

HP Operations Smart Plug-in for TIBCO

For the HP Operations Manager for Windows®, HP-UX, Linux, and Solaris operating systems

Software Version: 2.00

User Guide

Document Release Date: March 2013

Software Release Date: March 2013



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2004-2005, 2008, 2011, 2013 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Java are registered trademarks 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:

<http://www.hp.com/go/hpsoftwaresupport>

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

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

To find more information about access levels, go to:

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

Contents

User Guide	1
Contents	5
Introduction	9
Licensing Structure	9
Conventions Used	9
Product Documentation	10
Monitoring TIBCO Environment	10
Deployment Scenarios	11
Scenario 1: TIBCO SPI within the TIBCO domain	11
Scenario 2: TIBCO SPI outside the TIBCO Domain	12
Scenario 3: TIBCO SPI on Each Node	13
Scenario 4: TIBCO SPI Deployment for Selective Monitoring	13
Installing the TIBCO SPI	15
Installation Packages	15
Installation Prerequisites	16
Hardware Requirements	16
Software Requirements	16
Installing the TIBCO SPI on HPOM for Windows Management Server	17
Installing the TIBCO SPI on a Local Management Server	17
Installing the TIBCO SPI in a Cluster Environment	18
Installing the TIBCO SPI on HPOM for UNIX Management Server	19
Mounting the DVD	19
Installing the TIBCO SPI through Graphical User Interface	20
Installing the TIBCO SPI through Command Line Interface	21
Installing the TIBCO SPI in a Cluster Environment	22
JCODA Installation (Optional)	22
Removing JCODA	26
Verifying the Installation	27
Components of TIBCO SPI	28
On HPOM for Windows	28

Services	28
Tools	29
Policy Management	30
On HPOM for UNIX	31
Services	31
Tools	32
Policy Management	33
Configuring the TIBCO SPI	35
Steps for Configuring the TIBCO SPI on HPOM for Windows management server	36
Deploy Instrumentation	37
Update and Deploy Configuration Policies	37
Deploy Discovery and Collector Logfile Policies	45
Verify the Discovery Process	47
Steps for Configuring the TIBCO SPI On HPOM for UNIX Management Server	49
Add Nodes to the TIBCO Node Group	54
Assign Categories to the Managed Node	55
Deploy Instrumentation on the Managed Node	56
Assign Policies to the Managed Node	57
Verify the Discovery Process	57
Configuring Out-Of-The-Box (OOTB) Metrics	58
Edit the Metric Policy	58
Create and Deploy the Metric Monitoring Policy	61
Schedule the Metric	63
Verification	65
Example Metrics 1	65
Configuring User-Defined Metrics (UDMs)	66
Edit the Metric Policy	66
Create and Deploy the Metric Monitoring Policy	69
Schedule the Metric	71
Verification	73
Example Metrics 2	73
Formula Elements	74

Creating UDM for all instances discovered in a domain	74
Mapping Strings to Numbers in UDM	75
Monitoring Logfile using UDM	77
Advanced Timeout Configuration (Optional)	79
Forwarding Alerts Generated by Hawk Rules	79
Using Tools	81
TIBCO SPI Tool Group	81
Launching Tools	81
On HPOM for Windows Management Server	81
On the HPOM for UNIX Management Server	82
Using Policies	84
Policy Types for TIBCO SPI	84
Policy Group for TIBCO SPI	84
TIBCO BW Policies	85
TIBCO EMS Policies	87
TIBCO Hawk Agent Monitoring Policies	89
TIBCO RV Policies	89
TIBCO SPI Collector Policies	91
Configuring Monitoring Frequency	91
Discovery Configuration	92
Self-Monitoring Policies	92
LogFile Monitoring Policies	92
Using Reports	94
TIBCO RV Reports	94
TIBCO BW Reports	96
TIBCO EMS Reports	97
Using Graphs	100
TIBCO RV Graphs	100
TIBCO BW Graphs	101
TIBCO EMS Graphs	102
Performance Recommendations	103
Test Environment	103

Test Setup	103
Test Scenario	104
Memory Utilization	104
CPU Utilization	105
Response Time for Logical Systems Data Access Operation	106
Recommendation	106
Removing the TIBCO SPI	107
On the HPOM for Windows Management Server	107
On the HPOM for UNIX management server	109
Troubleshooting	111

Chapter 1

Introduction

The HP Operations Smart Plug-in for TIBCO (TIBCO SPI) is a monitoring solution for TIBCO environment that discovers and monitors the TIBCO infrastructure elements. TIBCO SPI monitors TIBCO Rendezvous (RV), Enterprise Messaging Service (EMS), TIBCO ActiveMatrix Business Work (BW) and LogFiles. TIBCO SPI uses Hawk Java Application Programming Interface (API) for data collection. It monitors customized applications with the help of User-Defined Metrics (UDMs). You can integrate TIBCO SPI with HP Reporter to generate reports and HP Performance Manager to generate graphs. You can view the data represented graphically for quick and easy analysis of a serious or critical error message reported. For more information, see [Using Graphs](#) and [Using Reports](#).

Key Features:

- One policy is set for a TIBCO domain which consist of TIBCO RV, TIBCO BW, and TIBCO EMS.
- Custom metrics are defined with the help of UDMs.
- Remote Logfile monitoring available for EMS and RV
- Out-Of-The-Box (OOTB) reports and graphs are available for the historical analysis.

Licensing Structure

TIBCO SPI license is calculated in terms of microagents being used for monitoring. One license is required for monitoring maximum 50 TIBCO microagents. One managed object is equivalent to one microagent in *HP Operations Smart Plug-in for TIBCO 2.00*.

Conventions Used

The following conventions are used in this document.

Convention	Description
HPOM for UNIX	Refers to HPOM on HP-UX, Linux, and Solaris. It identifies the following operating systems: <ul style="list-style-type: none">• HPOM on HP-UX• HPOM on Linux• HPOM on Solaris
TIBCO SPI	Refers to HP Operations Smart Plug-in for TIBCO.
HPOM Server	Refers to HPOM for Windows and HPOM for UNIX management server.

Product Documentation

TIBCO SPI information is available in the following documents.

Document	Location	Purpose
User Guide	<CD\DVD-ROM\en>	To provide information on: <ul style="list-style-type: none">• Installation of SPI• Configuration of SPI• Using the SPI policies• Using the SPI tools• Using Reports• Using Graphs
Release Notes	<CD\DVD-ROM\en>	To provide information on the current SPI release.

The User Guide and Release Notes are available on the TIBCO SPI DVD. You can directly access the guides from the DVD or copy the documents to the local system for reference.

However, to check for recent updates, go to:

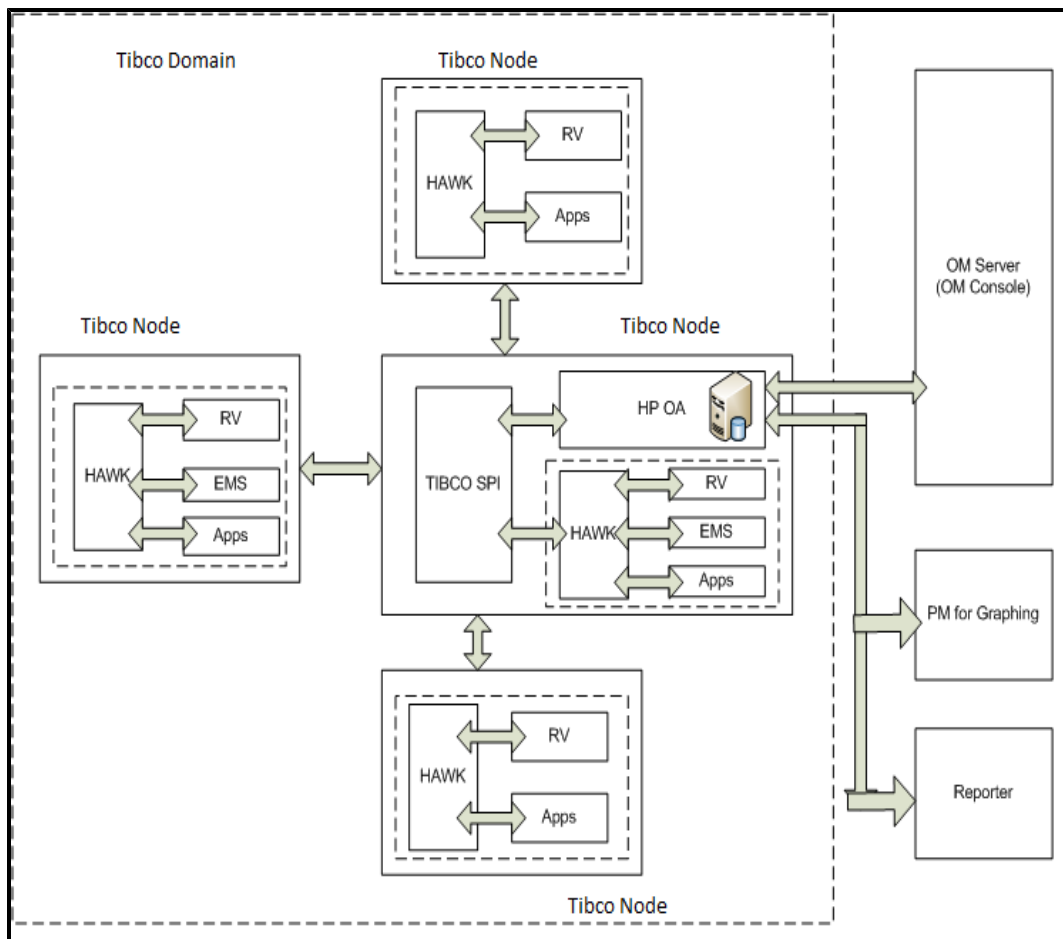
<http://h20230.www2.hp.com/selfsolve/manuals>

Monitoring TIBCO Environment

TIBCO SPI is deployed on the nodes within the domain along with the policies. These policies are deployed from the HPOM console.

TIBCO SPI requests the hawk agents for metric data, which in turn request the particular microagent to provide the data. TIBCO SPI collects data and stores in the database. This data is used to monitor the health and performance of the system.

The below figure depicts an example of TIBCO environment with TIBCO SPI installed.

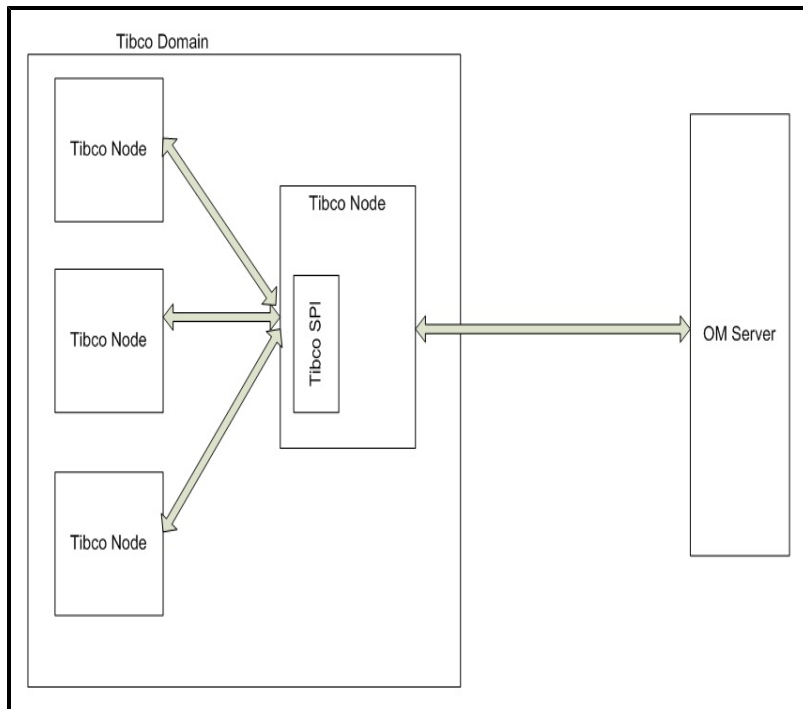


Deployment Scenarios

The TIBCO SPI monitors TIBCO infrastructure elements through different deployment configurations. This section provides some common deployment scenarios and does not represent every possible configuration.

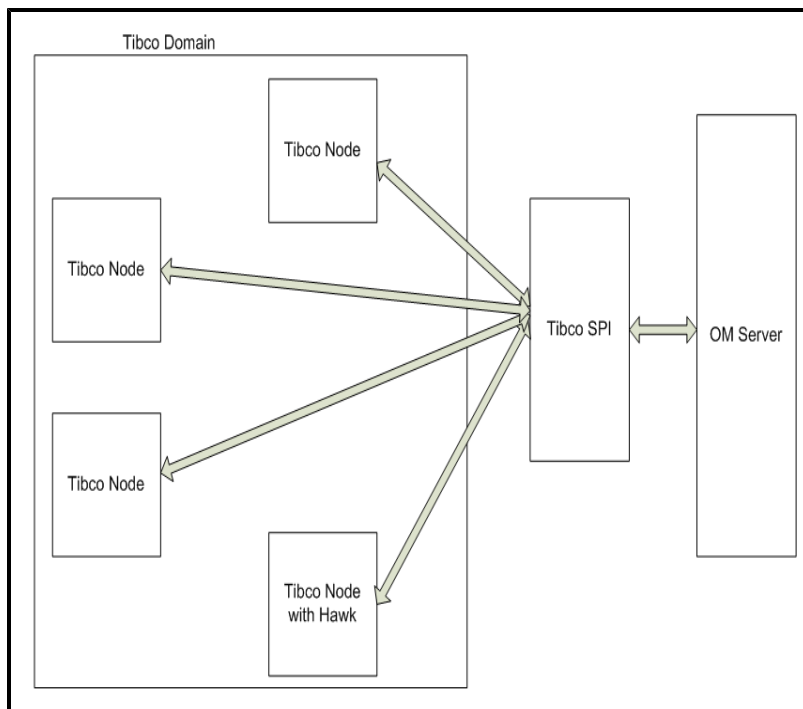
Scenario 1: TIBCO SPI within the TIBCO domain

In this scenario, the TIBCO domain consists of the TIBCO SPI and nodes containing RV, Hawk, and EMS deployed on a particular node. This scenario is useful in monitoring a small number of applications.



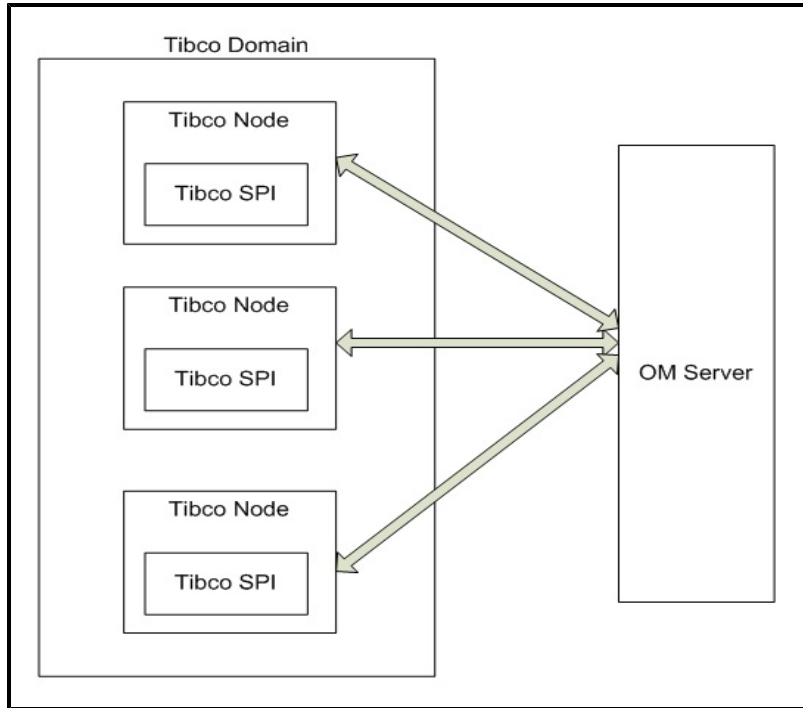
Scenario 2: TIBCO SPI outside the TIBCO Domain

In this scenario, the TIBCO SPI is deployed outside the domain along with the policies which have the thresholds for each metric that is governed. This scenario can be used to monitor TIBCO infrastructure elements deployed through TIBCO Silver Fabric 5.0.2. TIBCO SPI monitors the domains remotely.



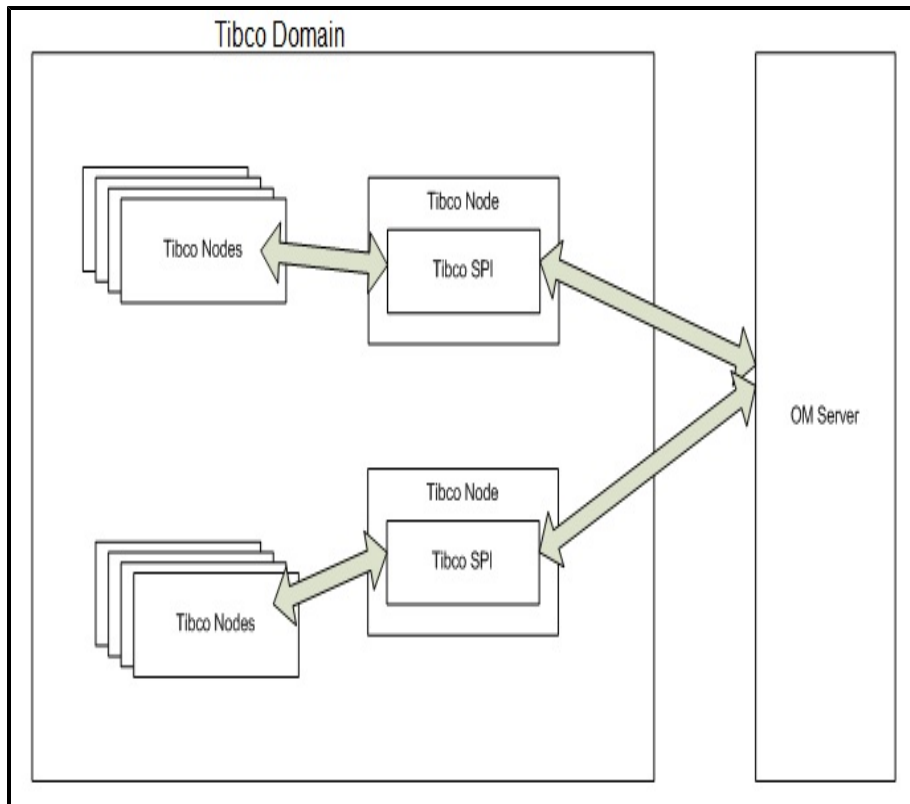
Scenario 3: TIBCO SPI on Each Node

In this scenario, TIBCO SPI is deployed on each node and monitors specific nodes instead of the whole domain. In case you want to run automatic actions on a threshold breach, this scenario is useful compared to other deployment scenarios. This is not possible with other deployment scenarios as the TIBCO domain is monitored remotely.



Scenario 4: TIBCO SPI Deployment for Selective Monitoring

This scenario is useful in monitoring more than 1000 applications. TIBCO SPI can be configured on *one* managed node to monitor *x* number of hawkagents and the remaining hawkagents can be monitored from the other node. This may enhance the performance of TIBCO SPI.



Chapter 2

Installing the TIBCO SPI

This chapter provides installation instructions for the various components of the TIBCO SPI. You must install the TIBCO SPI on the HPOM for the Windows and UNIX management servers.

Installation Packages

The TIBCO SPI installation package includes the SPI, Graphing, and Reporter packages.

SPI Package

You must install the package on a server managed by HPOM. The name and location of the SPI package is as follows:

- HPOM for Windows (version 8.1x and 9.x)

```
<SPI DVD>\OMW_SPIDVD_App_13.00.000_setup.exe
```

- For HP-UX

```
<SPI DVD>\TIBCO_OMU_SPIDVD_App_13.00.000_setup.bin
```

- For Linux

```
<SPI DVD>\TIBCO_OML_SPIDVD_App_13.00.000_setup.bin
```

- For Solaris

```
<SPI DVD>\TIBCO_OMS_SPIDVD_App_13.00.000_setup.bin
```

Graphing Package

The Graphing package contains the default graphing policies provided by TIBCO SPI. Graphs are drawn from metrics collected in the datasources created by the SPI.

The name and location of the graphing package is as follows:

- For Windows,

```
<SPI DVD>\packages\HPOvSpiTibG-2.00.016-Win5.2_64.msi
```

- For HP-UX,

```
<SPI DVD>\packages\HPOvSpiTibG-2.00.016-HPUX11.11.depot
```

- For Linux,

```
<SPI DVD>\packages\HPOvSpiTibG-2.00.016-Linux2.6_64.rpm
```

- For Solaris,

```
<SPI DVD>\packages\HPOvSpiTibG-2.00.016-SunOS5.8.sparc
```

Reporter Package

The Reporter package contains the default reporter policies provided by the SPI. The TIBCO SPI Reporting package is present at the following location in the media:

- For 64 bit Windows:

```
<SPI DVD>\HPOvSpiTibR-2.00.016-Win5.2_64.msi
```

- For 32 bit Windows:

```
<SPI DVD>\HPOvSpiTibR-2.00.016-WinNT4.0.msi
```

Installation Prerequisites

Make sure that all the requirements are met before you begin the installation. Install the HPOM server before installing the TIBCO SPI. It is not necessary to stop HPOM sessions before you start installing TIBCO SPI.

Hardware Requirements

For information about hardware requirements, see the *HP Operations Manager for Windows* documentation for Windows management server and *HP Operations Manager for Unix* documentation for UNIX management server. For information on hardware requirements for the managed nodes, see the Support Matrix (SUMA) link <http://support.openview.hp.com/selfsolve/document/KM323488>.

Software Requirements

Make sure that the following software requirements are met before you start installing the TIBCO SPI:

On the Management Server:

Windows

- HP Operations Manager for Windows: 8.1x and 9.x
- HP Performance Manager: 9.00 (required, if you want to create graphs)
- HP Reporter: 3.90 or above (required, if you want to create web-based reports).

HP-UX, Linux, or Solaris

- HP Operations Manager for UNIX: 9.1x
- HP Performance Manager: 9.00 (required, if you want to create graphs)
- HP Reporter: 3.90 or above (required, if you want to create web-based reports).

On the Managed Nodes:

- HP Operations agent (version 11.10 or above must be installed and configured).

Installing the TIBCO SPI on HPOM for Windows Management Server

Note: On the management server, set an environment variable JAVA_HOME to the JRE installation directory.

To install TIBCO SPI on the management server, you can perform any one of the following procedures:

- [Installing TIBCO SPI on a Local Management Server](#)
- [Installing TIBCO SPI in a Cluster Environment](#)

Installing the TIBCO SPI on a Local Management Server

You can use the wizard to complete the installation. Follow these steps:

1. Insert the HP Operations Smart Plug-ins DVD into the DVD drive of the management server system, and open the media contents in the Explorer Window.
2. On the media, double-click **TIBCO_OMW_SPIDVD_App_13.00.000_setup.exe** to start the installer.

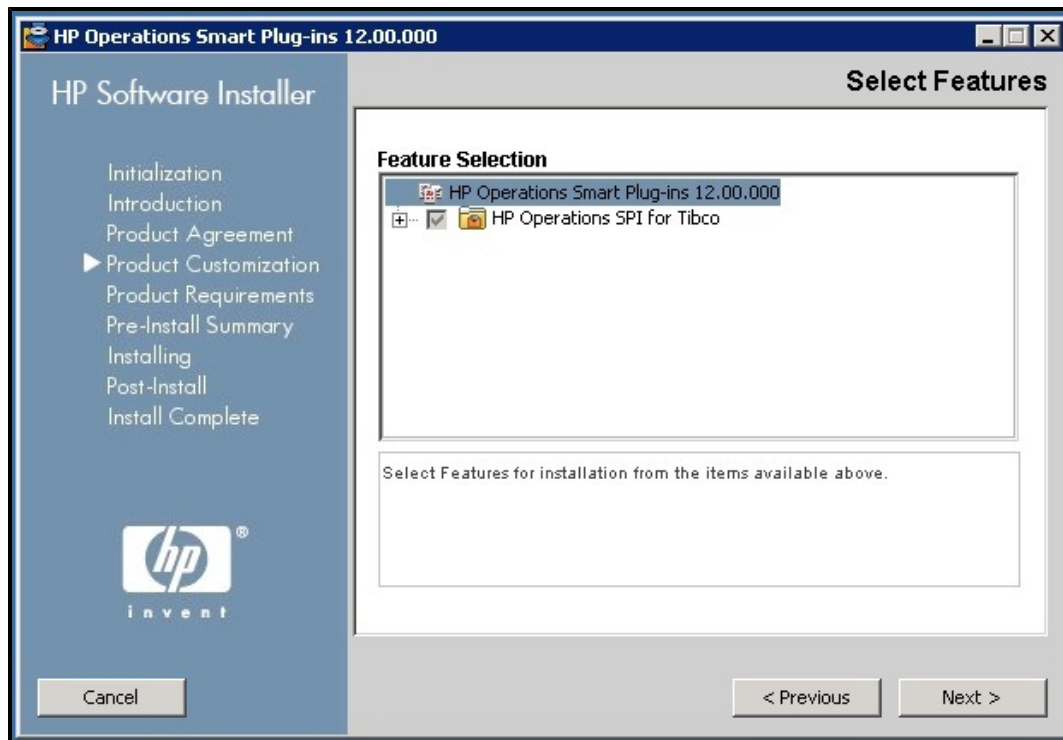
The Introduction (Install) page appears.

3. On the Introduction (Install) page, click **Next**.

The License Agreement page appears.

4. Read the terms of the license agreement, select the `I accept the terms of License Agreement` option and click **Next**.

The Select Features page opens displaying the installation option.



5. Select the feature and click **Next**.

The installer starts performing the installation checks.

6. Follow the on-screen instructions and continue the installation process using the **Next** button.

The Installation Complete dialog box appears after you complete the installation.

7. Click **Done** to complete the installation. TIBCO SPI is installed.

Installing the TIBCO SPI in a Cluster Environment

You must first install the HPOM management server in the cluster. After you complete cluster installations, you must start installing TIBCO SPI.

Make sure that each node in the cluster has sufficient disk space for the TIBCO SPI. After installing the HPOM management server, follow these steps:

1. For the first installation (Node A) in the cluster -- Refer to the standard installation procedure, [Installing the TIBCO SPI on a Local Management Server](#). After you complete the installation on Node A, you will receive an instruction to proceed to the next node Node B.
2. For the Node B installation in the cluster -- Follow the same procedure as Node A. The installation detects the cluster configuration and copies all the required installation packages from Node A to Node B.
3. For Node C and all the remaining nodes in the cluster -- Follow the same procedure as of Node B where the installation packages are copied from Node B to Node C until TIBCO SPI is installed on all the nodes.

Install the TIBCO SPI on the First Cluster-Aware Management Server

Note: Before you begin with the installation, make sure that sufficient disk space is available on each management server. Avoid canceling the installation process before it is completed as it can result in incomplete installation.

Follow the steps mentioned in the section [Installing the TIBCO SPI On a Local Management Server](#) and then proceed to the next management server. Selecting **Cancel** after the installation has started does not halt the installation process.

Install the TIBCO SPI on the Next Cluster-Aware Management Server

Follow these steps on each management server in the cluster until TIBCO SPI is installed on all the nodes.

1. Insert the HP Operations Smart Plug-ins DVD in the DVD drive of the management server and follow the instructions on the wizard as it appears.
2. After the installation is complete, proceed as directed to the next management server until the installation on every management server in the cluster is complete.

Installing the TIBCO SPI on HPOM for UNIX Management Server

You must uninstall the older version of TIBCO SPI from the management server before proceeding with the installation of TIBCO SPI version 2.00. To uninstall the TIBCO SPI from the management server, see [Removing TIBCO SPI](#).

To install the TIBCO SPI mount the DVD and then follow the Installation steps either through Graphical User Interface or Command Line Interface.

Mounting the DVD

To mount the DVD on HPOM for UNIX, follow these steps:

1. Log on as a `root` user.
2. Set the user's root umask by entering:

```
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 and enter:

```
mount /dev/<dvdrom_drive_name> /<mount_point>
```

For example, for a local DVD, you enter:

```
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.

Installation Steps

To install TIBCO SPI on HPOM for UNIX, perform any of the following procedures:

- [Graphical User Interface](#)
- [Command Line Interface](#)

Installing the TIBCO SPI through Graphical User Interface

To install the TIBCO SPI 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, Solaris, or Linux 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 installation, type one of the following command, according to your management server:

For HP-UX:

```
./TIBCO_OMU_SPIDVD_App_13.00.000_setup.bin
```

For Solaris:

```
./TIBCO_OMS_SPIDVD_App_13.00.000_setup.bin
```

For Linux:

```
./TIBCO_OML_SPIDVD_App_13.00.000_setup.bin
```

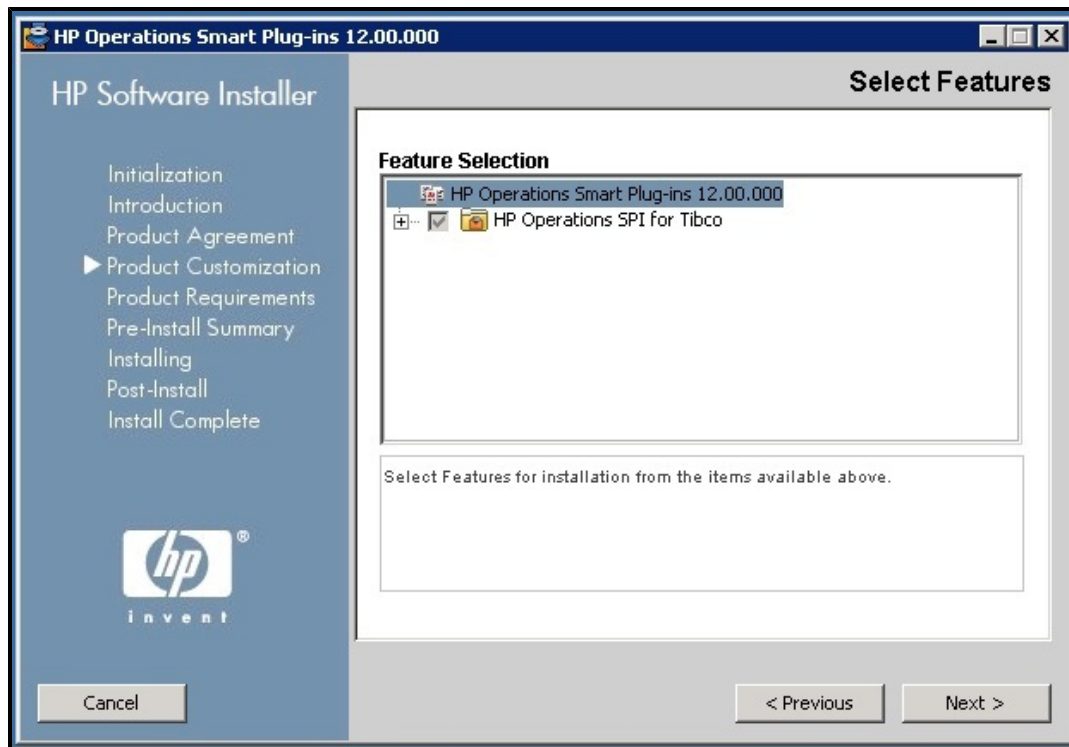
The Introduction (Install) page of the installation wizard appears.

