

HP Operations Smart Plug-in for TIBCO

for HP Operations Manager for HP-UX, Linux, and Solaris

Software Version: 1.06

User Guide

Document Release Date: May 2011
Software Release Date: May 2011



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

© Copyright 2004-2005, 2008, 2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

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

UNIX® is a registered trademark of The Open Group

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<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.

Support

Visit the HP Software Support Online web site at:

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 user 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

Contents

1	HP Operations Smart Plug-in for TIBCO	9
	Audience	9
	Prerequisites	10
	Quick Start Instructions	10
	Instructions for All Users	10
	Instructions for First Time Users	10
	Instructions for Repeated Users	11
	Related Documents	11
	HPOM-TIBCO Business Management	11
	Standard Management Functionality	12
	TIBCO SPI Components	12
	TIBCO SPI Backend Service	14
	TIBCO SPI Frontend Service	14
	Resource Explorer	14
	TIBCO SPI Reports	14
	TIBCO Enterprise Management Advisor	15
	Deployment Scenarios	17
	Consolidated Scenario	17
	Scenario 1: Co-located Components Scenario	18
	Scenario 2: Remote Frontend Service	18
	Scenario 3: Fully Distributed (Recommended)	19
	Web Services Distributed Management	20
	XML interfaces	21
2	Installing, Configuring, and Upgrading TIBCO SPI	23
	Installation Packages	23
	Prerequisites	24
	Hardware Requirements	25
	Software Requirements	25
	Installing TIBCO SPI	26
	Installing TIBCO SPI on HP-UX, Linux, or Solaris	26
	Verifying Installation	31
	Configuring Management Server	31
	Assigning User Profiles	31
	Assigning Tools	32
	Assigning Operator Responsibilities	32
	Assigning Categories to the Managed Nodes	33
	Deploying Instrumentation on the Managed Node	33
	Installing Frontend Service	34

Configuring Frontend and Backend Service	35
Assigning TIBCO SPI Policies	37
Configuring Data Sources for Metric Data Collection	37
Assigning Policies to the Managed Node	37
Assigning Backend Service Policies	38
Deploying TIBCO SPI Policies	38
Assigning Frontend Service Policies	38
Deploying policies to Frontend Node	39
Assigning Policy Groups	39
Verifying Deployed Policies	41
Starting TIBCO SPI Tool	41
Starting TIBCO SPI Using the Tool	42
Launching Discovery	42
Checking TIBCO SPI Status	42
Installing Resource Explorer	43
Starting HP Resource Explorer from Console	43
Starting HP Resource Explorer form Command Line	44
Installing Reporter	45
Configuring TIBCO SPI to Run as Non-Root User	45
Upgrading TIBCO SPI	47
Upgrading the Management Server from HPOM 8.xx to HPOM 9.1x	49
Migrating TIBCO SPI 1.50 from HPOM 8.xx to HPOM 9.1x	49
Upgrading TIBCO SPI 1.50 to TIBCO SPI 1.60 on HPOM 9.1x	50
3 Performing Standard Management Functions	53
Service Management	53
Viewing TIBCO Managed Resources	54
Linking Other Service Maps	54
Filtering Unwanted MO types	56
Event Management	57
Viewing TIBCO Events	57
Automatically Responding to Events	58
Monitoring and Data Collection of TIBCO	59
Metric Definition Configuration Files	59
Modifying Data Collection	61
Collecting Data for Custom Adapters	62
Configuring Multi-Instance Metric Data	65
Collecting Data for Specific Metrics	69
Monitoring Custom Adapter Metric Thresholds with HPOM	70
Changing Metric Data Collection Interval	71
Changing Metric Threshold Value	71
Changing which Logfile to Monitor	72
Reporting and Performance Graphs	72
Using Embedded Performance Component (CODA)	73
Embedded Performance Component (CODA) Logging	73
Viewing TIBCO SPI Reports	74
Defining a User Friendly Name for an MO	74

Monitoring Performance Metrics with HP Performance Manager	76
Configuring HP Performance Manager	76
Creating Graph for RVDs	76
TIBCO SPI Self Management	77
Modify Logging and Tracing Levels	77
Changing Log Levels	78
Changing Trace Levels	79
4 Implementing Failover	81
Adding Multiple Location Candidates	82
5 Security Features and Configuration	85
Conceptual Architecture	85
Configuring HTTPS Communication	87
Configuring Frontend Service	87
Creating a Keystore and Importing Certificates	89
Configuring Resource Explorer	91
Customizing HTTPS Configuration Parameters	94
6 Troubleshooting	95
Self-Healing Info Tool	95
Runtime Problems	95
Frontend Service Does Not Stop	95
Frontend Service Does Not Start	96
Frontend Service is Unable to Connect to EMA	96
TIBCO SPI Uses Backup EMA Instead of Primary EMA	99
TIBCO Service is Not Visible	99
Missing Operational Notification	99
Performance Agent Does Not Start Up	107
TIBCO SPI Fails to Detect HP Performance Agent	107
Configure TIBCO SPI Tool Errors	108
Configure TIBCO SPI Tool Does Not Start	108
Configure TIBCO SPI Tool Does Not Display Content	108
Configure TIBCO SPI Tool Fails to Transfer WConfig.xml	108
Configure TIBCO SPI Tool Throws AWTEException	109
Frontend Logfile Errors	109
Error Starting Notification HTTP Server	110
Error Adding Service to Map	110
Frontend does not Connect to the Backend	111
Problem Logging Metric Data	111
7 Removing TIBCO SPI	113
Stopping TIBCO SPI	113
Removing Frontend Service	113
Removing TIBCO SPI Software from Management Server	114
Removing TIBCO SPI using Graphical User Interface	114
Removing TIBCO SPI using Command Line Interface	115
Removing TIBCO SPI Message Groups	116

Removing TIBCO SPI Tools Group	116
Removing TIBCO SPI User Profile	116
Removing TIBCO SPI Policy Groups	117
Removing TIBCO SPI Node Groups From the HPOM Database	117
Removing HP Report Package (Optional)	117
A TIBCO SPI Configuration Parameters	119
Editing WCConfig.xml	119
Editing Configuration Parameters Using Configure TIBCO SPI Tool	119
WCConfig.xml Configuration Parameters	120
<FrontendSection>	120
<BackendSection>	124
B Policies, Tools, and Reports	125
Message Groups	125
Tools	126
Policies	127
TIBCO SPI Self Management	131
Performance Metrics	132
Reports	135
Glossary	141
Index	145

1 HP Operations Smart Plug-in for TIBCO

The *HP Operations Smart Plug-in for TIBCO User Guide* provides detailed information to set up and configure the management systems that enable you to manage a TIBCO environment. The management solution is based on two different product packages: HP Operations Smart Plug-in for TIBCO (TIBCO SPI), and the TIBCO® Enterprise Management Advisor software, a product of TIBCO Software Inc. Together, these two products give IT and application managers the ability to distinguish between significant infrastructure events and events that impact business processes and applications, so that immediate and appropriate action can be taken to maintain uptime and keep mission-critical applications running efficiently. TIBCO solutions empower users to improve their business performance by enabling interoperability between diverse computer systems and help them streamline activities that span their extended enterprise. The Enterprise Management Advisor software enables users to actively manage TIBCO solutions.

HP and TIBCO, together delivers a multipart project that begins with a rich, robust SPI to manage the TIBCO environment and ends with the ability for applications to provide intelligent, adaptive management of the TIBCO environment.

Audience

This User Guide is intended for anyone who is responsible for operating and administering HP Operations Manager (HPOM). In particular, the guide is for HPOM administrators, HPOM operators, System Administrators, IT operators, and TIBCO application managers. It is expected that TIBCO application managers will work as HPOM Operators and use the Java console or Service Navigator to manage the TIBCO environment.

Prerequisites

Users of this Guide should have basic knowledge of the HPOM Management Console, and HPOM management solutions, including SPIs. In addition, users should have basic knowledge of TIBCO application management and the TIBCO software environment. Familiarity with Java, HP-UX, Linux, and Solaris are useful when completing some of the instructions. It is also recommended, but not required, that a user of this guide have general knowledge of management principles.

Quick Start Instructions

This section includes general guidelines that can facilitate installing and using the TIBCO SPI.

Instructions for All Users

All users should perform the following steps:

- complete the steps of [Chapter 2, Installing, Configuring, and Upgrading TIBCO SPI](#), which provides instructions for installing the TIBCO SPI with standard management features
- verify and validate the installation

Instructions for First Time Users

First time users should read this chapter completely to gain an understanding of the following:

- Standard functionalities of the TIBCO management solution
- Conceptual overview and the dependencies required for the various solution components
- Recommended deployment scenarios to help you decide an appropriate deployment configuration for your environment

Instructions for Repeated Users

Repeated users should read the *TIBCO SPI Release Notes* to find out new information about the TIBCO SPI or any known issues.

Related Documents

The TIBCO SPI integrates with several HPOM components. HP Software product guides can be downloaded from

<http://h20230.www2.hp.com/selfsolve/manuals>.

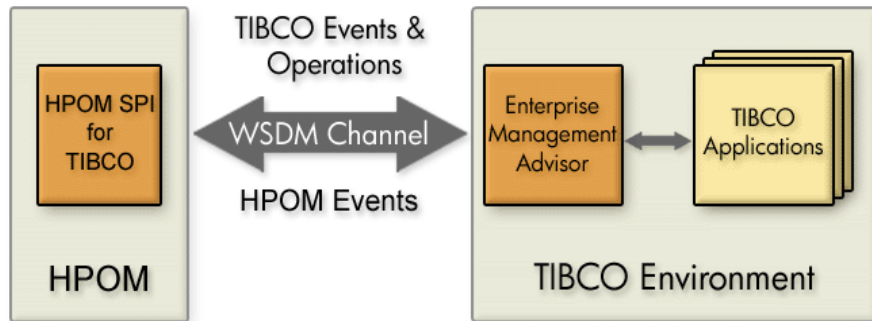
The following TIBCO documents, in HTML and PDF formats, are available on the TIBCO Enterprise Management Advisor installation CD.

- *TIBCO Enterprise Management Advisor User's Guide*
- *TIBCO Enterprise Management Advisor Release Notes*

HPOM-TIBCO Business Management

TIBCO provides a suite of enterprise integration products to bring together disparate and previously incompatible systems. Most of the TIBCO products and applications are management enabled using the TIBCO Hawk™ API. As a part of the HPOM-TIBCO integration, TIBCO has created the Enterprise Management Advisor (EMA), which is responsible for discovering the TIBCO software resources and publishing management data for these resources. More importantly, the status of the resources is kept active and up to date. The TIBCO SPI bridges HPOM and the TIBCO Enterprise Management Advisor software using a Web Services Distributed Management (WSDM) channel. As a result, the TIBCO SPI enables HPOM to manage TIBCO specific applications and products, as well as other elements in the user's environment such as computing and network infrastructure and non-TIBCO applications. [Figure 1](#) shows a high level view of the integrated system:

Figure 1 HPOM-TIBCO Business Management General Architecture



Standard Management Functionality

Standard management functionality that is provided by the TIBCO SPI includes the following:

- Service Discovery Management
- Event and Notifications
- Monitoring and Thresholds
- Performance Reporting and Graphing

These features are available by installing and configuring the TIBCO SPI using the instructions in [Chapter 2, Installing, Configuring, and Upgrading TIBCO SPI](#).

TIBCO SPI Components

The TIBCO SPI comprises five components. The components are distributed and used to manage the TIBCO environment and its applications.

The components are:

- TIBCO SPI Frontend Service

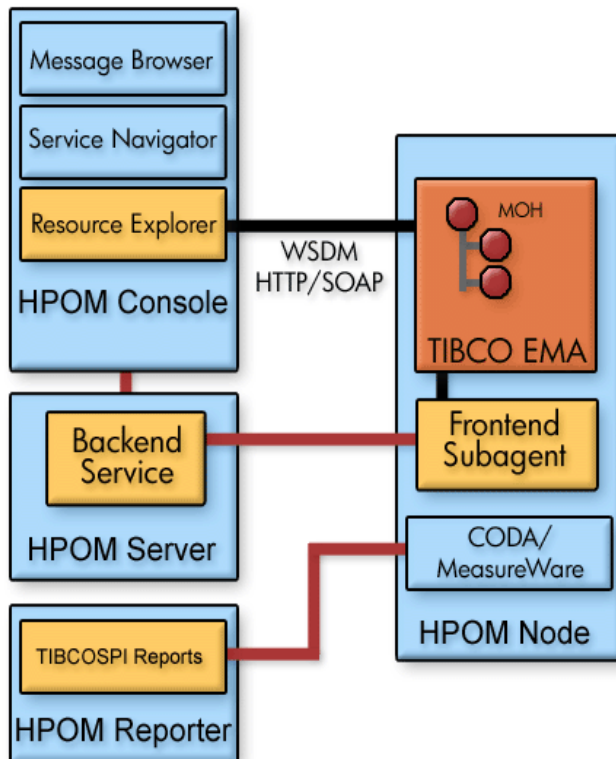
- TIBCO SPI Backend Service
- Resource Explorer
- TIBCO SPI Reports

Figure 2 shows a conceptual overview of the TIBCO SPI components and how they interact. While the TIBCO EMA component is not part of the TIBCO SPI, it is included in the figure for clarification. For more information about EMA component, see [TIBCO Enterprise Management Advisor](#) on page 15.



Figure 2 shows a typical deployment scenario that emphasizes the distributed nature of the TIBCO SPI solution. For additional deployment scenario options, see [Deployment Scenarios](#) on page 17.

Figure 2 Conceptual Overview of the TIBCO SPI Components



TIBCO SPI Backend Service

The Backend Service receives management data and information from the Frontend Service, converts the information to an HPOM recognized form and enables to manage a TIBCO environment using traditional HPOM tools. The Backend Service must be located on an HPOM for UNIX management server.



Both the Frontend and Backend can be located on the same system. In which case, the system must be the HPOM management server. This can be a likely scenario during testing.

TIBCO SPI Frontend Service

The Frontend Service is responsible for communicating with the TIBCO EMA component to gather management data and information. The Frontend Service is essentially a WSDM client communicating with Managed Objects (MOs) exposed as web services by TIBCO EMA.

Resource Explorer

The Resource Explorer is a user interface tool that is used to see and interact with Managed Objects (MOs). This tool is only available for Windows. The Resource Explorer can be either started from the HPOM console (if the Console is installed on Windows) or as a standalone application from the Windows command line.

TIBCO SPI Reports

The TIBCO SPI generates various customized reports that provide performance data of the TIBCO environment. These reports are implemented using the HP Reporter, which can interface with both HP Performance Agent and the Embedded Performance Component (or Coda).

TIBCO Enterprise Management Advisor

TIBCO EMA software is an instrumentation piece that resides in the TIBCO environment. EMA is the gateway through which the TIBCO environment is managed.



The TIBCO EMA software is developed and distributed by TIBCO. The information presented in this section is included to provide an end-to-end view of the management integration. For detailed implementation information about the EMA software, see the *TIBCO Enterprise Management Advisor User's Guide* included with the TIBCO software.

EMA is responsible for the following:

- Discovering TIBCO resources.
- Exposing TIBCO resources as MOs.
- Communicating topology changes to the TIBCO SPI using the WSDM Channel.
- Communicating TIBCO resource alerts to the TIBCO SPI.
- Invoking operations on TIBCO resources that are initiated by HPOM Operators.
- Communicating performance metrics to the TIBCO SPI.

The agent communicates with the HPOM management platform through the WSDM channel. Managed resources are instrumented as MOs using the TIBCO Hawk API. These MOs are dynamically discovered through the Hawk Console API at run time, and they communicate with the managed resources through the Hawk enabled MicroAgents. The TIBCO SPI can communicate with multiple EMAs, and there is generally one EMA per Hawk domain. [Figure 3](#) shows a high-level architecture for the TIBCO EMA software.

Figure 3 TIBCO Enterprise Management Advisor Architecture

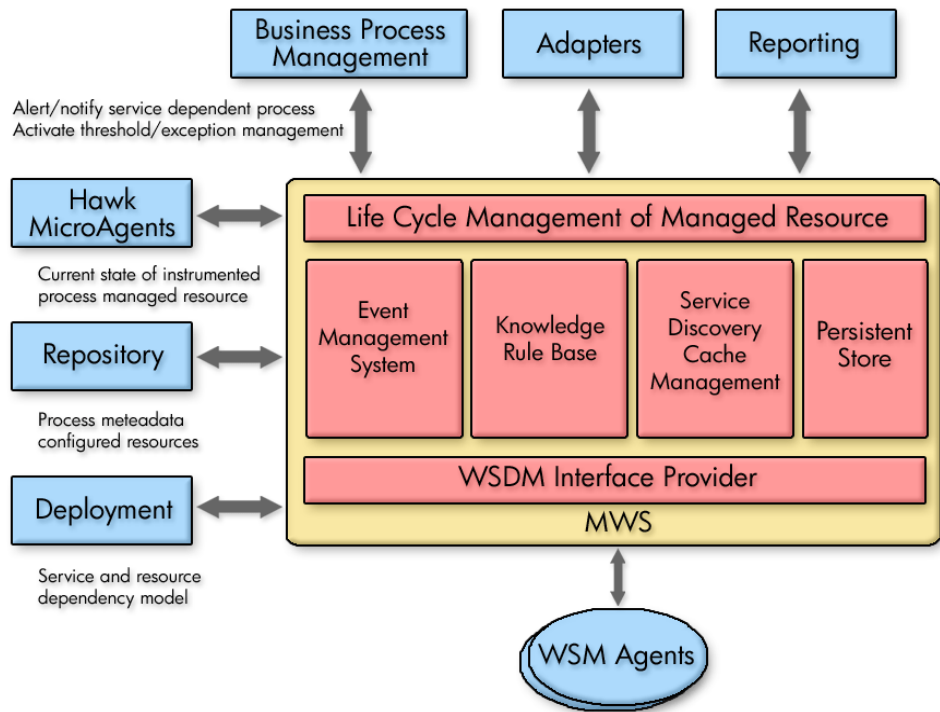


Figure 3 shows a container managing the life cycle of a resource. The state of the managed resource is instrumented through the Hawk API in the TIBCO environment, and the managed resource itself is exposed to HPOM. Each of the TIBCO components has to enlist the set of management aware resources used by it in order to provide the service as defined by the component's contract. This information can very well be an acyclic graph, which the NSM layer can later modify and create a representative policy. The repository and the deployment of EMA provide this information. For more information about TIBCO EMA architecture, see the *TIBCO Enterprise Management Advisor User's Guide*.

Deployment Scenarios

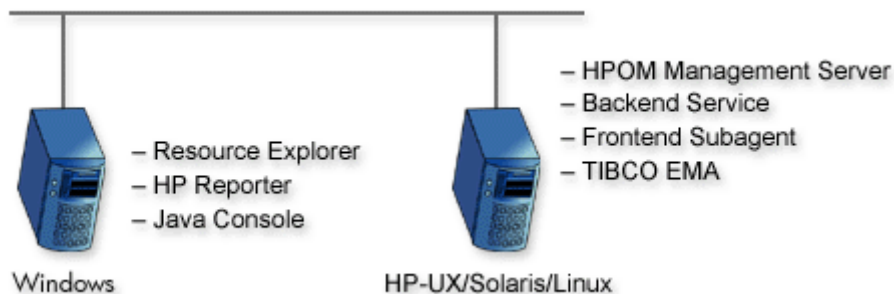
As discussed in the section [TIBCO SPI Components](#), TIBCO SPI is a distributed solution. Its components can be distributed in several different deployment configurations. This section provides some common deployment scenarios and does not represent every possible configuration.

- ▶ A fully distributed scenario is the recommended deployment scenario. See the section [Scenario 3: Fully Distributed \(Recommended\)](#) on page 19.

Consolidated Scenario

It is possible to have a single system that hosts all of the TIBCO SPI components (in addition to the TIBCO EMA component) except for the Resource Explorer and HP Reporter, which is only available for Windows. In this scenario, the Resource Explorer must be started from the Windows command line and cannot be started from the Java console. This scenario uses minimal hardware, but results in increased loads on a single system. Therefore, it is not recommended for production environments. You may need to reconfigure the default ports used by the components if port conflicts occur.

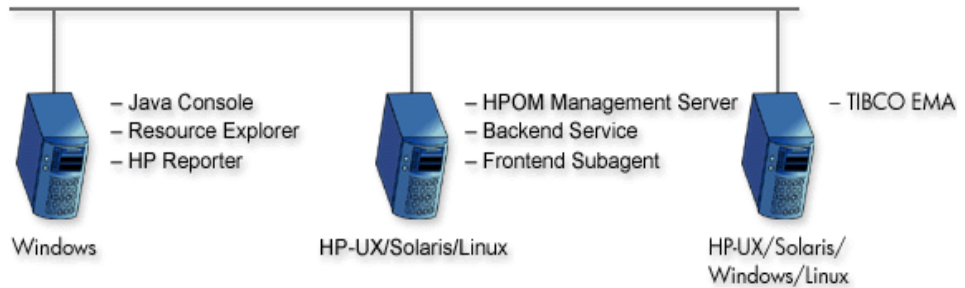
Figure 4 Consolidated Scenario



Scenario 1: Co-located Components Scenario

In this scenario, both the Frontend Service and Backend Service are located on the HPOM management server system. Management processing is concentrated on a single system. This scenario is good for testing and also for less demanding production environments.

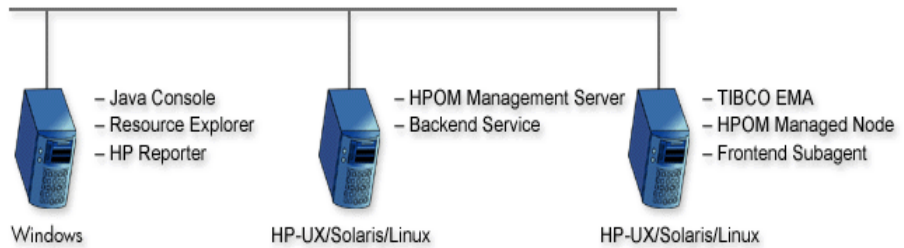
Figure 5 Co-located Component Scenario



Scenario 2: Remote Frontend Service

In this scenario, the Frontend Service is separated from the HPOM management server and is located with the TIBCO EMA component. This scenario effectively separates management processing between a managed node and the management server. This scenario is ideal for a production environment.

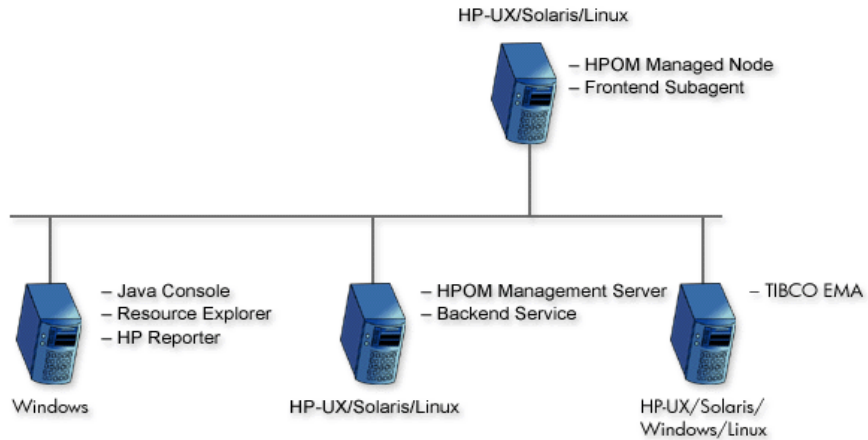
Figure 6 Remote Frontend Service Scenario



Scenario 3: Fully Distributed (Recommended)

In this scenario, the TIBCO SPI components, as well as the TIBCO EMA component, are located on different systems. Each system is relegated to a single task. This scenario provides the most efficient processing and resource utilization. However, this scenario introduces the most overhead. Maximum hardware is used and maintaining the solution can become cumbersome. This scenario is ideal for a production environment.

