Application Performance Management

Software Version: 9.50

Installation 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 Installation Guide. This guide provides a detailed workflow for installing APM.

This guide is for customers who do not have any version of APM.

If you have a previous version of APM, see the APM Upgrade Guide.

How This Guide is Organized

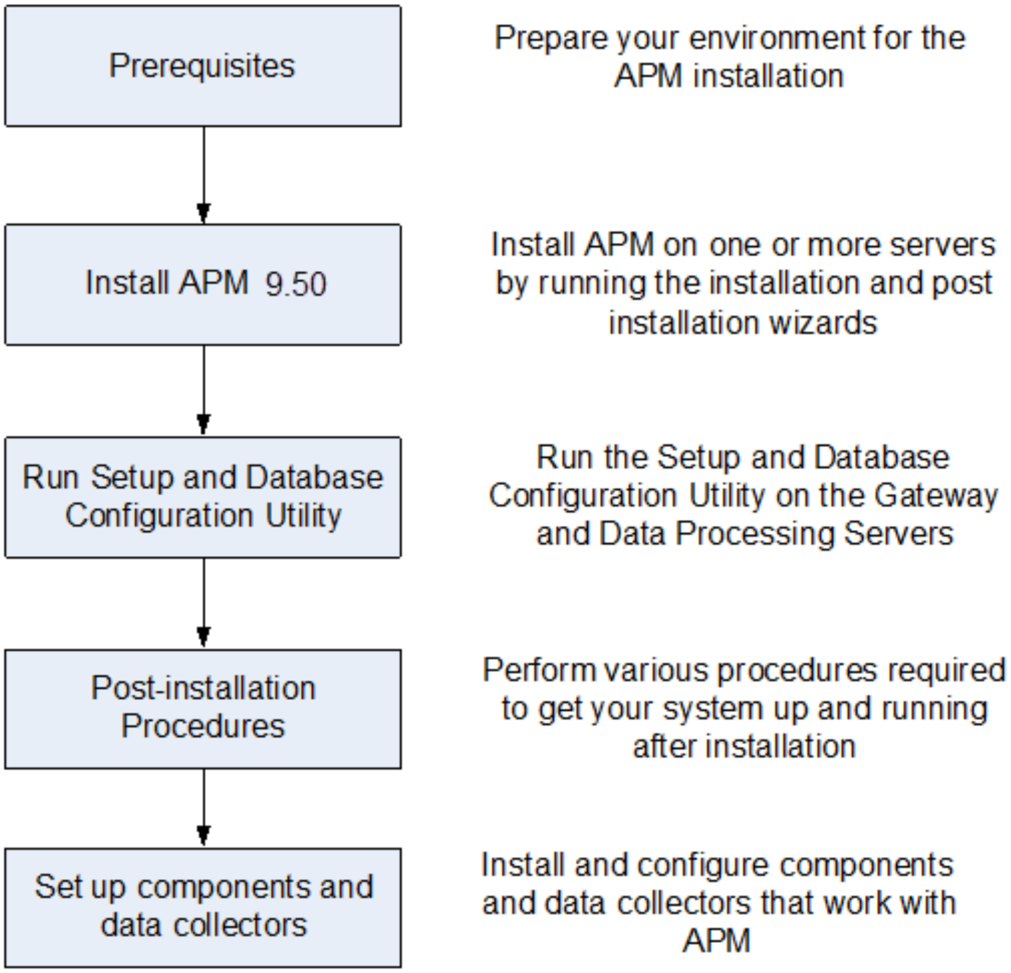
This book is divided into two parts:

- Part I contains the step-by-step workflow for installing APM.
- Part II, the appendix, contains reference information and optional procedures.

Part I: Installation Workflow

Chapter 1: APM 9.50 Installation Overview

The installation of APM 9.50 involves the following main steps:



Prerequisites

Prepare your environment for the APM installation

Install APM 9.50

Install APM on one or more servers by running the installation and post installation wizards

Run Setup and Database Configuration Utility

Run the Setup and Database Configuration Utility on the Gateway and Data Processing Servers

Post-installation Procedures

Perform various procedures required to get your system up and running after installation

Set up components and data collectors

Install and configure components and data collectors that work with APM

Chapter 2: General Prerequisites

Perform the following steps before starting the installation process:

1. Create a 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. 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).

3. Prepare hardware

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

4. Set up web server (optional)

APM installs the Apache web server on all APM Gateway servers during the installation. If you want to use the Apache web server and you have already installed IIS web server, stop the **IIS Web Server** service before installing APM. Do not change the **Startup Type** setting of this service. Do not remove **IIS Web Server** as a role. If you want to use the IIS web server, install and enable it on all Gateway servers before installing APM.

NOTE:
There can only be one running Web server on a server machine that uses the same port as APM. For example, if you use the 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. For more information, see:

- For Linux: Working with the Apache Web Server, on page 55
- For Windows: Working with the IIS Web Server, on page 47

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 47.
- 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.

- 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 unless you are installing APM in silent mode. For details, see Installing APM Silently, on page 69.
- 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: Install APM 9.50

Install APM 9.50 on a set of servers. This set can be either one Gateway Server and one Data Processing Server, or one one-machine server. In the first case, run the wizards on the Data Processing Server first. The wizard directs 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.
- If you are installing APM 9.50 on Windows Server 2008 R2 or 2012 R2:
    1. In **HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system** locate **Enable LUA** and change the value to **0**.
    2. Reboot the machine.

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 Managemen 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 44
- Installing APM on a Linux Platform, on page 53

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

Alternatively, you can run the Installation and Post-Installation wizards in silent mode. For details, see Installing APM Silently, on page 69.

NOTE:
Silent mode is not supported for the Upgrade wizards.

Chapter 4: Post-Installation Procedures

This chapter contains the following topics:

General Post-Installation Procedures

Perform these tasks to complete the installation 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.

- ## Create Profile Database

  You create the profile database schema after running the installation wizards. For more information, see "Creating Databases" in the APM Platform Administration Guide.

- ## Upload additional licenses

  The main APM license is entered during the main APM installation. However, a number of APM applications require additional licenses. To use these applications, obtain licenses from Support site.For more information visit Software Support site (https://softwaresupport.softwaregrp.com).

  You upload the license files in the License Manager. For more information, see "License Manager Page" in the APM Platform Administration Guide.

- ## Configure LW-SSO when load balancer is located in separate domain

  If you are using a load balancer and it is not in the same domain as servers integrating with APM (for example, NNMi, OO), you need to customize a LW-SSO configuration. For details, see "LW-SSO Configuration for Multi-Domain and Nested Domain Installations" in the APM Platform Administration Guide.

- ## Perform hardening procedures

  If you want to secure the communication between APM servers, perform the procedures in "Using TLS in APM” in the APM Hardening Guide.

- ## 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.

- ## Install and Configure System Health

  System Health enables you to monitor the performance of the servers, databases, and data collectors running on your APM system and ensure that they are functioning properly. It is recommended that you install and configure System Health after you deploy APM servers. For details, see the System Health 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%\..\HPOvInstaller\HPEApm_<version>** 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_2017.05.23_15_48_ HPOvInstallerLog.html).

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.

- ## 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.

- Restart APM

  Restart APM by disabling and then enabling all servers. For details, see Starting and Stopping APM, below.

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 > Application Performance Management > Administration > Enable | Disable 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 > Application Performance Managemen > Administration > Configure Application Performance Managemen**. 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.

Configuring Secure Access to APM Reverse Proxy

This chapter discusses only the security aspects of a reverse proxy. It does not discuss other aspects of reverse proxies, such as caching and load balancing.

A reverse proxy is an intermediate server that is positioned between the client machine and the Web server(s). To the client machine, the reverse proxy seems like a standard Web server that serves the client machine’s HTTP or HTTPS protocol requests with no dedicated client configuration required.

The client machine sends ordinary requests for Web content, using the name of the reverse proxy instead of the name of a Web server. The reverse proxy then sends the request to one of the Web servers. Although the response is sent back to the client machine by the Web server through the reverse proxy, it appears to the client machine as if it is being sent by the reverse proxy.

APM supports a reverse proxy in DMZ architecture. The reverse proxy is an HTTP or HTTPS mediator between the APM data collectors/application users and the APM servers.

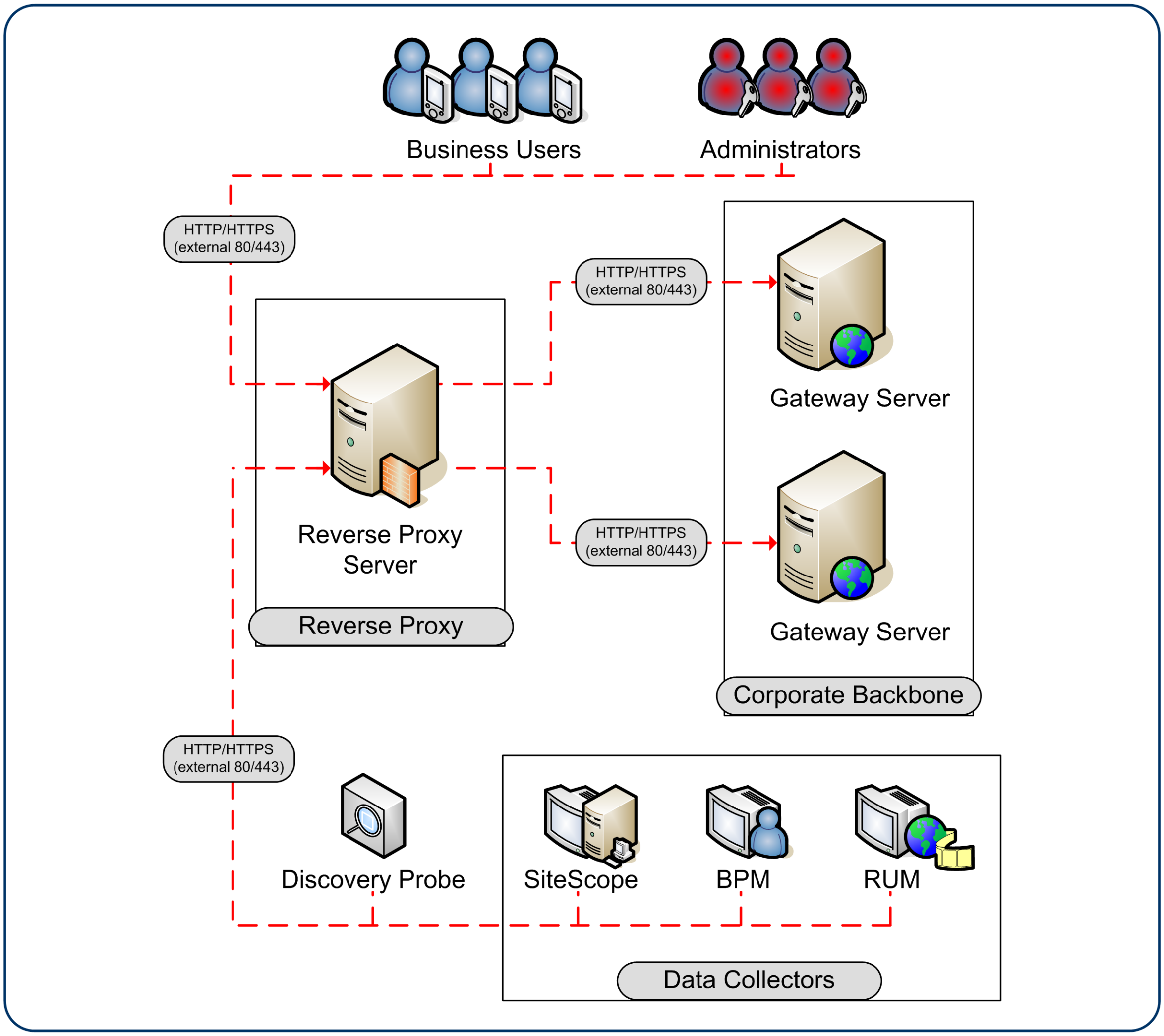
Your data collectors may access APM through the same virtual host or a different virtual host as your application users.

Reverse Proxy Configuration

In this topology, the reverse proxy context is divided into two sections:

- Communication that is redirected to the Virtual Host for Data Collectors.
- Communication that is redirected to the Virtual Host for Application Users.

The use of a reverse proxy is illustrated in the following diagram. Your data collectors may access APM through the same virtual host or a different virtual host as your application users. For example, your environment may use one load balancer for application users and one load balancer for data collectors.



Reverse proxy APM support should be configured differently in each of the following cases:

Scenario #	APM Components Behind the Reverse Proxy
1	Data collectors (Business Process Monitor, Real User Monitor, SiteScope, Data Flow Probe)
2	Application users
3	Data collectors and application users

Reverse Proxy Configuration Workflow

This section describes the overall workflow for configuring a reverse proxy to work with APM servers. The procedure differs depending on the web server of your reverse proxy.

1. If you have a load balancer that is functioning as a reverse proxy, you do not need to configure an additional reverse proxy. For details, see Load Balancing for the Gateway Server, on page 92.
2. Perform the relevant procedure depending on whether your reverse proxy is using the Apache or IIS web server.

   Apache. Configuring a Reverse Proxy - Apache, below.

   IIS. Configuring a Reverse Proxy - IIS, on page 34.
3. Configure APM to support your reverse proxy. For details, see APM Configuration, on page 37.
4. Configure APM to support multiple Secure Reverse Proxies. For details, see Enabling APM to Configure Multiple Reverse Proxies, on page 39.

Configuring a Reverse Proxy - Apache

This section contains the procedures describing how to configure a reverse proxy using apache web server versions 2.2.x.

NOTE:
Securing access to the reverse proxy should be performed as part of the Hardening Workflow. For details, see "Hardening Workflow" in the Hardening Guide.

This section contains the following topics:

- Configuring Apache to Work as a Reverse Proxy , below
- Reference - Support for APM Application Users, on page 31.
- Reference - Support for APM Data Collectors, on page 33.

Configuring Apache to Work as a Reverse Proxy

NOTE:
Securing access to the reverse proxy should be performed as part of the Hardening Workflow. For details, see "Hardening Workflow" in the Hardening Guide.

1. Configure Apache to work as a reverse proxy.

   Apache must be manually configured to function as a reverse proxy.

   For example:

   a. Open the <Apache installation directory>\Webserver\conf\httpd.conf file.
   b. Enable the following modules:
      - LoadModule proxy_module modules/mod_proxy.so
      - LoadModule proxy_http_module modules/mod_proxy_http.so

c. Add the following lines:

```
ProxyRequests off

<Proxy *>
       Order deny,allow
       Deny from all
       Allow from all
</Proxy>
ProxyTimeout 300
```

2. Add support for application users and data collectors as seen in the following example. For more details, see Reference - Support for APM Application Users, on the next page and Reference - Support for APM Data Collectors, on page 33.

Data Collectors:

```
ProxyPass              /ext                    http://DATA/ext
ProxyPassReverse       /ext                    http://DATA/ext
ProxyPass              /topaz/topaz_api        http://DATA/topaz/topaz_api
ProxyPassReverse       /topaz/topaz_api        http://DATA/topaz/topaz_api
ProxyPass              /mam-collectors         http://DATA/mam-collectors
ProxyPassReverse       /mam-collectors         http://DATA/mam-collectors
ProxyPass              /eum-web                http://DATA/eum-web
ProxyPassReverse       /eum-web                http://DATA/eum-web
```

Application Users:

```
ProxyPass              /mercuryam              http://USERS/mercuryam
ProxyPassReverse       /mercuryam              http://USERS/mercuryam
ProxyPass              /hpbsm                  http://USERS/hpbsm
ProxyPassReverse       /hpbsm                  http://USERS/hpbsm
ProxyPass              /topaz                  http://USERS/topaz
ProxyPassReverse       /topaz                  http://USERS/topaz
ProxyPass              /webinfra               http://USERS/webinfra
ProxyPassReverse       /webinfra               http://USERS/webinfra
ProxyPass              /filters                http://USERS/filters
ProxyPassReverse       /filters                http://USERS/filters
ProxyPass              /TopazSettings          http://USERS/TopazSettings
ProxyPassReverse       /TopazSettings          http://USERS/TopazSettings
ProxyPass              /opal                   http://USERS/opal
ProxyPassReverse       /opal                   http://USERS/opal
ProxyPass              /mam                    http://USERS/mam
ProxyPassReverse       /mam                    http://USERS/mam
ProxyPass              /mam_images             http://USERS/mam_images
ProxyPassReverse       /mam_images             http://USERS/mam_images
ProxyPass              /mcrs                   http://USERS/mcrs
ProxyPassReverse       /mcrs                   http://USERS/mcrs
ProxyPass              /rumproxy               http://USERS/rumproxy
ProxyPassReverse       /rumproxy               http://USERS/rumproxy
```

```
ProxyPass              /odb                    http://USERS/odb
ProxyPassReverse       /odb                    http://USERS/odb
ProxyPass              /uim                    http://USERS/uim
ProxyPassReverse       /uim                    http://USERS/uim
ProxyPass              /ucmdb-api              http://USERS/ucmdb-api
ProxyPassReverse       /ucmdb-api              http://USERS/ucmdb-api
ProxyPass              /ucmdb-ui               http://USERS/ucmdb-ui
       connectiontimeout=1000 timeout=1000
ProxyPassReverse       /ucmdb-ui               http://USERS/ucmdb-ui
ProxyPass              /excite-runtime         http://USERS/excite-runtime
ProxyPassReverse       /excite-runtime         http://USERS/excite-runtime
ProxyPass              /excite                 http://USERS/excite
ProxyPassReverse       /excite                 http://USERS/excite
ProxyPass              /OVPM                   http://USERS/OVPM
ProxyPassReverse       /OVPM                   http://USERS/OVPM
ProxyPass              /topaz/sitescope        http://USERS/topaz/sitescope
ProxyPassReverse       /topaz/sitescope        http://USERS/topaz/sitescope
ProxyPass              /cm                     http://USERS/cm
ProxyPassReverse       /cm                     http://USERS/cm
ProxyPass              /eum-web                http://USERS/eum-web
ProxyPassReverse       /eum-web                http://USERS/eum-web
```

NOTE:
If you are using IDM-SSO, you may need to add the following lines (replace siteminderagent in the syntax below with the name of your IDM-SSO vendor):

```
ProxyPass         /siteminderagent    http://USERS/siteminderagent
ProxyPassReverse  /siteminderagent    http://USERS/siteminderagent
```

3. Verify reverse proxy points to APM.
   - Restart Apache
   - Go to http://<RP>/topaz - verify that you see the APM login page. At this point, if you enter your credentials you would see an empty page because APM is not yet configured to work with a reverse proxy.

Reference - Support for APM Application Users

The following table can be used as a reference for application users to connect through the reverse proxy.

Requests for … on the Reverse Proxy Server	Proxy Request to be Served by:
/hpbsm/*	http://[Virtual Host for Application Users]/hpbsm/* https://[Virtual Host for Application Users]/hpbsm/*
/excite/*	http://[Virtual Host for Application Users]/excite/* https://[Virtual Host for Application Users]/excite/*
/excite-runtime/*	http://[Virtual Host for Application Users]/excite-runtime/* https://[Virtual Host for Application Users]/excite-runtime/*
/filters/*	http://[Virtual Host for Application Users]/filters/* https://[Virtual Host for Application Users]/filters/*
/mam/*	http://[Virtual Host for Application Users]/mam/* https://[Virtual Host for Application Users]/mam/*
/mam_images/*	http://[Virtual Host for Application Users]/mam_images/* https://[Virtual Host for Application Users]/mam_images/*
/mcrs/*	http://[Virtual Host for Application Users]/mcrs/* https://[Virtual Host for Application Users]/mcrs/*
/mercuryam/*	http://[Virtual Host for Application Users]/mercuryam/* https://[Virtual Host for Application Users]/mercuryam/*
/odb/*	http://[Virtual Host for Application Users]/odb/* https://[Virtual Host for Application users]/odb/*
/opal/*	http://[Virtual Host for Application Users]/opal/* https://[Virtual Host for Application Users]/opal/*
/OVPM/*	http://[Virtual Host for Application Users]/OVPM/* https://[Virtual Host for Application Users]/OVPM/*
/rumproxy/*	http://[Virtual Host for Application Users]/rumproxy/* https://[Virtual Host for Application Users]/rumproxy/*
/topaz/*	http://[Virtual Host for Application Users]/topaz/* https://[Virtual Host for Application Users]/topaz/*
/TopazSettings/*	http://[Virtual Host for Application Users]/TopazSettings/* https://[Virtual Host for Application Users]/TopazSettings/*

Requests for … on the Reverse Proxy Server	Proxy Request to be Served by:
/ucmdb-api/*	http://[Virtual Host for Application Users]/ucmdb-api/* https://[Virtual Host for Application users]/ucmdb-api/*
/ucmdb-ui/*	http://[Virtual Host for Application Users]/ucmdb-ui/* https://[Virtual Host for Application users]/ucmdb-ui/* Note: If you are using a Reverse Proxy and you have an integration with Universal CMDB, make sure your reverse proxy timeout setting is at least 1000 seconds. For example, in your reverse proxy http.conf file, modify the line that starts with ProxyPass as follows: ProxyPass /ucmdb-ui http://<myAPM GW server>/ucmdb-ui connectiontimeout=1000 timeout=1000
/uim/*	http://[Virtual Host for Application Users]/uim/* https://[Virtual Host for Application Users]/uim/*
/webinfra/*	http://[Virtual Host for Application Users]/webinfra/* https://[Virtual Host for Application Users]/webinfra/*
/eum-web/*	http://[Virtual Host for Application Users]/eum-web /* https://[Virtual Host for Application Users]/eum-web /*

Reference - Support for APM Data Collectors

The following table can be used as a reference for data collectors to connect through the reverse proxy.

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/topaz/topaz_api/*	http://[Virtual Host for Data Collectors]/topaz/topaz_api/* https://[Virtual Host for Data Collectors]/topaz/topaz_api/*
/topaz/sitescope/*	http://[Virtual Host for Data Collectors]/topaz/sitescope/* https://[Virtual Host for Data Collectors]/topaz/sitescope/*
/ext/*	http://[Virtual Host for Data Collectors]/ext/* https://[Virtual Host for Data Collectors]/ext/*

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/cm/*	http://[Virtual Host for Data Collectors]/cm/* https://[Virtual Host for Data Collectors]/cm/*
/mam-collectors/*	http://[Virtual Host for Data Collectors]/mam-collectors/* https://[Virtual Host for Data Collectors]/mam-collectors/*
/axis2/*	http://[Virtual Host for Data Collectors]/axis2/* https://[Virtual Host for Data Collectors]/axis2/* **Note:** Required if SOAP adaptor is used with embedded Run-time Service Model (RTSM) for replication into secure APM via reverse proxy.
/eum-web/*	http://[Virtual Host for Data Collectors]/eum-web /* https://[Virtual Host for Data Collectors]/eum-web /*

NOTE:

- Make sure your reverse proxy supports priority handling logic, which enables a specific expression to be handled before a more generic one, if required. For example, the **/topaz/topaz_api/*** expression must be handled before the **/topaz/*** expression.
- For some reverse proxies, a reverse pass is also required. The reverse pass changes the HTTP or HTTPS headers returned from the server to relative headers. For an example of a reverse pass, see Configuring Apache to Work as a Reverse Proxy , on page 29.

Configuring a Reverse Proxy - IIS

This section contains the procedure describing how to configure a reverse proxy using an IIS web server. Procedures describing steps that are performed in products other than APM are only for example purposes.

NOTE:
Securing access to the reverse proxy should be performed as part of the Hardening Workflow. For details, see "Hardening Workflow" in the Hardening Guide.

This section contains:

Configure IIS to Work as a Reverse Proxy , on the next page

Configure IIS Reverse Proxy to Work with SSL, on the next page

Configure IIS to Require Client Authentication - Optional, on page 37

Configure IIS to Work as a Reverse Proxy

This procedure may differ depending on your version of IIS.

For example:

1. Install the Application Request Routing (ARR) extension. For details, see http://www.iis.net/downloads/microsoft/application-request-routing.
2. Open the IIS Manager.
3. Create a new IIS website, or use the default website.
4. Create a new IIS Server Farm named APM.
   a. Add a new server to the farm with the IP of your APM Gateway server.
   b. When prompted, allow it to create a URL rewrite rule.
5. Enable IIS to function as a proxy.
   a. Select the main tree node (server name) > Application Request Routing Cache > Server Proxy Settings.
   b. Check the **Enable proxy** box.
   c. Set the **HTTP version** to **Pass through**.
   d. Check the **Reverse rewrite host in response headers** box.
   e. Click **Apply**.
6. Verify reverse proxy points to APM.

   Go to http://<Reverse Proxy FQDN>/topaz - verify that you see the APM login page. At this point, if you enter your credentials you would see an empty page because APM is not yet configured to work with a reverse proxy.

Configure IIS Reverse Proxy to Work with SSL

NOTE:
Securing access to the reverse proxy should be performed as part of the Hardening Workflow. For details, see *Hardening Workflow* in the Hardening Guide.

1. Establish trust on the reverse proxy to the CA that issued the server certificate

   Import the CA root certificate of the authority that issued the server certificate for this server into the computer truststore using mmc

   For example:

   a. From the reverse proxy, open the Microsoft Management Console (**Run > mmc**).

   b. Add a snapin (**File > Add / Remove snapin**).

   c. Select Certificates and click **Add**.

   d. Select Computer Account and click **Next**.

   e. Select Local Computer and click **Finish**.

   f. Click **OK**.

   g. Import the certificate

      Import ca.cer into the Trusted Root Certificate Authorities list.

2. Import the server certificate to the Microsoft Management Console

   Import the server certificate you obtained earlier into Personal > Certificates in the Microsoft Management Console.

3. Enable SSL on IIS

   For example:

   a. In the IIS Manager, select your website.

   b. In the actions pane, select **Bindings**

   c. Add an HTTPS binding for port 443

   d. Specify your server certificate in the SSL Certificate field.

4. Configure the Reverse Proxy to Require SSL

   For example:

   a. In the IIS Manager, select your website, and select **SSL settings**.

   b. Check the **Require SSL** checkbox.

5. Configure SSL Offloading

   If your SSL terminates on the reverse proxy, perform the following steps:

   a. Run the following command to configure IIS to allow large data samples (1 MB) to pass through:

      C:\Windows\System32\inetsrv>appcmd.exe set config -section:system.webserver/serverruntime /uploadreadaheadsize:1048576 /commit:apphost

   b. In the ISS Manager, Select the main tree node (server name) > Application Request Routing Cache > Server Proxy Settings

   c. Check the **enable SSL offloading** checkbox.

Configure IIS to Require Client Authentication - Optional

1. Recreate the SSL binding to enable client negotiation

   The previous binding will function, but may have performance issues. This binding enables negotiation, thereby increasing performance when using client authentication.

   a. Remove the current binding using the IIS manager user interface

   b. Run the following commands from the IIS server:

   ```
   c:\windows\system32\inetsrv\appcmd set site /site.name:"Default Web Site"
   /+bindings.[protocol='https',bindingInformation='*:443:']
   ```

   ```
   netsh http add sslcert ipport=0.0.0.0:443 certhash=<your server certificate hash>
   appid={00112233-4455-6677-8899-AABBCCDDEEFF} clientcertnegotiation=enable
   ```

   NOTE:
   You can find the certificate hash from mmc by viewing the thumbprint in the details of the certificate.

2. Configure the Reverse Proxy to Require a Client Certificate

   For example:

   a. In the IIS Manager, select your website, and select **SSL settings**.

   b. In **Client certificates**, select **Require**.

3. Specify the header the reverse proxy passes to APM for client certificate authentication in base64 format

   For example:

   a. From the IIS manager, select your farm and select **Proxy**.

   b. Select the checkbox **Reverse rewrite host in response header**.

   c. In the field **forward encoded client certificate in the following header**, enter the header name **CLIENT_CERT_HEADER**.

   d. Click **Apply**.

APM Configuration

In addition to configuring the reverse proxy to work with APM, you must configure APM to work with the reverse proxy.

NOTE:
APM must be configured only if application users are connected via a reverse proxy to APM. If the reverse proxy is being used for data collectors only, skip the instructions in this section.

To configure APM to work with the reverse proxy:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. Click **Foundations** and select the **Platform Administration** context from the drop-down box.
2. In the Platform Administration - Host Configuration pane, set the following parameters:
   - **Default Virtual Gateway Server for Application Users URL and Default Virtual Gateway Server for Data Collectors URL.** Verify that these parameters represent the URL of the machine (reverse proxy, load balancer, or other type of machine) used to access the Gateway server machine. For example, `http://my_reverse_proxy.example.com:80`.

     If you are using a NAT device to access the Gateway server, enter the full URL of the NAT device. For example, `http://nat_device.example.com:80`.

     Local Virtual Gateway Server for Application Users URL and Local Virtual Gateway Server for Data Collectors URL (optional). If you must use more than one URL (the ones defined for the Default Virtual Server URLs, above) to access the Gateway server machine, define a Local Server URL for each machine through which you want to access the Gateway server machine. For example, `http://my_specific_virtual_server.example.com:80`.

     If the **Local Virtual Services Server URL** parameter is defined for a specific machine, this URL is used instead of the **Default Virtual Services URL** for the specifically-defined machine.
   - **Direct Gateway Server for Application Users Server URL**. Click the **Edit** button and delete the URL in the **value** field.
   - **Direct Gateway Server for Data Collectors URL**. Click the **Edit** button and delete the URL in the **value** field.
3. In the Reverse Proxy Configuration pane, set the following parameters:
   - **Enable Reverse Proxy**. Set this parameter to true. Note that this must be done after the above parameters have been configured.
   - **HTTP or HTTPS Reverse Proxy IPs** . Enter the internal IPs the reverse proxies or load balancers used to communicate with the Gateway server machine.
     - If the IP address of the reverse proxy sending the HTTP/S request is included, the URL returned to the client is either the Default Virtual Server URL or the Local Virtual Server URL (when defined).
     - If no IP addresses are defined for this parameter (not recommended), APM works in Generic Mode. This means that you will only be able to log into APM using the Virtual URL and not directly to the Gateway.

NOTE:
If your reverse proxy and APM Gateway Servers are not in the same domain, you must add the IP of the reverse proxy to the **HTTP or HTTPS Reverse Proxy IPs** parameter. For more details, see "LW-SSO Configuration for Multi-Domain and Nested Domain Installations" in the APM Platform Administration Guide.

To find the internal IP of your reverse proxy or load balancer:

- Log in to APM through the reverse proxy or load balancer.
- Open the log in the following location **<HPE APM Gateway root directory>\log\jboss\UserActions.servlet.log**.
- The IP that appears in the latest **login** line in this log is the reverse proxy or load balancer IP. The entry should have your user name.

4. Increase the reverse proxy timeout.
5. Restart the APM service on the APM Gateway and Data Processing servers.

NOTE:
After you change the APM base URL, it is assumed that the client is initiating HTTP or HTTPS sessions using the new base URL. You must therefore ensure that the HTTP or HTTPS channel from the client to the new URL is enabled.

Enabling APM to Configure Multiple Reverse Proxies

To enable APM to configure multiple reverse proxies:

1. In APM, select **Admin > Platform > Setup and Maintenance >Infrastructure Settings**.
2. Select > **Foundations**.
3. Select **Platform Administration**.
4. In the Platform Administration - Host Configuration table, locate **Default Virtual Gateway Server for Application Users URL** and edit the value by adding a list of reverse proxy URLs with their port number. Separate the items in this list with semicolons.
5. Click **Save**.
6. In the Platform Administration - Reverse Proxy Configuration table, locate **HTTP Reverse Proxy IPs** and edit the value to list all the reverse proxy IP addresses separated by semicolons. If a specific reverse proxy has more than one IP address, list all of its IP addresses separated by commas.

   For example:

<RevProxy1_IP1,RevProxy1_IP2;RevProxy2_IP1,RevProxy2_IP2;...;RevProxyN_IP1,RevProxyN_IP2>

In this example, different delimiters (comma or semicolon) are used to indicate whether an IP address belongs to the same reverse proxy or to the next one.

7. Click **Save**.
8. In the Platform Administration - Reverse Proxy Configuration table, locate **Enable Reverse Proxy** and set the value to **true**.
9. Click **Save**.
10. Restart APM.

Notes and Limitations

APM requires your reverse proxy to have a timeout of at least 300 seconds. This is the default for some versions of Apache, but it may have been reduced. For some processes such as installing a content pack, the timeout should be as high as 1000 seconds (see Configuring Apache to Work as a Reverse Proxy , on page 29).

If you configured APM to work in Generic Mode, all the APM clients must access the APM machine via the reverse proxy.

Specific and Generic Reverse Proxy Mode Support for APM

APM servers reply to application users by sending a base URL that is used to calculate the correct references in the HTML requested by the user. When a reverse proxy is used, APM must be configured to return the reverse proxy base URL, instead of the APM base URL, in the HTML with which it responds to the user.

If the reverse proxy is being used for data collectors only, configuration is required only on the data collectors and reverse proxy, and not on the APM server(s).

There are two proxy modes that control user access to APM servers:

- Specific Mode, on the next page.
- Generic Mode, on the next page.

Specific Mode

This mode should be used if you want to concurrently access APM servers through specific reverse proxies and by direct access. Accessing the server directly means that you are bypassing the firewall and proxy because you are working within your intranet.

If you are working in this mode, each time an application user's HTTP/S request causes APM to calculate a base URL, the base URL is replaced with the value defined for either the **Default Virtual Gateway Server URL** or the **Local Virtual Gateway Server URL** (when defined), if the HTTP/S request came through one of the IP addresses defined for the **HTTP** or **HTTPS Reverse Proxy IPs** parameter. If the HTTP/S request did not come through one of these IP addresses, the base URL that APM receives in the HTTP/S request is the base URL that is returned to the client.

Generic Mode

This mode is used when you try to access the Gateway server via the reverse proxy. Any URLs requested are rewritten and sent back with the virtual IP of the Gateway server.

If you are working in this mode, each time an HTTP/S request causes the APM application to calculate a base URL, the base URL is replaced with the value defined for either the **Default Virtual Gateway Server URL** or the **Local Virtual Gateway Server URL** (when defined).

Note that when using this mode, you must ensure that all APM clients are accessing the APM servers via the URL defined for the **Default Virtual Gateway Server URL** or the **Local Virtual Gateway Server URL** parameters.

Chapter 6: Install and Configure Additional Components

For an end-to-end, high-level workflow for setting up APM, as well as details about APM components and concepts, see the APM Getting Started Guide, available as part of the APM Help.

Use the following references to install and configure additional components:

Item	Resource
APM Platform	To configure the APM platform, see the APM Platform Administration Guide, available as part of the APM Help.
APM Integrations	Information about integrations between APM and other products can be found on the Software Solution and Integration Portal at https://hpe.sharepoint.com/teams/aztec/Portal/index.html
APM Components	• **Real User Monitor:** See the Real User Monitor Installation and Upgrade Guide. • **Business Process Monitor:** See the Business Process Monitor Deployment Guide. • **SiteScope:** See the SiteScope Deployment Guide. • **Diagnostics:** See the Diagnostics Installation and Configuration Guide. • **System Health:** See the System Health Guide. • **Data Flow Probe:** See the Data Flow Probe Installation Guide.

You can access the above resources in the following locations:

- The Planning and Deployment Guides page: Can be found on the APM installation root directory (**Get_documentation.htm**), or from APM, go to **Help > Planning and Deployment Guides**.
- The Downloads Page: **Admin> Platform > Setup and Maintenance > Downloads**.
- The Software Support site https://softwaresupport.softwaregrp.com/.

Part II: 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 page 49.

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 the previous page.

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 47.

Configuring existingResponse 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 69.

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 69.

> **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: Server Deployment and Setting Database Parameters

This appendix contains the following topics:

NOTE:
If you work with Oracle Server, substitute the term **user schema** for the term **database** in this section.

Setup and Database Configuration Utility Overview

You configure your server deployment and create and connect to the databases/user schemas by using the Setup and Database Configuration utility.

You can run the Setup and Database Configuration utility as part of the APM server installation by selecting it in the last page of the post-installation wizard. Alternatively, you can run the Setup and Database Configuration utility independently after server installation. The steps involved are the same for both procedures.

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

If, at a later time, you want to modify any of the database types or connection parameters, you can run the Setup and Database Configuration utility again. The APM server on which you are running the utility must be disabled. For details, see Starting and Stopping APM, on page 23.

After modifying database type or connection parameters, restart all APM servers and data collectors.

NOTE:

- If you modify connection parameters for the management after APM is up and running, the RTSM database may cause serious data loss and integrity problems.
- The startup time for RTSM ODB service takes more than 30 minutes for the first time due to RTSM initialization which loads all the packages from the file system to the database.

Before beginning this procedure, it is recommended that you review Setting Database Parameters, on page 61 and Required Information for Setting Database Parameters, on page 63.

For detailed information on preparing either MS SQL Server or Oracle Server in your system for use with APM, see the APM Database Guide.

NOTE:
Do not use the Setup and Database Configuration Utility instead of or before the Upgrade Wizard. Use it only when the upgrade process is complete and the destination environment is set to production.

Setting Database Parameters

You can set connection parameters for the following databases:

- Management
- RTSM

To configure the connections for these databases, you must:

- Select the type of database you plan to use— MS SQL Server or Oracle Server
- Select to create or re-use the database on MS SQL Server, or user schema on Oracle Server. See Creating Databases, below.
- Specify the connection parameters to the database or user schema. See Connecting to Existing Databases, below.

NOTE:
If you need to change an active management database for APM, contact Support.

Creating Databases

You can either use the Setup and Database Configuration utility to create the databases for you on MS SQL Server or Oracle Server, or you can create these databases manually, directly in the relevant database server (for example, if your organization does not allow the use of administrator credentials during Setup). If you created the databases manually, you must still run the Setup and Database Configuration utility to connect to them.

For instructions on creating databases manually on MS SQL Server, see "Creating and Configuring Microsoft SQL Server Databases" in the APM Database Guide. For instructions on creating user schemas manually on Oracle Server, see "Manually Creating the Oracle Server Database Schemas" in the APM Database Guide.

NOTE:
Each database/user schema created in APM (whether on the same database server or on different database servers) must have a unique name.

Connecting to Existing Databases

When running the Setup and Database Configuration utility, you select whether you want to create a new database/user schema or connect to an existing one.

You generally use the **Connect to an existing schema** option in the following scenarios:

- When connecting to a database/user schema you manually created directly on MS SQL Server/Oracle Server.
- When installing APM in a distributed environment and running the utility on servers subsequent to the first server. In this case, you should run the wizard on the Data Processing Server first and then on the Gateway servers.

You connect to the databases/user schemas that you created during the installation of the first Data Processing Server. After you have connected to the management database, by specifying the same connection parameters that you set during the installation of the first server, the connection parameters for the other databases appear by default in the appropriate screens. Not all databases appear when running on the Gateway Server.

For information on implementing a distributed deployment of APM, see "Deployment Configurations" in the APM Getting Started Guide.

Required Information for Setting Database Parameters

Before setting database parameters, you should prepare the information described in the following sections.

Configuring Connection Parameters for MS SQL Server

You need the following information for both creating new databases and connecting to existing ones:

- **Host name.** The name of the machine on which MS SQL Server is installed. If you are connecting to a non-default MS SQL Server instance in dynamic mode, enter the following: <host_ name>\<instance_name>

  CAUTION:
  There is a twenty six (26) character limit for the **Host name** field while running the utility. If using a host name without a domain name is not appropriate in your environment, perform one of these workarounds:

  - Use the IP instead of the host name in the **Host name** field.
  - Map the host name to the IP in the Windows Hosts file. Use the host name you mapped in the **Host name** field.

- **Port.** The MS SQL Server's TCP/IP port. APM automatically displays the default port, **1433**.
  - If you connect to a named instance in static mode, enter the port number.
  - If you connect to a named instance in dynamic mode, change the port number to **1434**. This port can dynamically listen to the correct database port.
- **Database name.** The name of the existing database that has been manually created, or the name that you will give your new database (for example, APM_Management).

  NOTE:
  Database names starting with numbers are not supported.

- **User name and Password.** (If you use MS SQL Server authentication) The user name and password of a user with administrative rights on MS SQL Server. Note that a password must be supplied.

  TIP:
  We recommend not using the default **sa** user for security reasons.

You can create and connect to a database using Windows authentication instead of MS SQL Server authentication. To do so, you must ensure that the Windows user running the APM service has the necessary permissions to access the MS SQL Server database. For information on assigning a Windows user to run the APM service, see Changing APM Service Users , on page 113. For information on adding a Windows user to MS SQL Server, see "Using Windows Authentication to Access Microsoft SQL Server Databases" in the APM Database Guide.

> **NOTE:**
> In Linux environments, Windows authentication is not supported.

Configuring Connection Parameters for Oracle Server

> **NOTE:**
> If your Oracle Server is on a Real Application Cluster (Oracle RAC), some of the parameters in this section should be assigned different values. For details, see the section about "Support for Oracle Real Application Cluster" in the APM Database Guide.

Before setting database parameters, ensure that you have created at least one tablespace for each user schema for application data persistency purposes, and that you have set at least one temporary tablespace according to the requirements. For details on creating and sizing the tablespaces for APM user schemas, see "Oracle Server Configuration and Sizing Guidelines" in the APM Database Guide.

You need the following information for both creating a new user schema and for connecting to an existing one:

- **Host name.** The name of the host machine on which Oracle Server is installed.

  CAUTION:
  There is a twenty six (26) character limit for the **Host name** field while running the utility. If using a host name without a domain name is not appropriate in your environment, perform one of these workarounds:

  - Use the IP instead of the host name in the **Host name** field.
  - Map the host name to the IP in the Windows Hosts file. Use the host name you mapped in the **Host name** field.

- **Port.** The Oracle listener port. APM automatically displays the default port, **1521**.
- **SID.** The Oracle instance name that uniquely identifies the Oracle database instance being used by APM.
- **Schema name and password.** The name and password of the existing user schema, or the name that you will give the new user schema (for example, APM_MANAGEMENT).

If you are creating a new user schema, you need the following additional information:

- **Admin user name and password.** (to connect as an administrator) The name and password of a user with administrative permissions on Oracle Server (for example, a System user).
- **Default tablespace.** The name of the dedicated default tablespace you created for the user schema.
- **Temporary tablespace.** The name of the temporary tablespace you assigned to the user schema. The default Oracle temporary tablespace is **temp**.

  NOTE:
  To create a new user APM user schema, you must have administrative permissions and CREATE USER, CONNECT, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, UNLIMITED TABLESPACE, CREATE VIEW, and CREATE PROCEDURE privileges on the Oracle Server.

Running the Setup and Database Configuration Utility

You can run the Setup and Database Configuration utility either as part of the APM Installation process or separately. If you run the Setup and Database Configuration utility separately from APM Installation process, note the following important points:

- If the command prompt window is open on the APM server machine, you must close it before continuing with the Setup and Database Configuration utility.
- If you are running this wizard after installation to modify existing configuration and not during initial installation, you must disable APM before running the Setup and Database Configuration utility (select **Start > Programs > Application Performance Management > Administration > Disable Application Performance Management**).
- Use only English characters when entering database parameters.

  NOTE:
  You can also run this utility in silent mode. For details, see Installing APM Silently, on page 69.

To set database parameters and configure server deployment:

1. Launch the Setup and Database Configuration utility in one of the following ways:
   - At the end of the post-installation wizard, select the option to run the Setup and Database Configuration utility.
   - **Windows:** On the APM server, select **Start > Programs > Application Performance Managemen > Administration > Configure Application Performance Managemen**. APM launches the Setup and Database Configuration utility. 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**.
2. Follow the on-screen instructions for configuring the databases.
   a. **License**. If you are running this utility for the first time, you can select to use the evaluation license or download your new licenses. If this is not the first time you are running this utility, you can select to skip this step or download additional licenses. The license file has a .DAT suffix and must be in a local or network location accessible to the server running the utility.

      You can update your licenses after APM is installed in the Licenses Management page of Platform Administration. For details, see "Licenses" in the APM Platform Administration Guide.

> **NOTE:**
> 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.

b. **Server Deployment**. The recommended workflow is to enter your deployment information in the capacity calculator to determine the scope of your deployment and which applications and features you will be running. You can upload the saved capacity calculator Excel file into this page of the utility. The required fields are automatically populated with the data from the capacity calculator, based on your entries in the Excel sheet. For details, see the APM Getting Started Guide.

- **Users**. The number of logged in users determines whether your user load is **small**, **medium**, or **large**.
- **Model**. The number of configuration items in your model determines whether your model is **small**, **medium**, **large**, or **extra-large**.
- **Metric Data**. The number of monitored applications, transactions, locations, and hosts determines whether your metric data load is **small**, **medium**, or **large**.
- **<List of Applications>**. Select or clear the applications to activate or deactivate for this deployment. Clear those applications you are not using to free memory and processor speed for those applications that you are using.

  > **NOTE:**
  > If you do not enable functionality while running this utility, it is not available to any users. For details on the application options, see the tooltips in the capacity calculator.
  >
  > After the installation is complete and you want to change your deployment, you can adjust capacity levels and enable or disable applications and functionality in the Server Deployment page in Platform Administration.

You can also manually enter the information in this page, but it is highly recommended that you use the capacity calculator to determine the scope and capacity of your deployment.

c. **Login Settings**. Enter passwords for the administrator user ("admin") to access APM and the JMX console.

Optionally, set an **Access to RTSM password** to secure communication to the Run-time Service Model from RUM.

> **NOTE:**
> If you change the **Access to RTSM** password during the APM installation, you must similarly change the password in Diagnostics and RUM.

d. **IIS Configuration**. If you are using Microsoft Internet Information Server (IIS), APM requires that the following IIS roles are enabled:

   - ISAPI Extensions
   - ISAPI Filters
   - IIS Management Scripts and Tools
   - Static Content

   If they are already enabled, the IIS Configuration screen is not displayed.

   If any of the roles are not enabled, you can request that they are automatically configured now by selecting **Automatically enable IIS roles** and clicking **Next**.

   If you want to configure them manually, select **Manually enable IIS roles** and click **Next**.

e. **Firewall Configuration**. If you are running APM behind a firewall, when running the utility on a Gateway Server, you have the option of configuring the firewall either automatically or manually.

   - You may need to open additional ports if a firewall is enabled on this server. For details, see "Port Usage" in the APM Platform Administration Guide
   - If you choose to configure manually, no port configuration is executed and you must manually configure on both the Gateway Server and the Data Processing Server.

f. To enable the database connections, you must click **Finish** at the end of the utility.

3. If you ran the Setup and Database Configuration utility as part of the APM server installation, you must start APM on all servers only after successfully setting the parameters for all the databases. For details, see Starting and Stopping APM, on page 23.

   If you ran the Setup and Database Configuration utility to add a new Gateway Server or modify the previously defined database types or connection parameters, restart all APM servers and data collectors after successfully completing the parameter modification process.

   NOTE:
   If you used this utility to modify any databases on a running APM deployment, MyBSM and Service Health will no longer contain any pages and components. To restore MyBSM and Service Health pages and components:

   - Open the following directory: **<Gateway Server root directory>\conf\uimashup\import**. This contains two directories: **\loaded**, and **\toload**.
   - Copy the contents of the **\loaded** directory into the **\toload** directory. Restart APM.

Appendix D: 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:

     HPEApm_9.40_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

6. Log out of and in to Linux (optional). If you are installing APM in a Linux environment, and you specified a non-root user in the post-installation wizard, log out and log in using the non-root user you selected.

7. Run the Setup and Database Configuration Utility Silently.

   a. Open the **emptyRspFile.xml** file.

   b. Under the **configServer** section, enter details related to the database you are planning to configure.

   c. Run the following command to perform the database configuration:

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

8. Enable APM. For details, see Starting and Stopping APM, on page 23.

9. Enabling APM for the first time may take up to an hour. To check the status of APM, use the following URL:

   http://localhost:11021/invoke?operation=showServiceInfoAsHTML&objectname=Foundations%3Atype%3DNannyManager

How to Generate a Response File to Rerun the Post-Installation Wizard and the Setup and Database Configuration Utility Silently

You can create an xml file with the value entries you used when running the Setup and Database Configuration Utility. This file can be used to run the wizard on different machines.

1. Run the Setup and Database Configuration Utility normally on an existing APM system.
2. The response file is generated and stored in the **<HPE APM root directory>/temp** directory or in a location you specified. It is automatically filled in with the values you specified when running the Post-Installation Wizard and the Setup and Database Configuration Utility.
3. You can now run the Post-Installation Wizard and the Setup and Database Configuration Utility on any machine silently with the response file using the following syntax:

   silentConfigureBSM.sh <path to response file>/<response file name>.xml

   > **NOTE:**
   > You can run the two wizards separately by appending the appropriate command as follows:
   >
   > **silentConfigureBSM.sh <path to response file>/<response file name>.xml [postinstall | configserver]**

   The silentConfigureBSM.sh file can be found in the **<HPE APM root directory>/bin** directory.

How to Configure Windows Authentication When Running the Setup and Database Configuration Utility Silently

The Setup and Database Configuration Utility allows you to configure APM to take the database schema credentials directly from the windows authentication credentials. To enable this feature when manually creating a response file, leave the UserName and Password keys for each relevant schema blank. The following example shows the Management schema section of the response file formatted to use windows authentication:

```
        <database name="management">
            <!--Enter 'create' to create a new database or 'connect' to connect to
an existing database-->
            <property key="operation" value="connect"/>
            <property key="dbName" value=" "/>
            <property key="hostName" value=""/>
            <property isEncrypted="true" key="password" value=" "/>
            <property key="server" value=" "/>
            <!--'sid' property is  relevant only if you are using an Oracle
database-->
            <property key="sid" value=" "/>
            <property key="UserName" value=" "/>
            <property key="port" value=""/>
            <!--Please enter your Management Database Server Type:'Oracle' or 'SQL
Server'-->
            <property key="dbType" value=" "/>
            <!--The following four items are only relevant if you are using an
Oracle database-->
            <property key="adminUserName" value=" "/>
            <property isEncrypted="true" key="adminPassword" value=" "/>
            <property key="defaultTablespace" value=" "/>
            <property key="temporaryTablespace" value=" "/>
        </database>
```

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.

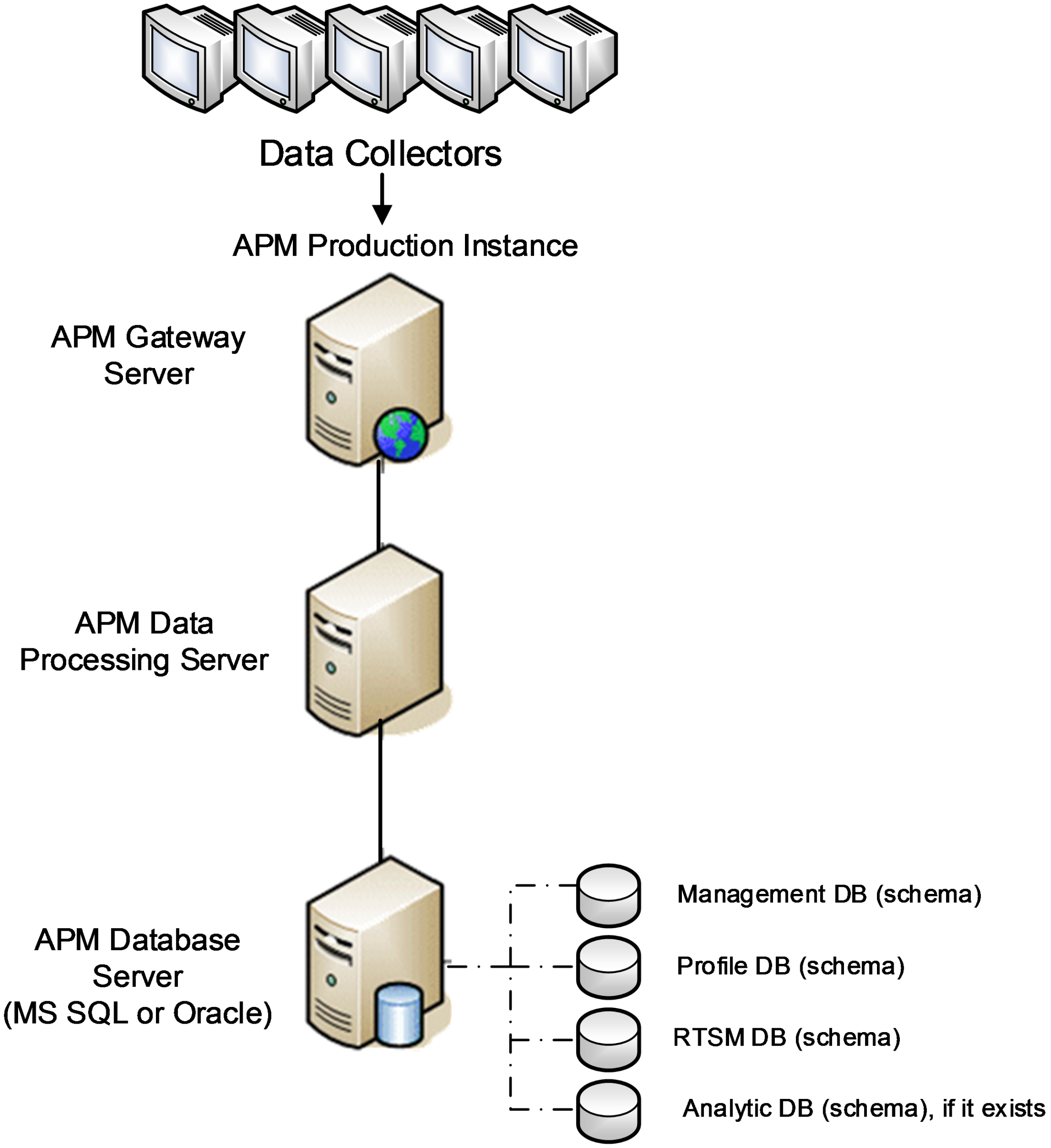
To remove password encryption, enter the passwords in the response file normally and set the value of **IsEncrypted="false"**.

Appendix E: Disaster Recovery for APM

Introduction to Disaster Recovery for APM

You can set up and activate (when necessary) a Disaster Recovery system for your APM system.

The following describes the basic principles and guidelines on how to set up a Disaster Recovery system, and the required steps to make the Secondary APM system become the new Primary APM system.



NOTE:

- Disaster Recovery involves manual steps in moving various configuration files and updates to the APM database schemas. This procedure requires at least one APM Administrator and one database administrator, who is familiar with the APM databases and schemas.
- There are a number of different possible deployment and configurations for APM. To validate that the disaster recovery scenario works in a particular environment, it should be thoroughly tested and documented. You should contact Professional Services to ensure best practices are used in the design and failover workflow for any disaster recovery scenario.
- A disaster recovery machine must use the same operating system and root directory as the original environment.

Preparing the Disaster Recovery Environment

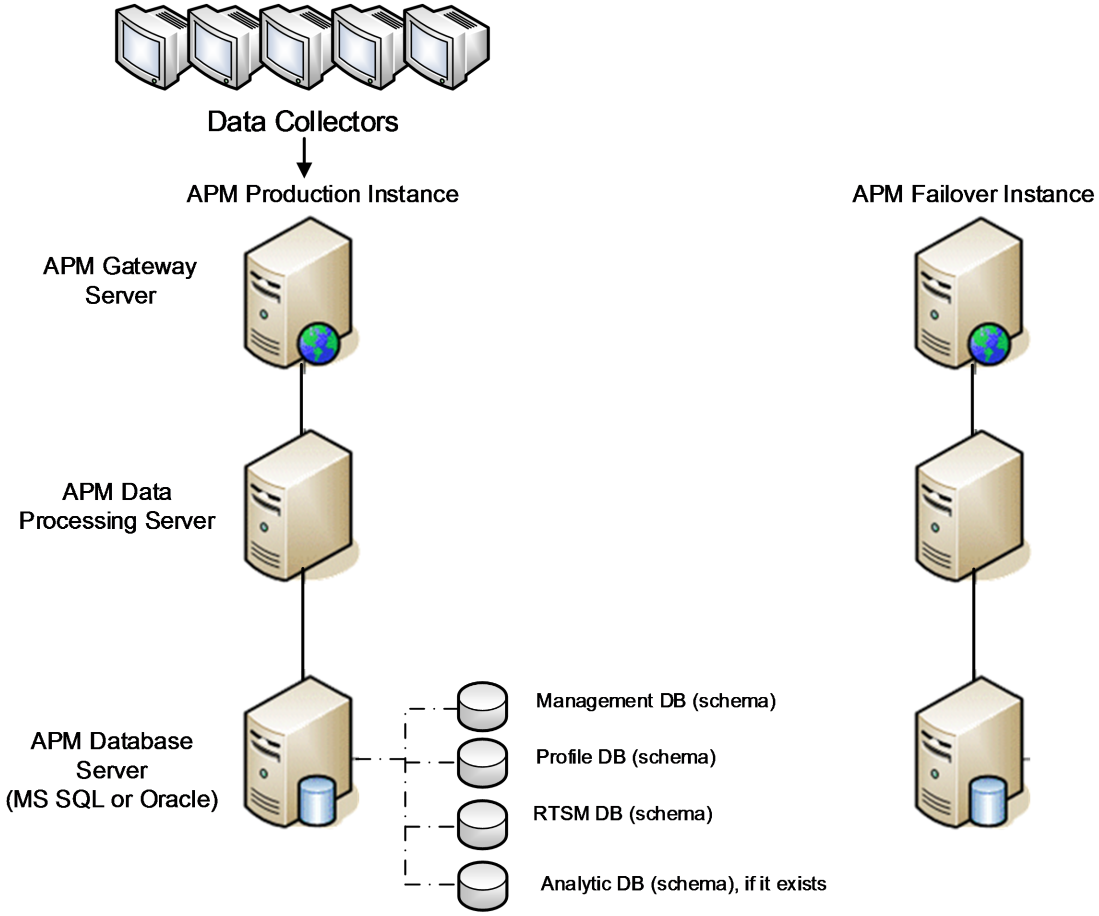
Preparing the Disaster Recovery environment by performing the following steps:

1. ## Install a set of APM servers

   Install a second instance of APM that matches your current production environment.

   - Install exactly the same version of APM in your backup environment as that used in your production environment.
   - The backup environment should be the same as your production environment (for example, one- or two-machine deployment, similar hardware), unless you have more than one GW or DPS in your production environment. In that case, you only need to create one set of APM servers (one GW and one DPS or one one-machine) as your disaster recovery environment.
   - The backup environment must use the same operating system and installation directory as the original environment.
   - Do not run the Server and Database Configuration utility and do not create any databases or enable the servers.

   The following diagram shows a typical APM environment with a Failover system also installed:



2. Copy configuration files from the original system

   Copy files you manually modified in any of the following directories from the APM Production instance to the same server type in the Failover instance:

   - odb/conf
   - odb/content/
   - BLE/rules/<custom rules>.jar

   If you used User Reports to create Excel reports, you must manually copy these to the Failover Instance. The reports are stored in the **<HPE APM root directory>\AppServer\webapps\site.war\openapi\excels\** directory in folders for each customer ID.

   Also copy any other files or directories in the system that you have customized.

   NOTE:
   It is recommended to have at least daily backups of APM servers. Depending on the amount and interval of configuration changes, it may be necessary to incorporate a faster

interval to prevent a large loss of configuration changes in the event of losing the Production instance.

3. Configure the Backup database

Replicate the original database. The original database can now be used as a backup, and the replicated database will be used as the primary database.

NOTE:
It is recommended that only an experienced database administrator perform this phase of the Disaster Recovery scenario.

- **Microsoft SQL–configure database logfile shipping**

  To provide the most up to date monitoring and configuration data, it is critical to enable log file shipping to minimize the time in data gaps. By using log file shipping you can create an exact duplicate of the original database – out of date only by the delay in the copy-and-load process. You then have the ability to make the standby database server a new primary database server, if the original primary database server becomes unavailable. When the original primary server becomes available again, you can make it a new standby server, effectively reversing the servers roles.

  The log file shipping needs to be configured for the following APM databases:

  - Management
  - RTSM
  - Profile (all databases)
  - Analytic (if it exists)

  For details about how to configure log file shipping for Microsoft SQL, refer to the appropriate Microsoft SQL documentation.

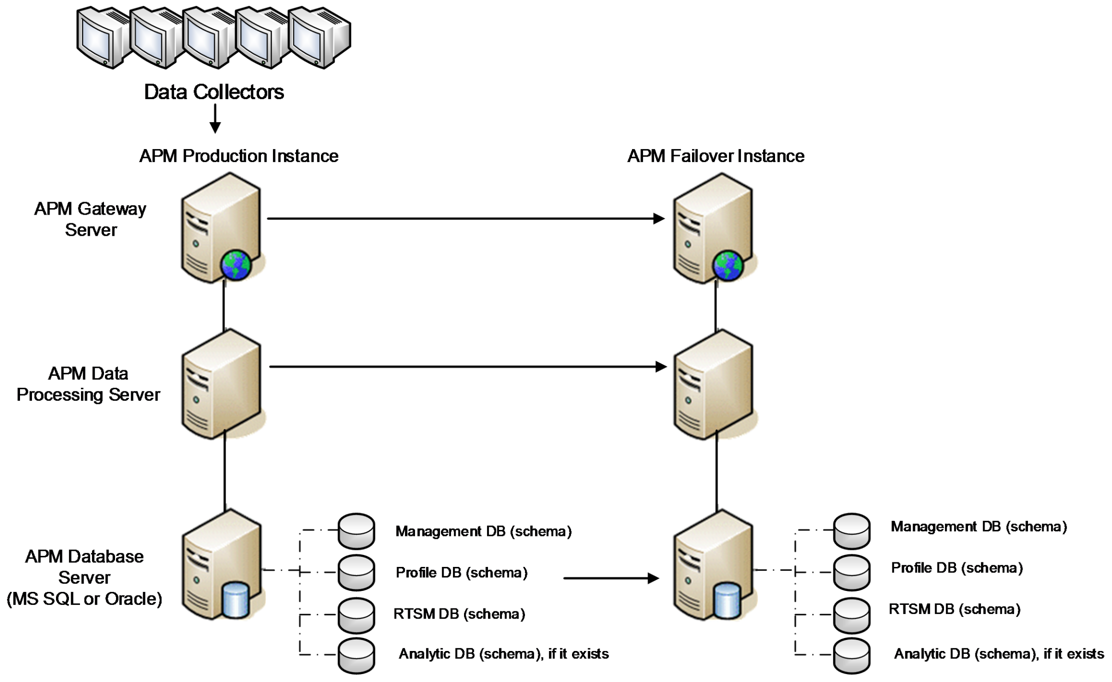
- **Oracle–configure the Standby database (Data Guard)**

  Oracle does not have logs for each schema, but only on a database level, which means that you cannot make a standby database on the schema level and must create copies of the production system databases on your backup system.

  For details about how to configure a Standby database, refer to the appropriate Oracle documentation.

Upon successful completion of the Backup database configuration, the APM Failover Database should be in sync with the APM Production Database.

The following diagram shows the production and Failover systems with database logfile shipping enabled:


Data Collectors
APM Production Instance
APM Failover Instance
APM Gateway Server
APM Data Processing Server
APM Database Server (MS SQL or Oracle)
Management DB (schema)
Profile DB (schema)
RTSM DB (schema)
Analytic DB (schema), if it exists
Management DB (schema)
Profile DB (schema)
RTSM DB (schema)
Analytic DB (schema), if it exists

Cleanup Procedure

Now that you have replicated the original environment, certain settings must be manually modified to avoid confusion between the original environment and the new environment. This procedure cleans up all the machine-specific references in the configurations from the Production instance.

NOTE:

- Before starting the activation procedures, the APM Administrator should ensure that the appropriate license has been applied to the Failover instance and that all the available data collectors can communicate with the Failover instance.
- It is recommended that an experienced database administrator perform the SQL statements included in this procedure.
- The SQL statements below to be run against the management database except for the last 2 steps. The SQL statements in the last 2 steps needs to be run against the RTSM database and the Event database respectively.

1. Delete old information from High Availability (HA) tables.

   Run the following queries on the management database of the disaster recovery environment:

   - **delete from HA_ACTIVE_SESS**
   - **delete from HA_BACKUP_PROCESSES**
   - **delete from HA_PROC_ALWD_SERVICES**
   - **delete from HA_PROCESSES**
   - **delete from HA_SRV_ALLWD_GRPS**
   - **delete from HA_SERVICES_DEP**
   - **delete from HA_SERVICES**
   - **delete from HA_SERVICE_GRPS**
   - **delete from HA_TASKS**
   - **delete from HA_SERVERS**

2. Run the following query on the management database of the DR environment:

   Delete from PROPERTIES where NAME = 'HAServiceControllerUpgrade'

3. Switch references in the Sessions table on the management database of the DR environment to the backup databases.

   a. Run the following query to retrieve all database names:

      SELECT * FROM SESSIONS

where SESSION_NAME like '%Unassigned%'

b. Update the following columns in each received row with the following values:

- **SESSION_NAME:** Replace with the new restored database name (only where SESSION_NAME is like '%Unassigned%'). Use the following script:

  UPDATE SESSIONS set SESSION_NAME='Unassigned<NEW_DB_Server_name><NEW_schema_name><DB_User_name>'

  WHERE SESSION_NAME='Unassigned<OLD_DB_Server_name><OLD_schema_name><old_DB_User_name>'

- **SESSION_DB_NAME:** Replace with the new restored schema name. Use the following script:

  UPDATE SESSIONS set SESSION_DB_NAME='<<NEW_schema_name>'

  WHERE SESSION_DB_NAME='<OLD_schema_name>'

- **SESSION_DB_HOST:** Replace with the new restored database host name. Use the following script:

  UPDATE SESSIONS set SESSION_DB_HOST='<<NEW_host_name>'

  WHERE SESSION_DB_HOST='<OLD_host_name>'

- **SESSION_DB_PORT:** Replace with the new restored port name. Use the following script:

  UPDATE SESSIONS set SESSION_DB_PORT='<NEW_port_name>'

  WHERE SESSION_DB_PORT='<OLD_port_name>'

- **SESSION_DB_SID:** Replace with the new restored session ID name. Use the following script:

  UPDATE SESSIONS set SESSION_DB_SID='<<<NEW_SID_name>>>'

  WHERE SESSION_DB_SID='<OLD_SID_name>'

- **SESSION_DB_UID:** Replace with the new restored name. Use the following script:

  UPDATE SESSIONS set SESSION_DB_UID='<NEW_UID_name>'

  WHERE SESSION_DB_UID='<OLD_UID_name>'

- **SESSION_DB_SERVER:** Replace with the new restored server name. Use the following script:

  UPDATE SESSIONS set SESSION_DB_SERVER='<NEW_server_name>'

  WHERE SESSION_DB_SERVER='<OLD_server_name>'

4. Switch references in the Analytics table on the management database to the backup databases.

   a. Run the following query to retrieve all database names:

   SELECT * FROM ANALYTICS_DATABASES

b. Update the following columns in each received row with the following values:

  - **DB_HOST:** Replace with the new restored database host name. Use the following script:

    update ANALYTICS_DATABASES set DB_HOST=”NEWDatabasehostname’ where DB_HOST=”OLDDatabasehostname”;

  - **DB_SERVER:** Replace with the new restored server name. Use the following script:

    update ANALYTICS_DATABASES set DB_SERVER=’ NEWDatabaseServerName” where DB_SERVER=’ OLDDatabaseServerName’’

  - **DB_SID:** Replace with the new restored session ID name. Use the following script:

    update ANALYTICS_DATABASES set DB_SID =’NEWSID’’ where DB_SID='OLDSID';

  - **DB_PORT:** Replace with the new restored port name. Use the following script:

    update ANALYTICS_DATABASES set DB_PORT= NewPort where DB_PORT=OldPort

5. Delete bus cluster info from PROPERTIES table on the management database.

   Run the following query:

   Delete from PROPERTIES where

   NAMESPACE='MessageBroker' or NAMESPACE='SonicMQ_Namespace' or NAMESPACE='BrokerName' or NAMESPACE like 'hornetq-%'

6. Delete machines from Deployment table on the management database.

   Run the following query:

   DELETE from DEPLOY_HW

7. Setting Manager Values of **SETTING_PARAMETERS** table on the management database.

   Update the URLs and LDAP Server in the SETTING_PARAMETERS table.

   The following table shows the keys in the Setting Manager table that need to be updated if they are present:

SP_CONTEXT	SP_NAME	Description
platform	settings.smtp.server	Name of the SMTP server used for the alert engine
scheduledreports	settings.smtp.server	Name of the SMTP server used for scheduled reports
platform	default.core.server.url	The URL used by data collectors to access the Gateway server in APM.
platform	default.centers.server.url	The URL used by users to access APM.
platform	virtual.centers.server.url	

SP_CONTEXT	SP_NAME	Description
platform	virtual.core.server.url	

For each key in the table, modify and run the following query:

update SETTING_PARAMETERS set SP_VALUE='<new value>'

where SP_CONTEXT='<context value>' and SP_NAME='<name value>'

As follows:

- update SETTING_PARAMETERS set SP_VALUE='<IP of new primary DPS>' where SP_CONTEXT='opr' and SP_NAME='opr.cs.host'
- update SETTING_PARAMETERS set SP_VALUE='<newmachinename>' where SP_CONTEXT='platform' and SP_NAME='settings.smtp.server'
- update SETTING_PARAMETERS set SP_VALUE='<newmachinename>' where SP_CONTEXT='scheduledreports' and SP_NAME='settings.smtp.server'
- update SETTING_PARAMETERS set SP_VALUE='http://<newmachinename>:80' where SP_CONTEXT='platform' and SP_NAME='default.core.server.url'
- update SETTING_PARAMETERS set SP_VALUE='http://<newmachinename>:80' where SP_CONTEXT='platform' and SP_NAME='default.centers.server.url'
- update SETTING_PARAMETERS set SP_VALUE='<eventschemaname>' where SP_CONTEXT='opr' and SP_NAME='opr.db.connection.dbname'
- update SETTING_PARAMETERS set SP_VALUE='<dbhostname>' where SP_CONTEXT='opr' and SP_NAME='opr.db.connection.host'

The last two settings in the table above do not need to be updated unless you are using a load balancer or a reverse proxy. In that case, update the settings as follows:

- update SETTING_PARAMETERS set SP_VALUE='http://<Load Balancer or Reverse Proxy>:80' where SP_CONTEXT='platform' and SP_NAME='virtual.centers.server.url'
- update SETTING_PARAMETERS set SP_VALUE='http://<Load Balancer or Reverse Proxy>:80' where SP_CONTEXT='platform' and SP_NAME='virtual.core.server.url'

8. Update SYSTEM Keys.

   Update the following keys in the SYSTEM table on the management database:

AdminServerURL	http://<DPS1>:port	By default, there is no port number.
GraphServerURL	http://<GW1>/topaz/	
GraphServerURL4.5.0.0	http://<GW1>/topaz/	

application.tac.path	http://<GW1>:port/AdminCenter	By default, the port number is 80.
application.flipper.path	http://<GW1>:port/monitoring	By default, the port number is 80.

For each value in the table, modify and run the following query:

update SYSTEM set SYS_VALUE='<new value>' where SYS_NAME='<key>'

where **<new value>** is the new URL in the format of the original URL.

For example:

update SYSTEM set SYS_VALUE='http://<newmachine>:port' where SYS_NAME='AdminServerURL'

NOTE:
The default port number is 80.

9. Empty and update tables on the RTSM database.

   This procedure cleans up all the machine-specific references in the RTSM configuration tables.

   Run the following SQL statements against the RTSM database:

   - **update CUSTOMER_REGISTRATION set CLUSTER_ID=null**
   - **truncate table CLUSTER_SERVER**
   - **truncate table SERVER**
   - **truncate table CLUSTERS**

Configure the New Environment

1. Run the Server and Database Configuration utility

Run the Server and Database Configuration utility on each machine to re-initialize the needed tables in the database. To run the Server and Database Configuration utility, select **Start > Alll Programs > Application Performance Management > Administration > Configure Application Performance Management.**

> **NOTE:**
> When running the Server and Database Configuration utility, make sure to reconnect to the same databases that were created for the Failover environment (that is, the one to which the backup data was shipped). Possible complete loss of configuration data will result if trying to run this on the Production instance.
>
> Run the Server and Database Configuration utility on the machines in the same order that APM was originally installed in the failover environment.

2. Enable APM

Enable APM on the new servers.

3. Run the Post Startup Cleanup procedure to disable any obsolete hosts that are not part of the Failover instance

To disable obsolete hosts:

a. In APM, go to **Admin > Platform > Setup and Maintenance > Server Deployment** and select **To Disable Machine**.

b. Disable any obsolete hosts.

4. Repeat Hardening Procedures (optional)

If your original environment was hardened, you need to repeat the hardening procedures on the new environment.

The reverse proxy procedures do not have to be repeated.

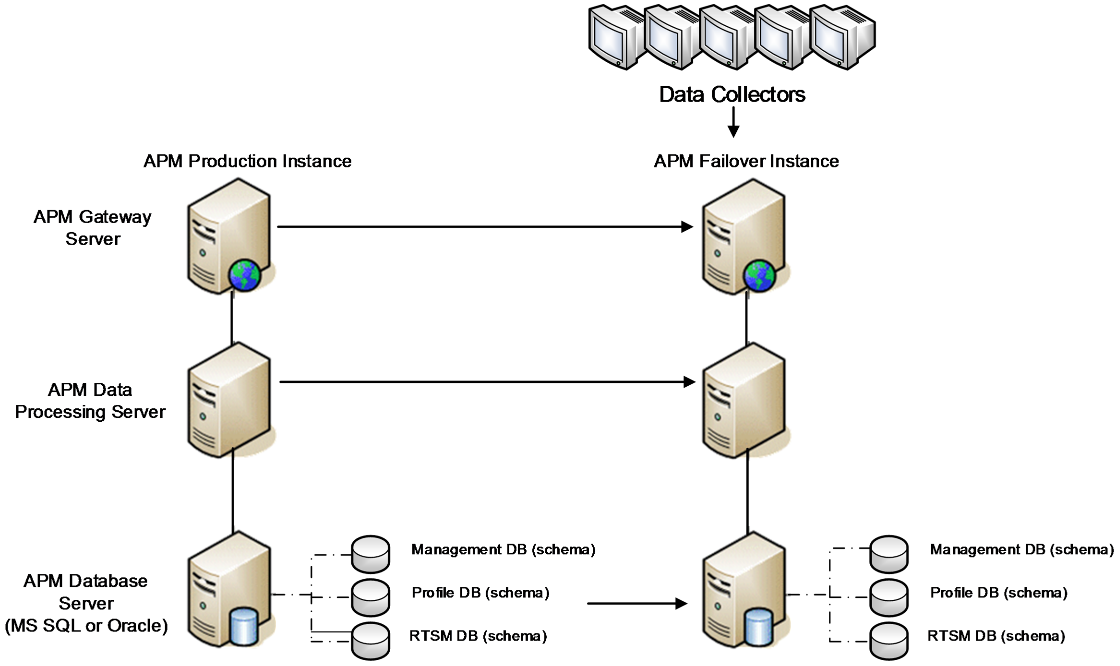
For details, see the APM Hardening Guide.

Configure Data Collectors

1. Configure data collectors.

Configure all the data collectors, including Business Process Monitor agents, Real User Monitor engines, SiteScopes, OM, Service Manager, and Operations Orchestration (if installed on a separate server) to work with the Failover instance. For details, see the relevant documentation for each data collector.

The following diagram shows a fully activated Failover instance:



2. Configuring failover data collector connections.

If any of the data collectors also experienced a failure and were moved to different machines, the new URLs must be communicated to the APM servers. This is done in various applications in APM. For example:

Data Collector	Procedure
SiteScope	Reconnect the SiteScope servers to the APM server from the SiteScope console.
Business Process	Reconnect the BPM servers to the APM server from the BPM console.

Data Collector	Procedure
Monitor	
Real User Monitor	Reconnect the RUM servers to the APM server from the RUM console.
Operations Orchestration	On the Operations Orchestration server, adopt the configuration to reflect the new APM server according to the procedure described in the Solutions and Integrations guide.
Service Manager	On the Service Manager server, adopt the configuration to reflect the new APM server according to the procedure described in the Solutions and Integrations guide.

Appendix K: High Availability for APM

This appendix contains the following topics:

Overview of High Availability Options

You can improve your system availability and reliability using high availability options that combine multiple servers, external load balancing, and failover procedures.

Implementing a high availability configuration means setting up your APM servers so that service is continuous despite power outages, machine downtime, and heavy load.

Load balancing and high availability can be implemented in one-machine or distributed deployments. You configure load balancing by adding an additional Gateway Server and high availability by adding a backup Data Processing Server.

You can install two typical APM environments and connect to one database.

High availability is implemented in two layers:

- **Hardware infrastructure.** This layer includes redundant servers, networks, power supplies, and so forth.
- **Application.** This layer has two components:
  - **Load balancing.** Load balancing divides the work load among several computers. As a result, system performance and availability increases.

    External load balancing is a software and hardware unit supplied by an outside vendor. This unit must be installed and configured to work with APM applications.
  - **Failover.** Work performed by the Data Processing Server is taken over by a backup server if the primary server or component fails or becomes temporarily unavailable.

  Implementation of load balancing and failover is discussed in detail throughout this chapter.

NOTE:
The Professional Services offers consulting services to assist customers with APM strategy, planning and deployment. For information, contact a representative.

Load Balancing for the Gateway Server

When you install multiple APM Gateway Servers, APM can utilize external load balancing mechanisms to help ensure the even distribution of processing and communication activities across the network. This is particularly important in cases of high load, to avoid overwhelming any single server.

> **NOTE:**
> We recommend installing APM behind a load balancer or reverse proxy. This enables additional security options and can simplify disaster recovery and upgrade procedures.

This section includes the following topics:

Configuring Load Balancing, below

Notes and Limitations, on page 94

Configuring Load Balancing

1. Create two virtual hostnames. The virtual hostname must be a fully qualified domain name (FQDN), in the format **<servername>.<domainname>**. This requirement is necessary to support Lightweight Single Sign On authentication, which is enabled by default.

   The first host name is for accessing the APM Web site on the Gateway Server. This URL can be distributed to APM users. The second host name is for the data collectors to access the Gateway Server. This URL must be used when configuring data collectors to communicate with APM.

2. Enter the relevant load balancer host names in the Infrastructure Settings for the virtual servers. To do so, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, choose **Foundations**, select **Platform Administration - Host Configuration table**:

   - **Default Virtual Gateway Server for Application Users URL.** Virtual host name for the APM Web site. The Gateway Server you are working on must be able to resolve this Virtual IP address. This means that **nslookup** for the **virtual host name for the application users** should return name and IP address when executed on this Gateway Server.

   - **Default Virtual Gateway Server for Data Collectors URL.** Virtual host name for Data Collectors. All data collectors must be able to resolve this Virtual IP address. This means that **nslookup** for the **virtual host name for the Data Collectors** should return name and IP address when executed on data collector server.

3. In the Reverse Proxy Configuration pane, set the following parameters:

   - **Enable Reverse Proxy parameter = true.**

   - **HTTP Reverse Proxy IPs**

     Add the internal IP addresses of the Load Balancers to this setting.

   - If the IP address of the load balancer sending the HTTP/S request is included, the URL returned to the client is either the Default Virtual Server URL or the Local Virtual Server URL (when defined).
   - If no IP addresses are defined for this parameter (not recommended), APM works in Generic Mode. This means that you will only be able to log into APM using the Virtual URL and not directly to the Gateway.

   NOTE:
   If your load balancer and APM Gateway Servers are not in the same domain, you must add the IP of the reverse proxy to the **HTTP or HTTPS Reverse Proxy IPs** parameter. For more details, see "LW-SSO Configuration for Multi-Domain and Nested Domain Installations" in the APM Platform Administration Guide.

   To determine the internal IP of your load balancer:

   a. Log in to APM through the load balancer.
   b. Open the log in the following location **<HPE APM Gateway root directory>\log\EJBContainer\UserActionsServlet.log**.
   c. The IP that appears in the latest login line in this log is the internal load balancer IP. The entry should have your user name.

4. After changing the reverse proxy settings, restart the APM service on the APM Gateway and Data Processing servers.

   NOTE:
   If your load balancer allows you to choose between Full-NAT and Half-NAT topologies, choose **Full-NAT**.

5. Configure the load balancer for data collector access. All data collectors must be able to access the Virtual IP of the Load Balancer. Use the standard settings for the load balancer, but set the following:
   - We recommend using a round robin algorithm in order to balance the load on all APM gateway servers.
   - Use the following KeepAlive URI:
     - Send String: **GET /ext/mod_mdrv_wrap.dll?type=test**
     - Receive String: **Web Data Entry is up**
6. Configure the load balancer for user access.
   - Use the standard settings for the load balancer, but set persistency to **stickiness by session enabled** or **Destination Address Affinity** (depending on the Load Balancer). If neither of these options are available and the choice is between **Cookie based** stickiness and **IP based** stickiness, then we recommend trying **IP based** stickiness. If this is not done properly, you may experience intermittent user interface failures.

- Use the following KeepAlive URI:
  - Send String: **GET /topaz/topaz_api/loadBalancerVerify_centers.jsp**
  - Receive String: **Success**

Notes and Limitations

- APM supports hardware and virtual appliance based load balancers. A hardware load balancer solution is preferred for performance reasons.All load balancers must be able to configure sticky session for users and being able to configure URL based health monitors.
- If you use two load balancers for failover, you must ensure that you configure the hostnames of both load balancers on the DNS server machine. You can then specify the machine name, hostname's FQDN, or URL of either load balancer when this information is required for the data collectors, or in the browser to open the APM site.
- If two Gateway servers are installed into different drive paths, for example, one was installed onto the C:\ drive and the other onto the E:\ drive, APM may not be accessible.

  Workaround: Create a duplicate path on the **C:\ drive by copying E:\<HPE APM root directory>\conf\settings** to **C:\<HPE APM root directory>\conf\settings.**
- If you use two load balancers for failover, and the load balancers each work with more than one server type, you should define a unique virtual hostname on each load balancer for each server type, map the virtual hostnames to the actual hostnames of the corresponding servers, and ensure that you configure all the virtual hostnames on the DNS server machine. You can then specify either of the relevant virtual hostnames for each data collector, or in the browser to open the APM site.
- When a load balancer or reverse proxy is configured, ensure that it can be reached from all APM servers (Gateway and Data Processing Servers) with the virtual addresses specified for the connections.

High Availability for the Gateway Server

Application Performance Management provides high availability for the Gateway Servers to ensure that data gets to its destination and that the users can use APM applications in the event of a server failure.

Protected Delivery for Incoming Data

APM provides protected data delivery for monitored data. Protected data delivery means that the data is not deleted from one data store until it is forwarded to, and stored in, the next data store.

> **NOTE:**
> The Professional Services offers best practice consulting on this subject. For information on how to obtain this service, contact your representative.

APM supports the following mechanisms to help ensure high availability for the raw data:

- If the Web server of the Gateway Server machine fails, the data is either redirected to another Gateway Server by the load balancer, or is queued on the data collector until the Web Server is up.
- If the Web server of the Gateway Server machine receives the data, but the bus is down, the data is stored on the data collector until the bus is up again.
- If the bus receives the data, but the monitoring data loader is down, the data is stored on the bus until the monitoring data loader is up again. The data is then sent to the database.

High Availability for Service Health

Application Performance Managemen provides high availability for Service Health on the Gateway Server to ensure that users can continue working with Service Health even if a Gateway Server fails while a user is in the middle of a session.

When a user logs in to APM and starts working with Service Health, the session information is registered on a specific Gateway Server and the load balancer sends all communications related to that session to the same Gateway Server. If that Gateway Server fails, the load balancer redirects the session to another Gateway Server and the session is re-registered on the new Gateway Server. The user continues working without any interruption of service and without having to log in to APM again.

The load balancer for the Gateway Server must be set with **stickiness by session enabled**. For details, see Configuring Load Balancing, on page 92.

> **CAUTION:**
> It is possible that in certain situations, the transition from one Gateway Server to another could take a few seconds. During this transition, errors may be received for some user actions.

High Availability for the Data Processing Server

To ensure high availability, you should install a backup Data Processing Server. For APM to function properly in the event of a primary Data Processing Server failure, the backup Data Processing Server can take over.

> **TIP:**
> It is recommended that when you install the primary and backup Data Processing Servers, the servers should be comparable in terms of hardware, memory, and performance.

If the high availability for the Data Processing Server is enabled and a backup server is defined, in the event that one or more services becomes unavailable, the High Availability Controller performs automatic failover and moves the services to the backup server. The server retrieves the current configuration from the management database and continues to provide the services as the new active Data Processing Server.

You can also use the JMX console to manually reassign services to the backup server. You may want to do this if for example, you are planning a maintenance on one of the Data Processing Servers. Moving the services manually can reduce APM's downtime.

> **NOTE:**
> When deploying a new APM installation, the first Data Processing Server started becomes the default server for the assigned Data Processing Server services—that is, it becomes the primary Data Processing Server. If a second Data Processing Server is started, you can assign it to act as a backup server.

This section includes the following topics:

Services Assigned to the Server

Various processes are assigned to the Gateway and Data Processing Servers. Each process is responsible for running specific services. You can use the JMX console to view the services running on the APM servers or on a specific server, such as the Data Processing Server.

To view services via the JMX Web console:

1. In a Web browser, open:

   http://<Data Processing Server machine name>:29000
2. When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
3. In the **Topaz** section, select **service=hac-manager.**
4. Under **java.lang.String listAllAssignments()** from the database, click **Invoke**.

   If you want to view the services of a specific server, such as the Data Processing Server, enter the name of the server in the parameter value. If you want to view all services, leave the parameter value for the server name empty.

The processes running on the server are displayed in a table. The JMX online table contains the following columns:

Column Name	Description
Service	The name of the assigned service.
Customer	The ID of the customer to which the service is assigned. The default customer ID for an individual APM system (one not managed by Software-as-a-Service) is 1. A service with a customer id of -1 is a global service used by all customers in a SaaS deployment.
Process	The name of the Data Processing Server and the name of the JVM process handling the service. The length of time the server has been running and the last time it was pinged are also displayed.
Assigned	Whether the service assignment is currently active or not, the date the service was assigned, and the length of time it has been assigned are displayed.
State	The current state of the service. Valid states are: 1 – Stopped 2 – Starting 3 – Stopping 4 – Running -1 – Failed -2 – Failed to stop

Column Name	Description
	-3 – Failed to start The date that the service acquired the state, and the length of time that it has been in the state are displayed.
Srv. Sign	Server signature.
State Sign	State signature (should match the server signature).

Services Managed by the High Availability Controller (HAC)

The Data Processing Server services that can be managed by HAC are described in the following table, including:

- Name of the process in JVM
- Name the High Availability Controller (HAC) uses for the process
- The services running on the process
- A description of the process

JVM Process Name	HAC Process Name	Service Name	Description of Service Location of Log File
Mercury AS	mercury _as	KPI_ ENRICHMENT	KPI_Enrichment service is responsible for adding dashboard KPIs to CIs that were added to the model by external monitoring systems. The KPIs to add and the CIs to which the KPIs are added are configurable.
		BSM_DT	BSM_DT handles the configured downtimes in the system. Downtimes can be configured onto CIs and can be configured to affect alerts, events, reports, KPI calculations, and monitoring.
		VERTICALS	Verticals service is for SAP that ensures compatibility with APM. SAP service links data retrieved from SiteScope and Business Process Monitors to SAP related entities brought from the RTSM.

JVM Process Name	HAC Process Name	Service Name	Description of Service Location of Log File
		EUM_ADMIN	EUM_ADMIN handles End User Management Administration where Business Process Monitors and Real User Monitors are configured for monitoring.
mercury_ odb	odb	BSM_ODB	The RTSM is a central repository for configuration information that is gathered from the various APM and third-party applications and tools. This information is used to build APM views.
hpbsm_ bizImpact	businessimpact_ service	BIZ_IMPACT	The Business Impact component enables you to see the business CIs and SLAs that are impacted by another CI in Service Health.
		LIV_SERVICE	Local Impact View enables you to also create local impact views in Service Health. These are independent of all other views. When you modify indicator definitions on a CI within a local impact view, this has no effect on this CI in all other views.
hpbsm _offline _engine	offline_ engine	NOA	The New Offline Aggregator service validates and synchronizes new tasks for the offline aggregator on an hourly or daily basis.
hpbsm _marble _ supervisor	marble_ supervisor	DASHBOARD	Dashboard service on the Data Processing Server is responsible for online business logic calculations for Service Health.
hpbsm_ pmanager	pmanager	PM	The Partition and Purging Manager splits fast-growing tables into partitions at defined time intervals. After a defined amount of time has elapsed, data in a partition is no longer accessible for use in APM reports. After an additional, defined amount of time, that

JVM Process Name	HAC Process Name	Service Name	Description of Service Location of Log File
			partition is purged from the profile database.
hpbsm_ pi_engine	pi_engine	PI_ENGINE	The Service Health Analyzer engine component searches for anomalies over the baseline behavior of the system.
hpbsm_ basel_ engine	basel_engine	BASELVALIDATOR	The baseline validator validates baseline tasks against metadata and add/removes tasks if needed.

Configuring Automatic Failover

You can configure automatic reassignment of services running on a primary Data Processing Server to a backup Data Processing Server. To configure the automatic reassignment of services running on a primary Data Processing Server to a backup Data Processing Server, you must:

- Define a backup Data Processing Server in the JMX console.
- Enable automatic failover.

  NOTE:
  If you enable automatic failover and set the keep alive timeout to less than ten minutes, this can cause APM services to move to the backup server after a restart. To prevent this from happening, when disabling APM, shut down the backup server before the primary server. When enabling APM, enable the primary server and verify that all services have started before enabling the backup server.

Defining a Backup Server

You must use the JMX console to define or remove a backup Data Processing Server. You can also view your high availability configurations.

To use the JMX console to define a backup server:

1. In a Web browser, open:
   http://<Data Processing Server machine name>:29000

   When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
2. In the **Topaz** section, select **service=hac-backup.**
3. Locate **addBackupServer** and enter the following values:

- **primaryServerName**. The name of the primary server.
- **backupServerName**. The name of the backup server.

Use the machine name (not the FQDN) for both these parameters. If you are unsure of the machine name, you can use the **listservers** method described below to retrieve the name of the machines already configured.

4. Click **Invoke**.

To remove a backup server:

1. Follow steps 1 and 2 above for accessing the JMX and **hac-backup** service.
2. Locate removeBackupServer and enter the following value:

   primaryServerName. The name of the primary server for which you are removing the backup server.
3. Click **Invoke**.

To view your high availability configuration:

1. Follow steps 1 and 2 above for accessing the JMX and **hac-backup** service.
2. Locate **listservers** and click **Invoke**.

The result displays a list of **Servers** and **Backup Servers**. If there are no backup servers defined or if high availability is not enabled, you get a message saying automatic failover is disabled.

Enabling Automatic Failover

You enable automatic failover either using the Infrastructure Settings in the APM interface or in the JMX console. You can also use the JMX console to check whether high availability is enabled.

To enable automatic failure in Infrastructure Settings:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings.**
2. Choose **Foundations**, select **High Availability Controller**, and locate the **Automatic Failover Enabled** entry in the General Properties table.
3. Modify the value to **true**. The change takes effect immediately.
4. Specify the other parameters in the table according to your needs. The details of each parameter are in the table.

To enable automatic failover in the JMX:

1. In a Web browser, open:
   http://<Data Processing Server machine name>:29000

   When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
2. In the **Topaz** section, select **service=hac-backup.**
3. Locate **void updateAutomaticFailoverEnabled ()**, select **True**, and click **Invoke**.

To check whether automatic failover has been configured:

1. Follow steps 1 and 2 above for accessing the JMX and **hac-backup** service.
2. Locate **boolean retrieveAutomaticFailoverEnabled ()**, click **Invoke**.

Reassigning Services with JMX Console

You can move services between Data Processing Servers as server availability and resource issues arise. Reassigning services can also limit downtime during maintenance of the Data Processing Servers.

You do not have to have high availability enabled to perform this procedure and the source and destination servers do not have to have been configured for high availability.

To use the JMX console to reassign services between Data Processing Servers:

1. In a Web browser, open:
   http://<Data Processing Server machine name>:29000

   When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
2. In the **Topaz** section, select **service=hac-backup.**
3. Locate **moveServices()** and enter the following values:
   - **customerId.** The default customer ID for a regular APM installation is **1**. Software-as-a-Service customers should use their customer ID.
   - **srcServer**. The name of the source server from where you are moving services.
   - **dstServer**. The name of the destination server to where you are moving the services.

     Use the machine name for both these parameters. If you are unsure of the machine name, you can use the **listservers** method described above to retrieve the name of the machines already configured.
   - **groupName**. Leave this parameter value blank.
4. Click **Invoke**. All services running on the source server are moved to the destination server.
5. Restart the online engine (MARBLE) processes after moving them to the destination server to ensure that the model remains synchronized.

Manually Reassigning Services

CAUTION:
This section is for advanced users only.

You can manually reassign services running on a primary Data Processing Server to a backup Data Processing Server should it be necessary. Since a service can only be active on one Data Processing

Server, you must either remove the existing assignment, or make it inactive, before reassigning the service to a different Data Processing Server.

To reassign a service, you can either add a new assignment, or activate a previously defined, but inactive, assignment.

> **TIP:**
> You can check that services have been reassigned, activated, or inactivated correctly by viewing the service status in the JMX Web console. For details, see Services Assigned to the Server, on page 96.

Removing a Service’s Assignment

Removing a service’s assignment deletes the entry from the HA_TASKS table in the management database so that it must be added as a new assignment if you wish to use it again in the future.

To remove a service’s current assignment:

1. In a Web browser, open:
   http://<Data Processing Server machine name>:29000

   When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
2. In the **Topaz** section, click **service=hac-manager.**
3. Under **removeAssignment()**, enter the following data:
   - **customer_id.** The default customer ID for an individual APM system is **1**.Software-as-a-Service customers should use their customer ID in this field.

     > **NOTE:**
     > The customer_id for the PM and NOA services is always -1, as they are services assigned to the system as a whole, as opposed to a specific customer.

   - **serviceName.** The name of the service for which you are removing the current assignment.
   - **serverName.** The name of the Data Processing Server to which the service is currently assigned.
   - **processName.** The name of the process (such as **mercury_as**, **mercury_online_engine**, **mercury_offline_engine**, **topaz_pm**).
4. Click **Invoke**. The assignment for the service is removed from the specified Data Processing Server.

Changing the Status of an Assigned Service

You can leave the assignment of a service to a specific Data Processing Server in the HA_TASKS table in the management database, but make it active or inactive by changing its assigned value.

NOTE:
The HA_TASK_ASSIGN table from previous versions is obsolete. Use the HA_TASKS table.

To change the assigned value of an existing assignment:

1. In a Web browser, open:
   http://<Data Processing Server machine name>:29000

   When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
2. In the Topaz section, click **service=hac-manager**.
3. Under **changeAssignment()**, enter the following data:
   - **customerId.** The default customer ID for a regular APM installation is **1**. Software-as-a-Service customers should use their customer ID.

     The customer_id for the PM and NOA services is always -1 as they are services assigned to the system as a whole, as opposed to a specific customer.
   - **serviceName.** The name of the service for which you are changing the assignment value.
   - **serverName.** The name of the Data Processing Server to which the service is assigned.
   - **processName.** The name of the process.
   - **assignValue.** The assigned value for the assignment. Any number between -9 and 9 is valid. The value **1** makes the assignment active and any other number makes it inactive.
4. Click **Invoke**. The assignment for the service is changed according to the **assignValue** entered.

Adding an Assignment for a Service

You can add an assignment for a service to a specific Data Processing Server and either activate it immediately, or keep it inactive until needed. This is useful when working with a primary and a backup Data Processing Server. Assignments for all the services can be created for each server, with the assignments to the primary Data Processing Server being active, and the assignments to the backup Data Processing Server being inactive.

To add a new assignment for a service:

1. In a Web browser, open:
   http://<Data Processing Server machine name>:29000

   When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
2. In the Topaz section, click **service=hac-manager.**
3. Under **addAssignment()**, enter the following data:
   - **customer_id.** The ID of the customer for which the service is to be assigned. The default customer ID for an individual APM system (that is, one not managed by Software-as-a-

Service) is **1**.

> **NOTE:**
> The customer_id for the PM and NOA services is always -1 as they are services assigned to the system as a whole, as opposed to a specific customer.

- **serviceName.** The name of the service you are assigning.
- **serverName.** The name of the new Data Processing Server to which the service is being assigned.
- **processName.** The name of the process.
- **assignValue.** The assigned value for the assignment. Any number between -9 and 9 is valid. The value **1** makes the assignment active and any other number makes it inactive.

4. Click **Invoke**. The assignment for the service is added for the specified Data Processing Server.

Manually Disabling Data Aggregator Services

The data aggregator can be disabled in System Health (preferred method). However, if you need to disable data aggregator services but either do not have or cannot use System Health, you can perform this manual procedure.

To disable the offline aggregation and business logic engine services on the Data Processing Server:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, choose **Foundations**.
2. Select **Offline Aggregator.**
3. Edit the **Run Aggregator** parameter. Change the setting to **False**. The change takes effect immediately.

Configuring APM Data Collectors in a Distributed Environment

This section describes how to configure the Application Performance Managemen data collectors to work in a distributed deployment.

Business Process Monitor and Real User Monitor

For Business Process Monitors to perform their work, you must specify the Gateway Server URL in the BPM Admin Console application on each host machine on which the Business Process Monitor is running. Edit the Gateway Server URL entry in the Configure Instance page for each Business Process Monitor instance. For more information, see "Application Performance Management Registration Properties Area" in the Business Process Monitor Administrator’s Guide.

For Real User Monitors to perform their work, APM requires you to specify the Gateway Server URL in the Real User Monitor Web Console. For more information, see "APM Connection Settings" in the Real User Monitor Administration Guide.

Specify the Gateway Server address as follows:

- If you install one Gateway Server, specify the URL of this machine.
- If you cluster two or more Gateway Servers behind a load balancer, specify the URL of the load balancer.

If you use two load balancers for failover, specify the URL of either load balancer, and ensure that you configure the host names of both load balancers on the DNS server machine.

SiteScope

For SiteScopes to perform their work, you must specify the Gateway Server URL in each SiteScope profile, using APM System Availability Management (**Admin > System Availability Management**). For details, refer to "Configuring the Connection" in the SAM part of the APM User Guide.

If you use a load balancer and have defined virtual IPs or URLs, you use the virtual IPs or URLs when defining the Gateway Server URL. If you use two load balancers for failover, specify the URL of either load balancer and ensure that you configure the hostnames of both load balancers on the DNS server machine.

For more information on configuring high availability for SiteScope, see the the SiteScope Failover Guide.

Appendix L: Uninstalling APM Servers

This appendix contains the following topics:

- Uninstalling APM, below
- Uninstalling a Build Patch (Rolling Back), on page 111

Uninstalling APM

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 **Uinstall**, 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).

   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 121.

4. Access the Windows Registry Editor by selecting **Start > Run**. Enter **Regedit**.

   During installation, the value of the Windows Registry key **HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ReservedPorts** was updated to include the following port ranges required by APM: 1098-1099, 8009-8009, 8080-8080, 4444-4444, 8083-8083, 8093-8093.

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

   > **TIP:**
   > When working with the registry, it is recommended that you back it up before making any changes.

Uninstalling APM servers in a Linux environment

1. Log in to the server as user **root**.
2. Stop all APM servers.
3. To access the uninstall program, type: **cd /opt/HP/BSM/installation/bin**
4. Run the following script to uninstall in UI mode: **./uninstall.sh**. To peform 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**.

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

Uninstalling a Build Patch (Rolling Back)

This procedure explains how to uninstall a build patch. For example, this means rolling back from APM 9.41 to APM 9.40. Follow the appropriate instructions depending on your operating system.

> **NOTE:**
> When you uninstall a patch, the L-Core version does not revert to the previous version

To roll back a APM patch to a previously installed version - Windows:

1. If you have smart card authentication enabled, it must be disabled before you begin uninstalling a patch. For details, see the Smart Card Authentication Configuration Guide, which can be found on the Planning and Deployment Documentation page (**Help > Planning and Deployment**) or the Software Support site (https://softwaresupport.softwaregrp.com/).
2. Stop the APM service on all servers and confirm that they are stopped.
3. Stop the web server process on all servers (IIS Admin Service for IIS; Apache service for Apache).
4. Select the build patch to remove from **Control Panel > Programs and Features > View Installed Updates**.

   To run this command in silent mode, execute **<HPE APM root directory>\installation\<Patch_Name>\bin\uninstall.bat -i silent**.
5. When the uninstall process is complete, restart the machine if requested. Verify that APM services are not running.
6. Delete the temporary internet files on each browser that accesses APM.
7. Run the Configuration Wizard to reconfigure APM.

   Click **Start > Programs > Application Performance Managemen> Administration > Configure Application Performance Managemen**.
8. Start the APM service.
9. Reload the required TQL.

   As part of the uninstall process, a required TQL was removed and must be redeployed. If this is not done, the BSM_DT service will not start. To redeploy the TQL:

   a. Make sure APM is started and the odb service has a status of **STARTED**.
   b. Open the following JMX console:

      <DPS Machine FQDN>:21212/jmx-console/HtmlAdaptor
   c. In the JMX console, select **UCMDB:service=Packaging Services**.
   d. In the method **deployPackages**, enter the following parameters:

      customerId = 1 (unless it is a "SAAS" enviroment) packagesNames = BSMDowntime

e. Select **invoke**

f. Verify that the **BSM_DT** service has started.

10. Make sure to uninstall or rollback any updated data collectors as well.

To roll back an APM service pack or intermediate patch to a previously installed version - Linux:

1. Change the Linux user to **root** before rolling back.
2. Stop BSM as follows:

   /opt/HP/BSM/scripts/run_hpbsm stop
3. Run the uninstall script as follows:

   /opt/HP/BSM/installation/<Patch_Name>/bin/uninstall.sh

   To run this script in silent mode, use the command:

   /opt/HP/BSM/installation/<Patch_Name>/bin/uninstall.sh -i silent
4. Delete the temporary internet files on each browser that accesses APM.
5. Reconfigure APM by opening a terminal command line and launch:

   /opt/HP/BSM/bin/config-server-wizard.sh
6. Start the APM service.

Appendix N: 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, below
- Switching the Linux User, on the next page

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 O: Switching Web Servers

If you have already installed APM, and want to switch your web server type, perform the procedure below.

> **NOTE:**
> If you have enabled smart card authentication and want to switch your web server from Apache to IIS or vise versa, you need to first disable smart card authentication. You can re-enable smart card authentication after you have switched web servers. For details on how to enable and disable smart card authentication, see "Smart Card Authentication" in the APM Platform Administration Guide.

1. Stop all APM Gateway and Data Processing servers. For details, see Starting and Stopping APM, on page 23.
2. If you are moving from IIS to Apache, stop the IIS service or select a different port in the post-installation wizard in the next step.
3. If you are moving from Apache to IIS, configure IIS. For more information, see:
   - Working with the Apache Web Server, on page 55
   - Working with the IIS Web Server, on page 47
4. Run the Post-Installation wizard and select the new web server type on the appropriate screen.

   The post-installation wizard can be run from the following location: **<HPE APM root directory>\bin\postinstall.bat**. However, if the wizard 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).
5. Start all APM Gateway and Data Processing servers.
6. If you are moving from Apache to IIS, restart the IIS service.

Appendix P: Troubleshooting

This appendix contains the following topics:

Troubleshooting Resources

- **Installation log files.** For details, see Check installation log files, on page 21.
- **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.

OutOfMemory error occurs in the hpbsm_RTSM process

Solution:

In the bin/odb_vm_params.ini file, increase the maximum size of the memory allocation pool (-Xmx param) by 1Gb and restart APM. If it doesn't resolve the issue, increase the maximum size of the memory allocation pool (-Xmx param) until the issue is resolved.

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 47.
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\**).

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 Installation 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!