5. On the Introduction (Install) page of the installation wizard, click **Next**.

The License Agreement page appears.

6. Read the terms of the license agreement, select the `I accept the terms of License Agreement` option and click **Next**.

The Select Features page opens displaying the installation option.



7. Select the feature and click **Next**.

The installer starts performing the installation checks.

8. Follow the on-screen instructions and continue the installation process using the **Next** button.

The Installation Complete dialog box appears after you complete the installation.

9. Click **Done** to complete the installation. TIBCO SPI is installed.

Installing the TIBCO SPI through Command Line Interface

To install the TIBCO SPI through 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, Solaris, or Linux management server. Mount the DVD if necessary.
3. To start the installation, type one of the following command, according to your management server:

For HP-UX:

```
./TIBCO_OMU_SPIDVD_App_13.00.000_setup.bin -i console
```

For Solaris:

```
./TIBCO_OMS_SPIDVD_App_13.00.000_setup.bin -i console
```

For Linux:

```
./TIBCO_OML_SPIDVD_App_13.00.000_setup.bin -i console
```

4. The Introduction screen appears. Press **Enter** to continue.
5. When the prompt, 'I accept the terms of the License Agreement' for the License agreement appears, press **Y** to accept the terms and continue installation.
6. When the prompt, 'Please select Features' for the selection of the feature appears, press the number corresponding to the feature you want to install.

Press **Enter**, a series of messages appear.
7. Follow the instructions as displayed in the message.

After the installation is complete, you will receive a message which states that the installation is completed.

Installing the TIBCO SPI in a Cluster Environment

To install the TIBCO SPI in a cluster environment, follow the steps in the section [Installing the TIBCO SPI in a cluster Environment](#) and proceed to the next management server until the installation in the cluster is complete.

JCODA Installation (Optional)

JCODA installation is optional on the managed node where TIBCO SPI is deployed. It helps in better performance with respect to data logging to coda. TIBCO SPI can also work without the installation of JCODA packages.

To install JCODA follow these steps:

1. On the media, go to
`<SPIDVD>/packages/JCODAInstaller/<AgentVersion>/<NodePlatform>.`
2. Install the packages with the platform specific installation commands in the specified order:

Node Plat- forms	Command
AIX_64:	installp -ac -d <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/AIX5.3_64/HPOvJXpl-11.11.030-AIX5.3_64-release.bff all
	installp -ac -d <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/AIX5.3_64/HPOvJSec-11.11.030-AIX5.3_64-release.bff all
	installp -ac -d <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/AIX5.3_64/HPOvJbbc-11.11.030-AIX5.3_64-release.bff all
	installp -ac -d <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/AIX5.3_64/HPOvJPacc-11.11.030-AIX5.3_64-release.bff all
HPUX 11.11	swinstall -s <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/ HPUX11.11/HPOvJXpl-11.11.030-HPUX11.11-release.depot *
	swinstall -s <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/ HPUX11.11/HPOvJSec-11.11.030-HPUX11.11-release.depot *
	swinstall -s <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/ HPUX11.11/HPOvJbbc-11.11.030-HPUX11.11-release.depot *
	swinstall -s <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/ HPUX11.11/HPOvJPacc-11.11.030-HPUX11.11-release.depot *

Node Plat- forms	Command
HPUX 11.23_ IPF	<pre>swinstall -s <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/ HPUX11.23_IPF32/HPOvJXpl-11.11.030-HPUX11.23_IPF32- release.depot *</pre>
	<pre>swinstall -s <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/ HPUX11.23_IPF32/HPOvJSec-11.11.030-HPUX11.23_IPF32- release.depot *</pre>
	<pre>swinstall -s <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/ HPUX11.23_IPF32/ HPOvJbbc-11.11.030-HPUX11.23_IPF32- release.depot *</pre>
	<pre>swinstall -s <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/ HPUX11.23_IPF32/HPOvJPacc-11.11.030-HPUX11.23_IPF32- release.depot *</pre>
Linux 2.6	<pre>rpm -ihv <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/ Linux2.6/HPOvJXpl-11.11.030-Linux2.6-release.rpm</pre>
	<pre>rpm -ihv <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/ Linux2.6/HPOvJSec-11.11.030-Linux2.6-release.rpm</pre>
	<pre>rpm -ivh <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/ Linux2.6/HPOvJbbc-11.11.030-Linux2.6-release.rpm</pre>
	<pre>rpm -ivh <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/ Linux2.6/HPOvJPacc-11.11.030-Linux2.6-release.rpm</pre>

Node Plat- forms	Command
Linux 2.6_64	rpm -ihv <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/Linux2.6_64/HPOvJXpl-11.11.030-Linux2.6_64-release.rpm
	rpm -ihv <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/Linux2.6_64/HPOvJSec-11.11.030-Linux2.6_64-release.rpm
	rpm -ivh <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/Linux2.6_64/HPOvJbbc-11.11.030-Linux2.6_64-release.rpm
	rpm -ivh <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/Linux2.6_64/HPOvJPacc-11.11.030-Linux2.6_64-release.rpm
Solaris_ sparc	pkgadd -d <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/SunOS5.8/HPOvJXpl-11.11.030-SunOS5.8-release.sparc HPOvJXpl
	pkgadd -d <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/SunOS5.8/HPOvJSec-11.11.030-SunOS5.8-release.sparc HPOvJSec
	pkgadd -d <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/SunOS5.8/HPOvJbbc-11.11.030-SunOS5.8-release.sparc HPOvBbc
	pkgadd -d <SPIDVD>/packages/JCODAInstaller/<AgentVersion>/SunOS5.8/HPOvJPacc-11.11.030-SunOS5.8-release.sparc HPOvJPacc

For WinNT:

- On the media, go to the following directory
<SPIDVD>/packages/JCODAInstaller/
<AgentVersion>/WinNT4.0/HPSHaredComp-11.11.030-WinNT4.0-release.msi
and follow the on-screen instructions.

For Windows x64:

- On the media, go to the following directory
<SPIDVD>/packages/JCODAInstaller/<AgentVersion>/Win5.2_64/HPSHaredComp-11.11.030-Win5.2_64-release.msi and follow the on-screen instructions.

Removing JCODA

To remove JCODA, type the commands in the specified order:

Node Platforms	Command
AIX_64	<code>installp -u HPOvLcore.HPOvJxpl</code>
	<code>installp -u HPOvLcore.HPOvJSec</code>
	<code>installp -u HPOvLcore.HPOvJbbc</code>
	<code>installp -u HPOvPerf.HPOvJPa</code>
HPUX 11.11	<code>swremove HPOvLcore.HPOvJxpl</code>
	<code>swremove HPOvLcore.HPOVJSEC</code>
	<code>swremove HPOvLcore.HPOVJBBC</code>
	<code>swremove HPOvPerf.HPOVJPACC</code>
HPUX 11.23_IPF	<code>swremove HPOvLcore.HPOvJxpl</code>
	<code>swremove HPOvLcore.HPOVJSEC</code>
	<code>swremove HPOvLcore.HPOVJBBC</code>
	<code>swremove HPOvPerf.HPOVJPACC</code>
Linux 2.6	<code>rpm -ev HPOvJxpl</code>
	<code>rpm -ev HPOvJSec</code>
	<code>rpm -ev HPOvJbbc</code>
	<code>rpm -ev HPOvJPacc</code>
Linux 2.6_64	<code>rpm -ev HPOvJxpl</code>
	<code>rpm -ev HPOvJSec</code>
	<code>rpm -ev HPOvJbbc</code>
	<code>rpm -ev HPOvJPacc</code>
Solaris_sparc	<code>pkgrm HPOvJxpl</code>
	<code>pkgrm HPOvJSec</code>
	<code>pkgrm HPOvJbbc</code>
	<code>pkgrm HPOvJPacc</code>
WinNT	<code>Msiexec /x {48C8FE1C-92FB-4DEE-B748-8181C57415DE}</code>
Windows x64:	<code>Msiexec /x {48C8FE1C-92FB-4DEE-B748-8181C57415DE}</code>

Verifying the Installation

On the HPOM for Windows Management Server

To verify the installation on the windows management server, check for the following:

1. On the management server, check if the *SPI for Tibco* policy group is available.
2. The %OvInstallDir%\Install\TIBSPI folder is added to the installation directory.
3. The related log files are available in the %temp%\HPOvInstaller\SPI_<version> directory.

The format of the file name of the log file is SPI_<version>_yyyy.MM.dd_xx_yy_HPOvInstallerLog.txt.

In this instance, yyyy indicates the year, MM indicates the month, and dd indicates the day. The xx and yy in the file name indicate the time stamp when the last install was performed.

4. The log file is available at: <OvDataDir>/log/SPIInstallLogs/TIBSPI_Install.log

On the HPOM for UNIX Management Server

To verify the installation on the UNIX management server, check for the following:

1. Type the command on the management server:
 - For HP-UX: swlist |grep -i HPOvSpiTib
 - For Linux: rpm -qa|grep -i HPOvSpiTib
 - For Solaris: pkginfo -l HPOvSpiTib
2. The log files for HPOM for UNIX are available in the /tmp/HPOvInstaller/SPI_<version> directory.

The format of the file name of the log file is SPI_<version>_yyyy.MM.dd_xx_yy_HPOvInstallerLog.txt.

In this instance, yyyy indicates the year, MM indicates the month, and dd indicates the day. The xx and yy in the file name indicate the time stamp when the last install was performed.

3. The application directory is /opt/OV/ and data directory is /var/opt/OV/.
4. The log file is available at: <OvDataDir>/log/SPIInstallLogs/TIBSPI_Install.log

Chapter 3

Components of TIBCO SPI

After you install the TIBCO SPI, you must add nodes that you want to monitor to the management console.

The TIBCO SPI has three main components available for Windows and UNIX management server:

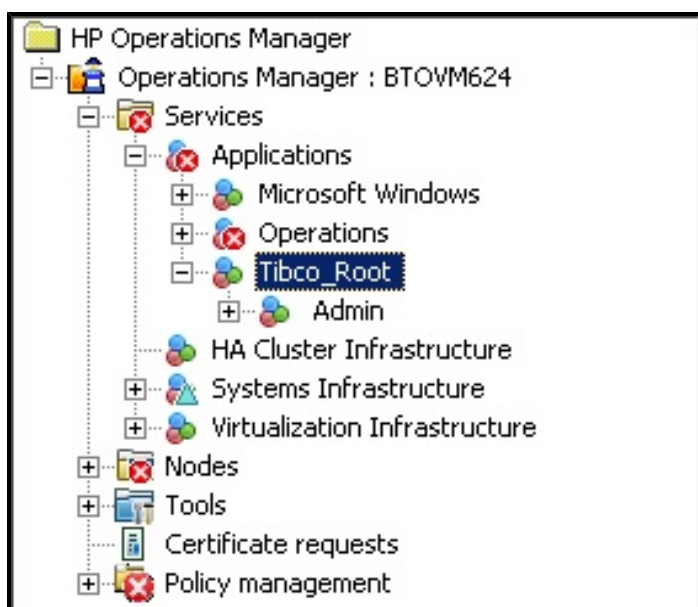
- Services
- Tools
- Policy Management

On HPOM for Windows

Services

To populate the service map you have to deploy the discovery policy on the managed node to the HPOM console. To view the TIBCO SPI service map, select **Services** → **Applications** → **Tibco_Root**.

The following image shows the appearance of the root element of TIBCO SPI under Services in the HPOM console.



The service discovery policy discovers the services on the node, and adds this information to the HPOM Services area.

Hierarchical View of TIBCO SPI Service Tree

The TIBCO SPI Service Tree consists of a root node known as `Tibco_Root`. `Tibco_Root` contains single or multiple domains depending on the number of SPIs installed. Each domain consists of a set of applications and services.

- Applications include all BW applications discovered in a domain for a particular node. Applications are created in the following format.

```
<application name><hawkagent name: domain name>
```

For Example:

```
getTimeEAR-1.Process Archive[IWFVM00237-0:tibco_spi_domain]
```

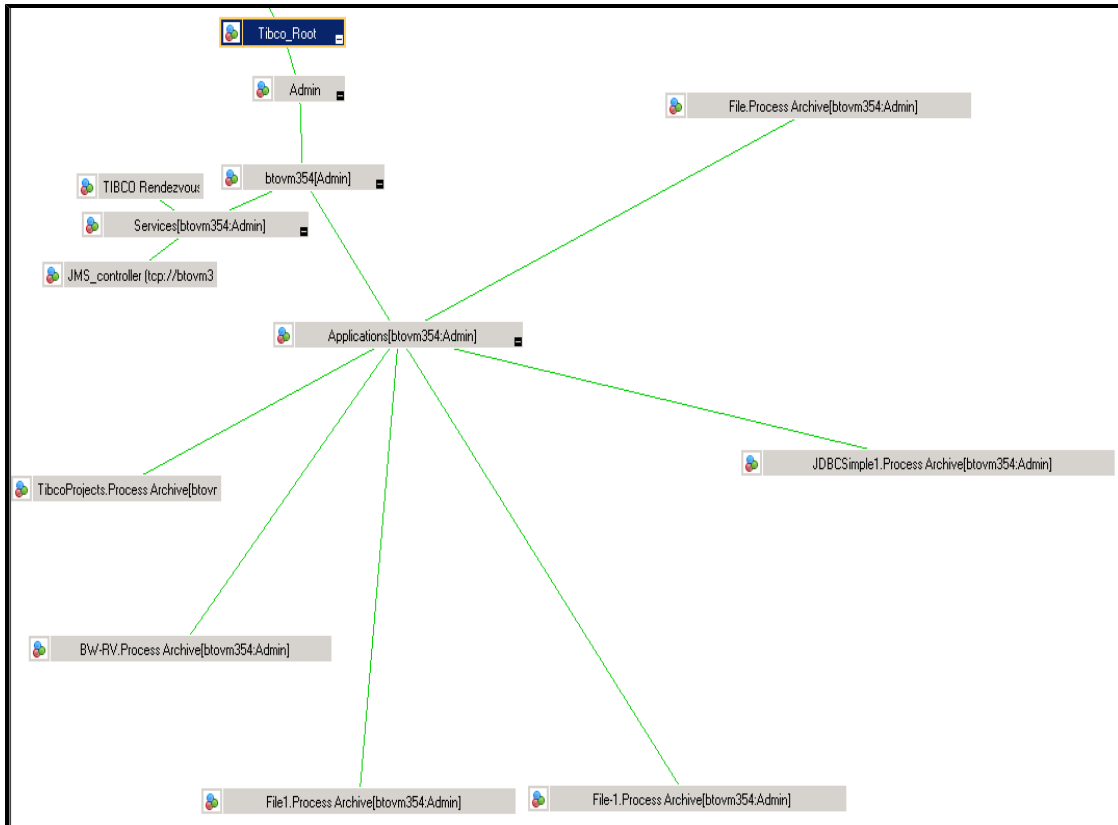
- Services include RVDs and EMS servers which are discovered and run on a particular node.

```
<service name><hawkagent name: domain name>
```

For Example:

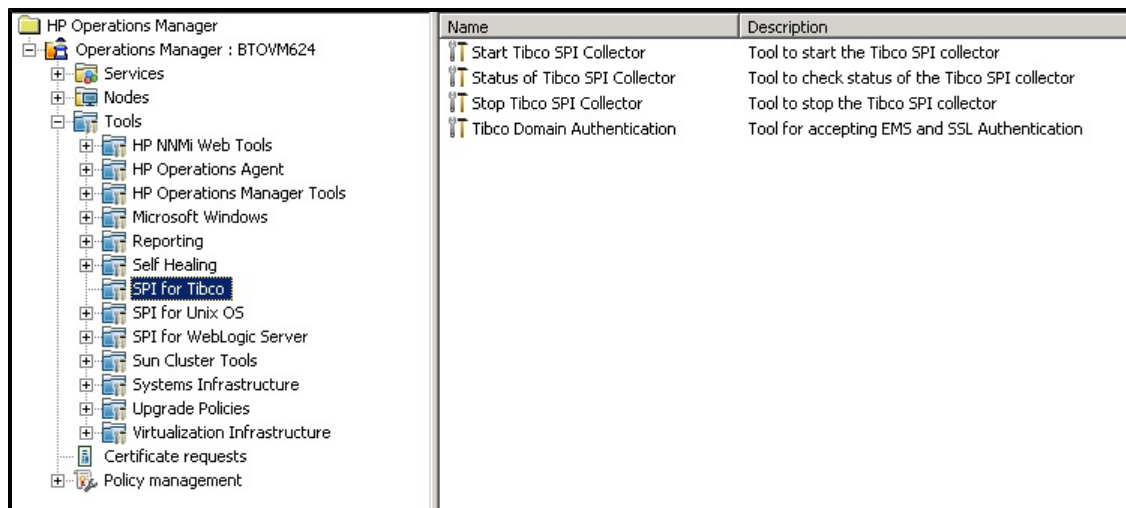
```
JMS_controller(tcp://localhost:7222) [IWFVM00080:TIBCOTESTEMSDOMAIN]
```

The TIBCO SPI service map graphically represents the discovered systems and instances.



Tools

The TIBCO SPI offers tools that help you to monitor and manage systems. To see the TIBCO SPI tool group, select **Tools** → **SPI for Tibco**.

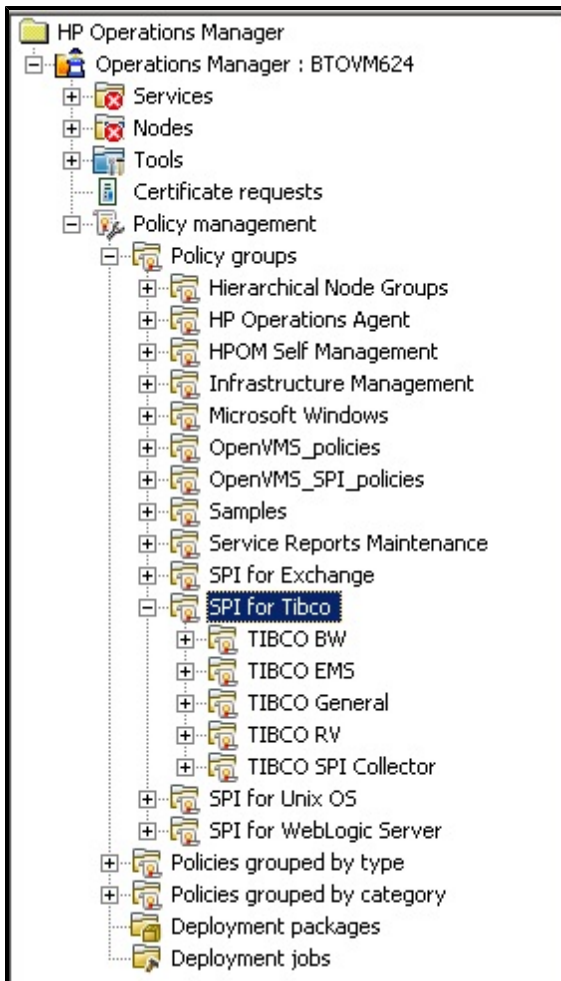


For information on the tools provided by TIBCO SPI, see ["Using Tools"](#) on page 81

Policy Management

The TIBCO SPI policies enable you to monitor the performance and availability of TIBCO infrastructure elements. You can create, edit, deploy, delete, or track policies based on your requirement. These policies contain a set of rules for monitoring logfiles, services, and threshold values.

To view the TIBCO SPI policies, select **Policy management** → **SPI for Tibco**.



For more information on Policy types supported by TIBCO SPI, see ["Policy Types for TIBCO SPI"](#) on page 84

On HPOM for UNIX

Services

To populate the service map you have to deploy the discovery policy on the managed node to the HPOM console. To see the TIBCO SPI service map on the Java interface, select **Services** → **Tibco_Root**.

The service discovery policy discovers the services on the node and adds information to the HPOM Services.

Hierarchical View of TIBCO SPI Service Tree

The TIBCO SPI Service Tree consists of a root node known as `Tibco_Root`. `Tibco_Root` contains single or multiple domains depending on the number of SPIs installed. Each domain consists of a set of applications and services.

- Applications include all BW applications discovered in a domain for a particular node.

Applications are created in the following format.

```
<application name><hawkagent name: domain name>
```

For Example:

```
getTimeEAR-1.Process Archive[IWFVM00237-0:tibco_spi_domain]
```

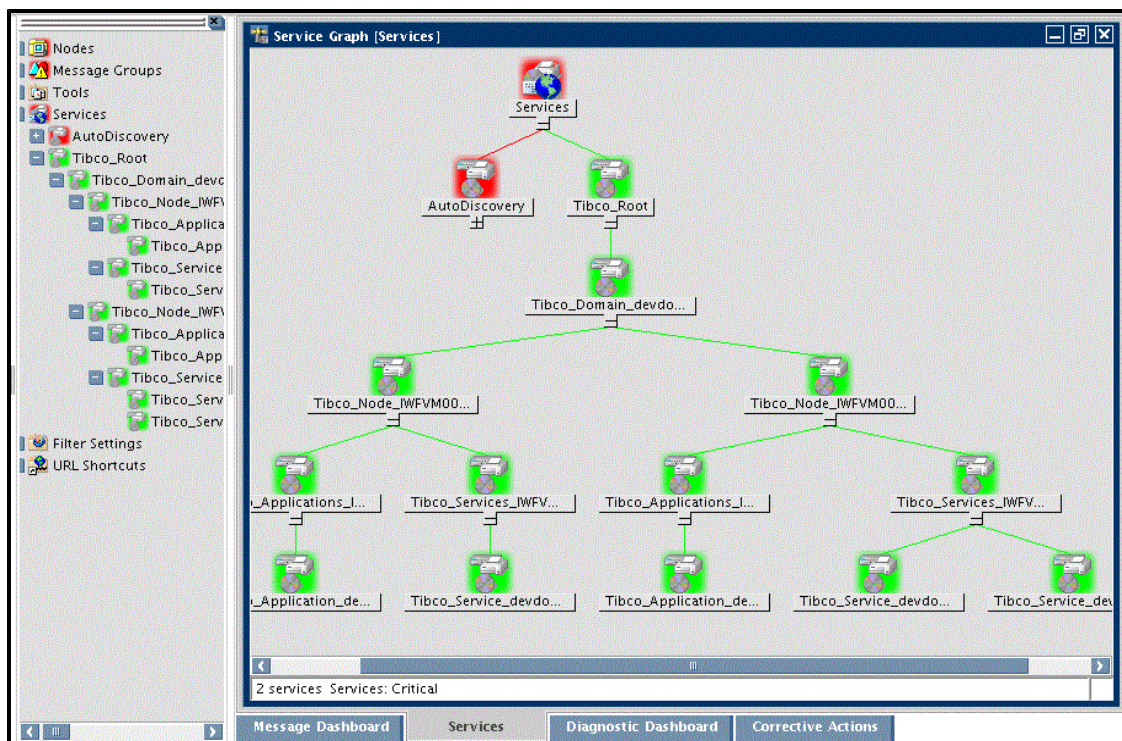
- Services include RVDs and EMS servers which are discovered and run on a particular node.

```
<service name><hawkagent name: domain name>
```

For Example:

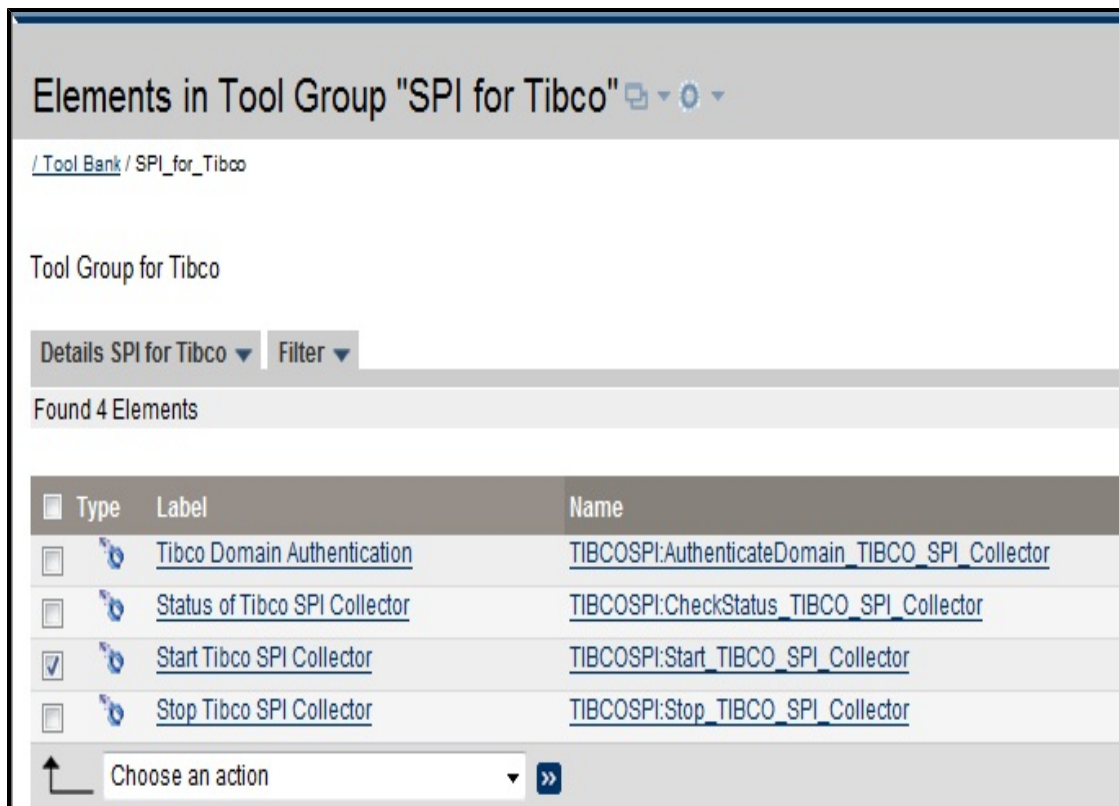
```
JMS_controller(tcp://localhost:7222) [IWFVM00080:TIBCOTESTEMSDOMAIN]
```

The TIBCO SPI service map graphically represents the discovered systems and instances in the below image.



Tools

The TIBCO SPI offers tools that help you to monitor and manage systems. To view the TIBCO SPI tool group, select **Tool Bank** → **SPI for Tibco**.



For more information on the tools provided by TIBCO SPI, see "Using Tools" on page 81

Policy Management



The TIBCO SPI policies enable you to monitor the performance and availability of TIBCO infrastructure elements. You can create, edit, deploy, delete, or track policies based on your requirement. These policies contain a set of rules for monitoring log files, services, and threshold values.

To view the TIBCO SPI policies, select **Policy Bank** → **SPI for Tibco**.























Elements in Policy Group "SPI for Tibco"




[/ Policy Bank / SPI for Tibco](#)

SPI for Tibco GROUP

Details SPI for Tibco  Filter 

Found 5 Elements

 Type	Name	 Assigned	Mode
 	TIBCO BW		 
 	TIBCO EMS		 
 	TIBCO General		 
 	TIBCO RV		 
 	TIBCO SPI Collector		 

 Choose an action  

For more information on Policy types supported by TIBCO SPI, see "Policy Types for TIBCO SPI" on page 84

Chapter 4

Configuring the TIBCO SPI

This chapter explains how to configure the TIBCO SPI on the HP Operations Manager (HPOM). Make sure that you check for the configuration prerequisites; then perform the configuration based on your environment.

Prerequisites on the managed node

Domain Transport

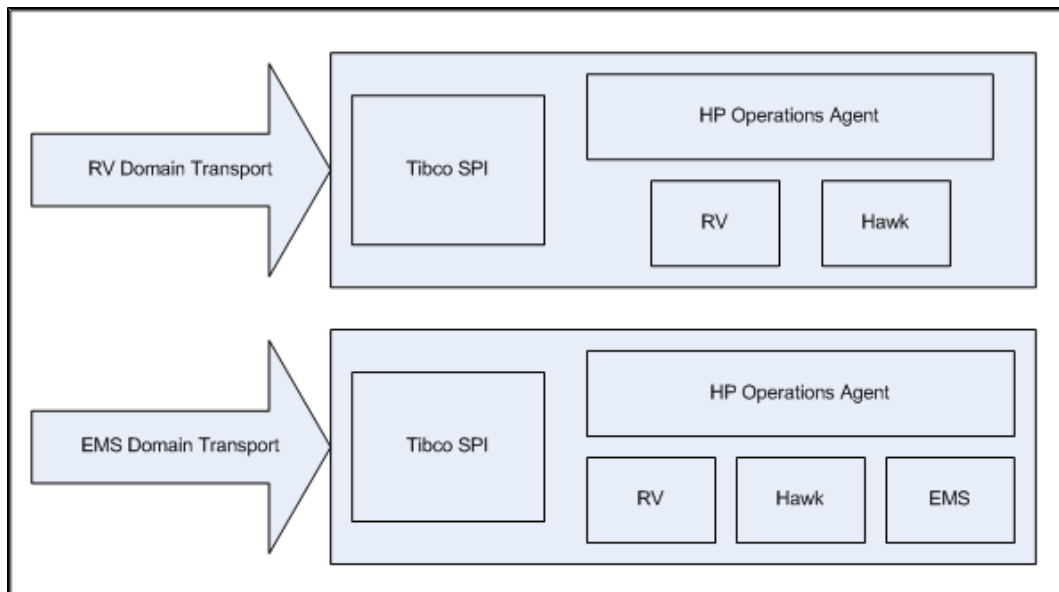
Based on the domain transport the prerequisites are as follows:

- **RV Domain Transport**

For the RV Domain Transport, SPI needs to be deployed on a node where Hawk and RV are available.

- **EMS Domain Transport**

For the EMS Domain Transport, SPI needs to be deployed on a node where Hawk, EMS and RV are available.