Figure 7 Fully distributed Scenario



Web Services Distributed Management

Web Service Discovery Management (WSDM) is a management specification for managing application resources using web services technology as well as managing web services using web services. The specification enables a common integration channel between an Independent Software Vendor (ISV) and a management station such as HPOM. The WSDM standard is defined by the WSDM Technical Community (TC) at OASIS. More information about the standard can be found at the WSDM TC site at OASIS.



The WSDM implementation in the TIBCO SPI is based on an HP-authored preliminary version of WSDM known as the Web Service Management Framework (WSMF).

WSDM provides a way to represent and realize management models and is based on Managed Objects (MOs) and the relationship between them. MOs provide management capabilities by implementing management interfaces. The management interfaces are described using WSDL. Hence, WSDM provides the architecture for defining management interfaces for MOs.

The foundational interfaces defined by WSDM can be extended in order to better manage resources in specific domains. In TIBCO SPI, there are two types of extensions:

- HPOM domain extensions that provide HPOM data and events to TIBCO applications
- TIBCO domain extensions that enable HPOM to access TIBCO specific manageability.

XML interfaces

WSDM defines a set of domain agnostic management interfaces, as well as domain specific management interfaces for web services. Vendors are free to extend WSDM to their specific domain in order to manage resources effectively.

- **Discovery** – a set of interfaces for discovering MOs and their relationships in the managed environments. There is a set of default relationship types defined in WSDM, and vendors can extend these relationship types as well.
- **Configuration** – a set of interfaces that enables a manager to find out the configuration information about a managed object.
- **Control** – a set of interfaces to control MOs or resources.
- **Performance** – a set of interfaces that enables a manager to find out performance information about MOs.
- **EventPush and Event Pull** – a set of interfaces for subscribing to events in either push or pull model.
- **EventCallback** – a set of interfaces for responding to events after subscription.

2 Installing, Configuring, and Upgrading TIBCO SPI

This chapter provides installation instructions for the various components of the TIBCO SPI. For more information about HPOM, see *HP Operations Manager for UNIX Concepts Guide*.

The following list highlights the installation and configuration process:

- 1 Select a deployment scenario from the section [Deployment Scenarios](#) on page 17
- 2 Fulfill the [Prerequisites](#)
- 3 [Installing TIBCO SPI](#)
- 4 [Configuring Management Server](#)
- 5 [Configuring Frontend and Backend Service](#)
- 6 [Assigning TIBCO SPI Policies](#)
- 7 [Starting TIBCO SPI Tool](#)
- 8 [Launching Discovery](#)
- 9 [Installing Resource Explorer](#)
- 10 [Installing Reporter](#)
- 11 [Upgrading TIBCO SPI](#)

Installation Packages

The TIBCO SPI installation package includes the following:

- SPI Package
- Reporter Package

The following section lists the installation packages for the TIBCO SPI on HPOM for:

- HP-UX
- Linux
- Solaris

SPI Package

The SPI package contains all the SPI functionality. The package must be installed on a server managed by HPOM.

Location of the main package is as follows:

For HP-UX,

```
<SPI DVD>\HP_Operations_Smart_Plug-ins_Hpux_setup.bin
```

For Linux,

```
<SPI DVD>\HP_Operations_Smart_Plug-ins_Linux_setup.bin
```

For Solaris,

```
<SPI DVD>\HP_Operations_Smart_Plug-ins_Solaris_setup.bin
```

Reporter Package

The package contains the default reporter policies provided by the SPI. The name and location of the reporting package is:

```
\WINDOWS\HP_REPORTER\TIBSPI\TIBSPI-Reporter.msi
```

Prerequisites

The following section details the requirements for installing and running the TIBCO SPI. Make sure that the requirements are met before you begin the installation.



TIBCO SPI 1.06 can only be used with TIBCO EMA 2.0 and 2.1. Before installing the TIBCO SPI, make sure the TIBCO EMA software is installed in the TIBCO environment and is operational. For additional TIBCO EMA requirements, see TIBCO EMA documentation. To verify whether EMA is running, perform the following:

For HP-UX, run the command `ps -ef | grep -l ema`.

For Windows, check the processes under the Windows Task Manager to verify that EMA is running.

Hardware Requirements

See the *HP Operations Manager for UNIX* documents for information about hardware requirements for the management server. See the following Support Matrix (SUMA) link, for information about hardware requirements for the managed nodes:

<http://support.openview.hp.com/selfsolve/document/KM323488>

Software Requirements

Ensure that the following software requirements are completed prior to the installation of TIBCO SPI.

On the Management Server:

- HP Operations Manager for UNIX: 9.1x
- HP Performance Manager: 9.00 (required, if you want to generate graphs)
- HP Reporter: 3.90 (required, if you want to generate web-based reports)
- HP Operations SPI Data Collector (DSI2DDF): 2.41
- HP SPI Self-Healing Services (SPI-SHS-OVO): 3.01

On the Managed Nodes (for HP-UX, Solaris, Linux, or Windows):

- HP Performance Agent: 5.00 (required, if you want to use HP Performance Agent for data logging)
- HP Operations Agent: 8.6x and 11.x

See the following Support Matrix (SUMA) link, for more information about supported versions of HP Operations Manager, HP Performance Agent, HP Operations agent, HP Performance Manager, and HP Reporter: <http://support.openview.hp.com/selfsolve/document/KM323488>

Installing TIBCO SPI

Install HPOM for UNIX before installing the TIBCO SPI. To install HPOM for UNIX, see *HPOM Online Help*. In addition, you must be logged on to the management server and managed nodes as root when completing the instructions in this section.

- ▶ Make sure that JRE 1.6 is installed on both the management server and the managed node. On the management server, set an environment variable `JAVA_HOME` to the JRE installation directory. Remove any older versions of the TIBCO SPI before completing the installation.

Installing TIBCO SPI on HP-UX, Linux, or Solaris

TIBCO SPI is installed on an HPOM management server. The TIBCO SPI Backend service is installed by default. However, the TIBCO SPI Frontend service and Resource Explorer must be installed after the TIBCO SPI is installed. In addition, you can also install the Frontend service on a managed node, from the management server, after installing the SPI.

- ▶ Both the Frontend and Backend services can be located on the same system. In this case, the system must be an HPOM management server.

Task 1: Mounting the DVD

To mount the DVD on HP-UX, Linux, or Solaris, follow these steps:

- 1 Log on as **root** user.
- 2 Set the user's root unmask by typing:
`umask 027`
- 3 Create a directory to mount the DVD:
`mkdir /<mount_point>`

For example: `mkdir -p/dvdrom`

- 4 Insert the DVD into the disk drive and mount it as user root by entering:
`mount /dev/<dvdrom_drive_name> /<mount_point>`

For example, for a local DVD, you can type:

```
mount /dev/dsk/c0t2d0 /dvdrom
```

You can also run SAM and mount the DVD to a specific path in the Disks and File *Systems* window.

Task 2: Installing TIBCO SPI

To install TIBCO SPI on HP-UX, Linux, or Solaris management server, you can use any of the following:

- Graphical User Interface
- Command Line Interface

Installing TIBCO SPI through Graphical User Interface

To install the TIBCO SPI using X-Windows client software, follow these steps:

- 1 Log on as **root** user.
- 2 Insert the HP Operations Smart Plug-ins DVD into the HP-UX, Solaris or Linux management server DVD drive.
- 3 Start the X-windows client software and export the DISPLAY variable by typing the following command:

```
export DISPLAY=<ip address>:0.0
```

- 4 To start the installation, type the following command:

For HP-UX:

```
./HP_Operations_Smart_Plug-ins_Hpux_setup.bin
```

For Solaris:

```
./HP_Operations_Smart_Plug-ins_Solaris_setup.bin
```

For Linux:

```
./HP_Operations_Smart_Plug-ins_Linux_setup.bin
```

The **Initialization** page appears.

▶ If another SPI is already installed on the management server, skip step 5 and 6. Go to [step 7](#).

5 On the **Introduction** page, check the information available for installation, and then click **Next**.

6 On the **License Agreement** page, select **I accept the terms of the License Agreement** and click **Next**.

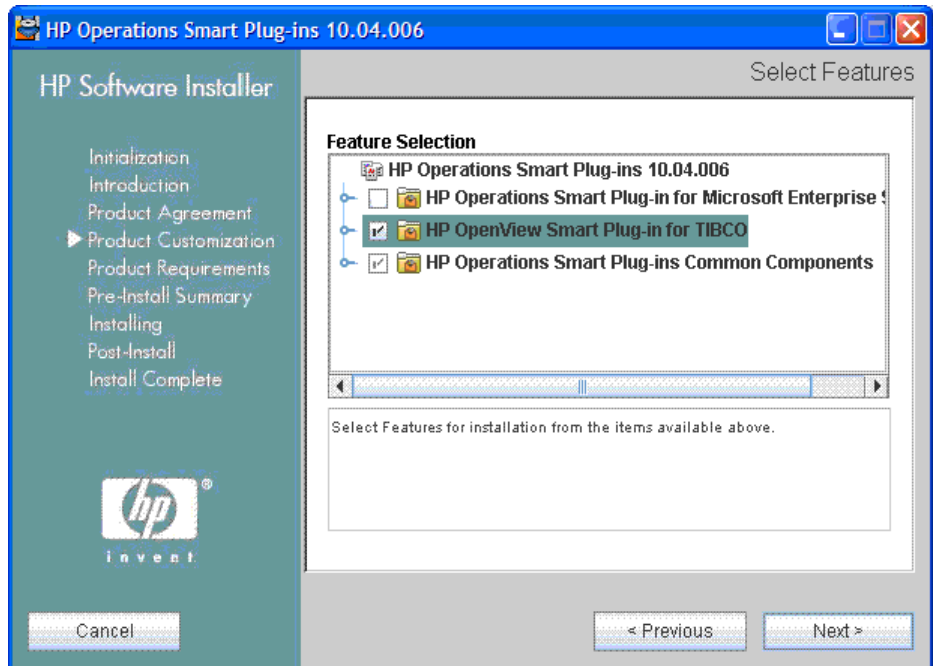
▶ If you are installing the SPI on the management which does not have any other SPI installed, skip steps 7 and 8. Go to [step 9](#).

7 On **Application Maintenance** page, select from the following options:

- To start the installation on the management server with previously installed SPIs, select **Modify**.
- If some errors appear while installing, select **Reinstall from Media**.

8 On the **Introduction (Modify)** page, check the installation package and instructions, and then click **Next**.


9 On the **Select Features** page, select **HP Operations Smart Plug-In for TIBCO**. By default, the HP Operations Smart Plug-ins component is selected.



While installing the SPIs on HPOM, select the previously installed SPIs on the management server, if any. If you do not select the previously installed SPIs, the installer automatically removes the previously installed SPIs and installs the selected ones.

- 10 After you select the TIBCO SPI and the previously installed SPIs on the management server, if any, click **Next**. The HP Operations Smart Plug-in Common Components is a mandatory component, which is selected by default.
- 11 On the **Install Checks** page, the installer checks the system for the available disk space. If the install check is successful, click **Next**.
- 12 On the **Pre-Install Summary** page, check the products that appear to be installed or already available on the management server, select the following:
 - To start the installation of the SPI, click **Install**.

- To start the installation on the management server with previously installed SPIs, click **Modify**.

 Select **Force reinstallation** to reinstall the selected components.

13 Click **Done** to complete the installation.

Installing TIBCO SPI through Command Line Interface

To install the TIBCO SPI through the command line interface, follow these steps:

- 1 Log on as a **root** user.
- 2 Insert the HP Operations Smart Plug-ins DVD into the Solaris or Linux management server DVD drive.
- 3 To start the installation, type the following command:

For HP-UX:

```
./HP_Operations_Smart_Plug-ins_Hpux_setup.bin -i console
```


For Solaris:

```
./HP_Operations_Smart_Plug-ins_Solaris_setup.bin -i  
console
```

For Linux:


```
./HP_Operations_Smart_Plug-ins_Linux_setup.bin -i console
```


The HP Software Installer content appears. Press **Enter** to continue.

 If another SPI is already installed on the management server, skip step 4 and 5. Go to [step 6](#).

- 4 In the **Introduction** content, check the information available for installation, and press **Enter** to continue.
- 5 In the **License Agreement** content, when the License agreement prompt, '**I accept the terms of the License Agreement**' appears, type **Y** and press **Enter** to accept the terms and continue with the installation.

The Feature selection options list appears.

 If another SPI is already installed on the management server, skip step 6. Go to [step 7](#).

- 6 In the **Application Maintenance** content, type the number corresponding to the feature **Modify**. Press **Enter** to continue.
- 7 In the **Select Features** content, do the following:
 - Type the number corresponding to the feature you want to install.
 - Type the number corresponding to the feature you want to retain.
-  While installing the SPIs on HPOM, select the previously installed SPIs on the management server, if any. If you do not select the previously installed SPIs, the installer automatically removes the previously installed SPIs and installs the selected ones.
- 8 After you select the SPIs that you want to install, uninstall, or retain, press **Enter** to continue.
- 9 The installer selects the other required features. Press **Enter** to continue.
- 10 In the **Install Requirements Checks** content, the installer verifies the system. If the install check is successful, press **Enter** to continue.
- 11 In the **Pre-Installation Summary** content, press **Enter** to continue.

The selected features are installed.

When the installation is complete, a message appears stating that the installation is completed successfully.

Verifying Installation

To verify TIBCO SPI Installation on the management server, use the following commands:

- For HP-UX: `swlist`
- For Linux: `rpm -qa`
- For Solaris: `pkginfo -l HPOvSpiTib`

For Linux, HP-UX, and Solaris, verify the `TIBSPI_Install.log` file to check if the installation is successful. The path of this file is `/var/opt/OV/log/SPIInstallLogs`.

Configuring Management Server

To configure the TIBCO SPI, you must complete all configuration prerequisites, TIBCO SPI configuration for managed nodes and the management server, and additional configuration based on your environment.

Log on to HPOM as an administrator. The Administration user interface window appears. Complete the following tasks before configuring the TIBCO SPI.

Assigning User Profiles

To assign User Profiles, follow these steps:

- 1 Select **All Users** → **<Operator Name>**. For example, `opc_admin`.
- 2 To assign a User profile, select **Assign Profiles....** from Action Menu. The Selector window opens.
- 3 Select **Profiles** from **Locate** list and set the **Name** to `tib`. Click **Filter**.
- 4 Select **TIBCO User Profile** from Filtered User Profiles list. Click **OK**. The User Profile is successfully assigned.

Assigning Tools

To assign TIBCO SPI Tools, follow these steps:

- 1 Select **All Users** → **<Operator Name>**. For example, `opc_admin`.
- 2 To assign tools, select **Assign Tools...** from Action Menu. The Selector window appears.
- 3 Set the Name to `tib`. Click **Filter**.
- 4 Select all TIBCO SPI tools from the filtered Tools list. Click **OK**. TIBCO SPI tools are successfully assigned.

Assigning Operator Responsibilities

To assign Operator responsibilities, follow these steps:

- 1 Select **All Users** → **<Operator Name>**. For example, `opc_adm`.
- 2 To change a User's responsibility, select **Edit Responsibilities....** from Action Menu. The Selector window opens.
- 3 Click **Edit View**. Edit Matrix View window opens.
- 4 Move **TIBSPI-UNIX**, **TIBSPI-WINDOWS** and **TIBSPI-External** Node groups from available Node groups column to Visible Node groups column. Move **TIBCO** and **TIBCO-SPI** message groups from available Message groups column to Visible Message groups column. Click **OK**.
- 5 Select all check boxes for **TIBCO** and **TIBCO Message Groups**.
- 6 Assign the TIBCO Node or Message Groups to any other appropriate operators.
- 7 Click **Close**.


Adding Nodes to TIBSPI-UNIX Node Group

If you are installing the Frontend service on a Managed node, the node must be configured as part of the TIBSPI-UNIX Node Group.




If you are installing Frontend service on the management server, you can skip this section.

To add a managed node to TIBSPI-UNIX Node Group, follow these steps:

- 1 Open the Node Bank window and select the nodes running Frontend service to add to the TIBCO SPI Node group.
- 2 Select **Assign Nodes...** from the **Choose an Action** list and click  to submit. The Selector window appears.
- 3 Select **Node** from the **Locate** list and type **tib** as **Name**. Click **Filter**.
- 4 Select **TIBSPI-UNIX** node group from the filtered node groups. Click **OK**. Nodes are assigned to the node group.


Assigning Categories to the Managed Nodes

To assign categories to the managed node, follow these steps:

- 1 Open the Node Bank window and select the managed nodes.
- 2 Select **Assign Categories...** from the **Choose an Action** list and click  to submit. The Selector window appears.
- 3 Select **SHS_Data_Collector**, **SPIDataCollector**, and **TIB_Instrumentation** categories.
- 4 Click **OK**. Categories are assigned to the managed nodes.

Deploying Instrumentation on the Managed Node

To deploy instrumentation on the managed node, follow these steps:

- 1 Open the Node Bank window and select the managed nodes.
- 2 Select **Deploy Configuration...** from the **Choose an Action** list and click  to submit.
- 3 Select **Distribute Instrumentation**.
- 4 Click **OK**. Instrumentation is deployed on the selected nodes.

Installing Frontend Service

The Frontend service can be installed on a management server or a managed node based on the following scenarios:

Scenario 1: Frontend and Backend Services on the management server.

To install the Frontend service on the management server, follow these steps:

- 1 On the Administration interface, select **Integrations**→**HPOM for UNIX UI**.
- 2 Login with administrative credentials. For example, `opc_admin`.
- 3 Click **Nodes**. Right-click the management server. Select **Start**→**Front End Installation**. The Frontend Installation Output window appears.
- 4 The following message appears on successful installation:

HTTPS

Scenario 2: Frontend service on the managed node, and Backend service on the management server.

To install the Frontend service on the managed node, follow these steps:

- 1 Assign categories and deploy instrumentation on the managed node.
- 2 Run frontend installation tool on the managed node and the management server.
- 3 Run Configure TIBCO SPI tool on the management server. The tool configures the `WCConfig.xml` file and pushes the configuration files - `appconfig.xml` and `WCConfig.xml` to the configured managed node.
- 4 Run the Start TIBCO SPI tool on the management server. The tool starts the backend on the management server and frontend on the managed node.
- 5 Run the TIBSO SPI Status tool to check the status of both backend and frontend services. The following message appears:

```
TIBSPI Backend is running...
```

```
TIBSPI Frontend is running...
```

Configuring Frontend and Backend Service

To configure the Frontend and Backend service, you must define various configuration options. You can define these options using the TIBCO SPI Configuration Editor that is present in the **TIBCO SPI Tools** group.

- 1 On the Administration interface, click **Integrations** → **HPOM for UNIX UI**.
- 2 Login with administrative credentials. For example, `opc_adm`.
- 3 Click **Nodes**. Right-click the selected node. Select **Start** → **Configure TIBCO SPI**. The TIBCO SPI Configuration Editor window appears.

For a Windows machine, start the X-windows client software to display the Configuration Editor.

- 4 On the TIBCO SPI Configuration Editor tree, select **OVO Management Server Info** under Back End Configuration.

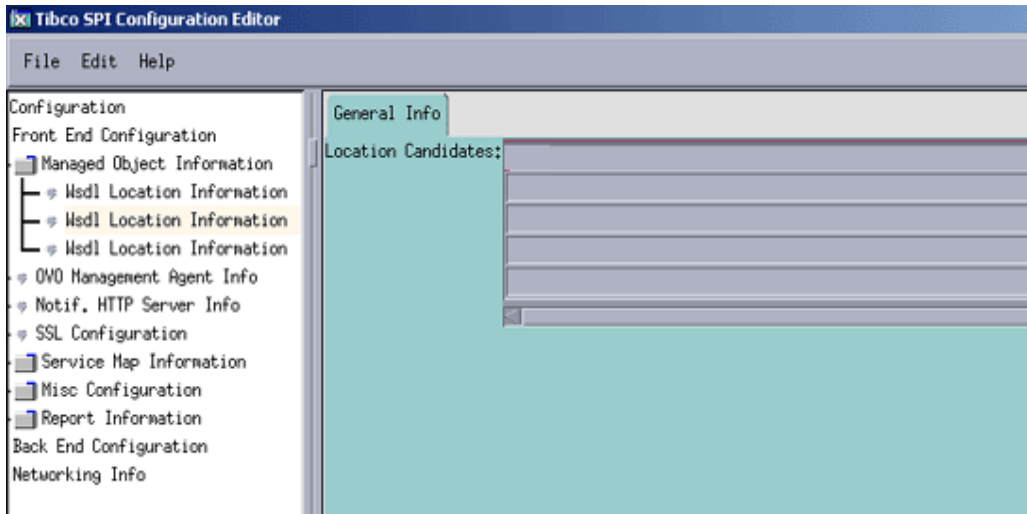
- 5 Modify the Host Name and any other fields if required. Make sure the default RMI port is not already in use.
- 6 Expand Front End Configuration. Select **Managed Object Information** → **WsdL Location Information**.
- 7 In the Location Candidates list, add a WSDL location for a managed object you want the Frontend to monitor. Managed objects are exposed by the TIBCO EMA software. See the TIBCO EMA documentation for instructions on finding a managed object's published WSDL location.



If the WSDL location uses HTTPS, then you must configure the Frontend security settings. For details, see Configuring HTTPS Communication section in [Chapter 5, Security Features and Configuration](#).

- 8 To configure an additional WSDL location, create a new Location Candidate by selecting **Managed Object Information** and from the menu click **Edit** → **New**.

Figure 8 TIBCO SPI Configuration Editor



- 9 In the new Location Candidates list, add a WSDL location for the managed object you want the Frontend to monitor.
- 10 Repeat steps 8 and 9 to add additional WSDL locations.



The WSDL locations that are configured in the Managed Object Information field must be accessible before starting the Frontend.

- 11 Select **OVO Management Agent Info**.
- 12 Modify the Host Name and other fields if required. Make sure the default RMI port is not already in use.
- 13 Select **File** → **Save** to save your changes to the configuration file.
- 14 Select **File** → **Exit**.
- 15 In the Output window, the following message appears:

```
TIBCO SPI configuration completed.
```

It can take a few minutes for the message to appear. Do not close the output of application window before you see the completion message.
- 16 Click **Close**.

Assigning TIBCO SPI Policies

HPOM-based policies are used to capture management data and metrics. The policies are specific to TIBCO SPI and are included with the TIBCO SPI installation. In general, the policies collect and monitor data. The data includes metric data, operational notifications, logging data, and UDM metrics. The data is used to effectively manage the TIBCO environment within HPOM. Before assigning TIBCO SPI policies, you must configure the data sources that are used to store the collected data metrics.

