the APM server installation, clean your browser's cache and restart your computer. It is recommended that you do this as soon as possible. Note that when the machine restarts, you must log in as the same user under which you were logged in before restarting the machine.

NOTE:
If the server is rebooted, all files from **tmp** folder are deleted automatically by default. So backup all log files after installing APM, before rebooting the server.

After installing the APM servers (either together on one machine, or at least one instance of each server type in a distributed deployment) and connecting the server machines to the databases, you launch APM on each server machine.

NOTE:
You can check which APM servers and features are installed on an APM server machine by viewing the [INSTALLED_SERVERS] section of the **<HPE APM root directory>\conf\TopazSetup.ini** file. For example, Data_Processing_Server=1 indicates that the Data Processing Server is installed on the machine.

To start or stop APM in Windows:

Select **Start > All Programs > Micro Focus Application Performance Management > Administration > Enable | Disable Micro Focus Application Performance Management.** When

enabling a distributed environment, first enable the Data Processing Server and then enable the Gateway Server.

To start or stop APM in Linux:

/opt/HP/BSM/scripts/run_hpbsm {start | stop | restart}

To start, stop, or restart APM using a daemon script:

/etc/init.d/hpbsmd {start| stop | restart}

NOTE:
When you stop APM, the APM service is not removed from Microsoft's Services window. The service is removed only after you uninstall APM.

Logging In and Out

You log in to APM from a client machine's browser using the login page. LW-SSO is APM's default authentication strategy. For details, see "Logging into APM with LW-SSO" in the APM Platform Administration Guide.

You can disable single sign-on authentication completely, or you can disable LW-SSO and use another supported authentication strategy. For details on selecting an authentication strategy, see "Set Up the Authentication Strategies" in the APM Platform Administration Guide.

To access the APM login page and log in for the first time:

1. In the Web browser, enter the URL http://<server_name>.<domain_name>/HPBSM where **server_name** and **domain_name** represent the FQDN of the APM server. If there are multiple servers, or if APM is deployed in a distributed architecture, specify the load balancer or Gateway Server URL, as required.

   NOTE:
   Users running previous versions of APM can still use bookmarks set to access the URL http://<server_name>.<domain_name>/mercuryam and http://<server_name>.<domain_name>/topaz

2. Enter the default administrator user ("admin"), and the password specified in the Setup and Database Configuration utility, and click **Log In**. After logging in, the user name appears at the top right.
3. (Recommended) Create additional administrative users to enable APM administrators to access the system. For details on creating users in the APM system, see "User Management" in the APM Platform Administration Guide.

NOTE:
- For login troubleshooting information, see "Troubleshooting and Limitations" in the APM

Platform Administration Guide.

- For details on login authentication strategies that can be used in APM, see "Authentication Strategies — Overview" in the APM Platform Administration Guide.
- For details on accessing APM securely, see the APM Hardening Guide.

When you have completed your session, it is recommended that you log out of the website to prevent unauthorized entry.

To log out:

Click **Logout** at the top of the page.

Adding Additional APM Servers

After you have a working APM 9.50 environment, you can add new Gateway and Data Processing servers as desired.

To add new APM servers to an existing APM environment:

1. Go to the Software Support web site (https://softwaresupport.softwaregrp.com) and sign in.
2. Click **Search**.
3. For Windows, select **Application Performance Management (BAC) > 9.50 > Windows**.

   For Linux, select **Application Performance Management (BAC) > 9.50 > Linux**.
4. Under Document Type, select **Patches**.
5. Locate the APM 9.50 package and save it locally.
6. Launch the relevant setup file to install APM 9.50
7. Run the installation files on all APM servers (Gateway and Data Processing).
8. The Post Install Wizard starts automatically. You should complete the information in this Wizard. On the last page, click the **Exit** option to prevent the Setup and Database Configuration utility from running.
9. Download and install the latest minor minor version (if avialable) from the Software Support site
   a. Go to the Software Support web site (https://softwaresupport.softwaregrp.com) and sign in.
   b. Click **Search**.
   c. Select the relevant product, version , and operating system.
   d. Under Document Type, select **Patches**.
   e. Locate the applicable patch, save it locally and launch the relevant setup file to install the patch.
   f. Run the installation file on APM server.

g. The post-installation wizard is automatically run after the patch installation in silent mode.

h. Repeat this procedure for the latest intermediate patch (if available).

10. Run the Setup and Database Configuration utility.
    - Windows: On the APM server, select **Start > All Programs > Micro Focus Application Performance Management > Administration > Configure Micro Focus Application Performance Management**.
      Alternatively, you can run the file directly from **<HPE APM root directory>\bin\config-server-wizard.bat**.
    - Linux: On the APM server machine, open a terminal command line and launch **/opt/HP/BSM/bin/config-server-wizard.sh**
11. Restart all APM servers.

After you have installed all additional servers, restart all other APM servers and data collectors to allow them to recognize the new servers.

SiteScope Post-Upgrade Procedure

For SiteScope versions lower than 11.33, after performing a staging upgrade, you need to configure SiteScope to communicate with the new APM Gateway Servers.

Integrate SiteScope and APM 9.50

To integrate SiteScope and APM 9.50, after upgrading to APM 9.50, perform the following procedure.

On the APM 9.50 server:

1. Access the UCMDB JMX server (**https://localhost:8443/jmx-console/HtmlAdaptor?action=inspectMBean&name=UCMDB:service=Packaging Services**).
2. From the Operations index, click **undeployPackages**.
3. In the packageNames Value field, type **sitescope.zip**.
4. Click **Invoke**.
5. From the Operations index, click **deployPackages**.
6. In the packageNames Value field, type **sitescope.zip**.
7. Click **Invoke**.

On the SiteScope server:

8. Stop SiteScope.
9. Copy the jar files and **SiSAPM940PostUpgradeUtil** files from **…/BSM/9.40/content/HPE_ APM_9.40_ SiS_Upgrade** and save them in **<SiteScope root dir>/bin**.

10. For SiteScope installed on Windows, run the **SiSAPM940PostUpgradeUtil.bat** file.

    For SiteScope installed on Linux, run the **SiSAPM940PostUpgradeUtil.sh** file.

Change the Gateway Server to which SiteScope sends data

After performing a APM staging upgrade, you need to configure SiteScope to communicate with the new APM Gateway Servers. To do so, perform one of the following:

- In SiteScope's BSM Integration Preferences, enter the new Gateway Server name or IP address in the **Business Service Management machine name/IP address** box. For user interface details, see BSM Integration Preferences Dialog Box in the Using SiteScope Guide in the SiteScope Help.
- In SAM Administration, update the SiteScope settings with the new Gateway Server name in **Distributed Settings**. For user interface details, see New/Edit SiteScope Page in the APM Application Administration Guide in the APM Help.

  NOTE:
  This can only be used for changing the Gateway Server for a SiteScope that is already registered with a given APM installation. It cannot be used to add a new SiteScope, or to connect a SiteScope to a different APM system.

Diagnostics Post-Upgrade Procedure

In previous releases of APM, Diagnostics sent CIs, metrics, and events to APM. Health Indicator status (coloring) for the Application Infrastructure CIs was based on events sent to APM through the OBM event channel.

In APM 9.40, due to the OBM removal, Diagnostics sends events to OBM and continues to send CIs and metrics to APM. As a result of this change, the Application Infrastructure CIs (Diagnostic Probe, IBM WebSphere MQ, WebSphere AS Dynamic Caching, IBM MQ, WebLogic AS, JBOSS AS, SQL Server, MSSQL Database, Oracle iAS, Oracle, SAP, SAP R3 Server, VMware ESX Server, Host Node) do not show the correct HI Status in APM 9.40.

The HI status for these CIs appears as *Undetermined* (blue question mark). If you are upgrading from APM 9.40, the last status received for the CI before the upgrade will be displayed.

Use the workaround below to view the HI status of these CIs in OBM.

Workaround:

To enable sending events related to threshold violation in Diagnostics to OBM, in the server\bin directory of the Diagnostics server:

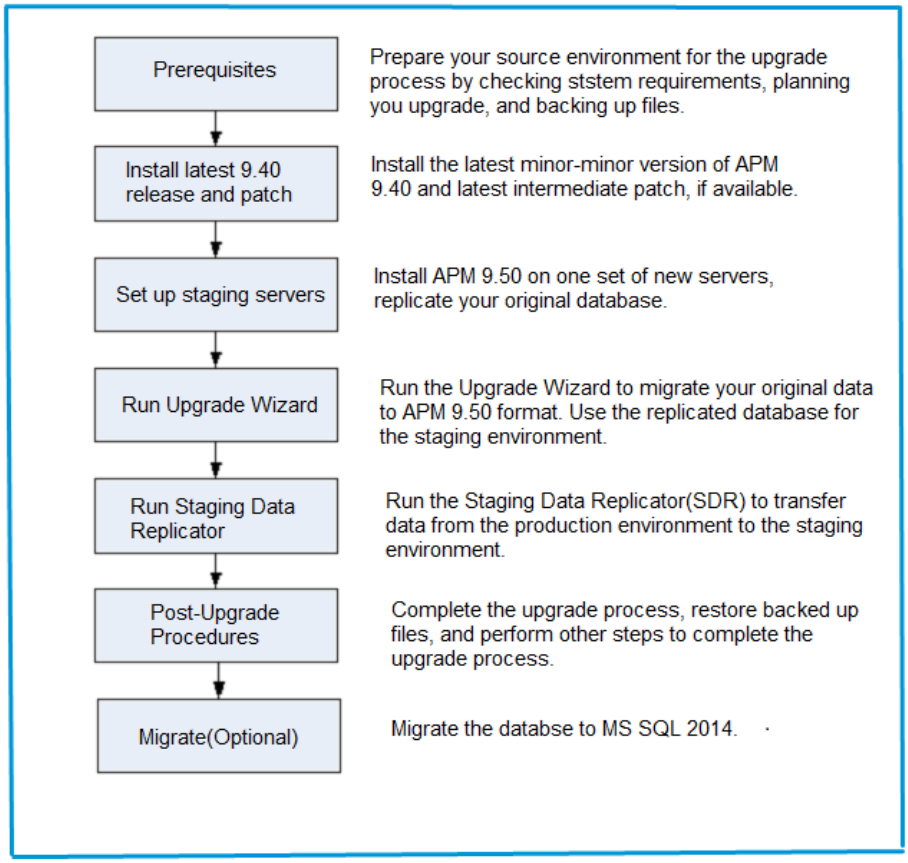
1. Run **cscript switch_ovo_agent.vbs -server <FQDN of OBM> -cert_srv <FQDN of OBM>**.
2. Go to **OBM Administration > Certificate Requests** and grant certificates.

3. Run **cscript switch_ovo_agent.vbs -server <FQDN of OBM> -cert_srv <FQDN of OBM>** again.
   All tasks should now display correctly.

Part 2: Staging Upgrade

Chapter 7: Overview of APM 9.40 to APM 9.50 Staging Upgrade

The upgrade from APM 9.40 to APM 9.50 involves a number of milestones. The following diagram shows the major steps and how they affect your environment.



Chapter 8: Prerequisites

Perform all steps specified in this chapter before continuing with the upgrade process.

General Prerequisites

Perform the following steps where relevant before continuing with the upgrade process.

1. ## Create deployment plan

   Create a complete deployment plan including the required software, hardware, and components. For details, see the APM Getting Started Guide and the APM System Requirements and Support Matrixes.

2. ## Create upgrade plan

   Create an upgrade plan, including such items as whether you will be performing a staging or direct upgrade, estimated down time, and so on.

   Allocate additional disk space. The database replication requires 1.5 times the amount of disk space in your original (production) database. If you want to save original data by selecting this option in the upgrade wizard, you will need two times the amount of disk space in your original database.

   Staging Data Replicator. If you need to run the Staging Data Replicator (SDR) on an external server, you will need an additional server to run the SDR during staging mode. For more information, see Staging Data Replicator, on page 53.

   Database Administrator. During the upgrade process, the services of your Database Administrator may be required.

   Multiple servers. If you are upgrading multiple APM servers, perform the upgrade procedure on only one Gateway and one Data Processing server. When the upgrade process is complete, install any additional servers and connect them to the database schemas using Configuration Wizard as described in the APM Installation Guide.

3. Order and register licenses

Order licenses with a sales representative based on your deployment plan. Register your copy of APM to gain access to technical support and information on all products. You will also be eligible for updates and upgrades. You can register your copy of APM on the Support site https://softwaresupport.softwaregrp.com.

4. Set up database server

NOTE:
You cannot change the database type during the upgrade if you want to keep your configuration and runtime data. For example, if you currently run Oracle, you must also use Oracle with the new APM environment.

Verify that your database has the following settings:

- Oracle: The Oracle Partitioning option must be enabled. Make sure that the parameter **RECYCLEBIN** is set to **Off**, as specified in the APM Database Guide.
- SQL: If you are upgrading with a staging environment, the collation must be identical in both the production and staging environments.

For information about setting up your database server, see the APM Database Guide.

5. Migrate operating systems (optional)

- APM supports switching the operating systems of your Gateway and Data Processing servers if you are upgrading in staging mode (for example, from Windows to Linux).
- APM supports switching the operating system of your database server during the upgrade (staging and direct) provided that this is also supported by your database vendor.

6. Set up web server (optional)

APM installs the Apache web server on all APM Gateway servers during the installation. If you would like to use the IIS web server, install it on all Gateway servers before installing APM .

7. Migrate manual changes to conf directory

If you made changes to any files in the **<HPBSM root directory>\WebServer\conf** directory, back up the changed files and, after the upgrade, reapply the changes to the new files (**do not copy the old files on top of the new ones**).

8. Back up database schema (recommended)

We recommend backing up database schemas as close as possible to the upgrade procedure.

9. ## Disable RTSM integrations (optional)

   If integrations are configured in the RTSM Integration Studio (for example, topology synchronization integrations between central UCMDB and RTSM), after upgrading, the Data Flow Probe will run population jobs immediately for active integration points, even if the integration is not scheduled. If you do not want the integration to run, disable the integration before running the upgrade .

10. ## Back up files

    Back up the following files from your original APM servers:

    - **<Gateway Server root directory>\AppServer\webapps\site.war\openapi\excels directory**
    - **<Data Processing Server root directory>\BLE\rules\<custom rules jar> file(s)**
    - **<Gateway Server root directory>\JRE\lib\security\cacerts**
    - **<Gateway Server root directory>\JRE64\lib\security\cacerts**
    - **<Data Processing Server root directory>\BLE\rules\groovy\rules\ file(s)**

11. Back up your license folder.

    - **On Windows:** C:\HPBSM\conf\license
    - **On Linux:** /opt/HP/BSM/conf/license

12. ## Copy customized Java database connectivity properties (jdbc) - Oracle RAC (optional)

    When upgrading, the custom modifications you made in the **jdbc.drivers.properties** file are overwritten. If you configured APM with an Oracle RAC database, and if you have custom modifications in the jdbc.drivers.properties file:

    Create a new file in **<HOME_APM >/conf** called **jdbc.drivers.extension<number>.<name>.properties** and copy only the custom properties from jdbc.drivers.properties to this file before performing the upgrade.

    For example, before upgrading, copy this string: **ddoracle.url=jdbc:mercury:oracle:TNSNamesFile=<HOME_APM>\\conf\\bac-tnsnames.ora;TNSServerName=${sid}** from the **jdbc.drivers.properties** file to the **<HOME_APM>/conf/jdbc.drivers.extension1.RAC.properties** file.

    After upgrading, the **jdbc.drivers.extension1.RAC.properties** file is not overwritten so all the custom properties are saved.

    If there are multiple custom files in the **<HOME_APM >/conf/** directory with the same property name, APM uses the one with the latest extension number.

13. Delete MyBSM pages with OBM components

After upgrading to APM, MyBSM pages with OBM components will be blank due to the removal of OBM from APM. Therefore, before upgrading to APM, you should delete the entire page or remove the OBM components.

14. Disable APM-OBM integration

If OBM Integration is enabled, disable it by clearing the OBM URL before upgrading.

a. Check whether the OBM integration is enabled in the JBoss JMX console:

OMi-Integration > OMi-Integration:service=Settings > boolean isIntegrationEnabled for customer 1

b. If the OBM integration is enabled:

i. Issue **DELETE REST** call to URL: **http://<APM_HOST>/topaz/omi/integration/customer/1/settings/url** to delete the OBM URL setting.

ii. In APM, locate the names of the CI Status Alerts that need to be deleted:

Admin > Platform > Infrastructure Settings > Foundations > OMi Integration > OMi Integration - Statuses Synchronization

iii. In APM, select **Admin > Service Health > CI Status Alerts** and locate and delete the required alerts.

iv. On the OBM side, delete the APM Connected Server:

OMi > Administration > Setup and Maintenance > Connected Servers

NOTE:
After completing the upgrade, you will need to perform the integration again. See the OBM Integration Guide for instructions.

Installation Prerequisites - Windows

Note the following before installing APM servers on a Windows platform:

- It is recommended that you install APM servers to a drive with at least 40 GB of free disk space. For more details on server system requirements, see the APM System Requirements and Support Matrixes.
- If APM servers, including the database servers, are installed on multiple network segments, it is highly recommended that the number of hops and the latency between the servers be minimal. Network-induced latency may cause adverse affects to the APM application and can result in performance and stability issues. We recommend the network latency should be no more than 5 milliseconds, regardless of the number of hops. For more information, contact Support.

- APM servers must be installed on dedicated machines and must not run other applications. Certain APM components can coexist on APM servers. For details on coexistence support, see the APM System Requirements and Support Matrixes.
- If you plan to use the IIS web server, install it prior to APM installation and enable it after the installation is completed. For more information, see Working with the IIS Web Server, on page 73.
- APM servers must not be installed on a drive that is mapped to a local or network resource.
- Due to certain web browser limitations, the names of server machines running the Gateway Server must consist only of alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and periods (.). For example, if the names of the machines running the Gateway Server contain underscores, it may not be possible to log into the APM site when using Microsoft Internet Explorer 7.0 or later.
- During APM server installation, you can specify a different path for the APM directory (default is **C:\HPBSM**), but note that the full path to the directory must not contain spaces, cannot contain more than 15 characters, and should end with **BSM**.
- The installation directory name should consist of only alphanumeric characters (a-z, A-Z, 2-9).

  NOTE:
  You cannot use 0 or 1 in the installation directory name

- User Access Control (UAC) must be disabled before installing APM. UAC is enabled by default in some version of Windows Server. To manually disable UAC run the following command:

  C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f

  C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v ConsentPromptBehaviorAdmin /t REG_DWORD /d 0 /f
- If you plan to run APM servers on a hardened platform (including using HTTPS protocol), review the hardening procedures described in the APM Hardening Guide.
- If you do not have a profile database on your source environment, please add one before starting the upgrade. The database should be marked as the default profile database. Most users already have a profile database.
- You must have administrator privileges to install APM on the server machine.
- In the APM cluster, open port 21212 on the Data Processing Server.

NOTE:
During installation, the value of the Windows Registry key HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ReservedPorts is updated to include the following port ranges required by APM: 1098-1099, 2506-2507, 8009-8009, 29000-29000, 4444-4444, 8083-8083, 8093-8093.

These port ranges are not removed from the registry key at APM uninstall. You should remove the ports from the registry key manually after uninstalling APM if they are no longer needed by any other application.

Installation Prerequisites - Linux

Note the following before installing APM servers on a Linux platform:

- It is recommended that you install APM servers to a drive with at least 40 GB of free disk space. The /tmp directory should have at least 2.5 GB of free disk space. You can change the /tmp directory by running the following command:

  ```
  export IATEMPDIR=/new/tmp/dir
  ```

  ```
  export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp/dir
  ```

  where `/new/tmp/dir` is the new /tmp directory

  For more details on server system requirements, see the APM System Requirements and Support Matrixes.
- If APM servers, including the database servers, are installed on multiple network segments, it is highly recommended that the number of hops and the latency between the servers be minimal. Network-induced latency may cause adverse affects to the APM application and can result in performance and stability issues. We recommend the network latency should be no more than 5 milliseconds, regardless of the number of hops. For more information, contact Support.
- APM servers must be installed on dedicated machines and must not run other applications. Certain APM components can coexist on APM servers. For details on coexistence support, see the the APM System Requirements and Support Matrixes.
- Before installing APM on a Linux machine, make sure that SELinux does not block it. You can do this by either disabling SELinux, or configuring it to enable java 32-bit to run.

  To disable SELinux, open the **/etc/selinux/config** file, set the value of **SELINUX=disabled**, and reboot the machine.

  On systems with SELinux disabled, the `SELINUX=disabled` option is configured in **/etc/selinux/config**:

  ```
  # This file controls the state of SELinux on the system.
  # SELINUX= can take one of these three values:
  #       enforcing - SELinux security policy is enforced.
  ```

```
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Also, the `getenforce` command returns **Disabled**:

```
~]$ getenforce
Disabled
```

To confirm that the aforementioned packages are installed, use the rpm utility:

```
~]$ rpm -qa | grep selinux
selinux-policy-3.12.1-136.el7.noarch
libselinux-2.2.2-4.el7.x86_64
selinux-policy-targeted-3.12.1-136.el7.noarch
libselinux-utils-2.2.2-4.el7.x86_64
libselinux-python-2.2.2-4.el7.x86_64
```

```
~]$ rpm -qa | grep policycoreutils
policycoreutils-2.2.5-6.el7.x86_64
policycoreutils-python-2.2.5-6.el7.x86_64
```

```
~]$ rpm -qa | grep setroubleshoot
setroubleshoot-server-3.2.17-2.el7.x86_64
setroubleshoot-3.2.17-2.el7.x86_64
setroubleshoot-plugins-3.0.58-2.el7.noarch
```

Before SELinux is enabled, each file on the file system must be labeled with an SELinux context. Before this happens, confined domains may be denied access, preventing your system from booting correctly.

To prevent this, configure `SELINUX=permissive` in the **/etc/selinux/config file**:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

As a root user, restart the system. During the next boot, file systems are labeled. The label process labels all files with an SELinux context:

```
~]# reboot
```

In permissive mode, SELinux policy is not enforced, but denials are logged for actions that would have been denied if running in enforcing mode.

Before changing to enforcing mode, as a root user, run the following command to confirm that SELinux did not deny actions during the last boot. If SELinux did not deny actions during the last boot, this command does not return any output.

```
~]# grep "SELinux is preventing" /var/log/messages
```

If there were no denial messages in the **/var/log/messages** file, configure `SELINUX=enforcing` in **/etc/selinux/config**:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#       targeted - Targeted processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Reboot your system. After reboot, confirm that `getenforce` returns **Enforcing**:

```
~]$ getenforce
Enforcing
```

```
~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
```

- To configure SELinux to enable java 32-bit to run, execute the command **setsebool –P allow_ execmod on**.
- APM servers must not be installed on a drive that is mapped to a network resource.
- Due to certain Web browser limitations, the names of server machines running the Gateway Server must only consist of alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and periods (.). For example, if the names of the machines running the Gateway Server contain underscores, it may not be possible to log in to the APM site. To access the APM site in this case, use the machine's IP address instead of the machine name containing the underscore.
- If you plan to run APM servers on a hardened platform (including using HTTPS protocol), review the

hardening procedures described in the APM Hardening Guide.

- You must be a root user to install APM on the server machine.
- The **DISPLAY** environment variable must be properly configured on the APM server machine. The machine from which you are installing must be running an X-Server as the upgrade process cannot be performed silently.
- If you do not have a profile database on your source environment, please add one before starting the upgrade. The database should be marked as the default profile database. Most users already have a profile database.
- In the APM cluster, open port 21212 on the Data Processing Server.
- To install APM 9.50 on Oracle Linux (OEL) or Red Hat Enterprise Linux operating systems supported 6.x and 7.x versions, the following RPM packages must be installed in the machine:

◦ glibc	◦ libXext
◦ glibc-common	◦ libXtst
◦ nss-softokn-freebl	◦ compat-libstdc++-33
◦ libXau	◦ libXrender
◦ libxcb	◦ libgcc
◦ libX11	◦ openssl1.0.2g
	◦ rpm-devel

The installer attempts to install or update these packages.

If the installation of one of the above packages fails:

1. Click **Cancel** to stop the installation.
2. Refer the problem to your system administrator.
3. When the problematic package is fixed, re-run the installation

NOTE:
If the installer fails to install **compat-libstdc++-33**, manually download the following RPM packages:

- **compat-libstdc++-33.i686**
- **compat-libstdc++-33.x86_64**

If the Yum Linux upgrade service is not functional on your machine, you will need to download and install the necessary RPM packages manually by running the following command:

yum install -y openssl1.0.2g glibc.i686 glibc-common.i686 nss-softokn-freebl.i686 libXau.i686 libxcb.i686 libX11.i686 libXext.i686 libXtst.i686 compat-libstdc++-33.i686 libXrender.i686 libgcc.i686 rpm-devel

NOTE:
The version of these packages changes from system to system. You can download the packages from any RPM repository site that matches your system specifications. The following RPM search tool can assist you in this task (http://rpm.pbone.net/).

To determine the package version you need to download:

- Run the following command in a terminal window:

  rpm –qa ${PACKAGE_NAME} (ex: rpm -qa glibc)

  The command will return the following text:

  ```
  # rpm -qa glibc

  glibc-2.12-1.132.el6.x86_64
  ```

  This text indicates the package version required for your machine.

  For example, in this case you would need to download the i686 architecture package with the same version - glibc-2.12-1.132.el6.i686 – and install it manually.

Chapter 9: Set Up Staging Servers

Perform all steps specified in this chapter to set up the staging servers.

Install APM 9.50

Install APM 9.50 on a set of APM servers. This set can be either one Gateway Server and one Data Processing Server or a single one-machine server. In the first case, run the wizards on the Data Processing Server first. The wizard will direct you as to when to begin installation on the Gateway Server.

NOTE:

- Do not install additional servers at this time, you can install them towards the end of the workflow.
- You must install APM using a user with root (Linux) or administrative privileges (Windows). If necessary in case Windows OS, switch the user which has administrative privileges that is being used to install and enable APM.
- Run the installation and post-installation wizards. Do not run the upgrade wizard yet. Exit the wizard on the last screen of the post-installation wizard without continuing.

Download the software

1. Go to the Software Support web site (https://softwaresupport.softwaregrp.com) and sign in using your Passport.
2. Click **Product Information > Downloads**.
3. Click **Select an SAID** and select **application performance management (bac)** from the Products list.

   or

   Click **Directly enter an SAID** and enter your SAID.
4. Accept the terms and conditions.
5. Click **View available products**.

6. In the Show a single category/product center drop down list, select **Application Performance Management**.
7. Select **Application Performance Managemen version 9.50** in the language you require (for example, Application Performance Management version 9.50 English Software E-Media).
8. Click **Get software updates**.
9. Click **Get Software** for your selected product.
10. Confirm that your product is selected in the Product name field.
11. From the Downloads field, select the required download:
    - **Application Performance Managemen 9.50 Windows Setup (APM_9.50_Windows_Setup.zip)**
    - **Application Performance Managemen 9.50 Linux Setup (APM_9.50_Linux_Setup.zip)**
12. Click **Download**.
13. Unzip the file and run the installation program.

Run Installation and Post Installation Wizards

- Installing APM on a Windows Platform, on page 72
- Installing APM on a Linux Platform, on page 81
- Installing APM Silently, on page 85

If there is a patch available, Go to the Software Support web site (https://softwaresupport.softwaregrp.com) and download the required patch.

Alternatively, you may run the Installation and Post-Installation wizards in silent mode. However, silent mode is not supported for the Upgrade Wizards. For details, see Installing APM Silently.

Replicate Database

Replicate the following original databases onto a new database server. The new database will be used by the staging environment, upgraded, and eventually used as your APM 9.50 database.

- Management DB (schema)
- RTSM DB (schema)
- Profile DB (schema) (If there is more than one profile database, replicate all of them)
- Analytics DB (schema) (If present and if there is more than one analytics database, replicate all of them)

  NOTE:
  The Event and BPI schemas are no longer used for APM .

Make sure that your database version is supported in both the original APM and new APM environments.

Migrate Database to MS SQL 2012 and MS SQL 2014 (optional)

If you would like to use either MS SQL 2012 or MS SQL 2014, migrate your database to a new MS SQL 2012 or MS SQL 2014 database. For details, see the MS SQL documentation.

Chapter 10: Run 9.50 Upgrade Wizard

You should only have one set of 9.50 servers installed at this time. Do not run the Upgrade Wizard on more than one set of 9.50 servers.

You can launch the Upgrade Wizard from the Post-Install Wizard by choosing the following option:

- Upgrade. Continue with the upgrade from APM 9.40 with latest intermediate patch

If you can choose **Exit. Complete the upgrade or installation process at a later time.** you will need to run the Upgrade Wizard manually.

The upgrade wizard can be found on all Gateway, Data Processing, and One-machine servers in the following locations:

- **Windows:**
  - If you want to upgrade from 9.30 to 9.50 version, select the upgrade wizard from the following location:

  <HPE APM root directory>\bin\upgrade_wizard_run_from930.bat
  - If you want to upgrade from 9.40 to 9.50 version, select the upgrade wizard from the following location:

  <HPE APM root directory>\bin\upgrade_wizard_run_from940.bat
- **Linux:**
  - If you want to upgrade from 9.30 to 9.50 version, select the upgrade wizard from the following location:

  /opt/HP/BSM/bin/upgrade_wizard_run_from930.sh
  - If you want to upgrade from 9.40 to 9.50 version, select the upgrade wizard from the following location:

  /opt/HP/BSM/bin/upgrade_wizard_run_from940.sh

For details about the upgrade wizard, see Upgrade Wizard, on page 88.

Chapter 11: Staging Data Replicator

Staging Data Replicator - Overview

The Staging Data Replicator (SDR) is a tool that transfers data from the production environment to the staging environment during staging mode. The purpose of this tool is to create a window of time in which the same data can be viewed in both environments, allowing you to verify functionality and configuration settings in the staging environment.

While the SDR is running, any configuration changes made to the original APM servers are not transferred to the staging servers. Only data samples are transferred. The SDR does not transfer event data.

Samples related to new configurations performed on the source environment may not be transferred by the SDR. To view the samples that were not transferred, view the ignored samples log at **log\sdreplicator\sdrIgnoredSamples.log** and the general SDR log at **log\sdreplicator\sdreplicator_all.log.**

You can change the log level of these files through the following file:

Embedded SDR: **<HPE APM>\SDR\conf\core\Tools\log4j\sdreplicator\sdreplicator.properties**

Standalone SDR: **HPBSMSDR\conf\core\Tools\log4j\sdreplicator\sdreplicator.properties**

This tool is only supported in staging mode. For more information about staging mode, see Staging vs. Direct Upgrade Overview, on page 9.

In Linux, you can change the installer working directory (default /tmp) by running the following commands:

```
export IATEMPDIR=/new/tmp/dir
```

```
export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp/directory
```

where `/new/temp` is the new /temp directory.

The SDR must be installed on a machine in the same network as the production environment, with the ability to access the staging environment. If the staging server cannot communicate with the production server, the SDR must be installed as a standalone utility on a different machine.

For task details, see Running the Staging Data Replicator (Standalone), on the next page.

SDR Set up

Perform the following steps to Set up SDR manually.

1. Stop the SDR process. For details, see Unsubscribing the Staging Data Replicator from the Source Server, on page 58.
2. Take a backup of the following files:
   a. **<HP_BSM_SDR_Home>\conf\encryption.properties**
   b. **<HP_BSM_SDR_Home>\conf\jmxsecurity.txt**
   c. **<HP_BSM_SDR_Home>\conf\seed.properties**
   d. **<HP_BSM_SDR_Home>\conf\legacy.properties**
   e. **<HP_BSM_SDR_Home>\JRE\lib\security\java.security**
   f. **<HP_BSM_SDR_Home>\lib\sdr_javacore.jar**
   g. **<HP_BSM_SDR_Home>\JRE\lib\security\local_policy.jar**
   h. **<HP_BSM_SDR_Home>\JRE\lib\security\README.TXT**
   i. **<HP_BSM_SDR_Home>\JRE\lib\security\US_export_policy.jar**
3. Copy the following files from BSM Gateway installation directory to the SDR installation directory:
   a. **<HPBSM_Gateway_Home>\conf\encryption.properties to <HP_BSM_SDR_Home>\conf**
   b. **<HPBSM_Gateway_Home>\conf\jmxsecurity.txt to <HP_BSM_SDR_Home>\conf**
   c. **<HPBSM_Gateway_Home>\conf\seed.properties to <HP_BSM_SDR_Home>\conf**
   d. **<HPBSM_Gateway_Home>\conf\legacy.properties to <HP_BSM_SDR_Home>\conf**
   e. **<HPBSM_Gateway_Home>\JRE\lib\security\java.security to <HP_BSM_SDR_Home>\JRE\lib\security**
4. Download Unlimited Strength Jurisdiction JCE zip files (**UnlimitedJCEPolicyJDK7.zip**) from http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html after accepting license, and save at **java\lib\security** for JDK 7.
5. Unzip **UnlimitedJCEPolicyJDK7.zip** and save UnlimitedJCEPolicy file at **<HP_BSM_SDR_Home>\JRE\lib\security**. Overwrite the existing file versions.
6. Start the SDR process. For details, see Unsubscribing the Staging Data Replicator from the Source Server, on page 58

Running the Staging Data Replicator (Embedded)

The SDR typically runs embedded in the staging server as part of the upgrade wizard. However, it can also be run as a standalone utility on a different server. For details, see Running the Staging Data Replicator (Standalone), below.

NOTE:
The SDR must be installed on a machine in the same network as the production environment, with the ability to access the staging environment. If the staging server cannot communicate with the production server, the SDR must be installed as a standalone utility on a different machine. For details, see Running the Staging Data Replicator (Standalone), below.

To run the SDR (embedded)

1. If the staging server uses basic authentication, the SDR cannot communicate with the staging server unless you run the **basicauth** tool. For details, see Running the SDR with Basic Authentication, on page 59.
2. If the staging server uses SSL, you will need to perform custom configurations to allow the SDR to communicate with the staging server. For details, see SSL Configuration for the Staging Data Replicator, on page 60.
3. Verify that the SDR embedded in the staging server can communicate with the production server. For details, see Verifying that the SDR Server Can Communicate with the Production Server, on page 58.
4. If upgrading from APM 9.40, copy the following configuration files from the source (production) APM Gateway Server to the staging APM **<APM Staging Gateway Server root directory>\SDR\conf**. Do this before running the Upgrade Wizard.
   - **<APM Source Gateway Server root directory>\conf\encryption.properties**
   - **<APM Source Gateway Server root directory>\conf\seed.properties**
   - **<APM Source Gateway Server root directory>\conf\TopazInfra.ini**
5. After you have completed the staging process and are prepared to move your staging environment to a production environment, stop the SDR by rerunning the upgrade wizard and selecting the appropriate option to stop the SDR.
6. Unsubscribe the staging data replicator from the source server. For details, see Unsubscribing the Staging Data Replicator from the Source Server, on page 58.

Running the Staging Data Replicator (Standalone)

To use the Staging Data Replicator standalone utility:

1. To use the Staging Data Replicator as a standalone utility, you must install it on a separate machine with access to both your production and staging servers.
   - To check that the SDR server can connect to the staging server, enter the following url in an any internet browser from the standalone server:

     http://<_DESTINATION_>/ext/mod_mdrv_wrap.dll?type=test

     Where **_DESTINATION_** is the FQDN name of the Gateway Server or Load Balancer, depending on your configuration.
   - Check that the SDR server can connect to the production server. For details, see Verifying that the SDR Server Can Communicate with the Production Server, on page 58.
2. Run the appropriate replicator file.
   a. Go to the Software Support web site (https://softwaresupport.softwaregrp.com) and sign in.
   b. Click **Search**.
   c. For Windows, select **Application Performance Management (BAC) > 9.50 > Windows**.

      For Linux, select **Application Performance Management (BAC) > 9.50 > Linux**.
   d. Under Document Type, select **Patches**.
   e. Locate the Staging Data Replicator package and save it locally.
   f. Launch the relevant setup file.
3. Follow the on-screen instructions to install the Staging Data Replicator. Select the type of deployment based on the version of your source environment.
4. After you have completed the Staging Data Replicator installation, open the **<Staging Data Replicator root directory>\conf\b2G_translator.xml** file and modify the following:
   - **_SOURCE_HOST_NAME_.** Replace this with the FQDN host name of the source (production) APM Gateway Server. If you have more than one Gateway Server, you can use the name of any of them for this value.
   - **_DESTINATION_HOST_NAME_.** Replace this with the FQDN host name of the destination (staging) APM Gateway Server or Load Balancer, depending on your configuration. This string appears twice within this file in the following line:

     <ForwardURL url="http://__DESTINATION_HOST_NAME__/ext/mod_mdrv_wrap.dll?type=md_sample_array&acceptor_name=__DESTINATION_HOST_NAME__&message_subject=topaz_report/samples&request_timeout=30&force_keep_alive=true&send_gd=true"/>
   - **clientid="".** If you do not require guaranteed delivery of data when the Staging Data Replicator stops running, delete the value for this parameter. It is generally recommended that you do not modify this parameter.
5. If upgrading from APM 9.40, copy the following configuration files from the source (production) APM Gateway Server to the Staging Data Replicator **<Staging Data Replicator root**

directory>\SDR\conf:

- **<APM Source Gateway Server root directory>\conf\encryption.properties**
- **<APM Source Gateway Server root directory>\conf\seed.properties**
- **<APM Source Gateway Server root directory>\conf\TopazInfra.ini**

6. If the web server on the staging server uses basic authentication, the SDR cannot communicate with the staging server unless you run the **basicauth** tool. For details, see Running the SDR with Basic Authentication, on page 59.
7. If the web server on the staging server uses SSL, you will need to perform custom configurations to allow the SDR to communicate with the staging server. For details, see SSL Configuration for the Staging Data Replicator, on page 60.
8. Begin running the Staging Data Replicator.
   - Windows: Select **Start > APM Staging Data Replicator > Administration > Enable APM Staging Data Replicator**.

     Verify that the SDR is running by looking for **hpbsmsdr** in the Windows Task Manager.
   - Linux: Run the following command:
     <SDR root directory>/scripts/run_hpbsmsdr.sh start

     Verify that the SDR is running searching for the hpbsmsdr process (for example: **ps -ef | grep hpbsmsdr**)
9. After starting the SDR, copy the **<SDR root directory>/dat/sdr/SDRBusConnectionStartTime.properties** file from the SDR server to the staging Gateway server in the **<HPE APM root directory>/dat/sdr** directory and continue running the Upgrade Wizard.
10. After you have completed the staging process and are prepared to move your staging environment to a production environment, stop the Staging Data Replicator.
    - Windows: Select **Start > APM Staging Data Replicator > Administration > Disable APM Staging Data Replicator**.
    - Linux: Run the following command:
      <SDR root directory>/scripts/run_hpbsmsdr.sh stop
11. Unsubscribe the staging data replicator from the source server. For details, see Unsubscribing the Staging Data Replicator from the Source Server, on the next page.

Verifying that the SDR Server Can Communicate with the Production Server

1. Ping the production server.
   a. Ping the production Gateway Server from the SDR server using the Gateway Server's short name. If this works, continue to step 2. If it does not work, continue with step 1 b.
   b. Ping the production Gateway Server from the SDR server using the Gateway Server's fully qualified domain name (FQDN). If this works, open the relevant **hosts** file for your operating system and add the mapping between the production Gateway Server name and its IP address.
2. Verify connection.
   a. **Production Gateway Server runs Windows:** Run **ipconfig** on the production Gateway Server.

      Production Gateway Server runs Linux: Run **ifconfig -a** on the production Gateway Server.
   b. Verify all the listed IP addresses are open to connection to and from the server running the SDR.

      If this is not feasible, contact Support.
   c. Verify that the ports 1098, 1099, 2506, and 2507 are open on the SDR server.

Unsubscribing the Staging Data Replicator from the Source Server

This procedure unsubscribes the SDR from the source server's bus, preventing data from accumulating in the source server. It is performed after you have completed the staging process and disabled the SDR.

NOTE:
You do not have to perform this procedure if you are immediately uninstalling the previous version of APM from the source server.

To unsubscribe the SDR:

1. Stop the SDR.
   a. Open the Nanny Manager jmx console from **http://<FQDN machine name>:11021**, where **<machine name>** for an embedded SDR is the name of the Load Balancer (if it exists) or destination APM Gateway Server. For a Standalone SDR, **<machine name>** is **localhost**.

b. Select **Foundations: type=NannyManager**

c. Open **showServiceInfoAsHTML**

d. Stop the **HPBSMSDR-x.x** process.

2. Open the **<Staging Data Replicator root directory>\conf\b2G_translator.xml** file and locate the <Message Selector> element(s).
3. Within the **<Message Selector>** element(s), replace the attribute value of enabled to 0 (the default is **enabled="1"**) in the following line:

   <MessageSelector name="customer_name" value="Default Client" enabled="0" />
4. Start the SDR.

   a. Open the Nanny Manager jmx console from **http://<FQDN machine name>:11021**, where **<machine name>** for an embedded SDR is the name of the Load Balancer (if it exists) or destination APM Gateway Server. For a Standalone SDR, **<machine name>** is **localhost**.

   b. Select **Foundations: type=NannyManager**

   c. Open **showServiceInfoAsHTML**

   d. Start the **HPBSMSDR-x.x** process.
5. Wait several minutes, and then stop the SDR as described in step 1.

Running the SDR with Basic Authentication

If the staging server is using basic authentication, the SDR cannot communicate with the staging server without a user name and password. The **basicauth** tool allows you to enter this data into the APM in an encrypted format, thereby enabling the SDR to communicate with servers that use basic authentication.

To configure SDR to work with basic authentication:

From the command prompt, run the **basicauth** file using the following syntax:

<Staging Data Replicator root directory>\bin\basicauth [-embedded | -standalone] [enabled username password | disabled]

Where:

-embedded is for an SDR that is embedded in the destination environment.

-standalone is for a standalone SDR

enabled is to enable basic authentication. Specify a valid username and password. This tool encrypts the password before it is saved in the configuration file.

disabled is to disable basic authentication.

SSL Configuration for the Staging Data Replicator

If the staging server uses SSL, you need to perform the following procedure to allow the SDR to communicate with the staging server.

To configure the SDR to support SSL:

1. Configure SDR to use SSL.

   In the **<SDR root directory>\conf\b2g_translator.xml** file, locate ForwardURL and change **http** to **https**.

2. Configure the SDR to trust the APM certificate.

   a. Obtain a copy of the certificate used by the web server on the APM Gateway Server or certificate of Certificate Authority that issued APM web server certificate. This file must be a DER encoded binary X.509 (.CER) file.

   b. Import the above-mentioned certificate into SDR's truststore. For details, see the APM Hardening Guide.

      Default truststore for SDR is **<SDR root directory>\JRE\lib\security\cacerts**.

      Example:

      <SDR root directory>\JRE\bin>keytool -import -trustcacerts -alias <your CA certificate alias name> -keystore ..\lib\security\cacerts -file <CA certificate file>

   c. If you are not using the default truststore with SDR, configure the SDR to use a non-default truststore, and add additional options in the file **<SDR root directory>\bin\sdreplicator_run.bat**, as follows:

      Locate the following line:

      ```
      SET PROCESS_OPTS=%PROCESS_OPTS% -Dconf.file=%PRODUCT_HOME_PATH%\conf\b2g_
      translator.xml -Dprop.file=%PRODUCT_HOME_PATH%\conf\b2g_
      translator.properties -Dmsg.filter.file=%PRODUCT_HOME_
      PATH%\conf\includedSamples
      ```

      At the end of this line, add the following:

      ```
      -Dnet.ssl.trustStore=<keystore path>

      -Dnet.ssl.trustStorePassword=passphrase
      ```

Chapter 12: Post-Upgrade Procedures

Perform these tasks to complete the upgrade process:

General Post-Upgrade Procedures

Perform these tasks to complete the upgrade process:

Upgrading Customized Service Health KPIs

In APM, the internal format of the KPI parameter “KPI is critical if” was changed. As a result, this value may be incorrect following upgrade, if you have created or customized KPIs.

NOTE:
APM must be running to perform this step.

To fix this, perform the following:

1. Access the JMX console on the Gateway Server via http://<Gateway Server name>:29000/ and enter your user name and password.
2. Click **service=repositories_manager** in the Topaz section.
3. Locate the **upgradeCriticalIf()** and input **1** as the customer ID in the parameter field.
4. Click **Invoke**.

Delete temporary internet files

When logging into APM for the first time after upgrading, delete the browser's temporary Internet files. This should be done on each browser that accesses APM.

Disable firewall between APM Gateway and Data Processing servers

In general, placing firewalls between APM servers is not supported. If an operating system firewall is active on any APM server machine (GW or DPS), a channel must be left open to allow all traffic

between all APM Gateway and DPS servers.

Additionally, to enable APM users and data collectors to communicate with the APM Gateway servers, you must leave open the relevant ports depending on your APM configuration. The required ports are typically 443 or 80. For details, see "Port Usage" in the APM Platform Administration Guide.

- ## Update Data Collectors

  See the System Requirements and Support Matrixes, available from **Help > Planning and Deployment** and the Updated Components section in the Business Service Management Release Notes to determine if you must upgrade your data collector to the latest supported version.

- ## Restore the following files from backup

  Restore the following files to the APM server:

  - <Gateway Server root directory>/AppServer/webapps/site.war/openapi/excels directory
  - <Data Processing Server root directory>/BLE/rules/<custom rules jar> file(s)
  - <Gateway Server root directory>/JRE/lib/security/cacerts
  - <Gateway Server root directory>/JRE64/lib/security/cacerts
  - <Data Processing Server root directory>\BLE\rules\groovy\rules\ file(s)

- ## Perform hardening procedures

  If your original environment was secured with SSL and you are upgrading using a staging environment, you need to repeat the hardening procedures described in the APM Hardening Guide.

  If your original environment was secured with SSL and you are upgrading directly, you need to repeat the following hardening procedures:

  1. If you had previously made changes to **<HPBSM root directory>\EJBContainer\server\mercury\deploy\jboss-web.deployer\server.xml** while performing hardening procedures on your system, repeat the “Securing JBOSS” procedure in the Hardening Guide after the patch installation on all relevant APM machines.
  2. If you had previously configured SSL on an IIS web server used by APM, you need to verify HTTPS port binding in IIS is set to the correct port (443).
  3. If you had previously configured SSL on the Apache web server used by APM, you may need to reapply the changes to httpd.conf and httpd-ssl.conf files as follows:
     - In **<HPE APM root directory>\WebServer\conf\httpd.conf**, uncomment the following two lines:

       LoadModule ssl_module modules/mod_ssl.so
       Include conf/extra/httpd-ssl.conf

- In **<HPE APM root directory>\WebServer\conf\extra\httpd-ssl.conf**, specify paths to **SSLCertificateFile** and **SSLCertificateKeyFile**
- Restart the APM Apache web service

Ensure all processes started properly

You can check to ensure that all processes started properly. For details, see "How to View the Status of Processes and Services" in the APM Platform Administration Guide.

Check installation log files

You can see the installation log file by clicking the **View log file** link at the bottom of the installer window.

In a Windows environment, this log file, along with additional log files for separate installation packages, is located in the **%temp%\..\MicroFocusOvInstaller\HPEApm_9.50** directory.

In a Linux environment, the logs files are located in the **/tmp/HPOvInstaller/HPEApm_<version>** directory.

The installer log file name is in the following format:

HPEApm_<VERSION>_<DATE>_ HPOvInstallerLog.html or **HPEApm_<VERSION>_ <DATE>_ HPOvInstallerLog.txt** (for example, HPEApm_9.50_2018.05.10_11_53_ MicroFocusOvInstallerLog.txt).

Individual installation package log file names are in the following format:

Package_<PACKAGE_TYPE>_HPEApm_<PACKAGE_NAME>_install.log (for example, Package_msi_HPEApm_BPMPkg_install.log).

NOTE:
If the server is rebooted, all files from the **tmp** folder are deleted automatically by default. Therefore, backup all log files after installing APM, before rebooting the server.

Restore APM service changes

If you manually configured different users to run APM services, these settings must be configured again. For details, see Changing APM Service Users , on page 90.

Install component setup files

The component setup files are used to install the components used by APM. The component setup files are not installed as part of the basic APM installation. They are located separately in the Web delivery package download area. You can upload them to the APM Downloads page. The component setup files can then be downloaded from APM and used when required. For details on

working with the APM Downloads page, see "Downloads" in the APM Platform Administration Guide.

NOTE:

- The components on the Downloads page are updated for each major and minor release (for example, 9.00 and 9.20). To download updated components for minor minor releases and patches (for example, 9.26), go to the Software Support site (https://softwaresupport.softwaregrp.com).
- You can install a component by using the component's setup file directly from the network. For details on installing a component, refer to the individual documentation for the component you want to install. The relevant documentation is available from the Downloads page in APM after the component's setup files are copied to the Downloads page.

To install component setup files, copy the component setup files that you want available in the Downloads page from the appropriate directory in the release download area to the **<HPE APM root directory>\AppServer\webapps\site.war\admin\install** directory on the APM Gateway server. If required, create the **admin\install** directory structure.

Starting and Stopping APM

After completing the APM server installation, clean your browser's cache and restart your computer. It is recommended that you do this as soon as possible. Note that when the machine restarts, you must log in as the same user under which you were logged in before restarting the machine.

NOTE:
If the server is rebooted, all files from **tmp** folder are deleted automatically by default. So backup all log files after installing APM, before rebooting the server.

After installing the APM servers (either together on one machine, or at least one instance of each server type in a distributed deployment) and connecting the server machines to the databases, you launch APM on each server machine.

NOTE:
You can check which APM servers and features are installed on an APM server machine by viewing the [INSTALLED_SERVERS] section of the **<HPE APM root directory>\conf\TopazSetup.ini** file. For example, Data_Processing_Server=1 indicates that the Data Processing Server is installed on the machine.

To start or stop APM in Windows:

Select **Start > All Programs > Micro Focus Application Performance Management > Administration > Enable | Disable Micro Focus Application Performance Management.** When enabling a distributed environment, first enable the Data Processing Server and then enable the Gateway Server.

To start or stop APM in Linux:

/opt/HP/BSM/scripts/run_hpbsm {start | stop | restart}

To start, stop, or restart APM using a daemon script:

/etc/init.d/hpbsmd {start| stop | restart}

NOTE:
When you stop APM, the APM service is not removed from Microsoft's Services window. The service is removed only after you uninstall APM.

Logging In and Out

You log in to APM from a client machine's browser using the login page. LW-SSO is APM's default authentication strategy. For details, see "Logging into APM with LW-SSO" in the APM Platform Administration Guide.

You can disable single sign-on authentication completely, or you can disable LW-SSO and use another supported authentication strategy. For details on selecting an authentication strategy, see "Set Up the Authentication Strategies" in the APM Platform Administration Guide.

To access the APM login page and log in for the first time:

1. In the Web browser, enter the URL http://<server_name>.<domain_name>/HPBSM where **server_name** and **domain_name** represent the FQDN of the APM server. If there are multiple servers, or if APM is deployed in a distributed architecture, specify the load balancer or Gateway Server URL, as required.

   NOTE:
   Users running previous versions of APM can still use bookmarks set to access the URL http://<server_name>.<domain_name>/mercuryam and http://<server_name>.<domain_name>/topaz

2. Enter the default administrator user ("admin"), and the password specified in the Setup and Database Configuration utility, and click **Log In**. After logging in, the user name appears at the top right.
3. (Recommended) Create additional administrative users to enable APM administrators to access the system. For details on creating users in the APM system, see "User Management" in the APM Platform Administration Guide.

NOTE:

- For login troubleshooting information, see "Troubleshooting and Limitations" in the APM Platform Administration Guide.
- For details on login authentication strategies that can be used in APM, see "Authentication Strategies — Overview" in the APM Platform Administration Guide.
- For details on accessing APM securely, see the APM Hardening Guide.

When you have completed your session, it is recommended that you log out of the website to prevent unauthorized entry.

To log out:

Click **Logout** at the top of the page.

Adding Additional APM Servers

After you have a working APM 9.50 environment, you can add new Gateway and Data Processing servers as desired.

To add new APM servers to an existing APM environment:

1. Go to the Software Support web site (https://softwaresupport.softwaregrp.com) and sign in.
2. Click **Search**.
3. For Windows, select **Application Performance Management (BAC) > 9.50 > Windows**.

   For Linux, select **Application Performance Management (BAC) > 9.50 > Linux**.
4. Under Document Type, select **Patches**.
5. Locate the APM 9.50 package and save it locally.
6. Launch the relevant setup file to install APM 9.50
7. Run the installation files on all APM servers (Gateway and Data Processing).
8. The Post Install Wizard starts automatically. You should complete the information in this Wizard. On the last page, click the **Exit** option to prevent the Setup and Database Configuration utility from running.
9. Download and install the latest minor minor version (if avialable) from the Software Support site
   a. Go to the Software Support web site (https://softwaresupport.softwaregrp.com) and sign in.
   b. Click **Search**.
   c. Select the relevant product, version , and operating system.
   d. Under Document Type, select **Patches**.
   e. Locate the applicable patch, save it locally and launch the relevant setup file to install the patch.

f. Run the installation file on APM server.

g. The post-installation wizard is automatically run after the patch installation in silent mode.

h. Repeat this procedure for the latest intermediate patch (if available).

10. Run the Setup and Database Configuration utility.
    - Windows: On the APM server, select **Start > All Programs > Micro Focus Application Performance Management > Administration > Configure Micro Focus Application Performance Management**.
      Alternatively, you can run the file directly from **<HPE APM root directory>\bin\config-server-wizard.bat**.
    - Linux: On the APM server machine, open a terminal command line and launch **/opt/HP/BSM/bin/config-server-wizard.sh**
11. Restart all APM servers.

After you have installed all additional servers, restart all other APM servers and data collectors to allow them to recognize the new servers.

Complete the Upgrade Process

When you are ready to use your new servers as your production environment, perform the following tasks:

1. Update the data collectors to communicate with the new servers.
   a. If you have a Load Balancer or Reverse Proxy, set it to communicate with the new servers.
   b. If you do not have a Load Balancer or Reverse Proxy, you must configure each data collector individually to communicate with the new APM Gateway servers. For details, see the documentation of each data collector. We recommend upgrading each data collector to the latest supported version. For details, see the System Requirements and Support Matrixes, available from **Help > Planning and Deployment**.
      For the SiteScope integration, see SiteScope Post-Upgrade Procedure, on page 69.
2. End the SDR and unsubscribe it from the source server. For details, see Staging Data Replicator, on page 53
3. Exit staging mode
   a. Go to **Admin > Platform > Setup and Maintenance > Infrastructure Settings > Foundations – Platform Administration > Platform Administration – BSM Evaluation**.
   b. Set **Enable evaluation (staging) mode** to **false**.
   c. Set **Enable evaluation (staging) mode for customer** to **false**.
4. Keep production server alive

Even though no new events are sent to the production server, there is still a need to keep this server online. Any active events that were forwarded from OM to the production server will continue to send updates this server. These updates will be forwarded to the staging server. If receiving these updates is not important to you, you can decommission the production server immediately. Otherwise, you should wait until all or most of the events previously sent to the production server are closed. It is estimated that most events are typically closed within 1-2 weeks.

The upgrade process is now complete. If you experience any problems during the upgrade process, see Troubleshooting, on page 92.

Redirecting Business Process Monitor Instances

After you have run the Application Performance Managemen upgrade wizard in Staging mode, you must redirect each Business Process Monitor instance to report to the Application Performance Managemen Gateway Server.

You can redirect all Business Process Monitor instances simultaneously, using the Business Process Monitor redirect tool, as described below, or you can redirect each Business Process Monitor instance separately by editing each instance within Business Process Monitor Admin. For details on editing a Business Process Monitor instance within Business Process Monitor Admin, see "BPM Instances" in the Business Process Monitor Administration PDF. It is recommended that you use the Business Process Monitor redirect tool to redirect your Business Process Monitor instances.

NOTE:
Before running the redirect tool , ensure that environment variables are set for %JAVA_HOME% and %PATH% on the BPM system where the redirect tool needs to be executed.

To redirect Business Process Monitors instances using the redirect tool:

1. Extract the files within the **<Application Performance Managemen server root directory>\tools\RedirectTool.zip** file to a directory on a machine that has access to the Business Process Monitors whose instances you want to redirect.
2. In Application Performance Managemen, select **Admin > End User Management > Settings > Business Process Monitor Settings > BPM Agents**. The list of Business Process Monitors from your previous APM system is displayed.
3. Select the Business Process Monitor instances you want to redirect and click the **Export Business Process Monitor Agent Information for the Redirect Tool**  button. Save the file to a machine with access to the machine on which the RedirectTool.zip files are located.
4. In the **<RedirectTool installation directory>\conf\BPMRedirectTool.properties** file, specify the following parameters:

- **NEW_BAC_URL**. The URL of the Application Performance Managemen Gateway Server.
- I**NPUT_FILE_PATH**. The directory in which you saved the export file. Include the name of the file itself as well. For example: D:\\Tools\RedirectTool\BPMList.txt
- **USER**. The user name required to access the Business Process Monitors. (A user name is generally not required.)
- **PASSWORD**. The password required to access the Business Process Monitors. (A password is generally not required.)

5. Run the **<RedirectTool installation directory>\RedirectTool.bat** file. The Gateway Server URL is updated on all the Business Process Monitor instances. A log file containing information on each updated Business Process Monitor instance is created (**<RedirectTool installation directory>\RedirectTool\log**). If the redirect tool failed to update a Business Process Monitor instance, this information is included in the log file.

SiteScope Post-Upgrade Procedure

For SiteScope versions lower than 11.33, after performing a staging upgrade, you need to configure SiteScope to communicate with the new APM Gateway Servers.

Integrate SiteScope and APM 9.50

To integrate SiteScope and APM 9.50, after upgrading to APM 9.50, perform the following procedure.

On the APM 9.50 server:

1. Access the UCMDB JMX server (**https://localhost:8443/jmx-console/HtmlAdaptor?action=inspectMBean&name=UCMDB:service=Packaging Services**).
2. From the Operations index, click **undeployPackages**.
3. In the packageNames Value field, type **sitescope.zip**.
4. Click **Invoke**.
5. From the Operations index, click **deployPackages**.
6. In the packageNames Value field, type **sitescope.zip**.
7. Click **Invoke**.

On the SiteScope server:

8. Stop SiteScope.
9. Copy the jar files and **SiSAPM940PostUpgradeUtil** files from **…/BSM/9.40/content/HPE_ APM_9.40_ SiS_Upgrade** and save them in **<SiteScope root dir>/bin**.
10. For SiteScope installed on Windows, run the **SiSAPM940PostUpgradeUtil.bat** file.

    For SiteScope installed on Linux, run the **SiSAPM940PostUpgradeUtil.sh** file.

Change the Gateway Server to which SiteScope sends data

After performing a APM staging upgrade, you need to configure SiteScope to communicate with the new APM Gateway Servers. To do so, perform one of the following:

- In SiteScope's BSM Integration Preferences, enter the new Gateway Server name or IP address in the **Business Service Management machine name/IP address** box. For user interface details, see BSM Integration Preferences Dialog Box in the Using SiteScope Guide in the SiteScope Help.
- In SAM Administration, update the SiteScope settings with the new Gateway Server name in **Distributed Settings**. For user interface details, see New/Edit SiteScope Page in the APM Application Administration Guide in the APM Help.

  NOTE:
  This can only be used for changing the Gateway Server for a SiteScope that is already registered with a given APM installation. It cannot be used to add a new SiteScope, or to connect a SiteScope to a different APM system.

Diagnostics Post-Upgrade Procedure

In previous releases of APM, Diagnostics sent CIs, metrics, and events to APM. Health Indicator status (coloring) for the Application Infrastructure CIs was based on events sent to APM through the OBM event channel.

In APM 9.40, due to the OBM removal, Diagnostics sends events to OBM and continues to send CIs and metrics to APM. As a result of this change, the Application Infrastructure CIs (Diagnostic Probe, IBM WebSphere MQ, WebSphere AS Dynamic Caching, IBM MQ, WebLogic AS, JBOSS AS, SQL Server, MSSQL Database, Oracle iAS, Oracle, SAP, SAP R3 Server, VMware ESX Server, Host Node) do not show the correct HI Status in APM 9.40.

The HI status for these CIs appears as *Undetermined* (blue question mark). If you are upgrading from APM 9.40, the last status received for the CI before the upgrade will be displayed.

Use the workaround below to view the HI status of these CIs in OBM.

Workaround:

To enable sending events related to threshold violation in Diagnostics to OBM, in the server\bin directory of the Diagnostics server:

1. Run **cscript switch_ovo_agent.vbs -server <FQDN of OBM> -cert_srv <FQDN of OBM>**.
2. Go to **OBM Administration > Certificate Requests** and grant certificates.
3. Run **cscript switch_ovo_agent.vbs -server <FQDN of OBM> -cert_srv <FQDN of OBM>** again.
   All tasks should now display correctly.

Part 3: Appendixes

Appendix A: Installing APM on a Windows Platform

This appendix contains the following topics:

Preparing Information Required for Installation

Have the following information ready before installation:

- **Target directory names**. During installation APM installs the L-Core packages. If a lower version of these packages is already installed, the packages are automatically upgraded. Otherwise, the currently installed version is not overwritten. This change cannot be reversed.
- During the installation, you must select directories for installing these shared packages. They include:
  - Graphing Component
  - Graphing Component for APM
  - Operations agent Consolidated Package
  - Shared Component
  - Software Certificate Client
  - Software Configuration
  - Software Core Japanese Localization
  - Software Core Korean Localization
  - Software Core Simplified Chinese Localization
  - Software Core Spanish Localization
  - Software Cross Platform Component
  - Software Cross Platform Component Java
  - Software Deployment
  - Software HTTP Communication
  - Software HTTP Communication Java
  - Software Java Performance Access

  - Software Process Control
  - Software Security Core
  - Software Security Core Java
  - Timing Service
- **License key**. You have the option to use an evaluation license (60 days) or import your permanent license. You can browse to a local or network location to locate your license .DAT file.

  If at a later stage you need to update the license key (for example, if you acquire a license for one or more new APM components), you can do so within the APM site: Select **Admin > Platform > Setup and Maintenance > License Management** and click the **Add License from File** button. For information on updating the license key, see "Licenses" in the APM Platform Administration Guide.
- **Maintenance number.** This is the maintenance number you received with your APM package.
- **Administrator's email address.**
- **Port number used by the Web server.** This is the port for access to APM. The default is port 80.
- **Name of the Gateway Server machine.** This name must also include the domain name.
- **Name of the load balancer** (if applicable)**.** This is the load balancer used to access the APM site.
- **SMTP mail server name.**
- **SMTP sender name.** This name appears on notifications sent from APM. This name cannot contain spaces. If a name is entered with spaces the reports will not be delivered.

  NOTE:

  - After APM is started, you can configure an alternative SMTP server via **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
  - After the license import step in the post-installation wizard, a redundant error message may appear telling that the licenses could not be added because they already exist. This error has no impact and you can ignore it.

Working with the IIS Web Server

APM installed on a Windows platform works with Apache HTTP Server or Microsoft Internet Information Server (IIS). You specify the web server type in the post-installation wizard. You can re-run the post-installation wizard to modify these settings.

NOTE:

- There must be only one running Web server on a server machine that uses the same port that APM uses. For example, if you select to use Apache HTTP Server during APM server installation, and you are installing on a machine on which IIS is already running, make sure to stop the IIS service and set its startup status to **Manual** before you begin the installation process.
- Windows authentication and basic authentication in IIS are not supported.

Apache HTTP Server

APM uses an Apache HTTP Server version that has been adapted for use with APM. It is installed during the server installation.

By default, the Apache HTTP Server is not enabled for SSL use. For details on configuring the Web server to use SSL, see http://httpd.apache.org/docs/2.2/ssl/. SSL should be enabled for all the directories in use by APM, as configured in the Apache configuration file (**httpd.conf** and **httpd-ssl.conf**).

NOTE:
For security reasons, in SaaS configurations, you need to set the HTTPOnly attribute for the J,S EiSnS IONID cookie on the APM Gateway or APM Typical installation:

In **/<HPE APM root directory>/WebServer/conf/httpd.conf**, add the following line before line `# Secure (SSL/TLS) connections`:

```
Header edit Set-Cookie ^(JSESSIONID.*)(HttpOnly) $1
```

Microsoft Internet Information Server (IIS)

- For Microsoft Windows Server 2008 using IIS 7.x Web server, see Microsoft Windows Server 2008 using IIS 7.x Web Server, on the next page.
- For Microsoft Windows Server 2012 using IIS 8 Web server, see Microsoft Windows Server 2012 using IIS 8 Web Server, on the next page.
- For Microsoft Windows Server 2016 using IIS 10 Web server, see Microsoft Windows Server 2016 using IIS 10 Web Server, on page 76

NOTE:
For security reasons, in SaaS configurations, you need to set the HTTPOnly attribute for the JSESSIONID cookie on the APM Gateway or APM Typical installation:

Add the following lines to the `<outboundRules>` section of the `<rewrite>` section of the `<system.webServer>` section in **<Root directory of your Web Application>/web.config** (by default it is located in **C:\inetpub\wwwroot\web.config**)

```
<outboundRules>
              .....
```

```
            .....
   <rule name="removeHttpOnly_from_JSESSIONID" preCondition="JSESSIONID_
cookie">
      <match serverVariable="RESPONSE_Set_Cookie" pattern="^(JSESSIONID.*)
(HttpOnly)" />
      <action type="Rewrite" value="{R:1}" />
   </rule>
   <preConditions>
            .....
            .....
      <preCondition name="JSESSIONID_cookie">
         <add input="{RESPONSE_Set_Cookie}" pattern="." />
         <add input="{RESPONSE_Set_Cookie}" pattern="JSESSIONID" />
      </preCondition>
   </preConditions>
</outboundRules>
```

Microsoft Windows Server 2008 using IIS 7.x Web Server

If you are installing on a Microsoft Windows Server 2008 and using the IIS 7.X Web server, perform the following procedure:

1. In the **Control Panel**, select **Administrative Tools** > **Server Manager**.
2. Right-click **Roles** and select **Add server role** to launch the Add Roles wizard.
3. On the Select Role Services page, select **Web Server (IIS) role** to install.

   If a pop up window opens with the question **Add features required for Web Server (IIS)?**, click the **Add required features** button.
4. Click **Next** twice.
5. In the Select Role Services panel, select the following roles:
   a. **Common HTTP Features** section: **Static Content** (usually enabled by default)
   b. **Application Development** section: **ISAPI Extensions** and **ISAPI Filters.**
   c. **Management Tools** section: **IIS Management Scripts and Tools**
6. Click **Install**.
7. Continue with Working with the IIS Web Server, on page 73.

Microsoft Windows Server 2012 using IIS 8 Web Server

If you are installing on a Microsoft Windows Server 2012 and using the IIS 8 Web server, perform the following procedure:

1. In the **Control Panel**, select **Administrative Tools** > **Server Manager**.
2. Click **Manage** > **Add Roles and Features**.
3. Click **Next**.

4. Select **Role-based or feature-based installation**.
5. Click **Next**.
6. Select **Select a server from the server pool**.
7. Click **Next**.
8. On the Select Role Services page, select **Web Server (IIS) role** to install.

   If a pop up window opens with the question **Add features required for Web Server (IIS)?**, click the **Add required features** button.
9. Click **Next** twice.
10. In the Select Role Services panel, select the following roles:
    a. **Common HTTP Features** section:
       - **Static Content** (usually enabled by default)
       - **HTTP Redirection**
    b. **Application Development** section: **ISAPI Extensions** and **ISAPI Filters.**
    c. **Management Tools** section: **IIS Management Scripts and Tools**
11. Click **Next**.
12. Click **Install**.
13. Continue with Working with the IIS Web Server, on page 73.

Microsoft Windows Server 2016 using IIS 10 Web Server

If you are installing on a Microsoft Windows Server 2012 and using the IIS 10 Web server, perform the following procedure:

1. In the **Control Panel**, select **Administrative Tools** > **Server Manager**.
2. Click **Manage** > **Add Roles and Features**.
3. Click **Next**.
4. Select **Role-based or feature-based installation**.
5. Click **Next**.
6. Select **Select a server from the server pool**.
7. Click **Next**.
8. On the Select Role Services page, select **Web Server (IIS) role** to install.

   If a pop up window opens with the question **Add features required for Web Server (IIS)?**, click the **Add required features** button.
9. Click **Next** twice.
10. In the Select Role Services panel, select the following roles:

a. **Common HTTP Features** section:
   - **Static Content** (usually enabled by default)
   - **HTTP Redirection**

b. **Application Development** section: **ISAPI Extensions** and **ISAPI Filters.**

c. **Management Tools** section: **IIS Management Scripts and Tools**

11. Click **Next**.
12. Click **Install**.
13. Continue with Working with the IIS Web Server, on page 73.

Configuring existing Response when HTTP status code is in error

The following procedure defines that the server should process the existing response untouched when an HTTP error status code is returned.

1. In the Internet Information Service (IIS) Manager, select the server in the Connections Tree view.
2. Click **Configuration Editor**.
3. From the Configuration Editor Section drop down list, select **system.webServer/httpErrors**.
4. Set the value of the existingResponse parameter to **PassThrough**.
5. Click **Apply** in the upper right corner.
6. Select the server in the Connections Tree view.
7. Click **Restart** in the upper right corner.

Installing APM Servers on a Windows Platform

You install APM servers—the Gateway Server and Data Processing Server—from the APM distribution package. Unless you install on a machine running IIS, APM installs Apache HTTP Server during the installation process.

You need administrative privileges for the machines on which you are installing APM servers.

NOTE:

- Make sure that there are no other installations or processes that may be using the Windows Installer. If there are, the APM installation hangs and cannot continue running. You must stop the other installation, stop the APM installation by clicking the **Cancel** button in the installation wizard, and re-run the APM installation.
- This appendix does not replace the APM Installation Guide. It only provides common information about the installation flow. For installation details, see the APM Installation Guide and APM Patch Installation Guide.

The first installation wizard copies the files and packages onto your machine. The post-installation wizard enables registration, and configuring connection, Web server, and SMTP settings.

You can also install APM in silent mode. For details, see Installing APM Silently, on page 85.

To install APM servers:

1. Obtain the installation package.

   Go to My software updates (use your Passport credentials) and click the APM 9.50 installation package.

   or

   a. Go to the Software Support web site (https://softwaresupport.softwaregrp.com) and sign in.
   b. Click **Search**.
   c. Select **Application Performance Management (BAC) > 9.50 > Windows**.
   d. Under Document Type, select **Patches**.
   e. Locate the APM 9.50 package and save it locally.
2. Run the installation files on all APM servers (Gateway and Data Processing).
3. From the **Start** menu, select **Run**.
4. Enter the location from which you are installing, followed by **HPEApm_9.50_setup.exe**. The setup file for APM servers is located in the **Windows_Setup** directory. For example, enter d:\Windows_Setup\HPEApm_9.50_setup.exe

   NOTE:
   If you are installing on a virtual machine, you must copy the .exe file, as well as the packages directory, locally. If you attempt to run the installation over the network onto a virtual machine, the installation fails.

5. Click **OK**. Setup begins.
6. Follow the on-screen instructions for server installation.
   - **Language**. If your installer has been localized to offer additional languages, select one from the options available.

     NOTE:
     You may receive an anti-virus warning. You can proceed with the installation without taking any action and with the anti-virus software running on the machine.

   - **Setup type:**
     - Select **Gateway** setup type to install the Gateway Server on the current machine.
     - Select **Data Processing** setup type to install the Data Processing Server on the current machine.

- Select **Typical** setup type to install the Gateway Server and Data Processing Server on the same machine.

  NOTE:
  If you are installing onto a machine running Windows 2008 R2 Server, you may get the following message: The installation folder for shared content is not valid. The problem may in fact be that you do not have the necessary administrator permissions to install APM on the machine. Check with your system administrator.

- **Installation directories**. You must select the following directories for installation.
  - Select the installation directory for shared content. Note that there is additional shared data in **%ALLUSERSPROFILE%\HP\BSM**
  - Select the installation directory for product specific content. In Microsoft Windows environments, this path must be 15 characters or less, and must not contain blank spaces. If the name exceeds 15 characters or does not end with **BSM**, during the next step, the installation prompts you to give a different name.

    NOTE:
    During installation you may get the following message:
    The necessary ports are in use. If the installation indicates that there are ports in use, the installation does not fail but it is recommended that you free the necessary ports. Otherwise, you will have to re-configure APM to use a different set of ports.

This phase of the installation can take approximately 30-60 minutes in a virtual environment.

After the process completes, you see check marks next to each of the packages and applications successfully deployed. If there are errors, an Error window opens indicating which installation scripts may have failed.

7. The post-installation wizard opens. Do the following:
   - **Register the product.**
   - **Configure connection settings:**
     a. **Apache HTTP Server.** If port 80, the default port, is already in use by the existing Web server, APM notifies you to resolve the conflict. If you select Apache, you must also enter the email address of the APM administrator.
     b. **Microsoft IIS.** If IIS is using a port other than port 80, enter the IIS port. If you select IIS, you must also select the IIS Web site address to be used by APM.
   - **Select the Web server type:**
     - If APM does not detect an installation of Microsoft IIS on the machine, you are offered the **Apache HTTP Server** option only. If you want to run APM with Microsoft IIS, click **Cancel** to exit the wizard. Install IIS and rerun Post Install.
   - **Specify the SMTP mail server:**

- It is recommended that you specify the complete Internet address of your SMTP server. Use only alphanumeric characters.
- In the **Sender name** box, specify the name to appear in scheduled reports and on alert notices that APM sends. If APM was ever installed on the same machine, a default name, **HP_BSM_Notification_Manager**, may appear. You can accept this default or enter a different name.
- After APM is started you can configure an alternative SMTP server via **Platform Administration > Admin > Platform > Setup and Maintenance > Infrastructure Settings**.

If deploying on more than one server, install additional APM servers using the above steps.

NOTE:

- You can rerun the post-installation wizard to modify the settings. The post-installation wizard can be run from the following location: **<HPE APM root directory>\bin\postinstall.bat**. However, if you are running the post-installation wizard for the first time or it was closed before completion, use the following file instead <**HPE APM root directory>\bin\ovii-postinstall.bat <TOPAZ_HOME>**, where **<TOPAZ_HOME>** is the APM installation directory (typically C:\HPBSM).

Appendix B: Installing APM on a Linux Platform

This appendix contains the following topics:

Preparing Information Required for Installation

Have the following information ready before installation:

- **Maintenance number.** This is the number you received with your APM package.
- **Web server name.** This name must also include the domain name.

  NOTE:
  When installing on Linux, the domain name must be entered manually.

- **Administrator's email address.**
- **SMTP mail server name.**
- **SMTP sender name.** This name appears on notifications sent from APM.
- **Name of the Gateway Server machine.**
- **Name of the load balancer** (if any). This is the load balancer used to access the APM site.
- **Port number used by the Web server**. The default port is 80.

Working with the Apache Web Server

APM installed on a Linux platform works with Apache HTTP Server.

NOTE:
There must only be one running Web server on an APM server machine.

Apache HTTP Server

APM uses a version of the Apache HTTP Server that has been adapted for APM. It is installed during the server installation.

APM runs its Apache HTTP Server, by default, through port 80. If port 80 is already in use, there are two ways to resolve the port conflict:

- Before beginning APM installation, reconfigure the service using that port to use a different port.
- During APM installation, select a different port for the Apache HTTP Server.

By default, the Apache HTTP Server is not enabled for SSL use. For details on configuring the Web server to use SSL, see http://httpd.apache.org/docs/2.2/ssl/. SSL should be enabled for all the directories in use by APM, as configured in the Apache configuration file (**httpd.conf** and **httpd-ssl.conf**).

NOTE:
For security reasons, in SaaS configurations, you need to set the HTTPOnly attribute for the J,S EiSnS IONID cookie on the APM Gateway or APM Typical installation:

In **/<HPE APM root directory>/WebServer/conf/httpd.conf**, add the following line before line `# Secure (SSL/TLS) connections`:

```
Header edit Set-Cookie ^(JSESSIONID.*)(HttpOnly) $1
```

Installing APM Servers on a Linux Platform

NOTE:
This appendix does not replace the APM Installation Guide. It only provides common information about the installation flow. For installation details, see the APM Installation Guide and APM Patch Installation Guide.

You can install APM servers—the Gateway Server and Data Processing Server—from the APM 9.50 installation package.

To verify that the installation files are original and provided with code and have not been manipulated by a third-party, you can use the Public Key and verification instructions provided on this web site: https://hpcssweb-pro.austin.hp.com/hpcssui/HPCSSHome.xhtml.

You can also install APM in silent mode. For details, see Installing APM Silently, on page 85.

NOTE:
It is recommended that you do not use an emulator application, for example Exceed, to install APM. Installing via an emulator may slow the pace of the installation and may adversely affect the appearance and functionality of the user interface.

To install APM servers:

1. Log in to the server as user root.
2. Obtain the installation package.

   Go to My software updates (use your Passport credentials) and click the APM 9.50 installation package.

or

a. Go to the Software Support web site (https://softwaresupport.softwaregrp.com) and sign in.
b. Click **Search**.
c. Select **Application Performance Management (BAC) > 9.50 > Linux**).
d. Under Document Type, select **Patches**.
e. Locate the APM 9.50 package and save it locally.

3. (Optional) You can verify that the installation files are original and provided with code and have not been manipulated by a third-party by using the Public Key and verification instructions on the following website:
https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning.
4. Run the following script:

/HPEApm_9.50_setup.bin

5. Follow the on-screen instructions for server installation.

NOTE:
If APM detects a previous installation on the machine, a message is displayed warning that any customized configuration data will be overwritten.

- Select the setup type:
  - Select **Gateway** setup type to install the Gateway Server on the current machine.
  - Select **Data Processing** setup type to install the Data Processing Server on the current machine.
  - Select **Typical** setup type to install the Gateway Server and Data Processing Server on the same machine.
- The directory where the APM files are copied is **/opt/HP/BSM**.
- The data directory for shared content is **/var/opt/OV**.

NOTE:
During installation you may get the following message:

The necessary ports are in use. If the installation indicates that there are ports in use, the installation does not fail but it is recommended that you free the necessary ports.

This phase of the installation can take approximately 30-60 minutes in a virtual environment.

After the process completes, you see check marks next to each of the packages and applications successfully deployed. If there are errors, an **Errors** tab opens detailing what errors may have occurred.

6. The post-installation wizard opens. Do the following:

- **Register the product.** Enter **Name, Company,** and **Maintenance number.**
- **Configure connection settings:**
  - Host. Must be the fully qualified domain name (FQDN). The name of the server may appear by default but you must add the domain manually. If you use a load balancer, here you must enter the machine name for the load balancer.
  - Port. If port 80, the default port, is already in use by the existing Web server, APM notifies you to resolve the conflict.
- **View the Web server type and enter the APM administrator email address.** APM installs the Apache HTTP Server. This is the web server that must be used in Linux environments.
- **Specify the SMTP mail server:**
  - It is recommended that you specify the complete Internet address of your SMTP server. Use only alphanumeric characters.
  - In the Sender name box, specify the name to appear in scheduled reports and on alert notices that APM sends.

NOTE:
You can rerun the post-installation wizard to modify the settings. The post-installation wizard can be run from the following location: **<HPE APM root directory>/bin/postinstall.sh**. However, if you are running the post-installation wizard for the first time or it was closed before completion, use the following file instead **<HPE APM root directory>/bin/ovii-postinstall.sh <TOPAZ_HOME>**, where **<TOPAZ_HOME>** is the APM installation directory (typically /opt/HP/BSM).

Appendix C: Installing APM Silently

The wizards used to install and configure APM can be run in silent mode. Silent mode runs the wizards from a command line, without viewing the wizard interface. This allows Linux users without X-windows to run these wizards, however it can be used in windows environments as well.

The instructions have been written for Linux. To run the files for windows environments, replace all .bin file types with .exe and .sh file types with .bat.

NOTE:
Silent mode is not supported for upgrade wizards.

This appendix contains the following topics:

How to Fully Install APM 9.50 Silently

This procedure describes how to perform a complete installation of APM silently, including the installation wizard, post-installation wizard, and latest minor-minor release.

NOTE:
Silent mode is not supported for upgrade wizards.

1. Run the APM 9.50 Installation Wizard silently by running the installation file from the command line with a **-i silent** parameter. The installation file can be found in **<APM Installation Media>** root folder.
   - To install the Gateway and Data Processing servers on one-machine (typical installation) using the default installation directory, run the following command:

     APM_9.50_setup.bin -i silent
   - To install the Gateway and Data Processing Servers on different machines use the following procedure:
     a. Create an empty file called **ovinstallparams.ini** in the same directory as the installation executable file on both servers.
     b. Copy the following section to the .ini file on the Gateway Server:

        [installer.properties]

        setup=HPEApm

        group=**gateway**

c. Run the Installation Wizard in silent mode on the Gateway Server as follows:

HPEApm_9.50_setup.bin -i silent

d. Copy the following section to the .ini file on the Data Processing Server:

[installer.properties]

setup=HPEApm

group=**process**

e. Run the Installation Wizard in silent mode on the Data Processing Server as follows:

HPEApm_9.50_setup.bin -i silent

2. Install the latest minor-minor release silently (for example, 9.50) as follows:

a. Prerequisites

- It is recommended that you back up all APM databases and files you made custom changes to.
- Back up your license folder. If you uninstall the patch you will need restore this folder.

  Your license folder is located in:

  - Windows: **<HPE APM root directory>\conf\license**
  - Linux: **/opt/HP/BSM/conf/license**

b. Go to the Software Support web site (https://softwaresupport.softwaregrp.com) and sign in.

c. Click **Search**.

d. Select the relevant product, most recent minor minor 9.50 version, and operating system (for example, Application Performance Management (BAC) > 9.50 > Windows). Under Document Type, select **Patches**.

e. Locate the installation files.

f. Save the package locally and run the installation file silently using the following syntax:

HPEApm_9.50_setup.bin -i silent

3. Open the response file in **<HPE APM root directory>\Temp\emptyRspFile.xml** and complete the values in the Post Install section.
4. If you plan to use a non-root APM configuration, create an appropriate user.
5. Run the post-installation wizard

<HPE APM root directory>\bin\silentConfigureBSM.sh <HPE APM root directory>\Temp\emptyRspFile.xml postinstall

How to Encrypt Passwords in the Response File

The passwords that are stored in the response file can be encrypted for added security. To do this, run the password encryption tool located in:

<HPE APM root directory>/bin/encrypt-password.sh

You enter your password and the encryption tool returns a string. Copy the string to the response file where you would have entered your password.

Limitation: encrypted passwords are valid on the machine that ran the encryption tool.

To remove password encryption, enter the passwords in the response file normally and set the value of **IsEncrypted="false"**.

Appendix D: Upgrade Wizard

This appendix provides information about the APM upgrade wizard and contains the following topics:

Upgrade Wizard Overview

The upgrade wizard is run after the post-installation wizard. It replaces the setup and database configuration utility which is run in a regular deployment. The upgrade wizard performs the following tasks:

- Migrates data from original databases
- Migrates APM configurations
- Guides you through manual procedures necessary for the upgrade process

The upgrade wizard gives you the option of skipping some steps and running them later by restarting the wizard manually. This can be done as many times as is necessary. For example, if you do not have time to complete the data upgrade, you can skip it and complete the rest of the wizard. When you manually restart the wizard, your previous progress is saved. Make sure that you run the entire upgrade wizard from start to finish at least once.

The upgrade wizard runs the database schema verify program on your database schemas to verify that they have been configured properly. For details, see the APM Database Guide.

The wizards are located in the <HPE APM root directory>\bin directory as follows:

- **Windows:**
  - If you want to upgrade from 9.30 to 9.50 version, select the upgrade wizard from the following location:

  <HPE APM root directory>\bin\upgrade_wizard_run_from930.bat
  - If you want to upgrade from 9.40 to 9.50 version, select the upgrade wizard from the following location:

  <HPE APM root directory>\bin\upgrade_wizard_run_from940.bat
- **Linux:**
  - If you want to upgrade from 9.30 to 9.50 version, select the upgrade wizard from the following location:

  /opt/HP/BSM/bin/upgrade_wizard_run_from930.sh

- If you want to upgrade from 9.40 to 9.50 version, select the upgrade wizard from the following location:

/opt/HP/BSM/bin/upgrade_wizard_run_from940.sh

When installing APM in a distributed environment, first run the Upgrade Wizard on the Data Processing Server and then on the Gateway Server.

Preparing Information for the Upgrade Wizard

To speed up the upgrade process, we recommend that you have the following information prepared before starting the upgrade wizard:

- **Data collectors / components.** Access to all data collectors and components integrated with the original APM servers.
- **APM Architecture.** Knowledge of your original APM architecture including data collectors / components / servers.
- **APM Servers.** Location, credentials, and access to files for all original APM and new APM servers.
- **Database Information.** Locations, credentials, CMDB / RTSM configuration (for example: internal RTSM, external CMDB, both).
  - **SQL server:** Credentials for a member of the sysadmin group or a user with select permissions for the syslogins system view.
  - **Oracle server:** Credentials for a user with the DBA or SELECT_CATALOG_ROLE role.

Appendix E: Changing APM Service Users

This appendix provides the procedure for how to switch the Windows and Linux users associated with APM and contains the following topics:

Switching the Windows User

The APM service, which runs all APM services and processes, is installed when you run the Setup and Database Configuration utility. By default, this service runs under the local system user. However, you may need to assign a different user to run the service (for example, if you use NTLM authentication).

The user you assign to run the service must have the following permissions:

- Sufficient database permissions (as defined by the database administrator)
- Sufficient network permissions
- Administrator permissions on the local server

  NOTE:
  When the APM service is installed, it is installed as a manual service. When you enable APM for the first time, it becomes an automatic service.

To change the APM service user:

1. Disable APM (**Start > Programs > Application Performance Managemen > Administration > Disable Application Performance Managemen**).
2. In Microsoft's Services window, double-click the Service name: **hp_bsm** (Display name: **Business Service Management**). The Business Service Management Properties (Local Computer) dialog box opens..
3. Click the **Log On** tab.
4. Select **This account** and browse to choose another user from the list of valid users on the machine.
5. Enter the selected user's Windows password and confirm this password.
6. Click **Apply** to save your settings and **OK** to close the dialog box.
7. Enable APM (**Start > Programs > Application Performance Managemen > Administration > Enable Application Performance Managemen**).

NOTE:
This procedure must be repeated if APM is reinstalled or upgraded.

Switching the Linux User

APM must be configured to run on linux using a specific user. This user can be either the root or any other user. APM supports only one user at a time. The user is defined in the post-installation wizard.

To switch the user after APM is installed:

1. Stop APM.
2. Rerun the post-installation wizard and specify the new user. The post-installation wizard can be run from the following location: **/opt/HP/BSM/bin/postinstall.sh**.
3. Log out of Linux and log in with the new user.
4. Run the Setup and Database Configuration Utility

   Run the Setup and Database Configuration Utility on the Gateway and Data Processing Servers. The Setup and Database Configuration Utility can be run from the following location **/opt/HP/BSM/bin/config-server-wizard.sh**.
5. Start APM.

Appendix F: Troubleshooting

This appendix contains the following topics:

Troubleshooting Resources

- **Installation log files.** For details, see Check installation log files, on page 63.
- **Upgrade log tool.** To view a summary of errors that occurred during the configuration upgrade portion of the upgrade wizard, run the upgrade log tool located at **<HPE APM root directory>\tools\logTool\logTool.bat**. This generates a report in the same directory with the name **logTool.txt**.
- **Self-solve knowledge base.** For additional troubleshooting information, see the Self-solve knowledge base accessed from the Software Support (https://softwaresupport.softwaregrp.com).
- **APM Tools.** You can use APM tools to assist in troubleshooting the Application Performance Managemen environment. You access the tools from **<HPE APM root directory>\tools** directory. Most of the tools should only be used in coordination with personnel. The Database Schema Verification utility (dbverify) and Data Marking utility should be used according to documented instructions.
- **APM Logging Administrator.** This tool allows you to temporarily modify the level of details displayed in APM logs, as well as create custom logs. To open the APM Logging Administrator Tool, open the following URL:

  http://<APM Gateway Server FQDN>/topaz/logAdminBsm.jsp

Installation and Connectivity Troubleshooting

This section describes common problems that you may encounter when installing APM or connecting to APM following installation, and the solutions to these problems.

Cannot expand Application Performance Managemen group on Windows 2016 DC

This is a Windows Server 2016 DC issue.

Solution:

Log out of Application Performance Managemen and log back in again.

Unable to access APM using Internet Explorer with an FQDN that has a two letter domain

Internet Explorer does not support FQDNs with two letters domains for the APM default virtual URL (for example XXXX.aa).

Workaround:

If FQDN has a two letter domain, use another browser (not Internet Explorer) to access APM.

Receive error message: not enough space on the drive to extract the installation files

This happens during component installation. If you enter a new path for a different drive with sufficient space, the same error message is displayed.

During the file extraction process, certain data is always saved to the TEMP directory on the system drive, even if you choose to save the installation files to a different location from the default path.

Solution:

- Free up sufficient disk space on the system drive (as specified in the error message), then continue with the installation procedure.
- If it is not possible to free up sufficient disk space on the system drive, change the path for the system's TEMP variable.
  - **Windows:** Select **Start > Settings > Control Panel > System > Advanced tab > Environment Variables**, and edit the path for the **TEMP** variable in the User variables area.
  - **Linux:** Run the following commands:

    ```
    export IATEMPDIR=/new/tmp
    export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp
    ```

    where `/new/tmp` is the new working directory.

Installation fails due to security restrictions of the /tmp directory on Linux

If the /tmp directory has security restrictions that prevent script execution from it, the installation will fail.

Solution:

Set a new /tmp directory not affected by these restrictions, by running the following commands:

```
export IATEMPDIR=/new/tmp
```

```
export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp
```

where `/new/tmp` is the new working directory.

Connection to a Microsoft SQL Server database fails when running the Setup and Database Configuration Utility

Verify that the user under whom the SQL Server service is running has permissions to write to the disk on which you are creating the database.

A network login prompt appears when completing the APM server installation

Possible Cause:

This can occur if the IIS server's authentication method is not set to the default setting, **Allow Anonymous Access**.

Solution:

Reset the IIS server's authentication method to the default setting, **Allow Anonymous Access**, and ensure that the default user account **IUSR_XXX** (where "XXX" represents the name of the machine) is selected (the user account **IUSR_XXX** is generated during IIS installation). Then uninstall and reinstall APM.

Tomcat servlet engine does not start and gives an error

The error message is as follows:

java.lang.reflect.InvocationTargetException: org.apache.tomcat.core.TomcatException: Root cause - Address in use: JVM_Bind

Possible Cause:

Running Oracle HTTP Server, installed with a typical Oracle installation, on the same machine as APM servers causes a conflict with the Tomcat servlet engine.

Solution:

Stop the Oracle HTTP Server service, disable and then enable APM.

To prevent the problem from recurring after the machine is restarted, change the Oracle HTTP Server service's startup setting to **manual**.

Inability to install APM components due to administrative restrictions

Possible Cause:

The machine on which you are installing has policy management software that restricts access to files, directories, the Windows registry, and so forth.

Solution:

If this type of software is running, contact your organization's network administration staff to obtain the permissions required to install and save files on the machine.

After installing, receive http error 404 on the page when attempting to access APM

Perform the following tasks:

1. Verify that all APM processes were started by accessing the status page. For details, see "How to View the Status of Processes and Services" in the APM Platform Administration Guide.
2. If all the services appear green in the status page, browse to APM using port 29000 (http://MACHINE _NAME:29000).

   Try to access the JMX console. If you can access the console, continue with step 3 trying to discover the problem.
3. Check if the Web server is started (http://MACHINE _NAME). If the Web server is started, you probably have a problem with the ISAPI filter.
4. If the problem is with the ISAPI filter and you are running on a Microsoft Windows 2008 server, check that you followed the procedure for creating a role. For details, see Working with the IIS Web Server, on page 73.
5. The Apache server may not be successfully starting because of a port collision.

After uninstalling APM and reinstalling to a different directory, APM does not work

Possible Cause: When uninstalling and reinstalling to a different location, the IIS ISAPI filter did not get updated to the new path.

Solution:

To update the IIS ISAPI filter to the new path:

1. Open the IIS Internet Services Manager.
2. Right-click the machine name in the tree and select **Properties**.
3. With **WWW Service** displayed in the Master Properties list, click **Edit**.
4. Select the **ISAPI Filter** tab.
5. Ensure that **jakartaFilter** is pointing to the correct APM directory.

6. Apply your changes and quit the Internet Services Manager.
7. Restart the IIS service.

Business Process Monitor or SiteScope data are not being reported to APM

There are various conditions that may cause this problem. For details on causes and possible solutions, refer to the Self-solve Knowledge Base, and search for article number KM438393. (https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result/-/facetsearch/document/KM438393/).

Business Process Monitors fail to report to the Gateway Server running on IIS

Symptoms/Possible Causes:

- No data reported to loaders
- No data in Web site reports
- An error in the **data_deport.txt** log on the Business Process Monitor machine similar to the following:

```
Topaz returned an error (<html><head><title>Error Dispatching
URL</title></head>

<body>

The URI:<br/><b>api_reporttransactions_ex.asp</b><br/> is <b>not</b> mapped to
an API Adapter.<br/>Either the URI is misspelled or the mapping file is
incorrect (the mapping file is located at:
D:\HPBAC/AppServer/TMC/resources/ServletDispatcher.xml)

</body>

</html>)
```

The problem can be confirmed by opening the page http://<machine name>/ext/mod_mdrv_wrap.dll?type=report_transaction. If there is a problem, a Service Temporarily Unavailable message is displayed.

You can also submit the following URL to verify Web Data Entry status: http://<machine name>/ext/mod_mdrv_wrap.dll?type=test

This problem may be caused by the existence of **MercRedirectFilter**, which is a deprecated filter that is no longer needed for APM and may be left over from previous versions of APM.

Solution:

Delete the **MercRedirectFilter** filter and ensure that the **jakartaFilter** is the only IIS ISAPI filter running.

Business Process Monitor is unable to connect via the Internet to the Gateway Server installed on an Apache Web server

Possible Cause:

The Business Process Monitor machine is unable to resolve the Gateway Server name correctly.

Solution:

- Add the Gateway Server name to the Business Process Monitor machine's **<Windows system root directory>\system32\drivers\etc\hosts** file.
- Change the Gateway Server name in the **<HPE APM root directory>\WebServer\conf\httpd.conf** file on the Gateway Server to a recognized name in the DNS.

Post-Installation Wizard fails during APM installation on Linux machine

This may be due to a Linux bug. Open the **/etc/sysctl.conf** file and remove the line **vm.swapiness = 0**. Restart the post installation wizard.

Failed to install Adobe Flash Player

Adobe Flash Player is installed using the Adobe Download Manager which cannot handle automatic proxy configuration scripts. If Internet Explorer is configured to use an automatic proxy configuration, the download manager fails and hangs with no visual response. Try configuring a proxy host manually or see the Flash Player documentation.

APM fails to start or APM configuration wizard does not open

Check the supervisorwrapper.log file for the following error:

<HPE APM root directory>\conf\supervisor\manager\nannyManager.wrapper wrapper | OpenService failed - Access is denied.

If this error is present, the issue may be due to having User Access Control (UAC) enabled on a Windows system. Disable UAC on all APM servers running Windows.

Failure to log in based on FQDN

If you see the following error in the login screen: **The Application Performance Managemen URL must include the Fully Qualified Domain Name (FQDN). Please retype Application Performance Managemen URL in the address bar**, but you are connecting via FQDN, check if

there is a DNS resolution for Load Balanced virtual IPs from the APM gateways. You may need to add LB virtual IPs (for application users and for data collectors if needed) to the hosts file on APM gateway.

After pressing Login, nothing happens. Or user logs in, but Sitemap is empty.

Possible Cause:

You are trying to login to APM from the Windows Server instead of the client machine. On Windows Server, the Internet Explorer Enhanced Security Configuration is typically enabled. With this configuration, several APM UI features including APM login page, may not work.

Resolution:

Check if the Internet Explorer Enhanced Security Configuration is enabled. If it is enabled, use a regular client for login, and not the Windows server.

If you must login from the server, either disable Internet Explorer Enhanced Security Configuration (**Control Panel > Add/remove Windows components**) or add the APM URL to the trusted sites in the IE Security Settings.

Java applets not opening

- If you use Internet Explorer, select **Tools** > **Internet Options** > **Connections** > **Local Area Network (LAN) Settings**. Clear the following options: **Automatically detect settings** and **Use automatic configuration script**.
- Select **Control Panel** > **Java** > **General** tab > **Network Settings** > select **Direct connection** option (and not the default option to **Use browser settings**).

Uninstalling APM results in errors

If you receive a few errors that look like the following:

The package HPOv….can not be uninstalled.

You can ignore these errors. APM has been uninstalled correctly.

Unreadable Eastern Asian Characters

On some RHEL6.x distributions, when choosing to install APM in an Eastern Asian locale (Korean, Japanese or Simplified Chinese), the installation UI displays unreadable characters.

Workaround:

Launch the installer with a JRE that supports Eastern Asian Languages.

setup.bin LAX_VM ${PATH_TO_JAVA}

After installing APM, unable to start APM

APM failed to start. An error occurred when accessing **jmxremote.password**. This error appears in the **<HPE APM root directory>\log\supervisor\wrapper.log**.

Solution:

Make sure that the user who runs APM, is the owner of the jmxremote.access file and has read/ write permission on this file.

Server is not ready message

If you see the following, it is an indication that JBoss is not starting.

- The status page returns the “Server is not ready” message.
- Processes are not loading.
- The wrapper.log file from the <HPBSM>\log\supervisor folder contains this error: “Error: Password file read access must be restricted: c:\HPBSM/JRE64/lib/management/jmxremote.password”

The root cause of this problem is that the Windows Management Instrumentation command-line (WMIC) utility works incorrectly with different regional settings. As a result, it impacts the assignment mechanism of ownership and permissions (files jmxremote.access and jmxremote.password).

Workaround:

1. Disable APM.
2. Navigate to **<HPE APM root directory>\JRE\lib\management**.
3. Right-click **jmxremote.password** and select **Properties**.
4. Click the **Security** tab.
5. Click **Edit**.
6. Click **Add** and add the **Administrators** group.
7. Allow **Read** and **Write** permissions for the Administrators group.
8. Repeat steps 2 – 7 for the **jmxremote.access** file.
9. Navigate to **<HPE APM root directory>\JRE64\lib\management**.
10. Repeat steps 3 – 8.
11. Enable APM.

Restart Message after Rebooting

After rebooting your machine, the following message appears:

You may need to restart your system for the configuration changes made to the system to take effect. Would you like to quit this installation?

This occurs in the Windows 2016 operating system. The installer checks the following key in the registry after HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ Session Manager \ PendingFileRenameOperations to determine if the machine needs to be rebooted. After the reboot, this key should disappeared, but in Windows 2016, it still appears.

Solution:

- Click **Continue**.

Or

1. Click **Quit**.
2. Delete the registry **HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\ Control\Session Manager\PendingFileRenameOperations** .
3. Run the installer again.

Error when Running MSI Files

The Post Install Wizard installs several MSI files (Request Router application, Rewrite Rules module, Web Farm framework) when you are performing an IIS Web Server configuration. The Post Install Wizard has two attempts to run these MSI files. If the Post Install Wizard fails to run these files, the log file displays an “ErrorLevel 1603” message.

Solution:

1. Run the MSI files manually from **<HPE APM root directory>\bin\IIS** .
2. Rerun the Post Install Wizard (**postinstall.bat** from **<HPE APM root directory>\bin**).

Troubleshooting the Upgrade Process

This section describes problems that you may encounter when upgrading APM, and the solutions to these problems.

General issues

- If you are using remote desktop and the upgrade wizard is not displayed properly, try reconnecting with remote desktop at a different resolution, or from a different machine.
- Within the wizard, if the **Next** button or **Back** button do not work, check the upgrade Framework.log for the cause of the error. In most cases, restarting the upgrade wizard resolves the problem.
- RUM Engine permissions may be reset during the APM upgrade. Therefore, it is recommend to ensure that the RUM Engine View permission is selected after upgrading APM.

1. In APM, click **Admin > Platform**.
2. Click the **Users and Permissions** tab.
3. Click **User Management**.
4. In the tree, select an EUM context and click the **Permissions** tab.
5. Select the RUM Engine instance(s) and click the **Operations** tab.
6. Enable the **View** option if it is not already selected and if it is not inherited or granted from Group/Roles/Parent.

Limitation

- Search queries defined in **EUM Admin > Search and Replace** for BSM version 9.01 do not work in BSM 9.13 or later .

  Workaround: Recreate the queries in the later BSM/APM version.
- In the staging environment, you cannot retrieve any data for reports that query RUM when RUM is pointing to the APM side.

Master Key is Not Set for RTSM

Description: Since the UCMDB was upgraded, the APM upgrade can fail because the master key for RTSM is not set. This error appears as follows:

- During the APM upgrade, the log file contains an error for the ***** Executing step: set_rtsm_master_key** step. The log file is located here: **<HPE APM root directory>\log\upgrade\upgrade.all.log**.
- The **master key is not set** message appears when you open any RTSM page.

Workaround:

1. Start APM.
2. Open the RTSM JMX (DPS in case Distributed APM configuration) (https://localhost:8443/jmx-console/).
3. Locate and open the **UCMDB:service=Security Services** group.
4. Locate the **changeMasterKey** method.
5. Set the Master Key. It must be a string containing 32 characters including a number, special character, and an upper case character.
6. Invoke this method.
7. Restart the **hpbsm_RTSM** process.

Sending Scheduled Reports

Scheduled reports are not sent from the staging servers while they are in staging mode. This prevents multiple reports from being sent. Non-scheduled reports can be sent by opening the **Report Manager**, selecting the report, and clicking the **Email This Report** button.

You can manually modify this setting so that APMdoes send scheduled reports from the staging servers. To do so, enter an email address in the **Platform > Setup and Management > Infrastructure Settings > BSM Evaluation > Alerts mail address** setting.

SISConfigurationEnrichmentUpgrader failure

Description: During APM upgrade, if the SISConfigurationEnrichmentUpgrader reports FAILED, PARTIALLY FAILED, or NOT REQUIRED status, the APM content packs may not automatically upload upon restart.

Workaround: Delete the blockAutoUpload file located in the <HPE APM root directory>\conf\opr\content folder after SISConfigurationEnrichmentUpgrader finished and before APM restart.

Troubleshooting the Upgrade Wizard

Introduction screen

If the introduction screen opens without **Next** or **Back** buttons, close the wizard and reopen it. If repeating this action does not help, restart the wizard.

Upgrade Settings screen

If the server type shown in the upgrade settings screen is not the type you expect, you must reinstall APM on this machine.

Copying Files screen

- Make sure you copy DPS files to the DPS, and Gateway files to the Gateway. Do not accidentally copy Gateway files to the DPS.
- If you forget to copy the **excels** folder (or you copy it to the wrong location), you can copy it later without consequence. If you have not yet installed the Gateway, save the **excels** folder to a temporary location, and copy it to the correct location after you install the Gateway.
- If you have Service Health custom rule jars and you did not copy them (or copied them to the wrong location), after you start APM the online engine fails when calculating HIs or KPIs with the custom

rule. The log files contain errors, and the HIs or KPIs are shown without status. To resolve this, copy the custom rule jars at any stage and then continue with the upgrade.

- If you have SLM custom rule jars and you did not copy them (or copied them to the wrong location), the offline engine fails when calculating HIs or KPIs with the custom rule. The log files contain errors, and the HIs or KPIs are shown without status. To resolve this, copy the custom rule jars and run recalculation of all your SLAs, before the relevant data is purged from the database.

Database Connection - Profile Schema Settings

If you enter the details of the wrong profile database and you run the schema upgrade, the upgrade fails and the following message appears: **The current schema is not compatible with version 8.0.** The differences between your database and the schema will be greater than expected. Restore the Databases, and restart the upgrade.

Schema Upgrade

- If the schema upgrade step fails, follow the on-screen instructions. In most cases, an SQL script is generated that resolves the problems that caused the failure of the schema upgrade.
- If the schema upgrade fails because you have users connected to the database, but the user shown is the current machine, click **Next** and re-run the schema upgrade. If this happens more than a reasonable number of times, you can ask your DBA to kill the connections, and then click **Next**.

Update Environment

- Use the export tool log to verify that the LDAP Database Export/Import tool worked properly, or to see details of problems encountered.
- Server Deployment: If you select the wrong applications, you may fail with memory issues at any point in the upgrade. To fix the incorrect configuration, change the server deployment and restart APM.
- Server Deployment: If you receive a message stating that the machine is not aligned with the current deployment and a restart of APM is required, disregard this message. APM will be restarted as part of the upgrade process at a later stage.
- Login Settings: If you are using a non-default password for RTSM, update all data collectors with the new password when you finish upgrading to the new servers.
- Login Settings: If you re-run the upgrade wizard and enter a different password for RTSM than the one you used the first time, the configuration upgrade (Geo Attributes upgrader) will fail. The logs will contain the following message: **Failed to connect to RTSM**. Re-run the upgrade wizard, and enter the password for RTSM which you used the first time you ran the upgrade.
- Content Pack Import: If the user is not an administrative user, the oprContentUpgrader will fail. In

this case, delete the file OprUpload, and re-run the upgrade wizard using administrative credentials.

- Content Pack Import: If an LDAP was configured in the production environment and is not accessible, you will fail on the oprContentUpgrader. In this case, disable the LDAP and re-run the upgrade wizard.

CMDB Upgrade

- If an upgrader fails, review the following log file: <HPE APM root directory>\odb\runtime\log\upgrade\upgrade.short.log.
- If the CMDB upgrade fails, and the failure requires restoring the database, you only need to restore the CMDB schemas. You do not need to re-run all previous steps of the wizard. Additionally, you need to delete the following directory from the Data Processing Server running the upgrade wizard: HPBSM\odb\runtime.

Start APM

- At this point in the upgrade wizard, when you start APM not all processes are up, and the UI is not available. This is because APM is temporarily in Upgrade mode; at a later stage you will restart APM in Full Mode.
- When the upgrade wizard reaches the Start APM step, certain steps are marked as successful and will not run again. If you want to rerun these steps (for example, if the DB is restored to the backup) remove all files under **<HPE APM root directory>\Temp** that start with **opr**.

  NOTE:
  When you Start or Restart the services in upgrade wizard, the **Initializer: Startup** is failed. To fix this issue, Restart the APM services.

Staging Data Replicator (SDR)

To verify that SDR is working:

1. Open **<SDR root directory>\conf\core\Tools\log4j\sdreplicator\sdreplicator.properties**. Modify the **loglevel** to **debug**.
2. Open **<HPE APM root directory>\conf\core\Tools\log4j\sdreplicator\wde.properties.** Modify the **loglevel** to **debug**.
3. Find the most recent sample in **<SDR root directory>/log/sdrPublishedSamples.log** and make sure that you can locate it in **<HPE APM root directory>/log/wde/wdePublishedSamples.log**. If samples are appearing in both logs, the SDR is working.
4. Modify the **loglevel** settings to **INFO** in the **sdreplicator.properties** and **wde.properties** files.

Data Transfer Tool

- Verify that the SDR is working before running the Data Transfer Tool; you can check the SDR log to see that the SDR is working. If you ran the Data Transfer Tool and the SDR did not run, a message will appear when you click Next (SDR initiation Date warning).
- If you exit the wizard (or the wizard crashes) during the data transfer tool sequence of steps, re-run the tool on the same dates it ran earlier (see upgrade_all.log for the exact times).
- If you decide not to run the Data Transfer Tool, you will have missing data. Take this into account when looking at reports.
- If you did not record the time of the database backup, choose a date prior to the date of backup. You will have no data missing, but the Data Transfer Tool will take longer than necessary.
- When you run the Data Transfer Tool for a second time, you must choose a different path for the temporary folder than the one chosen for the first run.
- If you accidentally enter the credentials of the staging DB and not the production DB, you will receive the following error message: **Operation Failed … FileNotFoundException**. Enter the correct details, and continue.
- The UI allows you to pause the Transferred data upgrade, but actually this does not have any effect.

Verifying Digitally Signed Installation Files

All installation files that are in the format listed below are digitally signed:

- **Windows:** MSI, EXE, DLL, VBS, JS, CPL.
- **Linux:** RPM files only.

To verify that the installation files are original and provided with a code and have not been manipulated by a third party, you can do the following:

For Windows files:

1. Right-click the file and select **Properties**.
2. Select the **Digital Signatures** tab and verify that the name of the signer is Hewlett Packard Enterprise.

For Linux files:

Open a command line, and run the following commands:

rpm -v -checksig ${RPM_FILE_NAME}# rpm -v -qi -p ${RPM_FILE_NAME}

For example:

```
# rpm -v --checksig  HPBsmFndCom1-9.10.320-Linux2.6_64.rpm
```

```
HPBsmFndCom1-9.10.320-Linux2.6_64.rpm:
    Header V3 DSA signature: OK, key ID 2689b887
    Header SHA1 digest: OK (a4b436a86ca52dde34113c964866d5838b50bbc5)
    MD5 digest: OK (59def5f6719a78eac778324bdb0f6f05)
    V3 DSA signature: OK, key ID 2689b887

# rpm -v -qi -p  HPBsmFndCom1-9.10.320-Linux2.6_64.rpm
Name        : HPBsmFndCom1                 Relocations: (not relocatable)
Version     : 9.10.320                          Vendor: Hewlett-Packard Company
Release     : 1                             Build Date: Sun 27 Mar 2011 06:15:37
PM IST
Install Date: (not installed)               Build Host: LABM1AMRND02.devlab.ad
Group       : Applications/System           Source RPM: HPBsmFndCom1-9.10.320-
1.src.rpm
Size        : 298420659                        License: Hewlett-Packard
Development Company, L.P.
Signature   : DSA/SHA1, Sun 27 Mar 2011 07:04:03 PM IST, Key ID 527bc53a2689b887
Summary     : APM Foundations Common Components Pack_1
Description :
APM Foundations Common Components Pack_1
```

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on APM Upgrade Guide (Micro Focus Application Performance Management 9.50)

Add your feedback to the email and click **Send**.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docs.feedback@microfocus.com.

We appreciate your feedback!