List of microagents to be enabled for OOTB metrics to work for TIBCO SPI 2.00

The following microagents should be available along with the corresponding methods:

- **EMS server:** Enable `com.tibco.tibjms.admin.hawk.HawkController` microagent. After enabling a microagent is available with the name `JMS_Controller`. Following methods should be accessible once the microagent is enabled:

`getServerInfo, isRunning` and `getQueues`

- **BW applications:** Applications should be HawkEnabled so that corresponding microagents are available. After enabling a microagent is available with the name `COM.TIBCO.ADAPTER.bwengine`. Following methods should be accessible once the microagent is enabled:

`GetProcessDefinitions,getStatus` and `getHostInformation`

- **RV:** Once RV is installed there should be a microagent by name `TIBCO Rendezvous` available. `onRvDaemonStatus` method should be accessible after the microagent is enabled.

Other microagents which are necessary for TIBCO SPI to work are:

- **Logfile microagent:** `onNewLine` method should be accessible.
- **Self microagent:** `getMicroAgentInfo` method should be accessible.

Optional microagent to be enabled, if required:

- To capture alerts generated by hawkrules: `HawkEventService:<domain_name>` microagent should be enabled.

`onAlert` and `onClear` method should be accessible once the microagent is enabled.

Note: `TIB_hawk_4.9.0_hotfix003` should be installed on all the systems in the domain and also on the system where TIBCO SPI is deployed. This hotfix installation is required because multiple invocation requests the Hawk 4.9 Console API which results in a failure of metric collection.

Steps for Configuring the TIBCO SPI on HPOM for Windows management server

TIBCO SPI does not support data logging in HP Performance Agent. Before deploying the discovery policy go to the managed node where TIBCO SPI is deployed and perform the following steps:

1. Open the `datasources` file from the directory:

Windows: `%ovagentdir%/conf/perf`

HP-UX, Linux, or Solaris: `/var/opt/OV/conf/dsi2ddf`

2. Remove `TIBCO_SPI` from the `datasources` file.
3. Create an empty `nocoda.opt` file in the following directory `%ovdatadir%/conf/dsi2ddf/`
If the folder `dsi2ddf` does not exist, create it.
4. Restart the agent.

This will create the `datasources` in CODA and will also start the discovery of TIBCO SPI.

To complete the TIBCO SPI configuration, complete the following tasks:

1. [Deploy Instrumentation](#)
2. [Update and Deploy Config Policies](#)

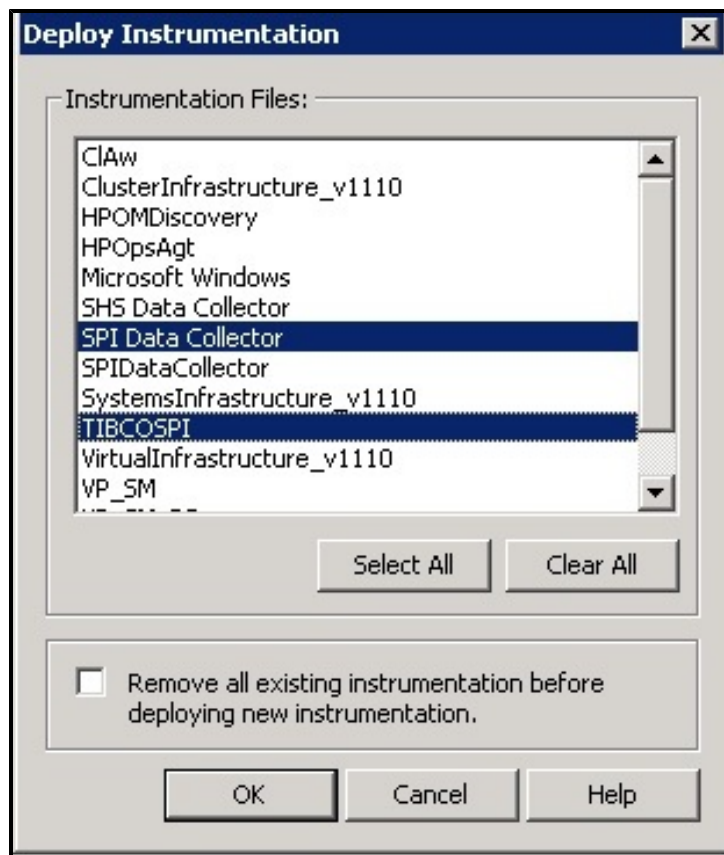
3. Deploy Discovery and Collector Logfile Policies
4. Verify the Discovery Process

Deploy Instrumentation

To deploy instrumentation, follow these steps:

1. From the HPOM console, select **Operations Manager** → **Nodes**.
2. Right-click on the managed node, where TIBCO SPI needs to be deployed.
3. Select **All Tasks** → **Deploy instrumentation**.

Deploy Instrumentation window opens.



4. Select **SPIDataCollector** and **TIBCOSPI** from the list of instrumentation files and click **OK**.

To verify that these files are deployed, check **Policy Management** → **Deployment Jobs**. There must be no error messages.

Update and Deploy Configuration Policies

Discovery Configuration file policy sets the basic configuration properties needed for deploying the TIBCO SPI discovery policies on the managed nodes and updates the service map on the HPOM console.

Step 1: Deploy TIB_OPC_MSG policy

To launch the TIB_OPC_MSG policy, follow these steps:

1. From the HPOM console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO SPI Collector** → **Discovery**.
2. Right-click the managed node on which you want to deploy the TIB_OPC_MSG policy.
3. Select **All Tasks** → **Deploy on**
The Deploy Policy window opens.
4. Select the option, **Select nodes from the tree**. From the managed nodes, select the node on which you want to deploy the policy and click **OK**.

Step 2: Deploy TIB_SPI_OOTBMetricsConfig policy

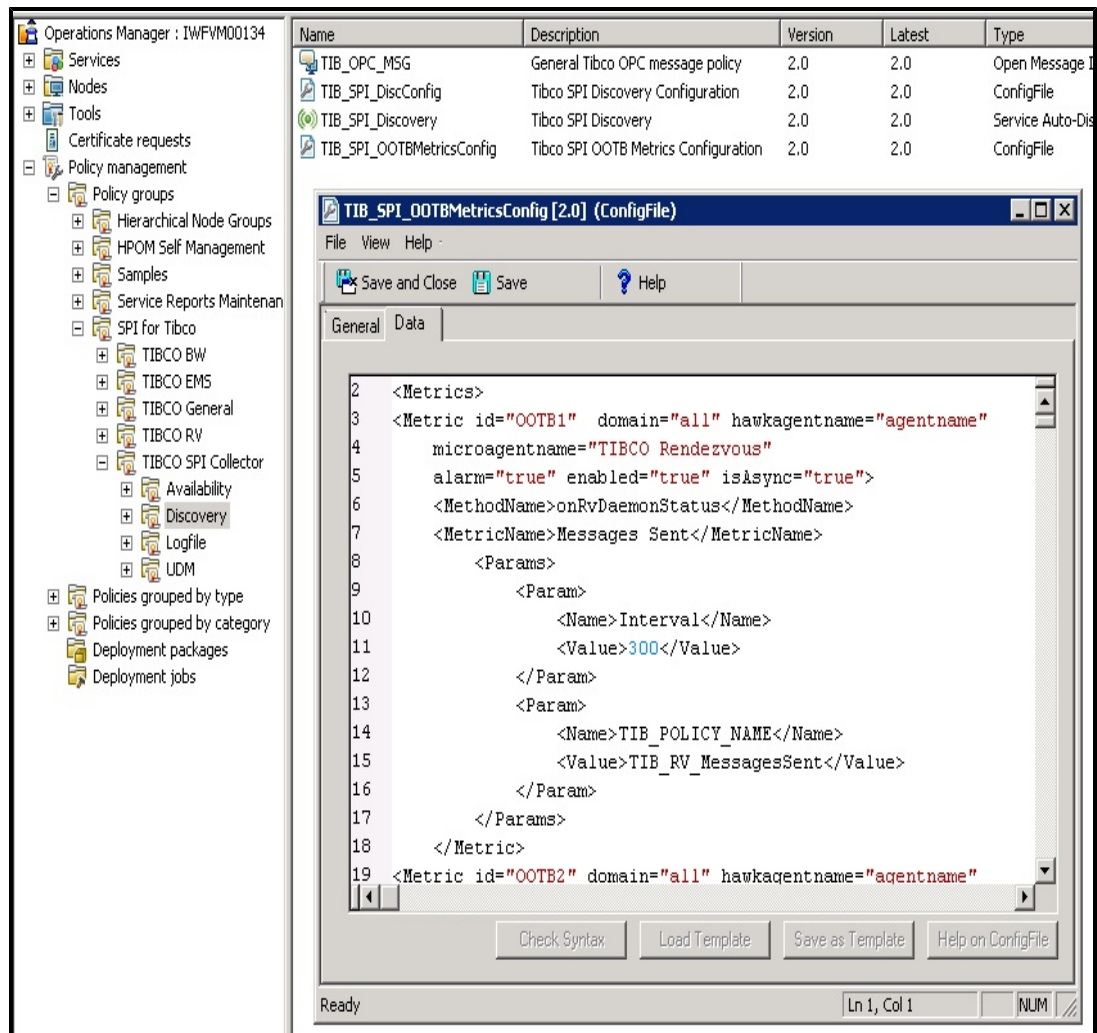
TIB_SPI_OOTBMetricsConfig policy includes metric definitions for the following TIBCO infrastructure elements:

- TIBCO BW
- TIBCO EMS
- TIBCO RV

To start the TIB_SPI_OOTBMetricsConfig policy, follow these steps:

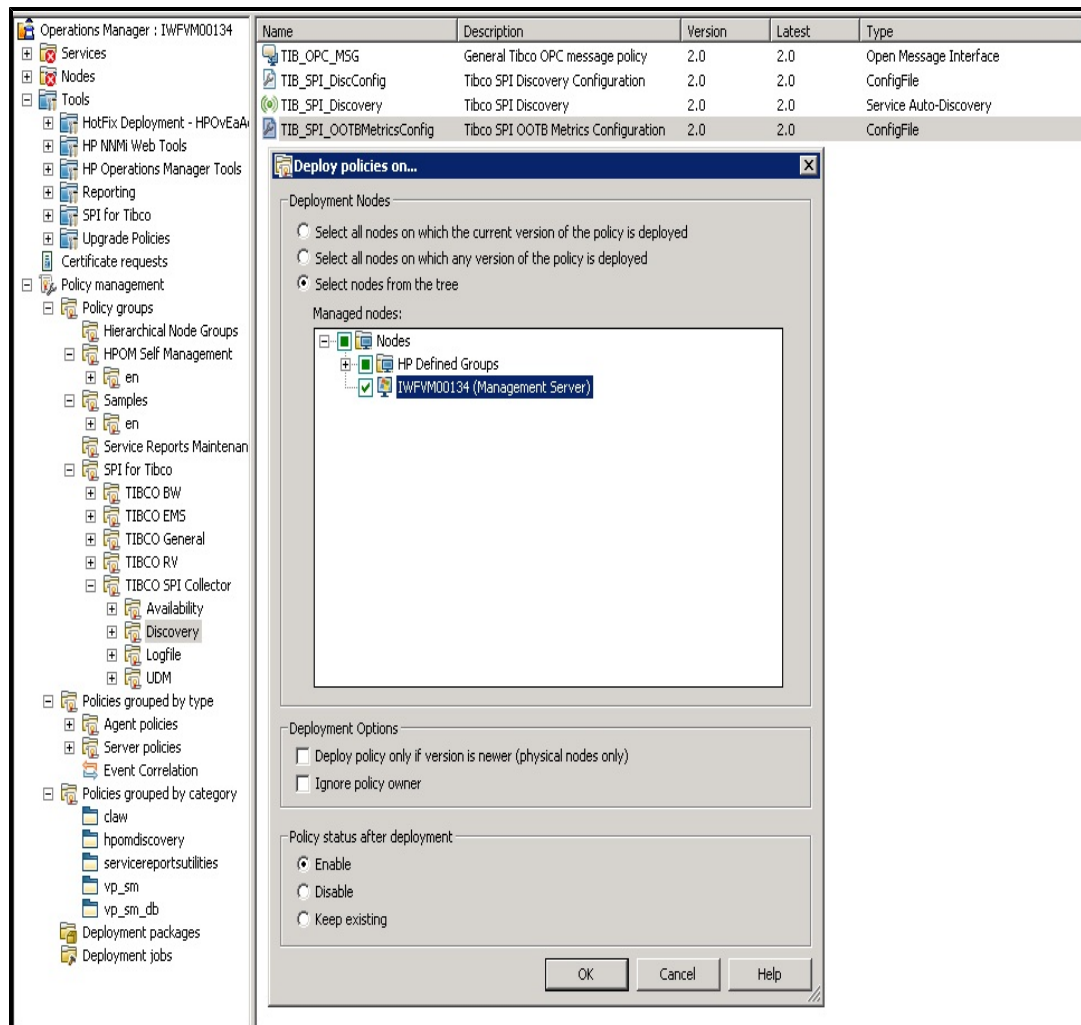
1. From the HPOM console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO SPI Collector** → **Discovery**.
2. Double-click **TIB_SPI_OOTBMetricsConfig**.

The Configuration Editor opens.



3. To change the metrics and RV metrics schedule, see ["Configuring Out-Of-The-Box \(OOTB\) Metrics" on page 58](#). If you do not want to change the RV metrics schedule or disable the metrics, go to step 4.
4. Click **Save and Close** to save any changes and exit the editor.
5. Right-click the managed node on which you want to deploy the TIB_SPI_OOTBMetricsConfig policy.
6. Select **All Tasks** → **Deploy on**

The Deploy Policy window opens.



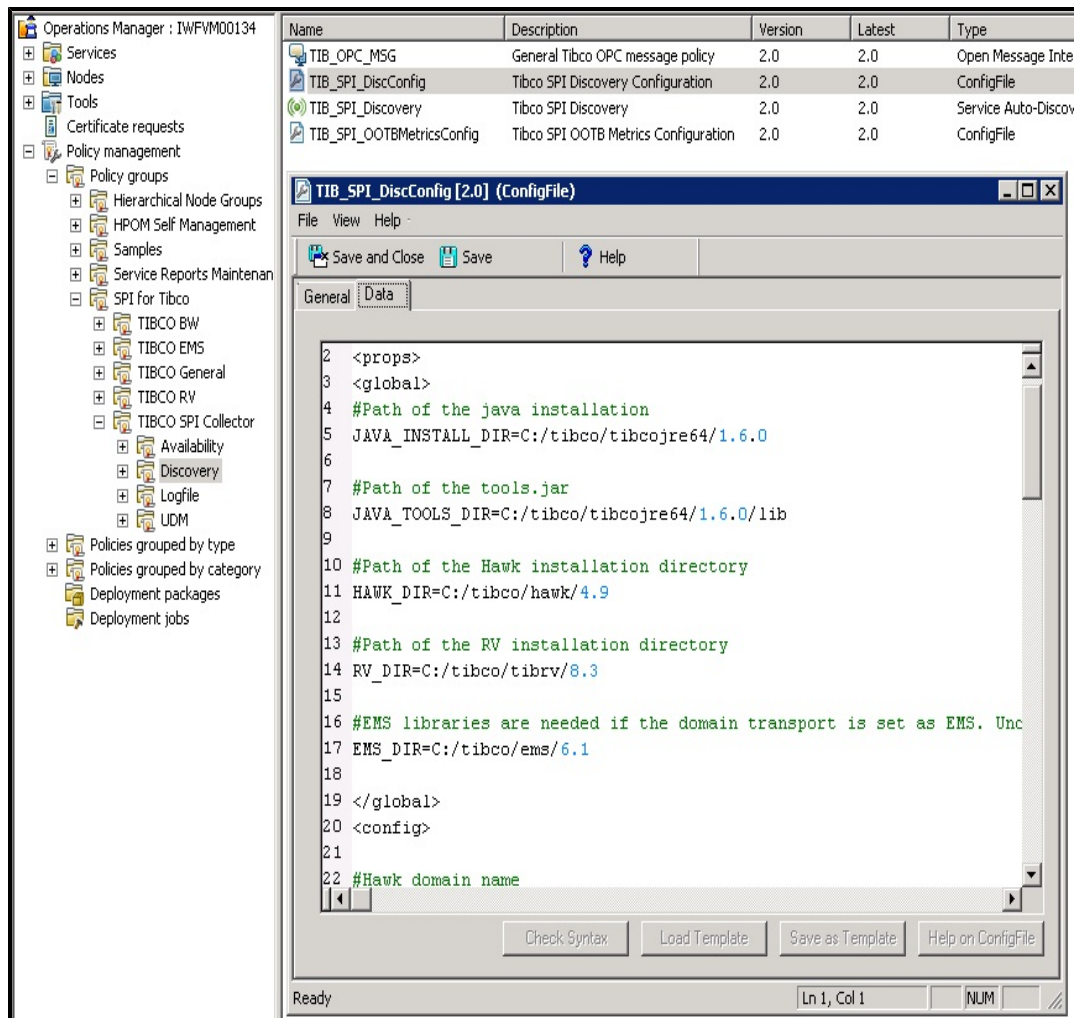
7. Select the option, **Select nodes from the tree**. From the managed nodes, select the node on which you want to deploy the policy and click **OK**.
8. Verify that the tool is launched on the selected node(s) and click **OK**.

Step 3: Update and Deploy TIB_SPI_DiscConfig policy

To deploy the TIB_SPI_DiscConfig policy, follow these steps:

1. From the HPOM console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO SPI Collector** → **Discovery**.
2. Double-click **TIB_SPI_DiscConfig**.

The Configuration Editor opens. Set the values at the global and domain level.



3. The configuration properties that are used at the global level are mentioned below. You can configure them accordingly based on your environment. To enable the field, remove the '#' from the below lines and set the values.

- a. The location of Java installation directory is:

```
JAVA_INSTALL_DIR = C:/tibco/tibcojre64/1.6.0
```

- b. The location of tools.jar directory is:

```
JAVA_TOOLS_DIR = C:/tibco/tibcojre64/1.6.0/lib
```

- c. The location of Hawk installation directory is:

```
HAWK_DIR = C:/tibco/hawk/4.9
```

- d. The location of RV installation directory is:

```
RV_DIR = C:/tibco/tibrv/8.3
```

- e. If the domain is set as EMS, you need to install the EMS libraries.

```
EMS_DIR = C:/tibco/ems/6.1
```

4. Set the configuration properties based on the specific domain level. The parameters must be enclosed within the `<config></config>` block.

- a. Provide the Hawk domain name:

For Example: `HAWK_DOMAIN_ID = Admin (Domain name)`

- b. Hawkagents and Microagents can be included or excluded from discovery and collection based on your selection. Multiple nodes can be separated by using a ",". To enable the field remove the "#" from the beginning of the parameter.

To exclude any hawk agent, remove '#' and 'none' from below line

```
#EXCLUDE_HAWKAGENTS=none
```

For example: `EXCLUDE_HAWKAGENTS=btovm812,btovm12`

To include only a set of hawk agent, remove 'all' from below line

```
INCLUDE_HAWKAGENTS=all
```

For example: `INCLUDE_HAWKAGENTS=btovm812,btovm12`

To exclude any microagent , remove '#' and 'none' from below line

```
#EXCLUDE_MICROAGENTS=none
```

For example: `EXCLUDE_MICROAGENTS=Process,System`

To include only a set of microagent , remove 'all' from below line

```
INCLUDE_MICROAGENTS=all
```

For example: `INCLUDE_MICROAGENTS=JMS_Controller
(tcp://localhost:7222), TIBCO Rendezvous`

- c. RV is used as the domain transport.

If RV is used as the domain transport, enter the values for `RV_SERVICE`, `RV_NETWORK`, and `RV_DAEMON`. The default values are mentioned below. These are TIBCO Hawk parameters. Remove the '#' from the below lines and set the value.

```
#RV_SERVICE=7474
```

```
#RV_NETWORK=;
```

```
#RV_DAEMON=tcp:7474
```

- d. EMS is used as the domain transport.

If EMS is used as the domain transport, remove the '#' from the below line and set the value.

```
#EMS_URL=(tcp|ssl)://(hostname):(port)
```

For Example:

```
For tcp: EMS_URL=tcp://x86vm455:7222
```

```
For ssl: EMS_URL=ssl://x86vm455:7222
```

Note: If there is a failover in the EMS domain you need to set the EMS url as:

```
EMS_URL = (tcp|ssl)://(hostname1):(port), (tcp|ssl)://
(hostname2):(port),
(tcp|ssl)://(hostname3):(port) and so on.
```

where hostname1 is the primary EMS and hostname2, hostname3 are secondary EMS.

- e. EMS is used as the domain transport and SSL is enabled.
 - i. If EMS is used as the domain transport and SSL is enabled, remove the '#' from the below lines and set the values.

For Example:

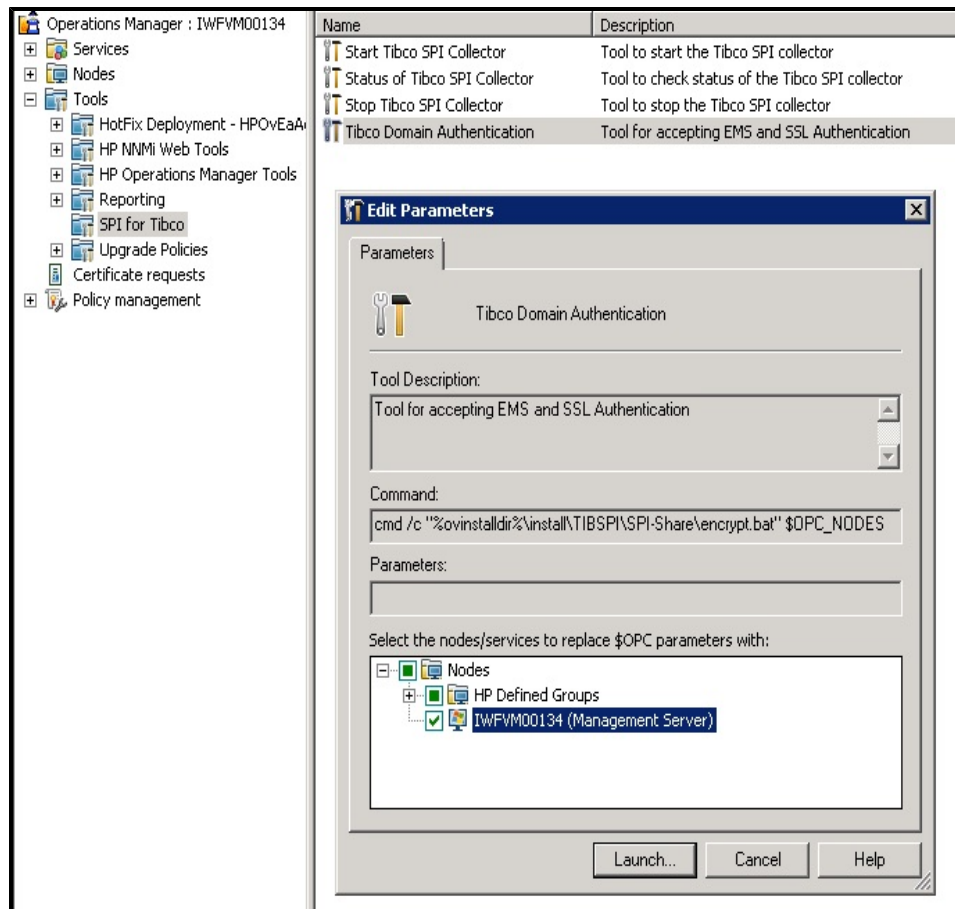
```
#SSL_TRACE = TRUE|FALSE
#SSL_VENDOR = j2se-default
#SSL_VERIFY_HOST = TRUE|FALSE
#SSL_TRUSTED = C:\tibco\ems\samples\certs\server_root_
cert.pem
#SSL_VERIFY_HOSTNAME = TRUE|FALSE
#SSL_EXPECTED_HOSTNAME: Expected name of the CN field of the
server certificates.
#SSL_IDENTITY = C:\tibco\ems\samples\certs\client_
identity.p12
#SSL_PRIVATE_KEY = C:\tibco\ems\samples\certs\client_
identity.p12
#SSL_CIPHERS = -ALL:+RC4-MD5:+DES-CBC-SHA:&lt;DES-CBC3-
SHA
```

Note: If `SSL_TRUSTED` contains multiple trusted certificates it should be separated by ","

For more information, see *TIBCO_HAWK_INSTALLATION_AND_CONFIGURATION_GUIDE* → "Chapter 7 Using the Configuration Utility" → "Connecting to TIBCO EMS using SSL". For the list of supported CIPHERS, see *EMS User Guide* → "Chapter 18: Using the SSL Protocol" → "Configuring SSL in EMS clients".

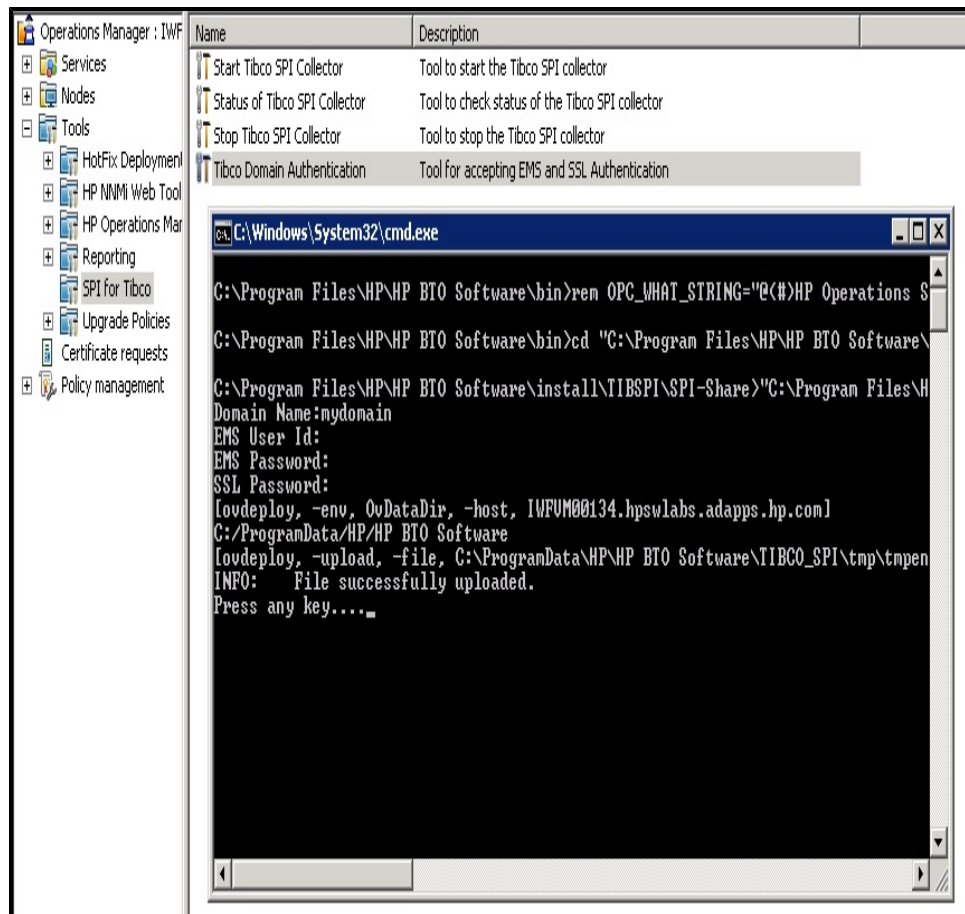
- ii. Click **Save and Close** to save any changes and exit the editor.
- iii. From the HPOM console, **Select Tools** → **SPI for Tibco** → **Tibco Domain Authentication**.

The Edit Parameter window opens.



- iv. Select the managed node and click **Launch**.

In the command prompt enter the Domain Name, EMS User Id, EMS Password, and SSL Password. If you leave the EMS password or SSL password blank, the credentials will still be deployed on the node.



You have to run **Tibco Domain Authentication** tool for each domain which has EMS/SSL passwords configured.

Note: To monitor multiple domains, copy and paste the `<config>` block for each domain in the **TIB_SPI_DiscConfig** policy. If n domains have to be monitored, there must be n `<config>` blocks that is one `<config>` block for each domain in the **TIB_SPI_DiscConfig** policy.

5. Click **Save and Close** to save any changes and exit the editor.

Deploy Discovery and Collector Logfile Policies

Before deploying the discovery policy, you must deploy all SPI opc message policies so that unnecessary alerts don't reach the OM server.

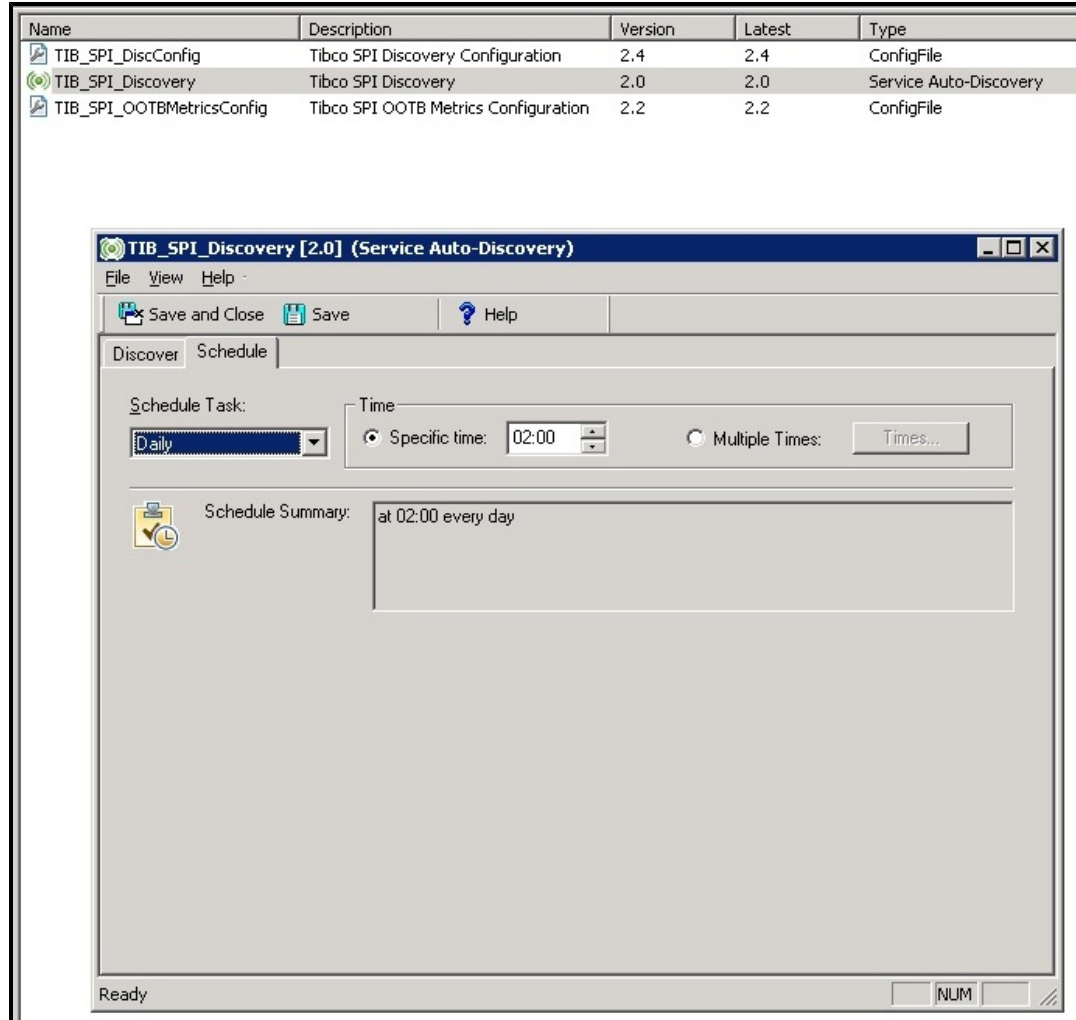
To deploy the discovery and collector logfile policies, follow these steps:

Step 1: Deploy TIB_SPI_Discovery policy:

The TIB_SPI_Discovery policy starts the discovery as well as the collector. To launch the TIB_SPI_Discovery policy, follow these steps:

1. From the HPOM console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO SPI Collector** → **Discovery**.
2. Double click **TIB_SPI_Discovery**.