Configuring Data Sources for Metric Data Collection

The metrics collected by the Frontend policies are stored in a data source. A script which creates and configures the data source is provided.


To configure data source for metric data collection, follow these steps:

- 1 From a command prompt, change directories to `/opt/OV/bin`.
- 2 Run the command:

```
./tib-perl tib-create-datasources
```
- 3 The following message appears:
Start Data Logging Integration

Assigning Policies to the Managed Node


To assign policies to the managed node, follow these steps:

- 1 Open the Node Bank window and select the managed nodes.
- 2 Select **Assign Policies / Policy Groups...** from the **Choose an Action** list and click  to submit.
The Selector window appears.
- 3 Click **Policy Bank**.
- 4 Select the policies you want to assign to the managed node from the **SPI for TIBCO** policy group.
- 5 Click **OK**. The policies are successfully assigned to the Managed nodes.

Assigning Backend Service Policies


The TIBSPI-UNIX-Backend-V1 group contains the policies that monitor the TIBCO SPI log files on the HPOM management server. This group is assigned and deployed on the management server.

To assign the TIBSPI-UNIX-Backend-V1 group to the management server, follow these steps:

- 1 In the Node Bank window, select the management server where the Backend service is running.
- 2 Select **Assign Policies / Policy Groups...** from the **Choose an Action** list and click  to submit. The Selector window opens.
- 3 Select **Policy Groups** from the **Locate** list and set the **Name** to **TIBSPI-UNIX**. Click **Filter**.
- 4 Select **SPI for TIBCO/TIBSPI-UNIX-Backend-V1** from the filtered policy groups. Click **OK**. The backend service policies are successfully assigned.

Deploying TIBCO SPI Policies

To deploy TIBCO SPI policies, follow these steps:


- 1 Open the All Node Groups window and select a TIBCO SPI node group.
- 2 Select **Deploy Configuration...** from the **Choose an Action** list and click  to submit.
- 3 Select **Distribute Policies** by selecting the corresponding check box.
- 4 Click **OK**. The TIBCO SPI policies are now distributed to the selected node group. The TIBCO SPI metrics will run according to their specific collection interval

Assigning Frontend Service Policies

The Frontend policy groups must be assigned and deployed to the node where the Frontend is installed before the policies can be used.


To assign Frontend policy groups to a node, follow these steps:

- 1 Click **All Nodes**. Select the node where the Frontend is running.

- 2 Select **Assign Policies / Policy Groups...** from the **Choose an Action** list and click  to submit. The Selector window opens.
- 3 Select **Policy Groups** from the Locate list and set the Name to **SPI for TIBCO/TIBSPI - EventService-VI**. Click **Filter**.
- 4 Select **SPI for TIBCO/TIBSPI - EventService-VI** from the filtered policy groups. Click **OK**. The Frontend policy groups are assigned to the node.

Deploying policies to Frontend Node

To deploy the policies to the Frontend Node, follow these steps:

- 1 In the Node Bank window, select the node where the Frontend is running.
- 2 Select **Deploy Configuration...** from the **Choose an Action** list and click  to submit. The Selector window opens.
- 3 Select **Distribute Policies** and **Force Update**.
- 4 Click **OK**. The frontend policies are successfully deployed.

Assigning Policy Groups

The `TIBSPI-UNIX-V1` group contains the policies that monitor various TIBCO products that are running on UNIX nodes, for instructions to assign policies, see the section, [Assigning TIBSPI-UNIX- V1 Policy Group](#)

The `TIBSPI-Windows-V1` group contains the policies that monitor various TIBCO products that are running on Windows nodes, for instructions to assign policies, see the section, [Assigning TIBSPI-Windows-V1 Group](#)


Assigning TIBSPI-UNIX- V1 Policy Group

The `TIBSPI-UNIX-V1` policy group contains the policies that monitor various TIBCO products that are running on UNIX nodes.




The HP Operations Agent must be deployed on the UNIX nodes where the TIBCO products are running before you can deploy the `TIBSPI-UNIX-V1` group.

To assign policy group to TIBSPI-UNIX-V1 node group, follow these steps:

- 1 Open the Node Group Bank window, select **TIBSPI-UNIX** node group.
- 2 Select **Assign Policies / Policy Groups...** from the **Choose an Action** list and click  to submit. The Selector window opens.
- 3 Select **Policy Groups** from the Locate list and set the Name to **TIBSPI-WINDOWS**. Click **Filter**.
- 4 Select **TIBSPI-Windows-V1** group from the filtered policy groups. Click **OK**. The policy groups are successfully assigned.

Deploying TIBSPI-UNIX-V1 Group to UNIX Nodes

To deploy TIBSPI-UNIX- V1 policy group to the UNIX node group, follow these steps:

- 1 In the Node Group Bank window, select the **TIBSPI-UNIX** node group.
- 2 Select **Deploy Configuration...** from the **Choose an Action** list and click  to submit. The Selector window opens.
- 3 Select **Distribute Policies** and **Force Update**.
- 4 Click **OK**.

Assigning TIBSPI-Windows-V1 Group


The TIBSPI-Windows-V1 group contains the policies that monitor various TIBCO product's log files that are running on Windows nodes.



The HP Operations agent must be deployed on the Windows nodes where the TIBCO products are running before you can deploy the TIBSPI-Windows-V1 group.

For this procedure, assume that TIBCO is running on all of the nodes in the TIBSPI-WINDOWS node group. Therefore, assign the TIBSPI-Windows-V1 group to the TIBSPI-WINDOWS node group.


To assign policy group to TIBSPI-WINDOWS node group, follow these steps:

- 1 Open the Node Group Bank window, select **TIBSPI-WINDOWS** node group.
- 2 Select **Assign Policies / Policy Groups...** from **Choose an Action** list and click  to submit. The Selector window opens.

- 3 Select **Policy Groups** from the **Locate** list and assign the **Name** as **TIBSPI-WINDOWS**. Click **Filter**.
- 4 Select **TIBSPI-Windows-V1** group from the filtered policy groups. Click **OK**. The policy groups are successfully assigned.

Deploying TIBSPI-Windows-V1 Policy Group to Windows Nodes

To deploy the policies to the Windows node group, follow these steps:

- 1 In the Node Group Bank window, select the **TIBSPI-WINDOWS** node group.
- 2 Select **Deploy Configuration...** from **Choose an Action** list and click  to submit. The Selector window opens.
- 3 Select **Distribute Policies** and **Force Update**. Click **OK**. The policy group is successfully deployed.

Verifying Deployed Policies

To verify deployed policies, follow these steps:

- 1 From a command prompt, change directories to `/opt/OV/bin/OpC`.
- 2 Run the command:

```
ovpolicy -list
```
- 3 In the output, verify that the deployed TIBSPI policies are displayed.

Starting TIBCO SPI Tool

TIBCO SPI tools can be started from the HPOM Administration interface. Before starting TIBCO SPI, make sure that you have installed and configured the Frontend. For more information about tools, see [Appendix B, Policies, Tools, and Reports](#)



Make sure you have set the `JAVA_HOME` variable to the JRE installation directory. See section [Configuring Frontend and Backend Service](#) on page 35.

Starting TIBCO SPI Using the Tool

To start TIBCO SPI, follow these steps:

- 1 On the Administration interface, click **Integrations** → **HPOM for UNIX UI**.
- 2 Login with administrative credentials. For example, `opc_admin`.
- 3 Select **Nodes**. Right click the selected node. Select **Start** → **Start TIBCO SPI**. The TIBCO SPI is started successfully.

Launching Discovery

To launch discovery of TIBCO SPI, follow these steps:

- 1 Select **Integrations** → **HPOM for Unix Operational UI**.
- 2 Log on with the default credentials:
 - User Name: `TIBSPI_Op user`
 - Password: `TIBSPI_Op`
- 3 Click **Services** tab in the message browser to view the service map. Using the Service Map, you can find out the application or services that have a problem (if any). The lines in the Service Map are coded with different colors to show various levels of severity. For example, red lines show that the application has critical problems.

Checking TIBCO SPI Status

You can check the status of the TIBCO SPI to see if it is started and operating successfully. You can also check the status to ensure that the TIBCO SPI has been stopped successfully. This is helpful when debugging any problems.

To check the Status of the TIBCO SPI, run TIBCO SPI Status Tool as follows:

- 1 On the Administration interface, click **Integrations** → **HPOM for UNIX UI**.
- 2 Login with administrative credentials. For example, `opc_admin`.

- 3 Select **Nodes**. Right-click the selected node. Select **Start** → **TIBCO SPI Status**. The following message appears:

TIBSPI Backend is running...

TIBSPI Frontend is running...

Installing Resource Explorer

The HP Resource Explorer is used to interact with TIBCO EMA Managed Objects (MOs) that are exposed for management purposes. The Resource Explorer interacts directly with the MOs and enables the operator to perform many client management tasks. These include:

- Browsing MO published events
- Browsing relationships between MOs
- Browsing and editing MO attributes
- Invoking operations on MOs and editing their parameter values

The HP Resource Explorer must be installed on a Windows platform. In addition, when accessing the Resource Explorer from the Java console, the Console and Resource Explorer must be installed on the same computer.

To install the HP Resource Explorer, follow these steps:

- 1 Transfer `hp_resource_explorer.zip` file, located on the management server at `/opt/OV/bin`, to a location on your system where service Navigator interface is running.
- 2 Unzip the HP Resource Explorer to any directory on your local computer.
- 3 Modify the user's `PATH` environment variable to include the directory where you installed the HP Resource Explorer. The `PATH` is used by the Java console to locate and start the Resource Explorer.
- 4 Make sure `JAVA_HOME` is set.

Starting HP Resource Explorer from Console

The HP Resource Explorer is typically started from the console. You can start multiple concurrent Resource Explorer sessions.

To start the Resource Explorer from the Java console, follow these steps:

- 1 Start the HP Java console.
- 2 From the Object Pane, expand the services node.
- 3 From the TIBService node, right-click a TIBCO service and then from the popup menu select **Start** → **Resource Explorer**. The Resource Explorer starts in its own window in a separate process.

Online help is included with the Resource Explorer. From the Explorer's menu bar, select **Help**. The Online Help includes instructions for browsing and editing MOs as well as invoking an MO's operations.

Starting HP Resource Explorer form Command Line

The Resource Explorer can also be started from the command line using the `hp_resource_explorer.bat` file. The file is located in the `root` directory where the Resource Explorer is installed.

As part of the command, you must pass the URL of the management web service. Once started, this web service becomes the root of the functional tree in the Resource Explorer. The following is an example command line:

```
hp_resource_explorer.bat -moUri http://<host>:8888/  
?wsdl:objid=tibema://www.tibco.com/ema/2005/01/mo/  
identity/ServiceInstance/tibtest1/TIBCOservers/  
<machine>.<domain name>-7500
```

Installing Reporter

TIBCO SPI integrates with HP Reporter, which is a Windows-based report management system. As part of the integration, a set of reports are included with the TIBCO SPI and used to see the performance of the TIBCO Applications.



HP Reporter must be installed prior to completing the instructions in this section. In addition, the Frontend service system must be running either HP Performance Agent or the Embedded Performance Component (Coda). See [Chapter 3, Performing Standard Management Functions](#) for more information about HP Performance Agent or the Embedded Performance Component (Coda).

To install the Reporter, follow these steps:

- 1 From the HP Operations Smart Plug-ins DVD, change directories to `\WINDOWS\HP_REPORTER\TIBSPI\TIBSPI-Reporter.msi`.
- 2 Double-click the **TIBSPI-Reporter.msi**. An InstallShield Wizard appears.
- 3 Click **Next**. The Setup Type screen appears.
- 4 Accept the default option (Complete) and click **Next**. The Ready to Install the Program screen appears.
- 5 Click **Install** to initiate the installation.
- 6 After the installation is complete, click **Finish**.

Configuring TIBCO SPI to Run as Non-Root User

HPOM processes normally run as user root on UNIX systems. The root or administrative privileges enable the processes to perform the following:

- Access HPOM related files and resources that are normally restricted to privileged access only
- Switch user for application specific access rights
- Access operating system resources such as log files and configuration files
- Start application or operating system specific commands and executables

TIBCO SPI processes function in a similar way. But there can be systems within IT environments where it is necessary to limit the number of processes that have root permissions to a small, well defined and tested group. TIBCO SPI on UNIX managed node can be configured to run under a user that does not have root permissions. This is often referred to as “running as non-root”.



This feature is not supported if both the Frontend service and Backend service are located on the HPOM management server.

Configuring TIBCO SPI to run as non-root is supported on HTTPS agents with HPOM using the `ovswitchuser` tool.

To configure SPI as non-root user, follow these steps:

- 1 Stop HPOM processes by running the following command:

```
ovc -kill
```

- 2 Run the following script to assign the permissions and ownership to non-root user for agent processes:

```
/opt/OV/bin/ovswitchuser.sh -existinguser <non-root user>  
-existinggroup <non-root group>
```

For example:

```
/opt/OV/bin/ovswitchuser.sh -existinguser tibuser -  
existinggroup tibcogroup
```

- 3 Run the following script to assign the permissions and ownership to non-root user for TIBCO SPI:

```
/var/opt/OV/bin/instrumentation/tib-switch-user.pl  
<non-root user> <non-root group>
```

- 4 Change BBC port from 383 (default value) to any available port greater than 1024, on both the systems where Backend and Frontend are running.

- a On the managed node (where Frontend is installed) run the following command.

```
ovconfchg -ns bbc.cb.ports -set PORTS "<host name of the  
system where frontend is installed>:<port number>"
```

For Example:

```
ovconfchg -ns bbc.cb.ports -set PORTS  
"<machine>.<domain name>:8001"
```

- b On the management server (system where the Backend service is installed) run the following command.

```
ovconfchg -ns bbc.cb.ports -set PORTS "<host name of the
management server>:<default port>,<host name of the machine
where frontend is installed>:<new port number>"
```

For Example:

```
ovconfchg -ns bbc.cb.ports -set PORTS
"machine1.domain.com:383, machine2.domain.com:8001"
```

- 5 If the performance agent is Coda, change the coda port on the managed node from 381(default port) to any available port greater than 1024 by running the command:

```
ovconfchg -ns coda.comm -set SERVER_PORT <port number>
```

- 6 Confirm the port change by executing the following command on the system where frontend service is installed:

```
ovconfget
```

- 7 Start the agent as non-root user by running the following command on the system where frontend service is installed:

```
su - <non-root user>
```

- 8 Start ovc as non-root user by running the following command:

```
ovc -start
```

(ensure that all processes are running)

For information about supported agent platforms, see *HP Operations Smart Plug-in for TIBCO Release Notes*. For more information about configuring non-root user, see *HP Operations HTTPS Agent Concepts and Configuration Guide*.

Upgrading TIBCO SPI

You can upgrade the TIBCO SPI from HPOM for HP-UX or Solaris version 8.xx to HPOM for HP-UX, Linux or Solaris version 9.1x.

Note the following when you install TIBCO SPI version 1.06 on HPOM 9.1x which has TIBCO SPI 1.05:

- Complete the migration process from HPOM 8.xx to HPOM 9.1x before upgrading the TIBCO SPI to version 1.60.
- Before upgrading the SPI to version 1.60, take backup of the contents in the `/var/opt/OV/conf/tib` directory, if you need to use the old content again. When you upgrade TIBCO SPI to new version, the old content in the `/var/opt/OV/conf/tib` directory will be lost permanently.
- The HP-UX binary files does not work when migrated from HPOM for HP-UX 8.xx to HPOM for Linux 9.1x.
- Having the TIBCO SPI version 1.50 (migrated from HPOM 8.xx) and TIBCO SPI version 1.60 on HPOM 9.1x, you must move all managed nodes to the TIBCO SPI version 1.60 as soon as possible.
- If TIBCO SPI 1.60 is installed on an HPOM 9.1x system, which also has TIBCO SPI 1.50 installed, note the following points:
 - You must configure the newly added managed nodes using the TIBCO SPI 1.60.
 - No configuration is possible on the existing or old managed nodes monitored by the TIBCO SPI 1.50. This is because the TIBCO SPI 1.50 configuration tools are overwritten by the TIBCO SPI 1.60 tools and these tools are incompatible.
- Patches for TIBCO SPI version 1.50 must be installed before starting the HPOM migration process. After installing TIBCO SPI version 1.60, no patches or hot-fixes for TIBCO SPI version 1.50 can be installed on the HPOM server.
- To run the interface related to TIBCO SPI 1.60, you must install X-windows client software on the machine from which you will start the HPOM for HP-UX, Linux or Solaris 9.1x server Operator interface.
- Installing patches that will be released in future for TIBCO SPI version 1.50 are not supported on HPOM for HP-UX, Linux, or Solaris version 9.1x, after migration. However, a patch can be installed on the HPOM for HP-UX 8.xx server and migrated to HPOM for HP-UX, Linux, or Solaris version 9.1x environment.

To upgrade the earlier versions of the TIBCO SPI to version 1.60, perform the following tasks:

- [Upgrading the Management Server from HPOM 8.xx to HPOM 9.1x](#)
- [Migrating TIBCO SPI 1.50 from HPOM 8.xx to HPOM 9.1x](#)
- [Upgrading TIBCO SPI 1.50 to TIBCO SPI 1.60 on HPOM 9.1x](#)

Upgrading the Management Server from HPOM 8.xx to HPOM 9.1x

Read and follow the steps provided in *HPOM for UNIX 9.10 Installation Guide* for migrating or upgrading HPOM for UNIX 8.xx to HPOM for UNIX 9.1x.

Migrating TIBCO SPI 1.50 from HPOM 8.xx to HPOM 9.1x

The instrumentation files and other SPI specific data are migrated while migrating or upgrading HPOM for UNIX 8.xx server (where the TIBCO SPI 1.50 is installed) to HPOM for UNIX 9.1x. Some SPI specific data, however, must be migrated manually.

Migrating the HPOM from one system to another

Install HPOM for UNIX 9.1x on a new system. To perform the migration from one system to another, perform the following steps:

- 1 After you complete migrating HPOM for HP-UX or Solaris 8.xx to HPOM for HP-UX, Linux or Solaris 9.1x, create the following directories on the target HPOM 9.1x server:

```
/var/opt/OV/tmp/tib  
/var/opt/OV/conf/tib  
/var/opt/OV/datafiles/tib  
/opt/OV/license-agreements/tib/
```

- 2 Copy the files present in the directories created in step 1 from HPOM for HP-UX, Linux or Solaris 9.1x server at their respective folders.

Upgrading TIBCO SPI 1.50 to TIBCO SPI 1.60 on HPOM 9.1x

You can upgrade the TIBCO SPI on a standalone HPOM 9.1x server through HPOM Console.

Upgrading TIBCO SPI on a Standalone HPOM 9.1x Server through HPOM Console

To upgrade the TIBCO SPI on a standalone HPOM 9.1x server, follow these steps:

- 1 Rename the policy and tool group for TIBCO SPI from **SPI for TIBCO** to **SPI for TIBCO_OLD**. Rename both the **Name** and the **Label** (for example, **TIBSPI:TOOLS** to **TIBSPI:TOOLS_OLD**).
- 2 Un-assign the policies or policy groups assigned to the node.
- 3 Kill `rmid` and all Java processes started by the SPI on the node.
- 4 Delete the old policies, instrumentation, and datasources on the node manually. The existing data is deleted. Hence, take a backup of your existing data.

Manually delete the existing TIBCO SPI datasource when you upgrade the SPI. For example, `ddfutil /var/opt/OV/tib/dataalog/graph.log -rm all`. A new datasource is created and the existing data is lost. The datasource is deleted irrespective of whether you are using CODA or HP Performance Agent. When you upgrade from a previous installation, all your configuration entries are preserved

- 5 Install and Configure TIBCO SPI.

3 Performing Standard Management Functions

This chapter provides management tasks that are typically performed when managing a TIBCO environment. In particular, the following sections are included:

- Service Management
- Event Management
- Monitoring and Data Collection
- Reporting and Performance Graphs
- Monitoring Performance Metrics with HP Performance Manager
- TIBCO SPI Self Management
- Modify Logging and Tracing Levels

Service Management

Service management is achieved using the Service Navigator that is included in the HPOM console and using the HP Resources Explorer plug-in to the Service Navigator. At runtime, the TIBCO SPI automatically discovers TIBCO managed resources and represents them as a Service Map. Any deployment changes that occur in the TIBCO environment are dynamically synchronized with the Service Map.

The Service Navigator and HP Resource Explorer also enable detailed management of the resources that are presented in the Service Map. The detailed management includes browsing the managed resource hierarchy, their relationships, attributes, metrics, and invocation of methods that are exposed by the resource.

Viewing TIBCO Managed Resources

To see TIBCO managed resources, follow these steps:

- 1 Start the HPOM for UNIX console.
- 2 Log on with the username **TIBSPI_Op** and password **TIBSPI_Op** (if a different operator was configured, use that operator name instead of **TIBSPI_Op**). You can see the Managed Objects on the service map.

Linking Other Service Maps

This feature enables you to link the TIBCO service map to the infrastructure service maps that the TIBCO service nodes depend on. These infrastructure elements can be anything from hardware, to other applications like SAP or Database. To see an integrated service map, the infrastructure components must have a corresponding SPI installed and must have its own service map in the service navigator. There are two methods of linking other SPI service maps to the TIBCO SPI service map:

- Automatic
- Manually (based on a configuration file)



The Automatic linking is currently limited to the service map of the Operating System (OS) SPI. All other service maps can be linked manually.

Linking Automatically

To automatically link the OS SPI service map, the node hosting RVD (Rendezvous Daemon) should be managed using the OS SPI and the OS SPI's service discovery should be enabled.

Linking Manually

The TIBCO SPI enables to manually link to other SPIs. For example, if there is a Data Base (DB) adapter on the TIBCO EMA agent, then this adapter can be linked to a DB SPI, which is already deployed and available in the service map.

To manually link other service maps, follow these steps:

- 1 Run **Configure TIBCO SPI Tool**.

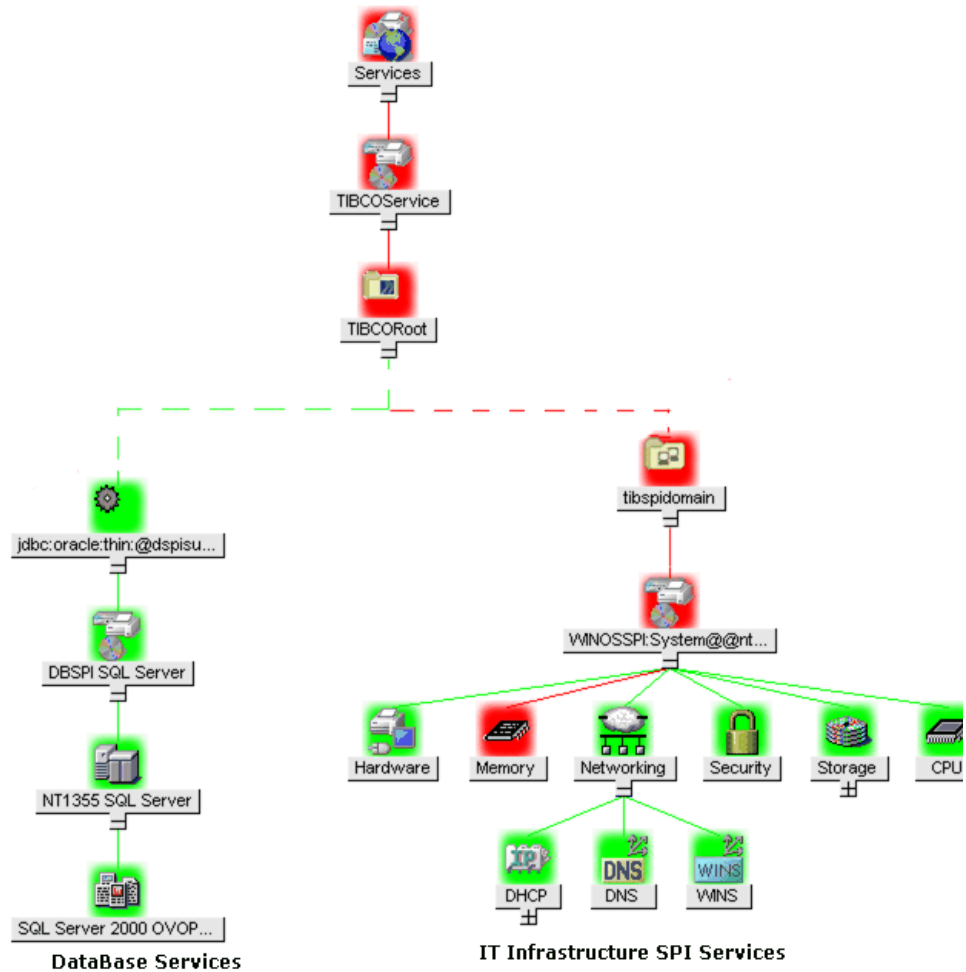
- 2 Type the following properties:
 - AliasInfo/ServiceName: Adapter's service name. The name can be found by clicking **Properties** on the service icon in the Java console's Service Navigator.
 - AliasInfo/AliasName: The service name on the SPIs (such as DB SPI, OS SPI, SAP SPI) which integrates with TIBCO SPI. The name can be found by clicking **Properties** on the service icon for a SPI in the Java console's Service Navigator.
 - AliasInfo/AliasLabel: The service label on the SPIs (such as DB SPI, OS SPI, SAP SPI) which integrate with TIBCO SPI. The label can be found by clicking **Properties** on the service icon for a SPI in the Java console's Service Navigator.
- 3 Run **Restart TIBCO SPI** tool.

End-to-End View of TIBCO SPI Integrations

The TIBCO SPI provides a unique capability to obtain an end-to-end view of the highest level domain in TIBCO down to the lowest level details. The view can also include information from custom applications that have been instrumented with TIBCO management APIs. All of these can be correlated with their underlying infrastructure components.

This end-to-end view enhances the root-cause analysis capabilities of the TIBCO SPI, so that one can locate the source of the problem easily.

Figure 9 End-to-End view of TIBCO SPI Integrations



Filtering Unwanted MO types

You can define a list of MO types that you do not want to be displayed in the Java console's Service Map. This feature is useful if there are many MOs being exposed.

To filter out unwanted MO types, follow these steps:

- 1 Run Configure TIBCO SPI tool.
- 2 In the `WCConfig.xml` configuration editor interface, select **Managed Objects to Ignore** under **Misc. Configuration of Front End Configuration**.
- 3 Fill in the managed object types you want to ignore in the General Info section.
- 4 Select **File** → **Save** to save your changes to the configuration file.
- 5 Select **File** → **Exit**.
- 6 In the Output of Tool window, you should see the message 'TIBCO SPI configuration completed.' It can take some time before this message appears. Do not close the Output of Tool window until you see the message.
- 7 Verify that the Frontend Service startup has completed. Look for the 'Service map created' message in the `/var/opt/OV/log/tib/frontend.log` file.
- 8 Start the HPOM for UNIX console and log on with the username **TIBSPI_Op** and password **TIBSPI_Op** (if a different operator was configured, use that operator name instead of **TIBSPI_Op**). The MO that you filtered is no longer visible in the service map.

Event Management

The TIBCO SPI solution monitors availability and status of TIBCO applications as well as providing the ability to run applications manually or automatically when events are received through both HPOM, as well as a WSDM channel. You can filter events by adding new conditions using the `TIBSPI-EventService-Msg-V1` or create your custom conditions.

Viewing TIBCO Events

All events through EMA are captured and displayed in the Java console message browser.

To see TIBCO Events, follow these steps:

- 1 Start and log on to the Java console.
- 2 From the Object Pane, expand the Message Groups node to see the TIBCO and TIBCO SPI message groups.
- 3 Right-click a message and select **Properties**. The Message Properties dialog box appears and lists additional details about the event.

Automatically Responding to Events

A script which enables you to run an MO's operations from the command line or from an HPOM is provided. Typically, the Resource Explorer is used to run operations. This script enables you to perform operator automated actions, where actions are performed based on captured events.

To start the operations from the command line:

- 1 Change directories to `opt/OV/bin`
- 2 Run the `tib-invoke-operation` script using the following parameters:
 - WSDL location of the MO
 - NamespaceURI of the PortType
 - PortType Name
 - OperationName

For example:

```
Tib-operation http://<machine1>.<domain name>:8888/  
?wsdl:objid=tibema://www.tibco.com/  
ema/2005/01/mo/identity/ServiceInstance/tibtest1/  
TIBCOservers/<machine2>.<domain name>-7500 http://  
schemas.hp.com/wsmf/2003/03/Foundation  
ManagedObjectConfigurationPT GetName
```

Monitoring and Data Collection of TIBCO

The Frontend Service uses metric definitions to capture TIBCO management data for use in HP Performance Manager or Service Reporter (when generating alarms, graphs, and reports). This section provides instructions on how to customize the collected data and how to change the default collection behavior. A brief overview of, how metrics are defined, is also provided.

Metric Definition Configuration Files

Metrics are configured using two XML configuration files:

`MetricDefinitions.xml` and `UDMMetricDefinitions.xml` (used for custom adapters) files. These files are located on the Frontend Service node in `/var/opt/OV/conf/tib`. The elements for these files are as follows.

- `<MetricDefinitions>` – The `MetricDefinitions` element is the top-level element within the document. It contains a collection of metrics, consisting of one or more metric definitions.
- `<Metric>` – The `Metric` element represents one metric. Each metric has a unique ID. If a user-defined metric is an alarming, graphing or reporting metric, the metric ID must be `'TIBSPI_0xxx'` where `xxx` is a number from 700 through 799. Otherwise, if the metric is used only within the calculation of another metric, the metric ID must begin with a letter (case-sensitive) and can be followed by any combination of letters, numbers and underscores. A metric element contains one more source elements that represent the metric data source. Two data sources are supported: WSM and calculations. The following table lists attributes for the `Metric` element:

Table 1 Metric Element Attributes

Attribute	Type/ Values	Required	Default	Description
id	ID	Yes	N/A	The metric ID.
name	Text	No	No	The metric name, used for graphing and reporting. The name can be up to 20 characters in length.
alarm	Yes/No	No	No	If yes, the metric value is sent to the agent using <code>opcmon</code> .
alarm	Yes/No	No	No	If yes, the metric value is sent to the agent using <code>opcmon</code> .
report	Yes/No	No	No	If yes, the metric value is logged for reporting.
previous	Yes/No	No	Yes	If yes, the metric value is saved in a history file so that deltas can be calculated. If you are not calculating deltas on a metric, set this to 'no' for better performance.
graph	Yes/No	No	No	If yes, the metric is logged for graphing.
description	No	text	“ ”	A description of the metric.

- `<WSM>` – The WSM element is used when the data source of the metric is a TIBCO metric definition. The WSM element contains the following sub-elements:
 - `<MetricName>` – The TIBCO metric definition name.
 - `<ObjectTypeList>` – List of MO types that will have metric value collected.
 - `<ObjectIDList>` – List of MO instances that will have metric values collected.
- `<Calculation>` and `<Formula>` – The Calculation element is used when the data source of the metric is a calculation using other defined metrics. The Calculation element contains a formula element whose content is a string that specifies the mathematical manipulation of other metric

values, to obtain the final metric value. The metrics are referred to in the calculated expression by their metric ID. The collector can perform calculations that combine one or more metrics to define a new metric. The result of the calculation is the metric value. Calculations must use syntax as follows:

- Operators supported are +, -, /, *, and unary minus.
- Operator precedence and associativity follows the Java model.
- Parentheses can be used to override the default operator precedence.
- Accepted operands are metric IDs and literal doubles.

A metric ID can refer to either a WSM metric or another calculated metric. Literal doubles can be specified with or without the decimal notation. The metric ID refers to the id attribute of the Metric element in the metric definitions document. The calculation parser also supports the following functions. All function names are lowercase and take a single parameter which must be a metric ID:

- Delta – returns the result of subtracting the previous value of the metric from the current value.
- Interval – returns the time elapsed since the last time the metric was collected in milli-seconds.

The following example defines a metric whose value is the ratio (as expressed as a percent) of Metric_1 to Metric_3:

```
<Formula>(Metric_1/Metric_3)*100</Formula>
```

The following example can be used to define a metric that is a rate (number of times per second) for Metric_1.

```
<Formula>(delta(Metric_1)/interval(Metric_1))*1000</Formula>
```

Modifying Data Collection

By default, data is collected for all RVDs, JMS Servers and BWEngines. If you want to collect data for a subset of the RVDs, JMS Servers or BWEngines or a subset of the metrics, you need to modify the `/var/opt/OV/conf/tib/MetricDefinitions.xml` file. For example, if you only want to collect `MissedPackets` for RVD:

```
tibema://www.tibco.com/ema/2005/01/mo/identity/ServiceInstance/  
tibtest1/TIBCOservers/ovw010-7500
```

you would change:

```
<Metric id="MissedPackets" alarm="no">  
  <WSM>  
    <MetricName>Missed Packets</MetricName>  
    <ObjectTypeList>  
      <ObjectType>  
        http://www.tibco.com/ema/2005/01/mo/type/RVD  
      </ObjectType>  
    </ObjectTypeList>  
  </WSM>  
</Metric>
```

to:

```
<Metric id="MissedPackets" alarm="no">  
  <WSM>  
    <MetricName>Missed Packets</MetricName>  
    <ObjectIDList>  
      <ObjectID>  
        tibema://www.tibco.com/ema/2005/01/mo/identity/  
        ServiceInstance/tibtest1/TIBCOservers/  
        ovw010-7500  
      </ObjectID>  
    </ObjectIDList>  
  </WSM>  
</Metric>
```

Collecting Data for Custom Adapters

To collect data and metrics for custom adapter, follow these steps:

- 1 On the Frontend Service node, run the command:

```
cd /var/opt/OV/conf/tib
```

```
cp UDMMetrics-sample.xml UDMMetricDefinitions.xml
```

- 2 Add the metrics for the custom adapters to the `UDMMetricDefinitions.xml` file.
- 3 Bring up the HP Resource Explorer on the custom adapter MO. Follow the instructions in the [Starting HP Resource Explorer from Console](#) section.
- 4 Click **+** next to the custom adapter MO.
- 5 Note the value for the `Type` property. This information is required for another task.
- 6 Click **+** next to `ManagedObjectMetric` Interface.
- 7 Right-click **MetricValues** and select **Open** from the popup menu. Add each metric definition you want to alarm, graph, or report in the `UDMMetricDefinitions.xml` file.

- **Metric Definition Name:** A name for the definition.

- **Messages Sent:** The total number of messages sent since the adapter was started.

- **Message Drop Rate:** The percentage of messages dropped per second.

For example: If you want to graph the number of messages sent per collection interval and alarm on the message drop rate, the `UDMMetricDefinitions.xml` file contains the following entries:

```
<Metric id="TIBSPI_0700" name="MessagesSent" alarm="no"
      graph="yes" report="no">
```

```
  <Calculation>
```

```
    <Formula>delta (MessagesSentInt) </Formula>
```

```
  </Calculation>
```

```
</Metric>
```

```
<Metric id="MessagesSentInt" alarm="no">
```

```
  <WSM>
```

```
    <MetricName>Messages Sent</MetricName>
```

```
  <ObjectTypeList>
```

```

        <ObjectType>http://www.tibco.com/ema/2005/01/mo/type
            /ServiceInstance/Adapter</ObjectType>
    </ObjectTypeList>
</WSM>
</Metric>

<Metric id="TIBSPI_0701" name="MessageDropRate"
    alarm="yes" graph="no" report="no">
    <WSM>
        <MetricName>Message Drop Rate</MetricName>
    <ObjectTypeList>
        <ObjectType>http://www.tibco.com/ema/2005/01/mo/type
            /ServiceInstance/Adapter</ObjectType>
    </ObjectTypeList>
    </WSM>
</Metric>

```

- 8 **Make sure** `/var/opt/OV/bin/OpC/monitor` is in your PATH. Create the UDM data sources by running the following script (change directory to `/opt/OV/bin`):

```
./tib-perl tib-create-udm-datasources
```

- 9 Run **Stop TIBCO SPI** tool.
- 10 Run **Start TIBCO SPI** tool.

It is assumed that you have already assigned the `TIBSPI-Metrics-V1` group to the Frontend Service node.

Modify the `TIBSPI-Collect-Mon-V1` in the `TIBSPI-Metrics-V1` group to collect the UDM metrics as follows:

- 1 Click **All Policy** groups on the HPOM console. Click **TIBSPI-Metrics-V1**. Select the **TIBSPI-Collect-Mon-V1** and click **Edit** from the Actions Menu.

- 2 In the **Modify Threshold Monitor** dialog, add the UDM metrics to the **Monitor Program** or **MIB ID** field. For example, if you added metrics `TIBSPI_0700`, `TIBSPI_0701` and `TIBSPI_0702` to your `UDMMetricDefinition.xml` file, add `'700-702'` to the end of the **Monitor Program** or **MIB ID** field. Click **Save**.

Redeploy the policies by following the instructions in the [Deploying policies to Frontend Node](#) section.



The metrics values are not logged to the data source until the `TIBSPI-Metric-V1` group is assigned and deployed. See [Assigning Policy Groups](#) and [Deploying policies to Frontend Node](#).

Configuring Multi-Instance Metric Data

This procedure configures a metric which has multi-instance data. The metric is configured using the `MetricDefinitions.xml` file. The `UDMMetricDefinitions.xml` file is used for custom adapters.

To configure a metric that has multi-instance metric data modify the `MetricDefinitions.xml` file and add the following:

- For the metric that has multi instance data, add `instanceType="multi"` to the `<WSM>` tag.
- If you want the metric to only match certain instances, add `<InstanceList>` with `<Instance>` values.
- If you want the metric to match all instance values, do not include the `<InstanceList>` tag.

Example: All Instance Data (Collect)

```
<Metric id="WSFSPI_0011" name="SpotAll" alarm="yes"
graph="yes"
report="yes">
  <WSM instanceType="multi">
    <MetricName>getColorAssignmentCount-Count</MetricName>
    <ObjectTypeList>
      <Type>http://www.tibco.com/ema/2005/01/
        mo/type/ServiceInstance/Custom </Type>
```

```
</ObjectTypeList>
</WSM>
</Metric>
```

Metric WFSFPI_0011 is used to collect all instance data for the TIBCO Spot application. The getColorAssignmentCount-Count operation returns the count for each color.

```
return[0].row[0].Color = red
return[0].row[0].Count = 5
return[1].row[0].Color = black
return[1].row[0].Count = 1
return[2].row[0].Color = green
return[2].row[0].Count = 0
return[3].row[0].Color = orange
return[3].row[0].Count = 0
return[4].row[0].Color = darkGray
return[4].row[0].Count = 0
return[5].row[0].Color = pink
return[5].row[0].Count = 0
return[6].row[0].Color = yellow
return[6].row[0].Count = 2
return[7].row[0].Color = blue
return[7].row[0].Count = 9
return[8].row[0].Color = lightGray
return[8].row[0].Count = 0
return[9].row[0].Color = gray
return[9].row[0].Count = 0
return[10].row[0].Color = cyan
return[10].row[0].Count = 0
return[11].row[0].Color = magenta
return[11].row[0].Count = 2
```

The metric is configured for the following functions:

- Call `opcmon` for each instance with object as `<servername>:<instancename>` and the following options: `servername`, `instancename`, and `serverhost`.

- Log data for graphs. For graphs, only one value is logged and this is the sum of the instance values. This is a limitation in the data collector. For the users to graph instance data, they have to use the data from the reports. For the above example, the graph data logged is 19 for Spot-ovw022 (server name).
- Log data for reports. Data is logged for each instance. For the above example, the report data logged is:

```

red          5
black       1
green       0
orange      0
darkGray    0
pink        0
yellow      2
blue        0
lightGray   0
gray        0
cyan        0
magenta     2

```

Example: Specific Instance Data (Collect)

```

<Metric id="WSFSPI_0012" name="SpotBlue" alarm="yes"
graph="no"
  report="no">
  <WSM instanceType="multi">
    <MetricName>getColorAssignmentCount-Count</MetricName>
    <ObjectTypeList>
      <ObjectType>http://www.tibco.com/ema/2005/01
        /mo/type/ServiceInstance/Custom</ObjectType>
    </ObjectTypeList>
    <InstanceList>
      <Instance>blue</Instance>
    </InstanceList>
  </WSM>
</Metric>

```

Metric `WSFSPI_0012` is used to collect the count for blue in the TIBCO Spot application. The metric is configured to call `opcmon` for the blue instance and no graph or report data is logged.

Configuring a Threshold for Multi-Instance Metric Data

Configuring a threshold on multi instance metric data is achieved using a monitor. The ISV developer creates a monitor with the same name as the metric id. The developer then adds conditions for each instance. A condition that matches all instances can also be added. For example:

For the `WSFSPI_0011` metric, the ISV developer creates a monitor with the following information:

- Monitor Name: `WSFSPI_0011`
- Monitor: External
- Condition: `WSFSPI_0011: Magenta`
 - Object Pattern: `magenta`
 - Threshold: 1
 - Severity: minor
 - Message Text: `<$OPTION(instancename)> count (<$VALUE>) too high (>=<$THRESHOLD>)`
 - Service Name: `<$OPTION(serverhome)>`
- Condition: `WSFSPI_0011: All`
 - Object Pattern: `<*>`
 - Threshold: 4
 - Severity: warning
 - Message Text: `<$OPTION(instancename)> count (<$VALUE>) too high (>=<$THRESHOLD>)`
 - Service Name: `<$OPTION(serverhome)>`

Assuming that `opcmon` is called with the values defined in the All Instance Data (Collect) example and the `WSFSPI_0011` monitor is deployed. The following messages would be in the HPOM message browser:

- HPOM message

- Severity: Min
- Message Text: 'magenta' count (2.00) too high (>=1.00)
- HPOM message
 - Severity: Warn
 - Message Text: 'red' count (5.00) too high (>=4.00)
- HPOM message
 - Severity: Warn
 - Message Text: 'blue' count (9.00) too high (>=4.00)

Collecting Data for Specific Metrics

The `TIBSPI-Collect-Mon-V1` monitor is used to log the metric data for graphs. You can modify the metrics to collect data for a subset of the available metrics. For example, to collect data for metrics `TIBSPI_0001` – `TIBSPI_0004` and `TIBSPI_0026`, follow these steps:

- 1 Open the Policy group window. Click **SPI for TIBCO**.
- 2 Click **TIBSPI-Metrics-V1** group.
- 3 Select **TIBSPI-Collect-Mon-V1** and click **Edit** from the Actions Menu.
- 4 In the **Edit Scheduled_Task Policy "TIBSPI-Collect-Mon-V1"** window, modify the command as follows:

```
Tib-perl -s TIBSPI-Collect-data -c TIBSPI-Collect-Mon-V1  
-m 1-4, 26
```

- 5 Click **Save**.
- 6 Redeploy the policies by following the instructions in the [Assigning Frontend Service Policies](#) section.

Monitoring Custom Adapter Metric Thresholds with HPOM

To monitor custom adapter metric thresholds with HPOM, follow these steps:

- 1 The metric has to be added to the `/var/opt/OV/conf/tib/UDMMetricDefinitions.xml` file on the Frontend Service node. The alarm attribute for the metric has to be set to 'yes'. If you are currently not collecting data for the metric, follow the instructions in the [Collecting Data for Custom Adapters](#) section.
- 2 If you made modifications to the `UDMMetricDefinitions.xml` file in the above step then follow these steps:
 - a Remove the `/var/opt/OV/conf/tib/UDMMetricDefinitions.ser` file on the Frontend Service node.
 - b Stop the Frontend Service using frontend un-installation tool.
 - c Start the Frontend Service using frontend installation tool. See [Installing Frontend Service](#) on page 34
- 3 On the administrator interface, select Policy Bank → **SPI for TIBCO SPI for TIBCO** → **TIBSPI-Metrics-V1** → **TIBSPI_0009**. Click **Copy** from the Actions Menu.
- 4 In the Copy Threshold Monitor dialog, update the Name and Description fields. The Name value must be the id value for the appropriate metric in the `/var/opt/OV/conf/tib/UDMMetricDefinitions.xml` file. For example, if you want to monitor the message drop rate and your `UDMMetricDefinitions.xml` file contains the following entry:

```
<Metric id="TIBSPI_0701" name="MessageDropRate"
  alarm="yes" graph="no" report="no">
  <WSM>
    <MetricName>Message Drop Rate</MetricName>
    <ObjectTypeList>
      <ObjectType>http://www.tibco.com/ema/2005/01/mo/type/
        ServiceInstance/Adapter</ObjectType>
    </ObjectTypeList>
  </WSM>
</Metric>
```

Use `TIBSPI_0701` as the Monitor Name value.
- 5 Click **Save**.
- 6 In the Message Source policy window, click **Conditions**.

- 7 Modify the conditions in the Message and Suppress Conditions dialog. Click **Save**.
- 8 Close the Message Source policy window.
- 9 The `TIBSPI-Collect-Mon-V1` has to be assigned and deployed on the Frontend Service node. The policies also should collect the custom adapter metric's data.
 - a See the instructions at the end of the [Collecting Data for Custom Adapters](#) section on how to verify that the custom adapter metric's data is being collected.
 - b Run `ovc` on the Frontend Service node. See the [Assigning Frontend Service Policies](#) and [Deploying policies to Frontend Node](#) sections if the `TIBSPI-Collect-Mon-V1` is not in the returned list.

Changing Metric Data Collection Interval

To change the metric data collection interval, change the Polling Interval in the `TIBSPI-Collect-Mon-V1` and `TIBSPI-Graph-Mon-V1` policies. For example, to change the metric data collection from 5 minutes to 10 minutes, follow these steps:

- 1 On the Policy bank window, click **SPI for TIBCO** → **TIBSPI-Metrics-V1** → **TIBSPI-Collect-Mon-V1**. Click **Edit** on the Actions Menu.
- 2 Modify the Polling Interval from 5m to 10m. Click **Save**.
- 3 Select the **TIBSPI-Graph-Mon-V1** and click **Edit** on the Actions Menu.
- 4 Modify the Polling Interval from 5m to 10m.
- 5 Click **OK**.
- 6 Redeploy the policies by following the instructions in the [Deploying policies to Frontend Node](#) section.

