HP Business Service Management

For the Windows, Linux operating systems

Version: 9.23

BSM - Diagnostics Integration Guide

Document Release Date: December 2013

Software Release Date: December 2013

Legal Notices

Warranty

The only warranties for HP 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. HP 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 HP 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™ 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 in the Documentation directory on the product installation media.

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: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

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

This document was last updated: Tuesday, November 26, 2013

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP 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 HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Welcome To This Guide

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

Although Diagnostics versions 9.x can integrate with older versions of BSM such as 8.x, the procedures in this guide are specific to Diagnostics 9.23 with BSM 9.23.

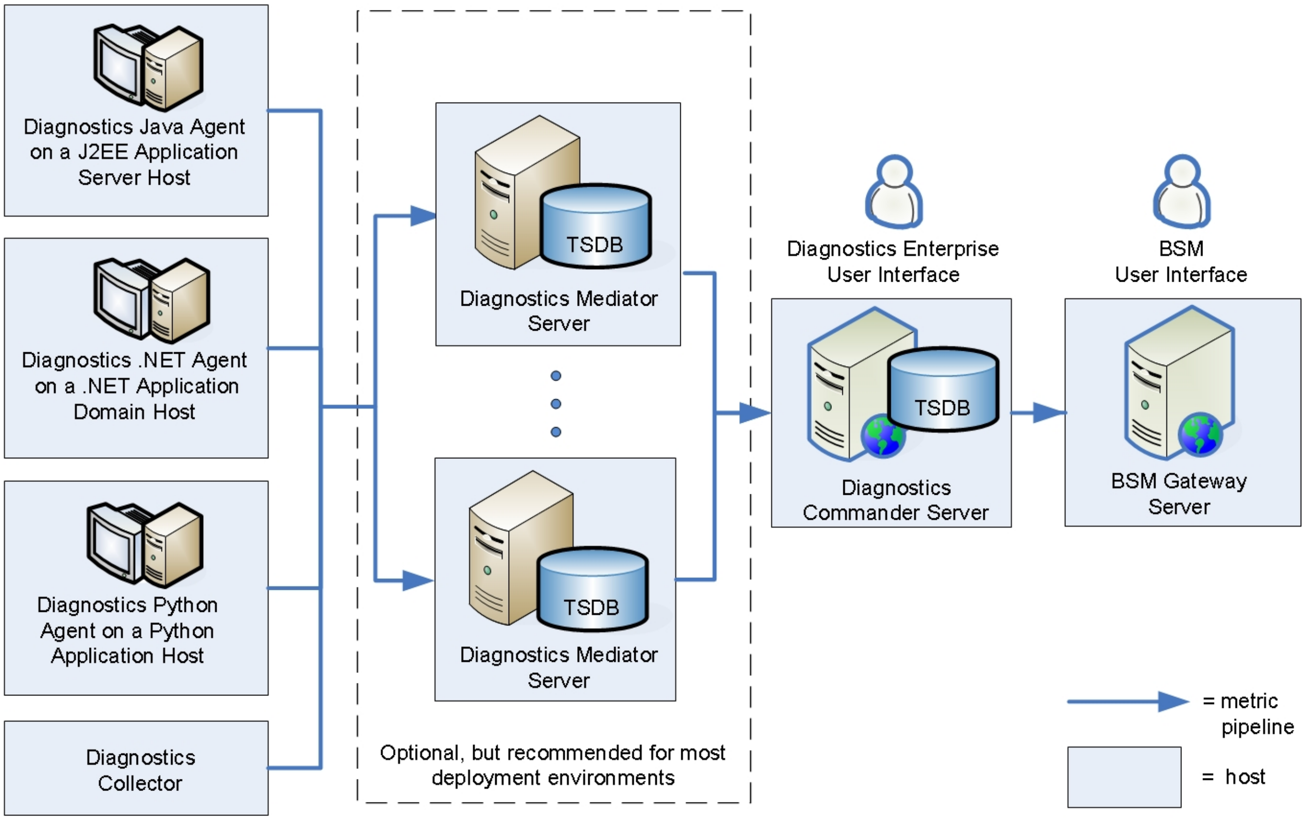
Chapter 1: Setting Up an Integration Between BSM and Diagnostics

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

This section includes:

About the Integration of Diagnostics with BSM

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


Diagnostics Java Agent on a J2EE Application Server Host
Diagnostics .NET Agent on a .NET Application Domain Host
Diagnostics Python Agent on a Python Application Host
Diagnostics Collector
TSDB
Diagnostics Mediator Server
TSDB
Diagnostics Mediator Server
Optional, but recommended for most deployment environments
Diagnostics Enterprise User Interface
TSDB
Diagnostics Commander Server
BSM User Interface
BSM Gateway Server
= metric pipeline
= host

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

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

Diagnostics Data Sent to BSM

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

- **Configuration items (CIs)**. Diagnostics populates an extensive set of application infrastructure, web service and business transaction CIs in the BSM 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 through the UCMDB interface.

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

  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 from Diagnostics in data samples. Diagnostics sends data samples to BSM and rules in BSM 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 Admin > Service Health. See the BSM Documentation Library for information on using Service Health Admin.

  Diagnostics sends data samples that contain the metrics toBSM where they re are persisted in the BSM 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.

  Diagnostics provides the following data samples to BSM:

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

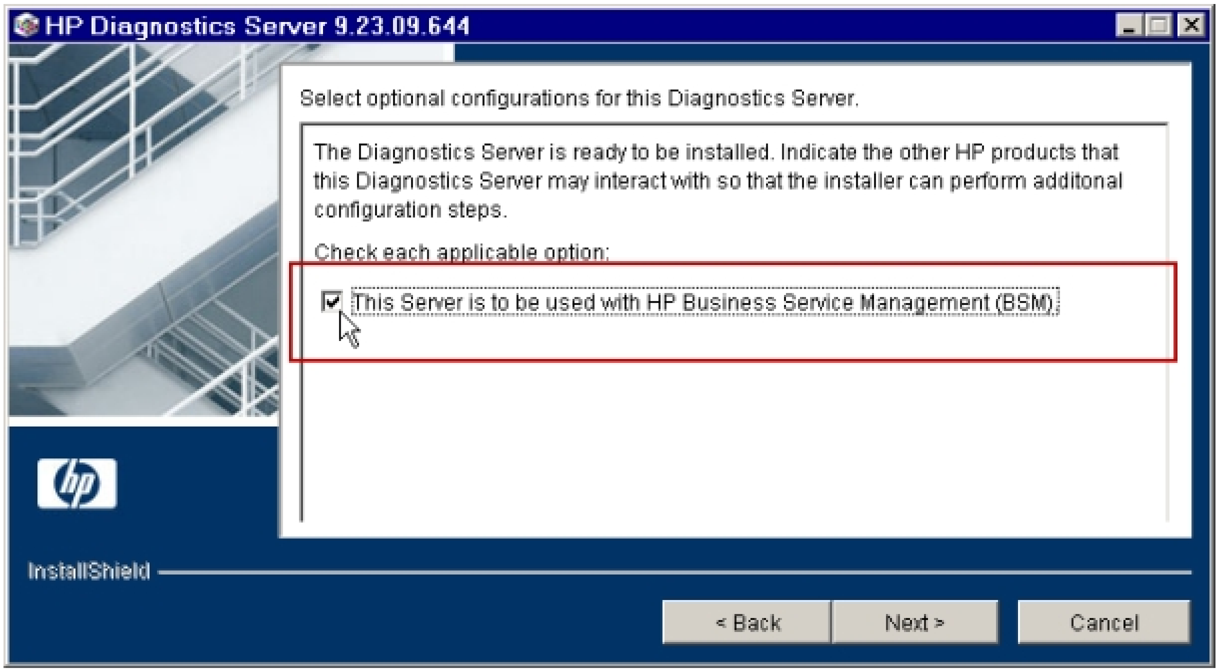
  This event channel is supported by the OM agent and IAPA components that are installed with the Diagnostics commander server.

See " Integrations with other HP Products" in the Diagnostics User’s Guide for more information on Diagnostics data in BSM.

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.
- Make sure that the Diagnostics commander server is configured to communicate with BSM. This configuration is typically accomplished when the Diagnostics commander server is installed by specifying the following option during the installation:



Select optional configurations for this Diagnostics Server.

The Diagnostics Server is ready to be installed. Indicate the other HP products that this Diagnostics Server may interact with so that the installer can perform additonal configuration steps.

Check each applicable option:

☑ This Server is to be used with HP Business Service Management (BSM).

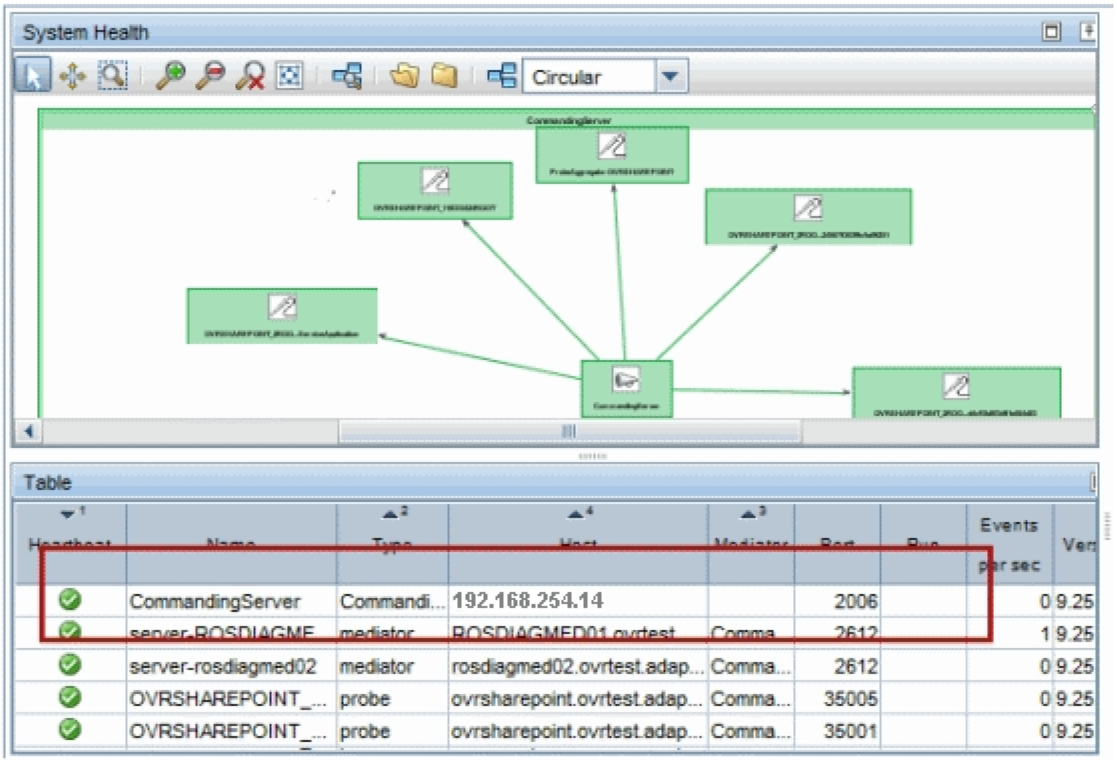
This option requires that the user running the installation have root access on Linux or Administrative privileges on Windows.

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 HP 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:



Heartbeat	Name	Type	Host	Mediator	Port	Bus	Events per sec	Ver
✓	CommandingServer	Commandi...	192.168.254.14		2006		0	9.25
✓	server-ROSDIAGME	mediator	ROSDIAGMED01.ovrtest	Comma	2612		1	9.25
✓	server-rosdiagmed02	mediator	rosdiagmed02.ovrtest.adap...	Comma...	2612		0	9.25
✓	OVRSHAREPOINT_...	probe	ovrsharepoint.ovrtest.adap...	Comma...	35005		0	9.25
✓	OVRSHAREPOINT_...	probe	ovrsharepoint.ovrtest.adap...	Comma...	35001		0	9.25

- If there is a firewall between the Diagnostics commander server and the BSM Gateway Server, open the port used by the Diagnostics commander server. See "Working with Firewalls " on page 23.

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

Identify the BSM Gateway Server and Processing Servers and understand how they are accessed. Work with the BSM 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 HP 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 has already been configured for Data Collectors, you can obtain these values from the BSM 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 HP Diagnostics.

See the BSM Platform Administration help for more information.

- 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 BSM Help.

Task 3: Enable HTTPS Communication (optional)

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

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

- Obtain the appropriate root CA certificate(s) from the BSM environment and import it into the JVM used by the data collector.

- Configure the connection to BSM to use HTTPS.

- Make sure data flows over the secure connection.

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

1. Enable the Diagnostics commander server for HTTPS communication as described in the "Enabling HTTPS Communication" chapter of the HP Diagnostics Server Installation and Administration Guide.

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

3. Import the copied certificate, **diag_server_commander.cer**, into the BSM server cacert keystore by running the following command on the BSM Gateway Server host:

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

   - Replace `<BSM_server_install_dir>` with the path to the installation directory for the BSM Gateway 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.

4. Copy the BSM certificate file, **<BSM_certificate_file.cer>,** to the Diagnostics Server host.

5. Import the copied certificate into the Diagnostics Server cacert keystore by running the following command on the Diagnostics Server host.

   ```
   <diag_server_install_dir>/_jvm/bin/keytool
   -import -file <copied_BSM_certificate_directory>/<BSM_certificate_file.ce
   r>
   -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_certificate_directory>` with the path to the copied BSM certificate file.

   When you are prompted to enter the keystore password, type the string that you assigned as the **storepass** password when you created the keystore.

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

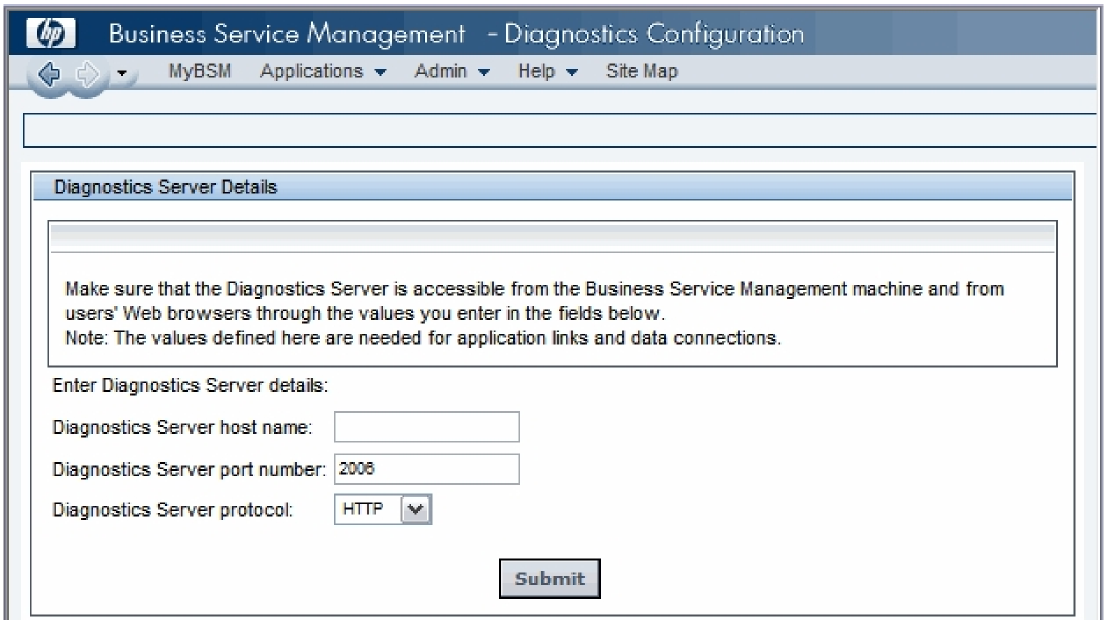
6. The communication between the Diagnostics commander server and the BSM Gateway Server is now secure. Select **HTTPS** for the Diagnostics Server protocol field when you register the Diagnostics commander server as described in See "Task 4: Register the Diagnostics Commander Server in BSM" below.

Task 4: Register the Diagnostics Commander Server in BSM

To register the Diagnostics Commander Server in BSM:

1. Log in to BSM.

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


Business Service Management - Diagnostics Configuration
MyBSM
Applications
Admin
Help
Site Map
Diagnostics Server Details

Make sure that the Diagnostics Server is accessible from the Business Service Management machine and from users' Web browsers through the values you enter in the fields below.
Note: The values defined here are needed for application links and data connections.

Enter Diagnostics Server details:

Diagnostics Server host name:

Diagnostics Server port number: 2006

Diagnostics Server protocol: HTTP

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 (optional)" on page 11), 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 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 (optional)" on page 11.

Diagnostics root context. If BSM 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 HP Diagnostics Server Installation and Administration Guide.

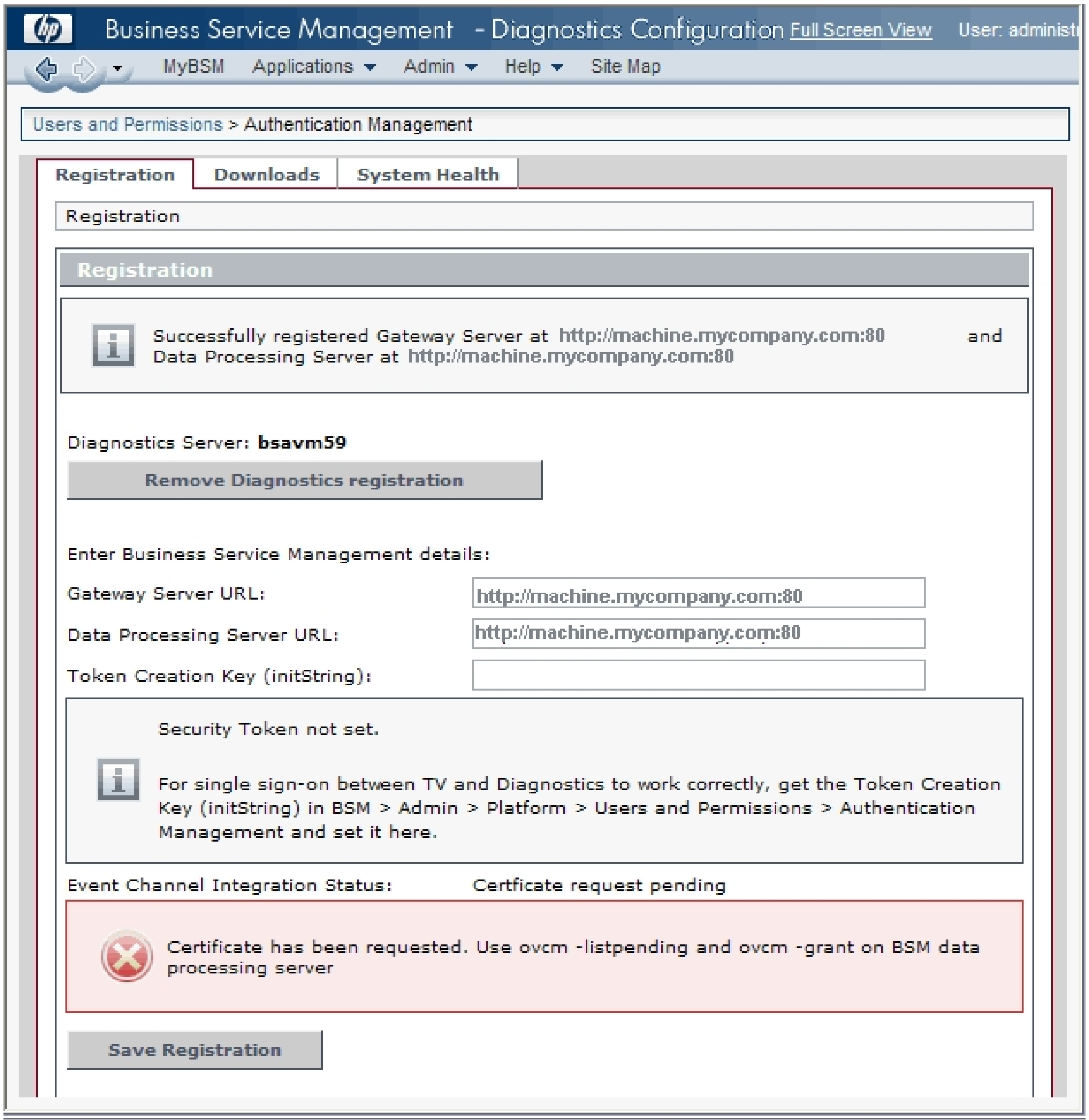
4. Click **Submit**.

   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 and the BSM server details are automatically registered on the Diagnostics commander server host.

   You can view the BSM 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 "BSM Server".

5. The **Registration** tab in the Diagnostics Configuration page opens:



Successfully registered Gateway Server at http://machine.mycompany.com:80 and Data Processing Server at http://machine.mycompany.com:80

Diagnostics Server: **bsavm59**

Enter Business Service Management details:

Gateway Server URL: http://machine.mycompany.com:80

Data Processing Server URL: http://machine.mycompany.com:80

Token Creation Key (initString):

Security Token not set.

For single sign-on between TV and Diagnostics to work correctly, get the Token Creation Key (initString) in BSM > Admin > Platform > Users and Permissions > Authentication Management and set it here.

Event Channel Integration Status: Certficate request pending

Certificate has been requested. Use ovcm -listpending and ovcm -grant on BSM data processing server

Provide the details for the BSM servers as follows:

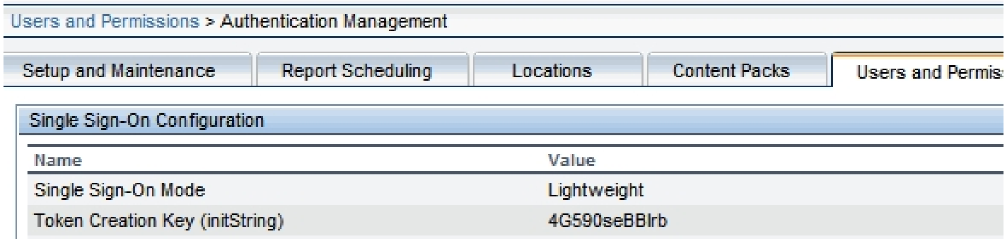
Gateway Server URL. By default, the root URL of the current BSM Gateway Server is displayed. Modify this as needed. See "Task 2: Identify the BSM Servers and Determine How They are Accessed" on page 10.

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 DPS server cannot be accessed from the Diagnostics Server and the BSM Gateway Server has been configured to tunnel certificate requests to the Processing Server (such as when the Gateway and Procesing 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). This setting is only relevant if the TransactionVision data collector is also being used in the deployment environment.

To avoid a user having to login again when drilling from Transaction Management to Diagnostics, enter the BSM token creation key in the field. You can copy the Token Creation Key (initString) from within BSM at **Admin > Platform > Users and Permissions > Authentication Management:**



Single Sign-On Configuration

Name	Value
Single Sign-On Mode	Lightweight
Token Creation Key (initString)	4G590seBBlrb

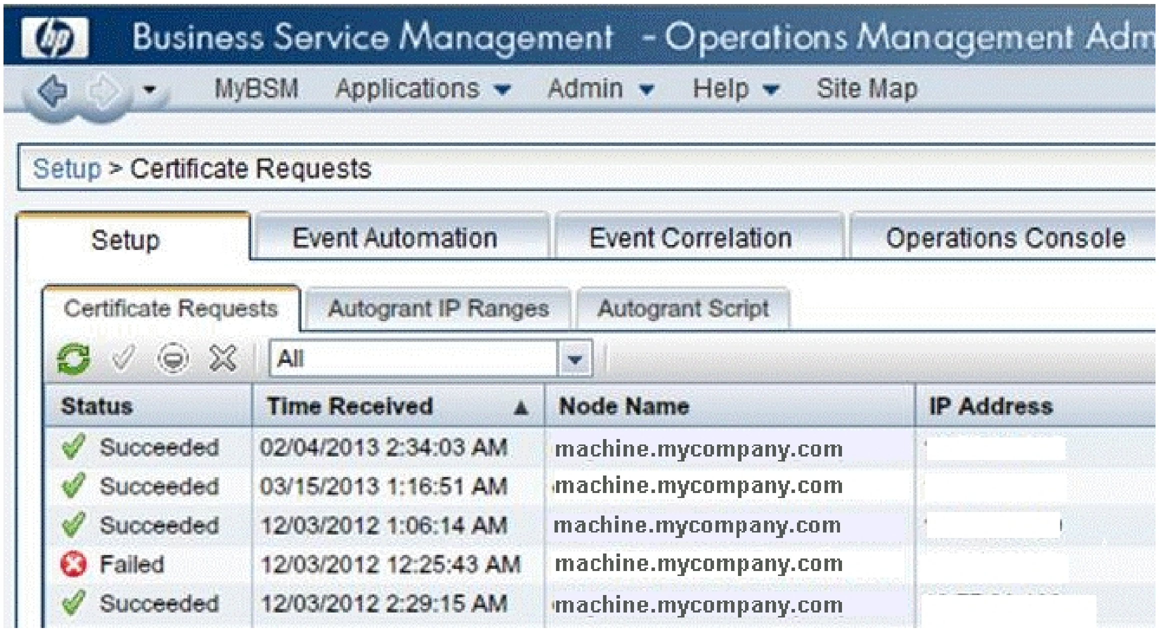
Once you save the registration, this token creation key is written to the Diagnostics **lwsso.properties** file.

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 BSM, where they in turn affect HI status. 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.

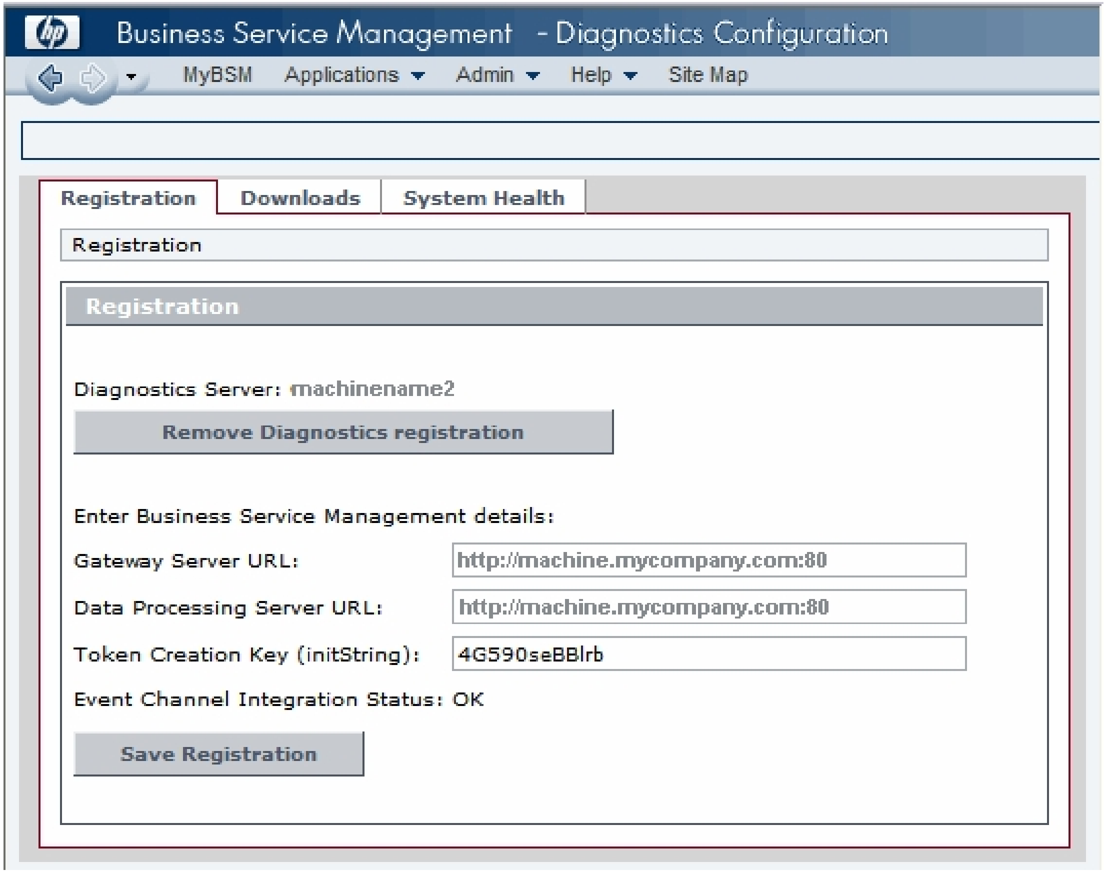
Some load balancer configurations require the certificates to be manually issued. See "Event Status Integration Status Errors" on page 32.

6. Still in the BSM user interface, select **Admin > Operations Management > Setup > Certificate Requests**. Select and grant the OM agent certificate from the Diagnostics commander server.



Status	Time Received ▲	Node Name	IP Address
✓ Succeeded	02/04/2013 2:34:03 AM	machine.mycompany.com	
✓ Succeeded	03/15/2013 1:16:51 AM	machine.mycompany.com	
✓ Succeeded	12/03/2012 1:06:14 AM	machine.mycompany.com	
✖ Failed	12/03/2012 12:25:43 AM	machine.mycompany.com	
✓ Succeeded	12/03/2012 2:29:15 AM	machine.mycompany.com	

7. Navigate back to the **Admin > Diagnostics > Registration** tab in the BSM user interface. Click **Save Registration** and verify that the Event Channel Integration Status is now OK:



Diagnostics Server: machinename2

Enter Business Service Management details:

Gateway Server URL: http://machine.mycompany.com:80

Data Processing Server URL: http://machine.mycompany.com:80

Token Creation Key (initString): 4G590seBBlrb

Event Channel Integration Status: OK

See "Event Status Integration Status Errors" on page 32 for any problems with the OM Agent and IAPA installation or the certificates.

8. Click **Save Registration**.

Task 5: Perform Post-Registration Configuration

Perform the following steps as needed for your deployment environment.

- Enable cookies in the web browser used to access BSM

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

Task 6: Verify the Integration

You verify the integration of Diagnostics with BSM as follows:

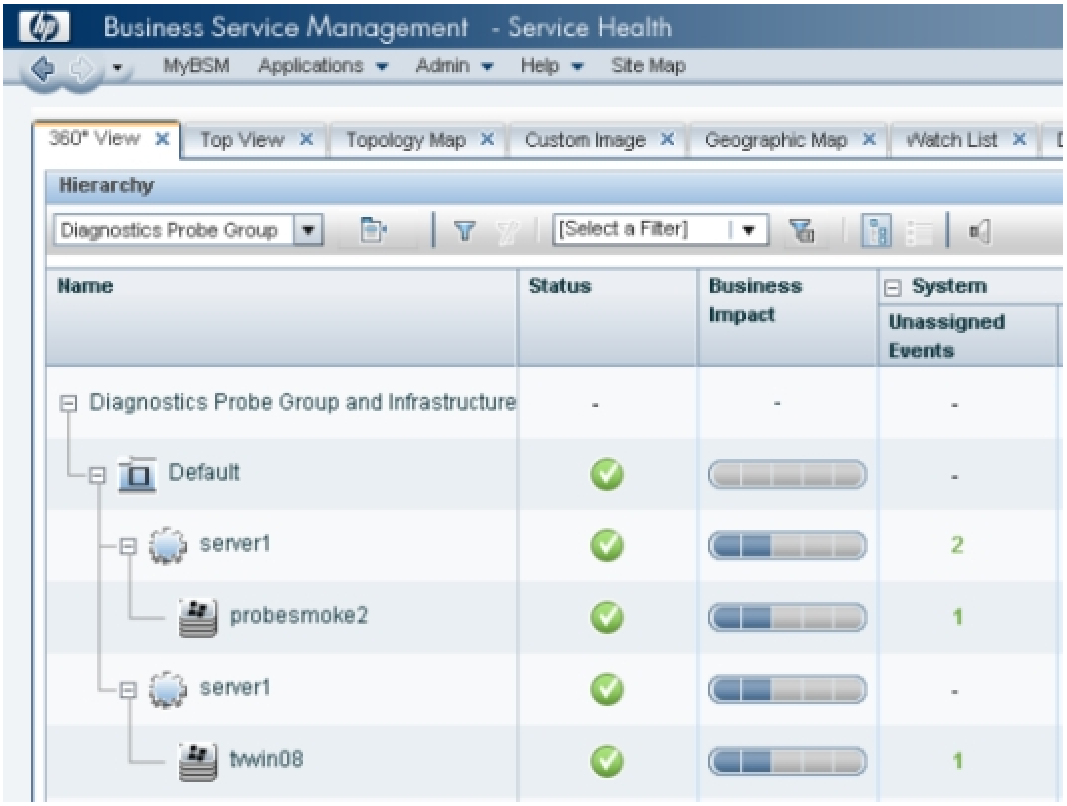
- In BSM, select **Applications > Diagnostics** to open the Diagnostics UI.

  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, 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.



Name	Status	Business Impact	System
			Unassigned Events
⊟ Diagnostics Probe Group and Infrastructure	-	-	-
⊟ Default	✓		-
⊟ server1	✓		2
probesmoke2	✓		1
⊟ server1	✓		-
twin08	✓		1

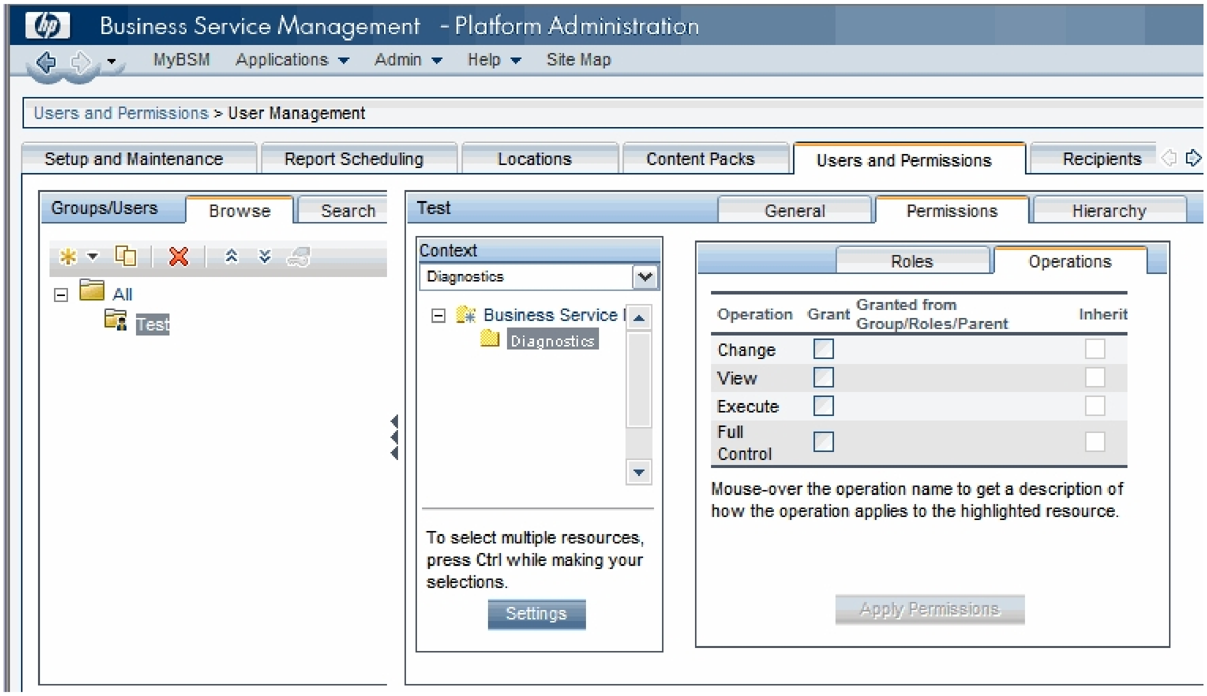
If these verification steps fail, see "Troubleshooting the Integration of BSM with Diagnostics" on page 32.

For more information about how Diagnostics data appears in BSM, see the HP Diagnostics User’s Guide.

Task 7: Assign Permissions for Diagnostics Users in BSM

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

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



Operation	Grant	Granted from Group/Roles/Parent	Inherit
Change	□		□
View	□		□
Execute	□		□
Full Control	□		□

Mouse-over the operation name to get a description of how the operation applies to the highlighted resource.

To select multiple resources, press Ctrl while making your selections.

When applying permissions in BSM, 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.
- **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 roles.

Note:

- Any roles that have been created in the Diagnostics system are not propagated to BSM when that Diagnostics system is integrated. For users that access Diagnostics by logging into BSM, any role permissions defined in Diagnostics Applications do not apply. Application permissions must be set on specific BSM 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 User Management page.

- Updates to BSM 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 passwords are never sent to Diagnostics—Diagnostics trusts a successful BSM login.

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

Chapter 2: Additional Configuration of the Integration

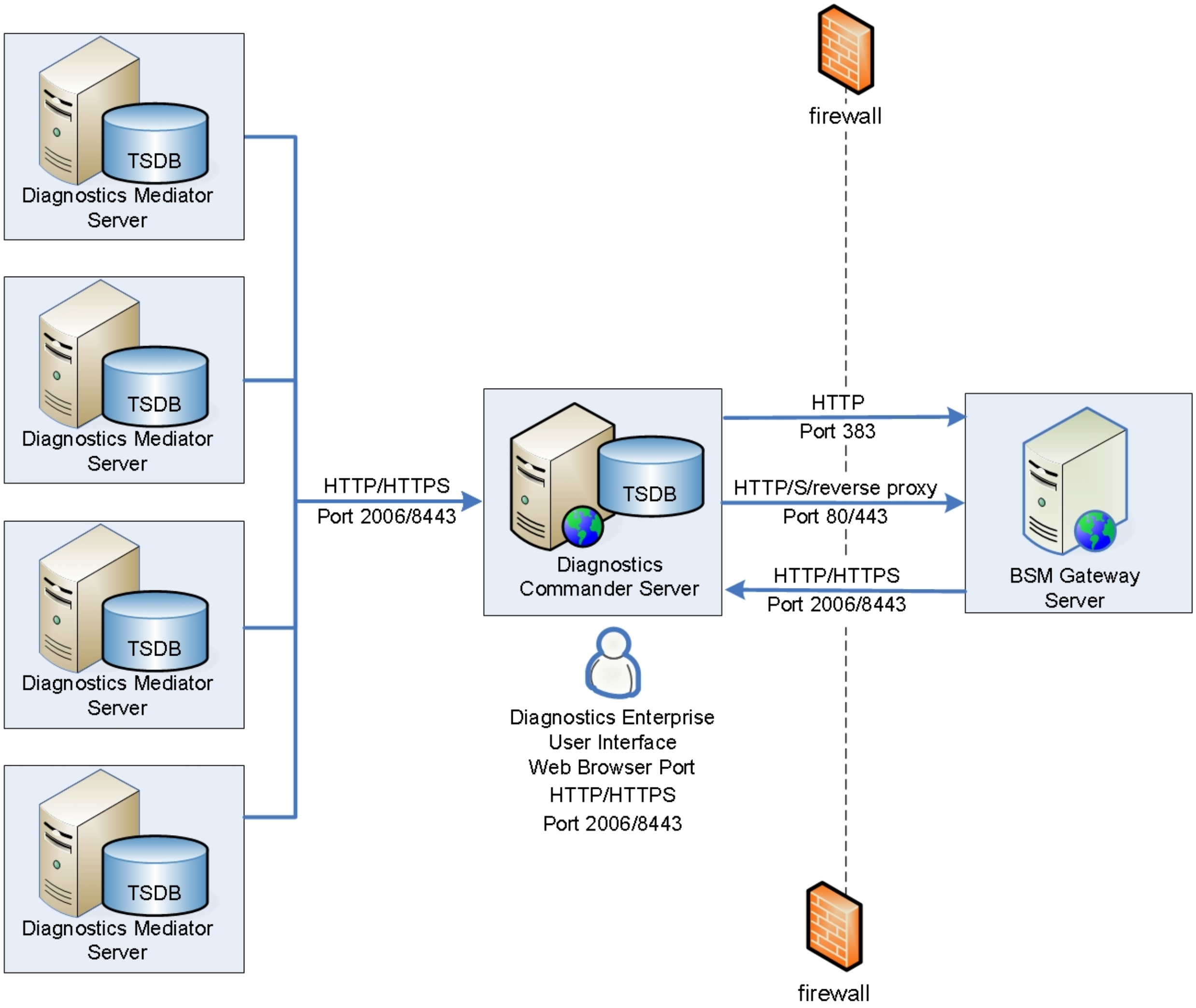
The following configurations of the integration of Diagnostics with BSM may be needed in your deployment environment:

- "Working with Firewalls " on the next page
- "Set the Password for Data Collectors to Access RTSM" on page 24
- "Enabling Integration with BSM’s SHA" on page 24
- "Integration with BSM’s Performance Graphing" on page 25
- "Discovery of IIS Metadata for CI Population of IIS Deployed ASP.NET Applications" on page 26
- "Removing the Diagnostics Registration" on page 27
- "Diagnostics and OM Server Co-existence" on page 27
- "Upgrading When an Integration Exists" on page 31

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 deployment.


TSDB
Diagnostics Mediator Server
TSDB
Diagnostics Mediator Server
TSDB
Diagnostics Mediator Server
TSDB
Diagnostics Mediator Server
HTTP/HTTPS
Port 2006/8443
TSDB
Diagnostics Commander Server
firewall
HTTP
Port 383
HTTP/S/reverse proxy
Port 80/443
HTTP/HTTPS
Port 2006/8443
BSM Gateway Server
Diagnostics Enterprise User Interface Web Browser Port HTTP/HTTPS Port 2006/8443
firewall

To configure the firewall to enable the communications between Diagnostics components and BSM, 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 server to the Diagnostics Commander Server, on port 2006 (HTTPS 8443).
- HTTP requests from the Diagnostics commander server to BSM Server on port 80 (Rerverse proxy 443). HI updates from the Diagnostics Commander Server to BSM on port 383.

- 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 administrators configure the BSM servers to create and connect to the BSM 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 BSM Installation Guide.

Enabling Integration with BSM’s SHA

You can enable an integration between Diagnostics and BSM’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 where the metrics are put into the BSM 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’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’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.

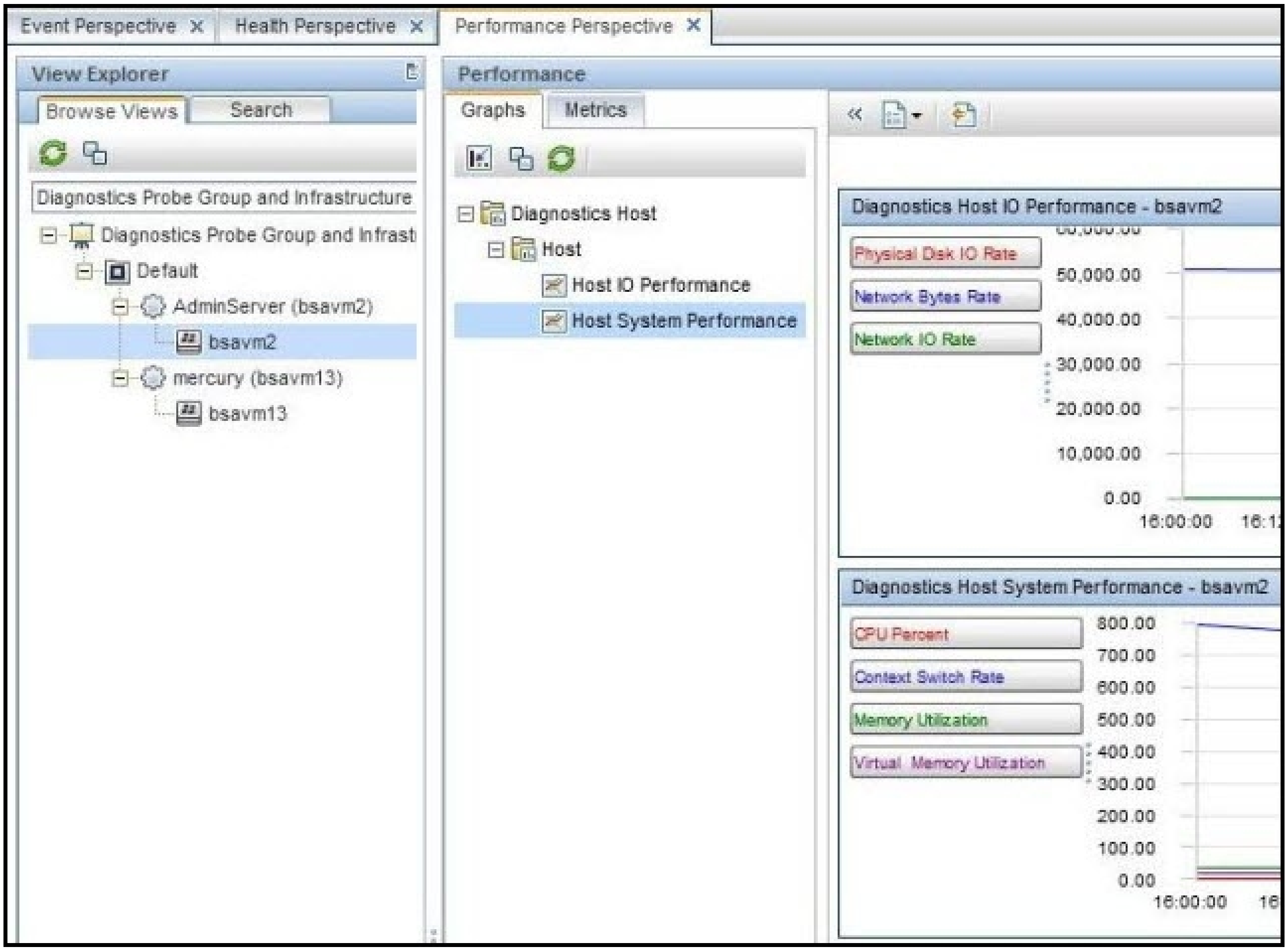
   - **shaHostMetrics.xml.** Include/exclude filters for host metrics

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

Integration with BSM’s Performance Graphing

The integration of Diagnostics with BSM allows you to graph Diagnostics data in BSM's Performance Graphing.

In the BSM UI (**Applications > Operations Management > Performance Perspective**) when you select a CI in the View Explorer tree you can see applicable Diagnostics graph templates in the Graphs tab. You can also graph individual Diagnostics metrics from the Metrics tab. An example from BSM is shown below.



If you do not see Diagnostics data as expected in the Performance Perspective tab, verify that the **Diagnostics Server host name** field specifies the FQDN of the Diagnostics commander server. See "Task 4: Register the Diagnostics Commander Server in BSM" on page 13.

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, select **Start > HP Diagnostics .NET Probe > Rescan ASP.NET Applications** on the .NET Agent Host.

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

For troubleshooting information related to the discovery of IIS Metadata, see "IIS Configuration Data Not Showing in BSM" on page 39.

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.

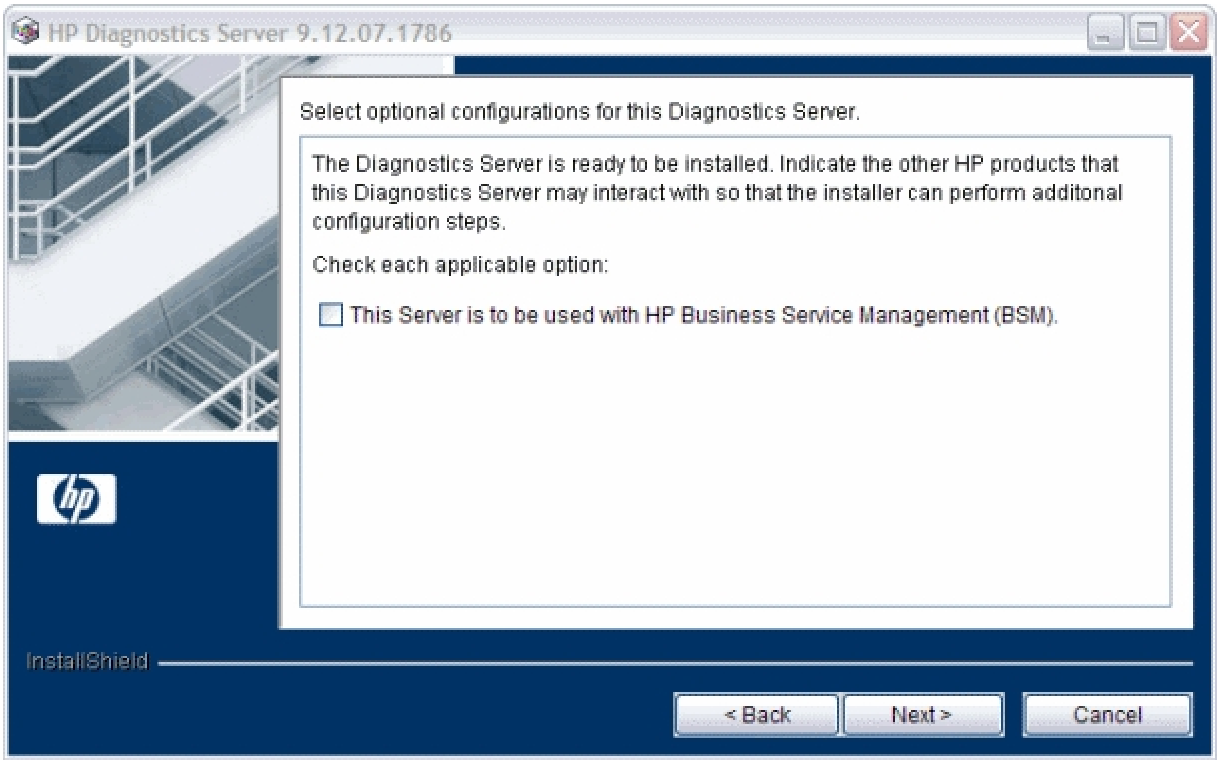
OM Agent Installed Before Diagnostics commander server is Installed

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. Being the Diagnostics commander server installation as described in HP Diagnostics Server Installation and Administration Guide.

At this step, check the BSM integration checkbox:



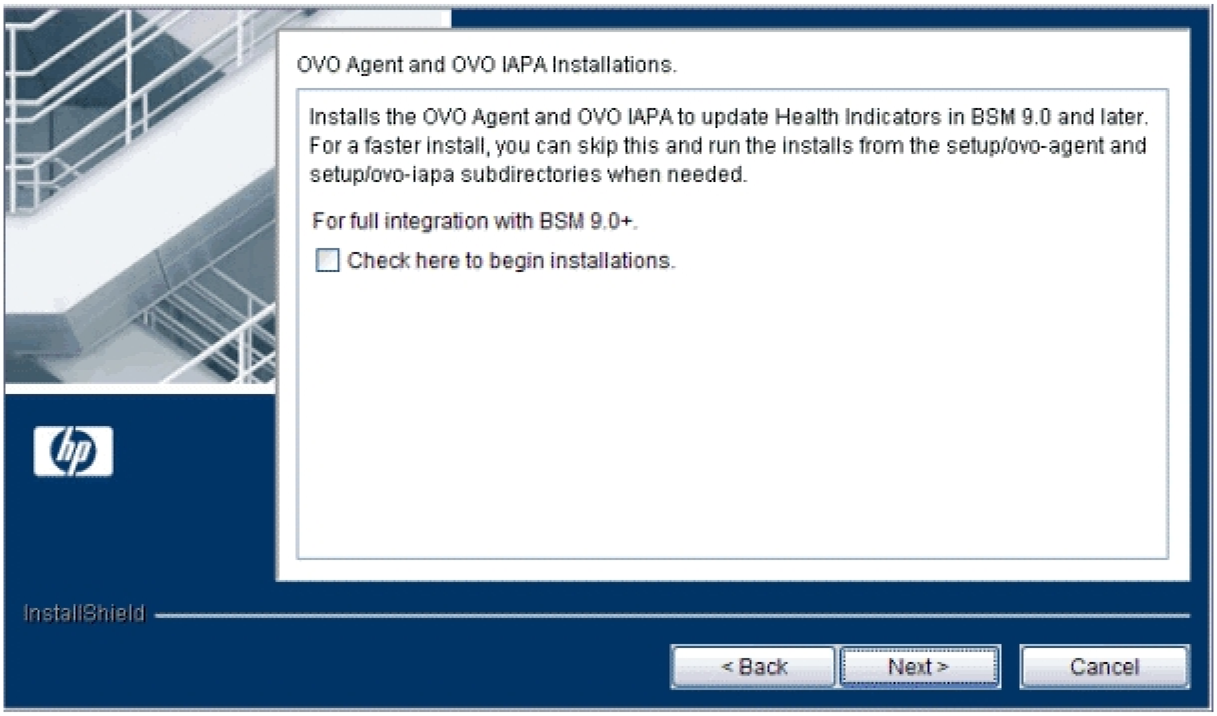
Select optional configurations for this Diagnostics Server.

The Diagnostics Server is ready to be installed. Indicate the other HP products that this Diagnostics Server may interact with so that the installer can perform additonal configuration steps.

Check each applicable option:

□ This Server is to be used with HP Business Service Management (BSM).

When the install comes to this step, leave this checkbox clear (unchecked):



OVO Agent and OVO IAPA Installations.

Installs the OVO Agent and OVO IAPA to update Health Indicators in BSM 9.0 and later. For a faster install, you can skip this and run the installs from the setup/ovo-agent and setup/ovo-iapa subdirectories when needed.

For full integration with BSM 9.0+.

□ Check here to begin installations.

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 HP Diagnostics Server Installation and Administration Guide.).

3. Register Diagnostics in BSM as described in "Task 4: Register the Diagnostics Commander Server in BSM" on page 13.

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 mach
ine.mycompany.com .com
```

5. Determine the core IDs for the BSM Gateway Server and OM Server. On the Diagnostics commander execute:

   ```
   bbcutil -ping <OM Server>

   bbcutil -ping <BSM Gateway 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 HPOM management server.

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

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

   - Locate the string ${OMi_MGR_SRV_ID} and replace all occurrences with the core ID of the BSM gateway 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
   ```

9. The Diagnostics specific logfile encapsulator template that comes with the agent will now report to the BSM server and all of the other policies will report to the OM server.

Configure Trusted Certificates

In an environment with multiple BSM/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 BSM/OM servers.

To configure trusted certificates for every BSM/OM:

1. On every BSM/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 BSM System Requirements and Support Matrixes for information about which versions of BSM are compatible with Diagnostics.

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

If the BSM system is upgraded or re-installed:

- Re-register the Diagnostics Commander Server in BSM. See "Task 4: Register the Diagnostics Commander Server in BSM" on page 13.

- It takes 12 hours before CIs from Diagnostics resume being sent to BSM. You can force the CIs to be sent to BSM sooner by performing a Synchronize operation. See "Synchronize CIs Between Diagnostics and BSM" on page 38.

If the Diagnostics system is upgraded or re-installed:

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

2. Check the Integration as described in "Task 6: Verify the Integration" on page 19. If it is not working, re-register the Diagnostics Commander Server in BSM. See "Task 4: Register the Diagnostics Commander Server in BSM" on page 13.

Chapter 3: Troubleshooting the Integration of BSM 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.

Event Status Integration Status Errors

If the Event Channel Integration Status field on the Registration tab contains an error instead of the value "OK," troubleshoot as follows.

Issue and Import OM Agent Certificate Manually

This procedure is only needed if the automatic certificate request fails. That is, "Certificate request pending" does not appear on the Registration tab. This occurs in BSM deployments where the Load Balancer is configured to operate on network layer 7, the Diagnostics Commander Server is not reachable from the DPS due to firewall settings, or other errors due to network setup.

1. On the Diagnostics commander server host, run the following in a command shell:

   ```
   ovcoreid
   ```

   The output is a GUID representing the CoreID of the Diagnostics server. You specify this value in the next step.

2. On the DPS host, run the following in a command shell:

   ```
   ovcm -issue -file diag_server_certificate.cer -name <FQDN of diag server>
   -coreid <CoreID of Diag server>
   ```

   Specify a password when prompted.

3. Copy the **diag_server_certificate.cer** file to the Diagnostics commander server host.

4. On the Diagnostics commander server host, run the following in a command shell:

   ```
   ovcert -importcert -file diag_server_certificate.cer
   ```

   Provide the password from **Step 2** when prompted.

5. Navigate back to the **Admin > Diagnostics > Registration** tab in the BSM user interface. Click **Save Registration** and verify that the Event Channel Integration Status is now OK.

Other Troubleshooting Tips

- Make sure that the OM Agent and IAPA components are installed on the Diagnostics commander server host. See "Task 1: Prepare the Diagnostics Commander Server" on page 9.

- Check the following log file on the Diagnostics commander server host for errors related to the OM Agent and IAPA components: **<diag_server_install_dir>/server/log.txt**.

- Make sure that the Diagnostics commander server can access the BSM Gateway Server. During registration certificates are requested and granted between these hosts. You can test the access from the Diagnostics commander server as follows:

  ```
  bbcutil -ping <gateway server hostname>
  ```

  This is the expected output:

  ```
  machine.mycompany.com: status=eServiceOK
  coreID=6c852d02-9ae6-7543-1d6e-b6fab24428f0
  bbcV=06.20.101 appN=ovbbccb appV=06.20.101 conn=2
  time=218 ms
  ```

  If you get an eSSLError, this typically indicates that the communication between the Diagnostics Server and BSM OMi is broken.

  If the Diagnostics commander server is also to be monitored by an HPOM server, establish the trust relationship between BSM/OMi and HPOM before you connect the Diagnostics commander server to BSM/OMi. For information on this process, see the BSM - Operations Manager Integration Guide.

If the Diagnostics commander server is to be monitored by an HPOM server that is not synced with BSM/OMi, configure the certificates as described in the "Certificate Handling for OMi in Service Provider Environments" whitepaper .

- If an old certificate is registered on the Diagnostics Server, you must remove it before registering a new one as described in Step 4 above. Remove the certificate as follows:

  ```
  ovcert -remove <CoreID of Diag server>
  ```

  To view the currently registered certificates on the Diagnostics Server, enter:

  ```
  ovcert -list
  ```

- Check the following log file for errors indicating that the agent cannot communicate with the server:

  C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\log\System.txt

  If those errors exist, verify that **com.hp.ov.opc.msgr** is running on the BSM Gateway Server as follows:

  ```
  bbcutil –reg
  BasePath=/com.hp.ov.ctrl.ovcd/
    Protocol=HTTPS
    BindAddress=localhost
    Port=1057
    Authentication=REMOTE
    BasePath=/com.hp.ov.opc.msgr/
    Protocol=https
    BindAddress=ANY
    Port=2506
    Authentication=REMOTE
  ```

- If the registration times out and you see an error like the one below:

```
Timed Out: cscript //NoLogo C:\MercuryDiagnostics\Server\bin\switch_ovo_agen
t.vbs
-server machine.mycompany.com -cert_srv
machine.mycompany.com
64-bit OS
```

```
Server is currently set to '' need to register 'machine.mycompany.com'
Certificate server is currently set to '' need to register
'machine.mycompany.com'
```

Click **Save Registration** again in the BSM Registration page to pick up the changes.

Missing Link in the Standalone Diagnostics UI

If the Diagnostics UI is launched from BSM 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.

Authentication Dialog Displayed in MyBSM

If the Diagnostics Diagnostics commander server is installed in a different domain than the BSM 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's Single Sign-On page.

1. In BSM 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. Log back in to BSM and open the MyBSM Diagnostics Dashboard.

Event Based Health Indicator Status Troubleshooting Flow

If the Event Status Integration is OK, but Health Indicator status events are still not being sent to BSM from Diagnostics, troubleshoot as follows:

- Verify whether Diagnostics writes to **bachi_data.log** on Health Indicator status change on a probe metric:

  a. Entry:

  ```
  C|latency|jbossas|machine.mycompany.com|17b87476ac6de3938ff9898cd19c8bd8
  |mercury|Default Client|1|J2EE|PROBE|2010-05-17 13:40:51|latency [BpmTxJ
  paImpl.getBamNodeStatusKey()  (144.5µs > 122.6µs)]
  ```

  b. Verify whether **opcle** is up via **ovc -status**:

  ```
  opcle              OVO Logfile Encapsulator            AGENT,EA     (552
  8)   Running
  opcmsga            OVO Message Agent                   AGENT,EA     (546
  0)   Running
  ```

  c. Check the agent log file for errors (for example, unable to communicate to BSM server or certificate errors).

  C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\log\System.txt

  d. Enable tracing if necessary:

  ```
  ovconfchg -ns eaagt -set OPC_TRACE TRUE -set OPC_TRC_PROCS opcle -set OP
  C_TRACE_AREA ALL
  ```

  Traces are written to **C:\Documents and Settings/All Users/Application Data/HP/HP BTO Software/tmp/OpC and /var/opt/OV/log/tmp**.

- Test the event channel on the BSM Gateway Server:

  a. Check if OPR (hpbsm_opr-backend) is running by manually submitting an event.

  First get the CMDBID of a CI that Diagnostics populates (look in the BSM Diagnostics Probe and Infrastructure view).

Then go to **opr\support** and run the following (replace the CMDBID in bold with the one from the previous step):

```
sendEvent.bat -s critical -t foo -eh CPU Critical -rch UCMDB:7b75a57ee89
fe6c076ce8d258be4a971
```

b. Verify the flow in **log\opr-backend\opr-backend.log**:

```
2010-05-11 06:17:18,981 [Thread-37] INFO Step.process(45) - Pipeline Step
'PipelineEntry': got 1 events
2010-05-11 06:17:18,981 [Thread-37] INFO Step.process(45) - Pipeline Step
'CIResolver': got 1 events
2010-05-11 06:17:18,981 [Thread-37] ERROR
EventChannelCiResolver.resolveHost(172) - No host CI found for event
com.hp.opr.common.model.Event@4ef05e84[865b7200-5cff-71df-00eb-0f2bf8e70
000,
Back to normal: Threshold violation(s) for latency onmachine.mycompany.c
om,<null>,OPEN,NORMAL,NONE,J2EE,<null>,
<null>,UCMDB:17b87476ac6de3938ff9898cd19c8bd8,<null>,<null>,<null>,com.h
p.opr.
common.model.ResolutionHints@6cd5499[<null>,machine.mycompany.com,15.43.
248.231,ad2c79b2-9af7-7543-002d-ceeb548960bc],com.hp.opr.common.mo
del.ResolutionHints@126d0c4c[Diagnostics:mercury,machine.mycompany.com,1
5.43.248.231,ad2c79b2-9af7-7543-002d-ceeb548960bc],<null>,<null>,false,-
1,
-1,[],{},Tue May 11 06:17:18 PDT 2010,Tue May 11 06:17:18 PDT 2010,Tue M
ay 11
06:17:18 PDT
2010,0,latency:Normal,<null>,<null>,Diagnostics,latency,N:17b87476ac6de3
938ff9898
cd19c8bd8:latency,^<*>:17b87476ac6de3938ff9898cd19c8bd8:latency$,N|laten
cy|jbos
sas|machine.mycompany.com|17b87476ac6de3938ff9898cd19c8bd8|mercury|D
efault Client|1|J2EE|PROBE|2010-05-11
06:16:48|latency,false,com.hp.opr.common.model.MatchInfo@35425b07,<null>
,<null>]
2010-05-11 06:17:18,981 [Thread-37] INFO Step.process(45) - Pipeline Step
'CiVariableReplacer': got 1 events
2010-05-11 06:17:18,981 [Thread-37] INFO Step.process(45) - Pipeline Step
'DowntimeProvider': got 1 events
2010-05-11 06:17:18,981 [Thread-37] INFO Step.process(45) - Pipeline Step
'EtiResolverByHint': got 1 events
2010-05-11 06:17:18,981 [Thread-37] INFO Step.process(45) - Pipeline Step
'EtiResolverByRule': got 1 events
2010-05-11 06:17:18,981 [Thread-37] INFO Step.process(45) - Pipeline Step
```

```
'HIUpdater': got 1 events
2010-05-11 06:17:18,981 [Thread-37] INFO MarbleHealthSubmitter.submit(12
9) -
submitting 1 health updates for customer 1
2010-05-11 06:17:18,981 [Thread-37] INFO Step.process(45) - Pipeline Step
'ResolutionCompleted': got 1 events
2010-05-11 06:17:18,981 [Thread-37] INFO Step.process(45) - Pipeline Step
'IMDBStore': got 1 events
2010-05-11 06:17:18,981 [Thread-37] INFO Step.process(45) - Pipeline Step
'PairwiseCorrelation': got 1 events
```

c. Enable more tracing if needed:

```
HPBSM\conf\core\Tools\log4j\opr-backend\opr.backend.properties
```

Diagnostics Cannot Access RTSM

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

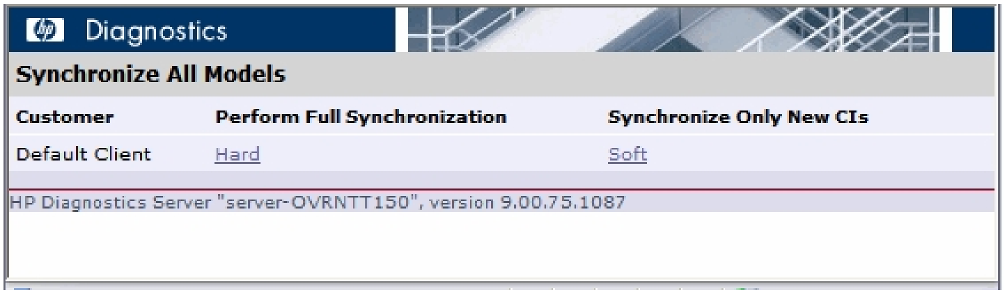
```
WARNING : BAC uCMDB relay failed for customer Default Client. Connection to
BAC failed
java.lang.Exception: InvalidCredentialsException Authentication failed
```

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 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 24.

Synchronize CIs Between Diagnostics and BSM

If you need to force a synchronization between Diagnostics and BSM 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.



Synchronize All Models

Customer	Perform Full Synchronization	Synchronize Only New CIs
Default Client	Hard	Soft

HP Diagnostics Server "server-OVRNTT150", version 9.00.75.1087

Anytime a BSM 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. To do a hard sync, select **Hard**.

IIS Configuration Data Not Showing in BSM

If the CI population from a .NET agent is not occurring in BSM as expected, first rescan the environment as described in "Discovery of IIS Metadata for CI Population of IIS Deployed ASP.NET Applications" on page 26.

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 **Start > HP Diagnostics .NET Probe > Rescan ASP.NET Applications** shortcut 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 HP Support for analysis.