The Auto-Discovery window opens.



3. Select **Schedule** → **Schedule Task**. Schedule the task as per your requirement.
4. Click **Save and Close** to save any changes.
5. From the managed nodes, select the node on which you want to deploy the policy and click **OK**.
6. After the discovery is completed, you will receive a message on the HPOM console stating the discovery is successful.

Note: It might take several minutes to discover the whole domain based on the domain size.

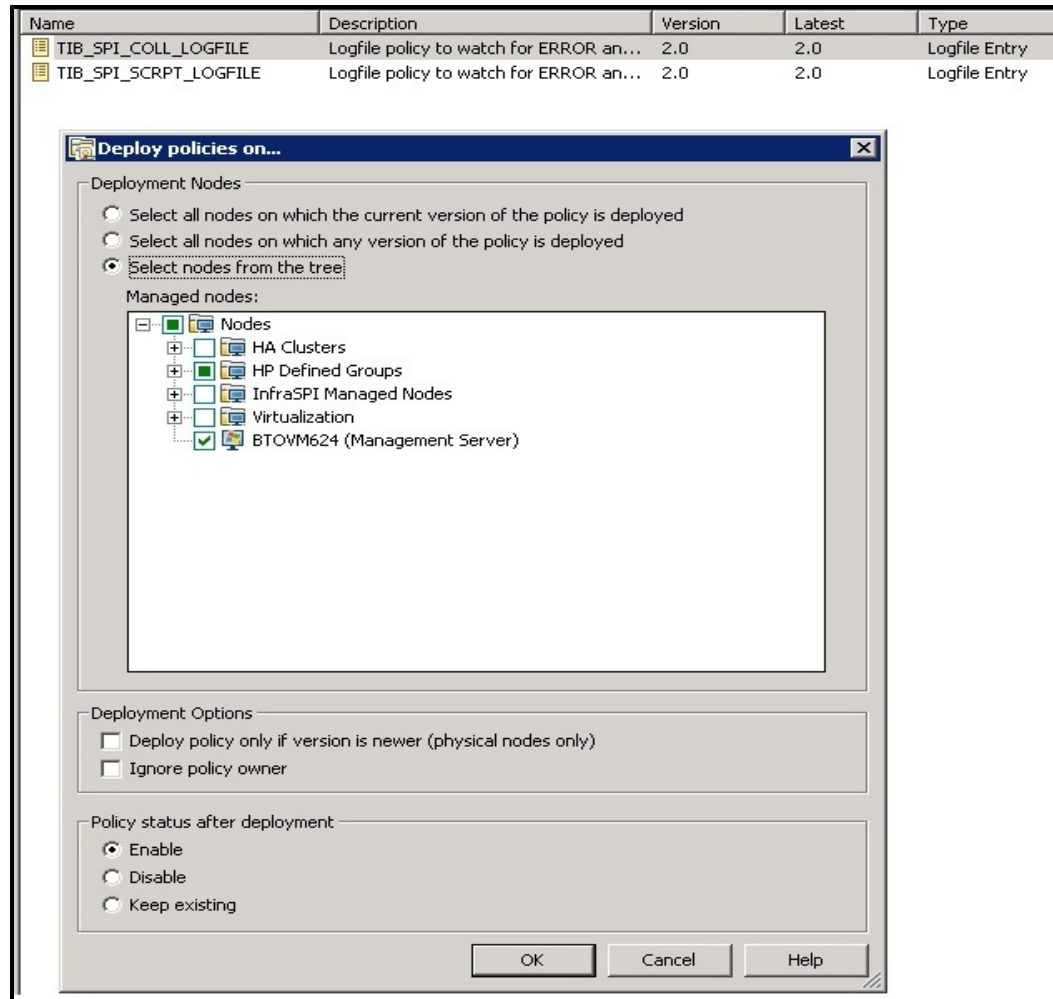
Step 2: Deploy Logfile Policies

The logfile policies monitor the logfiles created by TIBCO SPI. The information from these logfiles includes changes to the configurations and errors that occur in the operations of the TIBCO SPI.

To launch the logfile policies, follow these steps:

1. From the HPOM console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO SPI Collector** → **Logfile**.
2. Right-click the managed node on which you want to deploy the logfile.
3. Select **All Tasks** → **Deploy on**.

The Deploy Policy window opens.



4. Select the option, **Select nodes from the tree**. From the managed nodes, select the node on which you want to deploy the policy and click **OK**.
5. Verify that the tool is launched on the selected node(s) and click **OK**.

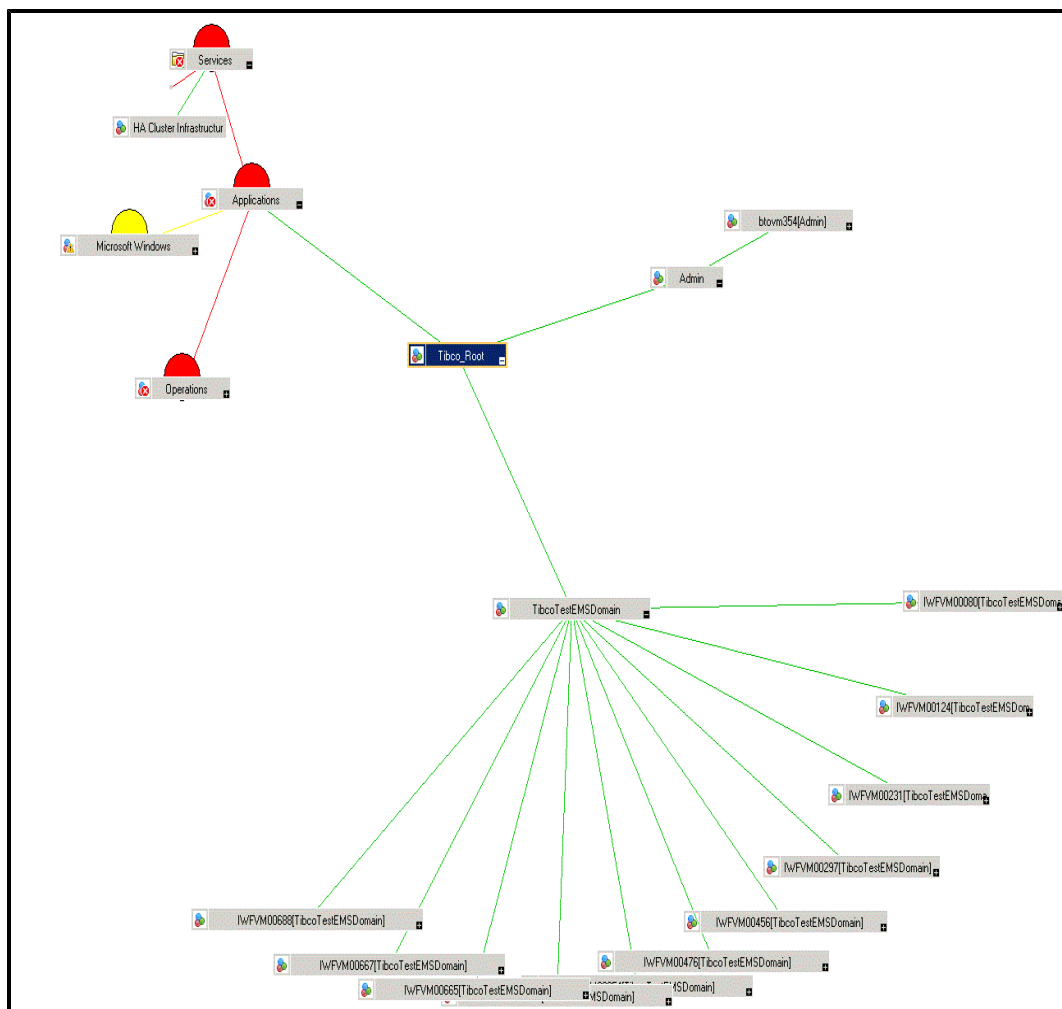
Verify the Discovery Process

Verification might take several minutes to complete, depending on the number of managed nodes in your environment.

1. After the discovery is completed, there would be a discovery successful message in the message browser.

There would be a message like `Discovery completed successfully for SPI_TEST, MyDomain` in the message browser.

- The lines in the service map are color coded to show various levels of severity. For example, red lines show that the application has critical problems and the green lines show that the application is healthy.



3. The discovery service map should get updated with the TIBCO environment details such as:
 - a. Servers in TIBCO environment.
 - b. BW Applications in TIBCO environment.

- c. EMS services.
 - d. RV services
4. To check the error messages from the collector log files, go to **Policy Management** → **Deployment Jobs**. The SPI is deployed if it contains no error messages.

Steps for Configuring the TIBCO SPI On HPOM for UNIX Management Server

Prerequisites

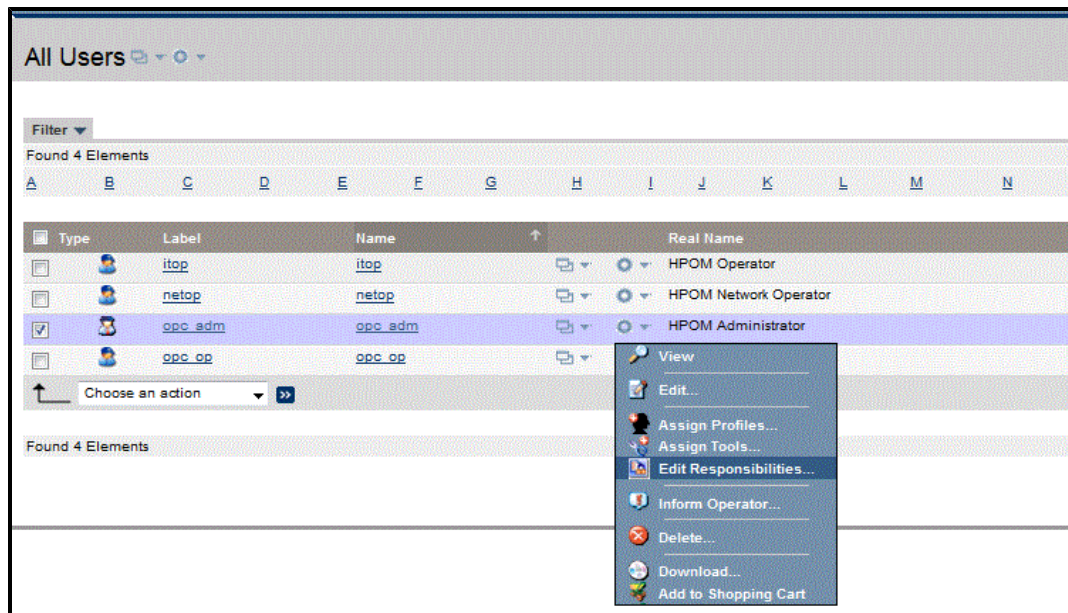
Log on to HPOM as an administrator. The Administration UI window opens. Complete the following tasks before configuring the TIBCO SPI:

- [Assign Operator Responsibilities for User](#)
- [Assign Tools to the Operator](#)
- [Assign Service Tree](#)


Assign Operator Responsibilities for User

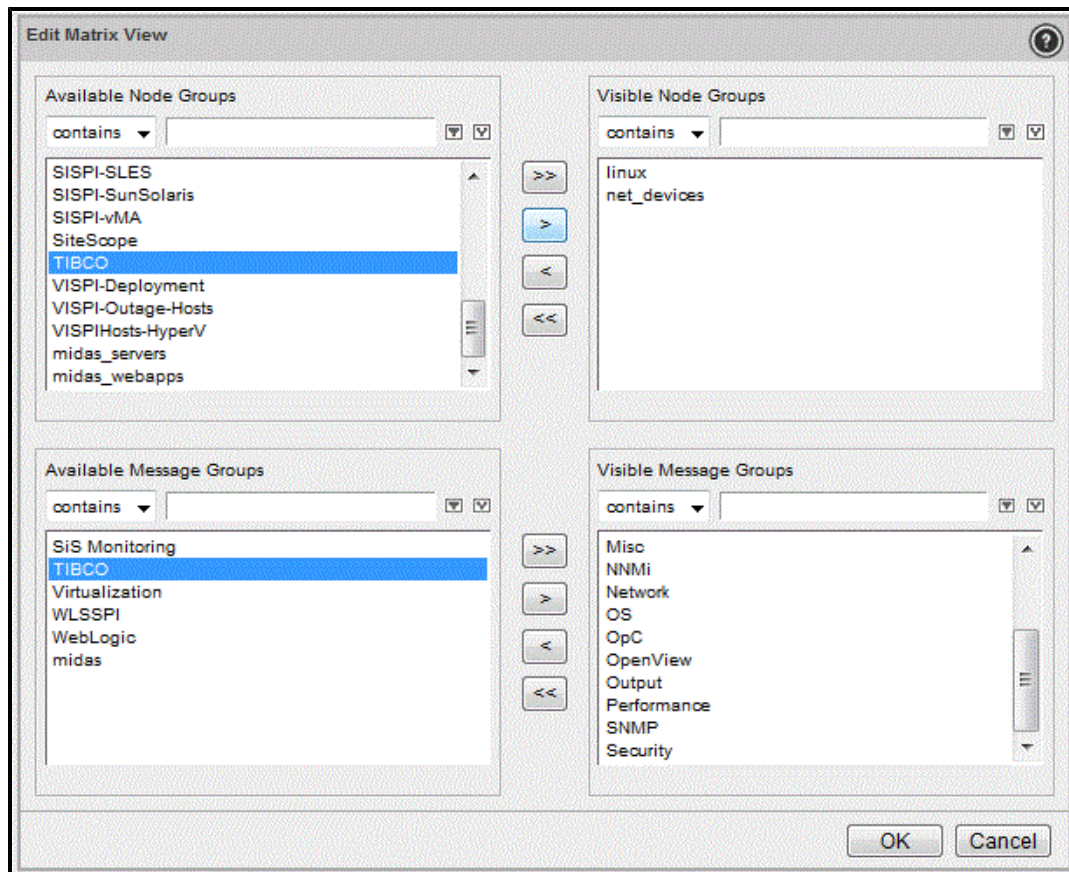
To assign operator responsibilities for `opc_adm`, follow these steps:

1. Select **All Users** → **opc_adm**.
2. To change a user's responsibility, select **Edit Responsibilities....** from the drop-down list as shown in the following figure.



3. The Edit Responsibilities window opens. If TIBCO does not appear in the Message Groups or Node Groups, go to step 4 else go to step 5.
4. Select **Edit View**. The Edit View matrix window opens.

Select **TIBCO** from the Available Node Groups and Available Message Groups and using  move it to the Visible Node Groups and Visible Message Groups as shown below:



5. Select all check boxes for TIBCO Message Groups.

Edit Responsibilities for User "opc_adm"

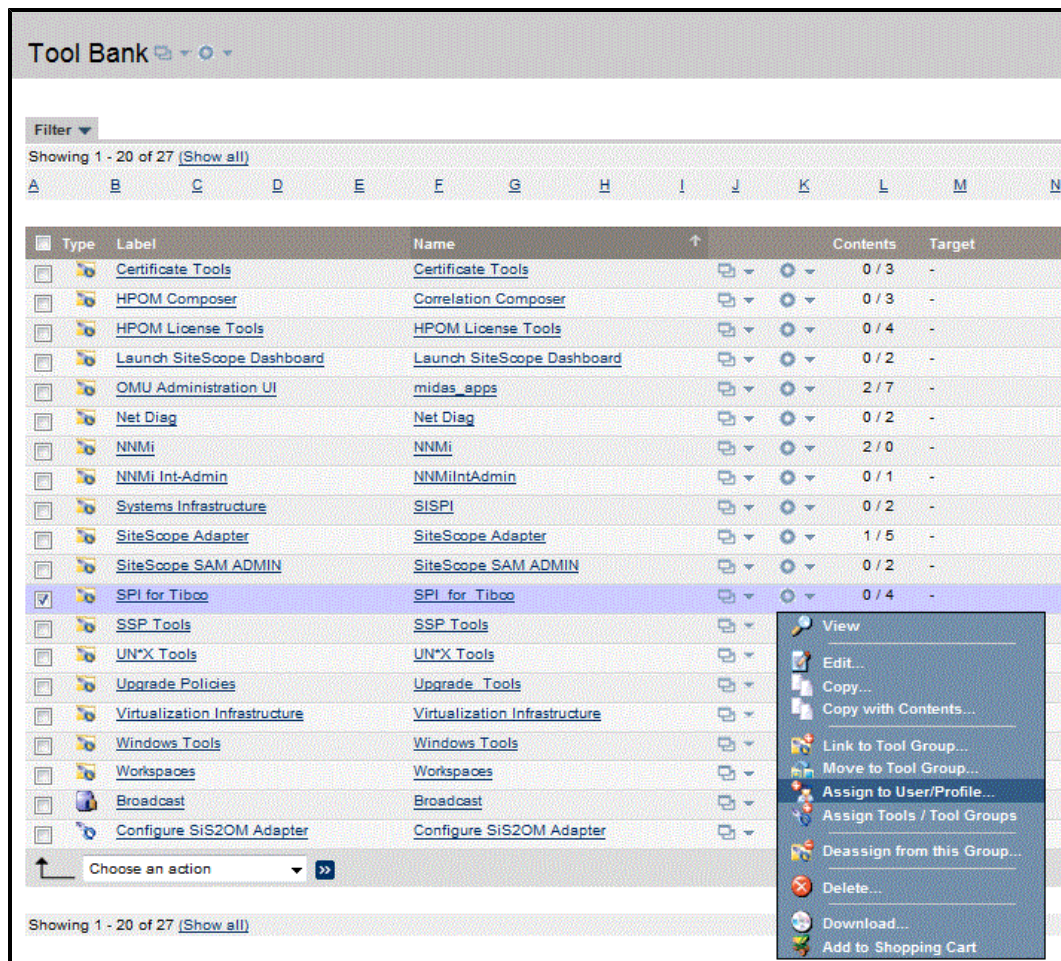
Node Groups [30]	linux	net_devices	TIBCO
Message Groups [22]			
Backup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Database	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Hardware	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Job	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Misc	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Network	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NNMi	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
OpC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
OpenView	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
OS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Output	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Performance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SNMP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TIBCO	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

6. Click **Close**.

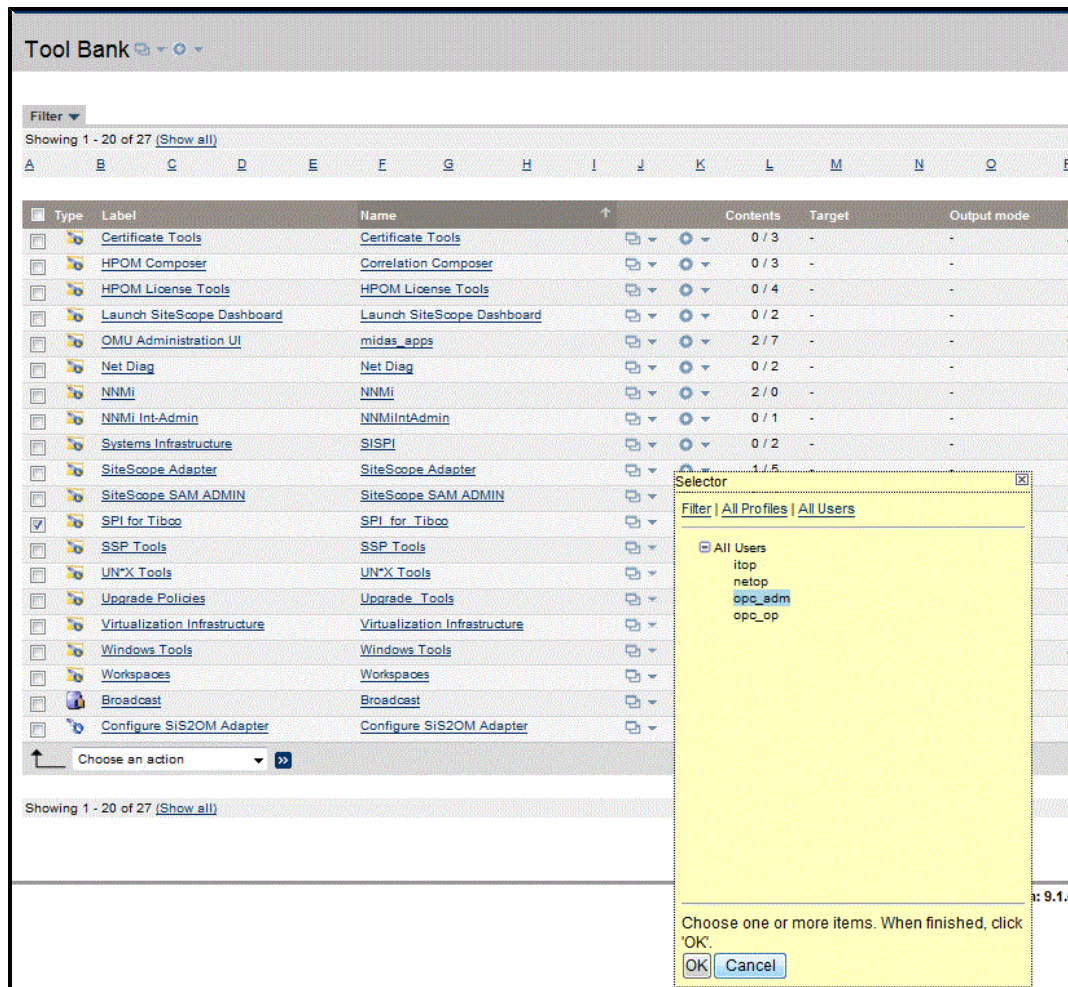
Assign Tools to the Operator

To assign tools to the operator, follow these steps:

1. Click **Browse** → **Tool Bank**. In the Tool Bank window select **SPI for Tibco**.



2. Select **Assign to User/Profile...** from Choose an Action drop-down list and click **>>** to submit. The Selector window opens.
3. In the Selector window, click **All Users** tab.
4. Select the operator to which you want to assign the tools.



5. Click **OK**. The tools are assigned to the operator.

Assign Service Tree

You must run the following command on the management server for the Service Tree to appear in the Java Interface.

```
opcservice -assign opc_admin Tibco_Root
```


Configuration Steps:

To configure the TIBCO SPI from the management server, you must complete the following tasks.:

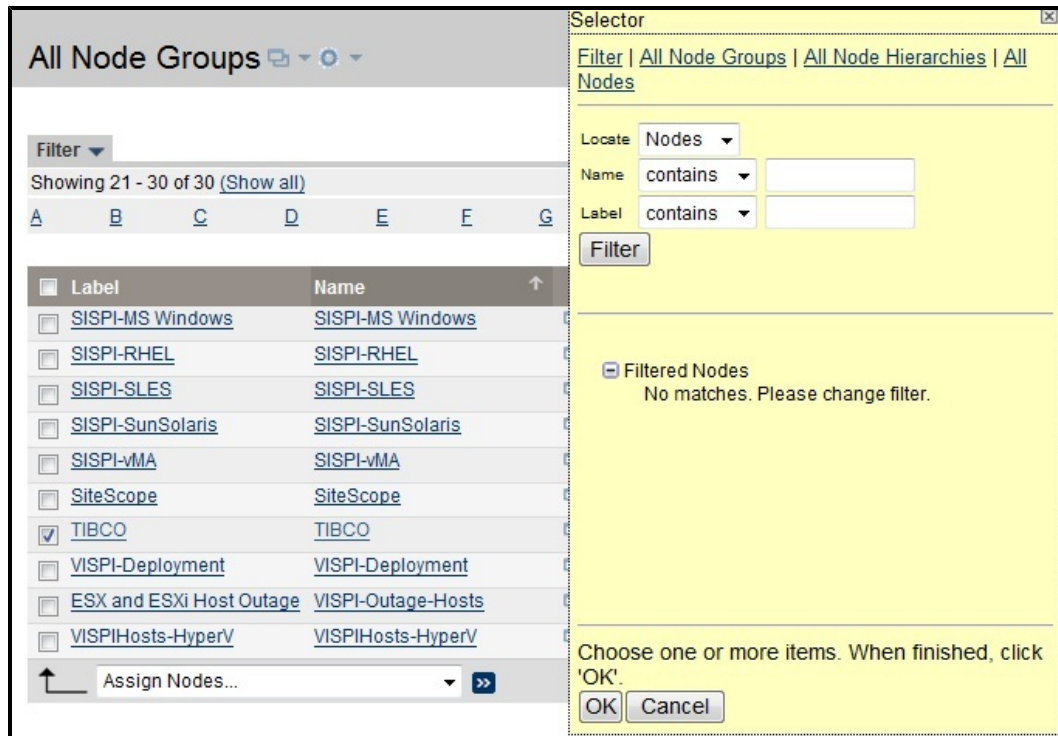
1. [Add Nodes to the TIBCO Node Group](#)
2. [Assign Categories to the Managed Node](#)
3. [Deploy Instrumentation on the Managed Node](#)
4. [Assign Policies to the Managed Node](#)
5. [Verify the Discovery Process](#)

Add Nodes to the TIBCO Node Group

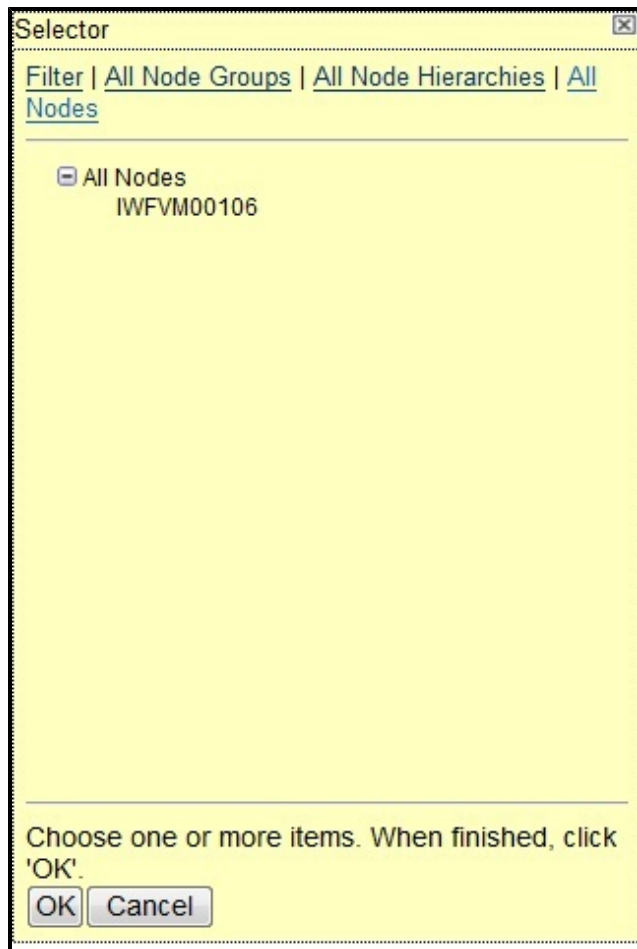
The TIBCO SPI automatically creates the TIBCO node group with preassigned policy groups. To place all nodes running in the TIBCO Application Server in the node group follow these steps:

1. Open the All Node Groups window and select the TIBCO Node Group.
2. Select **Assign Nodes...** from the  drop-down list.

The Selector window opens.




3. Click **All Nodes**.
4. Select the nodes running on the TIBCO Application Server.



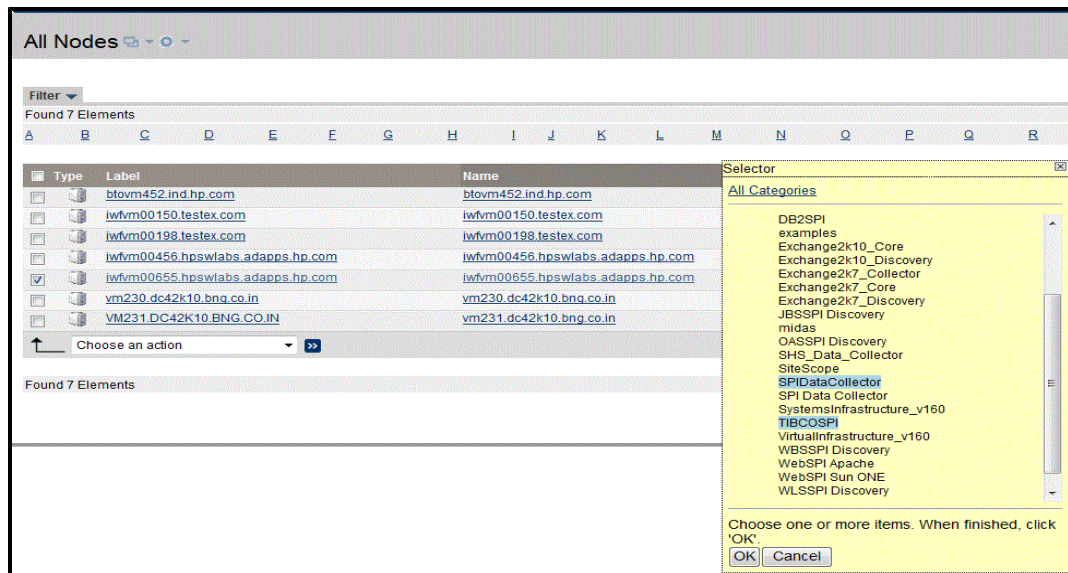
5. Click **OK** to add nodes to the TIBCO Node Group.