Changing Metric Threshold Value

By default, there are a couple of monitor policies monitoring individual metrics data. For example, the `TIBSPI_0009` monitor policies monitors RVD re-transmitted packet rate. If the re-transmitted packet rate is ≥ 5 , a message of major severity appears in the HPOM message browser. If the retransmitted packet rate is ≥ 2 and < 5 , a message with minor severity

appears in the HPOM message browser. To create a message with minor severity when the retransmitted packet rate is ≥ 1 and < 5 , perform the following steps:

- 1 On the Policy bank window, select **SPI for TIBCO** → **TIBSPI-Metrics-V1** → **TIBSPI_0009**. Click **Edit** on the Actions Menu.
- 2 On the **Thresholds** tab, select **TIBSPI_0009.2**. Modify the Threshold from 2 to 1. Click **Save**.
- 3 Redeploy the policies by following the instructions in the [Deploying policies to Frontend Node](#) section.

Changing which Logfile to Monitor

If you installed the TIBCO EMA Agent in `c:\tibco\ema` and TIBCO Hawk in `c:\tibco\hawk` then the policies function correctly or else you need to modify the location of the logfile.

Follow these steps to change the location of the TIBCO Hawk logfile if TIBCO Hawk is installed in the same directory on all Windows Nodes:

- 1 On the Policy bank window, select **SPI for TIBCO** → **TIBSPI-Windows-V1** → **TIBSPI-WIN-HAWK-Agent-V1** → **TIBSPI-Hawk-WIN-Log-V1**. Click **Edit** on the Actions Menu.
- 2 Click **Source**. Modify the Logfile to include the location of the TIBCO Hawk Agent log file.
- 3 Click **Save**.
- 4 Redeploy the policies by following the instructions in the [Deploying policies to Frontend Node](#) section.

Reporting and Performance Graphs

This section provides instructions for using the Embedded Performance Component (CODA) for the purpose of generating reports and performance graphs. In addition, instructions for viewing reports in HP Reporter is also provided.

Using Embedded Performance Component (CODA)

The Embedded Performance Component (CODA) is a performance subagent that is bundled for free with the HP Operations agent in HPOM for UNIX 7.0 and later. It is a light-weight performance agent comparable to HP Performance Agent. The Embedded Performance Component (CODA) holds only 5 weeks worth of data where as HP Performance Agent can potentially hold years worth of data. The Embedded Performance Component (CODA) Database is stored in the `<OVAgentDataDir>/databases` directory. There is a `coda.db` and `coda##### logs`.

To check if the Embedded Performance Component (CODA) is running, run the following command from the command prompt:

```
ovc -status -id coda (HPOM for HP-UX, Linux, or Solaris 9.1x)
```

The output should verify that the Performance Agent `/opt/OV/bin/coda` is running. You can also run the Coda utility program. On HP-UX, the command is:

```
/opt/OV/bin/ovcodauti1 -support (HPOM for HP-UX, Linux, or Solaris 9.1x)
```

The result is a list of the last logged interval for all the standard metrics and their values.

Embedded Performance Component (CODA) Logging

The Embedded Performance Component (CODA) keeps up to 5 weeks of data. Every Sunday at 12:00am (midnight), a new log file is created. The Embedded Performance Component (CODA) will continue to create a new logfile each week until it has accrued 5 weeks of logfiles. When the sixth logfile is created, the oldest file is deleted. The Embedded Performance Component (CODA) log file (`coda.log`) is located in `<OVAgentDataDir>/log/`. For example, on HP-UX the file is `/var/opt/OV/log/coda.log`. To check if the Embedded Performance Component (CODA) is logging data, use the following procedure:

- 1 Open `/var/opt/OV/log/coda.log`
- 2 At the end of the `coda.log` file, you should see the starting message; information about files which were opened, deleted and/or created and finally the 'Waiting for requests...' message. As the Embedded Performance Component (CODA) logs data, the timestamp for the newest `coda##### log` changes.

Viewing TIBCO SPI Reports

This section provides instructions to use HP Reporter to gather TIBCO SPI Metric data and creates TIBCO SPI reports. The section is intended only as a quick start reference and does not represent a replacement for the Reporter documentation.

To view TIBCO SPI reports, follow these steps:

- 1 From the Windows Taskbar, select **Start** → **Programs** → **HP Software** → **Reporter** → **Reporter**.
- 2 From the left tree, right-click **Discover Area** and select the **Add Single System** command. The Add Single System dialog box appears.
- 3 In the System field, type the full Domain Name System (DNS) name of the computer where the Frontend Service is installed (hostname.mycompany.com).
- 4 Click **Add**. The Reporter's discovery program runs, discovers the system, and automatically gathers metric data (collected by either HP Performance Agent, or the Embedded Performance Component (CODA) from the system.
- 5 From the Main toolbar, click **Generate Reports**. The TIBCO SPI reports are generated. This can take several minutes to complete.
- 6 From the Main toolbar, click **Show Reports**. A browser appears and lists all of the TIBCO SPI reports. The reports are organized into 4 categories that show the metric data over different time ranges: TIBCO Full Range, TIBCO Last Full Month, TIBCO Last Full Week, and TIBCO Yesterday.

Defining a User Friendly Name for an MO

You can define a user friendly name for the MOs that appears on TIBCO graphs and reports. The name is also used as the name of the file where the data is logged for graphs before it is sent to HP Performance Agent, or the Embedded Performance Component (CODA). Therefore, the name must be a valid file name.

In order to use the Service Reporter reports that compare network and TIBCO RVD performance metrics, a user friendly name for each RVD is automatically defined in the following format as part of the out-of-box solution:

<RVD fully qualified host name>-<RVD port>-RVD

For example:

ovw010.hp.com-7500-RVD

To define a user friendly name, follow these steps:

- 1 Run Configure TIBCO SPI tool.
- 2 From the configuration editor interface, click + icon next to Front End Configuration.
- 3 Click **Report Information**.
- 4 In the menu bar, select **Edit** → **New**.
- 5 Use the **ReportGroupObjectID** and the **ReportGroupName** fields to type the group object ID and the group name. Remember that the **ReportGroupName** must be able to be used as a valid file name. For example:

Assume:

The WSDL location for the RVD using port 7500 on <machine>.<domain name> is **http://<machine>.<domain name>:8888/?wsdl:objid=tibema://www.tibco.com/ema/2005/01/mo/identity/ServiceInstance/tibtest1/TIBCO Servers/machine-7500**

Then:

ReportGroupObjectID = http://<machine>.<domain name>:8888/?wsdl:objid=tibema://www.tibco.com/ema/2005/01/mo/identity/ServiceInstance/tibtest1/TIBCO Servers/machine-7500

ReportGroupName = <machine>.<domain name>-7500-RVD

- 6 Continue to add new entries for each MO.
- 7 Select **File** → **Save**.
- 8 Select **File** → **Exit**.
- 9 Click **Close** in the Output of Tool window.

Monitoring Performance Metrics with HP Performance Manager

You can monitor performance using HP Performance Manager. For more information about HP Performance Manager, see *HP Performance Manager Administrator Guide*.

- ▶ The following procedures must be completed in the order listed.

Configuring HP Performance Manager

To configure HP Performance Manager, follow these steps:

- 1 Open the file `pmsystems.txt`. For example, on a Windows system, open `<Data_Dir>\shared\server\conf\perf\pmsystems.txt` file.

- ▶ If the file `pmsystems.txt` does not exist, create a new file.

- 2 Add the list of nodes, to be imported to HP Performance Manager, in this file.
- 3 Group the nodes by placing them in between the **GROUP:** tag and **END_GROUP** tags.

For example:

```
GROUP: MyTibcoGroup
System1.domain.com
END_GROUP
```

- 4 Run the command `ovpm uploadsystems`.

Creating Graph for RVDs

To create an HP Performance Manager graph (bytes sent) for an RVD, follow these steps:

- 1 Click **Start** → **Programs** → **HP** → **HP performance manager** → **Performance Manager**.

- 2 On the Performance Manager home page, click **Diagnostic View**.
- 3 Click **DataSources** → **Add**.
- 4 Select the Frontend node and click **List Data Sources**.
- 5 Select a Data Source and click **Connect**.
- 6 Select **Data Source** to view the Metric Classes, Instances and Metrics under the Selection Panel.
- 7 Select the class **TIBSPI_METRICS:TIBSPI_METRICS** and the metric **B003_BYTESSENT**. Drag and Drop the on the Graph Panel to view the graph.
- 8 Select the date range under the Graphs tab.
- 9 To save the state, click **Graphs** → **Save State**.

TIBCO SPI Self Management

The TIBCO SPI is capable of managing itself and all Frontend and Backend processes. The TIBCO SPI contains policies that need to be deployed to the node, to activate this feature. In addition, the TIBCO SPI monitors EMA agent process. For EMA agent monitor feature to be activated, the host where the EMA agent is running has to be a managed node, and the policies to monitor the process have to be deployed to that node.

Modify Logging and Tracing Levels

Logging and tracing levels can be changed for both the Frontend Service and the Backend Service and are useful for debugging and auditing purposes.

Changing Log Levels

The TIBCO SPI supports two log levels (**ERROR** and **INFO**) for both the Frontend Service and Backend Service log messages. By default the log level is set to **INFO** for both the Frontend and the Backend. Log levels can be customized by modifying the log property files. The property files are as follows:

- /var/opt/OV/log/tib/frontend.properties
- /var/opt/OV/log/tib/backend.properties

Changing Frontend Log Levels

To change the Frontend's log level from **INFO** to **ERROR**, follow these steps:

- 1 Open the /var/opt/OV/conf/tib/Frontend.properties file.
- 2 Set the java.util.logging.FileHandler.level to **ERROR**. For example:

```
java.util.logging.FileHandler.pattern = %h/frontend.log
java.util.logging.FileHandler.level = ERROR
```

- 3 **Save** and **Close** the file.
- 4 Restart TIBCO SPI. The Frontend log file is /var/opt/OV/log/tib/frontend.log

Changing Backend Log Levels

To change the Backend log level from **ERROR** to **INFO**, follow these steps:

- 1 Open the /var/opt/OV/conf/tib/Backend.properties file.
- 2 Set the java.util.logging.FileHandler.level to **ERROR**. For example:

```
java.util.logging.FileHandler.pattern = %h/backend.log
java.util.logging.FileHandler.level = ERROR
```

- 3 **Save** and **Close** the file.
- 4 Restart TIBCO SPI. The Backend log file is /var/opt/OV/log/tib/backend.log

Changing Trace Levels

The TIBCO SPI provides a mechanism that collects and stores all trace data in a `trace` file. By default, tracing is configured to show INFO messages. To get a detailed level of trace messages, the trace level has to be set to FINE. Trace levels can be customized by modifying the trace property files. The property files are as follows:

- `/var/opt/OV/log/tib/frontend.trace`
- `/var/opt/OV/log/tib/backend.trace`

Changing Frontend Trace Levels

To change Frontend trace levels from INFO to FINE, follow these steps:

- 1 Open the `/var/opt/OV/conf/tib/Frontend.properties` file.
- 2 For the Frontend trace file, set the `java.util.logging.FileHandler.level` value to FINE. For example:

```
java.util.logging.FileHandler.pattern = %h/frontend.trace
java.util.logging.FileHandler.level = FINE
```
- 3 **Save** and **Close** the file.
- 4 Run **Restart TIBCO SPI** tool. The Frontend trace file is `/var/opt/OV/log/tib/frontend.trace`.

Changing Backend Trace Levels

To change the Backend trace levels from INFO to FINE, follow these steps:

- 1 Open the `/var/opt/OV/conf/tib/Backend.properties` file.
- 2 For the Backend trace file, set the `java.util.logging.FileHandler.level` to FINE. For example:

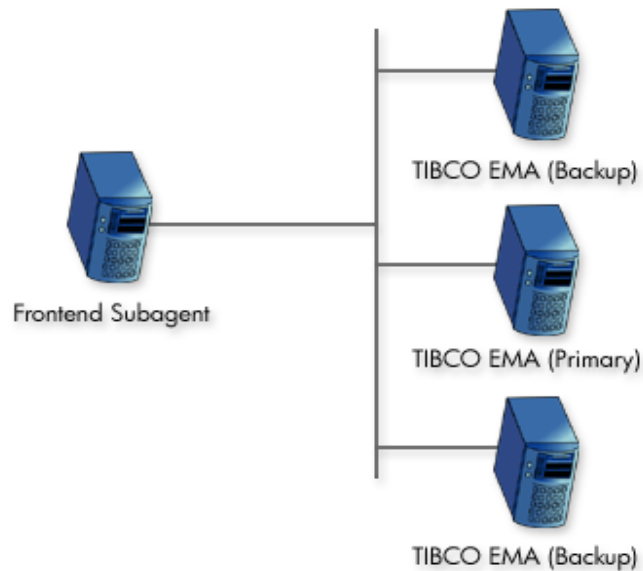
```
java.util.logging.FileHandler.pattern = %h/backend.trace
java.util.logging.FileHandler.level = FINE
```
- 3 **Save** and **Close** the file.
- 4 Run **Restart TIBCO SPI** tool. The Backend trace file is `/var/opt/OV/log/tib/backend.trace`.

4 Implementing Failover

This chapter provides instructions for implementing failover between the Frontend Service and two or more TIBCO EMA components.

The Frontend Service can be configured to use multiple EMA installations. This enables the Frontend Service to continue collecting management data of a TIBCO environment even when a TIBCO EMA stops responding. The failover solution depends on multiple installations of the TIBCO EMA.

Specifically, the Frontend Service uses one or more location candidates. Each candidate contains WSDL locations for managed objects that are exposed by a particular EMA. The first candidate is considered the primary candidate. Any subsequent candidates are considered backups for the primary candidate.



When the Frontend Service starts, it tries the first location candidate. If the location candidate responds, it is used. If there is no response, the Frontend tries the next location candidate. This process is repeated until a location candidate responds. For example, you can provide two location candidates:

```
http://hostA.domain.com:8888/?wsdl:objid=tibema//  
www.tibco.com/ema/2005/01/mo/identity/Domain/tibtest  
  
http://hostB.domain.com:8888/?wsdl:objid=tibema//  
www.tibco.com/ema/2005/01/mo/identity/Domain/tibtest
```

In this example, the EMA on Host A is serving as the primary EMA and Host B is the backup. If Host A fails, then the EMA on Host B becomes the primary. When a failover takes place, the Frontend performs the following actions:

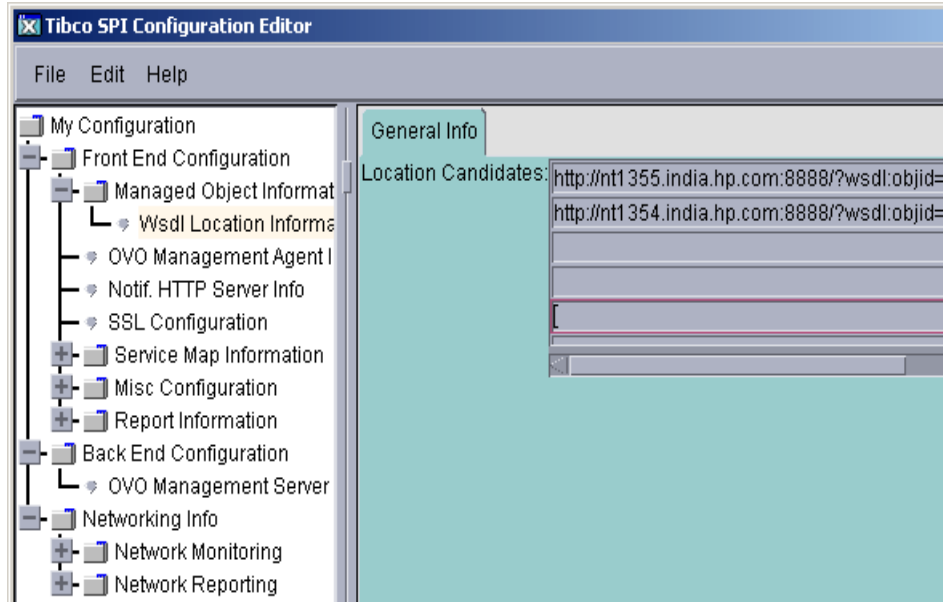
- Discards all managed object information for the EMA on Host A
- Discovers all managed objects for the EMA on Host B
- Reconstructs the service map
- Subscribes the notifications to the EMA on Host B

Adding Multiple Location Candidates

Managed object WSDL locations are configured using the TIBCO SPI Configuration Editor, which is available from the TIBCO SPI Tools group. If you want to implement failover, you must provide multiple location candidates for the same WSDL location.

To add multiple location candidates, follow these steps:

- 1 From the TIBCO SPI Configuration Editor, select **Managed Object Information** under Front End Configuration.
- 2 In the menu bar, select **Edit** → **New**.



- 3 In the Location Candidates list, add additional WSDL locations for the managed objects you want the Frontend Service to monitor.
 - ▶ If the WSDL location uses HTTPS, you must configure the Frontend Service security settings. For more information, see [Chapter 5, Security Features and Configuration](#).
- 4 Select **File** → **Save** to save your changes to the configuration file.
- 5 Select **File** → **Exit**.
- 6 In the Output of Tool window, you will see the message 'TIBCO SPI configuration completed.' It can take a few minutes for the message to appear. Do not close the Output of Tool window until you see the completion message.
- 7 Click **Close** on the Output of Tool window.

5 Security Features and Configuration

This chapter provides instructions for securing the management channels that are used by the TIBCO SPI. Knowledge of SSL and HTTPS security principals are required to complete some of the instructions in this chapter.

The TIBCO SPI security features are used to prevent unauthorized access to the TIBCO Managed Resources exposed by TIBCO EMA. This ensures that only trusted or authorized users are able to perform any actions on TIBCO Managed Resources in the managed environment. These features do not focus on data protection (data being passed to the TIBCO SPI from the TIBCO EMA as part of Event Notifications).

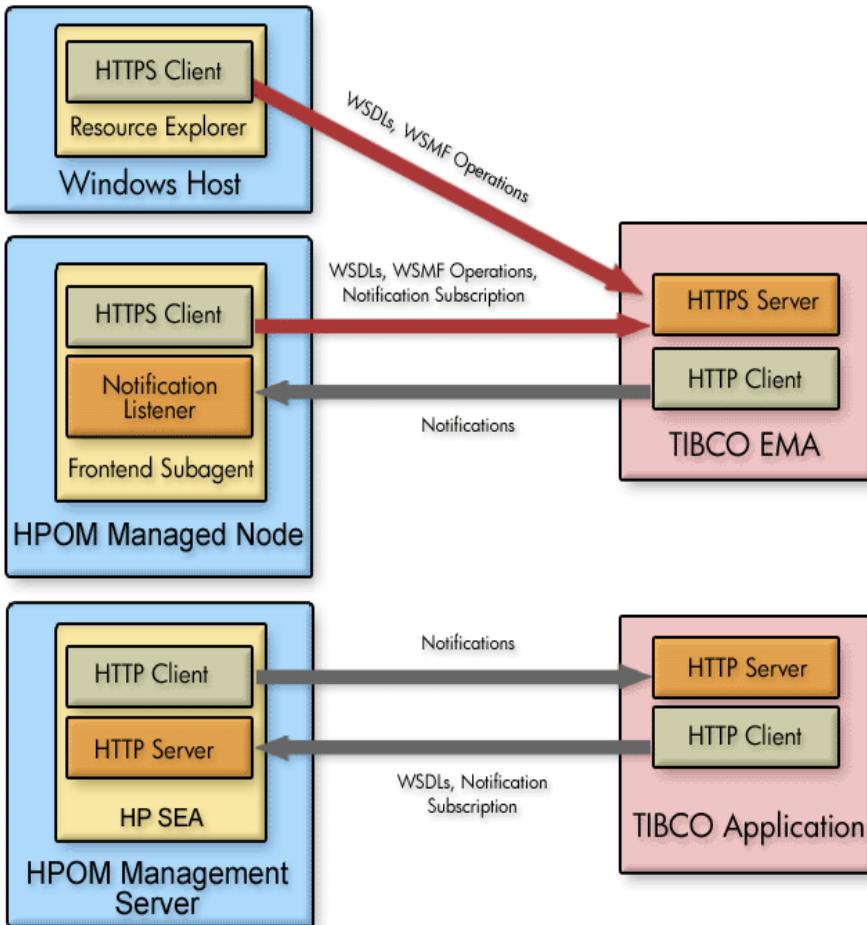
Conceptual Architecture

There are various communication channels between the TIBCO EMA and TIBCO SPI components as shown in [Figure 10](#). These communication channels are secured using HTTPS (SSL over HTTP) to ensure that the TIBCO Resources exposed by EMA are securely accessed from various components of the TIBCO SPI.

The standards supported for HTTPS include the following:

- X.509v3 for the certificate format
- SSLv3/TLS1.0
- Cipher suites available from JDK 1.6 JSSE library

Figure 10 Communication Channel Security



Securing TIBCO Resources

As shown in [Figure 10](#), HTTPS is used to secure the TIBCO resources and any operations exposed to these managed resources through the EMA WSMF channel.

Limitations

The security features of the TIBCO SPI have the following limitations:

- Notifications from TIBCO EMA are received by the Frontend Service over HTTP. The HTTPS protocol is not supported for this communication channel.
- An HPOM operator can perform all operations exposed for various Managed Resources from the Resource Explorer after successfully authenticating itself to TIBCO EMA for HTTPS communication. There is no mechanism to establish roles that enable only a specific set of operations to be accessible to a specific operator depending upon the role of the operator, or only enable access to limited set of Managed Resources.
- If the Keystore that contains the client certificate and the associated private key for the Frontend Service also contains certificates for other entities (this can be applicable for an enterprise where all the certificates used by various applications are stored in a central Keystore), then the TIBCO SPI requires that all the private keys associated with corresponding certificates are protected by the same password. Otherwise, the TIBCO SPI will not be able to recover the private key for the Frontend Service from this Keystore.

Configuring HTTPS Communication

This section provides instructions for implementing HTTPS communication for the Frontend Service and the Resource Explorer. If you do not have a Keystore or Truststore, instructions are also included for creating a Keystore and Truststore as well as importing signed certificates.

Configuring Frontend Service

Digital certificates are used for mutual authentication for HTTPS communication between the Frontend Service and TIBCO EMA. The certificate for the Frontend is stored in a Keystore. The default location of the Keystore is `/var/opt/OV/conf/tib/frontend.ks` but can be changed to a

different location. By default, the Keystore format is assumed to be `JKS` but other Keystore types can be used. See the section [Customizing HTTPS Configuration Parameters](#).

▶ TIBCO EMA uses the term `Identity File` when referring to a Keystore. The term `Keystore` in this documentation is the same as `Identity File` in the EMA documentation.

The CA's root certificate for TIBCO EMA is stored in the JDK Truststore. The default location of the Truststore is `/$JAVA_HOME/jre/lib/security/cacerts` but can be changed to some other location.

Configuring SSL/HTTPS

To configure SSL/HTTPS for TIBCO SPI Frontend, follow these steps:

- 1 Start the TIBCO SPI Configuration Editor.
- 2 Under the Frontend Configuration node on the left panel, click **SSL Configuration**
- 3 On the right panel, type the following information:
 - **Keystore Location:** The full path to a Keystore file. The Keystore contains the client certificate for the Frontend Service. The path is set by default to the following:

```
/var/opt/OV/conf/tib/frontend.ks
```

▶ The Keystore does not exist, but needs to be created using a tool described in the [Setting up a Keystore and Truststore for Frontend Service](#) section. If you have an existing Keystore, type the path to your existing Keystore. When using an existing Keystore, the Frontend Service certificate must be imported into the Keystore.

- **Keystore Password:** The password to access the Keystore.
 - **Private Key Password:** The password used to protect the private key.
 - **TrustStore Location:** The file path to the TrustStore. The default path is set to `/$JAVA_HOME/jre/lib/security/cacerts`.
- 4 Select **File** → **Save**.

- 5 Select **File** → **Exit**.

Setting up a Keystore and Truststore for Frontend Service

HTTPS communication for the Frontend Service requires the use of a Keystore and Truststore as well as a signed certificate. The setup is typically completed in the following manner:

- Obtain (from your preferred Certificate Authority) a client side certificate for the Frontend Service.
- Import this certificate to the Frontend Service Keystore.
- Import the certificate of the CA who issued the TIBCO EMA certificate to the Frontend Service Truststore if it does not already exist in the Truststore. You can get the list of all the CA certificates that are already imported to the Truststore by running the following command:

```
keytool -list -v -keystore <full path to Truststore file>  
-storepass <truststorepassword>
```

If you have your own key management tool to create public key-private key pair and import certificates to an existing Keystore, then follow your procedure to obtain a client certificate for the Frontend Service and import it to the Frontend Service's Keystore. In addition, obtain the CA certificate of the issuer of the TIBCO EMA certificate and import it to the Frontend Service's Truststore. You will have to specify the alias name and the Keystore type used for the TIBCO SPI Frontend. For more information, see [Customizing HTTPS Configuration Parameters](#).

If the Frontend Service Keystore does not exist or you do not have your own tool for managing Keystores, the following section provides instructions for creating a Keystore, getting a certificate, and importing certificates to the Keystore and Truststore.

Creating a Keystore and Importing Certificates

A utility is provided that facilitates creating a Keystore and importing client-side certificates. The utility is typically used when you do not have an existing Keystore to use for the Frontend Service.

The utility is the same as the Java Keytool, but uses the information that is stored in `WCConfig.xml` (Keystore location, Keystore password, private key password and trust store location etc.) and will use the default information specified in the Frontend, properties file (For example: aliasname, keystore type) while generating a key and importing certificates.

To create a Keystore and import certificates, follow these steps:

- 1 From a command prompt, change directories to `/opt/OV/bin`.
- 2 Type the following command:

```
./tib-perl tib-keymgrutil -genkey -dname "<distinguished name>" [-keyalg <keyalg>] [-sigalg <sigalg>] [-keysize <keysize>]
```

- **dname**: This argument is entered in the form `CN=<your name / hostname> OU=<org unit> O=<organization> L=<locality / city> ST=<state / province> C=<two letter country code>`.
- **keyalg** (optional): The key algorithm to be used. If this argument is not specified, the default key algorithm is DSA.
- **sigalg** (optional): The digital signature algorithm to be used. If this argument is not specified, the default signature algorithm is SHA1withDSA if the key algorithm is DSA and MD5withRSA if the key algorithm is RSA.
- **keysize** (optional): if this argument is not specified, the default key size is 1024 bits.

For example:

```
./tib-perl tib-keymgrutil -genkey -dname "CN=tibfrontend OU=OV O=HP L=Location ST=AB C=CD"
```

This will create the `frontend.ks` (if that is the name specified for the Keystore) which contains the private key and the self signed certificate for Frontend Service.

- 3 Create a certificate-signing request into the specified CSR file.

```
./tib-perl tib-keymgrutil -certreq -file <csr_file> [-sigalg <sigalg>]
```

- 4 Send the CSR file (typically emailed) to a CA, and save the reply from CA in some file `<client_cert_file>`. This file contains your client certificate.
- 5 Import the client certificate to the Truststore:

```
./tib-perl tib-keymgrutil -importcerts -clientcert  
<client_cert_file> -rootCA <root_cert_file> [-trustcert  
<trust_cert_file>]
```

- **clientcert**: This argument is the file returned from the CA for the Frontend Service's certificate, which can be a single certificate in X.509 format or a certificate chain in PKCS7 format. This argument imports the reply into the Keystore as specified during the SSL Configuration.
- **rootCA**: This argument is optional depending on the format of the client certificate.

This argument is required if the certificate reply is in X.509 format. In this case, you must import the Root Certificate of the CA who issued the Client certificate for the Frontend Service into the Keystore. This argument is the file that contains the Root Certificate of the CA

This argument is not required if the client cert is returned by the certificate authority in the PKCS7 format.

- **trustcert**: This argument is the certificate of the CA that issued the server certificate of TIBCO EMA. If the truststore that the user specified already has the CA certificate of the issuer of the TIBCO EMA certificate, this option is not required. Otherwise, the CA certificate included in *<trust_cert_file>* will be imported to the Truststore specified during SSL Configuration. If the specified Truststore does not exist already, it will be created with a password `changeit`.

Configuring Resource Explorer

As mentioned in the Overview section, the communication channel between the Resource Explorer and the TIBCO EMA can be secured using HTTPS. It is recommended that you reuse the Frontend Service client certificate as your Resource Explorer client certificate so that you do not need to maintain a separate client certificate for the Resource Explorer. However, a section for creating a separate client certificate for the Resource Explorer is also provided in this section.

Using Frontend Service Client Certificate

To use the Frontend Service client certificate for the Resource explorer, follow these steps:

- 1 Copy the Keystore file from the Frontend Service machine to the Resource Explorer machine and rename the Keystore file if required.



If you have an existing Keystore on the Resource Explorer machine which you want to use, you can import the client certificate you obtained for the Frontend Service into this existing Keystore using your preferred key management tool.

- 2 Stop the Resource Explorer if it is currently started.
- 3 Using a text editor, open the Resource Explorer script located at
`%RE_HOME%\hp_resource_explorer\hp_resource_explorer.bat`.

In the script, specify the Keystore and Truststore locations for the Resource Explorer as JVM system parameters. The defaults are set to the security directory under the directory `%JAVA_HOME%` as follows:

set:

```
JVM_ARGS=%JVM_ARGS%-Ddeployment.user.certs=%JAVA_HOME%\
jre\lib\security\client_certs
```

The `-Ddeployment.user.certs` argument refers to the full path to the Keystore file.

set:

```
JVM_ARGS=%JVM_ARGS%-Ddeployment.system.certs=%JAVA_HOME%\
jre\lib\security\cacerts
```

the `-Ddeployment.system.certs` argument refers to the full path to the Truststore file.

In addition, the file `%JAVA_HOME%\jre\lib\security\client_certs` does not exist and needs to be created using some key management tool.



You will also have to set or change these values in the security dialog when the Resource Explorer starts.

- 4 **Save** and **Close** the Resource Explorer script.
- 5 **Start** the Resource Explorer.

Using a Separate Client Certificate for the Resource Explorer

If you do not want to use the Frontend Service client certificate for the Resource Explorer, you can use a separate client certificate for the Resource Explorer. It is assumed that you are using your own key management tool to perform these steps.

To use a separate client certificate for the Resource Explorer:

- 1 Obtain a client certificate for the Resource Explorer from your preferred Certificate Authority.
- 2 Import the client certificate for the Resource Explorer into the Keystore on the Resource Explorer machine. The Keystore file should be located at the location specified in the `hp_resource_explorer.bat` file as explained in the previous section.
- 3 Import the certificate of the CA who issued the TIBCO EMA certificate into the Truststore that is specified in the `hp_resource_explorer.bat` file as explained in the previous section. This step needs to be performed only if the CA certificate of the issuer of the TIBCO EMA certificate does not already exist in the Truststore. To verify if a CA certificate already exists in the Truststore, you can run the following command:

```
keytool -list -v -keystore <full path to truststore file> -  
storepass <truststorepassword>
```

Starting Resource Explorer


When the Resource Explorer starts, if the URI to the root managed object uses the HTTPS protocol (**https://...**), a security dialog appears. Type the following information:

- Password for the private key
- Keystore location
- Truststore location

Default locations of the Keystore and Truststore are shown in the dialog, modify the values as necessary.

Customizing HTTPS Configuration Parameters

The `Frontend.properties` file that is located in the `/var/opt/OV/conf/tib` directory contains the following properties for customizing various SSL/HTTPS settings:

- `com.hp.wsmf.ssl.client.aliasname = <aliasname>`
This value is set to `tibFrontEnd` by default. If you use a different alias name for the Frontend Service in your Keystore, then specify that name.
- `com.hp.wsmf.ssl.keyStoreType = <type>`
This value is set to `JKS` by default. If you are using a Keystore of different type, specify the type here.
- `com.hp.wsmf.ssl.socketTimeout = <timeout in milliseconds>`
This value is set to `120000` by default.
 If you get a Connection Timeout Socket Exception at runtime, increase this value.
- `com.hp.wsmf.certCheckWarnLevel1Days = <days>`
This value is set to `15` by default. If a certificate is found to expire within the days specified, a major severity message is sent to the HPOM console's message browser.
- `com.hp.wsmf.certCheckWarnLevel2Days = <days>`
This value is set to `30` by default. If a certificate is found to expire within the days specified, a warning severity message is sent to the HPOM console's message browser.

6 Troubleshooting

This chapter provides common troubleshooting tasks when using the TIBCO SPI. In addition, see the TIBCO SPI Release Notes for the latest information about the TIBCO SPI.

Self-Healing Info Tool

The Self-Healing Info tool gathers SPI troubleshooting data and stores it in a file that you can submit to HP support for assistance.



The file created by the Self-Healing Info tool might be hidden on some Windows managed nodes. If you do not see the file, open Windows Explorer and, from the **Tools** menu, select **Folder Options**. Click the **View** tab. Under Hidden files and folders, select **Show hidden files and folders**.

Runtime Problems

Frontend Service Does Not Stop

Problem	The Frontend Service does not stop if there is a problem canceling the subscription.
Solution	You must manually stop the Frontend Service Java processes.

Frontend Service Does Not Start

Problem	The Frontend Service does not start up.
Solution	To locate the error, look in the <code>/var/opt/OV/log/tib/frontend.log</code> file. See the Frontend Logfile Errors section later in this chapter for explanations on resolving the error.

Frontend Service is Unable to Connect to EMA

The Frontend Service can fail to connect to EMA for various reasons. Depending on the specific scenario, the Frontend logs specific message into the `frontend.log` file when it fails to connect to EMA. The following section describes the various error messages logged into `frontend.log` when Frontend Service fails to connect to EMA:

Problem	WARNING WSF-1097: Problem accessing https://<machine>.<domain name>:8888/?wsdl:objid=tibema://www.tibco.com/ema/2005/01/mo/identity/Root, WSDLException: faultCode=OTHER_ERROR: Unable to connect to server. Cause: Connection refused.
Solution	This error occurs when the EMA Gateway is down. Ensure that EMA is started successfully.

Problem	SEVERE TIBSPI-105 Fronted Startup Failed : Exception: WSF-1202: Failed to retrieve the Client Certificate for tibFrontEnd at the KeyStore <code>/var/opt/OV/conf/tib/frontend.ks</code> . Exception: Keystore was tampered with, or password was incorrect.
Solution	This error occurs when the password for the Frontend KeyStore is wrong. Verify that you have specified the correct password for the Frontend KeyStore when specifying the SSL Configuration Settings.

Problem	SEVERE TIBSPI-105 Fronted Startup Failed : Exception: WSF-12105: Failed to load the Keystore /var/opt/OV/conf/tib/frontend.ks. Exception: Cannot recover key.
Solution	This error occurs when the password for the Private Key is wrong. Verify that you have specified the correct password for the Private Key when specifying the SSL Configuration settings.

Problem	WARNING WSF-1097: Problem accessing https://<machine>.<domain name>:8888/?wsdl:objid=tibema://www.tibco.com/ema/2005/01/mo/identity/Root, WSDLException: faultCode=OTHER_ERROR: Unable to read WSDL document from 'https://<machine>.<domain name>:8888/?wsdl:objid=tibema://www.tibco.com/ema/2005/01/mo/identity/Root'.: sun.security.validator.ValidatorException: No trusted certificate found.
Solution	This warning occurs when the CA Certificate of issuer of EMA server certificate is not present in the TrustStore. Make sure you import the CA Certificate of issuer of EMA server certificate into the TrustStore that you specified in SSL Configuration Settings.

Problem	SEVERE TIBSPI-105 Fronted Startup Failed : Exception: WSF-1209: Client Certificate for tibFrontEnd has expired on Mon Feb 21 15:33:21 PST 2005. Client Certificate has to be renewed for successful SSL communication.
Solution	This error occurs when the certificate for Frontend has expired and requires to be renewed.

Problem	<p>WARNING: WSF-1097: Problem accessing https://<machine>.<domain name>:8888/?wsdl:objid=tibema://www.tibco.com/ema/2005/01/mo/identity/Root, WSDLException: faultCode=OTHER_ERROR: Unable to read WSDL document from 'https://<machine>.<domain name>:8888/?wsdl:objid=tibema://www.tibco.com/ema/2005/01/mo/identity/Root'.: java.security.cert.CertificateExpiredException: NotAfter: Fri Jan 07 16:01:27 PST 2005.</p>
Solution	<p>This warning occurs when the EMA Server Certificate has expired and requires to be renewed.</p>
Problem	<p>WARNING ><WSF-0004: Problem with push subscribe: http://<machine>.<domain name>:8888/?wsdl:objid=tibema%3A%2F%2Fwww.tibco.com%2Fema%2F2005%2F01%2Fmo%2Fidentity%2FExternalService%2FtibcoDomain%2Fovw009-C%3A%5CTibcoTestApp%5CDebugTest%5CWork; nested exception is: java.net.SocketTimeoutException: Read timed out.</p>
Solution	<p>If Frontend is connecting to TIBCO EMA using HTTP, then edit the /var/opt/OV/conf/tib/Frontend.properties file and increase the value for com.hp.wsmf.http.socketTimeout. The time specified here is in milliseconds.</p> <p>If Frontend is connecting to TIBCO EMA using HTTPS, then edit the var/opt/OV/conf/tib/Frontend.properties file and increase the value for com.hp.wsmf.ssl.socketTimeout. The time specified here is in milliseconds.</p>

TIBCO SPI Uses Backup EMA Instead of Primary EMA

Problem	On using failover, the TIBCO SPI uses the backup TIBCO EMA instance instead of the primary TIBCO EMA instance.
Solution	This occurs when the backup TIBCO EMA instance starts before the primary TIBCO EMA instance. Make sure all TIBCO EMA instances are fully started before starting the Frontend Service.

TIBCO Service is Not Visible

Problem	The TIBCO Service does not show up in the Resource Explorer.
Solution	Verify that the username used to log on to the HP Java console is the same user name that is configured as <code><OVOUserName></code> in the <code>WCConfig.xml</code> file on the Frontend Service node.

Missing Operational Notification

Problem: Operational notifications are not appearing in the HPOM message browser.

Solution: Complete the following procedures:

Verifying TIBSPI-EventService-MSG-V1 is Configured

Verify that the `TIBSPI-EventService-MSG-V1` is configured on the HPOM managed node where the Frontend Service is running.

- 1 From a window on the Frontend Service node, find out which policies are configured by running

```
ovpolicy -list
```

The list of configured policies appears.

If the `TIBSPI-EventService-MSG-V1` is in the list, you can skip the rest of the steps in this task. If you do not see the `TIBSPI-EventService-MSG-V1`, follow these steps:

- 2 In the Node Bank window, select the node where the Frontend Service is running.
- 3 Click **Assign Policy/Policy groups...** on the Action Menu. The Selector window appears.
- 4 Select **Policy Groups** from the **Locate** list and set **Name** to **Tib**. Click **Filter**.
- 5 Click **SPI for TIBCO/TIBSPI-EventService-V1**.
- 6 Click **OK**.

Deploying Policies

Deploy the policies for the Frontend node. You only need to do this if the `TIBSPI-EventService-MSG-V1` was not already configured.

- 1 In the Node Bank window, select the node where the Frontend Service is running.
- 2 Select **Deploy Configuration...** from the Actions Menu.
- 3 Select **Force Update** in the Options frame.
- 4 Click **OK**.

Verifying HPOM Messages Display in Message Browser

Verify that an HPOM test message appears in the HPOM message browser.

- 1 Launch the administrator interface on the HPOM management server and log on as **opc_adm** or **TIBSPI_Op**.
- 2 From a window on the Frontend Service node, send a test message by running

```
opcmsg severity=minor application=test object=test  
msg_text="my test" msg_grp=TIBCO
```

- 3 A message with minor severity will appear in the HPOM message browser. If a message does not appear, follow the steps in the section [Verifying Credentials](#).

Verifying TIBCO EMA Agent is Sending Notifications

Verify that the TIBCO EMA Agent is sending the notification to the Frontend Service.

- 1 Turn debugging on for the EMA Agent. On the system where the EMA Agent is installed:
 - a Modify the `<EMAAgentDir>/config/config.xml` file. Uncomment `<role>debugRole</role>` at the end of the file.
 - b Restart the EMA Agent.
- 2 Either wait for the Frontend Service to detect that the EMA Agent has restarted or restart the Frontend Service.
- 3 After the Frontend Service has restarted, create the operational notification. For example, if you are trying to see the status of an adapter reflected in the service map, stop the adapter if it is already running.
- 4 Look in the `<EMAAgentDir>/logs/emaagent.log` file. The following output appears:

```
2004 Feb 11 10:19:28:174 GMT -8 Info [Application] EMA-35411
The status of Managed Object 'tibema://www.tibco.com/ema/
2005/01/mo/identity/ServiceInstance/tibttest2/
DefaultDeployment/Spot' changed from 'http://schemas.hp.com/
wsmf/2003/03/Foundation/Status/Operational' to 'http://
schemas.hp.com/wsmf/2003/03/Foundation/Status/Inactive'
```

Verifying Frontend Service Receives Notifications

If the TIBCO EMA Agent is sending the notifications, we need to verify that the Frontend Service is receiving the notification.

- 1 Stop the Frontend Service.
- 2 Run the Frontend in a command window. Change the directory to `/opt/OV/bin`. On the system where the Frontend is installed, run the following command:

```
./tib-perl tib-start-frontend
```

The output is written to `stdout`. Wait until you see the message: Service map created.

- 3 Generate the operational notification. For example, start or stop an adapter.
- 4 The message 'Received an operation notification' is printed to stdout along with the information sent to opcmsg. For example, if the sample Spot application is started, the following is printed:

Received an operation notification

```
opcmsg:
object=Spot
msg_grp=TIBCO
service_id=<some wsdl>
severity=Normal

msg_text=Status Change from http://schemas.hp.com/wsmf/2003/
03/Foundation/Status/Inactive to http://schemas.hp.com/wsmf/
2003/03/Foundation/Status/Operational

node=<some node>

application=ServiceInstance/Custom

-option
WSMF_EVENT_TYPE=http://www.tibco.com/ema/2005/01/event/
StatusChange

-option MSG_CORR_ID=tibema://www.tibco.com/ema/2005/01/mo/
identity/
ServiceInstance/tibtest2/DefaultDeployment/Spot
```

Verifying Resource Host Name

The node must be in the Node Bank and in the TIBSPI-External or TIBSPI-UNIX node group.



The node value must be an exact match to the Hostname for the node in the Node Bank. The node cannot be an IP address and it must be accessible through DNS. Do not put the host name in the `/etc/hosts` file. The name needs to be in the DNS tables.

To verify the Resource host name, follow these steps:

- 1 In the Node Group Bank window, click the **TIBSPI-External** node group.
- 2 If the node is in the TIBSPI-External node group window, close the window and skip the following steps.
- 3 If the node is not in the TIBSPI-External node group window, go back to the Node group window.
- 4 Click the **TIBSPI-UNIX** node group.
- 5 If the node is not in the TIBSPI-UNIX node group, add it to either the TIBSPI-UNIX or TIBSPI-External node group.

Verifying Source Object

The source object which is entered as the *service_id* value in the Frontend output must be one of the objects that the Frontend Service recognizes.

- 1 Start the HPOM console.
- 2 Click the **+** icon in front of the services until you get to the service that represents the object that is the *service_id* value
- 3 Right-click the service and select **Properties** from the popup menu.
- 4 In the Services Properties [XXX] dialog box, the value in the Name field must be an exact match to the *service_id* value.
- 5 Click **Close** to close the dialog box.

Verifying Credentials

The HPOM operator that you are logged on as is able to see messages in the TIBCO message group. We assume for this example that the HPOM operator is `opc_adm`.

- 1 Click **All Users**. Select **opc_adm** and select **Edit** from the Action Menu.
- 2 In the Modify User: `opc_adm` window, click **Profiles**.
- 3 In the Profiles of User: `opc_adm` window, verify that the TIBSPI User Profile icon appears. If it does not appear, follow these steps listed:
 - a Open User Profile Bank window by selecting **Window** → **User Profile Bank**.

- b Drag the TIBSPI User Profile from the VPO User Profile Bank window and drop it into the Profiles of User: opc_adm window.
 - c Close the VPO User Profile Bank window.
- 4 Close the Profiles of user: opc_adm window.
 - 5 In the Modify User: opc_adm window, click **OK**.
 - 6 Restart the session. From any HPOM window, select **Map** → **Restart Session**.
 - 7 In the HP Operations Windows WARNING dialog, click **OK**.

Verify Communication with HPOM Management Server

If the Frontend is receiving the notification, you need to check if there are communication problems between the Frontend node and the HPOM management server. To do this, you need to turn on the HPOM message tracing.



See the HPOM documentation for instructions on enabling HPOM message tracing.

- 1 On the HPOM management server, add `OPC_TRACE TRUE` and `OPC_TRACE_AREA MSG` to the `/opt/OV/bin/OpC/install/opcsvinfo` file. Your file should look similar to:

```
OPC_INSTALLED_VERSION A.07.10
OPC_MGMT_SERVER <machine>.<domain name>
OPC_MGMTSV_CHARSET iso885915
OPC_INSTALLATION_TIME 03/25/03 15:28:11
OPC_SG FALSE
OPC_TRACE TRUE
OPC_TRACE_AREA MSG
```

- 2 Run `/opt/OV/bin/OpC/opcsv -trace`. The trace information is written to `/var/opt/OV/share/tmp/OpC/mgmt_sv/trace`.
- 3 Run `tail -f /var/opt/OV/share/tmp/OpC/mgmt_sv/trace` to see the trace messages as they are written.

- 4 On the Frontend node, add `OPC_TRACE TRUE` and `OPC_TRACE_AREA MSG` to the `/opt/OV/bin/OpC/install/opcinfo` file.
- 5 Run `/opt/OV/bin/OpC/opcagt -trace`. The trace information is written to `/var/opt/OV/tmp/OpC/trace`.
- 6 Run `tail -f /var/opt/OV/tmp/OpC/trace` to see the trace messages as they are written.
- 7 Send a notification. For example, you can start or stop the TIBCO Spot sample application. In the HP Operations agent trace file (`/var/opt/OV/tmp/OpC/trace`), you should see some messages similar to:

```
02/11 12:18:20.517 opcmsg(9930:001) [MSG]: Queueing message:
TIBCO 'Status Change from h'
```

```
02/11 12:18:20.523 opcmsgi(1791:001) [MSG]: Sending message:
6f732be6-5ccf-71d8-0be9-0ff414390000 TIBCO 'Status Change
from h' 15.244.60.103
```

```
02/11 12:18:20.534 opcmsga(1778:001) [MSG]: Message/Act.Resp.
received from agents: 6f732be6-5ccf-71d8-0be9-0ff414390000
TIBCO 'Status Change from h' 15.244.60.103
```

```
02/11 12:18:20.535 opcmsga(1778:001) [MSG]: OpC mgr for msg:
6f732be6-5ccf-71d8-0be9-0ff414390000 TIBCO 'Status Change
from h' 15.244.60.103  opcmgr : <machine>.<domain name>
15.244.20.57
```

```
02/11 12:18:20.535 opcmsga(1778:001) [MSG]: forwarding msg:
6f732be6-5ccf-71d8-0be9-0ff414390000 TIBCO 'Status Change
from h' 15.244.60.103  opcmgr : <machine>.<domain name>
15.244.20.57
```

```
02/11 12:18:20.538 opcmsga(1778:001) [MSG]: Sending msg (len =
554): Status Change from http://schemas.hp.com/wsmf/2003/03/
Founda
```

```
02/11 12:18:20.543 opcmsga(1778:001) [MSG]: Message forwarded:
6f732be6-5ccf-71d8-0be9-0ff414390000 TIBCO 'Status Change
from h' 15.244.60.103  opcmgr : <machine>.<domain name>
15.244.20.57
```

In the OVO management server trace file (`/var/opt/OV/share/tmp/OpC/mgmt_sv/trace`), you should see some messages similar to:

```
02/11 12:18:20.542 opcmsgrd(1595:02f) [MSG]: Message
received: 6f732be6-5ccf-71d8-0be9-0ff414390000 TIBCO
'Status Change from h' 15.244.60.103
```

```
02/11 12:18:20.543 opcmsgm(1611:001) [MSG]: Message
received from message receiver:
6f732be6-5ccf-71d8-0be9-0ff414390000 TIBCO 'Status Change
from h' 15.244.60.103
```

```
02/11 12:18:20.552 opcmsgm(1611:001) [MSG]: Message
processing: ip_addr=15.244.60.103 (mapped),
node_name='<machine>.<domain name>'
```

```
02/11 12:18:20.552 opcmsgm(1611:001) [MSG]: csm_db_msg_add
called with msg 6f732be6-5ccf-71d8-0be9-0ff414390000.
```

```
02/11 12:18:20.592 opcmsgm(1611:001) [MSG]: csm_db_msg_add
finished for msg 6f732be6-5ccf-71d8-0be9-0ff414390000.
Last err: 0-0
```

```
02/11 12:18:20.593 opcmsgm(1611:001) [MSG]: Message
forwarded to DM: 6f732be6-5ccf-71d8-0be9-0ff414390000
TIBCO 'Status Change from h' 15.244.60.103
```

- 8 **Change the state of tracing from off to on the HPOM management server by modifying OPC_TRACE to FALSE in the /opt/OV/bin/OpC/install/opcsvinfo file.**
- 9 **Run /opt/OV/bin/OpC/opcsv -trace.**
- 10 **On the Frontend node, turn tracing off by setting OPC_TRACE to FALSE in the /opt/OV/bin/OpC/install/opcinfo file.**
- 11 **Run /opt/OV/bin/OpC/opcagt -trace.**

Cleanup HPOM Message Queues

If you do not see the above trace messages, the HPOM message queues may be corrupt. In this case, follow these steps:

- 1 **Stop opcagt by running `opcagt -kill`.**
- 2 **Remove the temporary files by running `rm -f /var/opt/OV/tmp/OpC/*`.**
- 3 **Restart the opcagt by running `opcagt -start`.**
- 4 **Close all HPOM interfaces.**

- 5 Stop the HPOM management server by running `ovstop opc ovoacomm`.
- 6 Remove the temporary files by running `rm -f /var/opt/OV/share/tmp/OpC/mgmt_sv/*`
- 7 Restart the HPOM management server processes by running `opcsv -start`.

Performance Agent Does Not Start Up

Problem	When you run <code>opcagt -start -id 12</code> and <code>opcagt -status</code> the output shows that the Performance Agent is not running.
Solution	Verify that Embedded Performance Component (CODA) is not running by running <code>ps -ef grep coda</code> . If Embedded Performance Component (CODA) is running it means Embedded Performance Component (CODA) was either started up standalone, or the HPOM control agent has stopped, was restarted and is longer the parent. If Embedded Performance Component (CODA) is not running, look in the <code><OVAgentDataDir>/log/coda.log</code> file for any error messages.

TIBCO SPI Fails to Detect HP Performance Agent

Problem	The TIBCO SPI fails to detect the HP Performance Agent even though HP Performance Agent is running on the system.
Solution	Make sure the <code>systemsMWA.txt</code> file is located in <code>/var/opt/OV/conf/perf</code> directory. If not, you must copy <code>systemsMWA.txt</code> from its existing directory to <code>/var/opt/OV/conf/perf</code> . HP Performance Manager should than detect HP Performance Agent.

Configure TIBCO SPI Tool Errors

Configure TIBCO SPI Tool Does Not Start

Problem	The Configure TIBCO SPI tool does not start.
Solution	Delete <code>/var/opt/OV/conf/tib/appconfig.xml.ser</code> and restart the configuration tool.

Configure TIBCO SPI Tool Does Not Display Content

Problem	The Configure TIBCO SPI tool starts, but no content appears.
Solution	Delete <code>/var/opt/OV/conf/tib/appconfig.xml.ser</code> and restart the configuration tool. Open the file in your text editor and make sure to save it in UTF-8 encoding. If your editor does not have a save as option to do this and uses system default encoding, then make sure you set your session's LANG variable to UTF-8.

Configure TIBCO SPI Tool Fails to Transfer WCCConfig.xml

Problem	When you run the Configure TIBCO SPI tool, the Output of tool window has the following message: 'Error by transfer file from <code>/var/opt/OV/conf/tib/WCCConfig.xml</code> to <code>/var/opt/OV/conf/tib/WCCConfig.xml</code> (OpC40-745)'
Solution	There was a problem transferring the <code>WCCConfig.xml</code> file from the HPOM management server to the Frontend Service node. You need to manually transfer the file and restart the Backend service and Frontend Service as follows: <ol style="list-style-type: none">1 Ftp the <code>/var/opt/OV/conf/tib/WCCConfig.xml</code> file from the HPOM management server to <code>/var/opt/OV/conf/tib</code> on the Frontend Service node.2 Run Restart TIBCO SPI tool.

Configure TIBCO SPI Tool Throws AWTException

Problem	<p>When you close the Configure TIBCO SPI tool, you get the following exception in the tool Output window:</p> <pre>java.awt.AWTException: cannot open XIM</pre>
Solution	<p>By default, you cannot type Asian (Japanese, Chinese, Korean) characters into the Configure TIBCO SPI tool. To type Asian characters in a Java interface an input method is required. This input method can be a pure Java input method (independent of OS) or an input method provided by the OS. An input method is installed with Java 1.6. The Configure TIBCO SPI is a Java interface. Therefore, you need to modify the <code>JAVA_HOME</code> variable in the <code>/var/opt/OV/bin/OpC/cmds/tib_config</code> script on the HPOM server system to a JVM on the system that is configured to display Asian characters.</p>

Frontend Logfile Errors

The Frontend Service log file is located in `/var/opt/OV/log/tib/frontend.log`.

Error Starting Notification HTTP Server

Problem	NotifMgr: Error: Problem starting notification HTTP server. Please make sure port is not already in use: XXXX.
Solution	<p>Check to see if the Frontend is already running:</p> <p>If the following message appears, it indicates that the Frontend is already running.</p> <pre>TIBSPI Backend is running... TIBSPI Frontend is running...</pre> <p>If the following message appears:</p> <pre>TIBSPI Frontend is NOT running...</pre> <p>it indicates that the Frontend is not running, but the Frontend Java process might not have stopped. Wait for few minutes for the port to be released and try to start TIBCO SPI again.</p>

Error Adding Service to Map

Problem	Problem adding services to map: Connection refused to host: XXX; nested exception is: java.net.ConnectException: Connection refused
Solution	Use TIBCO SPI status tool to verify the status of TIBCO SPI and install the Backend if the service is down.

Frontend does not Connect to the Backend

Problem	Frontend is not able to connect to the Backend.
Solution	<p>This message appears just after installing the Frontend Service if the TIBCO SPI has not been configured yet or the Backend Service is not started.</p> <p>Make sure that you configure the SPI using the <code>Configure TIBCO SPI</code> tool located in the Tool Bank. See Chapter 2 for complete instructions.</p> <p>After the configuration is complete, use the <code>Start TIBCO SPI</code> tool located in the Tool Bank.</p>

Problem Logging Metric Data

Problem	WSF-0009: ddflog returned an error logging TIBSPI_RPT_METRICS:256
Solution	<p>This error can occur when the data sources for the TIBCO SPI metrics are not registered successfully. Make sure you register the TIBCO SPI Metric data sources by running the following commands on the Frontend Service machine:</p> <pre>cd /opt/OV/bin ./tib-perl tib-create-datasources.</pre>

7 Removing TIBCO SPI

To remove TIBCO SPI, complete the following procedures in the order in which they are listed.

Stopping TIBCO SPI

Run **Stop TIBCO SPI** tool to stop the Frontend and Backend services. Follow these steps:

- 1 On the Administration interface, click **Integrations** → **HPOM for UNIX UI**.
- 2 Log on with **opc_admin** credentials.
- 3 Click **Nodes**. Right-click the selected node. Select **Start** → **Stop TIBCO SPI**.
The TIBCO SPI is successfully stopped.

Removing Frontend Service

Run **frontend un-installation** tool to remove the Frontend service. Follow these steps:

- 1 On the Administration interface, click **Integrations** → **HPOM for UNIX UI**.
- 2 Log on with **opc_admin** credentials.
- 3 Click **Nodes**. Right-click the selected node. Select **Start** → **frontend un-installation**.

The Frontend Service is successfully removed.

Removing TIBCO SPI Software from Management Server

You can use one of the following ways to remove TIBCO SPI from the HP UX, Solaris, and Linux management server as follows:

- Graphical User Interface
- Command Line Interface

Removing TIBCO SPI using Graphical User Interface

To remove the TIBCO SPI through the Graphical User Interface from the HP-UX, Linux, or Solaris Management Server, using X-Windows client software, follow these steps:

- 1 Log on as a **root** user.
- 2 Insert the HP Operations Smart Plug-ins DVD into the DVD drive of the HP-UX, Linux, or Solaris management server. Mount the DVD if necessary.
- 3 Start the X-windows client software and export the DISPLAY variable by typing the following command:

```
export DISPLAY=<ip address>:0.0
```

- 4 To start the removal of TIBCO SPI, type one of the following commands, according to your management server:

```
./HP_Operations_Smart_Plug-ins_Hpux_setup.bin
```

or

```
./HP_Operations_Smart_Plug-ins_Linux_setup.bin
```

or

```
./HP_Operations_Smart_Plug-ins_Solaris_setup.bin
```

The initialization window appears.

- 5 Click **OK**. The Pre-uninstall Summary window appears.
- 6 Click **Un-install**. The Uninstalling window appears.
- 7 Click **Done** to complete the removal of the SPI.

Removing TIBCO SPI using Command Line Interface

To remove the TIBCO SPI through the Command Line Interface, follow these steps, :

- 1 Log on as a **root** user.
- 2 Insert the HP Operations Smart Plug-ins DVD into the DVD drive of the HP-UX, Linux, or Solaris management server. Mount the DVD if necessary.
- 3 To start the removal of the SPI, type one of the following commands, according to your management server:

```
./HP_Operations_Smart_Plug-ins_Hpux_setup.bin -i console
```

or

```
./HP_Operations_Smart_Plug-ins_Linux_setup.bin -i console
```

or

```
./HP_Operations_Smart_Plug-ins_Solaris_setup.bin -i  
console
```

The HP Software Installer content appears.

- 4 Press **Enter** to continue. The Maintenance Selection screen appears.
- 5 Press the appropriate option (number) to start the removal of the SPI.




When you have two SPIs installed on HP-UX, Linux, or Solaris management server and you want to remove one SPI out of the two installed SPIs, select Modify (1) option and then the SPI you want to retain. Do not select the SPI which you want to remove.

- 6 Press **Enter** to continue. When the removal is complete, you will receive a message which states that the removal is completed successfully.


Removing TIBCO SPI Message Groups

To remove TIBCO SPI Message groups, follow these steps:

- 1 From the Administration interface, open All Message Groups window.
- 2 Select the check boxes corresponding to TIBCO and TIBCO SPI message groups.
- 3 Select **Delete...** from the **Choose an Action** list and click  to submit.
The TIBCO SPI message groups are deleted.


Removing TIBCO SPI Tools Group

To remove the TIBCO SPI Tools group, follow these steps:

- 1 From the Administrative interface, open the All Tool groups window.
- 2 Select the tool groups check box.
- 3 Select **Delete** from the **Choose an Action** list and click  to submit.
The TIBCO SPI tool groups are deleted.


Removing TIBCO SPI User Profile

To remove the TIBCO SPI User profile, follow these steps:

- 1 From the Administration interface, open the All User Profiles window.
- 2 Select the User Profile check box.
- 3 Select **Delete** from the **Choose an Action** list and click  to submit.
The TIBCO SPI user profiles are deleted.


Removing TIBCO SPI Policy Groups

To remove the TIBCO SPI policy groups, follow these steps:

- 1 From the Administration interface, open the All Message Groups window.
- 2 Select the check boxes corresponding to the TIBCO and TIBCO policy groups.
- 3 Select **Delete** from the **Choose an Action** list and click  to submit.
The TIBCO SPI policy groups are deleted.

Removing TIBCO SPI Node Groups From the HPOM Database

To remove the TIBCO SPI node groups, follow these steps:

- 1 From the Administration interface, open the All Node Groups window.
- 2 Select the check boxes corresponding to the node groups.
- 3 Select **Delete** from the **Choose an Action** list and click  to submit.
The TIBCO SPI node groups are deleted.

Removing HP Report Package (Optional)

If you have installed TIBCO SPI Report package on your system running HP Reporter, remove it by following these steps:

- 1 On the Windows system running HP Reporter, from the Control Panel, double-click **Add/Remove Programs**.
- 2 Select TIBCO SPI report package and click **Remove**. The HP Reporter package is successfully removed. The HP Report Package is successfully removed.

A TIBCO SPI Configuration Parameters

This appendix is a reference for the TIBCO SPI configuration parameters. In particular, this appendix focuses on the `WCConfig.xml` configuration file. The parameters are discussed throughout this guide; however, they are listed here in a reference style so they can be easily accessed.

Editing `WCConfig.xml`

The `WCConfig.xml` file is located in `/var/opt/OV/conf/tib/` on the system running the TIBCO SPI Front-End Service. The `WCConfig.xml` file is structured using XML. You can edit this file using the SPI's configuration tool, or you can manually edit this file using an XML or text editor. If you chose to manually edit `WCConfig.xml`, you must restart the Front-End Service before the changes take effect.

Editing Configuration Parameters Using Configure TIBCO SPI Tool

To edit parameters, follow these steps:

- 1 On the Tool Group window, select **Configure TIBCO SPI** tool.
- 2 Select **Edit** from the Action Menu. Click **OM Tool**.
- 3 Edit the value of the parameters.
- 4 Click **Save**.

WCConfig.xml Configuration Parameters

The `WCConfig.xml` configuration file contains parameters that configure the Backend Service, Frontend Service. The root element of the configuration file is `<WcConfiguration>`. All elements must be children within the root element.

<FrontendSection>

This node contains parameters that are used to configure the Frontend Service. It contains six child nodes:

- `<ManagedObjectInfo>`
- `<OVOMgmtAgentInfo>`
- `<NotifHttpServerInfo>`
- `<ServiceMapInfo>`
- `<Miscellaneous>`
- `<ReportInfo>`

FrontendSection/ManagedObjectInfo

This element contains a list of WSDL locations that you want the Frontend Service to monitor. For each MO you want the Frontend Service to monitor, add the MO's WSDL location. You only need to add the 'root' MOs' WSDL locations because the Frontend Service recursively discovers the children. It retrieves information for the children that are related to the parent MO by the relation configured in the Relations to Use list on the Service Map Information area. By default, all children that are related to the parent MO by **`http://schemas.hp.com/wsmf/2003/02/Relations/Contains`** and **`http://schemas.hp.com/wsmf/2003/03/Relations/DependsOn`** types are discovered. You can add more entries to the Relations to Use list but you need to be careful about circular dependencies.



The MOs configured in the Managed Object Information list must be accessible before starting up the Frontend Service.

FrontendSection/ManagedObjectInfo/WsdllLocation

MO's WSDL location.

FrontendSection/OVOMgmtAgentInfo

Parameters for the Frontend Service

FrontendSection/OVOMgmtAgentInfo/HostName

The Frontend Service system's host name.

FrontendSection/OVOMgmtAgentInfo/JavaHome

The location of JAVA_HOME on Frontend Service system.

FrontendSection/OVOMgmtAgentInfo/RmiPort

The Frontend Service RMI port number.

FrontendSection/OVOMgmtAgentInfo/AgentType

The Frontend Service system type. Choices are: UNIX or Windows. (Windows is not implemented yet.)

FrontendSection/NotifHttpServerInfo

Configures the HTTP server in the Frontend Service to receive WSMF notifications

FrontendSection/HTTPPort

The HTTP server's port number that receives WSMF notifications

FrontendSection/Service MapInfo

This node contains parameters that enable you to configure the Service Map

FrontendSection/Service MapInfo/ActionsToBeIgnored

The Service Map will ignore actions that are listed in this node.

FrontendSection/Service MapInfo/ActionsToBeIgnored/Action

This node contains parameters for specifying which actions will be ignored.

**FrontendSection/Service MapInfo/ActionsToBeIgnored/Action/
ActionName**

The name of the action to be ignored

**FrontendSection/Service MapInfo/ActionsToBeIgnored/Action/
NamespaceURI**

Namespace of the action to be ignored

FrontendSection/Service MapInfo/RelationsToBeUsed

List of relations that are used by the Frontend Service to recursively discover children MOs.

FrontendSection/Service MapInfo/RelationsToBeUsed/Relation

Relation to use in discovery

FrontendSection/Service MapInfo/OVOUserForServiceMap

List of HPOM users that can view the TIBCO service.

**FrontendSection/Service MapInfo/OVOUserForServiceMap/
OVOUserName**

HPOM user name to associate with TIBCO service

FrontendSection/Service MapInfo/ServiceAliasMap

List of service names associated with TIBSPI that can be substituted with another service name. For example if there is a DB service node as part of DB SPI, the TIBSPI node connected to this DB can use the same service name as the DB service node.

FrontendSection/Service MapInfo/ServiceAliasMap/AliasInfo

**FrontendSection/Service MapInfo/ServiceAliasMap/AliasInfo/
ServiceName**

Service Name of the TIBSPI.

**FrontendSection/Service MapInfo/ServiceAliasMap/AliasInfo/
AliasName**

The service name to be replaced with this name.

**FrontendSection/Service MapInfo/ServiceAliasMap/AliasInfo/
AliasLabel**

The service label of SPIs (such as DB SPI, OS SPI, SAP SPI) which integrate with TIBCO SPI. The label can be found by clicking the properties on the service icon for a SPI in the Java console's Service Navigator.

FrontendSection/Service MapInfo/ServiceIconMap

This node contains parameters for defining icons for MO types.

FrontendSection/Service MapInfo/ServiceIconMap/ServiceIcon

List of icon/MO type. Displays the specified icon in the service map for an MO of the specified type

**FrontendSection/Service MapInfo/ServiceIconMap/ServiceIcon/
ServiceType**

MO type

**FrontendSection/Service MapInfo/ServiceIconMap/ServiceIcon/
IconFile**

Fully qualified name of the icon file

FrontendSection/miscellaneous/

This node is for miscellaneous parameters.

FrontendSection/miscellaneous/ManagedObjectsToBeIgnored/

This node enables you to list of MO types that you want to ignore. These MO types are not discovered and therefore will not appear in the service map.

FrontendSection/miscellaneous/ManagedObjectsToBeIgnored/

ManagedObjectType

MO type to ignore

FrontendSection/miscellaneous/RootServiceName

The root of the MO hierarchy

FrontendSection/ReportInfo

This node enables you to specify a user friendly name for MOs.

FrontendSection/ReportInfo/ReportGroupInfo

For each MO that you are collecting data, you can define a user friendly name that appears on the graphs and reports to identify the MO. The name is also used as the name of the file where data is logged for graphs before it is sent to the Performance Agent. Therefore, the name needs to be a valid file name.

FrontendSection/ReportInfo/ReportGroupInfo/ReportGroupObjectID

MO's WSDL location that data is being collected for

FrontendSection/ReportInfo/ReportGroupInfo/ReportGroupName

User friendly name of MO

<BackendSection>

This node contains parameters that are used to configure the Backend Service. It contains a single child node, <OVOMgmtServerInfo>.

BackendSection/OVOMgmtServerInfo

This node contains parameters that configure the Backend Service on the HPOM management server.

BackendSection/OVOMgmtServerInfo/HostName

Backend Service system's host name

BackendSection/OVOMgmtServerInfo/JavaHome

JAVA_HOME on the Backend Service system

BackendSection/OVOMgmtServerInfo/RmiPort

Backend Service RMI port number

BackendSection/OVOMgmtServerInfo/NodeGroupName

HPOM node group that the host name manager adds nodes to

B Policies, Tools, and Reports

This appendix provides reference information for the following:

- Message Groups
- Tools
- Policies
- TIBCO SPI Self Management
- Performance Metrics
- Reports

Message Groups

Table 1

Name	Description
TIBCO	For messages coming from the TIBCO environment.
TIBCO SPI	For messages coming from TIBCO SPI.

Tools

Table 2

Name	Group	Description
Configure TIBCO SPI	SPI for TIBCO	Launches an interface to modify the TIBCO SPI configuration file. Transfers the configuration file to the Frontend system and restarts the Backend and the Frontend Service.
frontend installation	SPI for TIBCO	Installs the frontend service on the selected node.
frontend un-installation	SPI for TIBCO	Un-installs the frontend service on the selected node.
Self-Healing Info	SPI for TIBCO	Self Healing Collector for TIBCO SPI.
Restart TIBCO SPI	SPI for TIBCO	Restarts TIBCO SPI.
Start TIBCO SPI	SPI for TIBCO	Starts the Backend and the Frontend Services.
TIBCO SPI Status	SPI for TIBCO	Checks the status of the Backend and the Frontend Services.
Stop TIBCO SPI	SPI for TIBCO	Stops the Backend and the Frontend Services.

Policies

Table 3

Name	Type	Group	Description
SPI for TIBCO	Group	N/A	Contains all of the TIBCO SPI groups and policies
TIBSPI-EventService-V1	Policy	SPI for TIBCO	Contains policies that intercept the HPOM messages sent by the TIBCO SPI
TIBSPI-Metrics-V1	Policy	SPI for TIBCO	Contain policies related to metric data collection and metric threshold monitoring
TIBSPI-UNIX-Backend-V1	Policy	SPI for TIBCO	Contains policies that monitor the TIBCO SPI log files on the Backend node
TIBSPI-UNIX-Frontend-V1	Policy	SPI for TIBCO	Contains policies that monitor the TIBCO SPI log files on the Frontend node
TIBSPI-UNIX-V1	Policy	SPI for TIBCO	Contains policies that monitor various TIBCO products that are running on UNIX nodes
TIBSPI-Windows-V1	Group	SPI for TIBCO	Contains policies that monitor various TIBCO products that are running on Windows nodes
TIBSPI-EventService-Msg-V1	Message	TIBSPI-Event Service-V1	The Frontend intercepts operational notifications from the TIBCO EMA. For each operational notification it receives, it sends an HPOM message that represents the notification. This intercepts these HPOM messages that are created by the Frontend.

Table 3

Name	Type	Group	Description
TIBSPI-Frontend-MSG-V1	Message	TIBSPI-Event Service- V1	Intercepts the HPOM message sent by the Frontend once it is started. Acknowledges previous HPOM messages that indicated that a TIBCO resource was down. This must be assigned and deployed to capture the messages sent from the TIBCOSPI-Frontend-Unix-Sched-V1
TIBSPI-Collect-Mon-V1	Monitor	TIBSPI-Metrics-V1	Collects metric data for alarming, reports and graphs. Note that the metric data is logged into the report data source. For the graphs, the metric data is saved in text files in: /var/opt/OV/datafiles/tib/datalog It is logged into the graph data source by the TIBSPI-Graph-Mon-V1.
TIBSPI-Graph-Mon-V1	Monitor	TIBSPI-Metrics-V1	Logs the metric data collect by the TIBSPI-Collect-Mon-V1 into the graph data source
TIBSPI_0009	Monitor	TIBSPI-Metrics-V1	Monitors the RVD Retransmission Packet Rate
TIBSPI_0010	Monitor	TIBSPI-Metrics-V1	Monitors the RVD Missed Packet Rate
TIBSPI-Backend-Log-V1	Logfile	TIBSPI-UNIX-Backend-V1	Monitors the Backend log file
TIBSPI-Frontend-Unix-Log-V1	Logfile	TIBSPI-UNIX-Frontend-V1	Monitors the Frontend log file
TIBSPI-UNIX-EMA-V1	Group	TIBSPI-UNIX-V1	Contains policies that monitor the TIBCO Enterprise Management Advisor running on a UNIX system

Table 3

Name	Type	Group	Description
TIBSPI-UNIX-RVRD-V1	Group	TIBSPI-UNIX-V1	Contains policies that monitor TIBCO Rendezvous running on a UNIX system
TIBSPI-UNIX-HAWK-Agent-V1	Group	TIBSPI-UNIX-V1	Contains policies that monitor the TIBCO Hawk Agent running on a UNIX system
TIBSPI-EMA-Unix-Log-V1	Logfile	TIBSPI-TIBCO-EMA-UNIX-V1	Monitors the TIBCO Enterprise Management Advisor log file on a UNIX system
TIBSPI-RVRD-Unix-Log-V1	Logfile	TIBSPI-TIBCO-RVRD-V1	Monitors the TIBCO Rendezvous Routing Daemon log file on a UNIX system
TIBSPI-Hawk-Unix-Log-V1	Logfile	TIBSPI-UNIX-Hawk-Agent-V1	Monitors the TIBCO Hawk Agent log file on a UNIX system
TIBSPI-HawkHMA-Unix-Log-V1	Logfile	TIBSPI-UNIX-Hawk-Agent-V1	Monitors the TIBCO Hawk MicroAgent log file on a UNIX system
TIBSPI-HawkTibRendezvous-Unix-V1	Logfile	TIBSPI-UNIX-Hawk-Agent-V1	Monitors the TIBCO Hawk Agent Rendezvous log file on a UNIX system
TIBSPI-WIN-EMA-V1	Group	TIBSPI-Windows-V1	Contains policies that monitor the TIBCO Enterprise Management Advisor running on a Windows system
TIBSPI-WIN-RVRD-V1	Group	TIBSPI-Windows-V1	Contains policies that monitor TIBCO Rendezvous running on a Windows system
TIBSPI-WIN-HAWK-Agent-V1	Group	TIBSPI-Windows-V1	Contains policies that monitor the TIBCO Hawk Agent running on a Windows system

Table 3

Name	Type	Group	Description
TIBSPI-EMA-WIN-Log-V1	Logfile	TIBSPI-WIN-EMA-V1	Monitors the TIBCO Enterprise Management Advisor log file on a Windows system
TIBSPI-RVRD-WIN-Log-V1	Logfile	TIBSPI-WIN-RVRD-V1	Monitors the TIBCO Rendezvous Routing Daemon log file on a Windows system
TIBSPI-Hawk-WIN-Log-V1	Logfile	TIBSPI-WIN-HAWK-Agent-V1	Monitors the TIBCO Hawk Agent log file on a Windows system
TIBSPI-HawkHMA-WIN-Log-V1	Logfile	TIBSPI-WIN-HAWK-Agent-V1	Monitors the TIBCO Hawk MicroAgent log file on a Windows system
TIBSPI-HawkTibRendezvous-WIN-V1	Logfile	TIBSPI-WIN-HAWK-Agent-V1	Monitors the TIBCO Hawk Agent Rendezvous log file on a Windows system

TIBCO SPI Self Management

Table 4

Name	Group	Description
TIBSPI-Mon-Backend- V1	TIBSPI-UNIX-Backend-V1	Monitors the TIBCO SPI Backend process on the management server. It sends a message to the HPOM Message Browser if Backend process is found not running. An operator initiated Action is available for that message to restart the Backend process.
TIBSPI-Mon-Frontend-V1	TIBSPI-UNIX-Frontend-V1	Monitors the TIBCO SPI Frontend process on the management server. It sends a message to the HPOM Message Browser if Frontend process is found not running. An operator initiated Action is available for that message to restart the Frontend process.
TIBSPI-EMA-Unix-Mon-V1	TIBSPI-UNIX-EMA-V1	Monitors the TIBCO EMA process running on UNIX. It sends a message to the HPOM Message Browser if this process is found not running. An operator initiated Action is available for that message to restart the EMA process. HPOM Administrator may have to modify the operator initiated action if they have installed the EMA in a directory other than <code>/opt/tibco/ema/2.0</code> directory, and provide the location where EMA is installed in the specific environment.
TIBSPI-EMA-WIN-Mon-V1	TIBSPI-WIN-EMA-V1	Monitors the TIBCO EMA process running on Windows. It sends a message to the HPOM Message Browser if the process is not running. An operator initiated Action is available for that message to restart the EMA process.

Performance Metrics

Table 5

Name	MO Type	Alarm	Graph	Report	Description
B001_MsgsSent	RVD		X	X	Number of messages sent by the RVD in the last polling interval
B002_MsgsRcvd	RVD		X	X	Number of messages received by the RVD in the last polling interval
B003_BytesSent	RVD		X	X	Number of bytes sent by the RVD in the last polling interval
B004_BytesRcvd	RVD		X	X	Number of bytes received by the RVD in the last polling interval
B005_PcktSent	RVD		X	X	Number of packets sent by the RVD in the last polling interval
B006_PcktRcvd	RVD		X	X	Number of packets received by the RVD in the last polling interval

Table 5

Name	MO Type	Alarm	Graph	Report	Description
B008_MissPcktRVD	RVD		X	X	Number of packets missed by the RVD in the last polling interval
B009_RetranPcktRate	RVD	X			The RVD's retransmitted packet rate
B010_MissedPcktRate	RVD	X			The RVD's missed packet rate
NumInboundMsgs	JMS Server		X	X	Number of inbound messages received by the JMS Server
InboundMsgRate	JMS Server	X			The JMS Server's inbound message rate per second
NumOutboundMsgs	JMS Server		X	X	Number of outbound messages sent by the JMS Server
OutboundMsgRate	JMS Server	X			The JMS Server's outbound message rate per second

Table 5

Name	MO Type	Alarm	Graph	Report	Description
NumPendingMsgs	JMS Server		X	X	Number of pending messages for the JMS Server
NumJobsCreated	BW Engine		X	X	Total number of jobs created for all process definitions in the BW Engine
NumJobsSuspended	BW Engine		X	X	Total number of jobs suspended for all process definitions in the BW Engine
NumJobsSwapped	BW Engine		X	X	Total number of jobs swapped for all process definitions in the BW Engine
NumJobsQueued	BW Engine		X	X	Total number of jobs queued for all process definitions in the BW Engine
NumJobsAborted	BW Engine		X	X	Total number of jobs aborted for all process definitions in the BW Engine

Table 5

Name	MO Type	Alarm	Graph	Report	Description
NumJobsCompleted	BW Engine		X	X	Total number of jobs completed for all process definitions in the BW Engine
NumJobsCheckpointed	BW Engine		X	X	Total number of jobs checkpointed for all process definitions in the BW Engine
TotalElapsedTime	BW Engine		X	X	Total elapsed time in milliseconds of all jobs completed by all process definitions in the BW Engine

Reports

Table 6

Name	Type	Report Family	Description
TIBCO Full Range	Report Family	N/A	Contains reports with all available data
TIBCO Last Full Month	Report Family	N/A	Contains reports with data for the last full month
TIBCO Last Full Week	Report Family	N/A	Contains reports with data for the last full week

Table 6

Name	Type	Report Family	Description
TIBCO Yesterday	Report Family	N/A	Contains reports with data from yesterday
TIBCO RVD & Network Interface Receive Rates (FR)	Report	TIBCO Full Range	This report shows the top 10 RVDs of all servers connected on the system. The top 10 RVDs are selected based on the highest rate of packets received. For each RVD also the Network Interface Receive Rates per second of the server appears.
TIBCO RVD & Network Interface Send Rates (FR)	Report	TIBCO Full Range	This reports shows the top 10 RVDs of all servers connected on the system. The top 10 RVDs are selected based on the highest rate of packets sent. For each RVD also the Network Interface Send Rates per second of the server are displayed.
TIBCO RVD Missed Packets (FR)	Report	TIBCO Full Range	This report shows the top 10 RVDs of all servers collected on the system. The top 10 RVDs are selected based on the highest number of missed packets.
TIBCO RVD Retrans & Network Interface Errors (FR)	Report	TIBCO Full Range	This report shows the top 10 RVDs of all servers collected on the system. The top 10 RVDs are selected based on the highest retransmission percentage. For each RVD also the Network Interface error percentages of the server appears.

Table 6

Name	Type	Report Family	Description
TIBCO Top 10 RVD Throughput (FR)	Report	TIBCO Full Range	This report shows the top 10 RVDs based on the highest number of messages sent. The chart displays the daily sum of messages sent for each RVD.
TIBCO RVD & Network Interface Receive Rates (LFM)	Report	TIBCO Last Full Month	This report shows the top 10 RVDs of all servers connected on the system. The top 10 RVDs are selected based on the highest rate of packets received over the last full month. For each RVD also the Network Interface Receive Rates per second of the server appears.
TIBCO RVD & Network Interface Send Rates (LFM)	Report	TIBCO Last Full Month	This reports shows the top 10 RVDs of all servers connected on the system. The top 10 RVDs are selected based on the highest rate of packets sent over the last full month. This report also shows the Network Interface Send Rates per second of the server for each RVD.
TIBCO RVD Missed Packets (LFM)	Report	TIBCO Last Full Month	This report shows the top 10 RVDs of all servers collected on the system. The top 10 RVDs are selected based on the highest number of missed packets over the last full month.

Table 6

Name	Type	Report Family	Description
TIBCO RVD Retrans & Network Interface Errors (LFM)	Report	TIBCO Last Full Month	This report shows the top 10 RVDs of all servers collected on the system. The top 10 RVDs are selected based on the highest retransmission percentage over the last full month. This report also shows the Network Interface error percentage of the server for each RVD.
TIBCO Top 10 RVD Throughput (LFM)	Report	TIBCO Last Full Month	This report shows the top 10 RVDs based on the highest number of messages sent over the last full month. The chart displays the daily sum of messages sent for each RVD.
TIBCO RVD & Network Interface Receive Rates (LFW)	Report	TIBCO Last Full Week	This report shows the top 10 RVDs of all servers connected on the system. The top 10 RVDs are selected based on the highest rate of packets received over the last full week. This report also shows the Network Interface Receive Rate per second of the server for each RVD.
TIBCO RVD & Network Interface Send Rates (LFW)	Report	TIBCO Last Full Week	This report shows the top 10 RVDs of all servers connected on the system. The top 10 RVDs are selected based on the highest rate of packets sent over the last full week. This report also shows the Network Interface Send Rates per second of the server for each RVD.

Table 6

Name	Type	Report Family	Description
TIBCO RVD Missed Packets (LFW)	Report	TIBCO Last Full Week	This report shows the top 10 RVDs of all servers collected on the system. The top 10 RVDs are selected based on the highest number of missed packets over the last full week.
TIBCO RVD Retrans & Network Interface Errors (LFW)	Report	TIBCO Last Full Week	This report shows the top 10 RVDs of all servers collected on the system. The top 10 RVDs are selected based on the highest retransmission percentage over the last full week. This report also shows the Network Interface error percentage of the server for each RVD.
TIBCO Top 10 RVD Throughput (LFW)	Report	TIBCO Last Full Week	This report shows the top 10 RVDs based on the highest number of messages sent over the last full week. The chart displays the daily sum of messages sent for each RVD.
TIBCO RVD & Network Interface Receive Rates (Y)	Report	TIBCO Yesterday	This report shows the top 10 RVDs of all servers connected on the system. The top 10 RVDs are selected based on the highest rate of packets received yesterday. For each RVD also the Network Interface Receive Rates per second of the server appear.

Table 6

Name	Type	Report Family	Description
TIBCO RVD & Network Interface Send Rates (Y)	Report	TIBCO Yesterday	This reports shows the top 10 RVDs of all servers connected on the system. The top 10 RVDs are selected based on the highest rate of packets sent yesterday. This report also shows the Network Interface Send Rates per second of the server for each RVD.
TIBCO RVD Missed Packets (Y)	Report	TIBCO Yesterday	This report shows the top 10 RVDs of all servers collected on the system. The top 10 RVDs are selected based on the highest number of missed packets yesterday.
TIBCO RVD Retrans & Network Interface Errors (Y)	Report	TIBCO Yesterday	This report shows the top 10 RVDs of all servers collected on the system. The top 10 RVDs are selected based on the highest retransmission percentage for yesterday. This report also shows the Network Interface error percentages of the server for each RVD.
TIBCO Top 10 RVD Throughput (Y)	Report	TIBCO Yesterday	This report shows the top 10 RVDs based on the highest number of messages sent yesterday. The chart displays the daily sum of messages sent for each RVD.

Glossary

Attributes

Attributes represents information about an MO as a set of properties.

Backend Service

Backend Service is a software component that receives data and information from the frontend service, converts the information to an HPOM recognized form, and enables HPOM to render the managed environment based on the management data.

Conversation

A managed object that implements the Conversation management interface which represents one service's view of a series of related messages.

Enterprise Management Advisor (EMA)

Enterprise Management Advisor is a TIBCO software that is the gateway through which the TIBCO environment is managed.

Event

An event is a change in the state of the MO.

Event Manager

An Event Manager manages all events emitting from MOs. The Event Manager is responsible for storing, retrieving and (if persistence is implemented) recovering events.

Frontend Service

The Frontend Service is a software component that is responsible for communicating with the TIBCO EMA software to gather management data about a TIBCO environment and its hosted applications.

Managed Object (MO)

An MO is a management representation of a resource. An MO implements a management interface to provide a means to monitor and/or control the underlying resource. HPOM manages all managed resources in TIBCO environment through their corresponding MOs. In the context of this document, when we talk about the MO, we also refer to the managed resource itself.

Management Interface

A management interface exposes the management capabilities of a resource. A Management interface is presented as a set of attributes, operations, and notifications to be accessed through a set of WSDL portTypes.

Managed Resource

Any TIBCO application, product, or abstract management notion such as a class of business process, is referred to as a managed resource.

Model

A model is a set of objects, properties, and their relations.

Namespaces

Namespaces are used to uniquely associate the port types for an interface with a URI. Namespaces are defined in an MO and used in the WSDL file for an MO.

Notification

A notification is a message that is sent or retrieved by one or more subscribers to inform that an event has occurred.

Notification Types

Notification types include the set of exceptions and state changes that can be reported by an MO.

Operations

Operations are set of functions that can be provided to support the management of an MO.

PortTypes

A PortType is the atomic unit of management functionality. MOs can choose which management portTypes to implement but cannot partially implement a portType. A portType is defined for each interface category and is used in the WSDL file for an MO.

Resource

A resource is a component of a deployed environment.

Resource View

An HPOM term that describes a UI representation of a computing environment from the system administrator point of view that starts with what applications are running on which hosts.

Relation

A relation is a type of association between MOs.

Relationship

A relationship specifies two managed objects and the relation to define how two specific objects are associated.

Service

An MO that implements the Service management interface which represents the management capabilities of a web service. This web service may be acting as the provider and/or the consumer of web service messages.

Service View

The service view is a UI representation of a computing environment that is application-centric and describes all application dependencies. This view is the bases for root cause analysis of a failure condition, as well as the initial AIA and simple event correlations.

Service Map

An HPOM term to describe a graphic view into a managed environment. This view shows relationships among MOs.

Simple Object Access Protocol (SOAP)

Simple Object Access Protocol is the standard for web services messages. Based on XML, SOAP defines an envelope format and various rules for describing its contents. Seen (with WSDL and UDDI) as one of the three foundation standards of web services, it is the preferred protocol for exchanging web services.

Subscriber

A subscriber is an entity that is interested in selected notifications from MOs. These notifications contain information about the state change in an MO. For scalability reason, subscription to notifications has an associated timeout. Subscription can be renewed before they expire.

Web Services Description Language (WSDL)

Web Services Description Language is the standard format for describing a web service. Expressed in XML, a WSDL definition describes how to access a web service and what operations it can perform.

Web Services Execution Environment (WSEE)

Web Services Execution Environment is a MO that implements the WSEE management interface which encapsulates the management capabilities of a web service execution environment.

Index

A

- agent node, 26
 - adding, 33
- assign policy groups, 38

B

- backend service, 14
- business management
 - architecture, 11

C

- CA root certificate, 88, 89
- check status
 - command, 42
- client certificate, 89
- configuration
 - data sources, 37
 - frontend subagent, 37
 - TIBCO SPI, 119
 - tool, 119
- custom adapters, 62
- custom adapters metric threshold values, 70

D

- data sources, 37
- deployment scenarios
 - co-located components, 18
 - consolidated, 17
 - remote frontend subagent, 18
- deploy policy groups, 39
- domain extensions, 21
 - TIBCO, 21

E

- Embedded Performance Component (Coda)
 - errors starting, 107
 - logging, 73
- Embedded Performance Component (Coda).log, 73
- emiagent.log, 36

- Enterprise Management Advisor
 - architecture, 15
 - business management overview, 11
 - monitor, 77
 - overview, 15

- event
 - invoking operations, 58
- event management, 57
- events
 - viewing, 57

F

- failover, 81
- frontend.log, 109
- frontend subagent, 14
 - assign policy groups, 38
 - configure, 37
 - deploy policy groups, 39
 - errors in log file, 109

G

- graphs, 72

H

- Hawk API, 11, 15
 - console, 15
- Hawk MicroAgent, 16
- HPOM, 23
- HP Performance Manager, 76
- HP Reporter, 59
- HTTPS, 85
 - configuration parameters, 94
 - configuring, 88

I

- installation
 - resource explorer, 43
 - TIBCO SPI, 26

K

- keystores, 87
 - setting up, 89
 - utility, 90

L

- location candidates, 82
- logging metrics, 59
 - custom adapters, 62, 70
- log levels, 78

M

- manageability, 53
- managed nodeSee agent node, 33
- managed resources
 - viewing, 54
- management console
 - resource explorer, 43
- management interfaces, 21
- management server, 26
- message drop rate, 63
- message groups
 - reference, 125
- MetricDefinitions.xml, 59, 62
- metric element attributes, 59
- metrics, 59
 - changing threshold values, 72
 - collect data, 69
 - configuration file, 59
 - data sources, 37
 - logging for custom adapters, 62, 70
 - multi-instance data, 65, 68

MO

- filtering unwanted, 56
- user friendly name, 75

- monitor EMA agent, 77
- multi-instance metric data
 - configuring, 65
 - configuring threshold, 68

O

- opcmsg, 39, 40, 41
- operational notification, 102
 - missing, 99
- operator automated actions, 58

P

- performance, 76
- performance graphs, 72
- performance metrics
 - reference, 125

R

- reports, 14, 72
 - reference, 125
 - view, 74
- resource explorer, 14
 - installing, 43
 - overview, 14
 - security configuration, 92
 - starting from command line, 44
 - starting from Java Console, 43
 - using, 39, 40, 41
- RVD
 - collecting, 62
 - monitoring, 76

S

- security, 85
- self management, for TIBCO SPI, 77
- service management, 53
- service map
 - linking, 54
 - viewing, 54
- SPI(TIBCO), see TIBCO SPI, 9
- SPI (TIBCO)See TIBCO SPI, 9
- SSL, 85
 - configuring, 88
- standard management, 53

T

- policy groups
 - assign, 38
 - assign to backend node, 38
 - assign to Windows nodes, 40
 - deploy, 39
 - deploy to individual UNIX nodes, 40
 - deploy to Windows nodes, 41
 - verify, 41

policies

- TIBSPI_0009, 72
- TIBSPI-Collect-Mon-V1, 71
- TIBSPI-Hawk-WIN-Log-V1, 72
- TIBSPI-UNIX-Backend-V1 policy group, 38
- TIBSPI-UNIX-Frontend-V1 policy group, 39, 40, 41
- TIBSPI-UNIX- V1 policy group, 39
- TIBSPI-Windows-V1 policy group, 40
- TIBSPI-WIN-HAWK-Agent-V1 policy group, 72

TIBCO Hawk logfile, 72

TIBCO SPI, 11

- applications reference, 125
- backend service, 14
- business management overview, 11
- check status command, 42
- configuration, 119
- frontend subagent, 14
- installation HP-UX and Solaris, 26
- Introduction, 9, 113
- introduction, 9
- message groups, 37
- reports, 14
- self management, 77
- self management reference, 125
- policy groups, 37

TIBSPI_0009 policy, 72

TIBSPI-Collect-Mon-V1 policy, 71

TIBSPI-EventService-V1, 38

TIBSPI-Hawk-WIN-Log-V1 policy, 72

TIBSPI-Metrics-V1, 38

TIBSPI-UNIX-Backend-V1 policy group, 38

TIBSPI-UNIX-Frontend-V1, 38

TIBSPI-UNIX-Frontend-V1 policy group, 39, 40, 41

TIBSPI-Unix node group, 33

TIBSPI-UNIX- V1 policy group, 39

TIBSPI-Windows-V1 policy group, 40

TIBSPI-WIN-HAWK-Agent-V1 policy group, 72

trace levels, 79

truststores, 87

- setting up, 89

U

UDMMetricDefinition.xml, 59, 65, 70

UDM metrics, 37

V

verify

- policy groups, 41
- TIBCO SPI, 42

W

WCConfig.xml, 119

transferring fails, 108

WC configuration file

- editing, 119
- editor error, 109
- parameters, 120
- reference, 119

WSDM

- channel, 11
- overview, 20
- XML interfaces, 21

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **docfeedback@hp.com**

Product name:

Document title:

Version number:

Feedback: