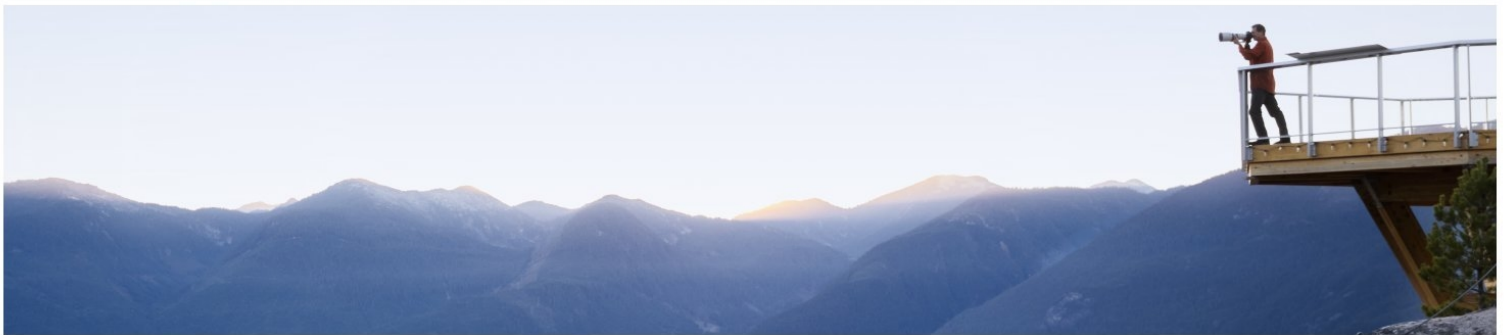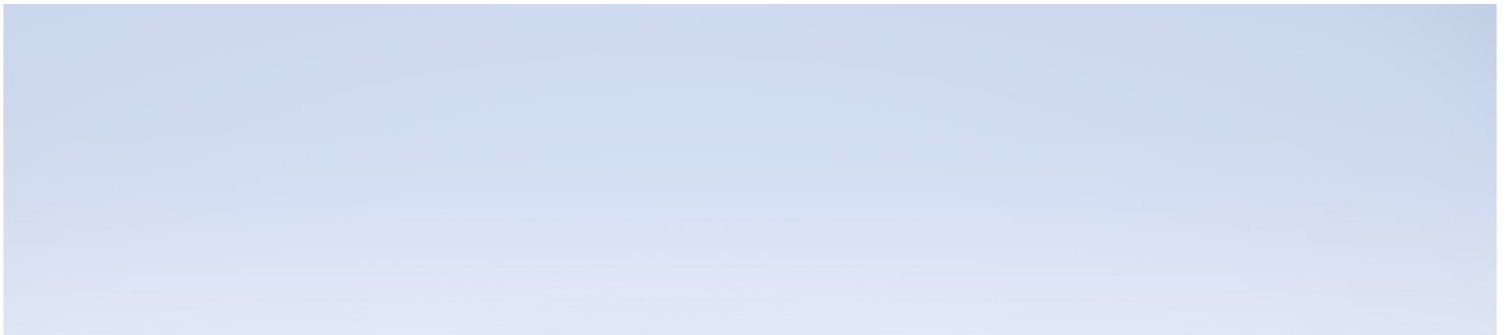# Diagnostics

Version 9.51, Released November 2018

APM - Diagnostics Integration Guide

Published November 2018

Legal Notices

Disclaimer

Certain versions of software and/or documents ("Material") accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

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

Contains Confidential Information. Except as specifically indicated otherwise, a valid license 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

© Copyright 2005 - 2018 Micro Focus or one of its affiliates

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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

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

Acknowledgements

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes software developed by the Spice Group (http://spice.codehaus.org).

For information about open source and third-party license agreements, see the *Open Source and Third-Party Software License Agreements* document.

Contents

Welcome to This Guide

Welcome to the BSM/APM - Diagnostics Integration Guide. This guide describes how to set up and verify an integration of Diagnostics with BSM/APM.

Integrating Diagnostics with BSM/APM enables integrating with the larger BSM/APM family of Software products, such as Real User Monitor, Business Process Monitor, SiteScope, Operations Manager i, Service Health Analyzer, and TransactionVision.

Integration with BSM/APM Platform services enables the following:

- Diagnostic discovered entities are published as configuration items (CIs) in the Run-Time Service model within a BSM/APM solution, aligned with all other discovery content sent by other domains.

- Access to Diagnostics from within BSM/APM (Service Health and myBSM).

- Drill down to Diagnostics data from various BSM/APM reports and Dashboard.

Chapter 1: Setting Up an Integration Between BSM/APM and Diagnostics

Information is provided on setting up the integration between BSM/APM and Diagnostics.

This section includes:

About the Integration of Diagnostics with BSM/APM

In an integration between Diagnostics and BSM/APM, all data flows from a single Diagnostics commander server in the deployment environment to a BSM/APM Gateway Server in the deployment environment. The Diagnostics commander server that is integrated with BSM/APM continues to provide the non-integrated Diagnostics Diagnostics Enterprise UI.

When a Diagnostics commander server is configured to communicate with BSM/APM, it includes the following components:

- **The Operations Manager (OM) agent**. The OM agent sends Health Indicator(HI) update events to OMi.
- **Integration Adapter Policy Activation (IAPA) components**. These components support communication with OMi.

Diagnostics Data Sent to BSM/APM

When Diagnostics is integrated with BSM/APM, a subset of its collected data is sent to BSM/APM as follows:

- **Configuration items (CIs)**. Diagnostics populates an extensive set of application infrastructure, web service and business transaction CIs in the BSM/APM Run-time Service Model (RTSM) and provides information on relationships between CIs in common data models. For example, Hosts, Application Servers, and Databases.

  CIs are sent to BSM/APM through the UCMDB interface.

- **Metrics.** Diagnostics sends metrics from probes and collectors to BSM/APM.

  Health Indicator status (coloring) for business transaction and web service CIs populated by Diagnostics is metric-based. Status for metric based KPIs and Health Indicators is sent to BSM/APM from Diagnostics in data samples. Diagnostics sends data samples to BSM/APM and rules in BSM/APM are used to evaluate the data and set the indicator's status. You can change default objectives for business transaction and Web service Health Indicators in BSM/APM Admin > Service Health. See the BSM/APM Documentation Library for information on using Service Health Admin.

  Diagnostics sends data samples that contain the metrics to BSM/APM where they are persisted in the BSM/APM profile database, typically one that is dedicated to Diagnostics data. Information from these samples is used in to determine status of KPIs and Health Indicators in BSM/APM.

  Diagnostics provides the following data samples to BSM/APM:

  - ws_perf_aggr_t (SOA Sample)

  - ws_event_aggr_t (SOA Sample)

  - appmon_vu_t (Transaction (BPM) Sample)

  - dg_trans_t (Business Transaction (Diagnostics) sample)

- **Events.** Diagnostics sends threshold violations as events to OMi. Health Indicator status (coloring) for application infrastructure CIs populated by Diagnostics is event-based. Status for event-based Health Indicators is sent to OMi from Diagnostics when there is a threshold violation on relevant metrics. The threshold violation event data is sent to OMi through the OMi event channel.

  This event channel is supported by the OM agent and IAPA components that are installed with the Diagnostics commander server.

See "Integrations with other Products" in the *Diagnostics User Guide* for more information on Diagnostics data in BSM/APM.

Task 1: Prepare the Diagnostics Commander Server

Identify the Diagnostics commander server to be used in the integration and prepare it as follows:

- Make sure that the Diagnostics commander server has the data that you want to expose in BSM/APM.

- Make sure that the Diagnostics commander server is configured to communicate with BSM/APM. This configuration is typically accomplished when the Diagnostics commander server is installed by specifying the following option during the installation:
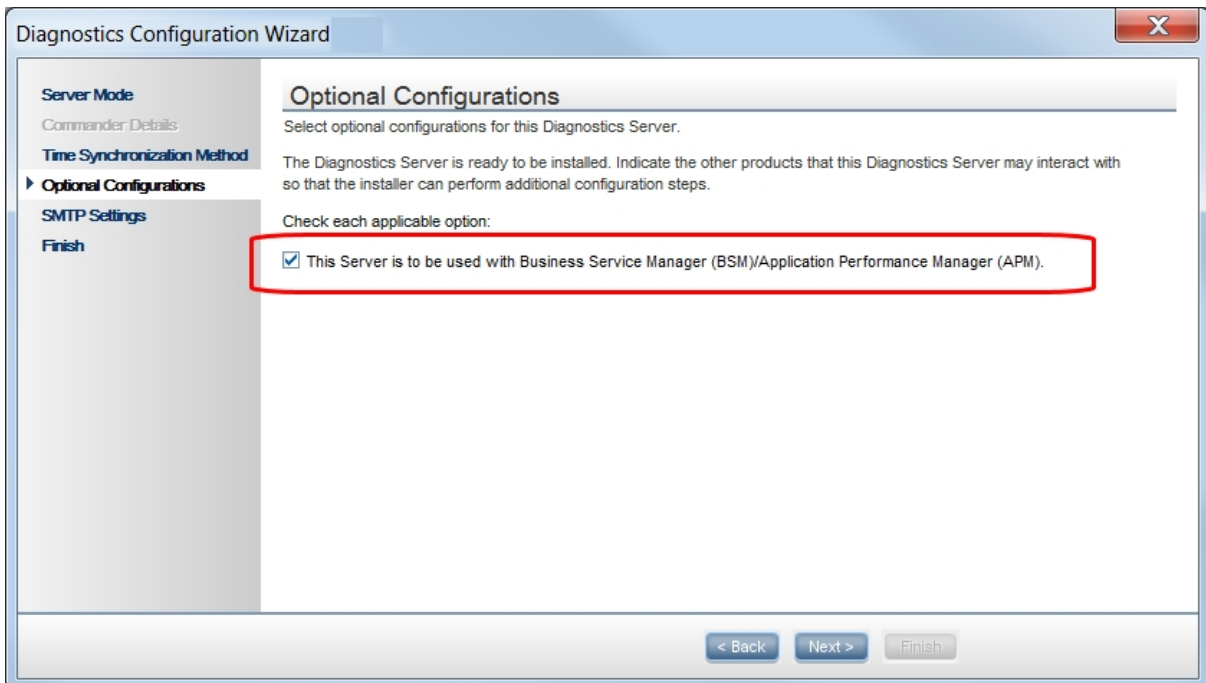
This option requires that the user running the installation have root access on Linux or Administrative privileges on Windows.

If the Diagnostics commander server was installed without this option, you can add the configuration to an existing Diagnostics commander server. You do not need to re-install the Diagnostics commander server. See "Manual Installation of OM Agent and IAPA Components" in the Diagnostics Server Installation and Administration Guide.

You can verify that the OMA Agent and IAPA Components are installed on an existing Diagnostics command server by checking if the following directory exists on the Diagnostics Commander Server host: **C:\Program Files\HP\HP BTO Software** or **/opt/HP/HP_BTO_Software**.

- Make a note of the fully-qualified domain name (FQDN) and port of the Diagnostics commander server. You will need this information in a later task.

You can access the System Health view in the Diagnostics UI to find this information:
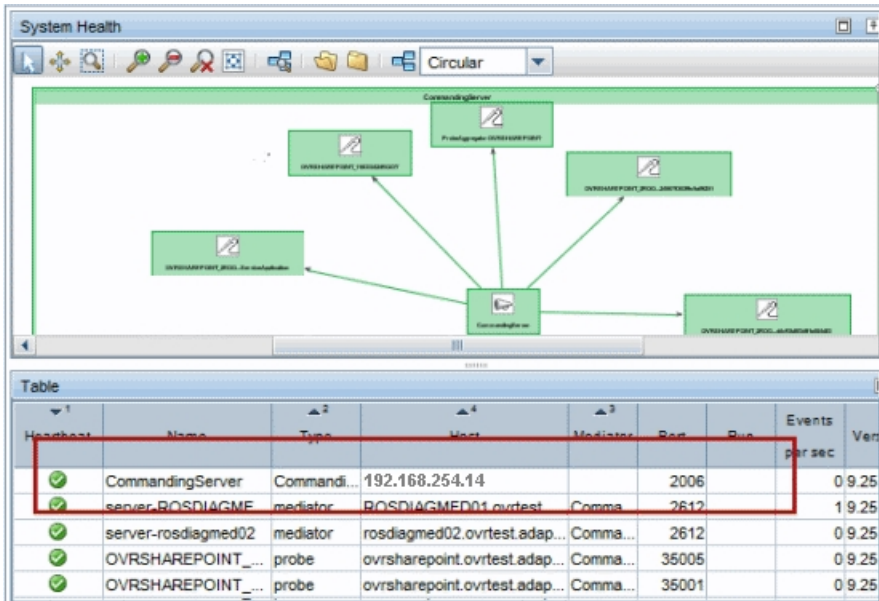
- If there is a firewall between the Diagnostics commander server and the BSM/APM Gateway Server, open the port used by the Diagnostics commander server. See "Working with Firewalls " on page 18.

Task 2: Identify the BSM/APM Servers and Determine How They are Accessed

Identify the BSM/APM Gateway Server and Processing Servers and understand how they are accessed. Work with the BSM/APM administrator to obtain this information. You need to know the following:

- The Gateway Server URL to be used for access by data collectors. This may be any of the following:

Default Virtual Gateway Server for Data Collectors URL. Defines the URL used to access the Gateway Server for Data Collectors. Specify the full URL with the port number (for example: http://myhost.mydomain.com:88). For the host name in the URL, supply the full name of the host, including the domain name and the port number. If a NAT device (i.e. load balancer, reverse proxy, SSL Accelerator) is in use to access the Gateway Server for Data Collectors, supply the URL of the NAT device including the port number (for example: https://virtualIP:99).

Direct Gateway Server for Data Collectors URL. Defines the URL used by internal services to access the Gateway Server for Data Collectors. Even if a load balancer is in use, supply the internal (not virtual) host name.

Local Virtual Gateway Server for Data Collectors URL. Defines the URL used to access the specified machine's Gateway Server for Data Collectors. Specify the full URL with the port number (for example: http://myhost.mydomain.com:88). For the host name in the URL, supply the full name of the host, including the domain name and port number. If defined, this setting's value overrides the Default Virtual Gateway Server for Data Collectors URL setting.

> **Tip:** If BSM/APM has already been configured for Data Collectors, you can obtain these values from the BSM/APM UI as follows. Access **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. In the Infrastructure Settings Manager section, select **Foundations** and

> then select **Platform Administration** from the drop-down list. In the "Platform Administration – Host Configuration" group you can view the Data Collector URLs that are to be used by Diagnostics.

See the the APM Application Administration Guide for more information.

- The Gateway Server URL to be used for access by application users. This is the **Default Virtual Gateway Server for Application Users URL**. If this URL is different from the Gateway Server URL used by data collectors you must edit the **<diag_server_install_dir>\etc\webserver.properties** file and add to the parameter **bac.gw.whitelist** the Gateway Server URL used by data collectors in the format:

  > http://<FQDN of the Gateway Server URL used by data collectors>/topaz

  For example: **http://apm_gw_machine.mydomain.com/topaz**

  > **Note:**
  >
  > - You can add multiple Gateway Servers using a comma (**,**) as a separator.
  >
  > - If you use different Gateway Servers for users and data collectors, you must add all of the Gateway Servers used.

- The Data Processing Server (DPS) URL that is to be used for access from the Gateway Server. Typically this is
  http://<data_processing_server_FQDN>:80.
- Login information to the DPS host. These credentials are needed as part of the certificate configuration in some scenarios.

  For more information about the DPS, see the Platform Administration section in the APM Help.

Task 3: Enable HTTPS Communication

If the Diagnostics commander server is going to send data to a BSM/APM server in a hardened environment, you must configure the Diagnostics commander server to communicate securely with the BSM/APM Gateway Server.

The basic flow for any data collector connecting to secure BSM/APM is as follows:

- Obtain the appropriate root CA certificate(s) from the BSM/APM environment and import it into the JVM used by the data collector.
- Configure the connection to BSM/APM to use HTTPS.
- Make sure data flows over the secure connection.

Note: APM 9.40 and later (https) does not accept self signed certificates. When integrating Diagnostics with APM 9.40 or later, make sure the Diagnostics server certificates are not self signed.

To enable secure communications between the Diagnostics commander server and the BSM/APM Gateway Server:

1. (Optional) Enable the Diagnostics commander server for HTTPS communication as described in the "Enabling HTTPS Between Components" chapter of the Diagnostics Server Installation and Administration Guide.

2. If your Diagnostics commander server is configured with SSL:

- Copy the Diagnostics certificate file, **diag_server_commander.cer**, from the Diagnostics commander server installation directory, **<diag_server_install_dir>/etc/**, to the BSM/APM host.

- Import the copied certificate, **diag_server_commander.cer**, into the BSM/APM server cacert keystore by running the following commands on all of the BSM/APM Gateway and Data Processing Servers, even if they are not accessed directly (for example, even if they are accessed using reverse proxy, or through a load balancer):

  ○
  ```
  <BSM/APM_server_install_dir>/jre/bin/keytool
  -import -file <copied _diag_certificate_directory>/diag_server_commander.cer
  -keystore <BSM/APM_server_install_dir>/jre/lib/security/cacerts -alias
  SERVER
  ```

  ○
  ```
  <BSM/APM_server_install_dir>/jre64/bin/keytool
  -import -file <copied _diag_certificate_directory>/diag_server_commander.cer
  -keystore <BSM/APM_server_install_dir>/jre64/lib/security/cacerts -alias
  SERVER
  ```

  - Replace `<BSM/APM_server_install_dir>` with the path to the installation directory for the BSM/APM server host.
  - Replace `<copied_diag_certificate_directory>` with the path to the copied Diagnostics certificate file.

  Type **changeit** when you are prompted to enter the keystore password.

  Type **yes** instead of the default **no** when you are asked if the certificate should be trusted.

- Restart all of the BSM/APM Gateway and Data Processing Servers.

3. Copy all root CA certificates (for example, for reverse proxy, Data Processing Servers, Gateway Servers) that were issued for the BSM/APM environment, **<BSM/APM_certificate_file.cer>,** to the Diagnostics Server host.

4. Import the copied certificates into the Diagnostics Server cacert keystore by running the following command on the Diagnostics Server host.

```
<diag_server_install_dir>/jre/bin/keytool
-import -file <copied_BSM/APM_certificate_directory>/<BSM/APM_certificate_
file.cer>
-keystore <diag_server_install_dir>/JRE/lib/security/cacerts
```

- Replace `<diag_server_install_dir>` with the path to the installation directory of the Diagnostics commander server.

- Replace `<copied_BSM/APM_certificate_directory>` with the path to the copied BSM/APM certificate file.

Type **changeit** when you are prompted to enter the keystore password.

Type **yes** instead of the default **no** when you are asked if the certificate should be trusted.

5. The communication between the Diagnostics commander server and the BSM/APM Gateway Server is

now secure. Select **HTTPS** for the Diagnostics Server protocol field when you register the Diagnostics commander server.

Task 4: Register the Diagnostics Commander Server in BSM/APM

1. Log in to BSM/APM.

2. Select **Admin > Diagnostics**.The Diagnostics Server Details page is displayed:

3. Provide the details for the Diagnostics commander server as follows:

   Diagnostics Server host name. Enter the fully-qualified host name of the Diagnostics commander server.

   If you have enabled HTTPS communication (as described in "Task 3: Enable HTTPS Communication " on page 9), enter the Diagnostics commander server name exactly as it was specified in the **CN** parameter when you created the keystore for the Diagnostics commander server. You should have used the **fully qualified domain name** for the subject (CN) in the certificate.

   Diagnostics Server port number. Enter the port number used by the Diagnostics commander server. Your Diagnostics commander server may use the default port numbers: **2006** for HTTP or **8443** for HTTPS.

   Diagnostics server protocol. Select the communication protocol through which BSM/APM connects to Diagnostics commander server, either **HTTP** or **HTTPS**.

   If you select **HTTPS** as your communication protocol, the Diagnostics commander server must be enabled for HTTPS. See "Task 3: Enable HTTPS Communication " on page 9.

   Diagnostics root context. If BSM/APM is configured to use a custom context root and you have configured Diagnostics commander server to use a custom context root, enter the Diagnostics commander context root. See "Configuring a Custom Context Root" in Diagnostics Server Installation and Administration Guide

   > **Note:** To be able to open Diagnostics or MyBSM from the BSM/APM user interface, the user must have access to the Diagnostics Commander through the URL configured when registering Diagnostics in BSM/APM.

4. Click **Submit**.

   If the server name you entered is incorrect or if the server is unavailable, an error message is displayed. Correct this information if necessary and click **Submit** again.

   The Diagnostics commander server details are saved in BSM/APM and the BSM/APM server details are automatically registered on the Diagnostics commander server host.

   You can view the BSM/APM server details in your Diagnostics Server configuration by viewing the Registered Components page at `http://<Diagnostics_Commanding_Server_ Name>:2006/registrar/`. View the rows where the type is "APM Server".

5. The **Registration** tab in the Diagnostics Configuration page opens.
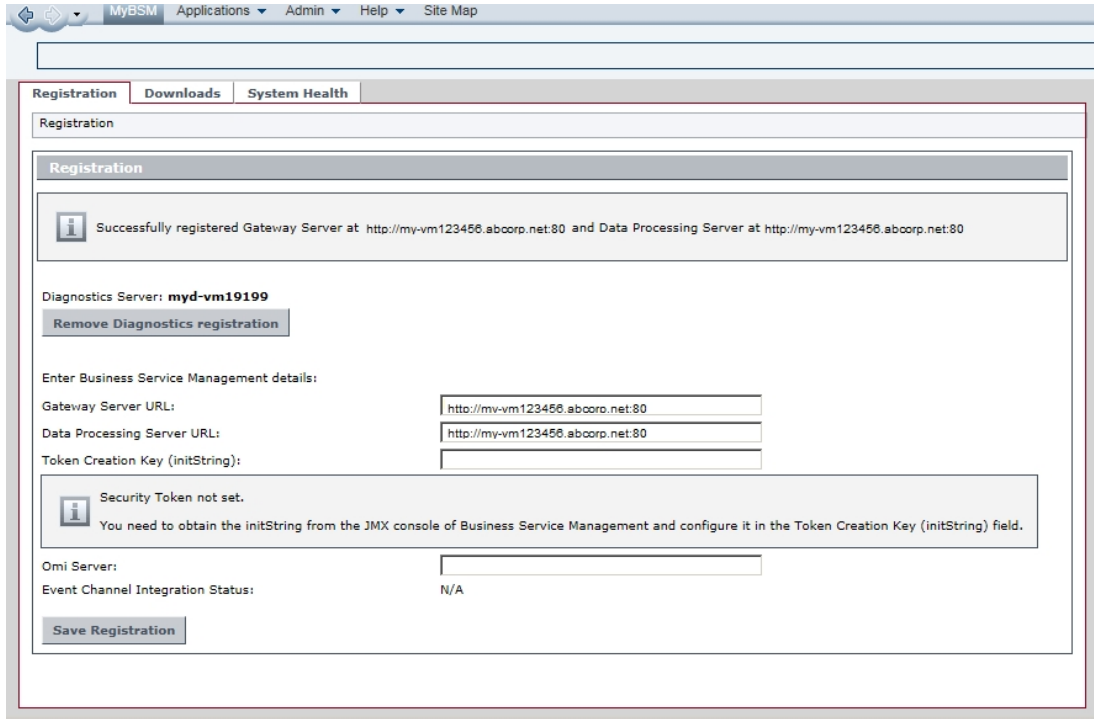
Provide the details for the BSM/APM servers as follows:

Gateway Server URL. By default, the root URL of the current BSM/APM Gateway Server is displayed. Modify this as needed. See "Task 2: Identify the BSM/APM Servers and Determine How They are Accessed" on page 8.

Data Processing Server URL. Typically you can leave this field at the default value. In high-availability deployments where the DPS's functionality changes from one DPS to another, enter the Gateway Server URL for this field. In such deployments the BSM/APM DPS server cannot be accessed from the Diagnostics Server and the BSM/APM Gateway Server has been configured to tunnel certificate requests to the Processing Server (such as when the Gateway and Processing Server are on the other side of a Load Balancer or SSL Accelerator).

You may still need to manually grant certificates as described in the following step.

Token Creation key (initString). Enter the BSM/APM token creation key in the field. To find the Token Creation Key (initString), enter the following URL in a browser and locate the initString in the table that is displayed:

-
    ```
    http://<BSM/APM Gateway Server>:29000/mbean?objectname=Topaz%3Aservice%3DLW-
    SSO+Configuration
    ```

Once you save the registration, this token creation key is written to the Diagnostics **lwsso.properties** file.

OMi Server. Specify the OMi server host name that Diagnostics needs to send threshold violation events.

Event Channel Integration Status. The event channel is how the OM agent and IAPA components of the Diagnostics commander server send threshold-violation events to OM. The event channel requires certificates to communicate securely.

If the Event Channel Integration status is "Certificate request pending" then the required certificates have been requested automatically. You can proceed to the next step.

6. Click **Save Registration**.

If the certificate grant is pending, the save will result in a message indicating that the certificate has been requested and it needs to be granted on the OMi server for successful Event Channel Integration.
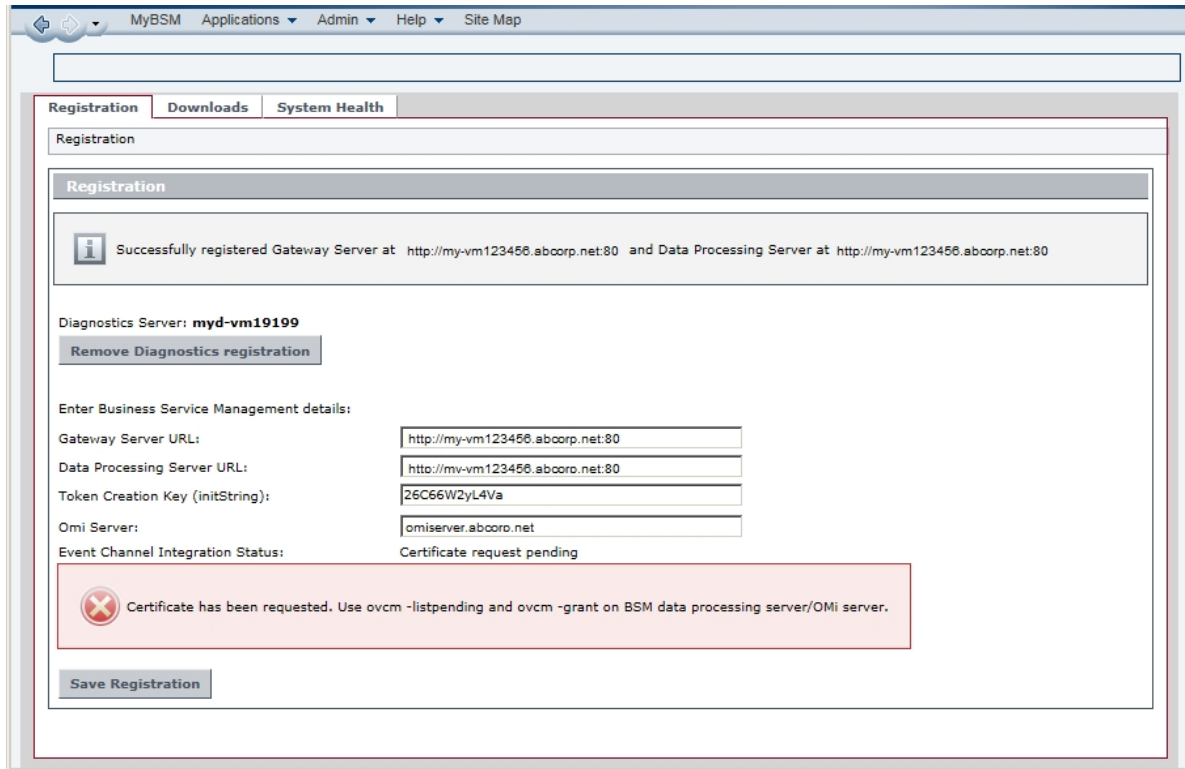
7. Log in to OMi and navigate to **Administration** > **Setup and Maintenance** > **Certificate Requests** page and grant the certificate.

> **Note**: You can also grant the certificates by running the command `ovcm -grant` on the OMi Server.

8. Click **Save Registration**. Event Channel Integration shows **OK**.
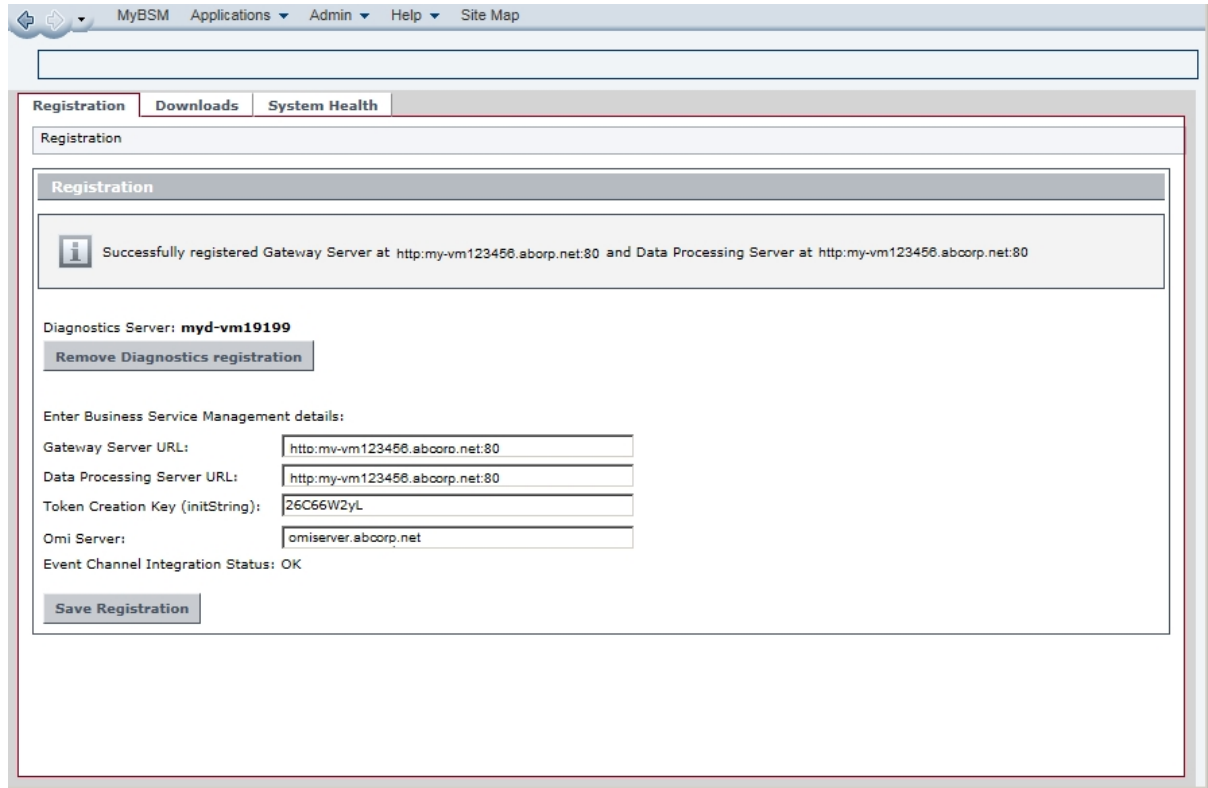
See "Event Status Integration Status Errors" on page 1 for any problems with the OM Agent and IAPA installation or the certificates.

Task 5: Manually Configure the Diagnostics Server with the OMi Server

To enable the Diagnostics server to send events related to threshold violations to the OMi server:

1. In the Diagnostics server, in the server\bin directory run the following:

   ```
   cscript switch_ovo_agent.vbs -server <FQDN of OMi> -cert_srv <FQDN of OMi>
   ```

2. Go to **OMi Administration > Certificate Requests** and grant the required certificates.

3. Run the following script again:

   ```
   cscript switch_ovo_agent.vbs -server <FQDN of OMi> -cert_srv <FQDN of OMi>
   ```

Task 6: Perform Post-Registration Configuration

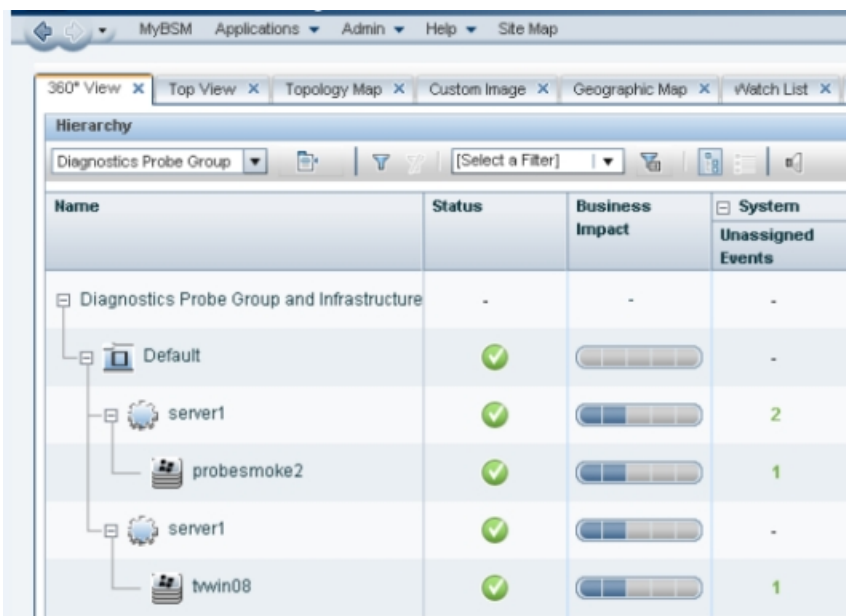Perform the following steps as needed for your deployment environment.

- Enable cookies in the web browser used to access BSM/APM.

  Cookies must be enabled to view Diagnostics data in BSM/APM. This can usually be accomplished by adding the registered Diagnostics commander server as a trusted site in the browser configuration.

Task 7: Verify the Integration

You verify the integration of Diagnostics with BSM/APM as follows:

- In BSM/APM, select **Applications > Diagnostics** to open the Diagnostics UI.

  If the "Do you want to run this application" prompt appears, click **Run**.

  You should see the same user interface that you see when accessing the standalone Diagnostics commander server.

- In BSM/APM, select **Applications > Service Health** to open the Service Health pages.

  On the 360° View tab, select **Diagnostics Probe Groups and Infrastructure**. Expand the root in the Name column. You should see a server for each agent that reports to the Diagnostics commander server.

If these verification steps fail, see "Troubleshooting the Integration of BSM/APM with Diagnostics" on page 26.

For more information about how Diagnostics data appears in BSM/APM, see the Diagnostics User Guide.

Task 8: Assign Permissions for Diagnostics Users in BSM/APM

When an existing or new BSM/APM user opens Diagnostics from BSM/APM, their permissions are picked up from the BSM/APM session.

In BSM/APM, the permissions for Diagnostics are specified in the **Admin > Platform > Users and Permissions > User Management** page, **Diagnostics** context:

When applying permissions in BSM/APM, administrators can grant Diagnostics users the following types of permission operations:

- **Change**: Enables viewing Diagnostics administration and configuring the Diagnostics settings.
- **View**: Enables viewing the Diagnostics application when accessing Diagnostics from BSM/APM.
- **Execute**: Enables setting thresholds in Diagnostics.
- **Full Control**: Enables performing all operations on Diagnostics, and granting and removing permissions for those operations.

Diagnostics permissions can also be inherited from BSM/APM roles.

> **Note:**
>
> - Any roles that have been created in the Diagnostics system are not propagated to BSM/APM when that Diagnostics system is integrated. For users that access Diagnostics by logging into BSM/APM, any role permissions defined in Diagnostics Applications do not apply. Application permissions must be set on specific BSM/APM user names or by using built-in user groups such as "(any_diagnostics_user)". You can assign and manage the comparable user permissions by using the BSM/APM User Management page.
> - Updates to BSM/APM user permissions are only picked up when the user opens Diagnostics. If Diagnostics is already open, changes will not be detected until it is closed and reopened. For example, changes to user specific permissions by an admin are not applied until that user logs in for a new session.

BSM/APM passwords are never sent to Diagnostics—Diagnostics trusts a successful BSM/APM login.

For detailed information about how to assign user permissions in BSM/APM, see Platform Administration in the BSM/APM Documentation Library.

Chapter 2: Additional Configuration of the Integration

The following configurations of the integration of Diagnostics with BSM/APM may be needed in your deployment environment:

- "Working with Firewalls " on the next page
- "Set the Password for Data Collectors to Access RTSM" on page 19
- "Enabling Integration with BSM/APM's SHA" on page 19
- "Discovery of IIS Metadata for CI Population of IIS Deployed ASP.NET Applications" on page 20
- "Configuring Individual IP Addresses for Multiple Application Servers" on page 20
- "Removing the Diagnostics Registration" on page 21
- "Diagnostics and OM Server Co-existence" on page 21
- "Upgrading When an Integration Exists" on page 24

Note: The examples in this chapter use hyphens to prefix command arguments. Copy-and-paste of the examples fails in some cases because the hyphen is pasted as a dash. Replace the dash with a hyphen (ASCII 0x2d) before running the command.

Working with Firewalls

The following diagram shows the default ports in a Diagnostics-BSM/APM deployment.
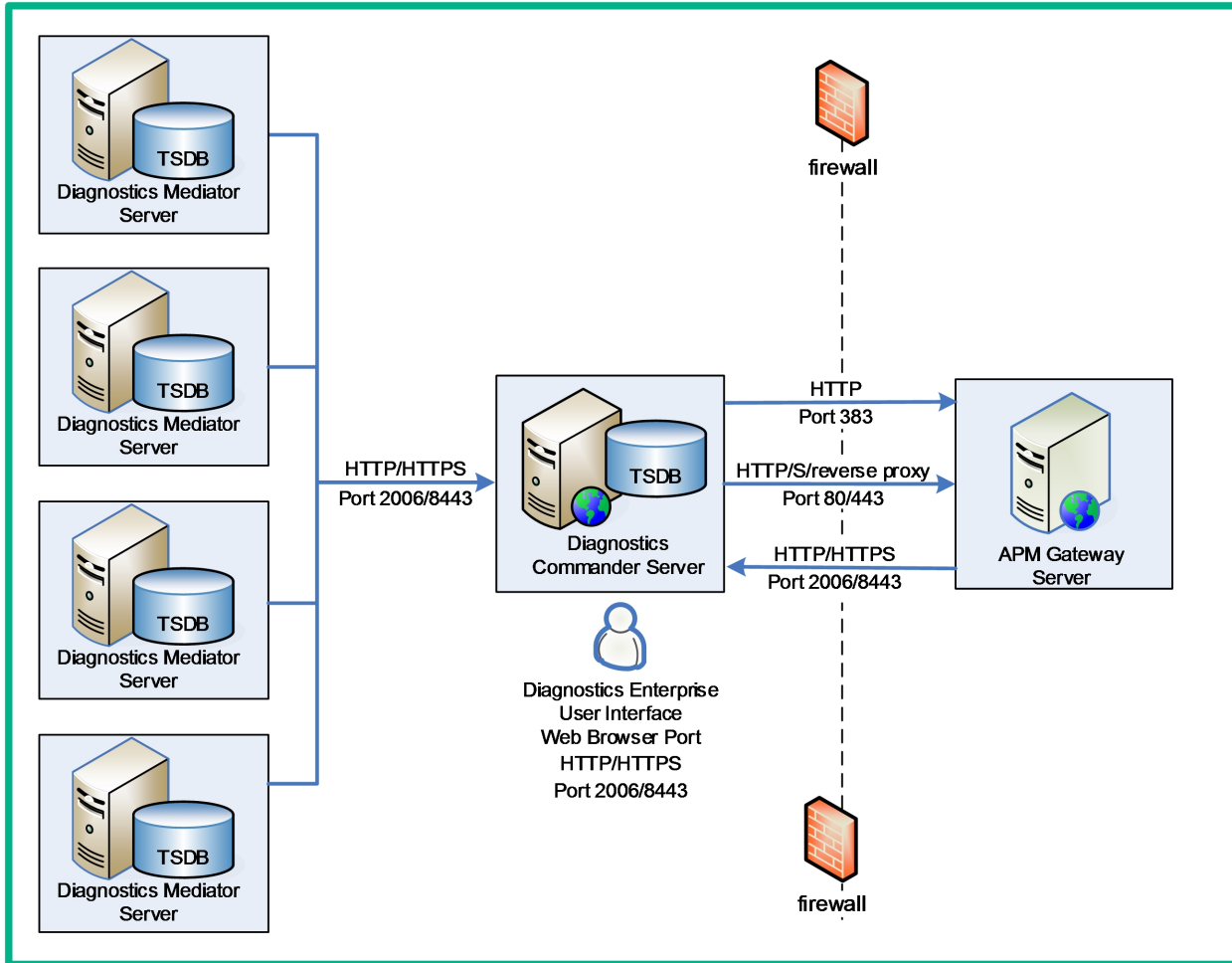
To configure the firewall to enable the communications between Diagnostics components and BSM/APM, open the ports that will allow the following:

- HTTP requests from the Diagnostics mediator servers to the Diagnostics Commander Server on port 2006 (HTTPS 8443).

- HTTP requests from the BSM/APM server to the Diagnostics Commander Server, on port 2006 (HTTPS 8443).

- HTTP requests from the Diagnostics commander server to BSM/APM Server on port 80 (Rerverse proxy 443).

- HTTP requests from the Diagnostics UI web browser client machine to theDiagnostics commander server on port 2006 (HTTPS 8443).

Set the Password for Data Collectors to Access RTSM

BSM/APM administrators configure the BSM/APM servers to create and connect to the BSM/APM databases/user schemas by using the Setup and Database Configuration utility.

This utility allows administrators to override the initial default password for all data collectors, including Diagnostics, to access the RTSM database. If the password is changed by using the Setup and Database Configuration utility, you must make a corresponding change to the password that is stored in the Diagnostics configuration.

To change the password in the Diagnostics configuration, access the Diagnostics commander server and modify the **<diag_server_install_dir>/etc/cmdbProperties.xml** file to add the obfuscated password to the <userPassword> entry:

```
<customer>
  <!-- customerId is an Integer -->
  <customerId>1</customerId>
  <customerName>Default Client</customerName>
  <userName>diagnostics</userName>
  <!-- userPassword may be obfuscated -->
  <userPassword>11z0h1wu61kxw1jyl1hse1jd21</userPassword>
  </customer>
<customer>
```

Create an obfuscated password using the web application included with Diagnostics. From standalone Diagnostics, access the Security page (http://<host name>:2006/security) and select **Encrypt Password** at the bottom of the page. Replace <host name> with the name of the host on which the Diagnostics server is installed.

For more information about the Setup and Database Configuration utility, see the APM Installation Guide.

Enabling Integration with BSM/APM's SHA

You can enable an integration between Diagnostics and BSM/APM's Service Health Analyzer (SHA). With this integration data samples containing host metrics and probe metrics are sent from the Diagnostics commander server to BSM/APM where the metrics are put into the BSM/APM SHA database.

The SHA application uses these metrics as well as metrics from other samples to create baselines. The SHA application compares metrics to the baseline and reports anomalies as performance issues are detected. For an anomaly you can drill down to Diagnostics Probes view or Hosts view for detailed Diagnostic data (see BSM/APM's Service Health Analyzer documentation for details on using SHA).

The integration of Diagnostics with SHA is not enabled by default.

To enable the integration:

1. On each Diagnostics mediator server that reports to the Diagnostics commander server, locate the **/etc/server.properties** file.

2. Make the following changes.

```
# Send host metrics for Service Health Analyzer (SHA)
bac.diag.sha.host.metric.create.samples=true
# Send probe metrics for Service Health Analyzer (SHA)
bac.diag.sha.probe.metric.create.samples=true
```

3. Restart each Diagnostics mediator server.

4. Once the integration is enabled and the host metrics and probe metrics from Diagnostics are available in BSM/APM's SHA database you then select these CIs in the SHA Admin application for use in anomaly detection.

   You can also define filters in Diagnostics to determine which host and probe metrics are sent to SHA's database. Use the following XML files in the Diagnostics server's **/etc** directory to filter these metrics. Filters are based on regular expression matching similar to data exporting.

   - **shaHostMetrics.xml.** Include/exclude filters for host metrics

   - **shaProbeMetrics.xml.** Include/exclude filters for probe metrics

Discovery of IIS Metadata for CI Population of IIS Deployed ASP.NET Applications

For CI population the .NET Agent installer automatically discovers the IIS configuration metadata for ASP.NET applications that are deployed under IIS versions 6.x or greater at the time of installation. You can request that the agent re-scan your IIS configuration to update for any additions or changes that occurred after installation. The re-scan does not occur automatically.

To request the rescan, execute **Rescan ASP.NET Applications** on the .NET Agent Host computer's Start menu.

For information about the CIs related to ASP.NET applications, see "CI Population and Models" in the Diagnostics User Guide.

For troubleshooting information related to the discovery of IIS Metadata, see .

Configuring Individual IP Addresses for Multiple Application Servers

By default, multiple application servers on the same machine monitored by a single Java Agent use the machine's main IP address for reporting purposes. This means that in the RTSM only one CI is created for all the application servers.

To configure the Java Agent to report each application server's individual IP address (so that in the RTSM a CI is created for each one), in the **probe.properties** file, set the **local.ip.for.reporting** parameter to the IP address to use for reporting. For example, `local.ip.for.reporting=123.123.123.123`. If you use individual property files for application servers you must set the local.ip.for.reporting parameter in each individual file.

You can also set the local.ip.for.reporting parameter using the application server start command: -Dlocal.ip.for.reporting parameter. For example, `-Dlocal.ip.for.reporting=123.123.123.123`.

For details on using individual property files and using the -D start command, see the "Specifying Probe Properties as Java System Properties" section in the Java Agent Guide.

Removing the Diagnostics Registration

You can remove the Diagnostics registration completely.

To remove the Diagnostics registration:

1. Select **Admin > Diagnostics**.

2. In the Registration tab, click the **Remove Diagnostics registration** button.

3. In the message that opens, click **OK** to confirm that you want to remove the Diagnostics registration.

   A message is displayed, confirming that you successfully removed the Diagnostics registration.

Diagnostics and OM Server Co-existence

If the Diagnostics commander server is to be installed on a host that already contains an OM agent, you must perform the following configuration.

# OM Agent Installed Before Diagnostics commander server is Installed

This scenario assumes that the OM agent is already present and reporting to an OM server on the host where the Diagnostics commander server is to be installed.

To setup coexistence when OM Agent is installed first:

1. Begin the Diagnostics commander server installation as described in Diagnostics Server Installation and Administration Guide.

At this step, select **This Server is to be used with Bsiness Service Manager (APM)/Application Performance Manager (APM)**.
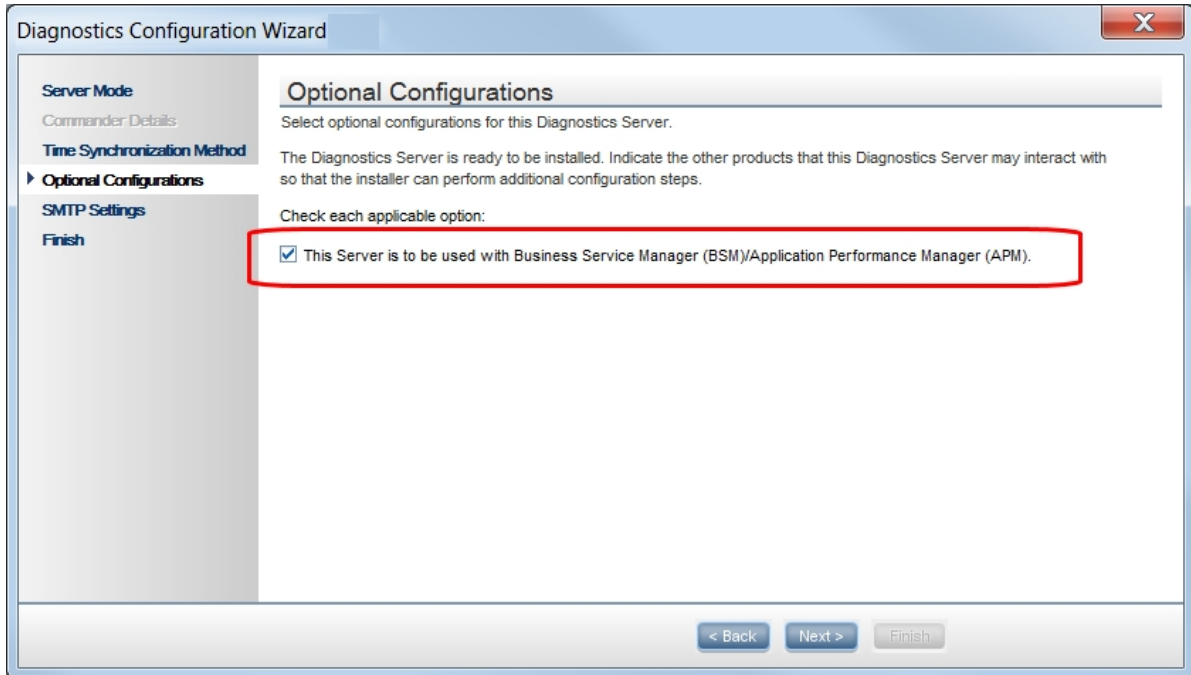
2. On the Diagnostic commander server, install the IAPA component manually.

   For more information, see "Manual Installation of OM Agent and IAPA Components" in the Diagnostics Server Installation and Administration Guide).

3. Register Diagnostics in BSM/APM as described in "Task 4: Register the Diagnostics Commander Server in BSM/APM" on page 11.

4. On the Diagnostics commander server host, go to **<diag_server_install_dir>\bin** and **execute switch_ ovo_agent.vbs** or on UNIX **switch_ovo_agent.sh**, specifying the OM server as the target for -server and -cert_srv.

   Note: On Linux, you have to run this command as root.

   For example:

   ```
   cscript switch_ovo_agent.vbs -server machine.mycompany.com -cert_srv
   machine.mycompany.com .com
   ```

5. Determine the core ID for the OM Server. On the Diagnostics commander execute:

   ```
   bbcutil -ping <OM Server>
   ```

6. Copy directory: **<diag_server_install_dir>\newconfig\ovo-agent\policies\mgrconf** to **<diag_server_ install_dir>\newconfig\ovo-agent\policies\tmp**

   If the mgrconf directory doesn't exist, contact support to get the content of this directory. Also if you have a more complex setup (for example with multiple OM managers) you may need to make additional changes to the file below.

7. Edit the file: **<diag_server_install_dir>\newconfig\ovo-agent\policies\tmp\mgrconf\FF9A8F04- B5E3-43C3-999B-7A9492C35014_data**.

- Locate the string ${OM_MGR_SRV} and replace all occurrences with the FQDN of the OM management server.

- Locate the string ${OM_MGR_SRV_ID} and replace all occurrences with the core ID of the OM management server.

- Locate the string ${OMi_MGR_SRV} and replace all occurrences with the FQDN of the OM management server.

- Locate the string ${OMi_MGR_SRV_ID} and replace all occurrences with the core ID of the OM management server.

> **Note:** In case of a more complex OM setup you may need to add additional entries in this file.

8. Go to the directory: **<diag_server_install_dir>\newconfig\ovo-agent\policies\tmp** and install the policy:

```
ovpolicy -install -dir mgrconf
```

Configure Trusted Certificates

In an environment with multiple OM servers, you must configure each server to trust certificates that the other servers issued. This task involves exporting every server's trusted certificate, and then importing this trusted certificate to every other server. You must also update the agent's trusted certificates, so that the agent also trusts the OM servers.

To configure trusted certificates for every OM server:

1. On every OM server, export the trusted certificate to a file using the following command:

```
ovcert -exporttrusted -file <file>
```

The command generates a file with the name that you specify.

2. Copy each file to every other server, and then import the trusted certificate using the following commands:

```
ovcert -importtrusted -file <file>

ovcert -importtrusted -ovrg server -file <file>
```

3. On the Diagnostics system (in case an agent was already installed), update the trusted certificates using the following

```
ovcert -updatetrusted
```

Upgrading When an Integration Exists

Check the Diagnostics Compatibility Matrix in the APM System Requirements and Support Matrixes for information about which versions of BSM/APM are compatible with Diagnostics.

An existing integration of BSM/APM and Diagnostics is affected by upgrades to either BSM/APM or Diagnostics.

If the BSM/APM system is upgraded or re-installed:

- Re-register the Diagnostics Commander Server in BSM/APM. See "Task 4: Register the Diagnostics Commander Server in BSM/APM" on page 11.

- It takes 12 hours before CIs from Diagnostics resume being sent to BSM/APM. You can force the CIs to be sent to BSM/APM sooner by performing a Synchronize operation. See "Synchronize CIs Between Diagnostics and BSM/APM" on page 28.

If the Diagnostics system is upgraded or re-installed:

1. Restore the **RegistrarPersistence.xml** file from the the backup etc directory folder to the new etc directory.

2. Check the Integration as described in "Task 7: Verify the Integration" on page 15.

After the upgrade, you will not be able to view events in APM. For further information, see "Diagnostics and OM Server Co-existence" on page 21.

Chapter 3: Diagnostics Event Forwarding to APM using SiteScope

You can forward Diagnostics HIs/KPIs to APM using SiteScope Technology Log File Integration monitor. The monitor enables you to view the CIs health in 360 degree view of APM.

To configure the SiteScope Technology Log File Integration monitor, follow these steps:

1. Log in to SiteScope.

2. Create a Technology Log File Integration monitor.

   > **Note**: Use the SiteScope Monitor Reference to configure the general properties of the monitor. Only attributes required for the integration are described below.

   - **Server** – Create a connected server to Diagnostics Commander and select it from the drop-down.

   - **Log file path** – Path must point to `\log\bachi_data.log` log file.
     For Diagnostics running on Windows, it can be something like this:
     `\\catvmdiag01.ftc.mynetwork.net\c$\MercuryDiagnostics\Server\log\bachi_data.log`

   - **Content match** – Use a regular expression to match `bachi_data.log`, for example, : `/(.)\|(.*)\|(.*)\|(.*)\|(.*)\|(.*)\|(.*)\|(\d)\|(.*)\|(.*)\|(.*)\|(.*)/`

   - **EMS time difference** – Use this field if SiteScope is not on the same timezone as the Diagnostics commander. You can offset the events' time_stamp using this offset.

   - **Field Mapping** – Make the following selections:
     - `time_stamp:DOUBLE=str_to_seconds($group10,"yyyy-MM-dd HH:mm:ss")`
     - `severity:INT=("C".equals($group0)) ? SEVERITY_CRITICAL : ("W".equals($group0)) ? SEVERITY_WARNING : ("N".equals($group0)) ? SEVERITY_INFORMATIONAL : SEVERITY_UNKNOWN`
     - `target_name=$group4`
     - `status="OPEN"`
     - `subject=$group3`
     - `instance=$group5`
     - `description=$group11`
     - `data_source="Diagnostics"`
     - `event_id=$group1 + "_" + $group4`
     - `logical_group=$group1`

   - **Data Type**– Select Legacy Events and click the **Load File** button.

   - **Topology Settings**– Select "custom" script, and leave it empty. We don't need EMS monitor to create topology, since Diagnostics created the topology directly in RTSM.

3. Save and run the monitor.

Chapter 4: Troubleshooting the Integration of BSM/APM with Diagnostics

This section includes:

-
-
-
-
-
-

Note: The examples in this chapter use hyphens to prefix command arguments. Copy-and-paste of the examples fails in some cases because the hyphen is pasted as a dash. Replace the dash with a hyphen (ASCII 0x2d) before running the command.

Unable to view HI status on Application Infrastructure CIs in APM

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

From APM 9.30, due to the OMi removal, Diagnostics sends events to OMi and continues to send CIs and metrics to APM.

As a result of this change, the Application Infrastructure CIs (Diagnostic Probe, Oracle/MSSql Database, IBM WebSphere MQ, WebSphere AS Dynamic Caching, IBM WebSphere MQ, IBM MQ, WebLogic AS. JBOSS AS, SQL Server, MSSQL Database, Oracle iAS, Oracle, SAP, SAP R3 Server, VMware ESX Server, and Host Node) do not show the correct HI Status in APM 9.30 and later.

The HI status for these CIs appears as *Undetermined* (blue question mark). If you are upgrading from BSM 9.2x to APM 9.50, the last status received for the CI before the upgrade will be displayed.

If SiS instance is available, follow the steps in .

Missing Link in the Standalone Diagnostics UI

If the Diagnostics UI is launched from BSM/APM and in addition the Diagnostics UI is launched in standalone mode on the same host, the Maintenance link in the Diagnostics UI in standalone mode is not available.

To resolve this issue close both instances of the Diagnostics UI and re-launch the Diagnostics standalone UI.

Unable to Reach Diagnostics Server

If after upgrade to APM 9.50, the following error message **Unable to reach Diagnostics server** is listed in **Admin** > **Diagnostics**, check the following:

- Make sure the Diagnostics server is also using https
- Make sure the Diagnostics server certificates are not self signed.

Authentication Dialog Displayed in MyBSM

If the Diagnostics Diagnostics commander server is installed in a different domain than the BSM/APM Gateway server, the MyBSM Diagnostics Dashboard may show an authentication dialog before the Diagnostics dashboard applet is displayed. This occurs if Lightweight Single Sign-On (LWSSO) has not been configured to add the Diagnostics server domain as a trusted domain.

To fix this issue, ensure that the domain that the Diagnostics server is running on is listed in BSM/APM's Single Sign-On page.

1. In BSM/APM select **Admin > Platform > Users and Permissions > Authentication Management > Single Sign-On Configuration**.
2. Click the **Configure** button.
3. Click **Next** in the wizard to get to the Single Sign-On page.
4. Click the **Add a Trusted host/domain** icon and enter the Diagnostics Server's domain.
5. Click **Next**.
6. Click **Next**.
7. Click **Finish**. This logs you out of BSM/APM. Log back in to BSM/APM and open the MyBSM Diagnostics Dashboard.

Diagnostics Cannot Access RTSM

If you do not see Diagnostics data in BSM/APM's Service Health application, check the **<diag_server_ install_dir>/log/ucmdb.log** file for errors such as:

```
WARNING : BAC uCMDB relay failed for customer Default Client. Connection to BAC
failed
java.lang.Exception: InvalidCredentialsException Authentication failed
```

This typically indicates that the password to access RTSM from Diagnostics is incorrect. All data collectors, including Diagnostics, must specify a password to access RTSM. This password is specified on the BSM/APM side by using the Setup and Database Configuration utility. On the Diagnostics side, this password is stored on the Diagnostics commander server in the **<diag_server_install_ dir>/etc/cmdbProperties.xml** file. These passwords must be the same. See "Set the Password for Data Collectors to Access RTSM" on page 19.

Synchronize CIs Between Diagnostics and BSM/APM

If you need to force a synchronization between Diagnostics and BSM/APM for Diagnostics populated models (CIs), a **synchronize** function is available on the Diagnostics commander server.

From the main Diagnostics UI select **Configure Diagnostics** (or from any Diagnostics view select the **Maintenance** link in the top right corner) and the Components page is displayed. Select the **synchronize** link to display the page for synchronizing models.

Anytime a BSM/APM system is upgraded or re-installed, a manual hard sync is needed (or a wait period of 12 hours) before CIs from Diagnostics are forwarded to BSM/APM. To do a hard sync, select **Hard**.

IIS Configuration Data Not Showing in BSM/APM

If the CI population from a .NET agent is not occurring in BSM/APM as expected, first rescan the environment as described in "Discovery of IIS Metadata for CI Population of IIS Deployed ASP.NET Applications" on page 20.

If the problem persists, the following summary of the workflow for CI population may be helpful in debugging:

- **The iis_discovery_data.xml file**. Discovered IIS configuration metadata is written to the **<probe_install_dir>\etc\iis_discovery_data.xml** file. Each rescan operation updates this file. At runtime the .NET Agent queries the **iis_discovery_data.xml** file for IIS configuration metadata associated with the instrumented appdomain. If the associated metadata is found, the agent forwards the data to its Diagnostic Server which populates the RTSM CIs for .NET application.

- **Privilege Requirements for Discovery of IIS Deployed ASP.NET Applications**. The user must have Administrator privileges on the machine that the .NET Agent is installed on, in order to execute WMI queries and create the **iis_discovery_data.xml** file.

- **Debugging the Discovery of IIS Deployed ASP.NET Applications**. If the **iis_discovery_data.xml** file is not created or there is any reason to suspect that some of its metadata may be inaccurate, you can enable the creation of a detailed debug file to examine the results of the WMI queries.

  To enable the creation of a detailed debug file, change the last parameter of the Target Property for the **Rescan ASP.NET Applications** shortcut on the computer's Start menu from "false" to "true". When the Rescan ASP.NET Applications shortcut is executed, a **<probe_install_dir>/log/AutoDetect.log** file is created. Note that you should have Administrator privileges when executing this shortcut. You can send the **AutoDetect.log** to Micro Focus Support for analysis.

Stop Sending Topology to APM

If you want to stop sending CI's and samples to APM, make the following configuration change.

In the `server.properties` file (located at `<commander-Server>/etc/server.properties`), modify the property:

`bac.ucmdb.model.population.enable=false`

Send Documentation Feedback

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

Feedback on APM - Diagnostics Integration Guide (Diagnostics 9.51)

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 docs.feedback@microfocus.com.

We appreciate your feedback!