Assign Categories to the Managed Node

To assign categories to the managed node:

1. Open All Nodes window and select the managed nodes.
2. Select **Assign Categories...** from the  drop-down list.


The Selector window opens.

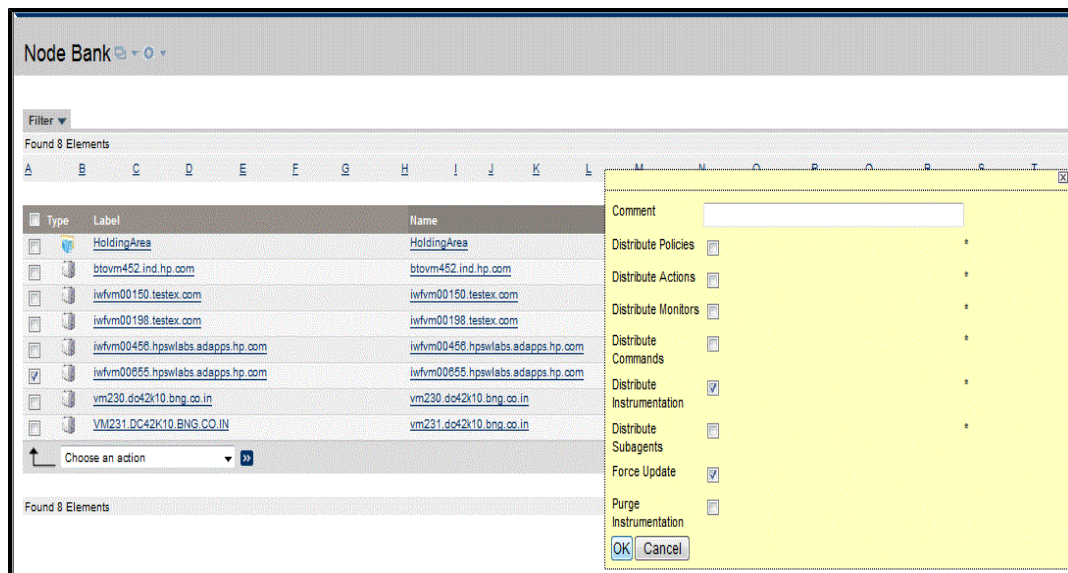


3. Select **SPIDataCollector** and **TIBCOSPI** from All Categories tab.
4. Click **OK** to assign categories to the managed node.

Deploy Instrumentation on the Managed Node

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


1. Open the Node Bank window and select the management server.
2. Select **Deploy Configuration...** from the  drop-down list.



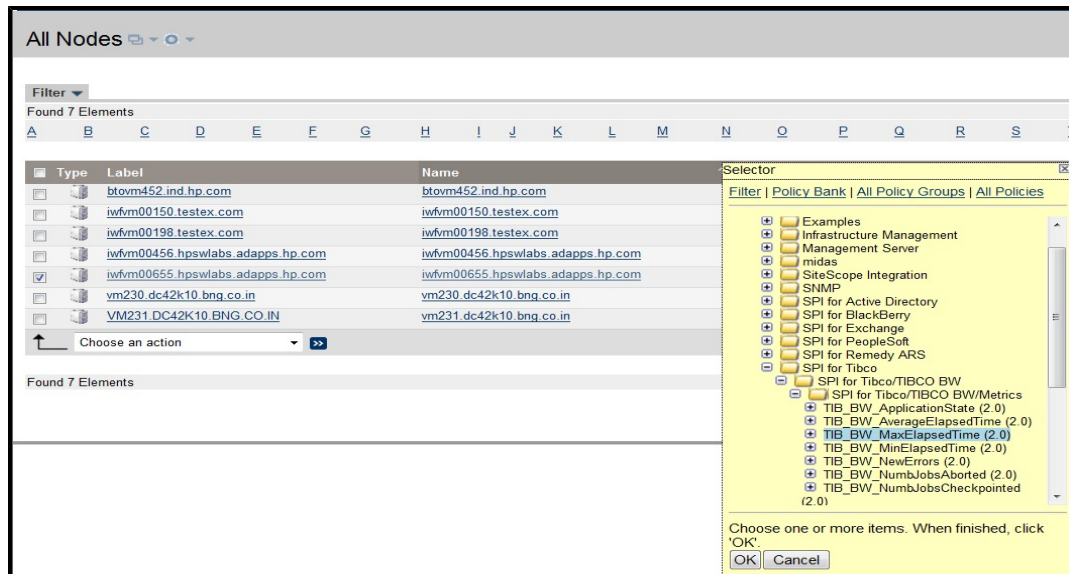
3. Select **Distribute Instrumentation** and **Force Update** by selecting the check box.
4. Click **OK** to deploy the instrumentations on the managed node.

Assign 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  drop-down list.

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** to deploy the policies on the managed node.

Verify the Discovery Process

Verification might take several minutes to complete, depending on the number of managed nodes in your environment.

To verify that the discovery process is completed, follow these steps:

1. After the discovery is completed, there would be a discovery successful message in the message browser.

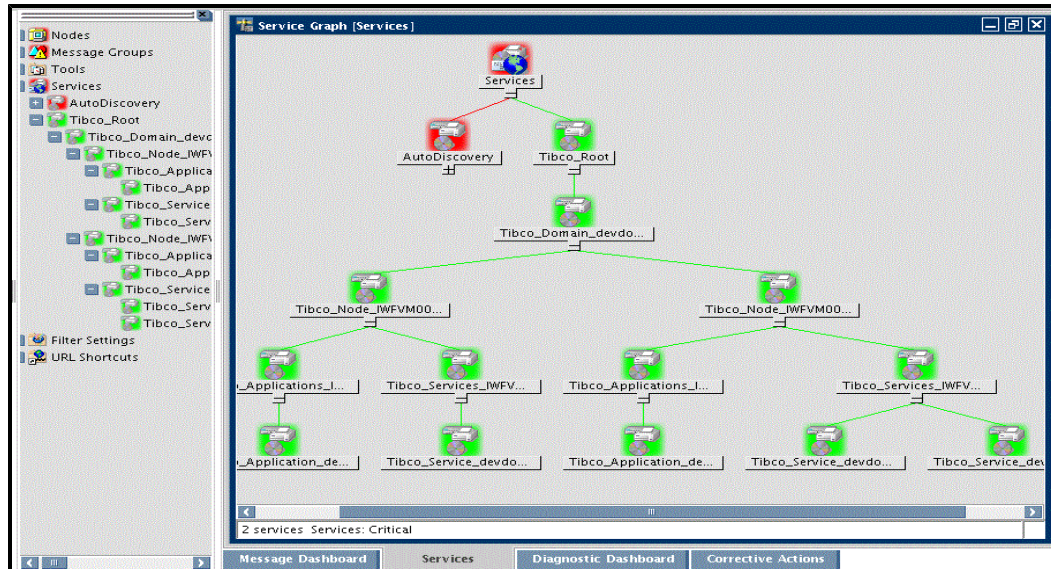
For example: TIBCO SPI is configured for three domains *MyDomain*, *TestDomain*, and *SPI_TEST*. Suppose the discovery is completed for *MyDomain* and *SPI_TEST* and has failed for *TestDomain*.

There would be a message like `Discovery completed successfully for SPI_TEST, MyDomain` in the message browser.

2. When the discovery is successful, the following Service Map appears on the Java interface.

Using the Discovery Service Map, you can find out if any application or services have a problem.

The lines in the Service Map are color coded to show various levels of severity. For example, red lines show that the application has critical problems and the green lines show that the application is healthy.



3. The discovery service map should get updated with the TIBCO environment details such as:
 - a. Servers in TIBCO environment.
 - b. BW Applications in TIBCO environment.
 - c. EMS services.
 - d. RV services.

Configuring Out-Of-The-Box (OOTB) Metrics

To configure OOTB Metrics, you need to update specific parameters in the following order:

1. [Edit the Metric Policy](#)
2. [Create and Deploy the Metric Monitoring Policy](#)
3. [Schedule the Metric](#)
4. [Verification](#)

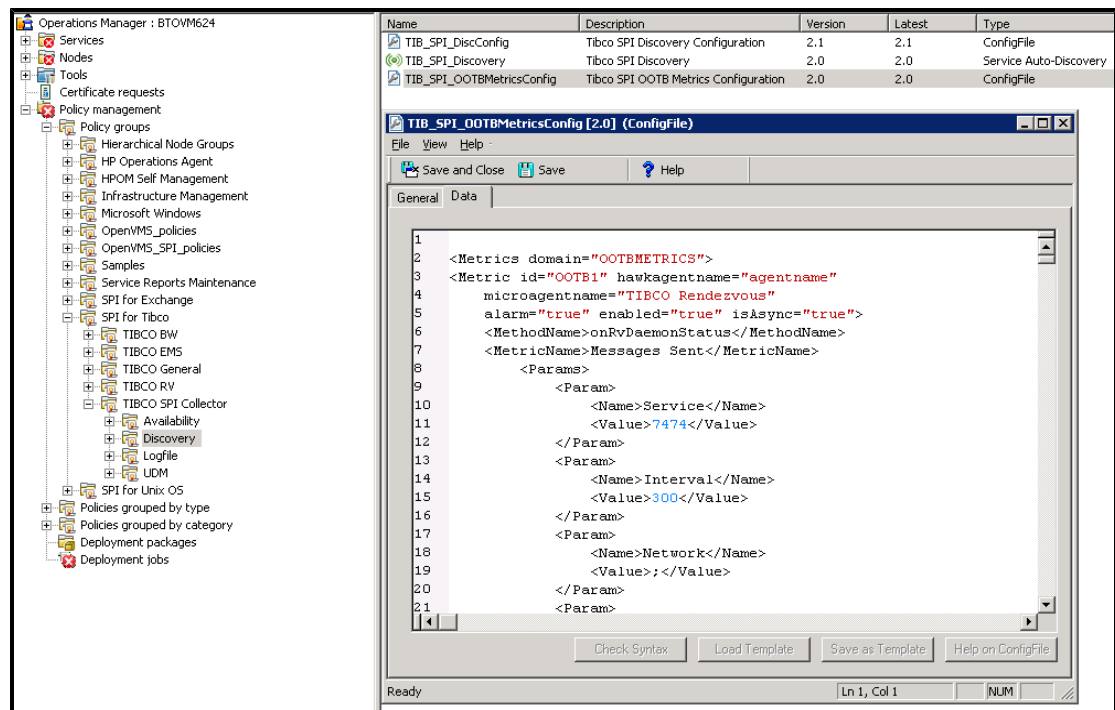
Edit the Metric Policy

1. **On HPOM for Windows:** From the console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO SPI Collector** → **Discovery**.

On HPOM for UNIX: From the Administration UI, select **Policy Bank** → **SPI for Tibco** → **TIBCO SPI Collector** → **Discovery**.

2. Double click **TIB_SPI_OOTBMetricsConfig**.

The Configuration Editor opens.



On HPOM for UNIX: Select **Edit (Raw Mode)...** from the drop-down list . The Edit ConfigFile Policy "TIB_SPI_OOTBMetricsConfig" opens. You can update the metric in the **Content** tab.

3. RV metrics are defined based on **Service**, **Network**, **Daemon** and **Interval** parameters. Depending on the metric type, enter the attributes of the parameters defined.

- a. By default, TIBCO SPI sets the following values to these parameters:

Service: 7474

Network: ;

Daemon: tcp:7474

- b. If a domain with RV domain transport is configured with below parameters:

RV_SERVICE= 1747

RV_NETWORK=;

RV_DAEMON=tcp:1747

then TIBCO SPI will automatically configure RV metrics with the below parameters:

Service=1747

Network=;

Daemon=tcp:1747

Note: If RVD is not running on non-default ports you have to edit the policy and

change the port numbers to the non-default port numbers.

- c. If you want to add OOTB metric for a specific domain, update the metric definition as follows:

The `domain` attribute in the `<Metric></Metric>` block for the required metric has to be updated with the required domain name in the **TIB_SPI_DiscConfig** policy.

For example: To configure `pendingMessageCount` only for EMS servers in the domain *MyDomain* out of the two domains *MyDomain* and *SPI_TEST*, you need to update the metric definition in the **TIB_SPI_DiscConfig** policy as follows:

```
<Metric id="OOTB29" domain="MyDomain" hawkagentname="agentname"
  microagentname="JMS_controller"
  enabled="true" isAsync="false">
  <MethodName>getServerInfo</MethodName>
  <MetricName>pendingMessageCount</MetricName>
  <Params>
    <Param>

        <Name>TIB_POLICY_NAME</Name>

        <Value>TIB_EMS_PendingMsgCount</Value>
    </Param>
  </Params>
</Metric>
```

4. Click **Save and Close** to save any changes and exit the editor.
5. Right-click the managed node on which you want to deploy the **TIB_SPI_OOTBMetricsConfig** policy.
6. Select **All Tasks** → **Deploy on**.
The Deploy Policy window opens.
7. Select the option **Select nodes from the tree**. From the Managed Nodes, select the managed node on which you want to deploy and click **OK**.

The description of the properties used in the metrics are given below:

Metric Properties Description

Property	TIBCO SPI Requirements	Description
id	Required	The format for the Metric id is OOTB [1-9]+. For Example : <Metric id="OOTB1">
alarm	Conditional Required if you want an alert for data logging.	alarm property is used to receive an alert on the HPOM console. By default, the value for this property is set to "false". For Example : <alarm="true">

Property	TIBCO SPI Requirements	Description
enabled	Required Required if you want to configure a particular metric.	This property is used to enable or disable the metric block. The value of this property is either "true" or "false". For Example : <enabled="true">
isAsync	Conditional	This property is required if you want to configure an asynchronous metric. isAsync property is set to "true", if it is an Asynchronous metric. For synchronous metric you can either set the value to "false" or remove the property. By default, the value of this property is set to "false". For Example: <isAsync="true">
MethodName	Required	This parameter is used to call the name of the method run by the microagent. For Example: <MethodName>onRvDaemonStatus</MethodName>
MetricName	Required	Metric name is used to store or query any result of the calculated metric. For Example: <MetricName>Messages Sent</MetricName>
TIB_POLICY_NAME	Conditional	This parameter takes the policy name as a value used for the metric. For Example: <Name>TIB_POLICY_NAME</Name> <Value>TIB_RV_MessagesSent</Value> If this parameter is not mentioned then TIBCO SPI would determine the policy name as TIBCO_<metric id>. For example: If Metric id is 00TB29 then SPI would determine the policy name as TIBCO_00TB29.
domain	Required	This property is used to configure a metric for a domain. If the metric is required for a particular domain the value of this property should be set to the target domain name. For Example: domain = "SPI_TEST". If a metric should be defined for all the configured domains then the value of this property should be set "all".

Create and Deploy the Metric Monitoring Policy.

To create a new measurement threshold policy with the required policy name, any existing policy can be copied and renamed. This enables you to keep custom policies separate from the original default policies.

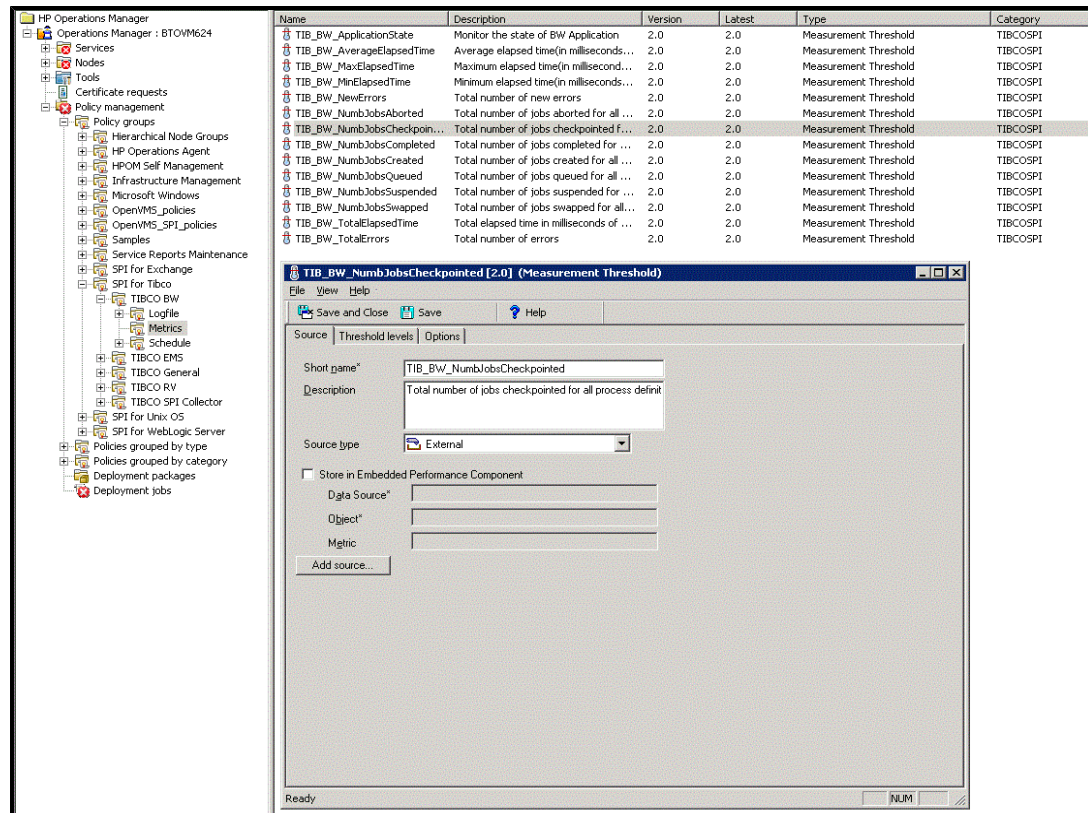
Follow these steps to create a new measurement threshold policy:

1. **On HPOM for Windows:** From the console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO BW** → **Metrics**. Double click any one of the existing threshold policy.

Alternatively, you can also right-click on the HPOM console and select **New** → **Measurement Threshold**.

On HPOM for UNIX: From the Administration UI, select **Policy Bank** → **SPI for Tibco** → **TIBCO BW** → **Metrics**.

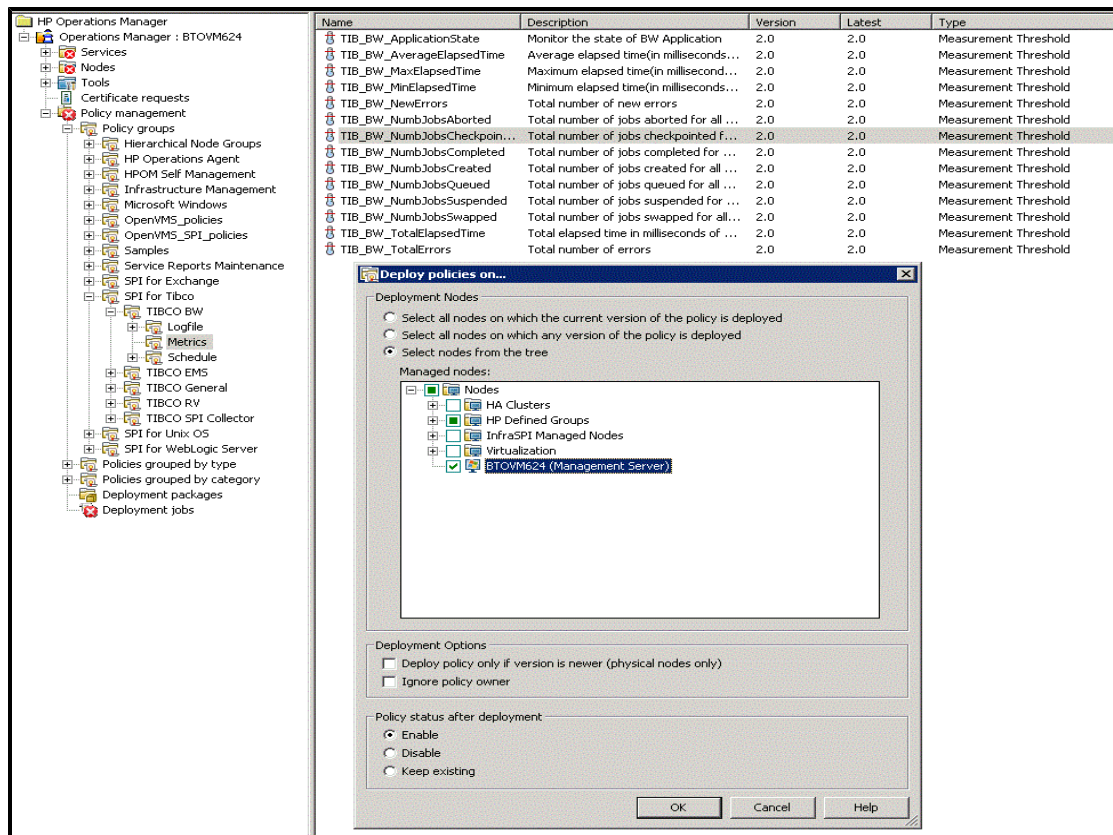
2. The measurement threshold window opens.



On HPOM for UNIX: Select **Copy...** from the drop-down list . The Copy Policy opens.

3. Enter the following values:
 - a. In the Source tab, enter the Short name and Description.
 - b. In the Threshold level tab, enter the values for the threshold limit.
4. Provide an appropriate policy name and click **Save and Close** to save any changes and exit.
5. Right-click the managed node on which you want to deploy the measurement threshold policy.
6. Select **All Tasks** → **Deploy on**.

The Deploy Policy window opens.



7. Select the option, **Select nodes from the tree**. From the list of managed nodes, select the node on which you want to deploy the policy and click **OK**.

Schedule the Metric

To create a new schedule metric, any existing schedule can be copied and renamed. This enables you to keep custom schedules separate from the original default schedule tasks.

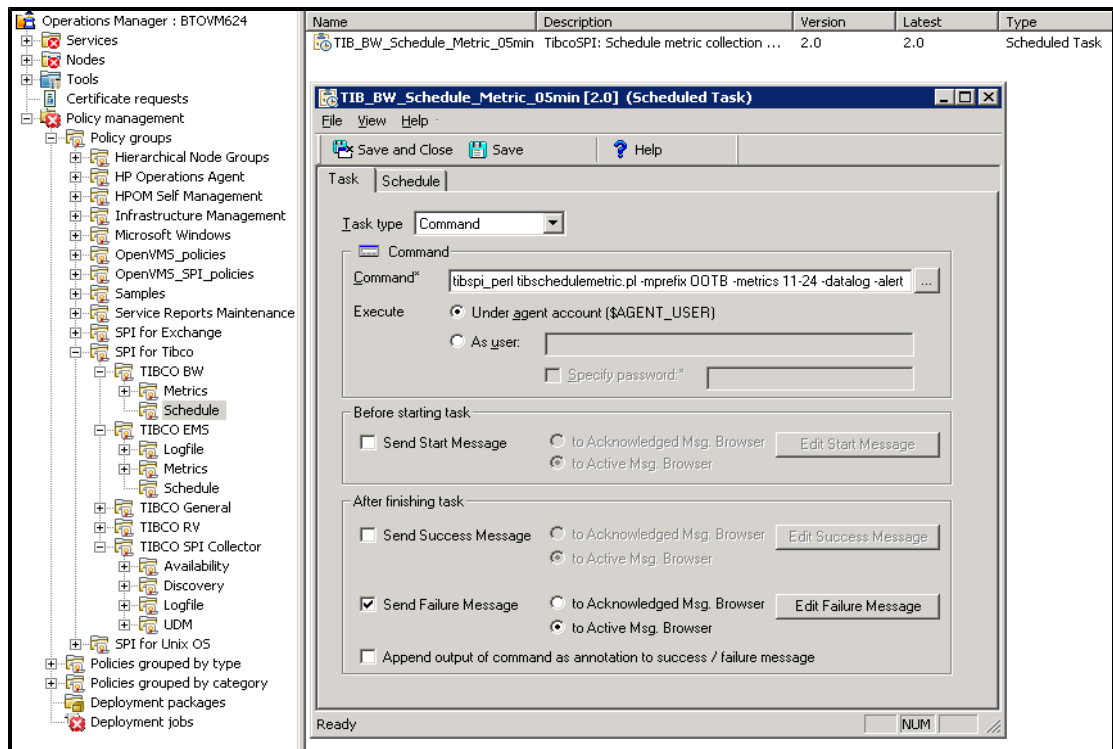
1. **On HPOM for Windows:** From the HPOM console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO BW** → **Schedule**.


Alternatively, you can select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO BW** → **Schedule**.

On HPOM for UNIX: From the Administration UI, select **Policy Bank** → **SPI for Tibco** → **TIBCO BW** → **Schedule**.

2. Double-click **Tib_BW_Schedule_Metric**.

The Schedule Task window opens.



On HPOM for UNIX: Select **Edit...** from the drop-down list . The Edit Scheduled_Task Policy "TIB_BW_Schedule_Metric_05min" opens.

3. a. By default, metrics are scheduled for all the configured domains.

In the task tab, enter the value for Command.

For Example:

```
Command = tibspi_perl tibschedulemetric.pl -mprefix OOTB -
metrics 11-24 -datalog -alert
```

where 1 is the metric id name (Metric id = "OOTB1")

An alert can be added if required for datalog.

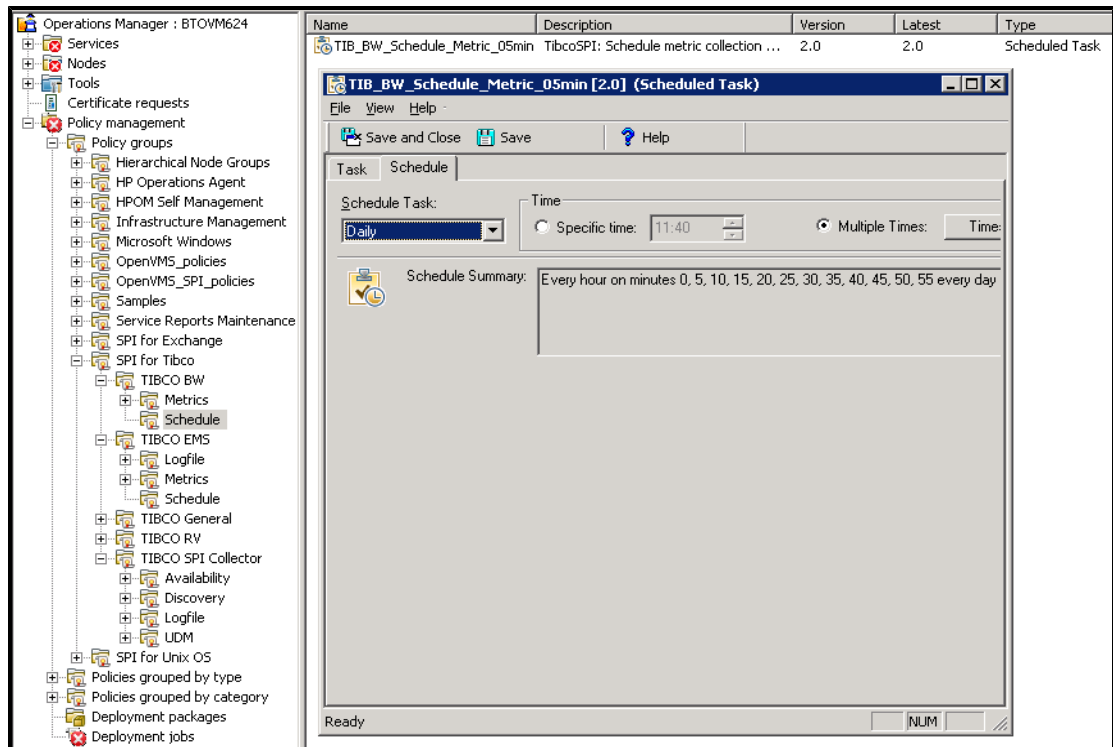
- b. For different schedules per domain, follow these steps:
 - i. Create a copy of the required schedule task policy for the required OOTB metrics for each domain.

For example: There are two domains *SPI_TEST* and *MyDomain* and you want to have different schedules for each domain. Copy the policy *TIB_EMS_Schedule_Metric_05min* as *TIB_EMS_Schedule_Metric_SPI_TEST* and *TIB_EMS_Schedule_Metric_MyDomain* for each domain.
 - ii. Open the policy and add `-tibd` parameter at the end of the command followed by the required domain name.

For example: Open the policy *TIB_EMS_Schedule_Metric_SPI_TEST* and update the command as `tibspi_perl tibschedulemetric.pl -mprefix OOTB -metrics 25-30 -datalog -alert -tibd SPI_TEST`. Edit the schedule as required.

Open the policy *TIB_EMS_Schedule_Metric_MyDomain* and update the command as `tibspi_perl tibschedulemetric.pl -mprefix OOTB -metrics 25-30 -datalog -alert -tibd MyDomain`. Edit the schedule as required.

4. In the schedule tab, enter the scheduled task and time.



5. Click **Save and Close** to save any changes and exit.

Verification

OOTB is properly configured if you receive an alert on the console according to the threshold limits set in the metric monitoring policy.

Example Metrics 1

Example 1:

The following sample illustrates the metric that returns the Average Elapsed Time.

```
<Metric id="OOTB11" domain="MyDomain" hawkagentname="agentname"
  microagentname="COM.TIBCO.ADAPTER.bwengine."
  enabled="true" isAsync="false">
  <MethodName>GetProcessDefinitions</MethodName>
  <MetricName>AverageElapsed</MetricName>
  <Params>
    <Param>
      <Name>TIB_POLICY_NAME</Name>
      <Value>TIB_BW_AverageElapsedTime</Value>
    </Param>
```

```

    </Params>
  </Metric>

```

Configuring User-Defined Metrics (UDMs)

To create and monitor UDMs, complete the following tasks in the specified order.

1. Edit the Metric Policy
2. Create and Deploy the Metric Monitoring Policy
3. Schedule the Metric
4. Verification

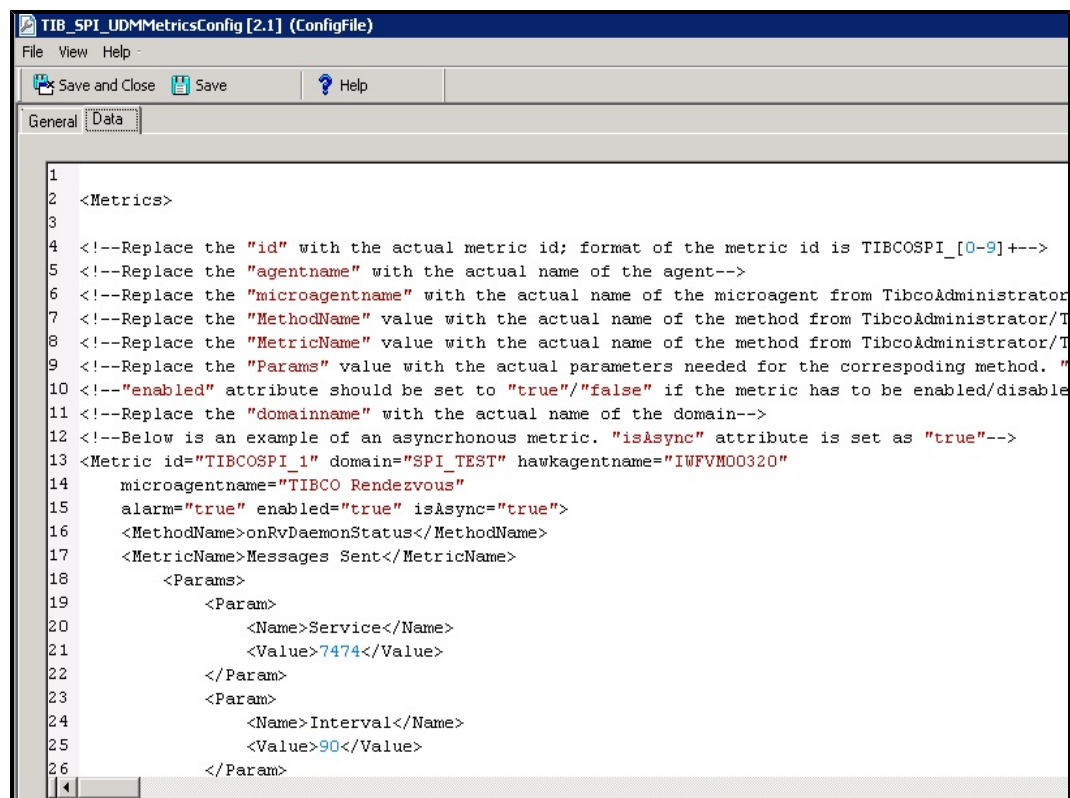
Edit the Metric Policy


1. **On HPOM for Windows:** From the console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO SPI Collector** → **UDM**.

On HPOM for UNIX: From the Administration UI, select **Policy Bank** → **SPI for Tibco** → **TIBCO SPI Collector** → **UDM**.

2. Double click **TIB_SPI_UDMMetricsConfig**.

The Configuration Editor opens.



On HPOM for UNIX: Select **Edit (Raw Mode)...** from the drop-down list . The Edit ConfigFile Policy "TIB_SPI_UDMMetricsConfig" opens. You can update the metric in the *Content* tab.

- Depending on the metric type whether synchronous or asynchronous, enter the attributes of the parameters defined. Below is an example of asynchronous and synchronous metrics and the set of parameters that you need to configure.

```
<Metrics domain="domainname">
```

Asynchronous Metric:

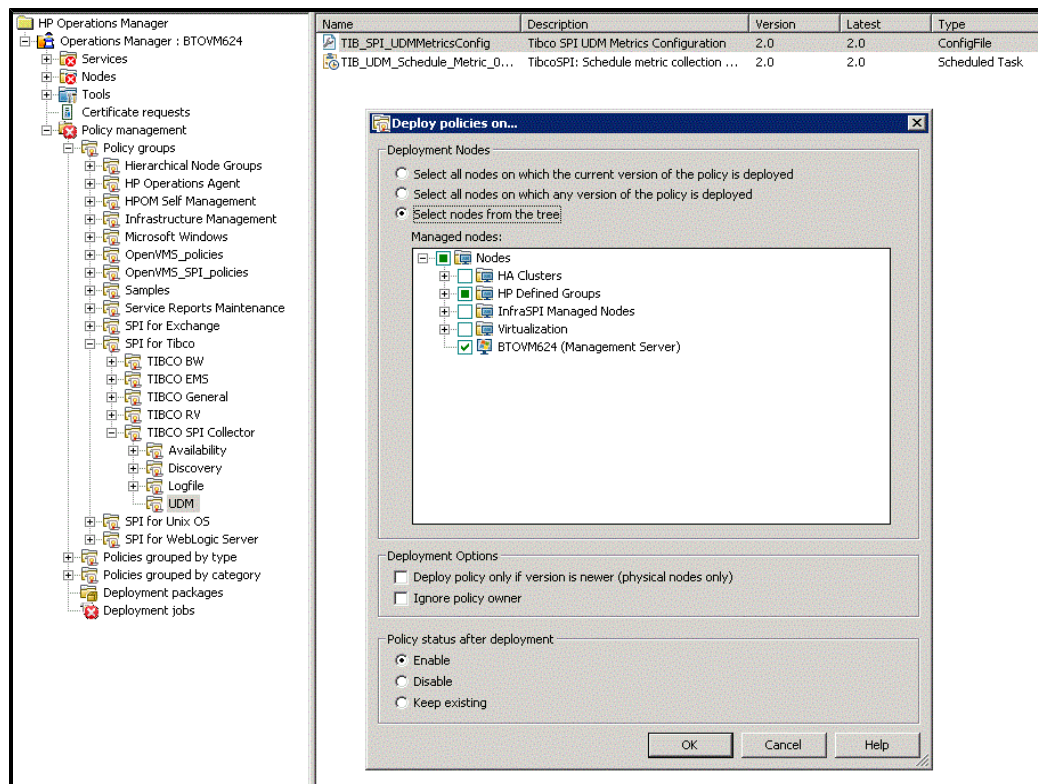
```
<Metric id="TIBCOSPI_1" hawkagentname="agentname"
  microagentname="microagent"
  alarm="true" enabled="false" isAsync="true">
  <MethodName>onRvDaemonStatus</MethodName>
  <MetricName>Messages Sent</MetricName>
  <Params>
    <Param>
      <Name>Service</Name>
      <Value>7474</Value>
    </Param>
    <Param>
      <Name>Interval</Name>
      <Value>300</Value>
    </Param>
    <Param>
      <Name>Network</Name>
      <Value>;</Value>
    </Param>
    <Param>
      <Name>Daemon</Name>
      <Value>tcp:7474</Value>
    </Param>
  </Params>
</Metric>
```

Synchronous Metric:

```
<Metric id="TIBCOSPI_2" hawkagentname="agentname"
  microagentname="JMS_controller"
  enabled="false" isAsync="false">
  <MethodName>getServerInfo</MethodName>
  <MetricName>outboundMessageRate</MetricName>
</Metric>
</Metrics>
```

- Click **Save and Close** to save any changes and exit the editor.
- Right-click the managed node on which you want to deploy the TIB_SPI_UDMMetricsConfig policy
- Select **All Tasks** → **Deploy on**.

The Deploy Policy window opens



7. Select the option, **Select nodes from the tree**. From the list of managed nodes, select the node on which you want to deploy the policy and click **OK**

The description of the properties used in the metrics are given below:

Metric Properties Description

Property	TIBCO SPI Requirements	Description
id	Required	The format for the Metric id is TIBCOSPI_ <u>[1-9]</u> +. For Example : <Metric id="TIBCOSPI_1">
domain	Required	Domain name is the actual name of the domain. For Example: <Metrics domain = "domainname">
hawkagentname	Required	Agent name is the actual name of the agent. It can be fetched from the TIBCO Administrator. For Example: <hawkagentname = "agentname">
microagentname	Required	Microagent name is the actual name of the microagent which can be fetched from the TIBCOAdministrator or TIBCOHawkDisplay. For Example: <microagentname = "TIBCO Rendezvous">

Property	TIBCO SPI Requirements	Description
alarm	Conditional Required if you want an alert for data logging.	Alarm property is used to receive an alert on the HPOM console. By default, the value for this property is set to "false". For Example : <code><alarm="true"></code>
enabled	Conditional Required if you want to configure a particular metric.	Enabled property is used to enable the metric block. The value of this property is either "true" or "false". For Example : <code><enabled="true"></code>
isAsync	Conditional	This property is required if you want to configure an asynchronous metric. isAsync property is set to "true" only if its an Asynchronous metric. For a synchronous metric you can either set the value to "false" or remove the property. For Example: <code><isAsync="true"></code>
MethodName	Required	Microagent uses the method name to call the metrics. For Example: <code><MethodName>getServerInfo</MethodName></code>
MetricName	Required	Metric Name is unique and is used to identify a metric to store/query individual measurement threshold values.
Params	Required	Parameters needed for the corresponding methods.

Create and Deploy the Metric Monitoring Policy

Creating a policy group for your UDMs enables you to assign multiple policies to a managed node as a single group rather than individually. Policies can be assigned to more than one policy group allowing you to customize the policies assigned to managed nodes.

To create a new measurement threshold policy with the required policy name, any existing policy can be copied and renamed. This enables you to keep custom policies separate from the original default policies.

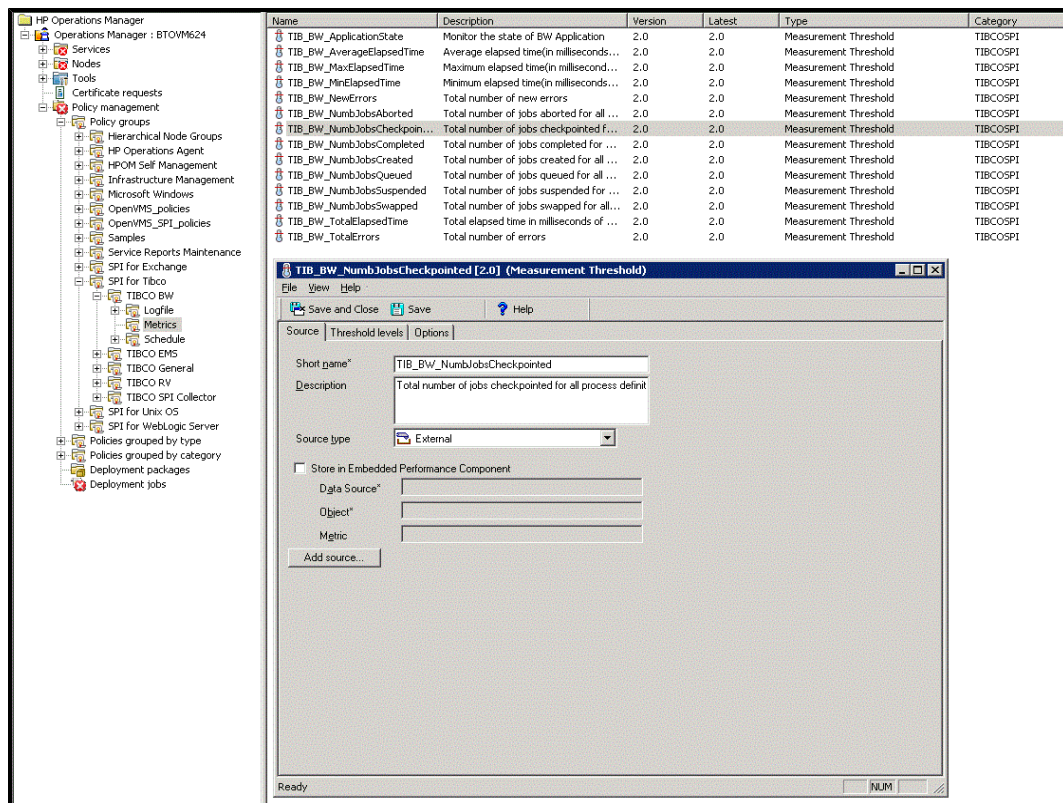
Follow these steps to create a new measurement threshold policy:

1. **On HPOM for Windows:** From the HPOM console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO BW** → **Metrics**. Double-click any one of the existing threshold policy.

Alternatively, you can also right-click on the HPOM console and select **New** → **Measurement Threshold**.

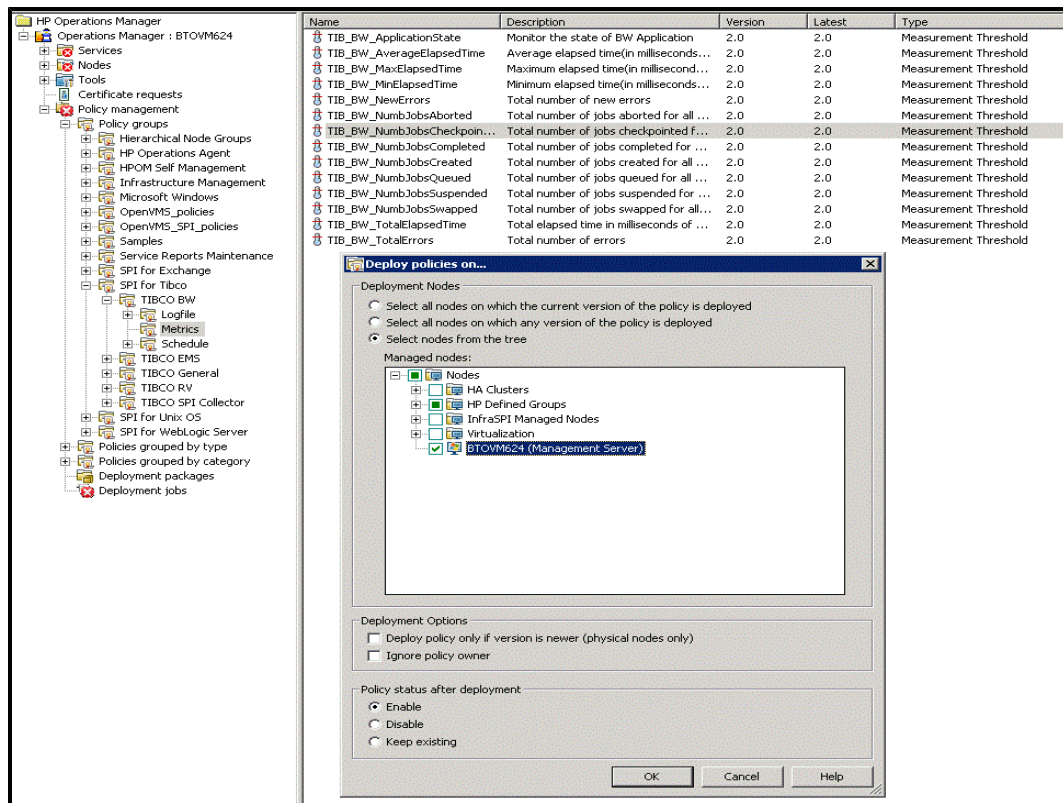
On HPOM for UNIX: From the Administration UI, select **Policy Bank** → **SPI for Tibco** → **TIBCO BW** → **Metrics**.

2. The measurement threshold window opens.



On HPOM for UNIX: Select **Copy...** from the drop-down list . The Copy Policy opens.

3. Enter the following values:
 - a. In the Source tab, enter the Short name and Description.
 - b. In the Threshold level tab, enter the values for the threshold limit.
 4. Click **Save and Close** to save any changes and exit.
 5. Right-click the managed node on which you want to deploy the measurement threshold policy.
 6. Select **All Tasks** → **Deploy on**
- The Deploy Policy window opens.



7. Select the option, **Select nodes from the tree**. From the managed nodes, select the node on which you want to deploy the policy and click **OK**.

Schedule the Metric

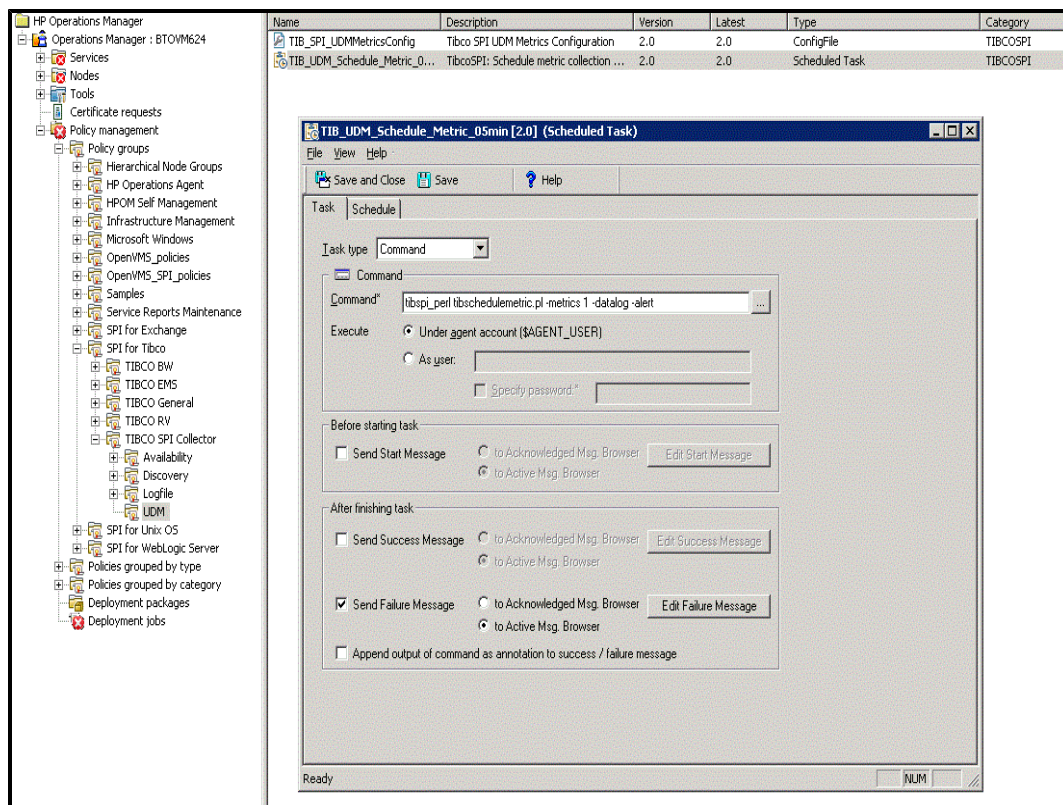
To create a new schedule with the required policy name, any existing schedule can be copied and renamed. This enables you to keep custom schedules separate from the original default schedule tasks.


1. **On HPOM for Windows:** From the HPOM console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO SPI Collector** → **UDM**.

On HPOM for UNIX: From the Administration UI, select **Policy Bank** → **SPI for Tibco** → **TIBCO SPI Collector** → **UDM**.

2. Double click **TIB_UDM_Schedule_Metric**.

The Schedule Task window opens.



On HPOM for UNIX: Select **Edit...** from the drop-down list . The Edit Scheduled_Task Policy "TIB_UDM_Schedule_Metric_05min" opens.

3. In the task tab, enter the value for Command.

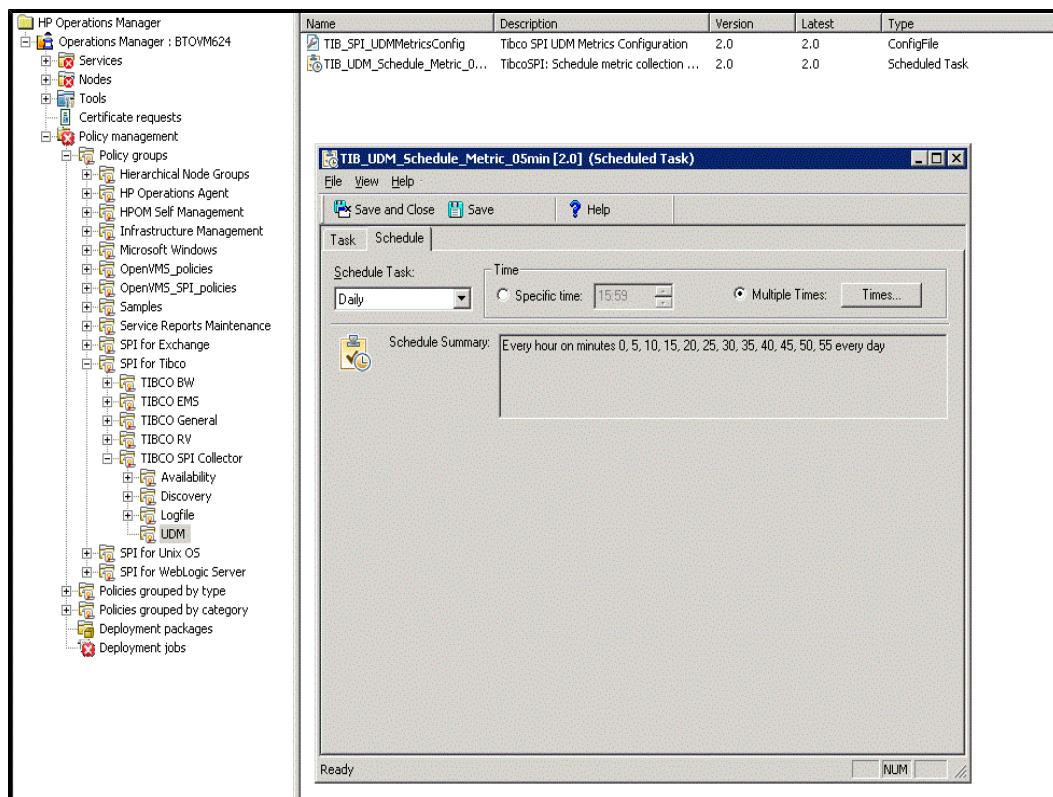
For Example:

```
Command = tibspi_perl tibschedulemetric.pl -metrics 1 -datalog -alert
```

where 1 is the metric id name (Metric id = "TIBCOSPI_1")

An alert can be added if required for datalog.

4. In the schedule tab, enter the scheduled task and time.



5. Click **Save and Close** to save any changes and exit.

Note: The values entered in the UDMs can be retrieved through the `TIBSPI_UDM` datasource.

Verification

UDM is properly configured if you receive an alert on the console according to the threshold limits set in the metric monitoring policy.

Example Metrics 2

Example 1:

The following sample metric illustrates a calculated metric. The metric returns the number of bytes used.

```
<Metric id="TIBCOSPI_5" hawkagentname="btovm354"
microagentname="COM.TIBCO.ADAPTER.bwengine.Admin.File.Process Archive"
enabled="true" isAsync="false">
<MethodName>GetMemoryUsage</MethodName>
<MetricName>UsedBytes</MetricName>
<Formula>TIBCOSPI_5/1024</Formula>
</Metric>
```

Example 2:

The below metric returns the result of a regular expression of a queue and sets the result in a descending format.

```
<Metric id="TIBCOSPI_3" hawkagentname="btovm354" microagentname="JMS_
controller (tcp://btovm354:7222)" enabled="true" isAsync="false">
<MethodName>getQueues</MethodName>
<MetricName>pendingMessageCount</MetricName>
<Params>
<Param>
<Name>queueRegExp</Name>
<Value></Value>
</Param>
<Param>
<Name>TIB_POLICYOPT_QNAME</Name>
<Value>name</Value>
</Param>
</Params>
<Formula>descend(5)</Formula>
</Metric>
```

Formula Elements

A Formula element contains content which is a string that specifies the mathematical calculations carried out to obtain the final metric value. The metrics are referred by their metric ID in the calculation expression. The result of the calculation is the metric value.

Following is the list of formulas that are supported:

1. **Basic arithmetic operations** supports operators such as +, -, /, *.
2. **Delta calculation** returns the result of subtracting the previous value of the metric from the current value.
3. **forwardall()** returns an alert for each row if method of a TIBCO microagent returns data in multiple rows.
4. **ascend(n)** returns the result in an ascending order for n number of rows that has been returned by a TIBCO microagent.
5. **descend(n)** returns the result in descending order for n number of rows that has been returned by a TIBCO microagent.


Creating UDM for all instances discovered in a domain

To define a new metric for all instances discovered in a domain follow these steps:

1. **On HPOM for Windows:** From the console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO SPI Collector** → **Discovery**.

On HPOM for UNIX: From the Administration UI, select **Policy Bank** → **SPI for Tibco** → **TIBCO SPI Collector** → **Discovery**.

2. Double click **TIB_SPI_OOTBMetricsConfig**. The Configuration Editor opens.

On HPOM for UNIX: Select **Edit (Raw Mode)...** from the drop-down list . The Edit ConfigFile Policy "TIB_SPI_OOTBMetricsConfig" opens. You can update the metric in the *Content* tab.

3. Add the below metric block in this policy, and set the attribute `usrDfndOOTB` to `true`.

For example: If `logFileSize` of all the EMS servers in the domain should be monitored then the metric definition would be defined as:

```
<Metric id="OOTB299" domain="all" hawkagentname="agentname"
  microagentname="JMS_controller"
  enabled="true" isAsync="false" usrDfndOOTB="true">
  <MethodName>getServerInfo</MethodName>
  <MetricName>logFileSize</MetricName>
</Metric>
```

Note: The metric id should be unique in this file.

4. Deploy the policy.
5. Create the required measurement threshold policy and also schedule the task policy and deploy it.

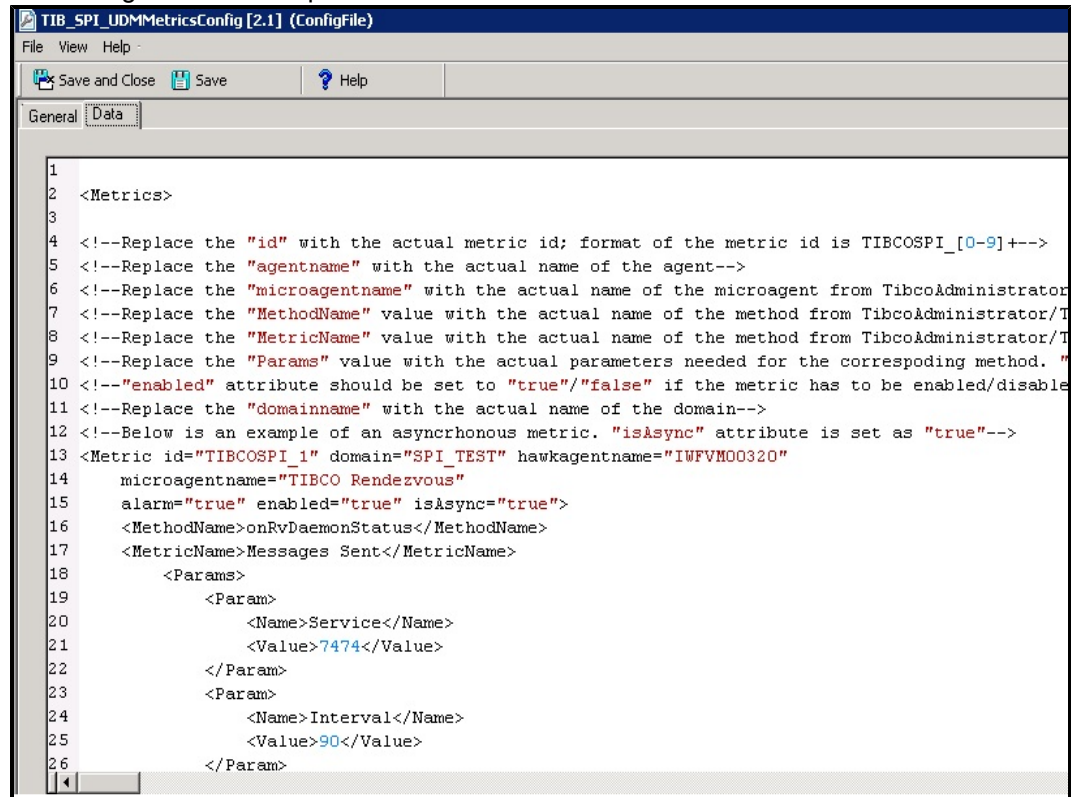
Note: The value of this metric will be logged to UDM table


Mapping Strings to Numbers in UDM

Use Case: You define a UDM to draw graphs or reports, but the microagent method and metric defined return a string rather than a number. Since, reports or graphs cannot be drawn on strings, you need to define corresponding number for the string returned.

1. **On HPOM for Windows:** From the console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO SPI Collector** → **UDM**.
On HPOM for UNIX: From the Administration UI, select **Policy Bank** → **SPI for Tibco** → **TIBCO SPI Collector** → **UDM**.
2. Double-click **TIB_SPI_UDMMetricsConfig**.

The Configuration Editor opens.



On HPOM for UNIX: Select **Edit (Raw Mode)...** from the drop-down list . The Edit ConfigFile Policy "TIB_SPI_UDMMetricsConfig" opens. You can update the metric in the *Content* tab.

3. Go to the `<Params>` tag in the metric definition. If the tag does not exist, add `<Params>` tag in the metric definition.
4. You can now add the `<Param>` tag under `<Params>` for string to numeric mapping.

For Example: A sample metric definition in the UDM config policy.

```
<Metric id="TIBCOSPI_3" hawkagentname="x86vm325"
  microagentname="JMS_controller (tcp://localhost:7222)"
  enabled="true" isAsync="false">
  <MethodName>isRunning</MethodName>
  <MetricName>running</MetricName>
  <Params>
    <Param>
      <Name>TIB_MAPVALUE_true</Name>
      <Value>1</Value>
    </Param>
    <Param>
      <Name>TIB_MAPVALUE_false</Name>
      <Value>0</Value>
    </Param>
  </Params>
```

```

    </Params>
  </Metric>

```

- In the above example `isRunning` method of EMS microagent returns *true/false* values which is mapped to *1/0* values correspondingly.
- The parameter name `TIB_MAPVALUE_true` is actually composed as `TIB_MAPVALUE_ + true`, where *true* is the value returned by `isRunning` method of EMS server. The value *true* is mapped to *1* by adding the below parameter:

```

<Param>

    <Name>TIB_MAPVALUE_true</Name>

    <Value>1</Value>
</Param>

```

- The parameter name `TIB_MAPVALUE_false` is actually composed as `TIB_MAPVALUE_ + false`, where *false* is the value returned by `isRunning` method of EMS server. The value *false* is mapped to *0* by adding the below parameter:

```

<Param>

    <Name>TIB_MAPVALUE_false</Name>

    <Value>0</Value>
</Param>

```


5. Click **Save and Close** to save any changes and exit the editor.
6. Right-click the managed node on which you want to deploy the `TIB_SPI_UDMMetricsConfig` policy
7. Select **All Tasks** → **Deploy on**.
The Deploy Policy window opens.
8. Select the option, **Select nodes from the tree**. From the list of managed nodes, select the node on which you want to deploy the policy and click **OK**.

Monitoring Logfile using UDM

Use Case: You need to monitor the `C:/tibco/tra/domain/SPI_TEST/logs/msghma.log` logfile available on the `x86vm103.indi.hp.com` machine whose hawkagent is `x86vm103` within the `SPI_TEST` domain.

Step 1: Update and Deploy the UDM Metric Policy.

1. On HPOM for Windows: From the HPOM console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO SPI Collector** → **UDM**.
On HPOM for UNIX: From the Administration UI, select **Policy Bank** → **SPI for Tibco** → **TIBCO SPI Collector** → **UDM**.
2. Double-click **TIB_SPI_UDMMetricsConfig**.

On HPOM for UNIX: Select **Edit (Raw Mode)...** from the drop-down list . The Edit ConfigFile Policy "TIB_SPI_UDMMetricsConfig" opens. You can update the metric in the *Content* tab.

3. The metric definition would look like:

```
<Metric id="TIBCOSPI_4" domain="SPI_TEST" hawkagentname="x86vm103"
microagentname="Logfile" alarm="true" enabled="true"
isAsync="true">
  <MethodName>onNewLine</MethodName>
  <MetricName>nextLine</MetricName>
  <Params>
    <Param>
      <Name>logfile</Name>
      <Value>C:/tibco/tra/domain/SPI_TEST/logs/msghma.log
    </Value>
    </Param>
    <Param>
      <Name>TIB_OPCMSG_APP</Name>
      <Value>TIBCO</Value>
    </Param>
    <Param>
      <Name>TIB_OPCMSG_OBJ</Name>
      <Value>MSGHMA</Value>
    </Param>
  </Params>
</Metric>
```

4. Click **Save and Close** to save any changes and exit the editor.
5. Right-click the managed node on which you want to deploy the TIB_SPI_UDMMetricsConfig policy.
6. Select **All Tasks** → **Deploy on**.
7. Select the option, **Select nodes from the tree**. From the list of managed nodes, select the node on which you want to deploy the policy and click **OK**

Step 2: Create and Deploy the Open message Interface Policy

1. In the below metric definition the *Application* and *Object* are mentioned using the parameters TIB_OPCMSG_APP and TIB_OPCMSG_OBJ respectively.

```
<Metric id="TIBCOSPI_4" hawkagentname="x86vm103"
microagentname="Logfile" alarm="true" enabled="true"
isAsync="true">
  <MethodName>onNewLine</MethodName>
  <MetricName>nextLine</MetricName>
  <Params>
    <Param>

      <Name>logfile</Name>
      <Value> C:/tibco/tra/domain/SPI_
```

```

TEST/logs/msghma.log</Value>
    </Param>
    <Param>
        <Name>TIB_OPCMSG_APP</Name>
        <Value>TIBCO</Value>
    </Param>
    <Param>
        <Name>TIB_OPCMSG_OBJ</Name>
        <Value> MSGHMA </Value>
    </Param>
</Params>
</Metric>

```

2. The policy should have a *Condition* where *Application* should be equal to `TIBCO` and *Object* should be equal to `MSGHMA`.
3. The policy should be further updated if a matching pattern is required on the *Message text*.
4. The policy should also be updated with the proper *Actions* whenever a particular *Condition* is met.

Advanced Timeout Configuration (Optional)

The `tibcfg.properties` and `tibcmconfiguration.properties` file provides the optional timeout configurations. On a managed node, these files are located in the following directory:

Windows managed node: `%OvDataDir%\bin\instrumentation`

UNIX managed nodes: `/var/opt/OV/bin/instrumentation`

The configurations mentioned in the above file are not required unless your environment demands.

Forwarding Alerts Generated by Hawk Rules

You must meet the following prerequisites and then follow the steps in the specified order.

Prerequisites:

1. You must install and configure the HawkEventService on a machine within the domain. Alerts generated by Hawk rules should be forwarded to OM console.

Once the HawkEventService is started for the required domain, there would be a microagent available for the hawk event service.

For example: If the domain name is `SPI_TEST`, then the HawkEventService microagent name would be `HawkEventService:SPI_TEST`

2. Only one instance of HawkEventService is sufficient for one domain.

To forward alerts generated by Hawk rules, you must follow these steps:

1. **On HPOM for Windows:** From the HPOM console, select **Policy Management** → **Policy Groups** → **SPI for Tibco** → **TIBCO General** → **TIB_HAWKALRT_FWD**.

On HPOM for UNIX: From the Administration UI, select **Policy Bank** → **SPI for Tibco** → **TIBCO General** → **TIB_HAWKALRT_FWD**.

2. Select the node on which you want to deploy the policy.
3. Re-deploy the discovery policy.

Chapter 5

Using Tools

This chapter describes the tools offered by TIBCO SPI, which help you to monitor and manage systems using the TIBCO Application Server. These tools enable you to configure the management server's connection on specific managed nodes.

TIBCO SPI Tool Group

The TIBCO SPI tool group contains the following tools:

Tibco SPI Tool Group

Name	Description
Start Tibco SPI Collector	Starts the TIBCO SPI Collector.
Status of Tibco SPI Collector	Checks the status of the TIBCO SPI Collector.
Stop Tibco SPI Collector	Stops the TIBCO SPI Collector.
Tibco Domain Authentication	Tool for accepting EMS and SSL Authentication

Launching Tools

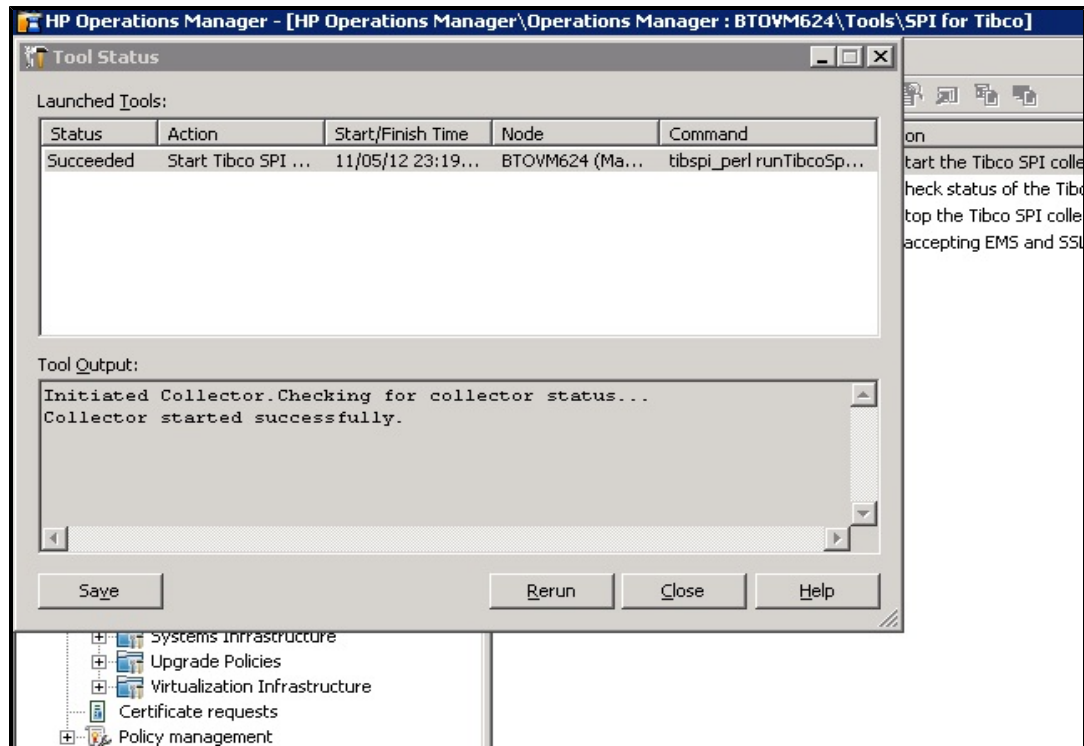
This section describes how you can launch the tools for TIBCO SPI. Before launching the tools make sure that the Discovery Config file policy is configured properly. To launch the tool, see the steps in ["Update and Deploy Configuration Policies" on page 37](#). Also, check the assignment of nodes on the management server.

On HPOM for Windows Management Server

To launch the tool on HPOM for Windows management server, follow these steps:

1. From the HPOM console, select **Tools** → **SPI for Tibco** → **<Tool Group>**.
2. Right-click the tool and select **All Tasks** → **Launch Tool**.
3. Select the managed nodes on which you want to launch the tool. Click **Launch**.
4. The Tool Status window opens. In the Launched Tools field, check the status of the tool for each node:

- a. Starting - The tool is running.



- b. Succeeded -The tool succeeded. Select the node in the Launched Tools field and scroll through the Tool Output field.
- c. Failed - The tool failed to run properly. Select the node in the Launched Tools field and scroll through the Tool Output field for more information about the problem.
5. Click **Close** to close the Tool Status window.

On the HPOM for UNIX Management Server

To launch the tool on the HPOM for UNIX management server, you must first meet the prerequisites and then follow the steps to launch the tool.

Prerequisites

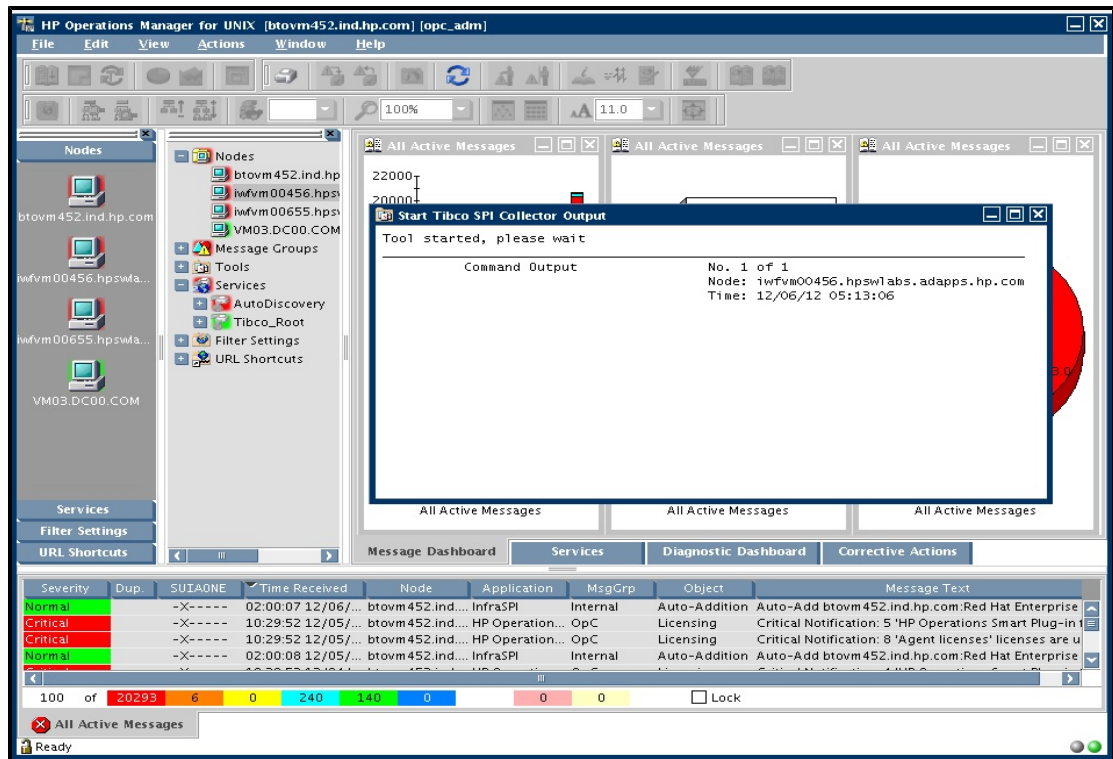
Before launching the tool you need to assign operator responsibilities. To assign operator rights, see [Assign Operator Responsibilities for User](#).

Once the rights are assigned you can view **SPI for Tibco** under the **Tools** section in the Java interface.

Steps to launch the tool

1. From the Administration UI, select **Integrations** → **HPOM for Unix Operational UI**.
2. Select **Nodes** and right-click the managed node on which you want to launch the tool.
3. Select **Start** → **SPI for Tibco** and select the tool you want to run.
4. The Tibco SPI Collector output window opens. The below image is an example of Start Tibco

SPI Collector.



Chapter 6

Using Policies

The TIBCO SPI policies enable you to monitor the performance and availability of TIBCO infrastructure elements. These policies contain a set of rules for monitoring logfiles, services, and threshold values.

Policy Types for TIBCO SPI

A policy type is a set of configuration information that defines what a policy can manage. Every policy belongs to one policy type. The following are the policy types for TIBCO SPI:

- Open Message Interface Policies
- Measurement Threshold Policies
- Scheduled Task Policies
- ConfigFile Policies
- Service Auto-Discovery Policies
- Logfile Entry

For more information about SPI policy types, see *HPOM Online Help*.

Policy Group for TIBCO SPI

Policy Groups are a set of policies that share some common attribute or logical connection. It enables you to work with multiple policies simultaneously more easily.

When you install TIBCO SPI, a new policy group for TIBCO SPI is added in the HPOM console under **Policy Management** → **Policy Group**. This TIBCO SPI group contains all the policies used for managing the TIBCO environment. The TIBCO SPI policies are primarily grouped on the basis of TIBCO applications/servers. The following are the TIBCO servers managed by TIBCO SPI:

- [TIBCO BW Policies](#)
- [TIBCO EMS Policies](#)
- [TIBCO Hawk Agent Monitoring Policies](#)
- [TIBCO RV Policies](#)
- [TIBCO SPI Collector Policies](#)

Depending on the functions, TIBCO SPI policies are further grouped as follows:

- Logfile
- Metrics
- Schedule

- General
- Availability
- Discovery
- UDM

TIBCO BW Policies

This group contains all policy subgroups for monitoring TIBCO BW application.

TIBCO BW Metrics

The TIBCO BW Metric policies enable you to define the measurement threshold values for monitoring the TIBCO BW application. The Operations Agent sends alerts to the HPOM console if the metric condition reaches or exceeds the threshold limits.

To view the TIBCO BW Metrics, expand **Policy management** → **SPI for Tibco** → **TIBCO BW**. The metrics are scheduled to run every 5 minutes. The following table lists the metric policies for TIBCO BW.

TIBCO BW Metrics

Name	Description	Threshold Levels
Metric Name: MinElapsed Policy Name: TIB_BW_MinElapsedTime	Deploy this policy to measure the minimum time elapsed among all process defined in the BW Engine.	<ul style="list-style-type: none">• Sends critical message if minimum elapsed time is >500• Sends warning message if minimum elapsed time is >200
Metric Name: Application State Policy Name: TIB_BW_ApplicationState	Monitors the application state.	<ul style="list-style-type: none">• Sends critical message if applications state code =<0• Sends major message if applications state code =<1• Sends minor message if applications state code =<2• Sends minor message if applications state code =<3

Name	Description	Threshold Levels
Metric Name: New Errors Policy Name: TIB_BW_ NewErrors	Monitors total number of new errors for applications.	<ul style="list-style-type: none"> • Sends critical message if total number of new errors are >20 • Sends warning message if total number of new errors are >10
Metric Name: Suspended Policy Name: TIB_BW_ NumbJobsSuspended	Monitors total number of jobs suspended for applications.	<ul style="list-style-type: none"> • Sends critical message if total number of suspended jobs are >50 • Sends warning message if total number of suspended jobs are >30
Metric Name: TotalElapsed Policy Name: TIB_BW_ TotalElapsedTime	Monitors total elapsed time in milliseconds for all the completed jobs.	<ul style="list-style-type: none"> • Sends critical message if total elapsed time for completed applications is >180000 • Sends warning message if total elapsed time for completed applications is >60000
Metric Name: Total Errors Policy Name: TIB_BW_ TotalErrors	Monitors total number of errors for applications.	<ul style="list-style-type: none"> • Sends critical message if total number of errors are >50 • Sends warning message if total number of errors are >20
Metric Name: Swapped Policy Name: TIB_BW_ NumbJobsSwapped	Monitors total number of jobs swapped for applications.	<ul style="list-style-type: none"> • Sends critical message if total number of jobs swapped are >50 • Sends warning message if total number of jobs swapped are >30
Metric Name: Created Policy Name: TIB_BW_ NumbJobsCreated	Monitors total number of jobs created for applications.	<ul style="list-style-type: none"> • Sends critical message if total number of jobs created are >50 • Sends warning message if total number of jobs created are >40

Name	Description	Threshold Levels
Metric Name: Checkpointed Policy Name: TIB_BW_ NumbJobsCheckpointed	Monitors total number of jobs check pointed for applications.	<ul style="list-style-type: none"> • Sends critical message if total number of jobs check pointed are >100 • Sends warning message if total number of jobs check pointed are >50
Metric Name: Queued Policy Name: TIB_BW_ NumbJobsQueued	Monitors total number of jobs queued for applications.	<ul style="list-style-type: none"> • Sends critical message if total number of jobs queued are >200 • Sends warning message if total number of jobs queued are >100
Metric Name: MaxElapsed Policy Name: TIB_BW_ MaxElapsedTime	Monitors maximum elapsed time for applications.	<ul style="list-style-type: none"> • Sends critical message if maximum elapsed time in milliseconds >2000 • Sends warning message if maximum elapsed time in milliseconds >1000
Metric Name: Aborted Policy Name: TIB_BW_ NumbJobsAborted	Monitors total number of jobs aborted for applications.	<ul style="list-style-type: none"> • Sends critical message if total number of jobs aborted are >200 • Sends warning message if total number of jobs aborted are >100
Metric Name: AverageElapsed Policy Name: TIB_BW_ AverageElapsedTime	Monitors average elapsed time for applications.	<ul style="list-style-type: none"> • Sends critical message if average elapsed time in milliseconds >2000 • Sends warning message if average elapsed time in milliseconds >1000

TIBCO EMS Policies

This group contains all policy subgroups for monitoring TIBCO EMS application.

TIBCO EMS Metrics

The TIBCO EMS Metric policies enable you to define the measurement threshold values for monitoring the TIBCO EMS application. To view the TIBCO EMS Metrics, expand **Policy management** → **SPI for Tibco** → **TIBCO EMS**. The metrics are scheduled to run every 5 minutes. The following table shows the metric policies available for TIBCO EMS.

TIBCO EMS Metrics

Name	Description	Threshold Levels
Metric Name: pendingMessageCount Policy Name: TIB_EMS_ PendingMsgCount	Monitors pending message count for EMS server.	<ul style="list-style-type: none">• Sends critical message if pending message count is > 300• Sends warning message if pending message count is > 200
Metric Name: EMS Server State Policy Name: TIB_EMS_ ServerState	Monitors TIBCO EMS server status.	<ul style="list-style-type: none">• Sends critical message if EMS server is down (error code <= 0)
Metric Name: outboundMessageCount Policy Name: TIB_EMS_ OutboundMsgCount	Monitors and gives the delta value of the outbound message count for EMS server.	<ul style="list-style-type: none">• Sends critical message if outbound message count is > 200• Sends warning message if outbound message count is > 100
Metric Name: outboundMessageRate Policy Name: TIB_EMS_ OutboundMsgRate	Monitors outbound message rate for EMS server.	<ul style="list-style-type: none">• Sends critical message if outbound message rate is > 500• Sends warning message if outbound message rate is > 200
Metric Name: inboundMessageRate Policy Name: TIB_EMS_ InboundMsgRate	Monitors inbound message rate for EMS server.	<ul style="list-style-type: none">• Sends critical message if Inbound message rate is > 500• Sends warning message if Inbound message rate is > 200
Metric Name: inboundMessageCount Policy Name: TIB_EMS_ InboundMsgCount	Monitors and gives the delta value of the inbound message count for EMS server.	<ul style="list-style-type: none">• Sends critical message if Inbound message count is > 200• Sends warning message if Inbound message count is > 100

Note: For all the above EMS metrics except the TIB_EMS_ServerState, the annotation text gives the information about the top 10 queues which are contributing to the threshold breach.

TIBCO Hawk Agent Monitoring Policies

This group contains generic policies for monitoring TIBCO applications. The following table shows the general policies available for TIBCO SPI.

TIBCO General Metrics

Name	Description	Threshold Levels
Metric Name: BW application availability Policy Name: TIB_SPI_McrAgntStatus	Monitors micro agent availability status.	Sends critical message if micro agent is down (code <=0)
Metric Name: Hawk Agent availability Policy Name: TIB_SPI_HwkAgntStatus	Monitors HAWK agent availability status.	Sends critical message if HAWK agent is down (code <=0)
Policy Name: TIB_HAWKALRT_FWD	Forwards alerts generated by Hawk rules.	Forwards hawk alerts which are of severity ALERT_HIGH and ALERT_MEDIUM

TIBCO RV Policies

This group contains all policy subgroups for monitoring TIBCO RV component.

TIBCO RV Metrics

The TIBCO RV Metric policies enable you to define the measurement threshold values for monitoring the TIBCO RV application. To view the Tibco RV Metrics, expand **Policy management** → **SPI for Tibco** → **TIBCO RV**. The metrics are scheduled to run every 5 minutes. The following table shows the metric policies available for TIBCO RV.

TIBCO RV Metrics

Policy Name	Description	Threshold Levels
Metric Name: PacketsSent Policy Name: TIB_RV_PacketsSent	Monitors number of packets sent by RV Daemon in last polling interval.	<ul style="list-style-type: none">• Sends critical message if number of packets sent >=150000• Sends warning message if number of packets sent >=60000

Policy Name	Description	Threshold Levels
Metric Name: MissedPackets Policy Name: TIB_RV_ MissedPackets	Monitors number of packets missed by RV Daemon in last polling interval.	<ul style="list-style-type: none"> • Sends critical message if number of packets missed ≥ 150000 • Sends warning message if number of packets missed ≥ 60000
Metric Name: BytesReceived Policy Name: TIB_RV_ BytesReceived	Monitors number of bytes received by RV Daemon in last polling interval.	<ul style="list-style-type: none"> • Sends critical message if number of bytes received ≥ 250000 • Sends warning message if number of bytes received ≥ 100000
Metric Name: PacketsReceived Policy Name: TIB_RV_ PacketsReceived	Monitors number of packets received by RV Daemon in last polling interval.	<ul style="list-style-type: none"> • Sends critical message if number of packets received ≥ 150000 • Sends warning message if number of packets received ≥ 60000
Metric Name: MessagesReceived Policy Name: TIB_RV_ MessagesReceived	Monitors number of messages received by RV Daemon in last polling interval.	<ul style="list-style-type: none"> • Sends critical message if number of messages received ≥ 150000 • Sends warning message if number of messages received ≥ 60000
Metric Name: RetransmittedPackets Policy Name: TIB_RV_ RetransmittedPackets	Monitors number of re-transmitted packets by RV Daemon in last polling interval.	<ul style="list-style-type: none"> • Sends critical message if number of re-transmitted packets ≥ 150000 • Sends warning message if number of re-transmitted packets ≥ 60000
Metric Name: BytesSent Policy Name: TIB_RV_ BytesSent	Monitors number of bytes sent by RV Daemon in last polling interval.	<ul style="list-style-type: none"> • Sends critical message if number of bytes sent ≥ 250000 • Sends warning message if number of bytes sent ≥ 100000

Policy Name	Description	Threshold Levels
Metric Name: MissedPacketsRate Policy Name: TIB_RV_ MissedPacketRate	Monitors missed packet rate of RV Daemon.	<ul style="list-style-type: none"> • Sends critical message if missed packet rate ≥ 50 • Sends warning message if missed packet rate ≥ 20
Metric Name: RetransmittedPacketsRate Policy Name: TIB_RV_ RetransmittedPacketRate	Monitors re-transmitted packet rate of RV Daemon.	<ul style="list-style-type: none"> • Sends critical message if re-transmitted packet rate ≥ 50 • Sends warning message if re-transmitted packet rate ≥ 20
Metric Name: MessagesSent Policy Name: TIB_RV_ MessagesSent	Monitors number of messages sent by RV Daemon in last polling interval.	<ul style="list-style-type: none"> • Sends critical message if number of messages sent ≥ 150000 • Sends warning message if number of messages sent ≥ 60000

TIBCO SPI Collector Policies

This group contains all policy subgroups for monitoring the TIBCO SPI Collector.

Configuring Monitoring Frequency

The TIBCO SPI Collector monitoring policies enable you to create metric policies for monitoring the TIBCO SPI Collector.

Configuring Monitoring Frequency

Policy Name	Description
TIB_BW_Schedule_Metric_05min	Schedules metric collection of TIBCO BW applications every 5 minutes.
TIB_BW_Schedule_Metric_Jobs_Completed_05min	Logs data every 5 minutes to CODA for jobs completed metric.
TIB_EMS_Schedule_Metric_05min	Schedules metric collection of EMS every 5 minutes.
TIB_RV_Schedule_Metric_Datalog_05min	Schedules metric collection of TIBCO RV every 5 minutes.
TIB_UDM_Schedule_Metric_05min	Schedules metric collection of UDM metrics every 5 minutes.
TIB_HwkStatus_Schedule_Metric_Datalog_05min	Logs hawk status agent to the CODA.
TIB_SPI_UDMMetricsConfig	Configures UDM metrics configuration.

Discovery Configuration

The TIBCO SPI Collector Discovery policies discover the managed nodes where the TIBCO applications and services are running and build a service map for all the TIBCO SPI discovered instances.

Discovery Configuration

Policy Name	Description
TIB_SPI_OOTBMetricsConfig	Configure TIBCO SPI OOTB Metrics.
TIB_SPI_DiscConfig	Configure TIBCO SPI Discovery Configuration.
TIB_SPI_Discovery	Configure TIBCO SPI Discovery.
TIB_OPC_MSG	Filters and forwards messages with application name TIBCO and TIBCO SPI open message interface policy type.

Self-Monitoring Policies

The TIBCO SPI Collector self-monitoring policies monitor and check for the state and availability of TIBCO SPI Collector.

Self Monitoring Policies

Policy Name	Description	Threshold Levels
TIB_SPI_Collector_Availability	Monitors TIBCO SPI collector availability status.	<ul style="list-style-type: none">• Sends critical message if collector availability status is >131• Sends warning message if collector availability status is >121
TIB_SPI_Collector_Availability_05min	Monitors TIBCO SPI collector every 5 minutes.	—

LogFile Monitoring Policies

The TIBCO SPI Collector logfile policies monitor the crucial logs for TIBCO SPI Collector.

Logfile Monitoring Policies

Name	Description
TIB_EMS_RemoteLogFile	Monitors TIBCO EMS log remotely.
TIB_RV_RemoteLogFile	Monitors TIBCO RV log remotely.

Name	Description
TIB_Hawk_RemoteLogFile	Monitors TIBCO HAWK log files remotely.
TIB_SPI_LOGFILE	Monitors TIBCO SPI log files.

Chapter 7

Using Reports

You can integrate the TIBCO SPI with HP Reporter to generate reports based on collected metric data from the managed nodes.

Note: To generate and view reports and graphs, you must install the HP Reporter in your environment and HP Performance Manager on the HPOM management server.

If HP Reporter is installed on the HPOM management server, you can view the reports on the management server directly. If HP Reporter is installed on a separate system connected to the HPOM management server, you can view the reports on HP Reporter system. For more information on integration of HP Reporter with HPOM, see *HP Reporter Installation and Special Configuration Guide*.

- **Location:** You can find the TIBCO SPI located in the HPOM console under **Reports** → **SPI for Tibco**. The SPI for Tibco **Reports** and **Graphs** folders are created when the data is collected on the managed nodes and the Service Reporter consolidation process has run, usually after 24 hours.
- **Scheduling:** Most reports generate the day after the data is collected and gathered from the managed node.

Note: When collection is disabled for a particular metric then the previous collected value will be logged to coda database. If the metric was never scheduled or the collection failed for the metric, then -1 will be logged to coda database.

Reports of TIBCO SPI are based on the following categories:

- [TIBCO RV](#)
- [TIBCO BW](#)
- [TIBCO EMS](#)

TIBCO RV Reports

TIBCO RV Reports

Report	Metric	Description
RVD Top 10 Messages Sent-Daily	Messages Sent	The report shows the top 10 RVDs based on the highest number of messages sent daily on the system.
RVD Top 10 Messages Sent-Monthly	Messages Sent	The report shows the top 10 RVDs based on the highest number of messages sent monthly on the system.

Report	Metric	Description
RVD Top 10 Messages Sent-Weekly	Messages Sent	The report shows the top 10 RVDs based on the highest number of messages sent weekly on the system.
RVD Top 10 Messages Sent-Yearly	Messages Sent	The report shows the top 10 RVDs based on the highest number of messages sent yearly on the system.
RVD Top 10 Packets Sent-Daily	Packets Sent	The report shows the top 10 RVDs selected based on the highest rate of packets sent daily.
RVD Top 10 Packets Sent-Monthly	Packets Sent	The report shows the top 10 RVDs selected based on the highest rate of packets sent monthly.
RVD Top 10 Packets Sent-Weekly	Packets Sent	The report shows the top 10 RVDs selected based on the highest rate of packets sent weekly.
RVD Top 10 Packets Sent-Yearly	Packets Sent	The report shows the top 10 RVDs selected based on the highest rate of packets sent yearly.
RVD Top 10 Packets Received-Daily	Packets Received	The report shows the top 10 RVDs selected based on the highest rate of packets received daily.
RVD Top 10 Packets Received-Monthly	Packets Received	The report shows the top 10 RVDs selected based on the highest rate of packets received monthly.
RVD Top 10 Packets Received-Weekly	Packets Received	The report shows the top 10 RVDs selected based on the highest rate of packets received weekly.
RVD Top 10 Packets Received-Yearly	Packets Received	The report shows the top 10 RVDs selected based on the highest rate of packets received yearly.
RVD Top 10 Retransmitted Packets-Daily	Retransmitted Packets	The report shows the top 10 RVDs selected based on the daily highest retransmission packets.
RVD Top 10 Retransmitted Packets-Monthly	Retransmitted Packets	The report shows the top 10 RVDs selected based on the monthly highest retransmission packets.
RVD Top 10 Retransmitted Packets-Weekly	Retransmitted Packets	The report shows the top 10 RVDs selected based on the weekly highest retransmission packets.
RVD Top 10 Retransmitted Packets-Yearly	Retransmitted Packets	The report shows the top 10 RVDs selected based on the yearly highest retransmission packets.

TIBCO BW Reports

TIBCO BW Reports

Report	Metric	Description
BW Aborted and Suspended Jobs-Daily	Aborted / Suspended	The report shows the total number of jobs aborted or suspended daily for all process definitions in the BW Engine.
BW Aborted and Suspended Jobs-Monthly	Aborted / Suspended	The report shows the total number of jobs aborted or suspended monthly for all process definitions in the BW Engine.
BW Aborted and Suspended Jobs-Weekly	Aborted / Suspended	The report shows the total number of jobs aborted or suspended weekly for all process definitions in the BW Engine.
BW Aborted and Suspended Jobs-Yearly	Aborted / Suspended	The report shows the total number of jobs aborted or suspended yearly for all process definitions in the BW Engine.
BW Total and New Errors-Daily	Total Errors / New Errors	The report shows the new errors and total number of errors daily for each BW application.
BW Total and New Errors-Monthly	Total Errors / New Errors	The report shows the new errors and total number of errors monthly for each BW application.
BW Total and New Errors-Weekly	Total Errors / New Errors	The report shows the new errors and total number of errors weekly for each BW application.
BW Total and New Errors-Yearly	Total Errors / New Errors	The report shows the new errors and total number of errors yearly for each BW application.
BW Availability-Daily	Availability	The report shows the daily BW Application availability for each application.
BW Availability-Monthly	Availability	The report shows the monthly BW Application availability for each application.
BW Availability-Weekly	Availability	The report shows the weekly BW Application availability for each application.
BW Availability-Yearly	Availability	The report shows the yearly BW Application availability for each application.

TIBCO EMS Reports

TIBCO EMS Reports

Report	Metric	Description
EMS Top 10 Queues Total Inbound Messages-Daily	inboundMessages	The report shows the top 10 queues based on the daily inbound messages.
EMS Top 10 Queues Total Inbound Messages-Monthly	inboundMessages	The report shows the top 10 queues based on the monthly inbound messages.
EMS Top 10 Queues Total Inbound Messages-Weekly	inboundMessages	The report shows the top 10 queues based on the weekly inbound messages.
EMS Top 10 Queues Total Inbound Messages-Yearly	inboundMessages	The report shows the top 10 queues based on the yearly inbound messages.
EMS Top 10 Queues Inbound Message Rate-Daily	inboundMessageRate	The report shows the top 10 queues based on the daily inbound message rate.
EMS Top 10 Queues Inbound Message Rate-Monthly	inboundMessageRate	The report shows the top 10 queues based on the monthly inbound message rate.
EMS Top 10 Queues Inbound Message Rate-Weekly	inboundMessageRate	The report shows the top 10 queues based on the weekly inbound message rate.
EMS Top 10 Queues Inbound Message Rate-Yearly	inboundMessageRate	The report shows the top 10 queues based on the yearly inbound message rate.
EMS Top 10 Queues Total Outbound Messages-Daily	outboundMessages	The report shows the top 10 queues based on the daily outbound messages.
EMS Top 10 Queues Total Outbound Messages-Monthly	outboundMessages	The report shows the top 10 queues based on the monthly outbound messages.
EMS Top 10 Queues Total Outbound Messages-Weekly	outboundMessages	The report shows the top 10 queues based on the weekly outbound messages.
EMS Top 10 Queues Total Outbound Messages-Yearly	outboundMessages	The report shows the top 10 queues based on the yearly outbound messages.

Report	Metric	Description
EMS Top 10 Queues Outbound Message Rate-Daily	outboundMessageRate	The report shows the top 10 queues based on daily outbound message rate.
EMS Top 10 Queues Outbound Message Rate-Monthly	outboundMessageRate	The report shows the top 10 queues based on monthly outbound message rate.
EMS Top 10 Queues Outbound Message Rate-Weekly	outboundMessageRate	The report shows the top 10 queues based on weekly outbound message rate.
EMS Top 10 Queues Outbound Message Rate-Yearly	outboundMessageRate	The report shows the top 10 queues based on yearly outbound message rate.
EMS Top 10 Queues Pending Message-Daily	pendingMessageCount	The report shows the top 10 queues based on the daily pending message count.
EMS Top 10 Queues Pending Message-Monthly	pendingMessageCount	The report shows the top 10 queues based on the monthly pending message count.
EMS Top 10 Queues Pending Message-Weekly	pendingMessageCount	The report shows the top 10 queues based on the weekly pending message count.
EMS Top 10 Queues Pending Message-Yearly	pendingMessageCount	The report shows the top 10 queues based on the yearly pending message count.
EMS Availability-Daily	Availability	The report shows the daily EMS Availability report for all EMS servers.
EMS Availability-Monthly	Availability	The report shows the monthly EMS Availability report for all EMS servers.
EMS Availability-Weekly	Availability	The report shows the weekly EMS Availability report for all EMS servers.
EMS Availability-Yearly	Availability	The report shows the yearly EMS Availability report for all EMS servers.
EMS Outbound Message Count-Daily	Outbound MessageCount	The report is based on the daily outbound message count.
EMS Outbound Message Count-Monthly	Outbound MessageCount	The report is based on the monthly outbound message count.
EMS Outbound Message Count-Weekly	Outbound MessageCount	The report is based on the weekly outbound message count.

Report	Metric	Description
EMS Outbound Message Count-Yearly	Outbound MessageCount	The report is based on the yearly outbound message count.
EMS Outbound Message Rate-Daily	Outbound MessageRate	The report is based on the daily outbound message rate.
EMS Outbound Message Rate-Monthly	Outbound MessageRate	The report is based on the monthly outbound message rate.
EMS Outbound Message Rate-Weekly	Outbound MessageRate	The report is based on the weekly outbound message rate.
EMS Outbound Message Rate-Yearly	Outbound MessageRate	The report is based on the yearly outbound message rate.

Chapter 8

Using Graphs

The TIBCO SPI provides a set of pre-configured graphs. If you want to access graphs from the HPOM console, you must install HP Performance Manager on the HPOM management server.

You can generate graphs using HP Performance Manager for the real-time data gathered from the managed nodes.

To access the graphs, select **Graphs** → **SPI for Tibco**

To access the graphs on **HPOM for UNIX**, select the active message and follow these steps:

1. Open the Message Properties window, and click **Actions**.
2. Under the Operator initiated action section, click **Perform**. Alternatively, right-click active message, select **Perform/Stop** Action and click **Perform Operator-Initiated Action**.

Note: When collection is disabled for a particular metric then the previous collected value will be logged to coda database. If the metric was never scheduled or the collection failed for the metric then -1 will be logged to coda database.

Graphs of TIBCO SPI are based on the following categories:

- TIBCO RV
- TIBCO BW
- TIBCO EMS

TIBCO RV Graphs

TIBCO RV Graphs

Graph	Metric	Description	Sum-marization
RV Hourly Missed and Re-transmitted packets	Missed Packets and Retransmitted Packets	The graph is displayed based on the hourly missed packets and retransmitted packets.	5 minutes
RV Daily Missed and Re-transmitted packets	Missed Packets and Retransmitted Packets	The graph is displayed based on the daily missed packets and retransmitted packets.	Hourly

Graph	Metric	Description	Sum-marization
RV Hourly Messages Sent and Received	Messages Sent and Received	The graph is displayed based on the hourly sent and received messages.	5 minutes
RV Daily Messages Sent and Received	Messages Sent and Received	The graph is displayed based on the daily sent and received messages.	Hourly

TIBCO BW Graphs

TIBCO BW Graphs

Graph	Metric	Description	Summarization
BW Application Hourly No.of processes Aborted and Suspended	Aborted / Suspended	The graph is displayed based on the number of jobs aborted or suspended hourly for all process definitions in the BW Engine.	5 minutes
BW Daily No.of Processes Aborted and Suspended	Aborted / Suspended	The graph is displayed based on the number of jobs aborted or suspended daily for all process definitions in the BW Engine.	Hourly
BW Hourly Total Errors and New Errors	Total Errors / New Errors	The graph is displayed based on the total errors or new errors raised hourly for each BW application.	5 minutes
BW Daily Total Errors and New Errors	Total Errors / New Errors	The graph is displayed based on the total errors or new errors raised daily for each BW application.	Hourly
BW Availability Hourly	BW App Availability	The graph is displayed based on the hourly BW application availability for each application.	5 minutes
BW Availability Daily	BW App Availability	The graph is displayed based on the daily BW application availability for each application.	Hourly

TIBCO EMS Graphs

TIBCO EMS Graphs

Graph	Metric	Description	Summarization
EMS Hourly Pending, Inbound and Outbound Messages	inboundMessageCount, outboundMessageCount and pendingMessageCount	The graph is displayed based on the hourly inbound message count, outbound message count and pending message count.	5 minutes
EMS Daily Pending, Inbound and Outbound Messages	inboundMessageCount, outboundMessageCount and pendingMessageCount	The graph is displayed based on the daily inbound message count, outbound message count and pending message count.	Hourly
EMS Hourly Inbound and Outbound Message Rate	InboundMessageRate and OutboundMessageRate	The graph is displayed based on the hourly inbound message rate and outbound message rate.	5 minutes
EMS Daily Inbound and Outbound Message Rate	InboundMessageRate and OutboundMessageRate	The graph is displayed based on the daily inbound message rate and outbound message rate.	Hourly
EMS Availability Hourly	EMS Availability	The graph is displayed based on the hourly EMS availability report for all EMS servers.	5 minutes
EMS Availability Daily	EMS Availability	The graph is displayed based on the daily EMS availability report for all EMS servers.	Hourly

Chapter 9

Performance Recommendations

Using the test results, you can derive the performance of TIBCO SPI for the microagents deployed in the TIBCO environment. The tests are performed for 1000 microagents. You can check the CPU utilization and memory utilization of the TIBCO SPI collector process.

Test Environment

The tests are performed using the following configuration:

Product Configuration

Product	Version
TIBCO SPI	2.00
HP Operations Agent	11.10

Infrastructure Configuration

Infrastructure Configuration	Value
Number of CPUs	2
Physical Memory	10 GB
Java JRE	TIBCO JRE 1.6.0_30

Test Setup

The following configuration is recommended for TIBCO SPI.

Test Configuration

Parameter	Value
TIBCO versions	TIBCO RV 8.4 and 8.3.2 TIBCO HAWK 4.9 TIBCO BW 5.10 and 5.9.3 TIBCO TRA 5.7.4 TIBCO EMS 6.1, 6.3 and 7.0
Domain Transport	EMS Stand-alone, RV, EMS Cluster
Number of TIBCO nodes	11

Parameter	Value
TIBCO domains	4
Total number of microagents	approximately 1000
Thread pool size	10
Java heap size	128 MB
Data logging	Using HP Operation Agents JCODA
Datasource	CODA
Test execution duration	5 Days
Policies deployed	32 TIBCO SPI monitoring policies deployed

Test Scenario

To verify the health of TIBCO environment which has 1000 microagents deployed consisting of nearly 950 BW Applications, 5 EMS servers, and 11 RVDs, the following processes are verified:

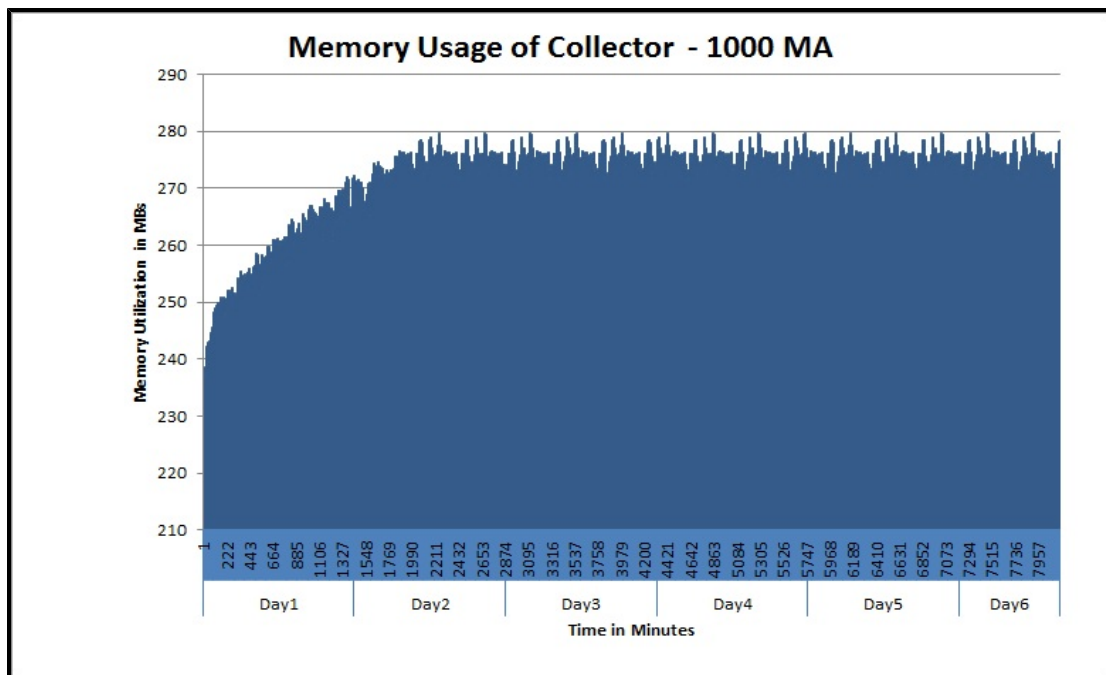
- **Discovery:** Discovering the TIBCO environment.
- **Collection:** Collection of metrics from TIBCO environment and data logging to CODA alerts generated by TIBCO SPI Policies.

To measure the parameters, the tests are performed for the following:

- **Memory Utilization:** TIBCO SPI collector process collects the memory utilization .
- **CPU Utilization:** TIBCO SPI collector process collects the CPU utilization.
- **Response Time:** The time taken for discovery and collection.

Memory Utilization

The graph depicts the usage of physical memory by TIBCO SPI collector monitoring 1000 microagents.

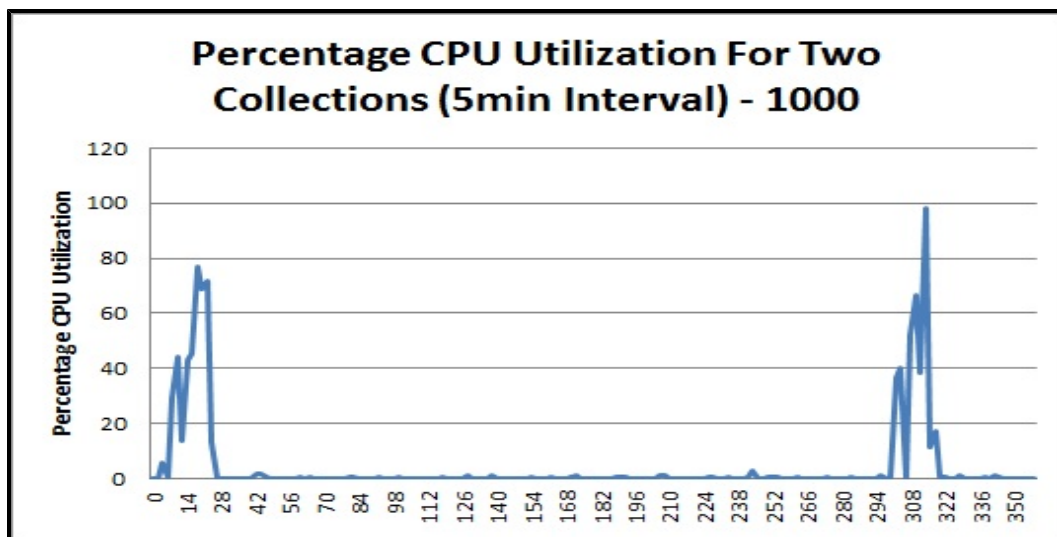


Facts that are derived from the test results :

Memory usage of the collector is approximately 280 to 300 MB and constant over a period of time.

CPU Utilization

The graph depicts the usage of CPU in percentage by TIBCO SPI collector monitoring 1000 micro agents for two consecutive collections.



Facts that are derived from the test results :

- Peak CPU usage is greater than 60% and is approximately 8 seconds for every collection.
- CPU utilization is less than 4% in between the collections.

Response Time for Logical Systems Data Access Operation

Observations:

- Average response time of TIBCO SPI collector for discovery with 1000 microagents is 2 minutes.
- Average response time of TIBCO SPI collector for collection of 10 metrics for each microagent with 1000 microagents is within 1 minute.

Recommendation

You can derive the following from the test results.

- Deploy TIBCO SPI within the domain.
- If there are approximately 1000 microagents in the domain, you can refer to the following table.

Configuration	Value
CPU	2 CPU
Physical Memory	2 GB
Java Heap Size	128 MB
Data logging	Using HP Operation Agents JCODA
Data Source	CODA

- You can use *One* instance of TIBCO SPI to monitor upto 1000 microagents.
- To monitor more than 1000 microagents TIBCO SPI must be deployed on multiple nodes. Each node must have the above mentioned configuration. The calculation used for SPI deployments in a TIBCO environment is:

Number of TIBCO SPI deployment = $(N/1000)$

where, N – Total number of microagents in the domain(s).

Note: One node can run only *One* instance of TIBCO SPI collector.

Chapter 10

Removing the TIBCO SPI

This chapter discusses the steps to remove the TIBCO SPI from the Windows and UNIX management server.

On the HPOM for Windows Management Server

Removing the TIBCO SPI from the managed nodes

To remove the TIBCO SPI from the managed nodes,

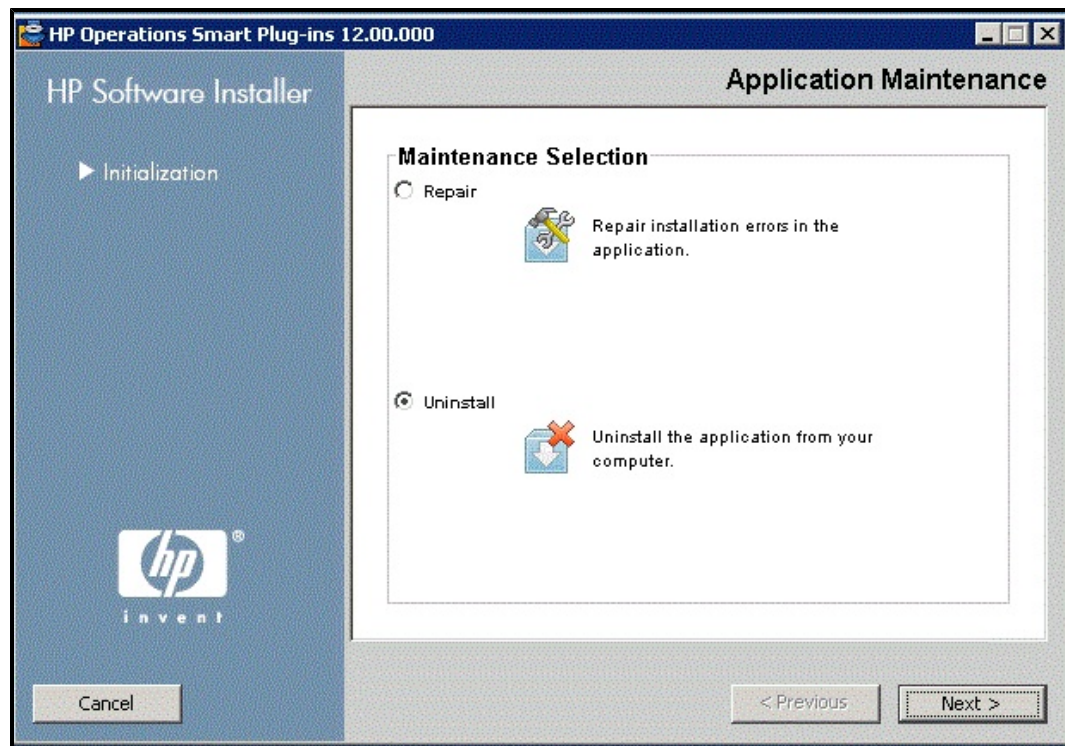
1. Stop the collector on the node, using **Stop Tibco SPI Collector** tool.
2. Undeploy all the policies and instrumentation from the category TIBCOSPI.

Removing the TIBCO SPI from the Management Server

To remove the TIBCO SPI from the management server, follow these steps:

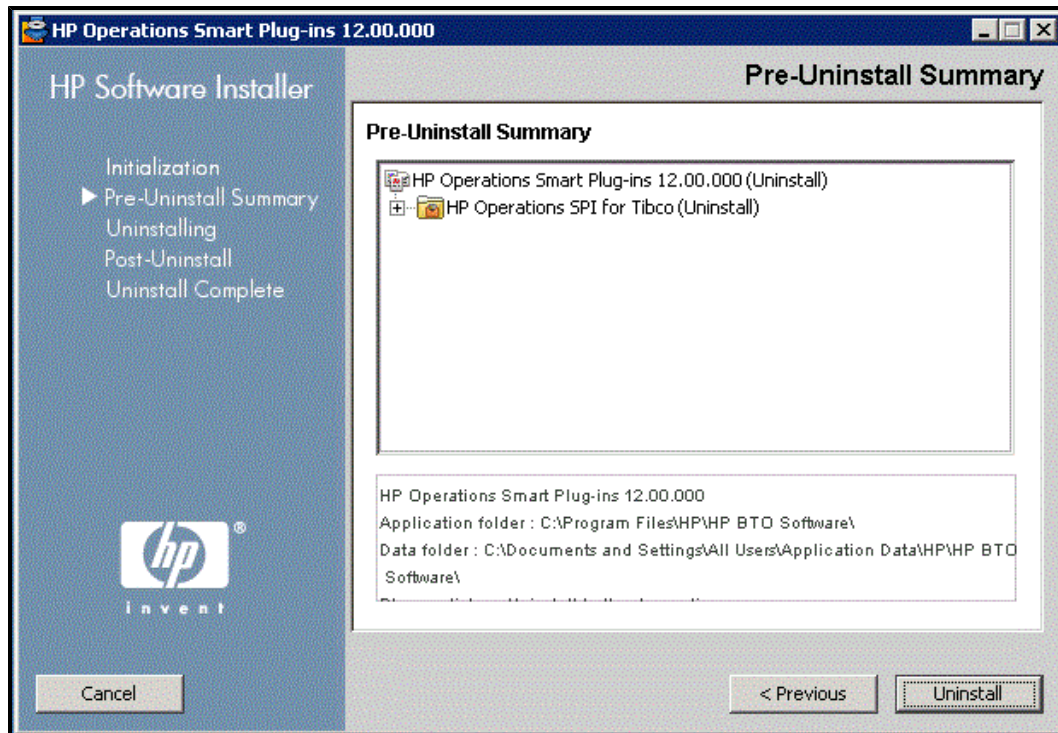
1. Insert the HP Operations Smart Plug-ins DVD into the DVD drive of the management server.

The Application Maintenance window opens.

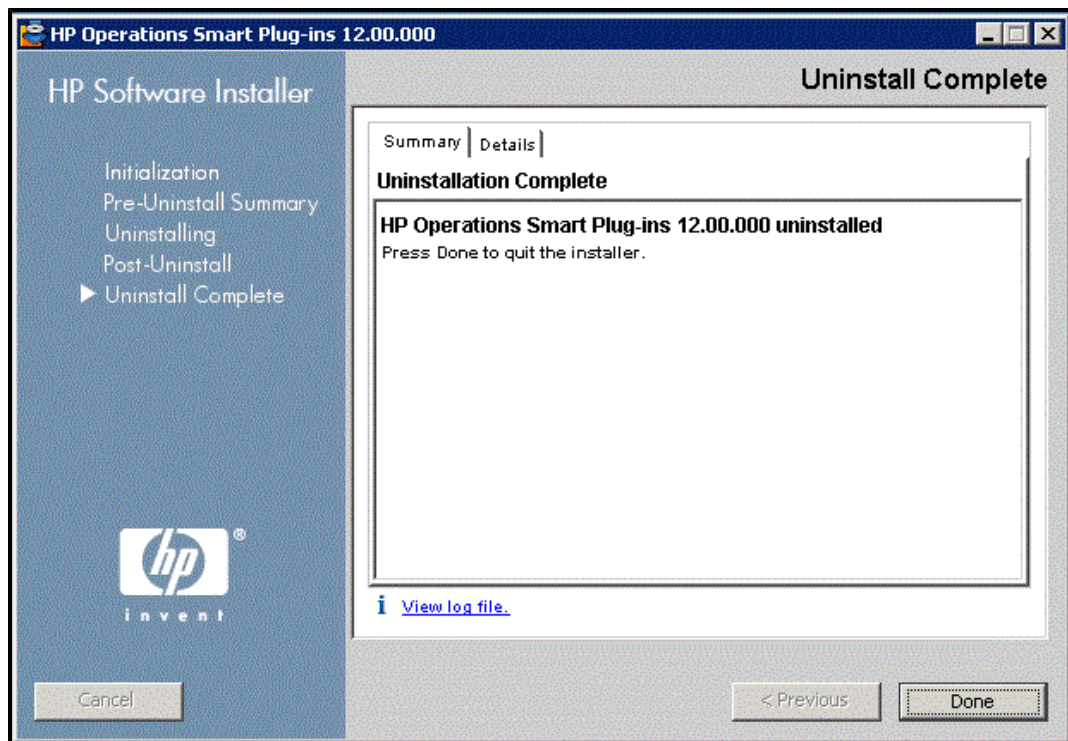


2. Select Uninstall and click **Next**.

3. The Pre-Uninstall Summary page appears. Click **Uninstall**.



4. The wizard starts uninstalling the SPI. Click **Done** to complete the removal of SPI.



Removing the TIBCO SPI from Clustered Environment

To remove the TIBCO SPI from a clustered environment, follow the steps in the section "[Removing the TIBCO SPI](#)" on page 107 .

When you complete the uninstallation on one management server, proceed to the next management server in the cluster.

You are notified when the uninstallation is complete. Uninstallation cleans up the entire TIBCO SPI node groups, policy groups, and instrumentation folders.

On the HPOM for UNIX management server

To remove TIBCO SPI from the HP-UX, Solaris, and Linux management server; follow these steps:

Removing the TIBCO SPI from the managed nodes

To remove the TIBCO SPI from the managed nodes,

1. Stop the collector on the node, using **Stop Tibco SPI Collector** tool.
2. Undeploy all the policies and instrumentation from the category TIBCOSPI.

Removing TIBCO SPI through 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 to view the console GUI properly by typing the following command :

```
export DISPLAY=<IP address or host name of local system>:0.0
```

4. To start the uninstallation of TIBCO SPI, type one of the following commands, depending on the type of 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. Click **OK**.

5. The Pre-uninstall Summary window appears. Select **Uninstall**.
6. The wizard starts uninstalling the SPI. Click **Done** to complete the removal of the SPI.

Removing TIBCO SPI through 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 uninstallation of TIBCO SPI, type one of the following commands, depending on the type of 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. Press **Enter** to continue.

4. The Maintenance Selection screen appears. Press the appropriate option (number) to start the removal of the SPI. Press **Enter** to continue.
5. You will receive a message when the uninstallation is completed.

Removing the TIBCO SPI from Clustered Environment

To remove the TIBCO SPI from each system in a cluster, follow the steps in the section "[Removing the TIBCO SPI](#)" on page 107 .

Chapter 11

Troubleshooting

This section describes the solutions or workarounds for the common problems encountered while working with TIBCO SPI. Areas covered in this section include:

- Collector
- Discovery
- Data Logging
- Logfile Location

Collector

Problem: Collector stopped collecting the metrics with Out of Memory error in the log file.

Solution:

- If an Out of Memory error appears, you need to change the jvm parameter in the `tibcfg.properties` file. The file is located in the following location:

Windows: %OvDataDir%\bin

HP-UX, Linux or Solaris: /var/opt/OV/bin/instrumentation

JVM Parameter:

```
JVMOPTS="-Xms64m -Xmx128m -XX:PermSize#eq#64m -  
XX:MaxPermSize#eq#128m"
```

- By default the minimum memory that the collector can take is set to 64mb and the maximum is set to 128mb.
- By default, the Permanent generation size (Permsize) is set to a minimum of 64 Mb and a maximum of 128 Mb.
- Increase these values to get rid of the "Out of Memory" error.

Problem: Metric collection timeout error appears as an alert on the management console.

Solution: Timeout takes place because of the following two reasons:

- **Cause 1:** Metric collection is taking more than two minutes which is default time out.
 - Open the instrumentation folder on the managed node.
 - Open the `tibcmconfiguration.properties` file and change the metric collection time out to a higher value.
 - You can configure the threadpool size and metric collection timeout in the above file.

For example: The threadpool size is *10* and the metric collection timeout is *120000* milliseconds. Following lines in the file can be modified to change metric timeout and threadpool size,

```
100-
1.collector=com.hp.openview.spi.tibco.collector.TibRvHawkCollector
{10}{120000}
100-
2.c-
collector=com.hp.openview.spi.tibco.collector.TibEmsHawkCollector
{10}{120000}
```

- **Case 2:** Microagent is not enabled for the metric.
 - You need to verify if the required microagent is enabled.
 - The list of required microagents is mentioned in the pre-requisites section of Configuring the TIBCO SPI, see ["List of microagents to be enabled for OOTB metrics to work for TIBCO SPI 2.00"](#) on page 35

Discovery

Problem: Discovery fails to create the *agtrep.xml* and inturn service map.

Solution:

1. Undeploy the discovery policy.
2. Remove the contents of `%ovdatadir%/tmp/agtrep`.
3. Take a backup of `agtrep.md` and `agtrep.xml` from the path mentioned below:
`%ovdatadir%/datafiles/agtrep.md` and
`%ovdatadir%/datafiles/agtrep.xml`.
4. Remove `%ovdatadir%/datafiles/agtrep.md` and
`%ovdatadir%/datafiles/agtrep.xml`.
5. Re-trigger the discovery policy.

Data Logging

Problem: Datasources is created in the HP Performance Agent. TIBCO SPI does not support the HP Performance Agent. You have to create a `nocoda.opt` file.

Solution:

TIBCO SPI does not support data logging in the HP Performance Agent. Before deploying the discovery policy, you must go to the managed node where TIBCO SPI is deployed and perform the following steps:

1. Open the `datasources` file from the directory
Windows: `%ovagentdir%/conf/perf`.
HP-UX, Linux, or Solaris: `/var/opt/OV/conf/dsi2ddf`
2. Remove the entry `TIBCO_SPI` from the `datasources` file.

3. Create an empty `nocoda.opt` file in the following directory `%ovdatadir%conf/dsi2ddf/`
If the folder `dsi2ddf` does not exist, create it.
4. Restart the agent.

This will create the `datasources` in CODA and will also start the discovery of TIBCO SPI.

Logfile Location

TIBCO SPI logfile is located in the following location on the managed node.

Windows: `%ovdatadir%\TIBCO_SPI\logs\Script_TibcoSpilog.log`

`%ovdatadir%\TIBCO_SPI\logs\TibcoSpilog.log`

HP-UX, Linux or Solaris: `/var/opt/OV/TIBCO_SPI/ogs/Script_TibcoSpilog.log`

`/var/opt/OV/TIBCO_SPI/ogs/TibcoSpilog.log`

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: