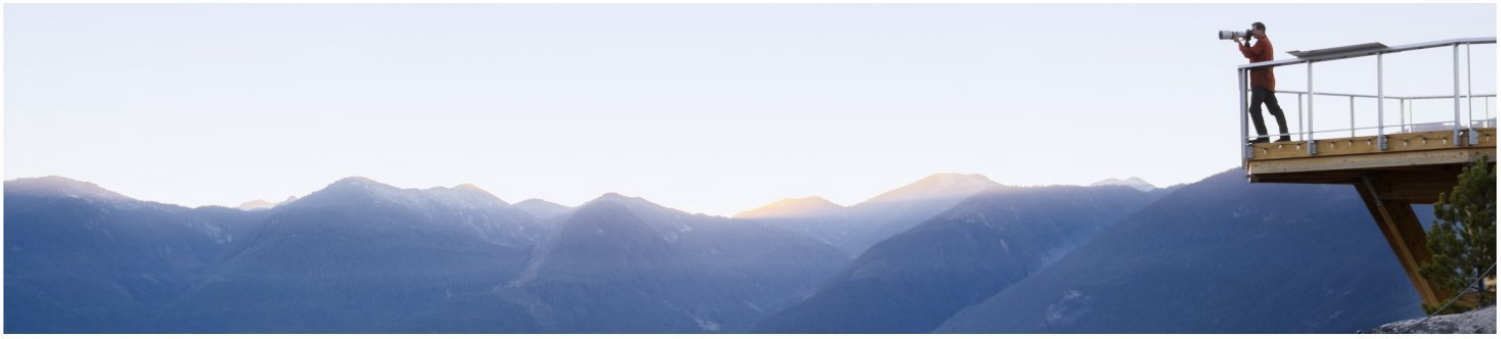
Hewlett Packard Enterprise

# Application Performance Managment

Version 9.40, Released August 2017

## Hardening Guide

Published September 2017



## Legal Notices

### Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE 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. Valid license from HPE 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 and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

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.

iPod is a trademark of Apple Computer, Inc.

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

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

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

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 check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=.

This site requires an HPE Passport account. If you do not have one, click the **Create an account** button on the HPE Passport Sign in page.

## Support

Visit the HPE Software Support website at: **https://softwaresupport.hpe.com**

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software 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 website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE 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 that you register as an HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to **https://softwaresupport.hpe.com** and click **Register**.

To find more information about access levels, go to:
**https://softwaresupport.hpe.com/web/softwaresupport/access-levels**

## HPE Software Integrations and Solutions

Visit the Integrations and Solutions Catalog at **https://softwaresupport.hpe.com/km/KM01702731** to explore how the products in the HPE Software catalog work together, exchange information, and solve business needs.

# Contents

# Chapter 1: Introduction to Hardening

This chapter introduces the concept of a secure APM platform and discusses the planning and architecture required to implement a secure platform. It is strongly recommended that you read this chapter before proceeding to the following chapters, which describe the actual hardening procedures.

The APM platform is designed so that it can be part of a secure architecture, and can therefore meet the challenge of dealing with the security threats to which it could potentially be exposed.

The hardening guidelines deal with the configuration required to implement a more secure (hardened) APM platform. The hardening guidelines relate to both single machine (where all APM components are installed on the same machine) and distributed (where all APM components are installed on separate machines) deployments of APM. You can also invoke dedicated Gateway deployment, in which several Gateway servers are assigned different tasks.

The hardening information provided is intended primarily for APM administrators, and for the technical operator of each component that is involved in the implementation of a secure APM platform (for example, the Web Server). These people should familiarize themselves with the hardening settings and recommendations prior to beginning the hardening procedures.

**Note:** In this document, the term *reverse proxy* also refers to *load balancing* in Layer 7 load balancing except for BBC channel reverse proxy configuration

# Deploying APM in a Secure Architecture

Several measures are recommended to securely deploy your APM servers:

- **DMZ architecture using a firewall**

  The secure architecture referred to in this document is a typical DMZ architecture using a device as a firewall. The basic concept of such an architecture is to create a complete separation, and to avoid direct access between the APM clients and the APM servers.
- **Secure browser**
  - **Firefox**

    Firefox in a Linux environment must be configured to securely handle Java scripts, applets, and cookies. TLS communication protocol Transport Layer Security protocol secures the connection between the client and the server. URLs that require a TLS connection start with HTTPS instead of HTTP.
  - **Autocomplete**

    The 3 major browsers ignore autocomplete=off in web forms.

    IE: http://blogs.msdn.com/b/ieinternals/archive/2013/09/24/internet-explorer-11-changelist-change-log.aspx

    Chrome: http://googlechromereleases.blogspot.com/2014/04/stable-channel-update.html

    Firefox: https://bugzilla.mozilla.org/show_bug.cgi?id=956906

As a result, when logging in to APM you may, depending on your browser configuration, be prompted to remember your login credentials.

If you are an end user of the APM and do not wish to have your login credentials remembered, they need not be; indicate when prompted by your browser that you do not wish to have your login or password information saved by the browser. Often you can instruct your browser not to prompt you in the future for this site.

It is often possible to configure your browser to not prompt you to remember passwords at all, if you wish to disable this ability entirely. This can often be configured either in the browser itself or via corporate IT policy. Refer to your browser documentation or contact your System Administrator for more details.

- **Secure browser**

  Internet Explorer in a Windows environment and Firefox in a Linux environment must be configured to securely handle Java scripts, applets, and cookies. TLS communication protocol Transport Layer Security protocol secures the connection between the client and the server. URLs that require an TLS connection start with HTTPS instead of HTTP.

- **Reverse proxy architecture**

  One of the more secure and recommended solutions is to deploy APM using a reverse proxy. APM fully supports reverse proxy architecture as well as secure reverse proxy architecture.

The following security objectives can be achieved by using a reverse proxy in DMZ proxy HTTP/HTTPS communication with APM:

- No APM logic or data resides on the DMZ.
- No direct communication between APM clients and servers is permitted.
- No direct connection from the DMZ to the APM database is required.
- The protocol used to communicate with the reverse proxy can be HTTP or HTTPS. HTTP can be statefully inspected by firewalls if required.
- A static, restricted set of redirect requests can be defined on the reverse proxy.
- Most of the Web server security features are available on the reverse proxy (authentication methods, encryption, and others).
- The reverse proxy screens the IP addresses of the real APM servers as well as the architecture of the internal network.
- The only accessible client of the Web server is the reverse proxy.
- This configuration supports NAT firewalls.
- The reverse proxy requires a minimal number of open ports in the firewall.

The reverse proxy provides good performance compared to other bastion host solutions. It is strongly recommended that you use a reverse proxy with APM to achieve a secure architecture. For details on configuring a reverse proxy for use with APM, see "Configuring Secure Access to APM Reverse Proxy" on page 25.

If you must use another type of secure architecture with your APM platform, contact HPE Software Support to determine which architecture is the best one for you to use.

# Notes and Recommendations

**Notes:**

- **Prerequisites.** To best use the hardening guidelines given here for your particular organization, do the following before starting the hardening procedures:
  - Evaluate the security risk/security state for your general network, and use the conclusions when deciding how to best integrate the APM platform into your network.
  - Review the entire guide, especially Chapter 2, "Hardening Workflow" on page 9.
- **Log management**. APM uses the log4j framework for managing log files. If you wish to change the locations of log files, these can be set in the log4j appenders, which are located in **<APM root directory>\conf\core\Tools\log4j**. There is a separate directory for each process, for example **EJB** for the JBoss application server.
- **Security officer.** The security officer is a user who has security privileges to view sensitive information in the system. The security officer is typically not a regular APM user and receives access to configure certain sensitive reporting information, such as which RUM transaction parameters to include or exclude from certain reports (For example Session Details or Session Analyzer). For details, see "Security Officer" in the APM Platform Administration Guide.

  The Security Officer can see the parameters and decide to expose them in the reports, but once they are exposed in the reports, anyone with access to these reports will be able to see this data, so it is imperative that the application being monitored encrypts sensitive data, such as passwords, credit card numbers, and identity numbers.
- **Changing the encryption algorithm**. You can change the encryption algorithm used by APM, but only before running the configuration wizard. Open the encryption properties file, **<APM root directory>\conf\encryption.properties**, and choose one of the predefined crypt configuration entries (**crypt.conf.x**) by setting **crypt.conf.active.id** to the appropriate index. If you want to add another entry, follow the standard Java Cryptography Extension (JCE) format.
- The hardening procedures are based on the assumption that you are implementing only the instructions provided in this guide, and not performing other hardening steps not documented here.
- Where the hardening procedures focus on a particular distributed architecture, this does not imply that this is the best architecture to fit your organization's needs.
- It is assumed that the procedures included in the hardening guide will be performed on machines dedicated to the APM platform. Using the machines for other purposes in addition to APM may yield problematic results.

**Recommendations:**

- Isolate APM servers in their own internal segment behind a firewall since the traffic between the various APM servers is not encrypted.
- Follow all security guidelines for LDAP servers and Oracle databases.
- Run SNMP and SMTP servers with low permissions.

**Note:** SNMP and mail traffic may not be secure.

- If you are using an Apache web server, see http://httpd.apache.org/docs/2.4/new_features_2_4.html for an overview of the new features in Apache HTTP Server 2.4.

# Chapter 2: Hardening Workflow

This section describes the overall workflow needed to harden the HPE Application Performance Management environment. The procedures in this book should not be performed outside of the context of this workflow.

1. **Hardening prerequisites**
   - **Verify APM functionality.** Verify that the APM environment is fully functioning before starting the hardening procedures. This includes the basic data flow into and out of APM.
   - **Define security requirements.** Before starting the hardening process, define what areas of your environment you want to secure (with TLS).
   - **Review recommendations and notes.** For details, see "Notes and Recommendations" on page 7.
2. **Configure Security Infrastructure Settings**

   We recommend that you review and configure the security infrastructure settings available in APM. For more information on these settings, see "General Security Recommendations for APM" on page 13.
3. **Obtain server certificates for the APM virtual gateway server URLs**

   Obtain a server certificate for each of the following front-end URLs that you want to secure: one for users to access APM, and one for data collectors to access APM. For details, see "Issuing TLS Certificates " on page 17.

   **Note:** If your TLS termination points are not the front-end URLs (APM virtual gateway server URLs), you need to issue server certificates for these termination points as well.

   The server certificates must be issued into the exact FQDNs. Later, these same FQDNs must be entered as your default URLs as follows:

   a. Log in to APM.

   b. Select **APM Console > Admin > Platform > Setup and Maintenance > Infrastructure Settings**.

   c. Click **Foundations** and select **Platform Administration** from the drop down list.

   d. In the Platform Administration - Host Configuration table, type the secured URLs in the following two rows:
      - Default Virtual Gateway Server for Application Users URL
      - Default Virtual Gateway Server for Data Collectors URL

   For example: If your URL is **https://bsmUsers.mycompany.com:443**, you would issue a certificate to **bsmUsers.mycompany.com**.
4. **Obtain root CA certificate(s)**

   Obtain the root CA certificates from the root, and any intermediate, authorities that issued the server certificates above.
5. **Configure TLS connection using the server certificates**

   Install the server certificates on the termination points of TLS. This may be a load balancer, a reverse proxy, or a APM Gateway server.

a. **Load Balancer.** Install the certificates on the termination points of TLS (this is usually the load balancer).
b. **Reverse Proxy.** Perform the procedure to configure the reverse proxy to work with TLS.
   i. **IIS.** See *Configure IIS Reverse Proxy to Work with TLS* in the APM Installation Guide.
   ii. **Apache.** See *Configuring a Reverse Proxy - Apache* in the APM Installation Guide.
c. **APM Gateway servers.** Refer to the following information:
   - For IIS web server. The Microsoft Web site (http://www.iis.net).
   - For Apache web server. See "Configuring Secure Access to Apache" on page 24.

6. **Establish trust to the Certificate Authority**

   On all APM Gateway servers, establish trust to the Certificate Authority that issued the server certificates above. Restart the servers on which you preformed this procedure.

   **Note:** The same procedure must be performed in both the JRE and JRE64 directories.

   **Example:**

```
cd <APM root directory>/JRE64/bin
> keytool -import -alias <myCA> -file c:\myCArootcert.cer -keystore
..\lib\security\cacerts -trustcacerts -storepass changeit
cd <APM root directory>/JRE/bin
> keytool -import -alias <myCA> -file c:\myCArootcert.cer -keystore
..\lib\security\cacerts -trustcacerts -storepass changeit
```

7. **Verify secure connection works**

   From a client browser, open the **Default Virtual Gateway Server for Application Users** and **Default Virtual Gateway Server for Data Collectors** URLs that you secured. If the login page appears, this verifies that the secure connection is configured.

8. **Update APM Virtual URLs to use https**
   a. Log in to APM.
   b. Select **APM Console > Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
   c. Click **Foundations** and select **Platform Administration** from the drop down list.
   d. Type the secured URLs in the following two rows:
      - Default Virtual Gateway Server for Application Users URL
      - Default Virtual Gateway Server for Data Collectors URL
   e. Enable and disable all APM Gateway servers, and verify (again) that a client can log in using those URLs.

9. **Connect data collectors to secure APM**

   Now that the APM servers are secured, you configure other servers to communicate securely with APM.

   The basic flow for any data collector connecting to secure APM is as follows:
   a. Import root CA certificate(s) obtained in step 3 into the JVM used by the data collector.
   b. Configure the connection to APM using https.
   c. Make sure data flows over the secure connection.

   Follow the appropriate procedures for more detailed descriptions for each of the data collectors:

| Data Collector / Server type | Relevant Documentation |
|---|---|
| BPM | HPE Business Process Monitor Administrator's Guide. |
| SiteScope | HPE SiteScope Deployment Guide |
| System Health | Using System Health |
| RUM | Real User Monitor Administration |
| Data Flow Probe | The default UCMDB TLS port, 8443, must be changed to the APM TLS port, 443, in the DiscoveryProbe.properties file.<br>For more information, see the Data Flow Probe Installation Guide. |

10. **Configure mutual TLS**

    If you want to configure APM to require a client certificate, perform this procedure:

    a. Follow the standard procedures for requiring client certificates on the front end APM server (could be a web server on the Gateway server, a load balancer, or a reverse proxy). For details, see the documentation of the load balancer, reverse proxy, or web server.

       For examples for reverse proxies

       **IIS.** See *Configure IIS to Require Client Authentication - Optional* in the APM Installation Guide.

       **Apache.** "Configuring Secure Apache Reverse Proxy to Require Client Authentication - Optional" on page 27

    b. If users are required to log in to APM with a digital certificate, see "How to Secure User Access to APM Using Client-Side Authentication Certificates" in the APM Platform Administration Guide.

    c. If users are required to log in to APM using smart cards, see the Smart Card Authentication Configuration Guide.

    d. To enable data collectors to connect to the APM front end server that now requires a client certificate, refer to the following documentation:

| Data Collector / Server type | Relevant Documentation |
|---|---|
| BPM | See the HPE Business Process Monitor Administrator's Guide. |
| SiteScope | See "Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate" in the HPE SiteScope Deployment Guide. |
| System Health | See the Using System Health Guide. |
| RUM | See the Real User Monitor Administration Guide. |
| Data Flow Probe | See the RTSM Data Flow Management Guide. |

11. **(Optional) Secure Management API (JMX-RMI channel)**

    In certain cases, you may need to secure the JMX-RMI channel used for internal APM communications. This procedure should be performed only if there is a specific reason to do so. For details, see "Configuring Secure Access to the JMX-RMI Channel Used for Internal APM Communications" on page 29.

12. **(Optional) Secure APM installation directory**

We recommend that you restrict access to the APM installation directory to privileged users. We recommend only allowing the **SYSTEM** account and **Administrators** groups to access this directory.

13. **(Optional) Configure Secure Tunnel between APM Gateway and Data Processing Servers**

    We recommend that you set up a host-to-host tunnel (or VPN) between all APM Gateway and Data Processing Servers. This ensures that the APM servers can communicate freely.

14. **(Recommended) Configure Secure Access to Data Collectors**

    This section describes how to secure access to the data collector admin consoles (UI). Follow the appropriate procedures depending on your data collectors:

| Data Collector / Server type | Relevant Documentation |
|---|---|
| BPM | "Configuring Secure Access to Data Collectors" on page 33 |
| SiteScope | "Configuring Secure Access to Data Collectors" on page 33 |
| System Health | "Configuring Secure Access to Data Collectors" on page 33 |
| RUM | "Configuring Secure Access to Data Collectors" on page 33 |

15. **Opening JBoss HTTP Port 8080**

    Opening HTTP port 8080 in JBoss 7 is a possible security risky because it allows public access to the APM application configuration interface. Therefore, if you open HTTP port 8080 in JBoss 7, create a firewall that restricts access to the port and configure access permissions are needed.

# Chapter 3: General Security Recommendations for APM

## Configuring Maximum Number of Sessions per Login Name

You can configure the maximum number of sessions that use the same login name. The default value is 0 which defines an unlimited number of sessions. It is highly recommended to set the maximum number of sessions to 1.

**To configure the maximum number of sessions per login name:**

1. In APM, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations > Security**.
3. In the Security - Login table, locate **Maximum machines per login name** and edit the value as needed.

## Configuring HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) is a web security policy tool that helps to protect websites against protocol downgrade attacks, cookie hijacking, and variants of man-in-the-middle attacks. It enables web servers to enforce that web browsers (or other complying user agents) should only interact with secure HTTPS connections, and not through the insecure HTTP protocol. For more information about HSTS, see RFC 6797.

HSTS provides two methods for sites to secure their connections:

- **Registering for a preload list:** You can register your websites to be hardcoded by major browsers to redirect HTTP traffic to HTTPS. This ensures that communications with these websites from the initial connection are automatically upgraded to be secure. The preload list is based on the Chromium HSTS preload list. From more information, see https://www.chromium.org/hsts.
- **Enabling HSTS on your server:** For sites not on the preload list, you can enable HSTS via the Strict-Transport-Security HTTP header. After an initial HTTPS connection from the client containing the HSTS header, the browser redirects all subsequent HTTP connections to be secured via HTTPS.

  You can enable this method on the APM Web Servers using Apache or IIS.

  **Note:**

  - For this feature, you must have access to APM over TLS protocol.
  - Once you enable this feature, all subsequent HTTP connections are redirected by the browser to be secured via HTTPS, even if you disable it for a specific purpose. However, you can clear

HSTS settings from your browser to allow HTTP access to the resource, please use browser documentation for the instructions.

- **For Apache:**
  i. Go to **<HPE APM root directory>\WebServer\conf\extra\httpd-ssl.conf** and uncomment the following line:

  ```
  Header always set Strict-Transport-Security "max-age=31536000"
  ```

  ii. Restart Apache.

- **For IIS 7.0 and higher:**
  i. Open a cmd window with administrative privileges and run the following command:

  **%SystemRoot%\System32\inetsrv\appcmd set config /section:httpProtocol /+customHeaders.[name='Strict-Transport-Security',value='max-age=31536000']**

  ii. Restart IIS by running the **iisreset** command in the same cmd session.

# Configuring a Strong Cipher Suite Order

To protect against attacks on 64-bit block ciphers in TLS, you need to configure a strong cipher suite order.

1. In Microsoft IIS, you can use the following methods to configure a strong cipher suite order:
   - Using GPO:
     i. At a command prompt, run **gpedit.msc** to open the Group Policy Object Editor.
     ii. In the Local Computer Policy tree, expand **Computer Configuration, Administrative Templates, Network**, and then click **SSL Configuration Settings**.
     iii. In the right pane, click **SSL Cipher Suite Order**.
     iv. Click **Policy setting**.
     v. Set up a strong cipher suite order using Mozilla's TLS configuration instructions ( see https://wiki.mozilla.org/Security/Server_Side_TLS) and the following list of Microsoft's supported ciphers:

     ```
     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_
     SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_
     SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_
     SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_
     SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_
     DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_
     WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_
     CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_
     RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_
     ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_
     ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,TLS_
     ECDH_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_
     ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_
     ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,TLS_
     ECDH_ECDSA_WITH_AES_128_CBC_SHA256
     ```

- Using IISCrypto created by Nartac Software (https://www.nartac.com/Products/IISCrypto). This tool enables you to set/change the appropriate Schannel settings using a simple and intuitive UI.

2. After creating the strong cipher suite order, restart APM.

# Chapter 4: Using TLS in APM

Transport Layer Security (TLS) technology secures communication by encrypting data and providing authentication. Without TLS encryption, packets of information travel over networks in plain text.

TLS encryption uses two keys:

- **Public key.** The public key is used to encrypt data.
- **Private key.** The private key is used to decipher data.

Both keys together are called a key pair. The certificate contains the public key. Every TLS certificate is created for a particular server in a specific domain by a Certificate Authority (CA). When an application user or data collector accesses a APM server, TLS authenticates the server, and can also be configured to authenticate the client. Additionally, APM establishes an encryption method and a unique key for the communication session.

APM supports all TLS protocol versions (1.0/1.1/1.2).

The TLS channel is configured on the APM servers/clients as required.

**Note:** The TLS best practice is to use the strongest currently available cryptographic algorithms when obtaining server or client certificates, as well as the largest key size (not less than 2048-bit RSA keys). To see the latest NIST approved cryptographic algorithms and key lengths, go to http://csrc.nist.gov/publications/PubsFIPS.html.

Additionally, we recommend disabling Weak Ciphers on the Java Security API level by editing the java.security file. This change affects the entire system, when it acts as a server as well as client.

1. Access the files:
   - \HPBSM\JRE\lib\security\java.security
   - \HPBSM\JRE64\lib\security\java.security
2. Locate the line:

   ```
   jdk.tls.disabledAlgorithms
   ```

   and replace it with the following:

   ```
   jdk.tls.disabledAlgorithms=MD5, DSA, DESede, DES_CBC, DHE, RC4, SSLv3, TLSv1,
   ECDH_anon, DH_anon, NULL, DH keySize < 768, RSA keySize < 2048
   ```

**Note:** We recommend not deactivating TLS v1.1 support since this may cause issues, such as preventing Java 7-based clients from running. However, if you must deactivate TLS v1.1 support:

In <APM root directory>/WebServer/conf/extra/httpd-ssl.conf,
replace `SSLProtocol -all +TLSv1 +TLSv1.1 +TLSv1.2`
with `SSLProtocol -all +TLSv1.2`

# Overview of TLS and APM

TLS provides APM with the following:

- **Server authentication.** Provides authentication of the APM server used for communication.
- **Client authentication (optional).** Provides authentication of the client communicating with the APM server. The client could be an application user or a data collector such as Business Process Monitor.
- **Encrypted channel.** Encrypts the communication between the client and the server using a variety of ciphers.
- **Data integrity.** Helps ensure that the information sent by one side over TLS is the same information received by the other side.

# Creating TLS Certificates

Server certificates can be obtained in various formats. Java uses a proprietary format (JKS) to store certificates in what is called a Keystore. This format is compatible with Java applications. Certificates can also be stored in other language-neutral formats such as PKCS#12.

Different components support different server certificate formats. For example, web-servers such as IIS and Apache work with PKCS#12 format and do not work with JKS format. Depending on the components included on your APM server, you may need to use either the JKS or PKCS#12 format.

# Issuing TLS Certificates

Secure communication via https can terminate either at the load balancer/ reverse proxy or on the APM Gateway.

If it terminates on the APM Gateway, the web server on the Gateway is configured to support/require TLS. Otherwise, if TLS terminates on the load balancer/reverse proxy, then only the load balancer/reverse proxy needs to be configured for secure communication.

Generally, server certificates must be issued to the name of the external access point (FQDN) that is configured in **Default Virtual Gateway Server for Application Users/Data Collectors URL**. This is the name that users and data collectors use to access APM.

**Note:** If SSL/TLS termination is configured on the APM Gateway Server and you are using Server Aliases with Subject Alternative Name (SAN) certificate in your environment and your deployment is using Apache as a APM Gateway Web Server, you need to add the list of all aliases to the following directives in Apache httpd-ssl.conf file as in the following example.

- List all the aliases in the file:

```
HPAPM\WebServer\conf\extra\httpd-ssl.conf
##
## SSL Virtual Host Context
##
<VirtualHost *:443>
```

```
    ServerName bsmgw.mycorporate
    Server Alias *.mycorporate.com
    .
    .
    .
</VirtualHost>
```

- Or list the hosts:

```
<VirtualHost bsmgw.mycorporate.com:443 02SRV00xxx.ad02.xxx.intranet:443
02log00xxx.hosts.xxx.intranet:443>
    ServerName bsmgw.mycorporate.com
    ServerAlias 02SRV00xxx.ad02.xxx.intranet
    ServerAlias 02log00xxx.hosts.xxx.intranet
    ServerAlias externalbsm.corporate.com
    .
    .
    .
</VirtualHost>
```

If there is a load balancer/reverse proxy in front of a APM gateway, it is recommended to have TLS terminate on the load balancer/reverse proxy.

As usual with TLS, you will need to have a CA root certificate present in your browser's **Trusted Certification Authorities** list and in the trustcacerts of the JVM on each data collector installation.

The following table addresses TLS termination in the High Availability environment:

| TLS Termination On | TLS on Load Balancer | TLS on Gateway | Advantages/ Disadvantages |
|---|---|---|---|
| Load Balancer | Yes | No | This is a recommended configuration. It allows:<br>• Maintenance of certificates in one place (on load balancer/reverse proxy)<br>• Reduced processing of load on APM Gateways<br>On each load balancer/reverse proxy, use server certificates issued to the name of the external access point (FQDN) that users/data collectors are using to access APM.<br>If multiple load balancers/reverse proxies share the load, each one must have these certificates imported. |

| TLS Termination On | TLS on Load Balancer | TLS on Gateway | Advantages/ Disadvantages |
|---|---|---|---|
| Load Balancer and Gateway (TLS all the way) | Yes | Yes | This is a less ideal configuration, especially where load balancers are concerned. It requires:<br>• Maintenance of certificates in multiple places (load balancer/reverse proxy and Gateways)<br>• Expensive TLS renegotiation in load balanced environment for data collectors (see note below)<br>In this configuration, in addition to installing certificates on the load balancer, also install server certificates on the Gateway, using a server certificate issued to the FQDN name of the Gateway.<br>**In a high availability environment with multiple Gateways:**<br>Traffic from the same data collector will be load-balanced between different Gateways using a round-robin mechanism. If you have a different certificate on each Gateway issued to a different name, in the worst case scenario, switching between Gateways will require an TLS renegotiation process to run each time there is a switch between Gateways. This is very expensive in terms of CPU use and network traffic, on both the server and client sides. For this reason, TLS termination is typically done on the load balancer. |
| Gateway | No | Yes | Not a recommended scenario. |

# Creating a Java Keystore

**Option 1: Convert a PKCS#12 certificate provided by your Certificate Authority.**

1. Request a client or server certificate from CA in the name of your server.
2. Export private key with a password that is at least six characters long. Example: **changeit**.
3. Convert the certificate from PFX/PKCS#12 to JKS format. For example: **keytool.exe -importkeystore -srckeystore c:\certificate.pfx -destkeystore c:\certificate.jks -srcstoretype PKCS12**
4. Import CA root certificate into the keystore just created, as in the following example.

   Download CA root certificate in BASE-64 format, for example, **c:\ca_root.cer**.

   Import CA root certificate into the keystore:
   **keytool -import -alias ca -file c:\ca_root.cer -keystore C:\certificate.jks -storepass changeit**

**Option 2: Create a keystore in JKS format manually and have it signed by your certificate authority as follows:**

1. Generate a keystore with a private key

```
keytool.exe -genkeypair -validity 1065 -keysize 2048 -keyalg rsa -keystore
```

```
mykeystore -storepass changeit -alias myserver.mydomain
```

Where validity (in days) and keysize depend on your certificate authority requirements.

2. Generate a server certificate request to have it signed by your certificate authority.

```
keytool.exe -keystore mykeystore -storepass changeit -alias myserver.mydomain  -
certreq  -file CERTREQFILE.csr
```

3. Download the signed server certificate **cert_signed.cer** from your certificate authority.
4. Obtain the root authority certificate (and any intermediate authority certificates if applicable).
5. Import the root certificate authority certificate (and any intermediate authority certificates if applicable) into the keystore created earlier in this procedure.

```
keytool.exe -import -trustcacerts -keystore mykeystore -storepass changeit -alias
 myRootCA -file c:\ca_root.cer
```

6. Import the signed certificate into the same keystore under the original alias.

```
keytool -import -v -alias myserver.mydomain -file cert_signed.cer -keystore
mykeystore -keypass changeit -storepass changeit
```

7. Verify that the keystore contains at least two entries: **Trusted Cert Entry** and **Private Key Entry**.

   keytool -list -keystore mykeystore

**Note:** Make sure that your private key password and keystore password are the same.

# Chapter 5: Configuring Secure Access to APM Front Ends

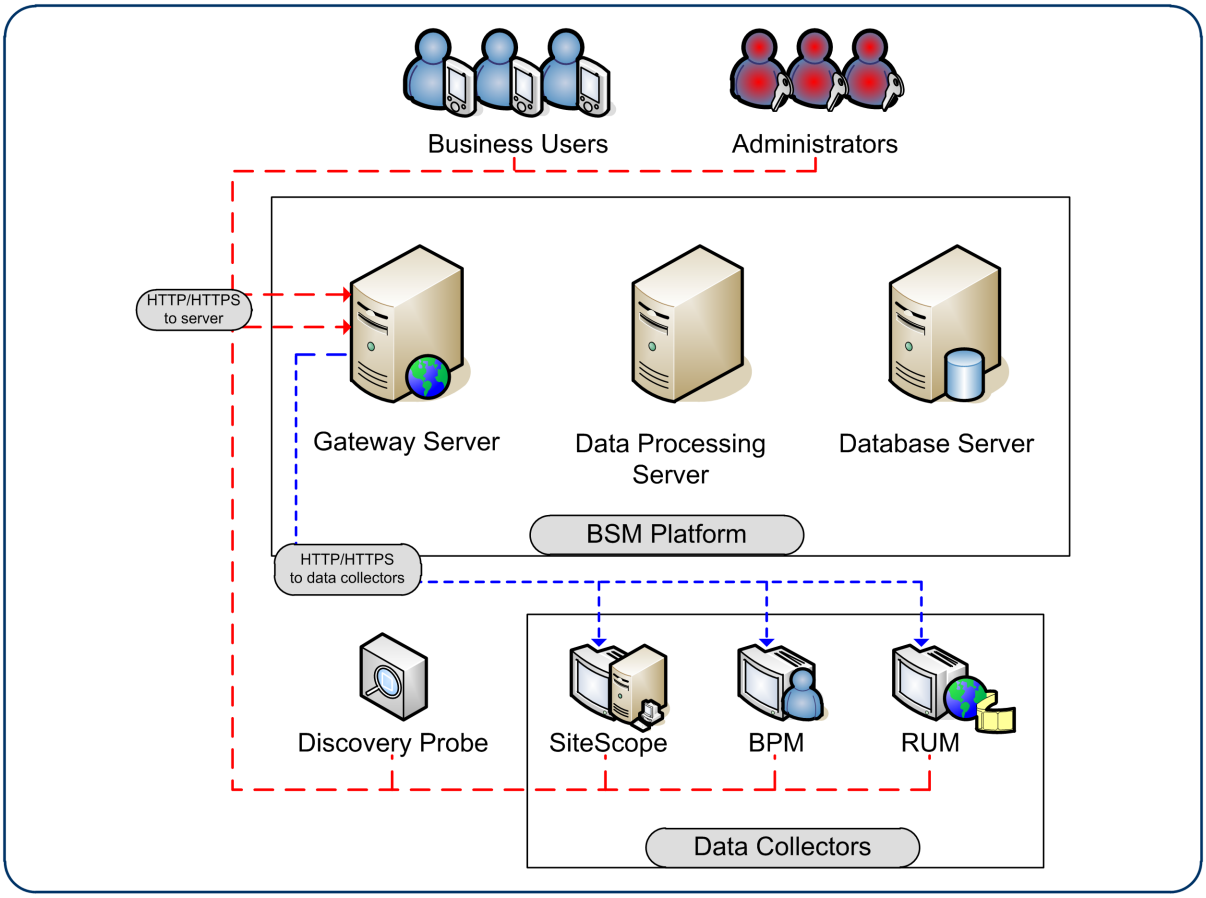
This chapter contains the following topics:



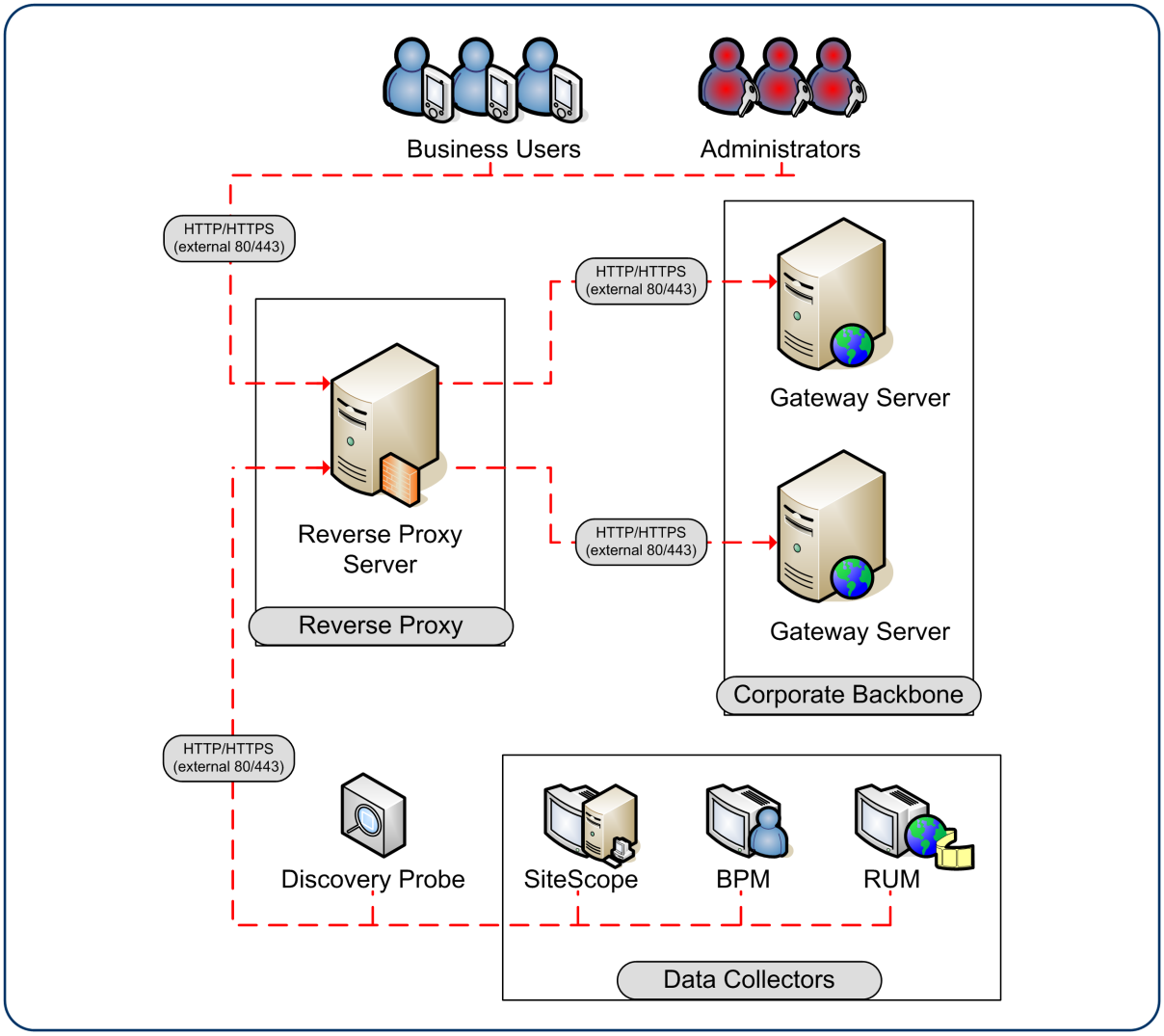
# Supported Topologies in APM

TLS supports the following topologies:

- Application users / data collectors that communicate with APM Gateway Servers directly.



- Application users / data collectors that communicate with APM Gateway Servers using Reverse Proxy.




Client authentication using a client-side certificate is optional with APM clients.

# Configuring Secure Access to APM Gateways

To configure secure access to the APM Gateway (or a APM machine, in the case of a single machine installation), you must enable TLS support on the Web server used by the Gateway Server.

**To enable TLS support on the Web Server:**

- **Microsoft Internet Information Server (IIS).** See Microsoft's site http://www.iis.net/ for information on enabling TLS for all interaction with the Web server. Note that TLS should be enabled for the entire IIS Web Site under which you installed the APM applications.
- **Apache HTTP Server 2.4**. The Apache web server is included in APM. For details about configuring TLS, see "Configuring Secure Access to Apache" on page 24.

If you are not using a publicly known Certificate Authority for your server certificate, you need to set the Java truststore to trust the Certificate Authority that issued the server certificate. For details, see step 5 in the "Hardening Workflow" on page 9.

After performing the above procedures, the Web server installed on the Gateway Server machine is configured to support HTTPS communication.

To disable weak ciphers and protocols on IIS and Apache, refer to BSM Update for Exploiting the SSL 3.0 - Poodle Attack.

# Additional Security Recommendations

To provide additional security for access to the APM Gateway Server or Data Processing Server, we recommend the following:

- **Disable Weak Ciphers on IIS.** See http://support.microsoft.com/default.aspx?scid=kb;EN-US;245030.
- **Remove Server Header.** By default, Microsoft adds a server response header with content looking like this `Server: Microsoft-IIS/7.5`. It is recommended to remove this header.
  a. Download and install URL Rewrite (if it is not already installed). See http://www.iis.net/downloads/microsoft/url-rewrite.
  b. Click **Add Rule(s)** and create a new blank outbound rule. Complete the following information:
     - **Name:** Remove response server
     - **Matching scope:** Server variable
     - **Variable name:** RESPONSE_SERVER
     - **Variable value:** Matches the Pattern
     - **Using:** Regular Expressions
     - **Pattern:** .+
     - **Action type:** Rewrite
     - **Value:** type bogus server name. For example, nginx, apache etc.
     - **Replace existing server variable value:** Select this option.
  c. Apply and use a header sniffer to check the results.

# Configure URL for Accessing APM with TLS

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. Click **Foundations** and select **Platform Administration**.
2. In the Host Configuration pane, set the following parameters:
   - Default Virtual Gateway Server for Application Users URL and Default Virtual Gateway Server for Data Collectors URL. You must enter the server URL with the TLS protocol https and the TLS port (default is 443). For example: https://my_server.example.com:443
   - 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 one defined for the Default Virtual Core Server URL parameter) to access the Gateway Server machine, define a Local Core Centers

Server URL for each machine through which you want to access the Gateway Server machine. For example:

**https://my_specific_virtual_server.example.com:443**

> **Note:** If the Local Virtual Core Services Server URL parameter is defined for a specific machine, this URL is used instead of the Default Virtual Core Services URL for the specifically-defined machine. If the Local Virtual Server URL parameter is defined for a specific machine, this URL is used instead of the Default Virtual Server URL for the specifically-defined machine.

3. **Direct Gateway Server for Application Users Server URL**. Click the **Edit** button and delete the URL in the **Value** field.
4. **Direct Gateway Server for Data Collectors URL**. Click the **Edit** button and delete the URL in the **Value** field.
5. Restart the HPE APM service on all APM machines.

> **Note:** Once 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.

**Configuring Secure Access to Apache**

If you are using an Apache web server on the APM Gateway server, and you decide to use TLS, you must configure the web server as described in this section. For more information, see http://httpd.apache.org/docs/2.4/en/ssl/.

1. Prepare the server certificate
   a. Obtain a signed server certificate from your certificate authority to the name of the APM Gateway server. Typically this certificate comes in PKCS#12 format with a password protected private key.
   b. Separate the private key and the server public key using the openssl utility.

      For example: Go to **HPBSM\WebServer\bin**, run openssl, and use the following commands:

      ```
      pkcs12 -in c:\bsmcert.pfx -clcerts -nokeys -out c:\bsm_server_cert.pem
      pkcs12 -in c:\bsmcert.pfx -nocerts -nodes -out c:\bsm_server_key.pem
      ```

2. Update the Apache TLS configuration file
   a. Go to **<APM Gateway Installation Directory>\WebServer\conf\extra**
   b. Open **httpd-ssl.conf** in a text editor.
   c. Look for the following lines and replace the file name in quotation marks with the path to the files produced in the previous step.

      ```
      SSLCertificateFile "c:/bsm_server_cert.pem"
      SSLCertificateKeyFile "c:/bsm_server_key.pem"
      ```

   d. Locate the line starting with **ServerName** and verify that this is the name that you issued the server certificate to.
   e. Close and save file.
3. Enable TLS

a. Go to **<APM Gateway Installation Directory>\WebServer\conf**
b. Open **httpd.conf** in a text editor.
c. Search the file for the string ssl to locate and uncomment the following lines (they are not consecutive):

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

d. Close and save the file.

4. When you have verified that the https connection works, if you want to disable clear text communication, close the http port by commenting out the line **Listen 80** in the **<APM Gateway Installation Directory>\WebServer\conf\httpd.conf** file.
5. Restart the Apache web service
   - In Windows:
     i. Go to **Start > Run** and type **services.msc**.
     ii. Locate **HP Business Service Management Web Server**.
     iii. Restart the Service.
     iv. Test your https connection to the APM Server to make sure you can log in. For example: **https://<APM Gateway Server>/topaz**.
   - In Linux:
     Run **/opt/HP/BSM/WebServer/bin/apache2start.sh**.

# 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.

# Configuring Secure Access to Apache Reverse Proxy

This procedure should be performed as part of the Hardening Workflow. For details, see "Hardening Workflow" on page 9.

1. Convert the root CA certificate obtained earlier to base 64 format.

   **Openssl > x509 -in c:\ca_64.cer -out c:\ca.pem**

2. Split certificate and private key.

   If the server certificate is in PFX format, split the certificate. In OpenSSL run the following commands to generate both certificate and private key in PEM format:

   **pkcs12 -in C:\<server_certificate>.pfx -clcerts -nokeys -out C:\mycert.pem**

   **Enter Import Password: <your_password>**

   **MAC verified OK**

   **pkcs12 -in C:\<server_certificate>.pfx -nocerts -nodes -out C:\mykey.pem**

   **Enter Import Password: <your_password>**

   **MAC verified OK**

3. Configure Apache to use the certificates.

   a. Edit **<Apache Installation Directory>/WebServer/conf/httpd.conf**

      uncomment these lines (remove #):

      **LoadModule ssl_module modules/mod_ssl.so**

      **Include conf/extra/httpd-ssl.conf**

   b. Edit **<Apache Installation Directory>/WebServer/conf/extra/httpd-ssl.conf**

      - Update SSLCertificateFile with path to <mycert.pem >
      - Update SSLCertificateKeyFile with path to <mykey.pem>
      - Insert the following lines in the virtual host section in httpd-ssl.conf with the path to the certificate authority key in PEM format:

        **VirtualHost <Reverse Proxy FQDN>**

        **ProxyRequests Off**

        **SSLProxyEngine On**

        **SSLProxyCACertificateFile <path to file of ca who issued the proxy certificate, for example c:\ca.pem>**

        **SSLProxyVerify require**

        **# General setup for the virtual host**

4. Close port 80

   Open **<Apache installation directory>\Webserver\conf\httpd.conf** and comment out **listen 80** by adding # as a prefix.

5. Verify that Apache runs using TLS

a. Restart Apache
b. Go to https://<Reverse Proxy FQDN>.

   Do not use localhost, use the full server name that matches the name on the certificate. You should see the message "it works!"
c. Go to http://<Reverse Proxy FQDN>.

   It should not work.

# Configuring Secure Apache Reverse Proxy to Require Client Authentication - Optional

Configuring a secure reverse proxy to require client authentication involves manual procedures

1. Make the following changes in **<Apache installation directory>/conf/extra/httpd-ssl.conf**:
   a. Uncomment (remove the #) the following lines:

      **SSLVerifyClient require**

      **SSLVerifyDepth 10**
   b. Search for **SSLCACertificateFile**, uncomment it and update the path to the client CA root certificate for the authority that issued your client certificate.

      **SSLCACertificateFile "C:\CA.pem"**
   c. Locate the line **#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire**

      Add the following line right below it: **SSLOptions +ExportCertData**
   d. Add the following line before </VirtualHost>:

      **RequestHeader set CLIENT_CERT_HEADER "%{SSL_CLIENT_CERT}s"**
2. Edit the **<Apache installation directory>/conf/httpd.conf** file

   Uncomment (remove the #) from the following lines:

   **LoadModule headers_module modules/mod_headers.so**

   **LoadModule rewrite_module modules/mod_rewrite.so**
3. Restart Apache.

   Go to https://<Reverse Proxy FQDN>/topaz

   Verify that you see a prompt for a client certificate.

# Configuring the URL for Accessing APM with TLS

See "Configure URL for Accessing APM with TLS" on page 23.

# Configuring Secure Access to the HTML JMX Console

This task describes how to configure secure access to the HTML JMX console in other APM processes.

**Note:** This procedure is for both gateway and data processing servers

**To configure secure access to the JMX console in other APM processes:**

1. Open the following files:
   - <APM root directory>\conf\spring\jmx-html-adaptor-spring.xml
   - <APM root directory>\conf\supervisor\spring\jmx-html-adaptor-spring.xml

   and locate the following section in each:

```
<bean id="jmx.html.adaptor" class="com.mercury.infra.utils.jmx.MX4JHtmlAdaptor"
       lazy-init="true">
<property name="sslEnabled"><value>false</value></property>
<property name="keyManagerAlgorithm"><value>SunX509</value></property>
<property name="keyStorePassword"><value>changeit</value></property>
<property name="keyManagerPassword"><value>changeit</value></property>
<property name="keyStoreType"><value>JKS</value></property>
<property name="sslProtocol"><value>TLS</value></property>
<property name="keyStoreName"><value>file.keystore</value></property>
</bean>
```

2. Update the relevant parameters, as indicated in the following table:

| Parameter Name | Required Value |
|---|---|
| sslEnabled | true |
| keyStorePassword | The password you use to protect the keystore. This is the value of the keystore's **-storepass** parameter, if you created the keystore yourself. |
| keyManagerPassword | The password you use to protect the private key. This is the value of the keystore's **-keypass** parameter, if you created the keystore yourself. |
| keyStoreName | The name and path of the file where the keystore is located. |

3. Create a keystore. For details, see "Creating a Java Keystore" on page 19.

# Configuring Secure Access to the JMX-RMI Channel Used for Internal APM Communications

To secure access to the JMX-RMI channel used for internal APM communications, you must configure JMX-RMI with basic authentication over TLS. This involves the following steps:

- Configuring user name/password authentication
- Configuring TLS for the JMX-RMI channel

**Note:**

- This procedure was written for Windows. Linux users should use Unix paths and commands as needed.
- If you are securing a JMX channel and using System Health, you must use the Encryption tool provided in the System Health installation to supply JMX monitor credentials to System Health. For details, see the HPE System Health Guide.
- This procedure must be performed on every Gateway and Data Processing server in the APM deployment.

**Configuring User Name/Password Authentication**

1. Add user role.

   Add the user role to:
   **<APM root directory>\JRE64\lib\management\jmxremote.access**.

   **Example:**

   ```
   adminUser readwrite \
          create javax.management.monitor.*,javax.management.timer.* \
          unregister
   ```

2. Create password file.
   a. Copy:
   **<APM root directory>\JRE64\lib\management\jmxremote.password.template**
   to:
   **jmxremote.password**
   b. Add the user role defined previously in jmxremote.access to the end of the jmxremote.password file, and set a clear text password. Remember this password so you can test it with the JMX console.

   Example:

   ```
   adminUser mypassword
   ```

3. Protect the password file.

   **In Windows:**

a. Change the owner of the **jmxremote.password** file to be an administrator user or the SYSTEM user.

   If you change the owner to the SYSTEM user, you will not be able to view data on the APM Status page.

   If you change the owner to an administrator user, you will need to change the default log on credentials to run the HPE Business Service Management service. This procedure is performed in your operating system. In Windows Server 2008, the procedure is as follows:

   i. Run **services.msc**.
   ii. Right click **HP Business Service Management** service and click **Properties**.
   iii. In the **Log on** tab, select **This account** and enter the administrator credentials.
   iv. Apply the changes. Wait for a message that **The account <> has been granted the Log On As A Service right**.
   v. Restart the HPE Business Service Management service.

   Whatever user you select, you must use the same user for any other similar steps in this procedure.

   To change the owner of the files:

   i. Navigate to **Properties > Security > Advanced > Owner**.
   ii. Click Other Users or Groups, type "**<domain\admin user name>**" or "**SYSTEM**", and click **Check Names**.
   iii. Verify that you see that the value of Current Owner is updated.

b. Change the permissions of jmxremote.password file to be **Full Control** for the owner defined above as follows:

   - For administrator user:

     **cmd: icacls <APM root directory>/JRE64/lib/management/jmxremote.password /reset /Q /C**

     **cmd: icacls <APM root directory>/JRE64/lib/management/jmxremote.password /inheritance:r /grant:r <domain\user name>:(r,w) /T /Q /C**

   - For SYSTEM user:

     **cmd: icacls <APM root directory>/JRE64/lib/management/jmxremote.password /reset /Q /C**

     **cmd: icacls <APM root directory>/JRE64/lib/management/jmxremote.password /inheritance:r /grant:r SYSTEM:(r,w) /T /Q /C**

**In Linux:**

Run the following command: **chmod 600 jmxremote.password**

4. Repeat the above steps for the **<APM root directory>\JRE** directory.
5. Enable authentication on all APM processes other than JBoss.

   Open **<APM root directory>\bin\service_manager.bat** (in Linux, **service_manager.sh**) and set the authentication to **true**, as in the following example:

   **-Dcom.sun.management.jmxremote.authenticate=true**
6. Enable authentication on nannyManager.

   Open **<APM root directory>\conf\supervisor\manager\nannyManager.wrapper** and set the following:

   **wrapper.java.additional.3=-Dcom.sun.management.jmxremote.authenticate=true**

### Configuring TLS for the JMX-RMI Channel

**Note:** When creating a Java keystore password, make sure your private key password and the keystore password are the same.

1. Create Java keystore (JKS file). For details, see "Creating a Java Keystore" on page 19.
2. Create a JMX-RMI properties file with TLS parameters.

   Create **jmx-rmi.properties file in <APM root directory>\conf** containing the following lines:

   ```
   com.sun.management.jmxremote.ssl=true

   javax.net.ssl.keyStore=<path to keystore file name with forward slashes>

   javax.net.ssl.keyStorePassword=<keystore password>
   ```

   **Note:**

   Use forward slashes only, not backslashes.

   **Example:**

   ```
   com.sun.management.jmxremote.ssl=true

   javax.net.ssl.keyStore=c:/certificate.jks

   javax.net.ssl.keyStorePassword=changeit
   ```

3. Protect the TLS parameters file.

   **In Windows:**

   a. Navigate to **Properties > Security > Advanced** and change the owner of the **jmx-rmi.properties** file to be an administrator user or the SYSTEM user.

      If you change the owner to the SYSTEM user, you will not be able to view data on the APM Status page.

      If you change the owner to an administrator user, you will need to change the default log on credentials to run the HPE Business Service Management service. This procedure is performed in your operating system. In Windows Server 2008, the procedure is as follows:

      i. Run **services.msc**.

      ii. Right click **HP Business Service Management** service and click **Properties**.

      iii. In the **Log on** tab, select **This account** and enter the administrator credentials.

      iv. Apply the changes. Wait for a message that **The account <> has been granted the Log On As A Service right**.

      v. Restart the HPE Business Service Management service.

      Whatever user you select, you must use the same user for any other similar steps in this procedure.

      To change the owner of the files:

      i. Navigate to **Properties > Security > Advanced > Owner**.

      ii. Click Other Users or Groups, type "**<domain\admin user name>**" or "**SYSTEM**", and click **Check Names**.

      iii. Verify that you see that the value of Current Owner is updated.

   b. Change the permissions of **jmx-rmi.properties** file to be **Full Control** for the file owner defined

above as follows:

- For administrator user:

  **cmd: icacls <APM root directory>/JRE64/lib/management/jmxremote.password /reset /Q /C**

  **cmd: icacls <APM root directory>/JRE64/lib/management/jmxremote.password /inheritance:r /grant:r <domain\user name>:(r,w) /T /Q /C**

- For SYSTEM user:

  **cmd: icacls <APM root directory>/JRE64/lib/management/jmxremote.password /reset /Q /C**

  **cmd: icacls <APM root directory>/JRE64/lib/management/jmxremote.password /inheritance:r /grant:r SYSTEM:(r,w) /T /Q /C**

**In Linux:**

**chmod 600 jmx-rmi.properties**

4. Enable TLS on JMX-RMI for all APM processes other than JBoss.

   Open **<APM root directory>\bin\service_manager.bat** (in Linux, **service_manager.sh**) and make the following changes:

   a. Set the value of `-Dcom.sun.management.jmxremote.ssl=true`

   b. Add the following string immediately after the string you just modified:

   ```
   -Dcom.sun.management.jmxremote.ssl.config.file=<APM root directory>/conf/jmx-rmi.properties
   ```

5. Enable TLS on JMX-RMI for Nanny process.

   Open **<APM root directory>\conf\supervisor\manager\nannyManager.wrapper** and set the following:

   a. Comment out the line with ssl:

   ```
   #wrapper.java.additional.4=-Dcom.sun.management.jmxremote.ssl=false
   ```

   b. Add this line instead:

   ```
   wrapper.java.additional.4=-Dcom.sun.management.jmxremote.ssl.config.file=<APM root directory>/conf/jmx-rmi.properties
   ```

6. Make JVM trust the key defined in the keystore file.

   a. Export the public key from the keystore file (use regular keytool).

   **Example:**

   ```
   keytool -export -alias ca -keystore c:\certificate.jks -rfc -file ca_root.cer
   ```

   where **certificate.jks** is the keystore file, and **ca_root.cer** is the exported public key file.

   b. Import the public key into **<APM root directory>\JRE\lib\security\cacerts and <APM root directory>\JRE64\lib\security\cacerts**.

   **Example:**

   ```
   <APM installation directory>\JRE64\bin\keytool -import -alias ca -file ca_root.cer -keystore <APM installation directory>\JRE64\lib\security\cacerts
   ```

```
<APM installation directory>\JRE\bin\keytool -import -alias ca -file ca_
root.cer -keystore <APM installation directory>\JRE\lib\security\cacerts
```

where **ca_root.cer** is the public key file, and **cacerts** is the default truststore used by JVM.

c. Enable the APM Server. If the APM server cannot be enabled, see **<APM installation directory>\log\supervisor\wrapper.log**.

# Configuring Secure Access to Data Collectors

For information on configuring secure access to data collectors, see the relevant data collector documentation.

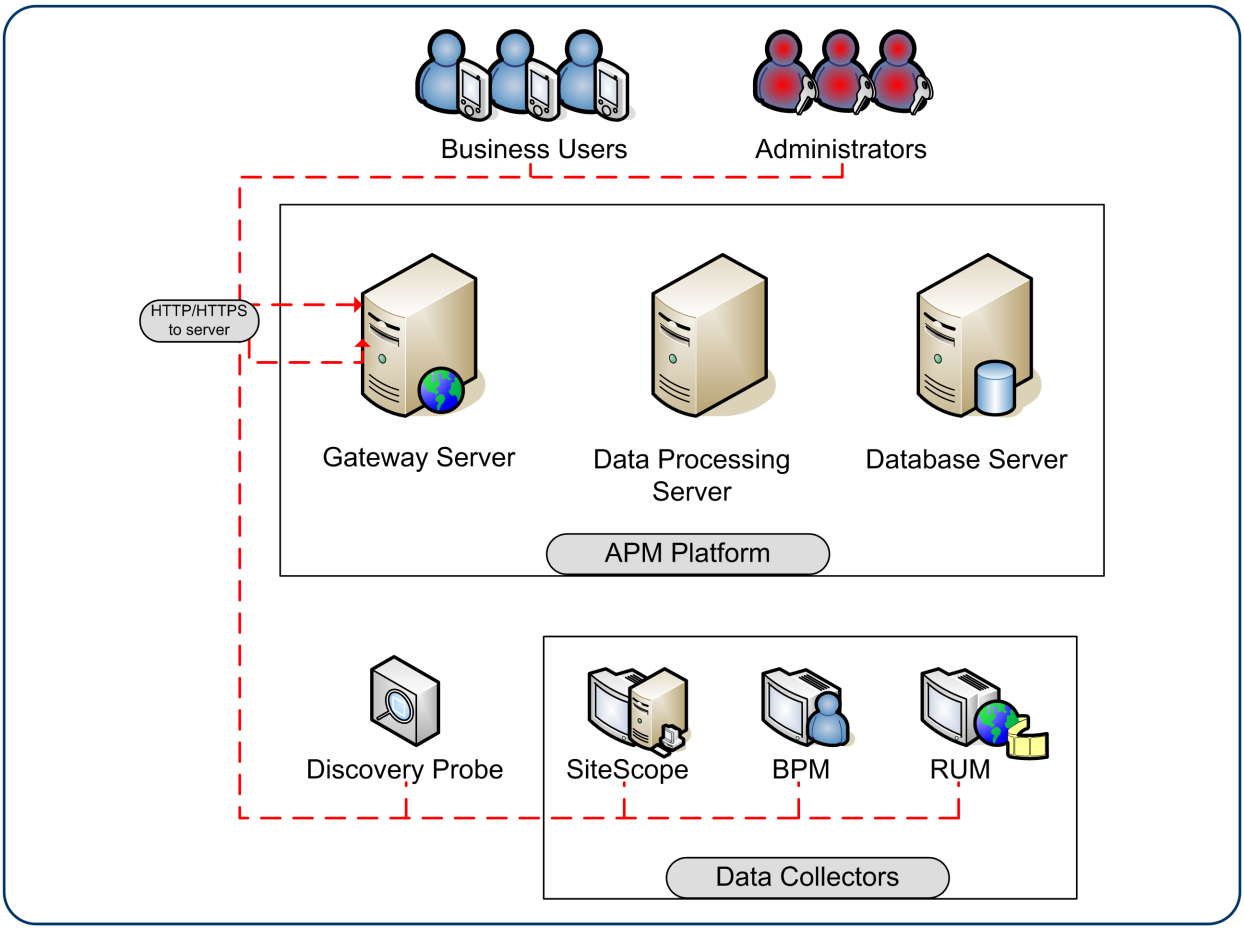
# Chapter 6: Using Basic Authentication in APM

The APM platform fully supports the basic authentication schema, which provides APM with the ability to authenticate a client communicating with a APM server via HTTP or HTTPS.

The basic authentication schema is based on the client sending its credentials to the server so that the server can authenticate the client. The client's credentials are sent in a Base64 encoding format and are not encrypted in any way. If you are concerned that your network traffic may be monitored by a sniffer, it is recommended that you use basic authentication in conjunction with TLS. This sends the client's credentials over an encrypted wire (after the TLS handshake has been completed).

For information on configuring the APM platform to support TLS communication, see "Using TLS in APM" on page 16.

Possible basic authentication channels in APM are illustrated in the following diagram:




**Note:** The APM components do not support basic authentication with blank passwords. Do not use a blank password when setting basic authentication connection parameters

# Overview of Configuring Basic Authentication in APM

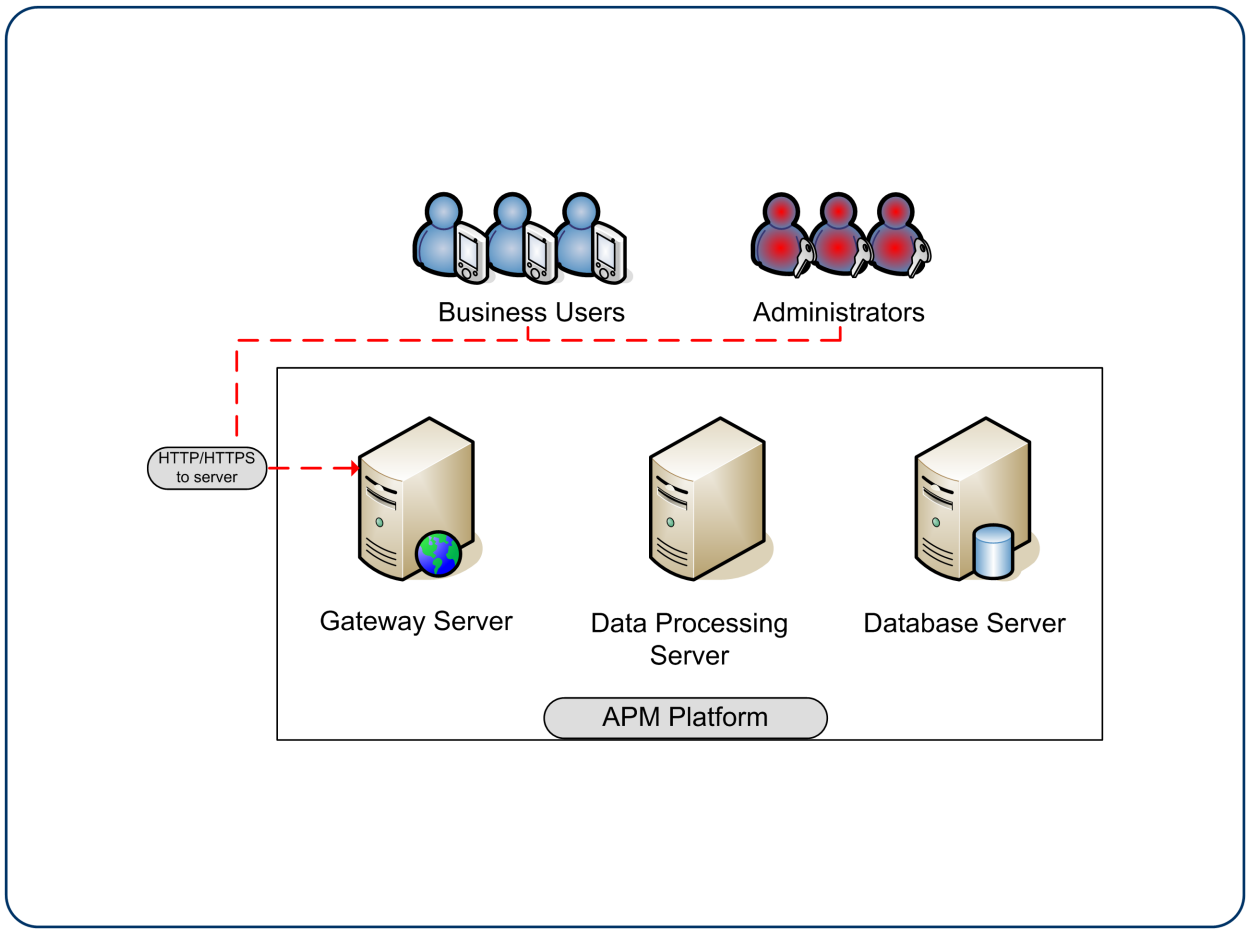
Before proceeding with the configuration steps, ensure that:

- The APM platform is operating as it is supposed to without basic authentication.
- You read this chapter in its entirety before you begin performing the configuration.
- You define your authentication requirements and use basic authentication only where required.

**Note:** The configuration specified for each APM server is also relevant for a single machine installation, in which the Gateway Server and Data Processing Server both reside on the same machine.

# Configuring Basic Authentication Between the Gateway Server and Application Users

The instructions in this section describe how to configure the Gateway Server (or a APM machine, in the case of a single machine installation) and its clients, and application users to support basic authentication.



**Basic Authentication Configuration for the Gateway Server**

This section provides instructions for configuring the Gateway Server (or a APM machine, in the case of a single machine installation) to support basic authentication.

**Caution:** Some JREs request an additional username and password confirmation when accessing applets imbedded in APM, such as the Service Health Topology Map, System Health, and IT Universe Manager.

*Enable Basic Authentication Support on the Web Server*

The first step in configuring the Gateway Server to support basic authentication is to configure the Web server used by the Gateway Server.

**Note:** On each Web server, make sure that you enable basic authentication only and disable anonymous access. Once you have enabled basic authentication, validate the settings by requesting a APM resource and ensuring that you are prompted to insert basic authentication parameters.

- **Microsoft Internet Information Server (IIS) 5.0 and 6.0.** See http://support.microsoft.com/kb/324276/en-us for information on enabling basic authentication for all interaction with the Web server. Note that basic authentication should be enabled for the entire IIS Web Site under which you installed the APM applications.
- **Apache HTTP Server 2.4**. See the http://httpd.apache.org/docs-2.4/howto/auth.html for information on enabling basic authentication for all interaction with the Web server, using **mod_auth**. Note that basic authentication should be enabled on all the directories used by the Web server.

Basic authentication can only be added in conjunction with enabling TLS on the web server.

Once you have performed the above configuration procedures, when you are using a Microsoft IIS 5.0 or 6.0 Web server, you must make sure that all the folders and files in use by APM have the required NTFS permissions required for the users connecting to APM.

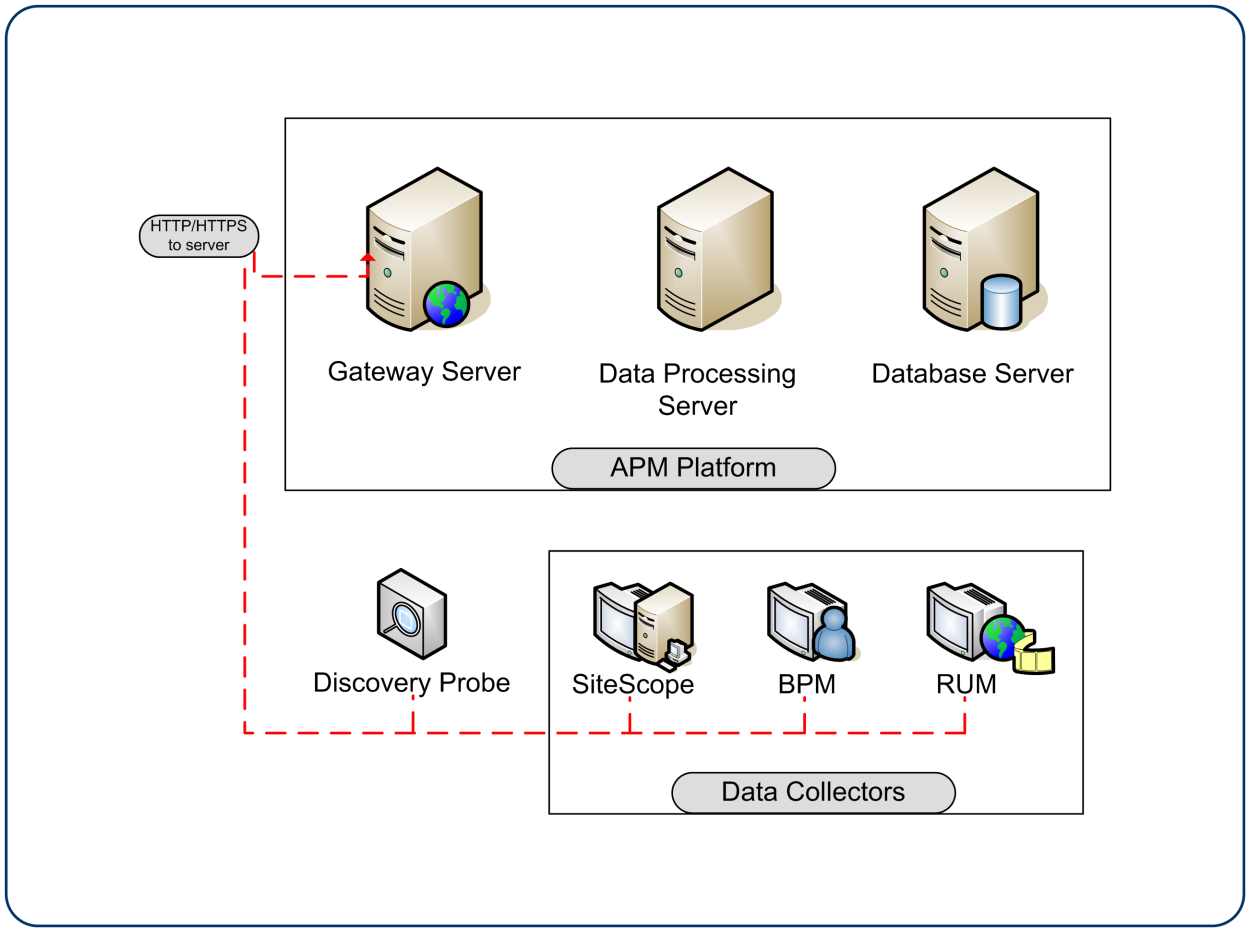
*Basic Authentication Configuration for the Application Users*

This section provides instructions for configuring the application users (Gateway Server clients) to support basic authentication.

To connect as an application user to a APM server that requires basic authentication, it is only necessary for you to know the credentials of the user permitted to log in to the APM Web server. When connecting to the Web server, you will be prompted to enter these credentials. The authentication is then performed automatically.

# Configuring Basic Authentication Between the Gateway Server and Data Collectors

The instructions in this section describe how to configure the Gateway Server and the APM data collectors to support basic authentication. To enable basic authentication support, you must make the required changes for all the Gateway Servers, as well as for all the APM data collectors connecting to it using HTTP/S.




**Basic Authentication Configuration for Gateway Servers**

This section provides instructions for configuring the Gateway Server (or a APM machine, in the case of a single machine installation) to support basic authentication.

*Enable Basic Authentication Support on the Web Server*

The first step in configuring the Gateway Server to support basic authentication is to configure the Web server used by the Gateway Server.

**Note:** On each Web server, make sure that you enable basic authentication only and disable anonymous access. Once you have enabled basic authentication, validate the settings by requesting a APM resource and ensuring that you are prompted to insert basic authentication parameters.

- **Microsoft Internet Information Server (IIS) 5.0 and 6.0**. See http://support.microsoft.com/kb/324276/en-us for information on enabling basic authentication for all interaction with the Web server. Note that basic authentication should be enabled for the entire IIS Web Site under which you installed the APM applications.
- **Apache HTTP Server 2.4**. See the http://httpd.apache.org/docs-2.4/howto/auth.html for information on enabling basic authentication for all interaction with the Web server, using mod_auth. Note that basic authentication should be enabled on all the directories used by the Web server.

Once you have performed the above configuration procedures, when you are using a Microsoft IIS 5.0 or 6.0 Web server, you must make sure that all of the folders and files in use by APM has the required NTFS permissions required for the users connecting to APM.

After performing the above procedures, the Web server installed on the Gateway Server is configured to support basic authentication for HTTP/S communication.

**Basic Authentication Configuration for Data Collectors**

This section provides instructions for configuring the following APM data collectors to support basic authentication. Perform these instructions in both the JRE and JRE64 directories.

**Note:** The Staging Data Replicator (used during a staging upgrade) does not support basic authentication.

*Business Process Monitor*

If you configured the Gateway Server to require basic authentication, you must configure the Business Process Monitor to connect to the Gateway Server using basic authentication.

**To configure the Business Process Monitor to use basic authentication:**

1. Open the Business Process Monitor Admin (**http://<Business Process Monitor machine>:2696**).
2. In the Business Process Monitor page, identify the Business Process Monitor instance you want to configure from the **Instances** list and click the Edit button for the instance. The Edit Instance page opens.
3. In the **Authentication** section, enter the following parameter values:
   - **Authentication user name**. The user name to be used to log in to the Gateway Server.
   - **Authentication user password**. The user password to be used to log in to the Gateway Server.
   - **Authentication domain**. The domain name to be used to log in to the Gateway Server.
4. Click **Save Changes and Restart Instance**.

*SiteScope*

If you configured the Gateway Server to require basic authentication, you must configure the SiteScope machine to connect to the Gateway Server using basic authentication.

**To configure the SiteScope machine to use basic authentication:**

1. If you are configuring SiteScope using System Availability Management Administration, right-click the SiteScope you want to instruct to use basic authentication, and select **Edit**.
   a. In the Profile Settings section of the Edit SiteScope page, enter the following parameter values:
      - **Web server authentication user name**. The user name and domain of the Gateway Server (in the format domain\user name).
      - **Web server authentication password**. The password of the Gateway Server.
   b. Click OK at the bottom of the page and restart the SiteScope instance.
2. If you are configuring SiteScope using the SiteScope interface, select **Preferences > Integration Preferences**.
   a. In the Optional Settings section of the APM Server Registration page, enter the following parameter values:
      - **Authentication username**. The user name and domain of the Gateway Server (in the format domain\user name).
      - **Authentication password**. The password of the Gateway Server.
   b. Click the **Update** button at the bottom of the page and restart the SiteScope instance.

*Real User Monitor*

If you configured the Gateway Server to require basic authentication, you must configure the Real User Monitor engine machine to connect to the Gateway Server using basic authentication.

**To configure the Real User Monitor engine machine to use basic authentication:**

1. Open the Real User Monitor Web Console (**http://<Real User Monitor engine name>:8180/rumconsole**).
2. Click the **Configuration** tab.
3. Under **Basic Authentication**, select the **Use basic authentication** check box and enter the following parameter values:
   - **Authentication user name**. The user name to be used to log in to the Gateway Server.
   - **Authentication user password**. The user password to be used to log in to the Gateway Server.
   - **Authentication domain**. The domain name to be used to log in to the Gateway Server.
4. Click **Save Configuration**.

# Chapter 7: Troubleshooting and Limitations

## Login Problems

| Issue | Resolution |
|---|---|
| Login page does not load when using TLS | Check that server certificate was generated correctly. All fields must be filled in properly, including email, city, state, etc. For example, in IIS6, go to **Default WebSite > Directory Security > Certificates > View > Details**. Subject should be filled in completely. Enhanced Key Usage must be "Server Authentication". |
| Cannot log in through Reverse Proxy; login page not fully displayed | Try to log in directly to APM Gateway, bypassing the proxy.<br>Make sure that the port (even if it is default port) is specified in Platform Administration infrastructure settings (**Default Virtual Gateway Server for Application Users URL**) for the virtual URLs. If you change virtual server URLs, restart APM. |
| Cannot log in through Reverse Proxy | A firewall in the environment may be blocking APM server from resolving Reverse Proxy IP address.<br>**Solution:** Remove Reverse Proxy IP address from the settings, restart APM servers, and try again. |
| Cannot log in; blank page or error in login.jsp - permission denied | • This is typically a result of inconsistency in Host Configuration infrastructure settings.<br>**Solution:** Try to log in directly to the APM Gateway (bypassing Reverse Proxy) and verify that the virtual host URL for application server is correct. Copy/paste it into the browser and check that the page will load.<br>• The virtual URLs may reference the reverse proxy, or vice versa, when reverse proxy is not used.<br>**Solution:** Fix the settings, restart APM server, and try again.<br>To restore to clean, set these to empty string using JMX console (context = platform):<br>• default.centers.server.url = empty or original (with port)<br>• default.core.server.url<br>• Enable.reverse.proxy = false<br>• Http.reverse.proxy.ip = empty |

| Issue | Resolution |
|---|---|
| Internal error when trying to load APM url; FileNotFound error in topaz_all.ejb.log for lwssofmconf.xml | Most likely, the path to the keystore is incorrect after upgrade or new lines were introduced into the setting when manually updated.<br>**Solution:**<br>1. Fix configuration:<br>http://<APM_SERVER>:<JBOSS_PORT>/jmx-console/ (Domain: Foundations, Service: Infrastructure Settings Manager)<br>To retrieve configuration in a string format, use **getGlobalSettingValue()** with:<br>contextName=**SingleSignOn**<br>settingName=**lw.sso.configuration.xml**.<br>Make sure that the new configuration is stored in a single-lined string! No newlines are expected.<br>You can use any text editor to change the configuration as desired.<br>To store configuration, use **setGlobalSettingValue()** with<br>contextName=**SingleSignOn**<br>settingName=**lw.sso.configuration.xml**<br>newValue=**<NEW_VALUE_STRING>**<br>2. Reload configuration:<br>go to service = **SSO**<br>invoke **Start()** |

# Establishing Trust in a Browser for Self Signed Certificates

APM application users (Gateway Server clients) use Web browsers to communicate with the Gateway Server. The Web browsers can be configured to support TLS.

When a session is started between the browser and the Gateway Server, the Gateway Server's Web server sends the browser a server-side certificate that was issued by a Certification Authority (CA). If the certificate used by the Web server is issued by a known CA, the certificate can generally be validated by the browser and no configuration is required. However, if the CA is not trusted by the browser, the browser machine must be configured to validate the server-side certificate that is sent. For instructions on setting CA certificate recognition in the browser and configuring browser certificate validation, refer to your browser vendor documentation.

For example, if you are working with Internet Explorer 9.0, you can import a certificate to the truststore used by the browser.

**To import a certificate to the truststore used by the browser:**

1. Select **Tools > Internet Options** and click the **Content** tab.
2. Click the **Certificates** button.
3. In the **Trusted Root Certification Authorities** tab, click **Import**.
4. Link to the certificate you want to trust and import it.

**Note:** You can import one of the following to the truststore:

- The Gateway Server's certificate.
- The certificate of the Certificate Authority (CA) that issued the Gateway Server's certificate.

If you do not import the CA's certificate, you must import the certificate of each individual Gateway Server that you are working with.

If you are not using a publicly known Certificate Authority (CA), you must import your own CA root certificate into the truststore of APM's JVM for communicating with the data collectors over TLS.

# Handling Security Certificate Expiration

If the webserver on APM Gateway is configured for TLS and the server certificate expires, perform the following steps:

1. Change the webserver configuration files to use a new certificate:
   - **IIS:** Import the new certificate.
   - **Apache**: Update **httpd-ssl.conf** to use new certificate files.
2. Restart the webserver (IIS or Apache service).
3. Make sure you get no certificate errors when accessing the APM user interface through the https protocol.

# Security Technical Implementation Guide

The US Government Security Technical Implementation Guide (STIG) requires standardized secure installation and maintenance of computer software and hardware. These guides (when implemented) lockdown common and typically permissive software to further reduce vulnerabilities.

To meet STIGs standards, in Linux:

- For JBoss processes, set **umask 072** in **/opt/HP/BSM/jboss-as/bin/standalone.sh**
- For all other processes, set **umask 077** in **/etc/init.d/hpbsmd** and **/opt/HP/BSM/scripts/run_hpbsm.sh**

# 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 Hardening Guide (Application Performance Managment 9.40)**

Just 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 docteam@hpe.com.

We appreciate your feedback!