HP Operations Smart Plug-in for SAP

for HP Operations Manager for Windows®

Software Version: 11.10

Printed On-line Help

Document Release Date: February 2009
Software Release Date: October 2008

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 Notices

Trademark Notices

Acrobat®, Adobe®, and PostScript® are trademarks of Adobe Systems Incorporated.

Intel®, Itanium®, and Pentium® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

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

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

This guide's title page 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

You can visit the HP Software Support web site at:

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

HP Software Support Online provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support 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 find more information about access levels, go to:

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

For more information about HP Passport, go to:

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

Contents

1 Introducing the Smart Plug-in for SAP

This section describes what information is in the *HP Operations Smart Plug-in for SAP Administrator's ReferenceHP Operations Smart Plug-in for SAP On-line Help* and where you can find it.

Overview

The *HP Operations Smart Plug-in for SAP On-line Help* provides information that is designed to help the administrators of both HP Operations Manager for Windows (HPOM for Windows) and SAP NetWeaver to configure the SPI for SAP to suit the needs and requirements of the SAP NetWeaver landscape, which they plan to manage with HPOM for Windows. The on-line Help system also explains how to install and configure the various, additional sub-agents that come with the SPI for SAP. Finally, the *HP Operations Smart Plug-in for SAP On-line Help* describes how to integrate the SPI for SAP with performance-related products that are available as part of HP Software.

The *HP Operations Smart Plug-in for SAP On-line Help* consists of the following sections:

- Customizing the SPI for SAP Monitors on page 19

  A general introduction to the SPI for SAP monitors, including configuration-file locations, environment variables, and information about default configurations.

- The SPI for SAP Alert Monitors on page 45

  Reference and configuration information for the CCMS alert monitors `r3monal`, `r3monpro` and `r3mondev`.

- The SPI for SAP Alert-Collector Monitors on page 95

  Reference and configuration information for `r3moncol` and the alert-collector monitors `r3monale`, `r3mondmp`, `r3monwpa` and so on.

- Understanding Message Flow on page 179

  This section describes how to use both HPOM for Windows functionality and CCMS to control the flow of messages between SAP NetWeaver and HPOM for Windows.

- The SPI for SAP Performance Monitors on page 201

  This section describes how to install, configure, and use the SPI for SAP performance monitors.

- The SAP ITS Monitor on page 245

  This section describes how to install and configure the ITS Monitor. The **Internet Transaction Server** (ITS) provides the SAP NetWeaver user with an SAP NetWeaver transaction interface in a web browser.

- Monitoring SAP NetWeaver Web Application Server (J2EE) on page 265

This section includes details on monitoring the SAP NetWeaver Web Application Server (J2EE) with the new set of policies.

- Service Views on page 347

  This section introduces the concept of service views and explains how to use service views to improve the management of your SAP NetWeaver landscape.

- Service Reports on page 355

  This section describes how to install the SPI for SAP service reports, configure the HP Reporter to generate the reports, and use the reports to monitor and manage your SAP NetWeaver landscape.

2 Customizing the SPI for SAP Monitors

This section describes how to set up the SPI for SAP monitors and deploy them to the SAP servers in your SAP landscape.

Introduction to the SPI for SAP Monitors

The SPI for SAP includes a set of monitors, which you configure to run at regular intervals to collect information regarding various aspects of your SAP environment's health.

The HPOM for Windows administrators, working from the HPOM for Windows console, deploy the appropriate SPI for SAP message-source policies to the SAP servers which they want to manage and monitor with HPOM for Windows. Monitor deployment is usually completed as part of the SPI for SAP installation and configuration process.

If you have never configured the SPI for SAP monitors, you will want to read the detailed description of each alert monitor and alert-monitor configuration file. The alert-monitor configuration files include information about default configurations as well as a list of changes you need to make to ensure that the monitor works correctly in your SAP environment.

This section contains information about the following topics:

Before Using the SPI for SAP Monitors

Before using any of these monitors, be sure to complete the following tasks:

- Set up the required SAP users and their associated logons as described in the *HP Operations Smart Plug-in for SAP Configuration Guide*
- Specify in the `r3itosap.cfg` file details of all SAP systems to monitor. You can define entries in `r3itosap.cfg`:
  - as part of the installation procedure (refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*)

    or,

— At any time, using the configuration-file policy editor. For more information, see r3itosap: Monitoring SAP NetWeaver on page 20.

If the SAP instance you want to monitor is part of a high-availability cluster, such as MC/ServiceGuard, you need to add an extra entry to the “cluster host mapping” section of the `r3itosap.cfg` file to tell the SPI for SAP about the nodes configured in the cluster. If the host-mapping entry is not present in the `r3itosap.cfg` file, the SPI for SAP might encounter problems monitoring the nodes in the cluster, for example; resolving the hostname of the cluster nodes, starting the monitors at the correct time, and associating messages with the appropriate managed nodes.

For more information about configuring the SPI for SAP to monitor SAP in a high-availability environment, see the *HP Operations Smart Plug-in for SAP Configuration Guide*.

r3itosap: Monitoring SAP NetWeaver

This section describes how to use the configuration-file policy editor to modify the `r3itosap.cfg` configuration file; the `r3itosap.cfg` configuration file defines the SAP NetWeaver Systems, which the SPI for SAP should monitor. To complete this task successfully, you need to ensure that you have already installed the ConfigFile Editor and, in addition, the appropriate SPI for SAP policies. For more information about installing packages and policies, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.

You have to set up SAP NetWeaver users for each SAP NetWeaver client. The list of SAP NetWeaver clients you made in “Before You Begin” in the *HP Operations Smart Plug-in for SAP Configuration Guide* includes the information you need for each configuration line. For more information about how to set up SAP NetWeaver users for HPOM for Windows, see “Setting Up an SAP User for HPOM” in the *HP Operations Smart Plug-in for SAP Configuration Guide*.

Using the format of the examples in the `r3itosap.cfg` configuration file, add an entry for each SAP NetWeaver instance, which you want to monitor with the SPI for SAP. In the central, SPI for SAP, monitor-configuration file `r3itosap.cfg`, the string =default is associated with the default ITOUSER password “HPSAP_30”. If you intend to make use of your own SAP user logins, you need to replace =default with the appropriate user password. If you use the HPOM for Windows configuration-file policy editor to edit the `r3itosap.cfg` file, the policy editor encrypts the password automatically when you save the file.

`r3status`, the tool the SPI for SAP uses to monitor the status of SAP Systems, does not attempt to verify the existence of the SAP Systems specified in `r3itosap.cfg`. If `r3status` cannot find a named SAP instance, for example: because of a spelling mistake, it reports the instance as unavailable.

If the SAP instance you want to monitor is part of a high-availability cluster, such as MC/ServiceGuard, you need to add an entry to the “cluster host mapping” section of the `r3itosap.cfg` file to tell the SPI for SAP about the nodes configured in the cluster. If the host-mapping entry is not present in the `r3itosap.cfg` file, the SPI for SAP could encounter problems monitoring the nodes in the cluster, for example; resolving the hostname of the cluster nodes and associating messages with the correct managed node in the cluster.

For more information about the SPI for SAP in high-availability clusters and configuring the `r3itosap.cfg` file, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.

The SPI for SAP Monitors

Table 1 provides an overview of SPI for SAP alert-monitors.

Table 1 The Alert Monitors

Alert Monitor	Monitor Function
`r3monal` [a]	Monitors SAP NetWeaver system log events and alerts from the internal SAP CCMS 4.x alert monitor
`r3mondev`	Monitors errors in SAP trace and log files
`r3mondisp`	Monitors the status of the ABAP dispatcher for all SAP instances configured in the SPI for SAP's central configuration rile `r3itosap.cfg`
`r3monpro`	Monitors SAP work processes and database processes
`r3monsec`	Monitors the security settings in SAP for instances configured in the `r3itosap.cfg` file
`r3status`	Monitors the status of the SAP instances configured in the `r3itosap.cfg` file

a. SAP syslog monitor `r3monxmi` is now obsolete.

Table 2 provides an overview of the alert-collector monitors used by `r3moncol`, the SPI for SAP alert collector.

Table 2 The r3moncol Alert-Collector Monitors

Alert-Collector Monitor	Monitor Function
`r3monaco`	Although this is not, strictly speaking, an alert-collector monitor, you must assign `r3monaco` to the managed nodes to monitor SAP's Temporary Sequential (TemSe) file. For more information, see Monitoring the TemSe file on page 177.
`r3monale`	Monitors the status of iDOCs in the SAP NetWeaver System
`r3monchg`	Monitors the SAP NetWeaver system change options.
`r3moncts`	Monitors the correction-and-transport system.
`r3mondmp`	Monitors ABAP/4 Dumps.

Table 2 The r3moncol Alert-Collector Monitors (cont'd)

Alert-Collector Monitor	Monitor Function
r3monjob	Monitors SAP NetWeaver batch jobs.
r3monlck	Monitors the Enqueue process, which manages logical locks for SAP NetWeaver transactions and reports on obsolete locks.
r3monoms	Monitors the operation mode switch to determine whether a scheduled operation mode started after the specified time. Note that changes in SAP mean there are no operation-mode switch errors to monitor in WebAS 7.
r3monrfc	Checks the status of RFC destinations in an SAP environment
r3monspl	Monitors spooler entries, spooler errors, and print errors.
r3montra	Monitors the transport system.
r3monupd	Monitors the update process for active status and errors
r3monusr	Monitors the number of users logged-in to SAP NetWeaver.
r3monwpa	Monitors the status of the work processes. It reports any processes that are running in debug, private, or no restart modes, compares the number of configured work processes with the actual number running, and checks the number of expected work processes waiting and the number running

Important Monitor-Configuration Concepts

This section describes the concepts underpinning the CCMS alert-monitors and, in addition, explains how to configure the monitors. The section covers the following areas:

Monitor-Configuration Files

Each alert or alert-collector monitor has an associated configuration file, which you can edit to define your own rules for how you want to monitor CCMS alerts. However, the monitors all have default configurations, which you can use without modification. For more information about the contents of the SPI for SAP's monitor-configuration files, see:

- The SPI for SAP Monitor-Configuration File on page 26

  General information which applies to the configuration of *all* the SPI for SAP monitors

- The Alert-Monitor Configuration Files on page 46

  Information about the keywords and parameters, which you use to configure the alert monitors `r3monal`, `r3mondev`, `r3monpro`, and `r3monsec`.

- The r3mondisp Configuration File on page 80

  Information about the keywords and parameters, which you use to configure the ABAP dispatch-queue monitor, `r3mondisp`.

- The r3status Configuration File on page 69

- The Alert-Collector Monitor Configuration Files on page 105

  Information which applies to the configuration of the alert-collector monitor `r3moncol` and the alert collectors it uses, for example; `r3monale`, `r3mondmp`, `r3monjob`, and so on.

Monitor-Configuration File: Global vs. Local

For more information about when to use each of these deployment methods and for instructions on editing the configuration files, see The SPI for SAP Monitor-Configuration File on page 26.

Monitor-Configuration Modes

The SPI for SAP supports the following configuration modes:

- **Global**

  You define in a single configuration file the monitoring conditions for all managed nodes. If you specified a *global* configuration, the monitoring conditions you define must cover the monitoring needs of all managed nodes.

- **Local**

  You define the monitoring conditions for a particular node in a configuration file associated only with that single, managed node. If a *local* configuration is used, each node can have its own configuration file, which defines only the monitoring conditions for that particular node.

You can deploy a mixture of global and local configurations. For an explanation of the relationship between local and global configuration as well as instructions on the use of each configuration mode, see Distributing Alert-Monitor Configuration Files on page 42.

Alert Monitor Order of Precedence

Each time an alert monitor runs, its behavior is determined by information defined in an alert-monitor-specific configuration file. An alert monitor chooses which configuration file to use according to a defined “order of precedence”, as follows:

1. The monitor first checks for the presence of the SAPOPC_<*R3monitor_name*>_CONFIGFILE variable and determines the location of the configuration files from this. For more information about the SAPOPC_<*R3monitor_name*>_CONFIGFILE variable, see the section about the specific monitor you want to configure, for example; r3monpro: Environment Variables on page 64.
2. On UNIX managed nodes:
   a. Local configuration file

      The monitor checks for (and if found uses) the HPOM for UNIX *local* configuration file in:

      <OvDataDir>`/conf/sapspi/local`

   b. Global configuration file

      If the monitor does not find an HPOM for UNIX local configuration file, the monitor checks for (and if found uses) the OVO for UNIX global configuration file in:

      <OvDataDir>`/conf/sapspi/global`
3. On Windows managed nodes:
   a. Local configuration file

      The monitor checks for (and if found uses) the HPOM for Windows local configuration file in:

      %OvAgentDir%`\conf\sapspi\local`

   b. Global configuration file

      If the monitor does not find an HPOM for Windows local configuration file, the monitor checks for (and if found uses) the HPOM for Windows *global* configuration file in:

      %OvAgentDir%`\conf\sapspi\global`

Remote Monitoring with the Alert Monitors

The SPI for SAP includes a feature which allows you to extend the scope of all the alert, alert-collector, and performance monitors (except `r3mondev`, `r3monpro`, `r3mondisp`) to monitor the status of SAP on remote SAP servers, which are *not* HPOM for Windows managed nodes and where the SPI for SAP is *not* installed. You set up and perform the remote monitoring from an HPOM for Windows managed node, where the SPI for SAP software is running.

Although the SAP Server defined in the RemoteHost parameter is not an HPOM for Windows managed node, it must still be present in the HPOM for Windows node list. If you do not add the SAP Server defined in RemoteHost to the HPOM for Windows node list, HPOM for Windows cannot resolve the host name associated with the remote host and, as a consequence, cannot display any messages from the remote host in the HPOM for Windows console.

In addition, the SAP Server defined in RemoteHost must appear in the `r3itosap.cfg` file to ensure that the SPI for SAP can log into (and extract information from) the SAP instances it is monitoring on the RemoteHost. For more information about the `r3itosap.cfg` file, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.

Note that SPI for SAP tools cannot start a SAP GUI on an SAP System, which the SPI for SAP is monitoring remotely from an HPOM for Windows Managed Node.

To make use of the remote-monitoring feature provided by the SPI for SAP, for example; to monitor an SAP System running in an environment that is not supported by the SPI for SAP, you need to perform the following actions. Specifying Individual Remote Servers to Monitor on page 25 shows how a new line is required for each *additional* SAP server, which you want to monitor remotely.

- Enable the **RemoteMonitoring** keyword by removing the leading hash symbol "#" in each monitor's configuration file.
- Define the name of the *local* host, which you want to perform the monitoring. Note that you need a new line for each *local* host that you want to associate with a remote host.
- Define the name of the *remote* SAP server (*RemoteHost*), which you want to monitor.
- Make sure that the remote host is added to the HPOM for Windows node list.

The RemoteMonitoring keyword accepts the following parameters:

- **LocalHost**

  This is the name of the local HPOM for Windows managed node where the SPI for SAP software is running and whose HPOM for Windows agent you want the SPI for SAP to use to remotely monitor the SAP server defined in the parameter "RemoteHost".

- **RemoteHost**

  This is the name of the *remote* SAP server you want to monitor from the host defined in the parameter "LocalHost". Although the remote host does not have the SPI for SAP software installed and is *not usually* an HPOM for Windows managed node, it must be present in the HPOM for Windows node list to ensure that messages are handled correctly.

- **SAP System/Number** (`r3monal` *only*)

  The CCMS alert and syslog monitor `r3monal` needs to know both the ID and the Number of the SAP System running on the SAP server defined in the parameter "RemoteHost".

For more information about any additional requirements when defining remote monitoring with the alert monitors, and in particular `r3monal` (the CCMS alert monitor), see The SPI for SAP Monitor-Configuration File on page 26 and The Alert-Monitor Configuration Files on page 46.

Specifying Individual Remote Servers to Monitor

```
#------------------------------------------------------------
# Remote               LocalHost    RemoteHost
# Monitoring
RemoteMonitoring       =sap1       =sdsap1
RemoteMonitoring       =sap1       =sdsap2
RemoteMonitoring       =sap2       =sdsap3
#------------------------------------------------------------
```

Note that you can use the Alert-classes section at the end of the monitor-configuration file to associate an instance of a monitor with a specific host, SAP instance, or processes on the remote server in the same way as you can with a normal (local) managed node. For more information about configuration-file keywords, see The SPI for SAP Monitor-Configuration File on page 26.

The SPI for SAP Monitor-Configuration File

During SPI for SAP installation and configuration, the SAP specialist must set up initial configuration values for the SPI for SAP monitors and deploy the modified configuration files to the managed nodes.

Each configuration file provided with the SPI for SAP defines default settings by means of keyword. Some keywords can only be used with specific monitors; all which are specific to a particular sub-section of the monitor configuration file. The information below lists the keywords that appear in the various sub-sections of the configuration file and explains the contents of the alert-classes section at the end of the configuration file, where you define conditions that, when met, generate messages about the SAP alerts you are monitoring. You can also see which keywords you can use with which monitors and find out the permitted values for keyword parameters:

- AlertMonFun on page 27

  Configure the `r3moncol` alert collectors in the SAP System
- AlertDevMon on page 27

  Configure trace- and log-file monitoring in the SAP System
- AlertMonPro on page 27

  Configure process monitoring per SAP System
- AlertInstMonPro on page 28

  Configure process monitoring per SAP instance
- AlerMonSyslog on page 28

  Configure filtering of CCMS alerts or system logs
- Alert Classes on page 28

  In the alert-classes section at the end of the configuration file, valid keywords are monitor-specific.
- CCMS Acknowledge Message on page 31
- CCMS Monitor Set on page 32
- Disable Monitoring With Severity on page 32
- DP Queue Check on page 33

  Monitor the size of the ABAP-dispatcher queue
- Enable DP Queue Check on page 35

  Check the status of the ABAP-dispatcher
- History Path on page 36
- Instance Profile Path on page 36

- Remote Monitoring on page 37
- RFCTimeOut on page 38
- Severity Values on page 38

  The Severity Values section contains the Severity<*Level*> keyword
- Trace File on page 39
- Trace Level on page 39
- XMISyslogMode on page 40

AlertMonFun

Only with `r3moncol`

Use the AlertMonFun keyword in the `r3moncol` configuration files to configure the SPI for SAP alert collectors, which monitor internal SAP alerts generated by, for example: the iDOC monitor, the ABAP-dump monitor, the spooler monitor, and so on. The AlertMonFun keyword requires a value for the following parameters:

```
AlertMonFun =<SAP Hostname> =<SAP System> =<SAP Number> \
=<SAP Client> =<AlertMonitor> =<Enable/Disable> \
=<OpC Severity> =<OpC Object> =<OpC MsgGroup> \
=<Alerttype> =<RFC Parameter>
```

For more information about the parameters that you need to define for the AlertMonFun keyword, see Alert-Collector Keywords and Parameters on page 105.

AlertDevMon

Only with `r3mondev`

Use the AlertDevMon keyword in the `r3mondev.cfg` file to configure the SPI for SAP to monitor trace- and log-files in the SAP System. The AlertDevMon keyword requires a value for the following parameters:

```
AlertDevMon =<SAP System> =<SAP Number> =<Enable/Disable> \
=<Filemask> =<Opc Severity> =<Opc Object> =<OpC MsgGroup>
```

For more information about the parameters that you need to define for the AlertDevMon keyword, see Alert Classes on page 28.

AlertMonPro

Only with `r3monpro`

Use the AlertMonPro keyword in the `r3monpro.cfg` file to configure the SPI for SAP to monitor SAP-related processes per SAP System. On SAP servers running the UNIX operating systems, `r3monpro` can identify processes at the instance level with Alert*Inst*MonPro. For more information about `r3monpro`, see r3monpro: The SAP Process Monitor on page 63.

The AlertMonPro keyword requires a value for the following parameters:

```
AlertMonPro =<Hostname> =<Process name> =<Enable/Disable> \
=<Mode> =<Process number> =<Opc Severity> =<Opc Object> \ =<OpC MsgGroup>
```

For more information about the parameters that you need to define for the AlertMonPro keyword, see Alert Classes on page 28.

AlertInstMonPro

Only with `r3monpro` in UNIX

Use the AlertInstMonPro keyword in the `r3monpro.cfg` file to configure the SPI for SAP to monitor SAP-related processes per SAP *instance*. The AlertInstMonPro keyword requires a value for the following parameters:

```
AlertInstMonPro =<Hostname> =<Process name> \
=<Enable/
Disable> =<Mode> =<Process number> =<Opc Severity>\=<Opc Object> =<OpC MsgGro
up>
```

For more information about the parameters that you need to define for the AlertInstMonPro keyword, see Alert Classes on page 28.

AlerMonSyslog

Only with `r3monal`

Use the AlerMonSyslog keyword in the `r3monal.cfg` file to configure the SPI for SAP to monitor Syslog filtering can be used *only* with the `r3monal` alert monitor CCMS alerts or system logs in combination with the XMI/XAL interface. If you want the format of the syslog alerts to resemble the style used by the now-obsolete `r3monxmi` monitor, see also XMISyslogMode on page 40. The AlerMonSyslog keyword requires a value for the following parameters:

```
AlerMonSyslog =<SAP System> =<SAP Number> =<SyslogId>
=<Enabled/Disabled>
```

For more information about the parameters that you need to define for the AlerMonSyslog keyword, see Alert Classes on page 28.

Alert Classes

The alert-classes section at the end of the monitor-configuration file allows you to use keywords and parameters to define conditions that, when met, generate messages about the SAP alerts you are monitoring. The contents of the alert-classes section change according to the monitor you are configuring; some monitors require a specific keyword, and each keyword requires a specific combination of parameters to configure a given SPI for SAP monitor.

For example, the keywords AlertMonPro and AlertInstMonPro appear exclusively in the configuration file for the SAP-process monitor, `r3monpro`. However, all `r3moncol` monitors use the keyword AlertMonFun to configure alert monitoring. The parameters `SAP Hostname`, `SAP System`, and `SAP Number` are present in all the monitor-configuration files, but the `=CHANGE_OPT` alert-type parameter can only be used with `r3monchg`, the SAP System-change Monitor.

For more information about which alert types and parameters are allowed with which monitor-specific alerts, see the information in this section and, in addition, the section which corresponds to the individual monitor you want to configure, for example: `r3monale`, or `r3mondmp`.

The SPI for SAP monitors are configured by default to manage *all* SAP Systems, which you define in the SPI for SAP's central configuration file `r3itosap.cfg`. The monitor-configuration files should not be edited by anyone who does not have a detailed knowledge of SAP NetWeaver and, in addition, the local SAP NetWeaver landscape, which you want to manage with the SPI for SAP.

The following list shows *all* the parameters in the alert-classes section of *all* the SPI for SAP monitor configuration files. Where appropriate, restrictions are indicated in brackets (), for example; (r3mondev only).

- **AlertMonitor** (r3moncol and r3monsec only):

=<*Monitor_Name*>	The short form of the alert monitor you are configuring, for example; =ALE for r3monale, =CTS for the r3moncts, and so on. Note: =SECURITY for r3monsec.

- **Alerttype** (r3moncol and r3monsec only):

=<*Alerttype*>	The alert type is monitor specific. For example, r3monale uses the IDOC_CURRENT_STATUS alert type to monitor alerts relating to the status of iDOCs; r3mondmp uses the alert type ABAP4_ERROR_EXIST to monitor alerts relating to each ABAP dump that occurs in a monitored SAP System. For more information about which alert types belong to which alert-collector monitor, see the "Alert-Types" section for a given monitor, for example; r3monale: The iDOC-Status Monitor on page 113 includes the alert type IDOC_CURRENT_STATUS on page 114.

- **Enable/Disable**:

=0	*Disable* the monitor
=1	*Enable* the monitor. This is the default setting.

- **Filemask** (r3mondev only):

=<*File_Name*>	The name of the trace file you want r3mondev to monitor. You can use the wildcard "*" (asterisk) to monitor multiple file names, for example; **=dev_***

- **Mode** (r3monpro only):

=<*mode_value*>	The mode or way in which you want to evaluate ProcessNumber, for example; Max, Min, Exact, and Delta. For more detailed information about the possible values, see r3monpro: The SAP Process Monitor on page 63.**s**

- **OPCMsgGroup**:

=<*HPOM_Msg_Group*>	The name of the HPOM for Windows message group to which the generated message belongs, for example: R3_CTS, or R3_DMP. The default names all start with "R3_" and reflect the names of the alert monitors to which they correspond, for example; r3moncts or r3mondmp. Note that if you change the names of the HPOM for Windows message groups in the monitor-configuration files, remember to ensure that the changes are reflected in the message conditions to avoid the generation of unmatched messages.

- **OPC Object**:

=<*HPOM_Object*> The HPOM for Windows object associated with the generated message. The object names tend to reflect the names of the alert types associated with the alert-collector monitor, for example; REQUEST or TASK for `r3moncts`.

If you change the names of the HPOM for Windows objects in the monitor-configuration files (or add new ones), you must ensure that these changes are reflected in the message conditions to avoid the generation of unmatched messages.

The =SyslogId string in the OPC Object field has nothing to do with the SyslogId alert parameter described below, which only appears in the syslog-filtering section of the `r3monal.cfg` file.

- **OPC Severity**:

  =<*HPOM_Msg_Severity*> The severity level of the HPOM for Windows message you want to map the CCMS alert to, for example: Normal, Warning, Major, Critical.

- **Process Name** (`r3monpro` only):

  =<*NameSID*> The name of the SAP process you want `r3monpro` to monitor.

- **Process Number** (`r3monpro` only):

  =<*nn*> The number (nn) of instances of the SAP process defined in ProcessName. You can qualify the number with Max, Min, Exact, and Delta. For more information see r3monpro: The SAP Process Monitor on page 63.

- **RFC Parameter** (`r3moncol` only):

  =<*RFC_Param*> The name of the parameter followed by any required query conditions, each with the prefix "=", for example; =CP (for "Contains Pattern") or EQ for ("Equals"). For more information about query conditions, see Alert-Collector Monitor Query Conditions on page 99. For more information about monitor-specific, alert-type parameters, see the appropriate monitor description, for example: Task 24 on page 114 for the `r3monale` monitor.

- **SAP Client**:

  =ALL Monitor all SAP instance numbers with the SPI for SAP. This is the default setting.

  =<*ClientID*> The number of the specific SAP client you want to monitor, for example; 099. Use a new line for each individual host.

- **SAP Hostname**:

=ALL	Monitor all SAP hosts with the SPI for SAP. This is the default setting.
=<*SAP_host*>	The host name of a specific SAP server you want to monitor. Use a new line for each individual host.

- **SAP Number**:

=ALL	Monitor all SAP instance numbers with the SPI for SAP. This is the default setting.
=<*Instance*>	The number of the specific SAP instance you want to monitor, for example; 00, 99. Use a new line for each host.

- **SAP System**:

=ALL	Monitor all SAP Systems with the SPI for SAP. This is the default setting.
=<*SAP_SID*>	The ID of a specific SAP System want to monitor, for example; DEV. Use a new line for each individual host.

- **SyslogId** (`r3monal` only):

=A00	The *lower* end of the range of SAP syslog IDs, whose CCMS Alerts or syslogs you want to monitor.
=ZZZ	The *upper* end of the range of SAP syslog IDs, whose CCMS Alerts or syslogs you want to monitor.

CCMS Acknowledge Message

The `r3monal` monitor uses the CCMSAcknowledgeMessage keyword to switch the CCMS auto-acknowledge feature on or off in SAP. CCMS alerts which are complete do not generate messages in HPOM for Windows. . This keyword requires a value for the following parameters:

```
CCMSAcknowledgeMessage =<SAP System> =<Ack. Filtered
Messages> =<Enabled/Disabled>
```

- **SAP System**:

  The SAP System ID whose CCMS Alerts you want to acknowledge (or **complete**) in SAP.

- **Ack. Filtered Messages**:

  This feature determines whether SAP acknowledges (or completes) CCMS Alerts which match the defined conditions in CCMS or not. Acknowledged CCMS alerts do not generate messages in HPOM.

=0 *Do not* acknowledge (complete) the CCMS Alerts in SAP. This is the default setting and leads to matched alerts generating an HPOM for Windows message.

=1 *Acknowledge* the CCMS Alerts in SAP. This is the same as clicking the `[Complete Alert]` button in SAP CCMS. No messages are sent to HPOM for Windows.

- **Enable/Disable**:

=0 *Disable* the auto-completion of CCMS alerts. Note that this also disables the setting for **Ack. Filtered Messages**. This is the default setting.

=1 *Enable* the auto-completion of CCMS alerts.

CCMS Monitor Set

Define a CCMS monitor set to use with the new, enhanced XMI/XAL interface (BAPI). The CCMSMonitorSet keyword requires a value for the following parameters:

```
CCMSMonitorSet =<SAP System> =<SAP Number> =<Monitor Set>
=<Monitor>
```

- **SAP System**:

  The SAP System ID whose CCMS Alerts are defined in the parameter Monitor Set

- **SAP Number:**

  This SAP *instance* number of the SAP System whose CCMS Alerts are defined in the parameter Monitor Set

- **Monitor Set**:

  =SAP CCMS Technical Expert Monitors

  The name of the monitor set as it appears in the CCMS Alert- Monitor tree.

- **Monitor**:

  =System / All Monitoring Segments / All Monitoring Context

  The names of the monitors belonging to the monitor set defined in the parameter “Monitor Set” separated by a forward slash (/).

Disable Monitoring With Severity

Only with `r3mondisp`, the ABAP dispatcher monitor

Specify which `r3mondisp` message severity should trigger the disabling of integrated SPI for SAP monitors to prevent the monitors increasing loads unnecessarily by requesting work processes from the SAP Systems, whose ABAP dispatcher you are monitoring with the SPI for SAP. The DisableMonitoringWithSeverity keyword accepts the following parameters:

```
DisableMonitoringWithSeverity   =<hostname>    =<SID>
=<InstanceNr> =<Severity>
```

- **Hostname**:

  The name of the SAP Server where the instance is running whose ABAP dispatcher you want to monitor:

=ALL	All hosts monitored by the SPI for SAP. This is the default setting.
=<*SAP_host*>	The name of the SAP server, where you want to disable dispatcher-queue monitoring. Use a new line (and keyword) for each, individual SAP server.

- **SID**:

  The SAP System ID of the instance whose ABAP dispatcher you are monitoring:

=ALL	All System IDs which the SPI for SAP monitors. This is the default setting.
=<*SAP_SID*>	The SAP System ID of the instance whose ABAP dispatcher you want to monitor, for example: “SP1”

- **InstanceNr**:

  The number of the SAP instance whose ABAP dispatcher you are monitoring:

=ALL	All System IDs which the SPI for SAP monitors. This is the default setting.
=<*SAP_InstNr*>	The number of the SAP instance whose ABAP dispatcher you want to monitor, for example: “45”

- **Severity**:

  The severity level of the message `r3mondisp` sends which would trigger the disabling of SPI for SAP monitors that require a work process to logon to SAP, for example: “warning”

The DisableMonitoringWithSeverity keyword must be used in conjunction with keywords DPQueueCheck, which you configure in the `r3mondisp.cfg` file, and EnableDPQueueCheck, which you define in the configuration file of the SPI for SAP monitor you want to integrate with `r3mondisp`.

DP Queue Check

Only with `r3mondisp`, the ABAP dispatcher monitor

Manages the pro-active monitoring of the ABAP dispatcher and its queues. If more than one threshold matches for the same managed node and the same work-process, `r3mondisp` only sends the message with the highest severity level. The DPQueueCheck keyword accepts the following parameters:

```
DPQueueCheck =<hostname> =<SID> =<InstanceNr> =<disable/enable>
=<OVO Msg Group> =<OVO Msg Object>  =<OVO Severity>
=<WP-Type>  =<Idle/Queue> =<percentage idle/full>
```

- **Hostname**:

  The name of the SAP Server where the instance is running whose ABAP dispatcher you want to monitor:

=ALL	All the hosts which the SPI for SAP monitors. This is the default setting.
=<*SAP_host*>	The name of a SAP server, where you want to enable monitoring of the dispatcher-queue. Use a new line for each individual host.

- **SID**:

  The System ID of the SAP instance whose ABAP dispatcher you want to monitor:

=ALL	All System IDs which the SPI for SAP monitors. This is the default setting.
=<*SAP_SID*>	The SAP System ID of the instance whose ABAP dispatcher you want to monitor, for example: “SP1”

- **Instance Nr**:

  The number of the SAP instance whose ABAP dispatcher you want to monitor:

=ALL	All instances which the SPI for SAP monitors. This is the default setting.
=<*SAP_InstNr*>	The number the SAP instance whose ABAP dispatcher you want to monitor, for example: “45”

- **Enable/Disable**:

  Enable (1) or disable (0) the DPQueueCheck for the defined SAP instance, for example: 1

- **HPOM Msg Group**:

  The name of the HPOM for Windows message group to which the message generated by `r3mondisp` should be assigned

- **HPOM Msg Object**:

  The name of the HPOM for Windows message object to which the message generated by `r3mondisp` should be assigned, for example: “Dialog”

- **HPOM Msg Severity**:

  The severity level assigned to the HPOM for Windows message generated by `r3mondisp`, for example: “critical”

- **WP-Type**:

  The type of work process whose queues you want to check, for example: DIA (for dialog), or BTC (Batch)

- **Idle/Queue**:

  The status of the work process in the queues you are monitoring. Use “IDLE” if you want to monitor what percentage of the allocated work processes in the monitored queue are idle (or available) at a given point in time; use “QUEUE” if you want to monitor what percentage of the maximum allowed work processes in the monitored queue are currently allocated.

- **Percentage Full**:

How full (or empty) the monitored queue must be as a percentage of the maximum before `r3mondisp` generates an alert. Note that =IDLE =10 generates an alert if *less* than 10% of the allocated work processes are idle; =QUEUE =70 generates an alert if *more* than 70% of the maximum allowed work processes in the queue are in use.

Enable DP Queue Check

Only with SPI for SAP monitors that require a dialog work process to log on to SAP.

Configure the SPI for SAP monitors that log on to SAP to check the status of the ABAP dispatcher and the size of its queues before starting. If there are no, or too few dialog work processes available, the monitor does not start and displays a message in the console indicating the reason why. Use this keyword if you think that allocating to the SPI for SAP monitor the work process it requires to logon to SAP might cause further performance problems for the ABAP dispatcher. For more information about monitoring the ABAP dispatcher and its queues, see r3mondisp: the ABAP Dispatcher Monitor on page 77.

The EnableDPQueueCheck keyword requires the following parameters:

```
EnableDPQueueCheck =<Hostname> =<SAP SID> =<SAP Number>
=<Enable/Disable>
```

- **Hostname**:

  The name of the SAP Server where the instance is running whose ABAP dispatcher you want the SPI for SAP monitors to check before starting:

=ALL	All the hosts which the SPI for SAP monitors. This is the default setting.
=<*SAP_host*>	The name of a SAP server, where you want to enable checking of the dispatcher-queue. Use a new line for each individual host.

- **SAP SID**:

  The SAP System ID of the instance whose ABAP dispatcher you want the SPI for SAP monitors to check before starting:

=ALL	All System IDs which the SPI for SAP monitors. This is the default setting.
=<*SAP_SID*>	The SAP System ID of the instance whose ABAP dispatcher you want to check, for example: “SP1”

- **SAP Number**:

  The number of the SAP instance whose ABAP dispatcher you want the SPI for SAP monitors to check before starting:

=ALL	All instances which the SPI for SAP monitors. This is the default setting.
=<*SAP_InstNr*>	The number the SAP instance whose ABAP dispatcher you want the SPI for SAP monitors to check, for example: “45”

- **Enable/Disable**:

Enable (=1) or disable (=0) this particular monitor to monitor the ABAP dispatcher for the defined SAP instance, for example: 1. The default is Disable (=0). You have to enable the SPI for SAP monitors individually.

Note that if you enable this feature, you do not need to schedule the ABAP dispatcher monitor r3mondisp; it is essential, however, to ensure that a valid configuration file for `r3mondisp` is available. The `r3mondisp.cfg` configuration file defines the path to the profile of the SAP instance the SPI for SAP is monitoring and, in addition, the severity level of the message sent to HPOM for Windows when a threshold is violated for the ABAP dispatcher.

History Path

The HistoryPath[Unix | AIX | WinNT] keyword in the monitor-configuration file accepts the following parameters:

```
HistoryPath<Unix|Aix|WinNT>  <HostName>  =<Path>
```

- **Hostname**:

=ALL	Monitor all hosts with the SPI for SAP. This is the default setting.
=<*SAP_host*>	The name of a SAP server, where you want to specify the path to the monitor history file. Use a new line for each individual host.

- **Path**:

UNIX:	`=default`
AIX:	`=default`
Windows:	`=default`

The `=default` value here is associated with the default path to the history files which the SPI for SAP monitors write. AIX uses `/var/[lpp | opt]/OV/conf/sapspi/` for [DCE | HTTPS] nodes respectively, all other UNIX managed nodes use `/var/opt/OV/conf/sapspi/`, and Windows managed nodes use `%OvAgentDir%\conf\sapspi\`.

Instance Profile Path

Only with `r3mondisp`, the ABAP dispatcher monitor

The path to the profile-configuration file for an SAP instance whose ABAP dispatcher you want to monitor; the InstanceProfilePath keyword accepts the following parameters:

```
InstanceProfilePath =<hostname> =<SID> =<InstanceNr>  =<path>
```

- **Hostname**:

  The name of the SAP Server where you want to specify a path to an SAP profile configuration file:

=ALL	All hosts monitored by the SPI for SAP. This is the default setting.
=<*SAP_host*>	The name of a SAP server, where you want to specify the path to the SAP profile configuration file. Use a new line for each individual SAP server.

- **SID**:

  The ID of the SAP System whose profile path you want to specify:

=ALL	All System IDs which the SPI for SAP monitors. This is the default setting.
=<*SAP_SID*>	The System ID of the SAP instance whose configuration-file path you want to specify, for example: “SP1”

- **Instance Nr**:

  The number of the SAP instance whose profile path you want to specify:

=ALL	All instance numbers which the SPI for SAP monitors. This is the default setting.
=<*SAP_InstNr*>	The number of the SAP instance whose configuration-file path you want to specify, for example: “45”

- **Path**:

  The path to the profile file for the specified SAP instance. The default location for SAP profile files is `/usr/sap/<SID>/SYS/profile`. If the SAP profile file resides in the default location, use =default; if the profile is *not* in the default location, specify the full path to the profile file, for example: `/usr/sap/<path>/profile`

Remote Monitoring

The RemoteMonitoring keyword allows you to configure the SPI for SAP on a local host to monitor an SAP instance on a remote host. You can use the RemoteMonitoring keyword with all the SPI for SAP monitors *except* `r3mondev`, `r3monpro`, and `r3mondisp`. RemoteMonitoring accepts the following parameters:

```
RemoteMonitoring =<LocalHost> =<RemoteHost> =<SAPSystem>  =<SAPNumber>
```

- **LocalHost**:

  The name of the HPOM for Windows managed node where the SPI for SAP is running and whose HPOM for Windows agent the SPI for SAP will use to do the monitoring on the host defined in “RemoteHost”.

- **RemoteHost**:

  The name of the *remote* SAP system monitored by the host defined in “LocalHost”. The RemoteHost does not have the SPI for SAP installed and is not usually (but could theoretically be) an HPOM for Windows managed node.

- **SAP System** (`r3monal` *only*):

  This is the ID of the SAP System running on the SAP server defined in the parameter “RemoteHost” which you want to remotely monitor with the SPI for SAP running on “LocalHost”.

- **SAP Number** (`r3monal` *only*):

  This is the specific instance number of the SAP System running on the SAP server defined in the parameter “RemoteHost” which you want to remotely monitor with the SPI for SAP running on “LocalHost”.

Note that the remote-monitoring feature does not work with all the alert monitors, for example; you cannot configure `r3mondev`, `r3monpro`, and `r3mondisp` to monitor SAP instances running on a remote server. For more information, see the appropriate section on the individual alert monitor.

Setting up Remote Monitoring for r3monal

```
#-----------------------------------------------------------
# Remote           LocalHost  RemoteHost  SAP       SAP
# Monitoring                              System    Number
RemoteMonitoring   =sap1      =sdsap1     =SP6      =00
RemoteMonitoring   =sap1      =sdsap2     =SP6      =00
RemoteMonitoring   =sap2      =sdsap3     =WA1      =33
#-----------------------------------------------------------
```

The name of the host where the remote SAP instance is running must appear in the SPI for SAP's central-configuration file (`r3itosap.cfg`) along with the appropriate login information.

For more information about using the RemoteMonitoring keyword, see the individual alert monitors and, in addition:

- Remote Monitoring with the Alert Monitors on page 24
- r3status: Monitoring SAP Remotely on page 71
- Remote Monitoring with the Alert-Collector Monitors on page 103
- Remote Performance Monitoring on page 214

RFCTimeOut

For all monitors except `r3mondev`, `r3monpro`, `r3mondisp`, and `r3status`

RFCTimeOut defines the maximum amount of time, in seconds, before an RFC XMI/XAL function call is canceled, for example: =120. If the RFC call takes longer than expected to complete, that is; to receive a reply to the initial request, the System is probably down or has a serious performance problem. Note that after the call completes and SAP allocates a free Dialog process, the time limit no longer applies.

Severity Values

Only with `r3monal`, the CCMS-alert monitor

In the Severity Values section of the `r3monal.cfg` configuration file, the Severity<*Level*> keyword configures the `r3monal` monitor to map the severity of CCMS alerts (for example; SeverityCritical) in the SAP subsystem to a specific message-severity level in HPOM for Windows (for example; CRITICAL). The Severity<*Level*> keyword accepts the following values:

```
Severity<Level> =<SAPSystem> =<SAPNumber> =<Enabled>
/<Disabled> =<OpcSeverity>
```

Note that the Enabled/Disabled parameter determines whether `r3monal` considers or ignores CCMS alerts with the specified SAP severity level for mapping to the defined message severity in HPOM for Windows:

=1 (Enabled) Consider CCMS alerts with the severity Severity<*Level*> (for example: SeverityCritical) and send a message to HPOM for Windows with the severity <OpcSeverity>.

=0 (Disabled) Ignore CCMS alerts with the severity Severity<*Level*> (for example: SeverityWarning) and do *not* send a message to HPOM for Windows.

Table 3 Mapping Severity Levels

CCMS Alert Severity	HPOM for Windows Message Severity
SeverityCritical (red)	= CRITICAL
SeverityWarning (yellow)	= WARNING
SeverityNormal (green)	= NORMAL
SeverityNull	= UNKNOWN

The alert-*collector* monitors (`r3moncol`) have two *additional* HPOM for Windows severity levels to map to; Minor and Major. The severity hierarchy in ascending order is; Normal, Warning, Minor, Major, Critical.

Trace File

The TraceFile keyword in the monitor-configuration file accepts the following parameters:

```
Tracefile =<HostName> =<FileName>
```

- **Hostname**:

  =ALL Monitor all SAP servers with the SPI for SAP. This is the default setting.

  =<*SAP_host*> The name of a specific host where tracing is enabled and you want to specify a trace level. Use a new line for each individual host.

- **Filename**:

  =r3mon<*alert_monitor_name*>.log, for example; `r3mondev.log`, or `r3mondmp.log`. This is the default setting. Alternatively, you can specify the name of the file to which you want to write the trace log. By default, monitor trace files are located in the following directories:

  — **UNIX**: `/var/opt/OV/log`

  — **AIX [DCE | HTTPS]**: `/var/[lpp | opt]/OV/conf/sapspi/`

  — **Windows**: `%OvAgentDir%\log`

  For more information about changing the path, see the environment variable SAPOPC_TRACEPATH in Alert-Collector Monitor Environment Variables on page 102.

Trace Level

The TraceLevel keyword in the monitor-configuration file accepts the following parameters:

```
Tracelevel =<HostName> =<Trace Level>
```

- **Hostname**:

=ALL	Monitor all SAP hosts with the SPI for SAP. This is the default setting.
=<*SAP_host*>	The name of a SAP server, where you want to specify a trace level. Use a new line for each individual host.

- **Trace level**:

=0	Disable logging; this is the default setting for all configuration files.
=1	`r3monal`, `r3mondev`, `r3monpro`: Enable all logging `r3moncol`, `r3mondisp`, `r3status`, `r3perfagent`: Log only error messages
=2	`r3moncol`, `r3mondisp`, `r3status`, `r3perfagent` only: Log all messages
=3	`r3moncol`, `r3mondisp`, `r3status`, `r3perfagent` only: Log everything including debug messages

XMISyslogMode

Alert monitor `r3monal` *only*.

The XmiSyslogMode keyword allows you to specify that the `r3monal` monitor sends SAP system log messages in the style and format previously used by the monitor `r3monxmi`, which is now obsolete. The XmiSyslogMode keyword accepts the following parameters;

```
XmiSyslogMode      =<Enable | Disable>
```

- Enable/Disable:

=0	*Disable* the XMI compatibility mode; this is the default setting.
=1	*Enable* XMI compatibility mode.

For more information about the XMISyslogMode keyword and when you can use it, see r3monal: XMI Compatibility Mode on page 56.

To Configure the SPI for SAP Alert Monitors

1. In the HPOM for Windows console, expand the following policy group:

   Policy Management > Policy Groups > SPI for SAP

2. In the details pane, double-click the appropriate configuration-file policy, for example; `global_r3moncts.cfg`. The selected alert monitor's configuration file opens in the configuration-file policy editor. Note that there are two types of configuration-file policy for the SPI for SAP:

   - global

     for *global* configurations, for example; `global_r3moncts.cfg`

   - local

for *local* configurations, for example; `local_r3moncts.cfg`

3 Edit or enter lines to define *trace levels*. For example, you can set a default for ALL hosts (hostname = ALL), then add lines for any hostname exceptions. For example:

```
TraceLevel     =ALL        =0
TraceLevel     =hpbbx10    =1
```

In this example, tracing is turned off for all hosts except for host `hpbbx10`. For more information about trace levels, see Trace Level on page 39.

4 Specify the name of the *trace file* in which you want to record trace information. For example:

```
TraceFile      =ALL        =r3monpro.log
```

Default trace file names for each monitor are given in Table 4

Table 4 Default Trace File Names

Tracefile Name	Monitor Alert Type
`r3monaco.log`	Alert Calls
`r3monal.log`	Alerts
`r3monale.log`	iDOC alerts
`r3monchg.log`	System Change
`r3moncts.log`	Correction and Transport System
`r3mondev.log`	Trace and Log Files
`r3mondisp.log`	ABAP dispatcher
`r3mondmp.log`	ABAP/4 Dumps
`r3monjob.log`	Job
`r3monlck.log`	Lock_Check
`r3monoms.log`	OM Switch
`r3monpro.log`	Work and Database Processes
`r3monsec.log`	Security
`r3monspl.log`	Spooling
`r3montra.log`	Transport
`r3monupd.log`	Update
`r3monusr.log`	User
`r3monwpa.log`	WorkProcess Availability

5 Specify the *history path*, which is the directory path by which you can locate an alert monitor's history file. Alert monitors include the following default paths for UNIX, AIX and Windows servers:

```
HistoryPathUnix    =ALL     =default
HistoryPathAIX     =ALL     =default
HistoryPathWinNT    =ALL      =default
```

You can tell the alert monitors to use a specific history path on Windows managed nodes rather than the default: `=default`, for example: `%OvAgentDir%\Tmp`. For more information, see the SAPOPC_HISTORYPATH environment variable and the alert-monitor configuration-file keyword, History Path on page 36.

Each alert monitor writes its own history file. Each time an alert monitor completes a run, it adds a new section to its history file. This feature enables the alert monitor to check for changes since the previous run.

Do *not* edit any of the monitor history (`*.his`) files. Editing the monitor history file could compromise the accuracy and consistency of your records. The monitor uses its history file to determine which, if any, events have occurred since the last run and whether to send any messages.

6 Define the monitoring conditions. Monitoring conditions are rules that control the checks which the alert monitor makes each time it runs. The monitoring conditions you enter are different for each alert monitor. See Alert Classes on page 28 for general information about the keywords and parameters that are allowed with each monitor.

For specific information on the monitoring conditions for each alert monitor, see the appropriate section on the particular alert monitor.

Distributing Alert-Monitor Configuration Files

You deploy configuration files to the HPOM for Windows managed nodes in the same way as HPOM for Windows policies, that is; using the standard policy-deployment mechanism.

It is possible to have configuration files in both the global and local directories on a managed node. When a monitor executable runs, it uses an order of precedence to determine which configuration file should be used. For more information, see Alert Monitor Order of Precedence on page 24.

Local and global configuration files

Local and global configuration files are installed in the following directories on the managed node:

- **UNIX**: `/var/opt/OV/conf/sapspi/[global | local]`
- **AIX [DCE | HTTPS]**:
  `/var/[lpp | opt]/OV/conf/sapspi/[global | local]`
- **Windows**: `%OvAgentDir%\conf\sapspi\[global|local]`

Local and Global Configurations

This section explains briefly how to apply either a local or a global alert-monitor configuration and, in addition, how to delete configurations, which have already been deployed. This section provides instructions for the following tasks:

- To Apply a Global Configuration on page 43
- To Apply a Local Configuration on page 44
- To Delete Selected Local Configurations on a Node on page 44

It is possible to configure both global and local directories on the same machine. When a monitor executable runs, it uses an order of precedence to determine which configuration file should be used. For more information, see Alert Monitor Order of Precedence on page 24.

The procedures described in this section assume that you have already deployed the SPI for SAP policies to the nodes you want to manage.

To Apply a Global Configuration

1. Microsoft Windows (HTTPS):
   In the HPOM for Windows console, browse to the following directory:

   Policy Management > Policy Groups > SPI for SAP

2. In the details pane, locate and double-click the configuration file associated with the alert monitor you want to configure, for example; the `global_r3mondmp` file for the ABAP-dump monitor. The configuration-file policy editor displays the selected file.

3. Make any modifications as required.

   You do not *have* to modify the configuration files: the default configuration-file policies work without modification.

4. Save your changes using the **Save as...** option and close the configuration-file policy editor. When saving the modified policy, we recommend that you use the naming conventions for configuration-file policy types, for example; `global_r3mondmp`. The modified configuration-file policy for the SPI for SAP `r3mondmp` monitor appears in the list of policies in the details pane.

   If you use the configuration-file policy editor to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

5. In the details pane, select and right-click the policies you want to deploy and use the following menu option:

   All Tasks > Deploy on...

6. Use the Deploy Policies on... window to select the managed nodes to which you want to deploy the selected policies. Click **OK** to start the deployment.

7. Verify that the deployment operation completed successfully by right-clicking a managed node in the console and selecting the following option from the menu that pops up:

   View > Policy Inventory

The configuration files are copied to one of the directories mentioned in Local and global configuration files on page 42 on each of the selected managed nodes.

To Apply a Local Configuration

1. In the HPOM for Windows console, browse to the following directory:

   Policy Management > Policy Groups > SPI for SAP

2. In the details pane, locate and double-click the configuration file associated with the alert monitor you want to configure, for example; the `local_r3mondmp` file for the ABAP-dump monitor. The configuration-file policy editor displays the selected file allowing you to make any modifications as required.

3. Save your changes using the **`Save as...`** option and close the configuration-file policy editor. When saving the modified policy, replace "local" with the name of the SAP NetWeaver server for which the local configuration is intended, for example; *<SAP_Server_Name>*`_r3mondmp`. The modified configuration-file policy for the SPI for SAP `r3mondmp` monitor appears in the list of policies in the details pane.

   If you use the configuration-file policy editor to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

4. Repeat steps 1 through 3 for each of the alert monitors for which you want to create a local configuration.

5. In the details pane, select and right-click the policies you want to deploy and use the following menu option:

   All Tasks > Deploy on...

6. Use the Deploy Policies on... window to select the managed nodes to which you want to deploy the selected policies. Click **`OK`** to start the deployment.

7. Verify that the deployment operation completed successfully by right-clicking a managed node in the console and selecting the following option from the menu that pops up:

   View > Policy Inventory

   The configuration files are copied to one of the directories mentioned in Local and global configuration files on page 42 on each of the selected managed nodes:

To Delete Selected Local Configurations on a Node

1. In the HPOM for Windows console, right-click the managed node whose local alert-monitor configuration you want to delete and select the following option from the menu that pops up:.

   View > Policy Inventory

2. Holding down the **Ctrl** key, select and right-click the local configuration-file policies you want to remove, and select the following option from the menu that pops up:

   All Tasks > Uninstall from...

3 The SPI for SAP Alert Monitors

This section describes the alert monitors `r3monal`, `r3monpro`, `r3mondev`, `r3status`, and `r3monsec` and explains how to use the configuration files to control them.

Introducing the SPI for SAP Monitors

The SPI for SAP includes a set of monitors, which you configure to run at regular intervals to collect information regarding various aspects of your SAP environment.

You deploy SPI for SAP monitors to the SAP NetWeaver servers, which you want to manage and monitor with HPOM for Windows. Monitor deployment is part of the SPI for SAP installation and configuration process. Before deploying a monitor, the HPOM for Windows administrator, working from the HPOM for Windows console, first deploys the appropriate SPI for SAP message-source policies.

If you are new to configuring the monitors, you will want to read the detailed description of each alert monitor and alert-monitor configuration file. Each alert-monitor configuration file includes information about default configurations as well as a list of changes you must make to the configuration file.

The information in this section covers the following areas:

Polling Rates for the Alert Monitors

The alert monitors have different polling rates, that is: the frequency at which the monitor runs. You can change the polling rate at the scheduled-task policy for the monitor. For more information about the default polling rates for each alert monitor, see Table 5, which shows the rates in days, hours, and minutes.

Table 5 Default Polling Rates for Alert Monitors

Alert-Monitor Name	Polling Rate		
	Days	Hours	Mins
r3monal			5
r3mondev			5
r3mondisp			3
r3monpro			2
r3monsec	1		
r3status			2

The Alert-Monitor Configuration Files

Each SPI for SAP alert monitor is defined and configured in an HPOM for Windows policy and in several files, including an executable file and a configuration file.

The policy defines the rules for generating messages that appear in the HPOM for Windows console. The policy also controls the frequency with which the associated executable file runs. If you want to customize a policy, follow the instructions given in the online help for HPOM for Windows administrators.

The monitor executable file runs at the regular interval specified in the monitor policy. The monitor executable checks for and, if present, reports conditions defined in the individual monitor's associated configuration file. You can define these monitoring conditions to suit the needs of your environment. For information about copying and renaming the monitor policies, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.

The SPI for SAP monitor's configuration file allows you to use keywords to set up the monitor to meet the requirements of your particular environment. Note that although most of the keywords appear in *all* the configuration files, some of the keywords can only be used in conjunction with specific monitors.

For more information about the keywords which you can use in the SPI for SAP alert-monitor configuration files, see Monitor-Configuration Files on page 23. Note too, that the contents of `r3status.cfg`, the `r3status` monitor configuration file, are explained in greater detail in The r3status Configuration File on page 69. Excerpt from the r3mondev.cfg File on page 46 shows what a configuration file looks like for the `r3mondev` monitor, which scans the trace and log files of the SAP system for the string "`ERROR`".

Excerpt from the r3mondev.cfg File

```
#-------------------------------------------------------------------------
-
# TraceLevel  hostname  only error messages=1  info messages=2  debug
messages=3
#                      Disable=0
TraceLevel     =ALL        =0
#-------------------------------------------------------------------------
-
# TraceFile  hostname    filename
#
TraceFile    =ALL        =r3moncts.log
#-------------------------------------------------------------
# History    hostname    path
# Path
#
HistoryPathUnix   =ALL   =default
HistoryPathAIX    =ALL   =default
HistoryPathWinNT  =ALL   =default
#-------------------------------------------------------------

# AlertDevMon  SAP  SAP     Enable =1  Filemask   Severity  Opc        OpC
#              Sys  Number  Disable=0                       Object     MsgGro
up
#AlertDevMon   =ALL  =ALL    =1        =dev_*     =WARNING  =r3mondev  =R3_Tr
ace
#AlertDevMon   =ALL  =ALL    =1        =std*      =CRITICAL =r3mondev  =R3_Tr
ace
#Dispatcher trace file
AlertDevMon    =ALL  =ALL    =1        =dev_disp  =WARNING  =r3mondev  =R3_Tr
ace
#Workprocess trace file for workprocess with number 0
AlertDevMon    =ALL  =ALL    =1        =dev_w0    =WARNING  =r3mondev  =R3_Tr
ace
#message server trace file
AlertDevMon    =ALL  =ALL    =1        =dev_ms    =WARNING  =r3mondev  =R3_Tr
ace
#screen processor trace file
AlertDevMon    =ALL  =ALL    =1        =dev_dy0   =WARNING  =r3mondev  =R3_Tr
ace
#tp process trace file
AlertDevMon    =ALL  =ALL    =1        =dev_tp    =WARNING  =r3mondev  =R3_Tr
ace
-------------------------------------------------------------------------
---
```

r3monal: the CCMS 4.x Alert Monitor

The `r3monal` monitor uses the SAP NetWeaver CCMS monitoring architecture introduced at SAP version 4.0 and enables you to monitor the output of SAP's own internal monitor, the CCMS alert monitor. The `r3monal` monitor maps the alerts identified by the CCMS monitor to HPOM for Windows messages, which you can view in the HPOM for Windows console.

Since SAP has indicated that it intends to phase out support for the shared-memory interface, the SPI for SAP only supports the XMI/XAL interface.

This section includes information about the following topics, which describe the contents of the `r3monal` configuration file:

r3monal: Monitoring Conditions

You must define and enable the keywords; Severity<*Level*>, RFCTimeOut, CCMSMonitorSet, and CCMSAcknowledgeMessage; all other keywords in the `r3monal.cfg` configuration file are optional. For more information, see Severity Values on page 38, RFCTimeOut on page 38, CCMS Monitor Set on page 32, and CCMS Acknowledge Message on page 31 respectively.

r3monal: CCMS Monitor Sets

The XMI/XAL interface allows the SPI for SAP to read, write, and reset CCMS alerts directly in the CCMS alert-monitor tree. The most obvious advantage of this feature is that you can use existing CCMS monitor sets as templates to define your own monitor sets, which contain only those CCMS alerts you want to monitor with the SPI for SAP.

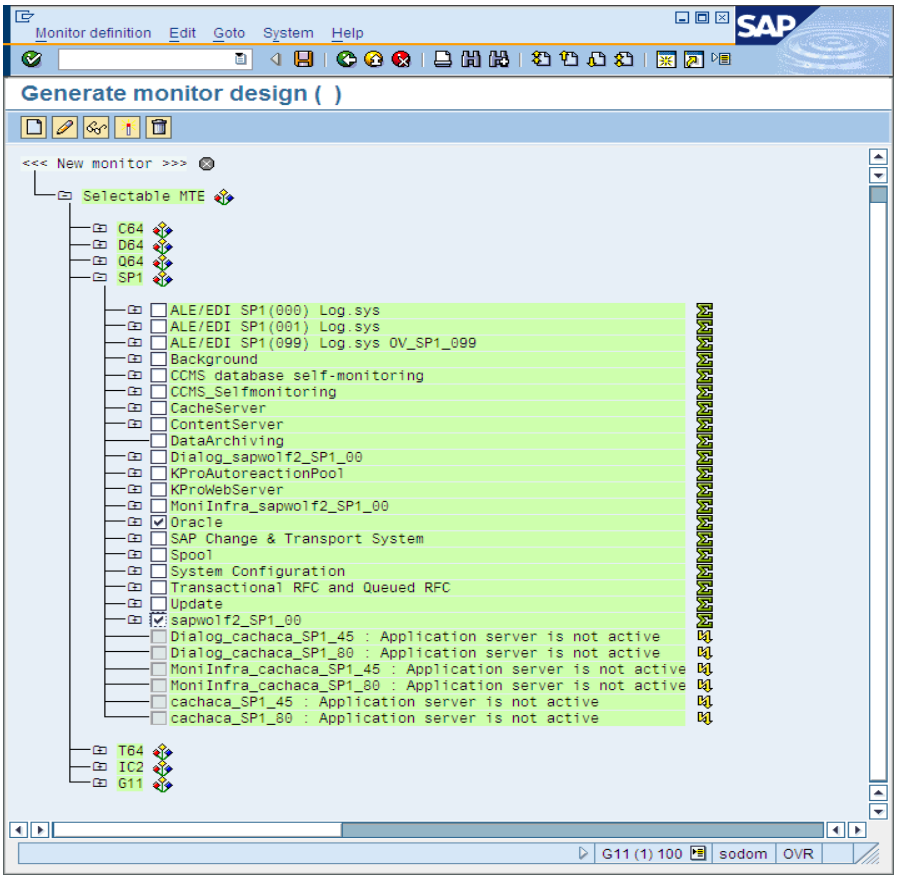
Remember to login to SAP and define the new CCMS monitor sets which you want the SPI for SAP to use to generate messages *before* you start the configuration of the `r3monal` monitor in HPOM for Windows. Figure 1 on page 49 shows how the application servers `bounty` and `hpspi003` appear in the Monitor-tree when you select and expand the central-instance item `WA1`.

To create or modify items in the CCMS monitor tree, you need to make sure that the Maintenance Function for the CCMS monitor sets is switched on. You can find the Maintenance function option in the Extras menu, as follows:

`Extras > Activate Maintenance Function`

If you are not interested in receiving messages concerning *all* the alerts present in the default monitor set, for example; OperatingSystem, DatabaseClient, and so on, you can expand the individual application-server item and select only the alerts which you want to use to generate messages that will be sent to HPOM for Windows. In the example configuration shown in Figure 1, we have also selected the Oracle ® item so that we hear about problems with the database, too.

Figure 1 Defining a Monitor Set



Make sure that the new monitor sets you define for the SPI for SAP are visible to and usable by the HPOM for Windows user, which you have defined for the SPI for SAP. If you are logged into SAP as the defined HPOM for Windows user, then you can see only the CCMS monitor sets defined for the defined HPOM for Windows user and those marked “Public”. If you are logged into SAP as the administrator, you can see *all* available monitor sets, in which case you have to remember to ensure that you make the *new* monitor sets you define for the SPI for SAP visible either to the defined HPOM for Windows user for the SPI for SAP or everyone by using the option “Public”. Remember to use only ASCII characters when defining the name of a CCMS monitor set; the SPI for SAP cannot currently interpret non-ASCII characters in monitor-set names.

One SAP System/SID can have multiple monitor sets. If you need to define multiple monitor sets for a SAP System/SID, remember to include each new monitor set on a new line in the monitor-set section of the `r3monal.cfg` monitor configuration file, as illustrated in Configuring Multiple Monitor Sets. The name you define in the monitor parameter must match the name of the monitor set as it appears in the CCMS alert-monitor tree. The names of monitors must appear in the configuration file exactly as they are shown in SAP including, for example, forward slashes (/), as shown in Configuring Multiple Monitor Sets.

Note that the combination of traditional long SAP names and the line break in the example configuration file shown in Configuring Multiple Monitor Sets disguises the name of the monitor. The complete name of the last monitor is: =System / All Monitoring Segments / All Monitoring Contexts. Note that the names you use do not have to be this long. In addition, if you want to associate multiple monitors with one, single monitor set, you have to specify each individual monitor on a new line as shown by the first two entries in Configuring Multiple Monitor Sets, where the **SPISAP** monitor set has two Monitors; **System** and **DB_ALERT**.

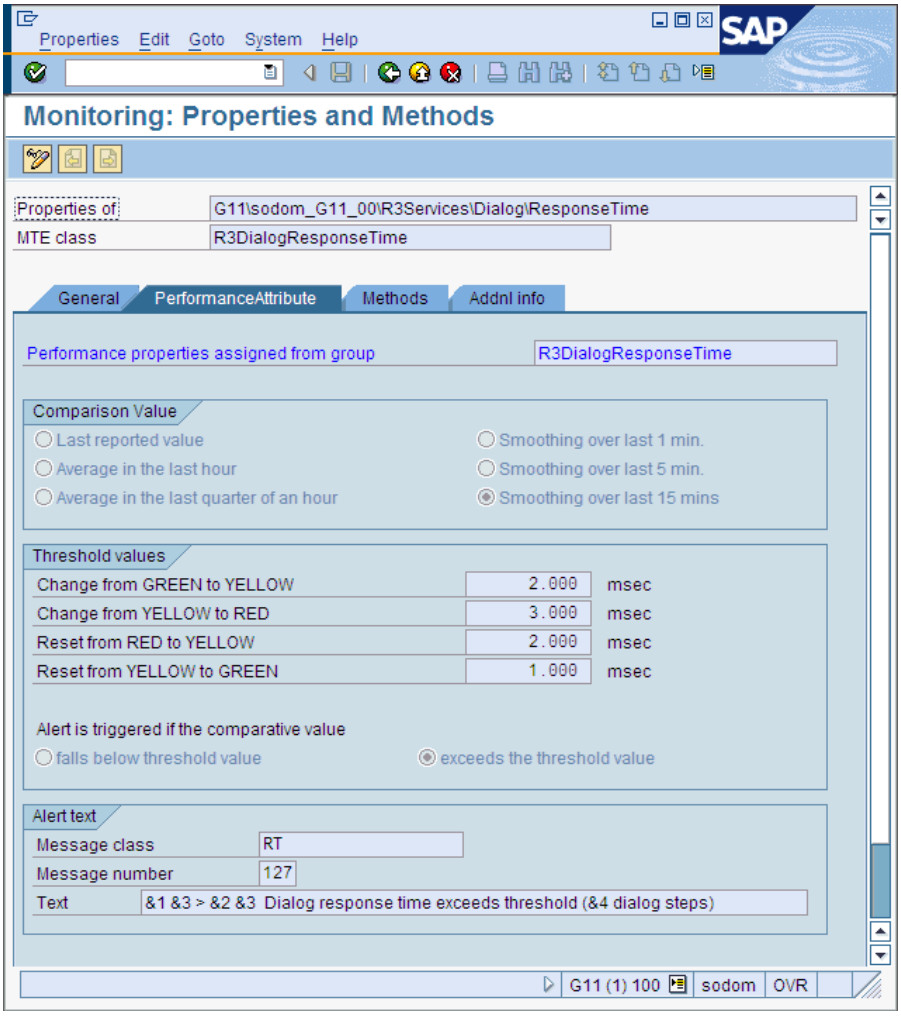
Configuring Multiple Monitor Sets

```
#-------------------------------------------------------------------------
--
# Monitor Set    SAP     SAP     Monitor Set                          Monitor
#                System  Number
CCMSMonitorSet   =WA1    =33     =SPISAP                               =System
CCMSMonitorSet   =WA1    =33     =SPISAP                               =DB_ALE
RT
CCMSMonitorSet   =SP6    =00     =SAP CCMS Technical Expert Monitors   =System
/\
                                 All Monitoring Segments / All Monitoring
Contexts
#-------------------------------------------------------------------------
--
```

The default configuration of individual CCMS alert monitors does not always meet the demands of your environment and, in some instances, you will need to change it. You can check and, if necessary, modify a monitor’s properties in the Performance Attribute tab of the Monitor: Properties and Methods window, as illustrated in Figure 2 on page 51. If you decide to change the monitor properties, you need to consider the following points:

- Ensure that the severity level of the CCMS Alerts matches the severity level of the HPOM for Windows messages, which are generated by the CCMS Alerts. For more information about configuring severity levels, see Severity Values on page 38.
- Ensure that severity-level thresholds configured for a given CCMS alert monitor are appropriate for your needs.

Figure 2 Checking and Modifying CCMS Alert-Monitor Thresholds



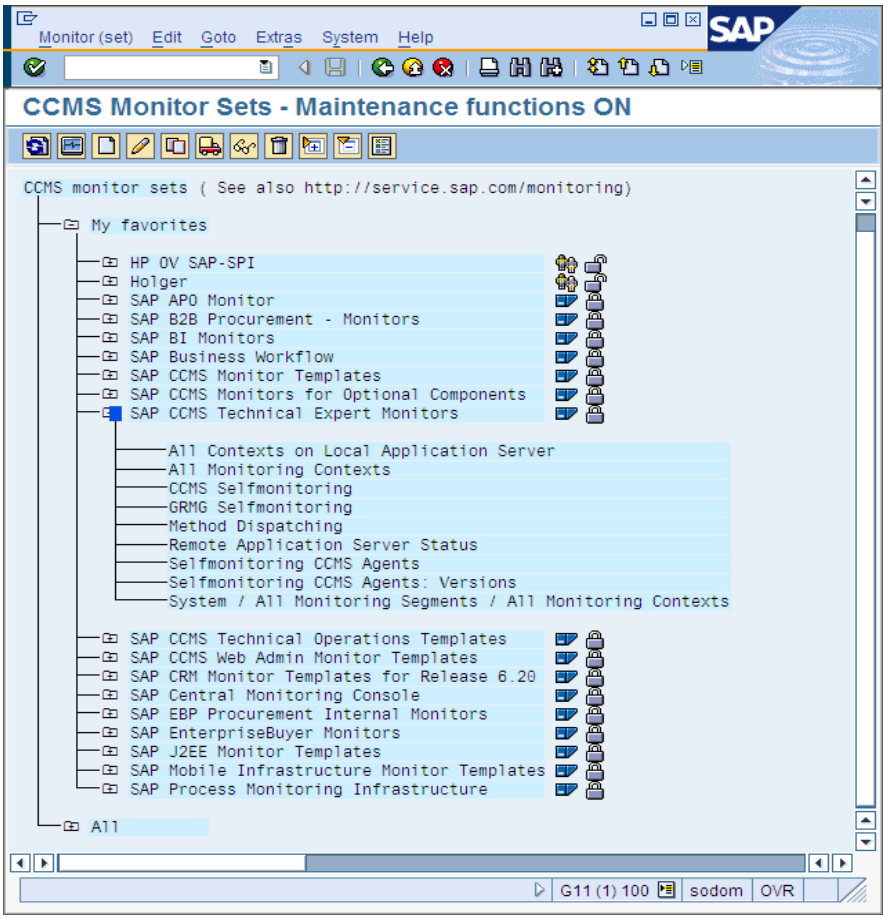
To open the Monitor: Properties and Methods window for a specific CCMS monitor, browse to the desired monitor in the monitor-set tree and either click the **Properties** button or double-click the monitor you want to view.

r3monal: CCMS Alert Monitors

Alerts are the most basic element of the strategy that SAP uses to monitor the health of the SAP Landscape. Alerts are associated with objects such as disks and CPUs, and objects have attributes such as response times and usage statistics. The status of the object as well as its performance and availability over time are important to the SAP System administrator. The SAP NetWeaver CCMS alert monitor displays the configured alerts (along with any associated objects and attributes) as CCMS **monitors** in a **monitor tree**, which you can browse, as illustrated in Figure 3. Note that *public* monitor sets are visible to (and usable by) all SAP users.

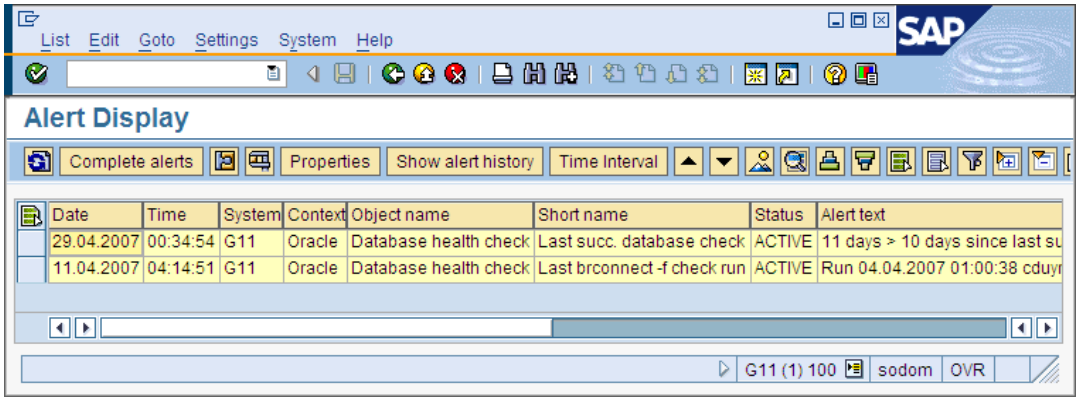
For ease of navigation, the CCMS monitors are grouped into pre-defined **monitor sets**, for example; `SAP CCMS Technical Expert Monitors` or `SAP CCMS Admin Workplace`. The pre-defined monitor sets contain a large number of sub sets and monitors, which can generate thousands of alerts, some of which you really do not need.

Figure 3 CCMS Monitor Sets



If you switch *on* the maintenance function for the CCMS monitor sets, you can create your own CCMS monitor sets, which contain only the monitors for the alerts you want to know about on a regular basis. When you have created your own monitor sets, you can add them to the monitor-set tree and configure the SPI for SAP to monitor them. In this way, you can reduce the alerts you hear about and the information you receive so that it is easier to manage. Remember to use only ASCII characters when defining the name of a CCMS monitor set; the SPI for SAP cannot currently interpret non-ASCII characters in monitor-set names.

Figure 4 CCMS Alert Properties



When a condition is reported in the SAP NetWeaver CCMS monitor, the monitoring object and its attributes are included in the resulting alert as shown in Figure 4.

r3monal: CCMS Acknowledge Message

The CCMSAcknowledgeMessage feature determines whether `r3monal` tells SAP to automatically acknowledge (complete) CCMS Alerts, which match the defined conditions. Enabling the CCMSAutoAcknowledge feature in the `r3monal.cfg` configuration file is the same as selecting the alert and clicking the **Complete Alert** button in SAP CCMS.

Automatically Acknowledging CCMS Alerts

```
# Triggers auto-acknowledge of CCMS alerts
#-------------------------------------------------------------
# CCMSAcknowledgeMessage  SAP     Ack. filtered   Enable=1
#                         System  Messages        Disable=0
CCMSAcknowledgeMessage    =ALL    =0              =0
CCMSAcknowledgeMessage    =SP6    =0              =0

#-------------------------------------------------------------
```

You can enable or disable the auto-acknowledgement feature for specific SAP Systems defined on individual lines in the `r3monal.cfg` configuration file. Note, however, that if you *disable* the auto-acknowledgement feature (=0) for a specific SAP System, `r3monal` ignores the setting for **Ack. Filtered Messages** defined on the same line.

If you enable the `Ack. Filtered Messages` keyword, messages that are filtered out (and not sent to the HP Operations agent) by the `AlerMonSyslog` specifications (which means, setting `Disabled=0` in the appropriate line) will be acknowledged in CCMS. Therefore, these alerts will not be visible in the HPOM message browser or in SAP CCMS anymore. For more information on `AlerMonSyslog`, see r3monal: Alert Classes on page 57.

Note that, if you enable the CCMSAcknowledgeMessages keyword, you also need to make sure that you enable the Severity<*Level*> keyword, too; the Severity<*Level*> keyword allows you to filter CCMS alerts according to severity. For more information, see r3monal: Severity Levels on page 55.

r3monal: Environment Variables

Table 6 lists the environment variables, which you can use to configure the `r3monal` monitor.

Table 6 r3monal Environment Variables

Environment Variable	Description
SAPOPC_DRIVE	The Windows drive where the HPOM for Windows agent is running, for example; `E:\usr\...`
SAPOPC_HISTORYPATH	Path to the `r3monal` history file
SAPOPC_R3MONAL_CONFIGFILE	Name of the `r3monal` configuration file

Table 6 r3monal Environment Variables (cont'd)

Environment Variable	Description
SAPOPC_SAPDIR	The Windows drive where SAP NetWeaver is running, for example; `E:\usr\sap`
SAPOPC_TRACEMODE	Trace mode: a = append w = create (default)
SAPOPC_TRACEPATH	Path to the `r3monal` trace file

r3monal: File Locations

The `r3monal` monitor uses the default files listed in Table 7. For more detailed information about the contents of the in SPI for SAP monitor-configuration files in general and the file `r3monal.cfg` in particular, see The SPI for SAP Monitor-Configuration File on page 26.

Table 7 r3monal File

File Name	Description
`r3monal(.exe)`	Executable for the SAP NetWeaver CCMS alert monitor
`r3monal.cfg`	Configuration file for the CCMS alert monitor
r3monal.his	History file for storing data after each monitor run

r3monal: Remote Monitoring

The RemoteMonitoring keyword allows you to configure the SPI for SAP on local host to monitor an SAP instance on a remote host. For more information about the parameters you can use with the RemoteMonitoring keyword, see the list of keywords in Remote Monitoring with the Alert Monitors on page 24. Note that SAP System and SAP Number are only required by `r3monal`.

Enabling Remote Monitoring in the r3monal.cfg File

```
#-----------------------------------------------------------
# Remote Host     Localhost   Remotehost    SAP      SAP
#                                          System   Number
RemoteMonitoring  =hpspi003   =ovsdsap6     =SP6     =00
#-----------------------------------------------------------
```

r3monal: RFC Time Out

You use the RFCTimeout keyword to define the maximum amount of time in seconds before an RFC XMI/XAL function call is canceled, for example: =120. You need to set a time-out which takes into account the environment in which SAP is running. For example, if the RFC

call takes longer than expected to complete, that is; to receive a reply to the initial request, the SAP System is probably down or has a serious performance problem. Note that after the RFC call completes and SAP allocates a free Dialog process, the time limit no longer applies.

Setting the Time-out period for XMI/XAL Function Calls

```
#-----------------------------------------------------------
# Max. time in sec. before a RFC XMI/XAL function call is
# canceled. If the RFC call takes longer than expected, the
# system is probably down or has a major performance problem.
RFCTimeOut = 120
#-----------------------------------------------------------
```

r3monal: Severity Levels

The "Severity Values" section of the `r3monal.cfg` file defines how you filter CCMS alerts in the CCMS monitor trees you are managing with `r3monal` and map the severity level of the filtered CCMS Alerts to the desired severity level for the corresponding HPOM for Windows messages. You use the keywords SeverityWarning and SeverityCritical in combination with the CCMSAcknowledgeMessage keyword, which is described in more detail in r3monal: CCMS Acknowledge Message on page 53. For more information about the SPI for SAP configuration files in general, see The SPI for SAP Monitor-Configuration File on page 26.

By adding a new line for individual combinations of SAP system ID and SAP number, you can restrict the severity mapping between CCMS Alerts and HPOM for Windows messages to a specific SAP System ID and SAP Number. Default Settings for Severity Levels in r3monal.cfg shows the default settings for severity levels in the `r3monal.cfg` file.

Default Settings for Severity Levels in r3monal.cfg

```
#-----------------------------------------------------------
#Severity         SAP      SAP     Enabled=1   OpCSeverity
#Values           System   Number  Disabled=0
SeverityWarning  =ALL     =ALL    =0          =WARNING
SeverityCritical =ALL     =ALL    =1          =CRITICAL
#-----------------------------------------------------------
```

You can edit the severity levels in `r3monal.cfg` in any one of the following ways:

1. **Enable or disable severity levels**

   If you want to disable (=0) the generation of messages for CCMS alerts with the severity "warning", add a new (or change the existing) SeverityWarning line as follows:

   ```
   SeverityWarning    =ALL    =ALL    =0    =WARNING
   ```

2. **Change how the SPI for SAP maps CCMS severity levels to message severity levels in HPOM**

   If you want the SPI for SAP to report all SeverityWarning events as critical, add a new (or change the existing) SeverityWarning definition, as follows:

   ```
   SeverityWarning      =ALL    =ALL    =1    =CRITICAL
   ```

3. **Define SID-Specific exceptions**

   If you want the SPI for SAP to report as critical all SeverityWarning events that occur on SAP system LP2, leave the default settings for ALL systems and add the following line:

   ```
   SeverityWarning    =LP2    =ALL    =1    =CRITICAL
   ```

Excerpt from the r3monal Configuration File

```
# A Monitor Set defines the messages you want to forward to HPOM.
#-------------------------------------------------------------------------
# Monitor Set     SAP    SAP     Monitor Set  Monitor
#                 System Number
#CCMSMonitorSet   =WA1   =33     =SPISAP      =System
#CCMSMonitorSet   =WA1   =33     =SPISAP      =DB_ALERT
#CCMSMonitorSet    =SP6    =00      =SAP CCMS Technical Expert Monitors
=System / All Monitoring Segments / All Monitoring Contexts
#-------------------------------------------------------------------------
# Remote Host      Localhost   Remotehost  SAP     SAP
#                                          System  Number
#RemoteMonitoring  =hpspi003   =ovsdsap6   =SP6    =00
#-------------------------------------------------------------------------
# CCMSAcknowledgeMessage  SAP      Ack. filtered     Enable=1
#                         System   Messages          Disable=0
CCMSAcknowledgeMessage    =ALL     =0                =0
CCMSAcknowledgeMessage    =SP6     =0                =0

# XMI compatibility mode
# makes the r3monal send syslog messages r3monxmi style
#-------------------------------------------------------------------------
# XmiSyslogMode    Enabled  =1
#                  Disabled =0
XmiSyslogMode      =0

# Syslog filtering
#-------------------------------------------------------------------------
# Alert Classes  SAP     SAP      SyslogId       Enabled=1
#                System  Number   From     To     Disabled=0
AlerMonSyslog    =ALL    =ALL    =A00     =MZZ   =1
AlerMonSyslog    =ALL    =ALL    =N00     =ZZZ   =0
AlerMonSyslog    =LPO    =01     =A00     =ZZZ   =1
```

r3monal: Trace Levels

For more information about the trace levels the alert monitors use and, in particular, the trace levels available to the `r3monal` monitor, see Trace Level on page 39 in the section Monitor-Configuration Files on page 23.

r3monal: XMI Compatibility Mode

The XmiSyslogMode keyword allows you to specify that the `r3monal` monitor sends SAP system log alerts in the style and format previously used by the `r3monxmi` monitor. Note that at SPI for SAP version 11.10, the `r3monxmi` monitor is now obsolete; to continue monitoring CCMS syslog alerts, you will have to use the `r3monal` monitor, which uses the BAPI External Alert Management Interface (XAL).

Sending Syslog Messages in XMI Format

```
# XMI compatibility mode
# makes the r3monal send syslog messages r3monxmi style
#-----------------------------------------------------------
# XmiSyslogMode    Enabled  =1
```

```
#                   Disabled =0
XmiSyslogMode       =1
#-------------------------------------------------------------
```

If you enable XmiSysLogMode you need to define in detail how the old `r3monxmi` monitor would filter SAP system-log messages. In most cases, you would do this by copying an existing configuration for the now-obsolete `r3monxmi` monitor and paste it into the `r3monal` configuration file, `r3monal.cfg`. If you do not provide the r3monxmi configuration, the SAP syslog messages will not appear in the XMI format you want. For more information about migrating from `r3monxmi` to `r3monal`, see r3monal: Migrating from r3monxmi on page 57.

r3monal: Alert Classes

In the alert-classes section of the `r3monal.cfg` file, you define how the SPI for SAP's CCMS alert monitor `r3monal` filters syslog events in the SAP System; the filtering mechanism ensures that you extract and display only those syslog events that you are interested in seeing. You filter the syslog events that you want to monitor by specifying ranges of message numbers (syslog IDs). Each line of the alert-classes section of the `r3monal.cfg` file is set up in a particular way. Each entry defines monitoring for a specified range of syslog events. You can specify which syslog events to monitor by enabling or disabling ranges of syslog IDs either globally or for specified SAP systems and instances.

In Syslog events in the r3monal.cfg file, `r3monal` monitors the syslog events with IDs A00 through MZZ on all SAP Systems and SAP numbers but does not monitor the syslog events with IDs N00 through ZZZ on all SAP Systems and numbers. Syslog event monitoring is enabled on SAP System LPO for IDs A00 through ZZZ.

Syslog events in the r3monal.cfg file

```
# Syslog filtering
#-------------------------------------------------------------
# Alert Classes  SAP     SAP      SyslogId       Enabled=1
#                System  Number  From    To      Disabled=0
AlerMonSyslog   =ALL    =ALL    =A00    =MZZ    =1
AlerMonSyslog   =ALL    =ALL    =N00    =ZZZ    =0
AlerMonSyslog   =LPO    =01     =A00    =ZZZ    =1
#-------------------------------------------------------------
```

r3monal: Migrating from r3monxmi

The old `r3monxmi` monitor used XMI, the eXternal Management Interface, which was first introduced with SAP 3.0F. Since the SPI for SAP no longer supports SAP version 3.x, you can no longer use `r3monxmi` to monitor SAP System-log messages. If you want to continue to monitor syslog messages and CCMS alerts, you will have to migrate your XMI configuration to `r3monal`, the CCMS 4.x alert monitor. However, you can use the contents of the message-filtering section of the old `r3monxmi.cfg` file in the new configuration file for `r3monal`.

The `r3monxmi` monitor was application-server *dependent*; you had to install `r3monxmi` on each application server of the SAP System whose syslog messages you wanted to monitor.

The `r3monal` monitor is application server *independent*; `r3monal` can read the syslog messages from all application servers from a single location. Typically, you install `r3monal` on the central instance of the SAP system, whose syslog messages you want to monitor.

To migrate syslog-message monitoring from r3monxmi to r3monal:

1 Define a CCMS monitor and monitor set for the syslog alerts

`r3monal` uses the internal SAP NetWeaver CCMS monitor to check for syslog alerts; use transaction RZ20 to configure CCMS monitors.

2 In the CCMS monitor tree, check the `r3syslog` branches of *all* the application servers, whose syslog messages you want to monitor with the SPI for SAP

You can automate the process by creating monitor-tree elements (MTEs) based on rules. When adding the new MTE node to the CCMS monitor, check the option Rule Node in the Create Nodes dialog; when setting up the CCMS rule, use the following values:

- **Rule Type:**

  CCMS_GET_MTE_BY_CLASS

- **MTE Class:**

  R3Syslog

3 Enable the XmiSyslogMode keyword in the `r3monal.cfg` file

If you want the `r3monal` monitor to use the old `r3monxmi` configuration based on XMI message conditions, use the XmiSyslogMode keyword in the `r3monal.cfg` file. In this mode, `r3monal` sends SAP system-log alerts in the style and format previously used by the `r3monxmi` monitor.

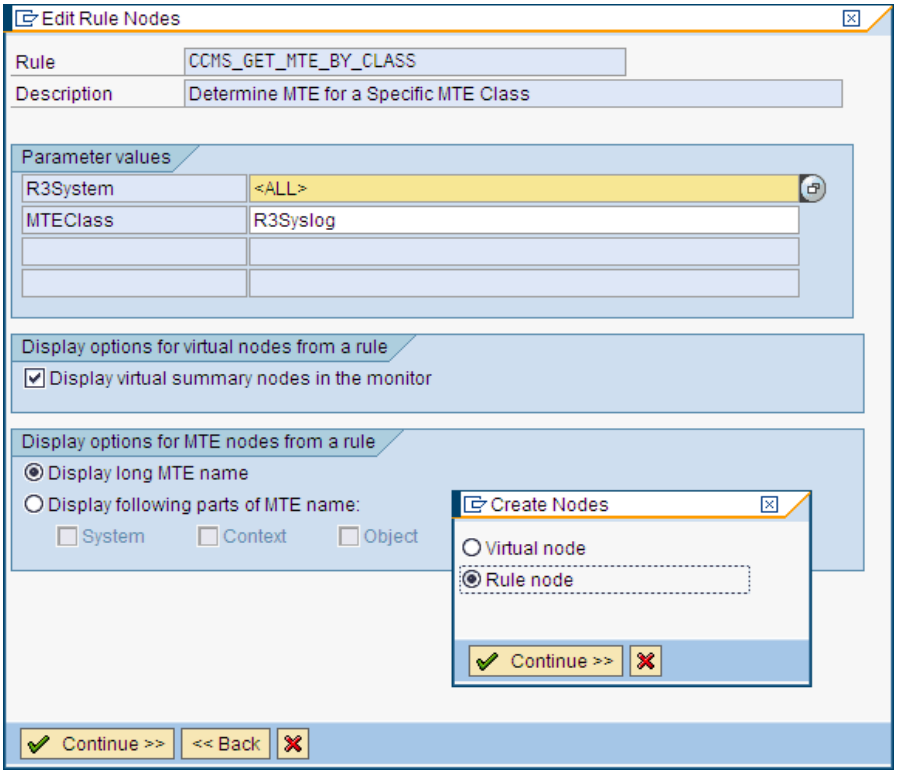
4 Set up the system-log filters

Since `r3monal` supports the same system-log message filtering as `r3monxmi`, you can copy an existing system-log filtering configuration from the old `r3monxmi.cfg` configuration file and paste it into the new `r3monal.cfg` file. System-log message filtering is defined with the AlerMonSysLog keyword in the AlertClasses section of the configuration file.

```
#-------------------------------------------------------
# Alert Classes SAP      SAP      SyslogId    Enabled=1
#               System   Number   From  To    Disabled=0
AlerMonSyslog   =ALL     =ALL     =A00  =MZZ  =1
AlerMonSyslog   =ALL     =ALL     =N00  =ZZZ  =0
AlerMonSyslog   =LP      =01      =A00  =ZZZ  =1
#-------------------------------------------------------
```

Figure 5 on page 59 shows you how the CCMS rule node for SAP syslog elements should look when you complete the configuration successfully.

Figure 5 Rules-based CCMS MTE for Syslog Elements



r3monal: Monitoring the J2EE Engine (Web AS Java)

The SPI for SAP can help you monitor the complete SAP NetWeaver environment, including the SAP J2EE Engine. Monitoring the SAP J2EE Engine is important since the combination of Java technology and the J2EE infrastructure is the foundation on which new SAP components such as the SAP Enterprise Portal or Exchange Infrastructure (XI) are built.

To monitor the SAP J2EE engine, you configure `r3monal`, the SPI for SAP's CCMS Alert monitor, to check for alerts generated by the J2EE monitor sets, which concern the status and availability of SAP's J2EE Engine, for example: the J2EE kernel, J2EE services, or the registered SAP CCMS agents within the SAP NetWeaver environments that you are monitoring with the SPI for SAP. For more information about configuring `r3monal` to monitor SAP's J2EE engine, see The J2EE (Web AS Java) Monitor on page 81.

r3monal: Monitoring Stand-alone Enqueue Servers

The enqueue server stores information about the locks currently in use by the users logged into the SAP System; the lock-related information is stored in the lock table of the main memory. If the host on which the enqueue server is running fails, the lock data is lost and cannot be restored even when the enqueue server restarts and all locks have to be reset. In a high-availability environment, you can avoid problems of this kind by configuring a stand-alone enqueue server. The combination of a stand-alone enqueue server and an enqueue replication server running on a separate host forms the basis of a high-availability solution.

To use the SPI for SAP to monitor alerts generated by a stand-alone enqueue server configured in a high-availability WebAS environment, you have to enable the appropriate CCMS monitors and MTEs (monitor-tree elements) in SAP and then configure `r3monal`, the SPI for SAP's CCMS alert monitor, to check for alerts concerning the status and performance

of the stand-alone enqueue server in the SAP System. For more information about configuring `r3monal` to monitor a stand-alone enqueue server in WebAS, see The Enqueue-Server Monitor on page 84.

r3monal: Monitoring SAP Security-Audit Logs

The SAP security-audit log keeps a record of security-related activities in the SAP System and stores the information it collects in an audit log on each application server. The SPI for SAP allows you to monitor the CCMS alerts logged by the security-audit use them to generate messages, which you can arrange to send to the HPOM for Windows console.

To use the SPI for SAP to monitor the SAP security-audit logs, you have to enable the appropriate CCMS monitors and MTEs (monitor-tree elements) in SAP and then configure `r3monal`, the SPI for SAP's CCMS alert monitor, to check for alerts generated by the security-audit-log monitor, which concern the status of security events in the SAP System. For more information about configuring `r3monal` to monitor SAP's security-audit logs, see The SAP Security-Audit Monitor on page 90.

r3monal: Monitoring the Enterprise Portal

The SAP Enterprise Portal provides a secure and stable web interface that gives users global access to the information, applications, and services that they need to work effectively in the SAP landscape. The SPI for SAP allows you to make use of standard SAP elements to monitor the components of the SAP Enterprise Portal and provide reports on availability, response time, configuration, and performance.

To use the SPI for SAP to monitor alerts generated by a fully configured SAP Enterprise Portal, you have to enable the appropriate CCMS monitors and MTEs (monitor-tree elements) in SAP and then configure `r3monal`, the SPI for SAP's CCMS alert monitor, to check for alerts concerning the status and performance of the Enterprise Portal. For more information about configuring `r3monal` to monitor an Enterprise Portal, see The SAP Enterprise-Portal Monitor on page 86.

r3monal: Monitoring the CEN

The central monitoring system (CEN) is a single SAP system that you designate as the central point of control for CCMS alerts originating from all over the monitored SAP landscape. The CEN concept allows you to reduce the overhead of monitoring and managing multiple SAP systems by making essential information concerning problem alerts available in one, central location.

After you configure SAP to use the CEN for the central management of CCMS alerts, you can use the SPI for SAP's `r3monal` monitor to intercept the CCMS alerts destined for the CEN and use the alerts to generate messages, which it forwards to the HPOM for Windows console. For more information about configuring `r3monal`to monitor an SAP CEN, see Monitoring CCMS Alerts in the CEN on page 193.

r3monal: Testing the Configuration

The SPI for SAP's optional test transport includes a program that generates an ABAP dump which you can use to verify that the `r3monal` monitor checks the syslog and sends a message to HPOM for Windows if a dump occurs in the SAP System. If the test completes successfully,

a message about the test dump appears in the HPOM for Windows console. Note that this test works only if you configure `r3monal` to monitor the appropriate SAP CCMS monitor sets, for example: `<SAPSID>/R3Abap/Shortdumps`.

For more information about SPI for SAP transports, see the transports read-me file `\usr\sap\trans\readme` on the HPOM for Windows managed node; for more information about importing and applying SPI for SAP transports, see the *HP Operations Smart Plug-in for SAP Configuration Guide*. After importing the transport, you can view the test programs installed by using the SAP transaction **`SE80`** to open the ABAP object navigator and browsing to the report (or program) `/HPOV/YSPI0004`.

r3mondev: The SAP Trace-file Monitor

The `r3mondev` monitor scans the trace files and log files of the SAP system for the string "`ERROR`". Because it monitors only what has occurred since its previous run, any error within a trace file generates only a single alert. The file monitor scans the following directories, where `<SID>` stands for the SAP system ID and `<InstanceNumber>` stands for the SAP instance number of the monitored SAP System:

- **UNIX/Linux**: `/usr/sap/<SID>/<InstanceNumber>/work/`
- **Windows**: `<drive:>\usr\sap\<SID>\<InstanceNumber>\work`

This section contains information about the following topics:

r3mondev: File Locations

The file monitor, `r3mondev`, includes the files listed in Table 8. For more detailed information about the contents of the in SPI for SAP monitor-configuration files in general and the file `r3mondev.cfg` in particular, see The SPI for SAP Monitor-Configuration File on page 26.

Table 8 r3mondev Files

File	Description
`r3mondev(.exe)`	Executable for the file monitor
`r3mondev.cfg`	Configuration file for monitored files
`r3mondev.his`	History file that stores data for each monitor run

r3mondev: Environment Variables

The file monitor uses environment variables listed in Table 9.

Table 9 r3mondev Environment Variables

Environment Variable	Description
SAPOPC_DRIVE	The Windows drive where the HPOM agent is running, for example; `E:\usr\...`
SAPOPC_HISTORYPATH	Path to the `r3mondev` history file
SAPOPC_R3MONDEV_CONFIGFILE	Name of the `r3mondev` configuration file
SAPOPC_SAPDIR	The Windows drive where SAP NetWeaver is running, for example: `E:\usr\sap`
SAPOPC_TRACEMODE	Trace mode: a = append w = create (default)
SAPOPC_TRACEPATH	Path to the `r3mondev` trace file

r3mondev: Monitoring Conditions

This section of the `r3mondev.cfg` file enables you to specify the device monitoring details for the SPI for SAP.

For more information about the entries in the `r3mondev.cfg` file including keywords and their possible values along with a description of each editable parameter, see The Alert-Monitor Configuration Files on page 46.

The monitoring conditions section of the `r3mondev.cfg` file includes the following default settings:

```
# AlertDevMon  SAP    SAP    Enable=1   File     Severity  Opc        OpC
#              System Number Disable=0  Mask               Object     MsgGrou
p
AlertDevMon    =ALL   =ALL      =1      =dev_*   =WARNING  =r3mondev  =R3_Tra
ce
AlertDevMon    =ALL   =ALL      =1      =std*    =CRITICAL =r3mondev  =R3_Tra
ce
```

r3mondev: Editing the Configuration File

You can edit the r3mondev monitor's configuration file, `r3mondev.cfg`, in the following ways:

- **Disable messages**

If you do not want to receive any messages relating to `dev_*` files for any of the SAP systems you are monitoring with the SPI for SAP, change the first line of the `r3mondev.cfg` configuration file as follows:

```
AlertDevMon    =ALL    =ALL      =0      =dev_* =WARNING =r3mondev =R3_Tr
ace
```

- **Change a message's severity level**

  If you want to reduce the severity of all messages relating to `std*` files from critical to warning, change the second line of the `r3mondev.cfg` configuration file as follows:

  ```
  AlertDevMon =ALL =ALL =1 =std* =WARNING =r3mondev =R3_Trace
  ```

- **Define exceptions to general rules**

  If you want to increase the severity of messages relating to `dev_*` files on SAP system LP2 from warning to critical, leave the default settings as they are and add the following line:

  ```
  AlertDevMon  =LP2  =ALL  =1  =dev_*  =CRITICAL  =r3mondev\
  =R3_Trace
  ```

Wildcards are only allowed at the end of the string. Only SAP trace files located in the work directory are relevant and the names of these files must begin with either `dev` or `std`.

r3monpro: The SAP Process Monitor

The `r3monpro` monitor scans all processes associated with a given instance, such as dialog, enqueue, update, batch, dispatch, message, gateway, and spool work processes. It is also used for monitoring database processes.

This section contains information about the following topics:

r3monpro: File Locations

The process monitor `r3monpro` contains the files listed in Table 10. For more detailed information about the contents of the in SPI for SAP monitor-configuration files in general and the file `r3monpro.cfg` in particular, see The SPI for SAP Monitor-Configuration File on page 26

Table 10 r3monpro Files

File	Description
`r3monpro(.exe)`	Executable for the process monitor
`r3monpro.cfg`	Configuration file for the process monitor
`r3monpro.his`	History file for storing data after each monitor run

r3monpro: Environment Variables

The process monitor `r3monpro` uses the environment variables listed in Table 11.

Table 11 r3monpro Environment Variables

Environment Variable	Description
SAPOPC_DRIVE	The Windows drive where the HPOM agent is running, for example; `E:\usr\...`
SAPOPC_HISTORYPATH	Path to the `r3monpro` history file
SAPOPC_R3MONPRO_CONFIGFILE	Name of the `r3monpro` configuration file
SAPOPC_SAPDIR	The Windows drive where SAP NetWeaver is running, for example: `E:\usr\sap`
SAPOPC_TRACEMODE	Trace mode: a = append w = create (default)
SAPOPC_TRACEPATH	Path to the `r3monpro` trace file

r3monpro: Monitoring Conditions

Monitoring conditions for `r3monpro` are specified in the `r3monpro.cfg` file. Individual rows define monitoring conditions for specific processes. You use the `r3monpro.cfg` file to set the rules which define how the number of processes running should be measured and what severity level should be assigned to the alert that is generated if the number of processes exceeds the limits you define.

You can set monitoring conditions for a specific process to any of the following modes:

- **Exact**

  The number of process running on a managed node must be equal to the specified number.

- **Min**

  The number of processes running on a managed node must not be less than the specified number.

- **Max**

  The number of processes running on a managed node must not be more than the specified number.

- **Delta**

  `r3monpro` triggers an alert if there is any change in the number of processes running on a managed node or if the specific amount of allowed change in the number of instances of the same process exceeds the defined limit. This mode enables you to recognize changes without having to define an absolute number of processes for a managed node.

For example, if Delta =2, then a difference of 2 or more between the number of processes (*n*) found in the previous and current monitor run on a managed node triggers an alert. Note that if `r3monpro` triggers an alarm, it resets *n* to the number of processes discovered in the most recent monitor run, and calculates the new Delta on the basis of the new number of processes found running.

Messages generated by matched conditions include an operated-initiated action; the action calls an SPI for SAP module which lists all the current processes for the affected SAP instance.

For more information about the entries in the `r3monpro.cfg` file including keywords and their possible values along with a description of each editable parameter, see The Alert-Monitor Configuration Files on page 46.

r3monpro: Example Configuration

The first row of the following example shows how to monitor the `saposcol` process on all hosts. Note that exactly one such process should run at any given time. Any violation of this number is critical. It affects the HPOM for Windows object `saposcol`. The associated HPOM for Windows message group is `R3_State`.

The last row of the same example specifies that eight or fewer instances of the `dw.sapSID` process should run on all hosts. If the number is larger than eight, the monitor generates a warning message associated with HPOM for Windows object `dw.sap` and HPOM for Windows message group `R3_State`.

The string `SID` has special meaning in this context. `SID` will be replaced by the SAP System name on the managed node. This enables global definitions for different SAP Systems.

```
AlertInstMonPro  =ALL =00  =saposcol  =1 =Exact=1 =CRITICAL =saposcol =R3_Sta
te
AlertInstMonPro  =C01 =00  =explorer  =1 =Max  =1 =CRITICAL =explorer =R3_Sta
te
AlertInstMonPro  =T11 =00  =dw.sapSID =1 =Min  =8 =WARNING  =dw.sap   =R3_Sta
te
```

It is also possible to ensure that a process is not running. To do so, use the mode `Exact` and enter 0 as the number.

On servers running the UNIX operating system, `r3monpro` can identify processes at the instance level. On servers running the Windows operating system, you need to define on a single line the total number of work processes on the node. For example, if there are two SAP instances, each with four (4) work processes, the total number of processes is eight (8).

For SAP servers running on UNIX operating systems, you can configure the SPI for SAP process monitor `r3monpro` to monitor the specific SAP-gateway read process `gwrd` associated with individual SAP SIDs, which is especially useful in a multi-SID environment. If you have multiple instances of SAP running in the same SID, you can configure `r3monpro` to monitor the specific SAP-gateway read process `gwrd` assigned to each, individual *instance*, too. For more information about how to configure `r3monpro` to monitor individual `gwrd` processes in an environment where multiple SAP instances or multiple SAP SIDs are running on the same SAP server, have a look at the following examples:

- Monitoring SAP-Gateway Read Processes per SID on page 66

  Monitoring SAP-Gateway Read Processes per SAP SID

- Monitoring SAP-Gateway Read Processes per SAP Instance on page 66

Monitoring SAP-Gateway Read Processes per SAP Instance

Monitoring SAP-Gateway Read Processes per SID on page 66 shows how to configure r3monpro to monitor the individual gwrd processes associated with specific SIDs on a SAP server hosting multiple SAP SIDs.

Monitoring SAP-Gateway Read Processes per SID

```
AlertInstMonPro  =Q12  =ALL  =gwrd -dp pf=/usr/sap/
SID* =1 =Exact =1 =CRITICAL \
=gwrd  =R3_State
AlertInstMonPro  =Q22  =ALL  =gwrd -dp pf=/usr/sap/
SID* =1 =Exact =1 =CRITICAL \
=gwrd  =R3_State
AlertInstMonPro  =Q32  =ALL  =gwrd -dp pf=/sapmnt/
SID*  =1 =Exact =1 =CRITICAL \
=gwrd  =R3_State
AlertInstMonPro  =Q52  =ALL  =gwrd -dp pf=/usr/sap/
SID* =1 =Exact =1 =CRITICAL \
=gwrd  =R3_State
```

Monitoring SAP-Gateway Read Processes per SAP Instance on page 66 shows how to configure r3monpro to monitor the individual gateway processes associated with specific SAP instances on a SAP server hosting multiple SAP instances per SAP SID.

Monitoring SAP-Gateway Read Processes per SAP Instance

```
AlertInstMonPro  =Q12  =12  =gwrd -dp pf=/usr/sap/
SID*  =1 =Exact =1 =CRITICAL \ =gwrd  =R3_State
AlertInstMonPro =Q22 =21 =gwrd -dp pf=/usr/sap/Q22/SYS/profile/
Q22_D21_sap2ap1 \ =1  =Exact  =1  =CRITICAL  =gwrd  =R3_State
AlertInstMonPro =Q22 =22 =gwrd -dp pf=/usr/sap/Q22/SYS/profile/
Q22_D22_sap2ap1 \ =1  =Exact  =1  =CRITICAL  =gwrd  =R3_State
AlertInstMonPro =Q32  =32  =gwrd -dp pf=/sapmnt/
SID*  =1 =Exact  =1  =CRITICAL \ =gwrd  =R3_State
AlertInstMonPro =Q52 =52  =gwrd -dp pf=/usr/sap/
SID* =1  =Exact  =1  =CRITICAL \ =gwrd  =R3_State
```

In the configuration file r3monpro.cfg, the path to the SAP-instance profile defined in the pf parameter is case-sensitive. To avoid problems, make sure that the path to the SAP-instance profile defined in the r3monpro.cfg configuration file matches the path displayed in the output of the ps command, for example:

```
[root@accra]# ps -eaf | grep gwrd
Q22adm 15691 15688  0  Jun  6  ?      52:54 gwrd -dp \ pf=/usr/sap/Q22/SYS/profile/Q22_D21_sap2ap1
root 20756 20599  0 10:22:58 pts/tb    0:00 grep gwrd
```

r3status: The SAP Status Monitor

The r3status monitor checks the current status of SAP NetWeaver and compares it with the last recorded status to determine whether any change in status occurred since the last time the monitor ran. Using the SAP NetWeaver function module RFC_SYSTEM_INFO, the r3status monitor provides the following features:

- Reports about local SAP NetWeaver system-availability

- Recognition and monitoring of each individual SAP NetWeaver instance
- SAP NetWeaver availability status reported may be: up, down, hanging (RFC time out).

The `r3status` monitor is of type *time frame*. It runs every two minutes and compares the current value with the previous value stored in the history file and generates a message if it finds a difference, which it needs to report. For more information about reporting types, see Report Types for the Alert-Collector Monitors on page 97.

The lack of response from SAP could be due to a problem which does not mean that the System is down. For example, SAP would not respond if all available dialog work processes were allocated. For more information about how `r3status` interprets the responses it receives from SAP, see r3status: Establishing the SAP Status on page 70.

This section contains information about the following topics:

r3status: File Locations

This table lists the files used by the `r3status` monitor.

Table 12 r3status Files

File	Description
`r3status(.exe)`	Executable for the `r3status` monitor
`r3status.log`	The `r3status` monitor creates a log/trace file after each run of the monitor. The trace file is stored in the standard HPOM Agent log directory.
`r3itosap.cfg`	The `r3status` monitor uses information in the `r3itosap.cfg` file to determine which SAP instances it is supposed to monitor.
`r3status.cfg`	The `r3status` monitor uses information in the `r3status.cfg` file to determine history paths, trace levels, and which SAP instances it is supposed to monitor on remote SAP servers.
`r3status.his`	History file for storing data after each run of the `r3status` monitor. The `r3status` monitor uses information in this file to determine whether a change of status has occurred. For more information, see r3status: History File on page 69.

r3status: Environment Variables

Table 13 lists the environment variables used by the `r3status` monitor.

Table 13 r3status Environment Variables

Environment Variable	Description
SAPOPC_RFC_TIMEOUT	set time out value for RFC connections - default is 20 seconds
SAPOPC_HISTORYPATH	Path to the `r3status.his` history file [a]
SAPOPC_R3STATUS_CONFIGFILE	Name of the configuration file, which the `r3status` monitor uses

Table 13 r3status Environment Variables (cont'd)

Environment Variable	Description
SAPOPC_R3ITOSAP_CONFIGFILE	Name of the general configuration file, which contains SAP login information used by the SPI for SAP monitors
SAPOPC_TRACEMODE	Trace mode: a = append w = create (default)
SAPOPC_TRACEPATH	Path to the `r3status` trace file

a. See: r3status: History File on page 69

r3status: History File

The first time the `r3status` monitor runs, it writes its findings to the history file, `r3status.his`. The next time the `r3status` monitor runs, it uses the information in the `r3status.his` file to determine whether a change of status has occurred since the last time the monitor ran and, as a consequence, which if any message it needs to send to the HPOM for Windows management server. For more information about the default location of the monitor history files on the managed nodes, see The SPI for SAP Monitor-Configuration File on page 26.

The `r3status` monitor updates the entries in the `r3status.his` file at the end of each time it runs, with the current timestamp and the current status of each monitored SAP instance.

Excerpt from the r3status.his file on page 69 shows the format and contents of the `r3status.his` file.

Excerpt from the r3status.his file

```
021028-11:18:29
#-------------------------------------------------------------
021028-11:18:29 #Keyword              SAP     SAP     SAP          State
021028-11:18:29 #                     System  Number  Instance
021028-11:18:29 #
021028-11:18:29 ConfiguredInstance    =DEV    =00     =DVEBMGS00   =UP
021028-11:18:29 ConfiguredInstance    =PKR    =99     =DVEBMGS99   =DOWN
-------------------------------------------------------------------------
---
```

The r3status Configuration File

The r3status monitor's configuration file allows you to use the keywords listed below to change the configuration from the default settings to meet the requirements of your particular environment. Where appropriate, possible values for a given keyword are also specified. Default r3status Configuration File on page 71 shows what a complete configuration file looks like for the `r3status` monitor, which monitors the status of both local and remote SAP Systems.

The following standard keywords work as expected in the context of the `r3status.cfg` configuration file. For more information about the parameters the keywords require, see The SPI for SAP Monitor-Configuration File on page 26:

- TraceLevel
- TraceFile
- HistoryPath[Unix | AIX | WinNT]

The following keywords require special attention when used in the context of the SPI for SAP `r3status.cfg` configuration file:

- **EnableDPQueueCheck**

  `r3status` requires a dialog work process to log on to SAP and determine the System's status. Enable the EnableDPQueueCheck keyword (=1) if the SAP System whose status you are monitoring is experiencing performance problems and you want `r3status` to check the size and status of the ABAP dispatcher before starting its monitor run. If there are no, or too few, dialog work processes available, `r3status` sends a message to the console indicating that it did not start due to the violation of a threshold defined for dialog processes. The command disables the monitor run only for the SIDs where the threshold violation for the dialog work processes occurred.

  If you use the EnableDPQueueCheck keyword in the `r3status` configuration file, remember to configure the keywords DPQueueCheck and DisableMonitoringWithSeverity in the `r3mondisp.cfg` configuration file, too. For more information about monitoring the ABAP dispatcher and its queues, see r3mondisp: the ABAP Dispatcher Monitor on page 77.

  The default run interval for `r3status` is two minutes. If your SAP landscape consists of large numbers of SAP instances running on multiple hosts, network congestion or a slow response from SAP might prevent EnableDPQueue from checking the status of the ABAP dispatchers on all the configured SAP instances before `r3status` starts its next run. In the unlikely event that this happens, the old instance of `r3status` aborts without reporting the status of any dispatchers that it has not yet checked. To avoid this problem re-occurring, increase the run interval for `r3status`.

- **RemoteMonitoring**

  `r3status` cannot check the status of the ABAP dispatcher on a SAP System, which the SPI for SAP is monitoring remotely.

  For more information about monitoring the status of remote SAP Systems, see r3status: Monitoring SAP Remotely on page 71.

r3status: Establishing the SAP Status

When the status monitor, `r3status`, checks the availability of an SAP System, it reports the status as: up, down, or connection time-out. Although the meaning of "up" and "down" is clear, the status of the connection time-out status requires some explanation. The time-out status could occur if an SAP System is hanging, in which case the problem could be due to an RFC time out, which itself needs investigating and is a good example to show how difficult it can sometimes be to establish the exact state of the SAP System the SPI for SAP is monitoring.

The status monitor, `r3status`, considers an SAP instance as "not available" if the SAP instance does not respond within 60 seconds. However, the lack of response from SAP could be due to a problem which does not mean that the System is down, for example: all available

dialog work processes are allocated, or all available SAP gateway connections are busy. The SPI for SAP status monitor, `r3status`, reports the status of the SAP System it is monitoring according to the following rules:

- Available:

  `r3status` reports an SAP System as available if it can log on to the SAP instance and, in addition, start and receive a response from the SAP function module RFC_SYSTEM_INFO within 60 seconds.

- Not Available:

  `r3status` reports an SAP System as *not* available if the SAP instance does not respond within 60 seconds or the function module RFC_SYSTEM_INFO could not start, for example: due to the fact that the instance is down.

r3status: Monitoring SAP Remotely

The SPI for SAP includes a feature which allows you to extend the scope of the monitors to remotely monitor the status of SAP on SAP servers (which are *not* HPOM for Windows managed nodes) from a host, which *is* already configured as an HPOM for Windows managed node and where the SPI for SAP is running.

To make use of the remote-monitoring feature provided by the SPI for SAP, for example; to monitor a SAP server running on an operating system that is not supported by the SPI for SAP, you need to enable the **RemoteMonitoring** keyword (by removing the leading hash symbol "#") in the `r3status.cfg` file. Next, on the same line, you define the name of the local host, which you want to perform the monitoring. Finally, you have to define the name of the remote SAP server, which you want to monitor. Default r3status Configuration File on page 71 shows how a new line is required for each *additional* SAP server, which you want to monitor remotely.

You can associate multiple remote SAP servers with one, single local host or you can associate single remote hosts with individual, different local hosts. Default r3status Configuration File on page 71 shows a mixed approach where one *local* host "sap1" is used to monitor two *remote* hosts; "sdsap" and "sapwolf". A third local host "sap2" remotely monitors the remote host "triosap".

For more information about the contents of the `r3status` monitor's configuration file including the keywords and parameters you use to define local and remote server names, see the entry concerning "Remote Monitoring" in The r3status Configuration File on page 69.

Default r3status Configuration File

```
#-------------------------------------------------------------
# TraceLevel   hostname   Disable=0  only error messages=1
#                         info messages=2  debug messages=3
#
TraceLevel     =ALL       =0
#-------------------------------------------------------------
# TraceFile   hostnam   filename
#
TraceFile     =ALL      =r3status.log
#-------------------------------------------------------------
# History          hostname    path
# Path
#
HistoryPathUniX   =ALL        =default
```

```
HistoryPathAIX    =ALL        =default
HistoryPathWinN   =ALL        =default
#-------------------------------------------------------------
# Check the ABAP dispatcher before a connection to SAP is
# opened. If the dialog queue is too full or not enough
# free work processes are available, monitoring is disabled.
#
# This feature should only be enabled in special cases. For
# regular dispatcher monitoring, use the r3mondisp.
#
# EnableDPQueueCheck  hostname  SAP      SAP      Enable=1/
                                System   Number   Disable=0
EnableDPQueueCheck    =ALL      =ALL     =ALL     =0
#-------------------------------------------------------------
# Remote            Local       Remote
# Monitoring        Host        Host
RemoteMonitoring    =sap1       =sdsap
RemoteMonitoring    =sap1       =sapwolf
RemoteMonitoring    =sap2       =triosap
#-------------------------------------------------------------
```

r3monsec: The SAP Security Monitor

The SPI for SAP security monitor checks the following areas in your SAP Systems:

- The privileges and authorizations assigned to (and used by) important SAP users
- Insecure (default) passwords in use by SAP and Oracle users
- SAP System parameters which affect overall system security
- Miscellaneous security events such as failed logins or attempts to change SAP System settings

In addition to the other SAP user roles and authorizations required by the SPI for SAP (such as SAPSPI_MONITORING_*), you also have to assign the authorizations defined in the SAP user role /HPOV/SAPSPI_SECURITY_MON to the HPOM for Windows user under which `r3monsec` runs before `r3monsec` starts; the user role /HPOV/SAPSPI_SECURITY_MON includes authorizations (such as S_TCODE or S_USER_AUT) that are needed to execute the SAP reports, which `r3monsec` calls by means of the SAP RFC interface.

This section contains information about the following topics:

- r3monsec: File Locations on page 73
- r3monsec: Alert Types on page 73
- r3monsec: Monitoring Security Remotely on page 76

If you use the SPI for SAP tools located in the console to configure `r3monsec`, the SPI for SAP checks the validity of the new configuration when you try to save the modified configuration file. For more information about the validation tool and the messages it generates, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

r3monsec: File Locations

The SAP System-security monitor `r3monsec` uses the files listed in this table.

Table 14 r3monsec Files

File	Description
`r3monsec(.exe)`	Executable for the SAP System-security monitor
`r3monsec.cfg`	Configuration file for the SAP System-security monitor.
`r3monsecpw.msg`	Contains encrypted passwords for standard Oracle users in an SAP environment.
`r3monsec.log`	File used to store trace data collected by the SAP System-security monitor.

r3monsec: Alert Types

The security monitor `r3monsec` uses the following alert types:

- r3monsec: SAP_PARAMETERS on page 73

  Monitors security-related parameters such as those defined in the SAP report RSPFPAR.

- r3monsec: DEFAULT_USERS on page 75

  Monitors settings for passwords defined for SAP and Oracle users to ensure that insecure default passwords are not in use.

- r3monsec: PRIVILEGED_USERS on page 75

  Monitors any special privileges granted to SAP users or being requested by users who are not normally entitled.

The SPI for SAP interprets *include* and *exclude* parameter values for an alert-type entry according to whether the values appear in the same parameters or in different parameters. The SPI for SAP compares values in *different* parameters using 'and'; the SPI for SAP compares values in the *same* parameter as follows.

- **Include**: use 'or' to compare the parameters
- **Exclude**: use 'and' to compare the parameters

The SPI for SAP evaluates *include* values before it evaluates *exclude* values.

Note that the SPI for SAP ignores include and exclude parameters for the `r3monsec` alert types SAP_PARAMETERS and DEFAULT_USERS; however, you *must* use include and exclude parameters for the alert type PRIVILEGED_USERS.

r3monsec: SAP_PARAMETERS

Use the SAP_PARAMETERS alert type to configure the SPI for SAP's security monitor, `r3monsec`, to monitor the settings of (and any changes to) security-related SAP parameters. The SAP_PARAMETERS alert type compares the values you define in the `r3monsec.cfg` file with the contents of the SAP report RSPFPAR, which contains security-related parameters for the SAP instances you are monitoring.

The default settings for the alert type SAP_PARAMETERS reflect a small selection of the parameters defined in the SAP report RSPFPAR; you can change the contents of the SAP_PARAMETERS section of the `r3monsec.cfg` file to suit the needs of your SAP environment by adding, modifying, or removing values accordingly.

The alert type SAP_PARAMETERS ignores the include (=I) and exclude (=E) parameter.

Example SAP_PARAMETERS settings on page 74 shows how to configure `r3monsec` to monitor the SAP parameter, which defines whether SAP should automatically unlock locked SAP users at midnight. The example configuration tells `r3monsec` to check that the automatic unlocking of locked SAP users is *disabled* in SAP (=EQ =0). In this example, `r3monsec` would generate a message with the severity level "critical" if it found that the parameter was enabled in SAP and assign the generated message to the HPOM for Windows message group R3_Security.

Example SAP_PARAMETERS settings

```
AlertMonFun  =ALL  =ALL  =ALL  =ALL  =SECURITY =1\
=CRITICAL =SAP_PARAMETERS =R3_Security\
=SAP_PARAMETERS =login/failed_user_auto_unlock =I =EQ =0 =
```

Table 15 on page 74 shows the default settings for the SAP_PARAMETERS alert type; if your SAP Systems are configured differently, `r3monsec` will generate alerts. For example, in the default configuration, SAP user passwords must have 6 characters or more and contain at least 4 letters and 2 integers. If you configure your SAP instance to allow passwords which do not conform to the rules defined in `r3monsec`'s configuration file, for example: passwords which contain only five characters or do not contain any integers, `r3monsec` sends a message to the console.

Note that `r3monsec` does not read or check the SAP passwords themselves; `r3monsec` compares the *rules* you define in `r3monsec.cfg` for the length and form of SAP passwords with the *rules* defined in SAP itself for password creation. If the rules for password creation, form, or length in the `r3monsec.cfg` file differ in any way from the rules for passwords defined in SAP, the SPI for SAP sends a message to the console.

Table 15 Default Settings for SAP_PARAMETERS

Parameter	Default Value
login/failed_user_auto_unlock	0 (0=disabled; 1=enabled)
login/fails_to_session_end	3
login/fails_to_user_lock	5
login/min_password_diff	3
login/min_password_lng	6
login/min_password_letters	4
login/min_password_digits	2
login/min_password_specials	0
login/no_automatic_user_sapstar	1
login/password_max_new_valid	10

Table 15 Default Settings for SAP_PARAMETERS (cont'd)

Parameter	Default Value
login/password_max_reset_valid	2
login/password_expiration_time	30
login/disable_password_logon	0 (0=disabled; 1=enabled)
login/disable_multi_gui_login	0 (0=disabled; 1=enabled)
login/disable_cpic	0 (0=disabled; 1=enabled)
login/system_client	100
login/disable_multi_rfc_login	0 (0=disabled; 1=enabled)
rdisp/gui_auto_logout	1800

r3monsec: DEFAULT_USERS

Use the DEFAULT_USERS alert type to configure the SPI for SAP's security monitor, `r3monsec`, to check the passwords for standard SAP or Oracle database users and determine whether any well-known, default passwords are still in use. Standard SAP users include SAP*, DDIC, SAPCPIC, and EARLYWATCH. The DEFAULT_USERS alert type makes use of the SAP report RSUSR003.

The `r3monsec.cfg` configuration file provides default settings for the alert type DEFAULT_USERS. Note that the include (=I) and exclude (=E) parameter is ignored for the alert type DEFAULT_USERS.

Default Settings for DEFAULT_USERS

```
AlertMonFun  =ALL  =ALL  =ALL  =ALL  =SECURITY =1\
=CRITICAL =DEFAULT_USERS =R3_Security\
=DEFAULT_USERS
```

The default configuration for the DEFAULT_USERS alert type enables the SAP and Oracle user check, which means the monitor generates an alert if it finds a default password in use.

r3monsec: PRIVILEGED_USERS

Use the PRIVILEGED_USERS alert type to configure the SPI for SAP's security monitor, `r3monsec`, to check the authorizations granted to SAP users in the Systems you are monitoring with the SPI for SAP. The PRIVILEGED_USERS alert type compares the values defined in the `r3monsec.cfg` file with the contents of the SAP report RSUSR005, which lists

information concerning the critical authorizations granted to SAP users. The SAP System-security monitor, `r3monsec`, generates an alert for any SAP user who has critical authorizations but is not defined in the `r3monsec.cfg` file.

The SAP report RSUSR005 is SAP-client dependent; `r3monsec` monitors only the users for the SAP clients defined in the central SPI for SAP configuration file `r3itosap.cfg`.

The `r3monsec.cfg` configuration file does not provide any default settings for the alert type PRIVILEGED_USERS; you have to decide which user authorizations you want to monitor in SAP and insert the strings that define them into the monitor-configuration file manually. You can use the report RSUSR005 to find the strings defining the authorizations you want to monitor, for example: "All rights for background jobs", as illustrated in Example Settings for PRIVILEGED_USERS on page 76. Note that you need to use a new line for each user authorization that you want to monitor.

After you have determined which user authorizations you want to monitor, set the include (=I) or exclude (=E) parameter to specify which SAP users you want to check for the use (or misuse) of the defined authorization. Example Settings for PRIVILEGED_USERS on page 76 shows how to exclude SAP user KWAME from the check to determine which users have permission to execute external operating-system commands.

Example Settings for PRIVILEGED_USERS

```
AlertMonFun  =ALL  =ALL  =ALL  =ALL  =SECURITY =1\
=CRITICAL =PRIVILEGED_USERS =R3_Security\
=PRIVILEGED_USERS =All rights for background jobs =I =EQ =ALL =
AlertMonFun  =ALL  =ALL  =ALL  =ALL  =SECURITY =1\
=CRITICAL =PRIVILEGED_USERS =R3_Security\
=PRIVILEGED_USERS =Execute external operating system commands\
=E =EQ =KWAME =
```

Note that the string you paste into the `r3monsec.cfg` file must match an existing string in SAP. If the string you paste into the `r3monsec.cfg` configuration file does not exist in SAP, for example because it contains a typo or is only a sub-set of a known SAP user-authorization string, no match occurs and the `r3monsec` monitor does not send any message to the console. For example: "Execute external operating" would not match, since it is only a part of the complete user-authorization string "Execute external operating system commands" defined in the `r3monsec.cfg` file.

r3monsec: Monitoring Security Remotely

To make use of the remote-monitoring feature provided by the SPI for SAP, for example; to monitor security on an SAP server running on an operating system that is not supported by the SPI for SAP, you need to enable the RemoteMonitoring keyword (by removing the leading hash symbol "#") in the `r3monsec.cfg` file.

You also need to specify the name of the local host, which you want to perform the monitoring and the name of the remote SAP server, whose security settings you want to monitor. Note that you must add a new line for each *additional* SAP server, which you want to monitor remotely.

Default r3monsec Configuration File

```
#-------------------------------------------------------------
# TraceLevel   hostname   Disable=0  only error messages=1
#                         info messages=2  debug messages=3
#
TraceLevel     =ALL       =0
```

```
#-------------------------------------------------------------
# TraceFile  hostname    filename
#
TraceFile    =ALL        =r3monsec.log
#-------------------------------------------------------------
# History    hostname    path
# Path
#
HistoryPathUnix    =ALL        =default
HistoryPathAIX     =ALL        =default
HistoryPathWinNT   =ALL        =default
#-------------------------------------------------------------
# Remote            Local       Remote
# Monitoring        Host        Host
RemoteMonitoring    =sap1       =sdsap
#-------------------------------------------------------------
# AlertMonFun  SAP       SAP      SAP      SAP     Alertmonitor   Enable =1/
  \
#              Hostname  System   Number   Client                  Disable=0
 \
#
#   OpC          OpC         OpC        \
#   Severity     Object      MsgGroup     \
#
# Alerttype     RFC Parameter
#               =Parameter     =Sign   =Opt    =Low    =High
#              [=Param         =Sign   =Opt    =Low    =High] ...

AlertMonFun  =ALL  =ALL  =ALL  =ALL  =SECURITY =1\
=CRITICAL =SAP_PARAMETERS =R3_Security\
=SAP_PARAMETERS =login/failed_user_auto_unlock =I =EQ =0 =

AlertMonFun  =ALL  =ALL  =ALL  =ALL  =SECURITY =1\
=CRITICAL =DEFAULT_USERS =R3_Security\
=DEFAULT_USERS = = = = =

AlertMonFun  =ALL  =ALL  =ALL  =ALL  =SECURITY =1\
=CRITICAL =PRIVILEGED_USERS =R3_Security\
=PRIVILEGED_USERS =All rights for background jobs =I =EQ =ALL =
```

r3mondisp: the ABAP Dispatcher Monitor

The SPI for SAP's ABAP dispatcher monitor, `r3mondisp`, checks the size, content, and status of the queues for the different types of SAP work-processes and generates an alert if a queue becomes so full that it could have an adverse effect on SAP-System performance, or if a low percentage of work processes is idle.

`r3mondisp` monitors the queues which belong to the SAP instances defined in the SPI for SAP's central configuration file, `r3itosap.cfg` and allows you to manage SAP performance issues more pro-actively by avoiding bottlenecks and helping to ensure that the monitored SAP Systems have enough work processes available to fulfill all user requests, even when loads are typically very high.

This section contains information about the following topics:

r3mondisp: Pre-requisites

If `r3mondisp` is not able to find either the correct version of the SAP executable `dpmon` or the profile of the SAP instance whose queues you want to monitor, it aborts its run, writes an entry in its log file, and sends a message to the console. `r3mondisp` requires a version of the `dpmon` executable, which recognizes the `-s[napshot]` option.

To check if the correct version of the `dpmon` executable is available on the SAP server which you want to monitor with `r3mondisp`, log on to the SAP server as user <SID>adm and run the `dpmon` command with the `-help` option. If the command output displays the `-s[snapshot]` option as shown in Checking the snapshot option on page 78, you can configure and use the `r3mondisp` monitor.

Checking the snapshot option

```
$>dpmon -help
Usage: dpmon <options>
with the following options:
-p[ing]           check dispatcher with NI ping
-i[nfo]           retrieve dispatcher info
-s[napshot]       show info and terminate
-t <trace_level>  tracelevel (default:1)
-f <trace_file>]  name of the tracefile (default: dev_dpmon)
-T <timeout>     network time-out value in ms (default:500)
```

On both UNIX and Windows operating systems, `r3mondisp` uses the environment variables SAPOPC_DPMON_PATH_ and SAPOPC_PROFILE_<*SID*>_<*InstNr*> to determine the location of `dpmon` and the SAP instance profile respectively. If the variables are not set, `r3mondisp` uses the registry on Windows operating systems to determine the path to `dpmon` and the profile-file for the monitored SAP instances.

On UNIX operating systems, `r3mondisp` does not require any special interface to determine the location of `dpmon` or the profile-file for the monitored SAP instances: it assumes they are in the default SAP location. If you know the profiles files are not in the default location, or the name of the profile does not follow standard SAP naming conventions, you must indicate this in the `r3mondisp.cfg` configuration file. The standard naming convention for an SAP profile is:

```
<SID>_[D|DVEBMGS]<SysNr>_<hostname>
```

For more information about the contents of the `r3mondisp` configuration file, see The r3mondisp Configuration File on page 80.

r3mondisp: File Locations

The SAP System-security monitor `r3mondisp` uses the files listed in this table.

Table 16 r3mondisp Files

File	Description
`r3mondisp(.exe)`	Executable for the ABAP Dispatcher-queue monitor
`r3mondisp.cfg`	Configuration file for the ABAP dispatcher-queue monitor.
`r3mondisp.log`	File used to store trace data collected by the ABAP dispatcher-queue monitor.

Integrating r3mondisp with the SPI for SAP Monitors

To prevent the SPI for SAP itself causing excessive and unnecessary load on the SAP System at critical times, you can configure the SPI for SAP's ABAP-dispatcher monitor `r3mondisp` to work together with the other SPI for SAP monitors so that the monitors check the status of the ABAP dispatcher and establish how full the dispatcher queues are *before* requesting a work process. SPI for SAP monitors require a dialog work process to logon to SAP. To enable this integration feature, use the EnableDPQueueCheck keyword in the configuration file for the SPI for SAP monitor, which you want to configure to check the dispatcher status before starting.

For example, if you want the CCMS monitor, `r3monal`, to check the status of the ABAP dispatcher before `r3monal` starts its monitor run, configure the EnableDPQueueCheck keyword in the file `r3monal.cfg`, as illustrated in Checking the ABAP Dispatcher Before Startup on page 79. If `r3monal`'s request for a work process violated a threshold for dialog work processes defined in the `r3mondisp.cfg` configuration file, the `r3monal` monitor would not start its monitor run; it would send a message to the console indicating the reason why it did not start. You should consider using this feature where SAP System performance could be further compromised as a result of a request for an additional dialog work process by a SPI for SAP monitor.

`r3mondisp` is not affected by the thresholds defined for the EnableDPQueueCheck keyword; `r3mondisp` continues to work normally even if other monitors do not start as a result of a lack of available dialog work processes.

Checking the ABAP Dispatcher Before Startup

```
# EnableDPQueueCheck    hostname    SAP    SAP       Enable =1
#                                  System  Number    Disable=0
#
EnableDPQueueCheck      =ALL      =ALL    =ALL       =1
```

For more information about the EnableDPQueueCheck keyword, see Enable DP Queue Check on page 35.

The r3mondisp Configuration File

The `r3mondisp` monitor's configuration file allows you to use the keywords listed in this section to configure `r3mondisp` to meet the requirements of your particular SAP environment. Excerpt from a r3mondisp Configuration File on page 81 shows an excerpt from the `r3mondisp` monitor's default configuration file.

If you configure the SPI for SAP monitors to check the status of the ABAP dispatcher before starting their monitor run, make sure they can see and read a valid `r3mondisp.cfg` configuration file. The monitors require the information stored in this file and will not start if they cannot find it.

You can use the following keywords in the SPI for SAP `r3mondisp` configuration file. For more information about allowed values for the parameters in the following list, see The SPI for SAP Monitor-Configuration File on page 26.

- **TraceLevel**

  Set the trace level for `r3mondisp` when it runs on the specified SAP server. The TraceLevel keyword accepts the following parameters:

  `TraceLevel` =<*hostname*> =<*TraceLevel*>

- **TraceFile**

  Set the name of the trace file, which `r3mondisp` uses to log entries. The TraceFile keyword accepts the following parameters:

  `TraceFile` =<*hostname*> =<*filename*>

- **DPQueueCheck**

  Manages the pro-active monitoring of the ABAP dispatcher. If more than one threshold matches for the same managed node and the same work-process, `r3mondisp` only sends the message with the highest severity. The DPQueueCheck keyword accepts the following parameters:

  ```
  DPQueueCheck =<hostname> =<SID> =<InstanceNr> \ =<disable/enable>\
  =<OVO Msg Group> =<OVO Msg Object>  =<OVO Severity> \
  =<WP-Type>  =<Idle/Queue> =<Percentage idle/full>
  ```

  Since the status of queued work-process is, generally speaking, more important than the status of idle work processes of the same work-process type, we recommend that the severity level assigned to messages concerning queued work processes is higher than the severity level you associate with messages about idle work processes. For example, you can assign the severity level Warning to messages about idle work processes and Critical to messages about queued work processes.

  For more information about required parameters, see The SPI for SAP Monitor-Configuration File on page 26.

- **DisableMonitoringWithSeverity**

  Specify which `r3mondisp` message severity should trigger the disabling of integrated SPI for SAP monitors to prevent the monitors increasing loads unnecessarily by requesting additional dialog work processes from the SAP Systems, whose dispatcher you are monitoring with the SPI for SAP. The DisableMonitoringWithSeverity keyword accepts the following parameters:

  ```
  DisableMonitoringWithSeverity   =<hostname>    =<SID> \
  =<InstanceNr> =<Severity>
  ```

For more information about the required parameters, see The SPI for SAP Monitor-Configuration File on page 26.

The DisableMonitoringWithSeverity keyword must be used in conjunction with keywords DPQueueCheck, which you configure in the `r3mondisp.cfg` file, and EnableDPQueueCheck, which you define in the configuration file of the SPI for SAP monitor you want to integrate with `r3mondisp`. For more information about the keyword EnableDPQueueCheck, see Enable DP Queue Check on page 35.

- **InstanceProfilePath**

  The path to the profile-configuration file for an SAP instance whose dispatcher you want to monitor; the InstanceProfilePath keyword accepts the following parameters:

  ```
  InstanceProfilePath =<hostname> =<SID> =<InstanceNr>  \ =<path>
  ```

  For more information about the required parameters, see The SPI for SAP Monitor-Configuration File on page 26.

Excerpt from a r3mondisp Configuration File on page 81 shows how to configure `r3mondisp` to send a warning message to the console if less than 15 percent of the total allocated dialog work processes for all SAP clients in all the SAP instances monitored by the SPI for SAP are idle.

Excerpt from a r3mondisp Configuration File

```
TraceLevel    =ALL    =0
TraceFile    =ALL    =default

InstanceProfilePath    =ALL    =ALL    =ALL    =default

DisableMonitoringWithSeverity  =ALL  =ALL  =ALL  =Warning

DPQueueCheck    =ALL    =ALL    =ALL    =1
=R3_Dispatch    =dialog    =Warning \
=DIA    =Idle    =15
```

Excerpt from a r3mondisp Configuration File on page 81 also shows how to use the keyword DisableMonitoringWithSeverity to configure `r3mondisp` to prevent SPI for SAP monitors from starting if the start up requires a dialog work process (for example, to logon to SAP) and the allocation of that work process would violate a threshold for idle dialog work processes defined in the configuration file and, as a result, generate a message with the severity “warning” or higher.

Note that you have to use the EnableDPQueueCheck keyword to configure each individual SPI for SAP monitor that logs on to SAP to check the dialog work-process queue before starting its run. For more information about the keyword EnableDPQueueCheck, see Enable DP Queue Check on page 35.

The J2EE (Web AS Java) Monitor

Monitoring the SAP J2EE Engine is essential if you want to manage your SAP environment effectively, since the combination of Java technology and the J2EE infrastructure is the base on which new SAP components such as the SAP Enterprise Portal or Exchange Infrastructure (XI) are built.

This section contains information about the following topics:

J2EE Monitor: Enabling CCMS Alerts

To enable the SPI for SAP to monitor the J2EE engine, you configure `r3monal`, the CCMS alert monitor, to monitor alerts in SAP generated by the J2EE and XI monitors. Monitoring Alerts from CCMS Monitor Sets on page 82 shows how to use the CCMSMonitorSet keyword in the `r3monal.cfg` configuration file to define which CCMS alerts to monitor and use to send messages to HPOM for Windows.

Monitoring Alerts from CCMS Monitor Sets

```
#-------------------------------------------------------------
# Monitor Set  SAP     SAP    Monitor Set    Monitor
#              System  Number
CCMSMonitorSet =ALL    =ALL   =HP OV SAP-SPI =J2EE Monitoring
CCMSMonitorSet =ALL    =ALL   =HP OV SAP-SPI =XI Monitoring
#-------------------------------------------------------------
```

Note that both the CCMS monitors (J2EE Monitoring/XI Monitoring) and the CCMS monitor set (HP OV SAP-SPI) shown in Monitoring Alerts from CCMS Monitor Sets on page 82 are automatically created when you apply the SPI for SAP transports to SAP. For more information about the contents of the SPI for SAP transports, see the transport README file, which you can find in the following location on the HPOM for Windows management server after the installation of the SPI for SAP bits:

`%OvShareDir%\Packages\SAPTransports\readme`

By default, the SPI for SAP monitor for Web AS Java allows you to monitor alerts from the following areas:

- **J2EE Kernel**

  Information about the registered managers such as the Connections Manipulator, the Locking Manager, or the Application Threads Pool. These managers provide the core functionality of the SAP J2EE Engine; it is essential to know if one of these managers is not working correctly since any malfunction could prevent the J2EE Services from working properly.

- **J2EE Services**

  Information about J2EE services such as the Connector Service, Transaction Service, or Web Service, which form the second level of the SAP System after the SAP Java Runtime Environment. The SPI for SAP's CCMS alert-monitor tree gives you an overview of the health of important services in the J2EE Engine.

- **SAPCCMSR Availability**

  Information about the availability of all registered and installed SAP CCMS agents within the SAP NetWeaver environments you are monitoring with the SPI for SAP.

- **GRMG Monitoring**

  Information about the availability of the different Web AS Java instances configured in an SAP NetWeaver environment. Using heartbeat monitoring, you can monitor the status and accessibility of the SAP J2EE Engines within your SAP NetWeaver environment

including the Web components such as: the EJB container (for Enterprise JavaBeans), the Java Connector (JCo), P4 services for managing communication between remote Java objects, the Java Servlet engine, and HTTP services.

Note that SAP's internal GRMG monitor does not enable monitoring of the SAP J2EE Engine by default. If you want to use the GRMG monitor, you will need to enable the CCMS monitors (such as heartbeat polling or Web Dynpro) so that CCMS alerts are generated, which the SPI for SAP CCMS alert monitor can use to send messages to the console.

- **J2EE System**

  Information about the J2EE system is now included as a separate CCMS-monitor node which collects information for both the dispatcher and the server. The SPI for SAP's CCMS alert-monitor tree gives you an overview of the health of important services in the J2EE Engine.

J2EE Monitor: Configuration Pre-requisites

If you want to use the SPI for SAP's J2EE monitor to manage the SAP J2EE environment, make sure that your environment meets the following pre-requisites:

- **J2EE**

  Install, register with the `-j2ee` option, and start the CCMS agent for J2EE on *each* J2EE 6.40 (or later) engine, which you want to monitor with the SPI for SAP. The SAP CCMS agent must report to an SAP Web AS ABAP version 6.40 (or higher).

  For more information about installing and configuring the CCMS agent, refer to the SAP product documentation, for example: *CCMS Agents: Features, Installation, and Operation*.

- **SPI for SAP Transports**

  The new SPI for SAP transports include the J2EE and security CCMS monitors, which you must apply to each of the SAP 6.40 (or later) Systems, to which the SAP CCMS agent monitoring the J2EE Engine reports.

  For more information about applying the SPI for SAP transports, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.

- **CCMS Agents**

  The CCMS agents ensure that CCMS alerts are reported in ABAP, where the SPI for SAP can intercept them. Make sure that the CCMS agent for J2EE is running on *each* J2EE Engine which you want to monitor with the SPI for SAP. This is especially important if multiple instances of the J2EE Engine are running in a stack.

- **SPI for SAP Monitors**

  The SPI for SAP monitors and their configuration files must be available for deployment to the SAP Systems, whose J2EE Engines you want to monitor.

Configuring the SPI for SAP J2EE Monitor

This section explains how to configure the SPI for SAP to monitor the J2EE engine. To configure the SPI for SAP to monitor the SAP J2EE engine:

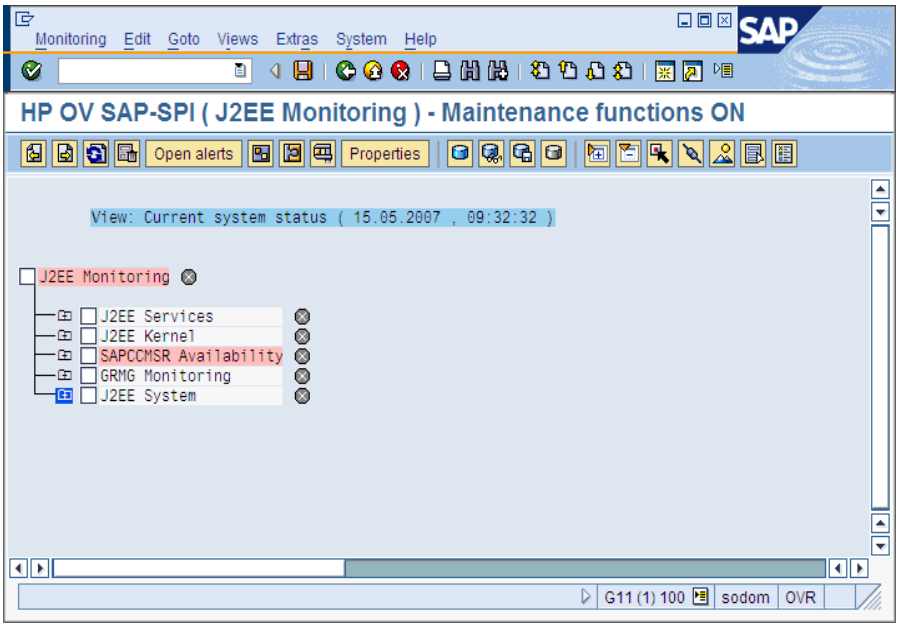
1. Make sure that the CCMS agent for J2EE is running on *each* J2EE Engine which you want to monitor with the SPI for SAP. This is especially important if multiple instances of the J2EE Engine are running in a stack.

2 Apply the new SPI for SAP transports to the SAP System hosting the J2EE Engines you want to monitor; the new SPI for SAP transports include the J2EE and security monitors.

3 Edit the monitor-set section of the `r3monal.cfg` configuration file and enable the monitoring of the J2EE monitor sets, by removing the leading hash (#) from the appropriate lines, as illustrated in Monitoring Alerts from CCMS Monitor Sets on page 82.

4 Enable the CCMS alerts for J2EE, which you want to monitor with `r3monal`. You enable CCMS alerts by checking the CCMS monitors in the CCMS monitor sets for J2EE, as illustrated in Monitoring Alerts from the J2EE Engine on page 84. For more information about which CCMS alerts you need to enable for J2EE, see J2EE Monitor: Enabling CCMS Alerts on page 82.

Figure 6 Monitoring Alerts from the J2EE Engine



The Enqueue-Server Monitor

The combination of a stand-alone enqueue server and replication server running on separate hosts forms the basis of a high-availability enqueue solution for SAP WebAS; separating essential services avoids the necessity of replicating the entire central instance in a high-availability environment and makes the SAP System faster and more efficient. In a high-availability environment, the failover of a stand-alone enqueue server does not lose any lock data or require you to reset locks when the enqueue server restarts.

If your System runs a stand-alone enqueue server, you can use the SPI for SAP's CCMS-alert monitor, `r3monal`, to monitor CCMS alerts relating to the status of the stand-alone enqueue server and configure `r3monal` to send messages to the HPOM for Windows console when problems occur that require urgent attention. This section contains information about the following topics:

- Enqueue Server: Enabling CCMS Alerts on page 85
- Enqueue Server: Configuration Pre-requisites on page 85
- Enqueue Server: Configuring the Enqueue-Server Monitor on page 86

Enqueue Server: Enabling CCMS Alerts

To enable the SPI for SAP to monitor a stand-alone enqueue server, you configure `r3monal`, the SPI for SAP's CCMS alert monitor, to monitor alerts in SAP generated by the CCMS monitor Standalone Enqueue Server Monitoring. Monitoring Enqueue Alerts in CCMS on page 85 shows how to use the CCMSMonitorSet keyword in the `r3monal.cfg` configuration file to define which CCMS alerts to monitor and use to send messages to HPOM for Windows.

Monitoring Enqueue Alerts in CCMS

```
#-------------------------------------------------------------------------
--
# Monitor Set  SAP    SAP  Monitor Set    Monitor
#              Sys.   Num.
CCMSMonitorSet =SP6   =00  =HP OV SAP-SPI =Standalone Enqueue Server
Monitoring
#-------------------------------------------------------------------------
--
```

By default, the SPI for SAP monitor for stand-alone enqueue servers allows you to monitor alerts from the following areas:

- **Enqueue-Server Status**

  Information about the status and availability of the current enqueue server, for example; whether the enqueue server is available or running, whether a connection to a replication server exists, and whether replication is active, on hold, or disabled, and so on.

- **Enqueue Replication-Server (ERS) Status**

  Information about the status and availability of the current enqueue-replication server, for example: whether the server is enabled, has acquired the replication table, is connected to the enqueue server, and so on.

Enqueue Server: Configuration Pre-requisites

If you want to use the SPI for SAP to monitor a stand-alone enqueue server running in a high-availability cluster, make sure that your environment meets the following pre-requisites:

- **SPI for SAP Transports**

  The new SPI for SAP transports include the enqueue-server CCMS monitor, which you must apply to each of the SAP Systems, to which the SAP CCMS agents report.

  For more information about applying the SPI for SAP transports, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.

- **CCMS Agents**

  The CCMS agents ensure that CCMS alerts are reported in ABAP, where the SPI for SAP can intercept them. Make sure that the CCMS agents are available on *all* the physical hosts in the high-availability cluster, where the stand-alone enqueue server that you want to monitor runs, that is: on both primary and backup nodes.

- **SPI for SAP Monitors**

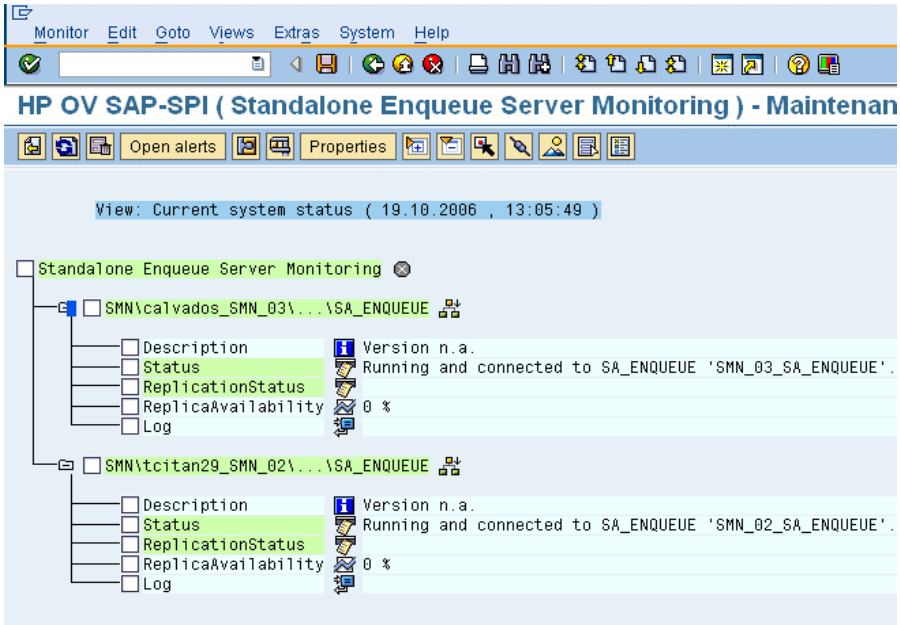
  The SPI for SAP monitors and their configuration files must be available for deployment to the SAP Systems, whose stand-alone enqueue server you want to monitor.

Enqueue Server: Configuring the Enqueue-Server Monitor

This section explains how to configure the SPI for SAP to monitor CCMS alerts generated by a stand-alone enqueue server, which is running in a WebAS high-availability environment. To configure the SPI for SAP to monitor the stand-alone enqueue server, perform the following steps:

1. Make sure that the CCMS agents are running on *each* physical host system in the high-availability environment on which the stand-alone enqueue server runs and which you want to monitor with the SPI for SAP.
2. Edit the monitor-set section of the `r3monal.cfg` configuration file and enable the monitoring of the stand-alone enqueue-server monitor sets, for example: Standalone Enqueue Server Monitoring as illustrated in Monitoring Enqueue Alerts in CCMS on page 85.
3. Enable the CCMS alerts for the stand-alone enqueue server, which you want to monitor with `r3monal`. You enable CCMS alerts by checking the CCMS monitors in the CCMS monitor sets for the Enqueue service, as illustrated in Figure 7 on page 86.

Figure 7 Enabling CCMS alerts for the Enqueue Server Instance



The SAP Enterprise-Portal Monitor

The SAP Enterprise Portal provides a secure and stable web interface that gives users global access to the information, applications, and services that they need to work effectively in the SAP landscape. The SPI for SAP allows you to monitor critical aspects of the Enterprise Portal such as availability, response times, configuration, and performance.

If your SAP System provides users with an Enterprise Portal, you can configure the SPI for SAP's CCMS-alert monitor, `r3monal`, to monitor CCMS alerts relating to the portal's status and send messages to the HPOM for Windows console when problems occur that require urgent attention. You can also use the SPI for SAP to collect and correlate performance and availability data and display the correlated data in service reports for more convenient viewing. This section contains information about the following topics:

Enterprise Portal: Enabling CCMS Alerts

To enable the SPI for SAP to monitor an instance of the Enterprise Portal, you configure `r3monal`, the SPI for SAP's CCMS alert monitor, to monitor alerts in SAP generated by the CCMS monitors J2EE Monitoring. Monitoring Enterprise-Portal Alerts in CCMS on page 87 shows how to use the CCMSMonitorSet keyword in the `r3monal.cfg` configuration file to define which CCMS alerts to monitor and use to send messages to HPOM for Windows.

Monitoring Enterprise-Portal Alerts in CCMS

```
#------------------------------------------------------------
# Monitor Set  SAP    SAP   Monitor Set     Monitor
#              Sys.   Num.
CCMSMonitorSet =ALL   =ALL  =HP OV SAP-SPI  =J2EE Monitoring
#------------------------------------------------------------
```

By default, the SPI for SAP monitor for the Enterprise Portal allows you to monitor alerts from the following areas:

- **Enterprise-Portal Status**

  You can monitor information concerning the status and availability of the Java- or HTTP-based components of the Enterprise Portal. Java-based components include: the EJB container (for Enterprise JavaBeans), the Java Connector (JCo), P4 services for managing communication between remote Java objects, the Java Servlet engine, and Java Web services; HTTP-based components include all HTTP services.

- **Enterprise-Portal Performance**

  You can monitor information concerning the performance of the Enterprise Portal, for example: request response times, request demand over time, the number of component calls per request, the average amount of outbound data per request, and so on.

- **Enterprise-Portal Configuration**

  You can monitor the information that is available concerning configuration parameters for Enterprise Portal components such as the portal runtime (PRT) and the portal content directory (PCD), for example: thread and connection pool size, security settings, cache length and validity times.

Enterprise Portal: Configuration Pre-requisites

If you want to use the SPI for SAP to monitor an instance of the Enterprise Portal, make sure that your environment meets the following pre-requisites:

- **SPI for SAP Transports**

  The new SPI for SAP transports include the Enterprise-Portal monitor; you must apply the new transports included in the transport file `SAPSPI_CCMS_Monitors.car` to each of the SAP Systems, to which the SAP CCMS agents report.

  For more information about applying the SPI for SAP transports, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.

- **CCMS Agents**

  The CCMS agents ensure that CCMS alerts are reported in ABAP, where the SPI for SAP can intercept them. Make sure that the CCMS agents are available on the machine hosting the instance of the J2EE engine on which the Enterprise Portal that you want to monitor is running. Note that, if the TREX component (for search and classification functionality) is running on a different system, you will have to make sure the CCMS agents are running there, too.

- **Java-Application Response-Time Measurement**

  To collect performance-related data from J2EE applications and components, you must enable Java-application response-time measurement (JARM) functionality. Note that JARM is enabled by default and maps all collected data to CCMS automatically; the J2EE engine's Visual Administrator displays the JARM status.

- **Generic Request and Message Generator (GRMG)**

  To monitor the availability of the Enterprise Portal in SAP, you need to customize the GRMG configuration files and upload the modified configuration files to the CCMS agent; the J2EE engine's Visual Administrator displays example XML files that are available for modification and upload to CCMS, as illustrated in Figure 19 on page 197. You can also use the transaction GRMG to display a list of active GRMG configuration scenarios that are available in the SAP central monitoring system.

  ➤ If you want to monitor system availability with the GRMG, you must assign and configure one SAP system as the central monitoring system (CEN) in your SAP landscape. For more information about setting up a CEN in SAP, see the SAP documentation; for more information about using the SPI for SAP to monitor the CEN, see Monitoring CCMS Alerts in the CEN on page 193.

- **Performance Agents**

  Either the HP Software Embedded Performance Component or the HP Performance Agent and, in addition, the SAP/Performance subagent must be running on the system hosting the Enterprise Portal you want to monitor. For more information about the SPI for SAP's performance monitor for the SAP Enterprise-Portal, see EP_PERF on page 225. Note that the SPI for SAP uses the performance data collected by EP_PERF to generate service reports.

- **SPI for SAP Monitors**

  The SPI for SAP monitors and their configuration files must be available for deployment to the SAP Systems, whose Enterprise Portal you want to monitor.

Enterprise Portal: Configuring the Portal Monitor

The information in this section explains how to configure the SPI for SAP to monitor CCMS alerts generated by the Enterprise Portal. To configure the SPI for SAP to monitor an instance of the Enterprise Portal:

1 Make sure that the CCMS agents are running on the system hosting the Enterprise Portal services that you want to monitor with the SPI for SAP.

  ➤ If you configure the TREX server to run on a separate host, you will need to make sure that CCMS agents are also running on the system hosting the remote TREX server and that CCMS alerts relating to search-and-classification functionality appear in ABAP.

2 If you have not already done so as part of the installation of the SPI for SAP, import the transport from `SAPSPI_CCMS_Monitors.car` file on each of the SAP Systems hosting the J2EE engine underlying the Enterprise Portal you want to monitor with the SPI for SAP; the `SAPSPI_CCMS_Monitors.car` transport file contains the CCMS monitors and objects that the SPI for SAP requires for EP performance monitoring. For more information about importing SPI for SAP transports, see the *HP Operations Smart Plug-in for SAP Configuration Guide*.

3 Enable the Java Application Response-Time Measurement (JARM) functionality for the Java stack on which the Enterprise Portal is running; JARM allows you to monitor the availability and performance of the Java components underlying the Enterprise Portal. Use the J2EE Engine Visual Administrator to check the JARM status. JARM is enabled by default.

   The jarm/switch property key enables or disables performance monitoring; the jarm/comp/ level property key allows you to modify the java-component monitor level, for example: 0 (default), 1, 2, or 3.

4 To monitor the availability of the web components in the J2EE engine underlying the Enterprise Portal, you need to customize an instance of the GRMG configuration files and upload the modified XML files to the CCMS agent. In particular, you need to define the names of the hosts where the instances of the j2EE engines are running. For more information about using the SAP Visual Administrator to modify GRMG-configuration files and upload them to SAP's central monitoring system (CEN), see the SAP documentation.

   Use the transaction GRMG to display a list of active GRMG configuration scenarios that are already uploaded to (and active in) CCMS.

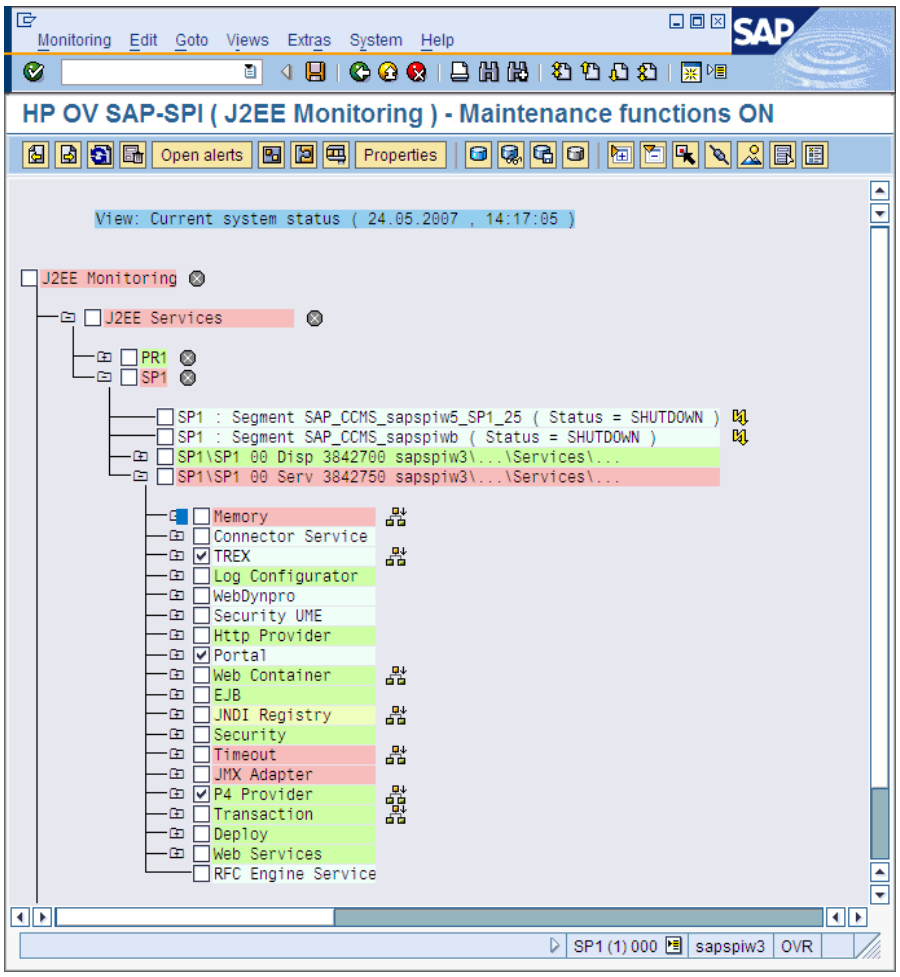
   ➤ It can take up to an hour for the GRMG scenarios that you upload in the Visual Administrator to be transferred to the central monitoring system and started.

5 Edit the monitor-set section of the `r3monal.cfg` configuration file and enable the monitoring of both the J2EE monitor set, for example: J2EE Monitoring, as illustrated in Monitoring Enterprise-Portal Alerts in CCMS on page 87.

6 Enable the CCMS alerts for the Enterprise Portal that you want to monitor with `r3monal`. You enable CCMS alerts by checking the CCMS monitors in the CCMS monitor sets for the Enterprise Portal, as illustrated in Figure 8 on page 90.

   Note that the Java-related CCMS alerts are available in the J2EE Services and J2EE System monitors, which you can find in the J2EE Monitoring CCMS monitor set. For more information about the SPI for SAP's J2EE monitor, see The J2EE (Web AS Java) Monitor on page 81.

Figure 8 Enabling CCMS alerts for the Enterprise-Portal Instance



The SAP Security-Audit Monitor

Monitoring security audits is essential if you want to manage your SAP environment effectively; you can use the security-audit monitor to check what security-related changes occur in the SAP Systems you are monitoring with the SPI for SAP, who or what is responsible for the change, and where and when the change occurred. The security-audit monitor checks for alerts concerning the following events in the SAP System:

- Logons
- RFC Logons
- Transaction Starts
- Report Starts
- RFC Calls
- User Master Records
- System
- Miscellaneous

This section explains how to set up SAP's self-monitoring feature and configure the SPI for SAP to monitor the alerts the self-monitoring feature generates. The information in this section helps you understand the following topics:

- SAP Security-Alerts on page 91
- Configuring the Security-Audit Monitor on page 91

SAP Security-Alerts

The SAP security-audit log keeps a record of security-related activities in the SAP System and stores the information it collects in an audit file on each application server. The audit log uses filters to determine what information is important enough to record and updates the log at regular intervals. When an event occurs that matches a configured filter (for example, for an RFC logon or a transaction start), the audit log generates a message and writes it to the audit file. At the same time, a corresponding alert appears in the CCMS alert monitor.

You can configure the SPI for SAP to monitor the CCMS alerts logged by the security audit in any areas of particular interest to you and use the alerts to generate messages, which you can send to the HPOM for Windows console. Table 17 on page 91 shows the security areas audited by the SAP self-monitoring feature; you can monitor all or any of these areas with the SPI for SAP.

Table 17 SAP Security-Audit Classes

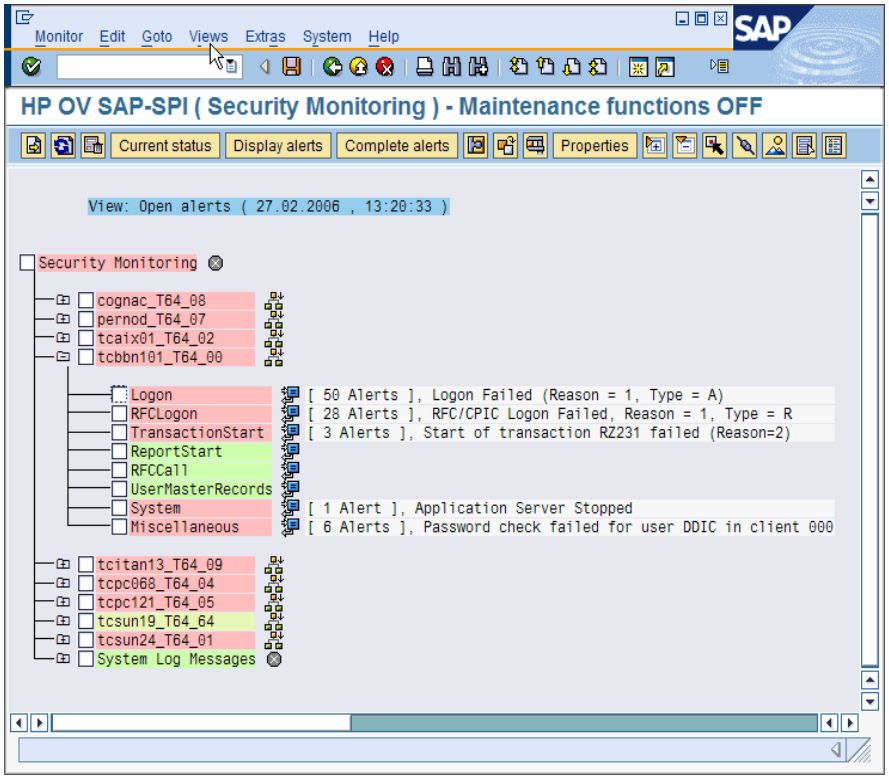
Audit Class	Description
Logons	An SAP logon or password check failed; an operator illegally locked or unlocked an SAP user.
RFC Logons	An RFC or CPIC logon failed due to user error or an unauthorized attempt to log on with an illegal user/password combination.
Transaction Starts	Possible unauthorized execution of code in the SAP System
Report Starts	
RFC Calls	
User Master Records	A security or licensing issue occurred concerning user records or the inappropriate activation of an authorization or profile.
System	An application server stopped or started; the security-audit configuration changed.
Miscellaneous	A transport request contains source objects, which are critical for security.

Configuring the Security-Audit Monitor

Enabling the monitoring of security events audited by SAP's security-audit feature involves a number of steps both in SAP and in HPOM for Windows; the number and complexity of the steps you have to perform depends on the version of SAP installed on the SAP System, whose

security events you want to monitor with the SPI for SAP. Figure 9 on page 92 shows what the CCMS monitor tree looks like when you complete the configuration on the SAP side successfully.

Figure 9 CCMS Monitor Set: Monitoring Security Events



To configure the SPI for SAP to monitor the security events logged in the SAP security audit, perform the tasks described in more detail in the following topics:

1 Installing the SPI for SAP's Security-Monitoring Feature on page 92

2 Configuring the SAP Security Audit on page 93

3 Enabling CCMS Security Monitoring on page 93

Installing the SPI for SAP's Security-Monitoring Feature

The number and complexity of the steps you have to perform to enable the security-monitoring feature in SAP depends on the version of SAP installed on the SAP System you want to monitor with the SPI for SAP.

- For SAP Web AS ABAP version 6.40 and higher, apply the SPI for SAP transport, `SAPSPI_CCMS_Monitors.car`, which imports the new, CCMS monitor set automatically into SAP.
- For all supported SAP ABAP versions before 6.40:
  - Use transaction **`RZ20`** to activate the SAP maintenance function.
  - Create a new CCMS monitor set called 'HP OV SAP-SPI'.
  - Create a new CCMS monitor called 'Security Monitoring' and add it to the monitor set HP OV SAP-SPI.

— Enable the alert classes you want to monitor with the new CCMS monitor 'Security-Monitoring'. You can enable the complete tree or individual classes, for example: Logon, or Transaction Start.

For more information about the individual security-audit alert classes you can choose to monitor, see SAP Security-Alerts on page 91.

Configuring the SAP Security Audit

The information in this section explains how to specify which events the new security-audit profile monitors, in which SAP client, and relating to which SAP user.

Before enabling the security-audit feature in SAP, review SAP OSS note 429343, which addresses SAP performance issues associated with the activation of the security-audit feature.

1 Use transaction **SM19** to create, customize, and activate a new profile for a security-audit.

To reduce administrative overhead, you can set up a system-wide profile which will monitor only the most important and critical security events, for example: critical SAP-logon events or important RFC-function calls.

Remember to check the Filter active option when configuring filter options.

2 Test the new profile for a security-audit.

You can test the activated profile by logging on to SAP with a false user/password combination. If you want to review the audit log, too, use transaction **SM20**.

3 Set up the SAP job REORG to maintain the security-audit logs:

The security audit writes logs to the file system which very quickly fills up if you do not implement a REORG job using the SAP report RSAUPURG. Transaction **SM38** allows you to create a variant of the RSAUPURG report, which meets the needs of your environment. For example, you can arranged to delete logs which are more than ten days old.

Enabling CCMS Security Monitoring

The information in this section explains how to enable `r3monal` to monitor the generation of CCMS alerts in SAP and in particular the alerts, which concern security-related events. After configuring `r3monal` to monitor security-related CCMS alerts, you also have to enable the SAP Security Monitoring monitor in CCMS and, in addition, the corresponding MTE's (monitor tree elements) of interest, for example: Logon, ReportStart, and so on.

The SPI for SAP creates the CCMS monitor "Security Monitoring" when you apply the SPI for SAP transport `SAPSPI_CCMS_Monitors.car` to SAP 6.40 Systems and higher, whose security events you want to monitor with the SPI for SAP. For older SAP versions, you have to create the CCMS monitors and monitor sets manually.

Monitoring Audit Alerts from CCMS Monitor Sets on page 93 shows an excerpt from the `r3monal` monitor's configuration file. The CCMSMonitorSets keyword allows you to define the CCMS alert monitor set and CCMS alert monitors created by the SPI for SAP. In the example shown, you configure `r3monal` to monitor security-audit alerts for all SAP Systems known to the SPI for SAP using the CCMS alert monitor set "HP OV SAP-SPI" and the CCMS alert monitor "Security Monitoring".

Monitoring Audit Alerts from CCMS Monitor Sets

```
#-------------------------------------------------------------
# Monitor Set  SAP     SAP    Monitor Set     Monitor
#              System  Number
CCMSMonitorSet =ALL    =ALL   =HP OV SAP-SPI  =Security \
                                               Monitoring
#-------------------------------------------------------------
```

For more information about enabling CCMS alerts, see r3monal: CCMS Monitor Sets on page 49.

4 The SPI for SAP Alert-Collector Monitors

This section describes the alert-collector monitors controlled by `r3moncol` and explains how to configure and use them.

Introducing r3moncol and the Alert-Collector MONITORS

The SPI for SAP uses the one, single alert collector `r3moncol` to collect alerts from a number of additional SAP NetWeaver alert monitors. Each of the alert monitors listed in this section takes its name from the nature of the alerts it monitors. For example, the `r3mondmp` alert-collector monitors ABAP dumps. The SPI for SAP groups the tasks that each monitor performs according to *alert types*. For example, the alert type IDOC_CURRENT_STATUS helps the `r3monale` monitor determine the current status of iDOCs in an SAP System.

You specify monitoring parameters at the alert-*type* (rather than alert-*monitor*) level. For example, you could use the parameter =CHECK_INBOUND to limit the range of the alert type IDOC_CURRENT_STATUS so that it checks the status of inbound iDOCs only.

This section contains information about the following topics:

- Configuring the SPI for SAP Alert-Collector Monitors on page 97
- The Alert-Collector Monitor Configuration Files on page 105

The following list shows which alert-collectors are available to `r3moncol` and gives a short description of each monitor's scope. For more detailed information about the alert types associated with each alert monitor as well as the parameters you can use to configure them, see the appropriate sections and tables later in this chapter:

- `r3monaco` - Monitoring the TemSe file on page 177

  To save runtime costs, a report now replaces the Temporary Sequential File (TEMSE) monitor. See Monitoring the TemSe file on page 177 for more details.

- r3monale: The iDOC-Status Monitor on page 113

  The iDOC Status monitor checks the status of the iDOCs present in the SAP NetWeaver Systems configured in your SAP Landscape. `r3monale` generates an alert when a defined threshold for the number of iDOCs with a given status is exceeded

- r3monchg: The System-Change-Option Monitor on page 120

  The SYSTEM CHANGE OPTION monitor checks for the occurrence of SAP System change options.

- r3moncts: The Correction & Transport System Monitor on page 125

  The CORRECTION and TRANSPORT SYSTEM monitor checks the correction and transport system for important transport requests, tasks and objects. It generates an alert according to the specifications you define.

- r3mondmp: The ABAP-Dump Monitor on page 134

The ABAP Dump monitor detects ABAP dumps which occur in the SAP System. The cause of the dump can be identified from the details which the message gives and used to determine any corrective action, which you need to take.

- r3monjob: The Job-Report Monitor on page 136

  The JOBREPORT monitor checks for jobs that:

  — exceed a specified run time

  — do not run as long as they are expected to run

  — do not start within a specified time frame

  — are aborted

- r3monlck: The Lock-Check Monitor on page 144

  The LOCK_CHECK monitor references the SAP NetWeaver Enqueue process which manages logical locks for SAP NetWeaver transactions and reports on obsolete locks. An obsolete lock is a lock which is older than the time period you specify.

- r3monoms: The Operation-Mode Monitor on page 147

  The OPERATION MODE monitor detects when:

  — a scheduled operation mode switch has occurred later than the time specified

  — a scheduled operation mode switch has not occurred at all

Changes in SAP mean there are no operation-mode-switch errors to monitor in WebAS 7.0/ Netweaver04s (kernel 7) environments.

- r3monrfc: The RFC-Destination Monitor on page 150

  The SAP-RFC monitor checks RFC destinations in an SAP environment:

  — the status of connections

  — the availability of connections

- r3monspl: The Spooler Monitor on page 152

  The SPOOLER monitor checks:

  — the number of spool entries

  — the number of erroneous spool requests in a specified range

  — spool entries with state ERROR for specified printers

- r3montra: The Transport Monitor on page 156

  The TRANSPORT monitor checks the following parts of the transport system:

  — the status of exports and imports

  — confirmed and unconfirmed repairs

  — performs a ping of the specified system

  — checks the TP interface

- r3monupd: The Update Monitor on page 163

  The UPDATE-alert monitor checks:

  — if an SAP user or the SAP System stops an update

— if update errors have occurred

- r3monusr: The SAP-User Monitor on page 165

  The USER monitor specifies the number of users which would trigger an alert, using SAP transaction `SM04` as reference

- r3monwpa: The Work-Process Monitor on page 168

  The WORKPROCESS monitor performs the following checks on work processes:

  — monitors their status and reports any processes that are running in *debug*, *private* or *no-restart* modes

  — compares the number of configured work processes with the number of work process actually running

  — checks the number of expected work processes waiting and the number of expected work processes running *for each work process type*

Configuring the SPI for SAP Alert-Collector Monitors

You can use the alert-collector monitors to define a series of monitoring tasks within SAP NetWeaver, for example; checks on SAP NetWeaver processing modes, SAP NetWeaver dumps, or the availability of SAP NetWeaver work processes. The alert-collector monitors ensure that each defined alert-collector configuration is executed on a regular basis and reports any messages that come back from the called function. For more information about the contents of the individual alert-collector monitor configuration files, see The Alert-Collector Monitor Configuration Files on page 105.

Report Types for the Alert-Collector Monitors

Each of the alert monitors uses one of two reporting types.

- **Time Frame**

  Time-frame monitors use a defined time range as their measurement base. For example, the `r3monjob` alert monitor uses a time frame which compares the time from the last monitor run with the configured start date and time of a batch job.

- **Snapshot**

  Snapshot monitors use one moment of time as their measurement base. For example, the `r3monlck` (LOCK_CHECK) monitor uses the moment the monitor runs to generate an alert indicating that a lock is “old”, whenever the age of the lock exceeds a defined time span. The snapshot type is dynamic and can run continuously because the alerts can be generated without being confined to a specific time frame.

Polling Rates for the Alert-Collector Monitors

The alert-collector monitors have different default polling rates, that is: the frequency at which the monitor runs. You can change the polling rate at the scheduled-task policy for the monitor. For more information about the default polling rates for alert-collector monitors, see Table 18, which shows the rates in days, hours, and minutes.

Table 18 Default Polling Rates for Alert-Collector Monitors

	Polling Rate		
Alert-Monitor Name	**Days**	**Hours**	**Mins**
r3monale			10
r3monchg		4	
r3moncts		1	
r3mondmp			5
r3monjob			5
r3monlck		1	
r3monoms			10
r3monrfc			5
r3monspl			30
r3montra	1		
r3monupd		1	
r3monusr			5
r3monwpa			5
`r3monaco` [a]			15

a. Strictly speaking, `r3monaco` is not an alert-collector monitor. See Monitoring the TemSe file on page 177.

Alert-Collector Monitor History

Unlike the SPI for SAP monitors `r3monal` or `r3mondev`, the alert-collector monitors controlled by `r3moncol` (such as `r3monale` or `r3mondmp`) do *not* write history information to a monitor-specific history file. Instead, any information relating to SAP alerts which come to the notice of the SPI for SAP alert-collector monitors is written directly to the SAP database, where it can be found by the alert collector `r3moncol`. At the start of each monitor run, `r3moncol` reads the relevant tables and uses the information to determine which if any events the HPOM for Windows management server has already been notified about and whether to generate further messages or not.

Alert-Collector Monitor Query Conditions

The data for each alert monitor is split into a number of alert types. For example, the JOBREPORT Monitor has four alert types: JOB_MAX_RUN-TIME, JOB_MIN_RUN_TIME, START_PASSED and JOB_ABORTED. For each of a given alert monitor's defined alert types you have to:

- specify which SAP NetWeaver Systems should be checked
- enter selection criteria which defines under what circumstances an alert will be raised. This is described in more detail below.

Parameter Data Types

Parameters in the monitoring-conditions section of the configuration files associated with each alert type define the conditions, which generate an alert. There are two general types of parameter data:

- **name**

  The parameter *name* describes the attributes of the SAP NetWeaver System for which you define the monitoring conditions. For example: MAX_RUNTIME and JOBNAME are the names of parameters for the alert type JOB_MAX_RUN_TIME, which is associated with the JOBREPORT Monitor, `r3monjob`.

- **delimiters**

  Parameter *delimiters* are used to specify the "select" options for each parameter. The parameter delimiters define the circumstances under which an alert should be generated. An HPOM for Windows message will be sent for each event that matches your specified conditions. There are four types of Parameter Delimiters, which must appear in the following order: SIGN, OPT(ION), LOW and HIGH. (See Table 19 on page 100)

Specifying Query Conditions

The following points apply generally when using parameter delimiters to specify query conditions:

- All possible and reasonable conditions can be used to configure the query condition, within the limitations given below.
- Messages which are excluded by your defined conditions will not appear in the HPOM for Windows console.
- Detailed descriptions of the alert-type configurations for each monitor follow this introductory section.

The SPI for SAP installs the alert monitors by default with an example configuration of the allowed parameters for each alert type. However, this example configuration should not be treated as necessarily ready to use for your particular environment. As a general rule, you first need to customize the alert type by editing the parameters. You can find information about when it is possible to use these unedited default values (and when editing is mandatory) in the detailed descriptions of each alert monitor's alert types, which follows this introduction. Note that the order of the parameter delimiters for the query conditions must

match the order shown in Table 19, namely; SIGN, OPTION, LOW, HIGH. For examples of the use of query conditions, see the sections for the appropriate alert collectors, for example: `r3moncts`.

Table 19 Description of Parameter Delimiters

Parameter Delimiters	Description
SIGN	**I:** Include **E:** Exclude
OPT	The standard SAP operators NE (Not Equal to), NB (Not Between... and...), and NP (does Not contain Pattern) cannot be used to configure the alert types described in this section. You should only use the following operators: • **EQ**: equal to • **BT**: between... and • **CP:** contains pattern • **LE**: less than or equal to • **GE**: greater than or equal to • **GT**: greater than • **LT**: less than
LOW	• A comparison value such as a string when used with the operator CP • The lower value of a range when used in conjunction with the operator BT. • For some ALERT_TYPES, the value X is also used simply as a flag or switch which enables monitoring, for example: `r3montra`'s TRANS and REPAIR.
HIGH	A numeric comparison value to specify the higher value of a range. This parameter delimiter should only be used in conjunction with the operator BT

Parameter Values

This section describes how the SPI for SAP interprets *include* and *exclude* parameter values for an alert type entry. The SPI for SAP compares values in *different* parameters using 'and'; the SPI for SAP compares values in the *same* parameter as follows.

- **Include**: use 'or' to compare the parameters
- **Exclude**: use 'and' to compare the parameters

Note that the SPI for SAP evaluates *include* values before *exclude* values, as shown in the Table 20.

Table 20 Comparing Include and Exclude Conditions for the Same Parameter

Select Options	Example Configuration of Select Options for JOB_MAX_RUN_TIME	Comparison
1	=JOBNAME =I =CP =ZREP* = =MAX_RUNTIME =I =GT =10 =	OR
2	=JOBNAME =I =CP =SAP* = =MAX_RUNTIME =I =GT =20 =	OR
3	=JOBNAME =E =CP =SAP_ZREP* =	AND

Query Conditions

The following rules apply to the use of blocks and line breaks when configuring the alert types for the alert collector monitors:

- Configure each parameter as a separate block. For example for JOB_MAX_RUN_TIME:

  =JOBNAME =I =CP =SAP* = is the block for the parameter JOBNAME

  =MAX_RUNTIME =I =GT =20 = is the block for the parameter MAX_RUNTIME.
- The symbol '\' indicates a line continuation.
- Use line breaks in the following locations:
  - Within each specified configuration between:
    - the general alert class configuration (SAP hostname, system, number and client)
    - the HPOM for Windows configurations (severity level, object)
    - the monitoring query conditions (parameter name and the SIGN, OPT, LOW and HIGH parameter delimiters).
  - Between each separate specified condition for AND comparisons.

Alert-Collector Monitor Environment Variables

This section describes the environment variables for all the alert- collector monitors managed by `r3moncol`. The configuration is identical for all alert collectors except that the name of the alert-collector configuration file is monitor specific, for example: `r3monjob`, `r3mondmp`, `r3monlck`, `r3monoms`.

Table 21 Environment Variables for r3moncol.exe

Environment Variable	Description
SAPOPC_TRACEMODE	Trace mode: a = append w = create (default)
SAPOPC_ <*R3MONNAME*>_CONFIGFILE	Configuration-file name [a]
SAPOPC_R3ITOSAP_CONFIGFILE	General SAP NetWeaver login configuration file
SAPOPC_TRACEPATH	Trace path config. file

a. Where <*R3MONNAME*> is the name of the monitor whose configuration file location you want to change. For example; SAPOPC_*R3MONDMP*_CONFIGFILE

Alert-Collector Monitor Command-Line Parameters

The command line parameters for all the alert-collector monitors controlled by the `r3moncol` are described in this section. In the same way as for the environment variables, the configuration is identical for all alert-collector monitors except that the name of the alert-collector configuration file is monitor specific, for example: `r3monjob.cfg`, `r3mondmp.cfg`, `r3monlck.cfg`, `r3monoms.cfg`.

Table 22 r3moncol Command-Line Parameters

Parameter	Description [a]
`-cfgfile`	Name of the monitor's configuration file. For example; `-cfgfile` <*R3MONNAME*>`.cfg`
`-trace`	The monitor writes an initial trace file `writetrace.log`, which contains information about the configuration file `r3itosap` and the monitor-specific config file `<R3MONNAME>.cfg`.

a. Where <*R3MONNAME*> is the name of the monitor whose configuration-file location you want to read. For example; `r3mondmp`

In the following example, the alert-collector monitor writes an initial trace file `writetrace.log`, which contains information about the general configuration file `r3itosap` and the monitor-specific configuration file `r3monjob.cfg`.

```
r3moncol -cfgfile r3monjob.cfg -trace
```

Remote Monitoring with the Alert-Collector Monitors

The current version of the SPI for SAP includes a feature which allows you to extend the scope of the alert-collector monitor to remotely monitor the health of SAP processes on additional SAP servers (which are *not* HPOM for Windows managed nodes) from an SAP server, which *is* already configured as an HPOM for Windows managed node.

Although the SAP Server defined in the RemoteHost parameter is not an HPOM for Windows managed node, it must still be present in the HPOM for Windows node list. If you do not add the SAP Server defined in RemoteHost to the HPOM for Windows Node list, HPOM for Windows cannot resolve the host name associated with the remote host and, as a consequence, cannot display any messages from the remote host in the HPOM for Windows console.

In addition, the SAP Server defined in RemoteHost must appear in the `r3itosap.cfg` file to ensure that the SPI for SAP can login to the SAP instances it is monitoring on the RemoteHost. For more information about the `r3itosap.cfg` file, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.

To make use of the remote-monitoring feature provided by the SPI for SAP, for example; to monitor an SAP System running an operating system that is not supported by the SPI for SAP, you need to enable the new **RemoteMonitoring** keyword (by removing the leading hash symbol "#") in the `r3mon<alert_monitor_name>.cfg` file (for example; `r3mondmp.cfg`) and then, on the same line, tell the SPI for SAP alert-collector monitor the name of the local server which you want to perform the monitoring and, finally, the name of the remote server, which you want to monitor. Default Configuration for the CTS Monitor (r3moncts) on page 109 shows how a new line is required for each *additional* SAP server, which you want to monitor remotely. You use the following keyword parameters to define local and remote server names:

- **LocalHost**

  the name of the HPOM for Windows managed node where the SPI for SAP is running and whose alert-collector monitor you want the SPI for SAP to use to do the monitoring on the remote host defined in "RemoteHost"

- **RemoteHost**

  the name of the *remote* system to monitor with the system defined in "LocalHost". The RemoteHost does not have the SPI for SAP installed and is not usually (but could theoretically be) an HPOM for Windows managed node.

For more information about the contents of the alert-collector monitor configuration file, see The Alert-Collector Monitor Configuration Files on page 105.

Specifying Monitoring Rules for Individual Remote Servers shows a hypothetical example of how to configure the SPI for SAP on two different HPOM for Windows managed nodes (`sap1` and `sap2`) to remotely manage three different SAP servers (`ovsdsap1`, `ovsdsap2`, and `ovsdsap3`) and, in addition, specify different monitoring rules to suit the different roles of the individual SAP servers, for example; production, development, or even test/unused:

- **Production System**

  The remote server `ovsdsap1` in Specifying Monitoring Rules for Individual Remote Servers is the *production* system, it has the monitor enabled (=1) and associates the HPOM for Windows message severity CRITICAL with alerts generated by the =REQUEST_CREATED alert type.

- **Development System**

The remote server `ovsdsap2` in Specifying Monitoring Rules for Individual Remote Servers is the *development* system, it has the monitor enabled (=1) and associates the HPOM for Windows message severity MAJOR with alerts generated by the =REQUEST_CREATED alert type.

- **Test System**

  The remote server `ovsdsap3` in Specifying Monitoring Rules for Individual Remote Servers is the test system whose configuration is unchanged from the default which has the monitor disabled (=0) and associates the HPOM for Windows message severity WARNING with alerts generated by the =REQUEST_CREATED alert type.

Specifying Monitoring Rules for Individual Remote Servers

```
#--------------------------------------------------------------------------
# Remote          LocalHost   RemoteHost
# Monitoring
RemoteMonitoring  =sap1       =ovsdsap1
RemoteMonitoring  =sap1       =ovsdsap2
RemoteMonitoring  =sap2       =ovsdsap3
#--------------------------------------------------------------------------
# AlertMonFun  SAP       SAP      SAP      SAP     Alertmonitor   Enable =1/
  \
#              Hostname  System   Number   Client                  Disable=0
\
#
# OpC        OpC     OpC \
# Severity   Object  MsgGroup \
#
AlertMonFun  =ovsdsap1  =ALL  =ALL  =ALL  =CTS  =1\
=CRITICAL =Request     =R3_CTS\
=REQUEST_CREATED   =USERNAME   =I    =CP      =*    =
AlertMonFun  =ovsdsap2  =ALL  =ALL  =ALL  =CTS  =1\
=MAJOR =Request     =R3_CTS\
=REQUEST_CREATED   =USERNAME   =I    =CP      =*    =
AlertMonFun  =ovsdsap3  =ALL  =ALL  =ALL  =CTS  =0\
=WARNING =Request     =R3_CTS\
=REQUEST_CREATED   =USERNAME   =I    =CP      =*    =
--------------------------------------------------------------------------
--
```

The Alert-Collector Monitor Configuration Files

The keywords listed in this section appear in the alert-collector monitors configuration files and can be used to set up the individual monitor to meet the requirements of your particular environment. Where appropriate, possible values for a given keyword are also specified. Default Configuration for the CTS Monitor (r3moncts) on page 109 shows what a complete configuration file looks like for the `r3moncts` monitor, which monitors the correction and transport system for important transport requests, tasks and objects. This section contains information about the following topics:

Alert-Collector Keywords and Parameters

The following list describes the keywords you can use in the configuration files for the SPI for SAP alert-collectors controlled by `r3moncol`; for more information about errors caused by incorrect configuration, see Validating the Alert-Collector Configuration Files on page 110:

- **TraceLevel**

  For more information, see The SPI for SAP Monitor-Configuration File on page 26.

- **TraceFile**

  For more information, see The SPI for SAP Monitor-Configuration File on page 26.

- **HistoryPath[Unix | AIX | Windows]**

  For more information, see The SPI for SAP Monitor-Configuration File on page 26.

- **AgentHostname**

  The AgentHostname keyword is not currently used.

- **RemoteMonitoring**

  Enables the SPI for SAP to monitor an SAP instance installed on remote SAP server. For more information, see Remote Monitoring with the Alert-Collector Monitors on page 103.

- **AlertMonFun**

  The AlertMonFun keyword defines a function for the alert-collector monitor and *requires* a value for the following parameters:

  ```
  AlertMonFun =<SAP Hostname> =<SAP System> =<SAP Number> =<SAP Client>
  =<AlertMonitor> =<Enable/Disable> =<OpC Severity> =<OpC Object> =<OpC
  MsgGroup> =<Alerttype> =<RFC Parameter>
  ```

  — **Alerttype:**

`=<Alerttype>`	The alert type is monitor specific. For example, `r3monale` uses the IDOC_CURRENT_STATUS alert type to monitor alerts relating to the status of iDOCs; `r3mondmp` uses the alert type ABAP4_ERROR_EXIST to monitor alerts relating to each ABAP dump that occurs in a monitored SAP System. For more information about which alert types belong to which alert-collector monitor, see the “Alert-Types” section for a given monitor, for example; r3monale: The iDOC-Status Monitor on page 113 refers to the alert type IDOC_CURRENT_STATUS.

  — **AlertMonitor:**

`=<Monitor_Name>`	The short form of the alert monitor you are configuring, for example; ALE for `r3monale`, CTS for the `r3moncts`, and so on.

  — **Enable/Disable:**

=0	*Disable* the monitor.
=1	*Enable* the monitor. This is the default setting.

  — **OPC Severity:**

`=<HPOM_Msg_Severity>`	The severity level of the HPOM for Windows message you want to map the CCMS alert to, for example: Normal, Warning, Major, Critical.

  — **OPC Object:**

`=<OpC_Object>` — The HPOM for Windows object associated with the generated message. These tend to reflect the names of the alert types associated with the alert-collector monitor, for example; Request, task or object for `r3moncts`. Note that if you change the names of the HPOM for Windows objects in the monitor-configuration files (or add new ones), you must ensure that these changes are reflected in the message conditions to avoid the generation of unmatched messages.

— **OPC MsgGroup:**

`=<OpC_Msg_Group>` — The name of the HPOM for Windows message group to which the generated message belongs, for example: R3_CTS, or R3_ABAP-4. The default names all start with "R3_" and reflect the names of the alert monitors to which they correspond, for example; `r3moncts` or `r3mondmp`. Note that if you change the names of the HPOM for Windows message groups in the monitor-configuration files, remember to ensure that the changes are reflected in the message conditions to avoid the generation of unmatched messages.

— **RFC Parameter:**

`=<RFC_Param> =I =CP =* =`

`=<RFC_Param>` — The name of a parameter for a given alert type, for example: USERNAME, followed by any required parameter-specific query conditions, each with the prefix "=", for example: = I (for include), =CP (for "Contains Pattern").

For more information about query conditions, see Alert-Collector Monitor Query Conditions on page 99. For more information about monitor- specific alert-type parameters, see the monitor descriptions. For example, for the `r3moncts` alert type REQUEST_CREATED, see: REQUEST_CREATED Configuration Parameters on page 128.

— **SAP Client:**

=ALL — Monitor all SAP clients with the SPI for SAP. This is the default setting.

`=<ClientID>` — The ID of a specific SAP client ID whose performance you want to monitor, for example; 099. Use a new configuration line for each entry.

— **SAP Hostname:**

=ALL	Monitor all SAP hosts with the SPI for SAP. This is the default setting.
=<SAP_host>	The host name of a specific SAP server which you want to monitor. Use a new configuration line for each individual entry.

— **SAP Number:**

=ALL	Monitor all SAP instances with the SPI for SAP. This is the default setting.
=<Instance>	The number of a specific SAP *instance* which you want to monitor, for example; 00, 99. Use a new configuration line for each entry.

— **SAP System:**

=ALL	Monitor all SAP Systems with the SPI for SAP. This is the default setting.
=<SAP_SID>	The ID of a SAP System ID which you want to monitor, for example; DEV. Use a new configuration line for each individual entry.

Severity Levels

The alert-collector monitors map the severity of alerts in the SAP subsystem to messages in HPOM. For example, SAP alerts with the severity level *SeverityCritical* are mapped by default to the HPOM for Windows message severity *Critical*. The HPOM for Windows message- status hierarchy is, in ascending order; Normal, Warning, Minor, Major, Critical.

You can customize these severity levels to suit the severity conditions you want to define. For example, for the alert type OLD_LOCKS for the alert monitor LOCK_CHECK you could specify that if the lock is older than 12 hours you receive a WARNING message and if it is older than 24 hours you receive a CRITICAL message.

Default Configuration for the CTS Monitor (r3moncts)

```
#--------------------------------------------------------------------------
# TraceLevel  hostname  Disable=0  only error messages=1  info messages=2  \
#                       debug messages=3
TraceLevel     =ALL        =0
#--------------------------------------------------------------------------
# TraceFile  hostname    filename
#
TraceFile    =ALL        =r3moncts.log
#--------------------------------------------------------------------------
# History    hostname    path
# Path
#
HistoryPathUnix    =ALL        =default
HistoryPathAIX     =ALL        =default
HistoryPathWinNT   =ALL        =default
#--------------------------------------------------------------------------
# Remote          LocalHost      RemoteHost
# Monitoring
RemoteMonitoring  =rum        =ovsdsap1
RemoteMonitoring  =whisky     =ovsdsap2
#--------------------------------------------------------------------------
# AlertMonFun  SAP       SAP      SAP      SAP     Alertmonitor   Enable =1/
  \
#              Hostname  System   Number   Client                  Disable=0
 \
#
#   OpC          OpC         OpC        \
#   Severity     Object      MsgGroup     \
#
# Alerttype     RFC Parameter
#               =Parameter     =Sign   =Opt    =Low    =High
#              [=Parameter     =Sign   =Opt    =Low    =High] ...
# Example:
#
AlertMonFun  =ALL  =ALL  =ALL  =ALL  =CTS  =1  \
=WARNING    =Request     =R3_CTS   \
=REQUEST_CREATED   =USERNAME   =I    =CP      =*    =
--------------------------------------------------------------------------
```

Validating the Alert-Collector Configuration Files

The configuration files used by `r3moncol`'s alert-collector monitors have a known structure and content; commands and parameters appear in a particular order and location as illustrated in Default Configuration for the CTS Monitor (r3moncts) on page 109. To ensure an alert-collector monitor remains available and runs correctly, it is essential that the monitor can read and understand the contents of its configuration file each time the monitor starts. If the file is not available or contains errors, the monitor cannot perform its monitor function and in some cases will not start. To help prevent the situation where an alert-collector monitor cannot start or perform correctly due to a configuration error, the SPI for SAP automatically validates the contents of `r3moncol` configuration files when the SPI for SAP user tries to save it and when a SPI for SAP monitor reads it on startup.

The SPI for SAP checks the contents of an alert-collector's configuration file only if you use the HPOM for Windows configuration-file policy editor to edit and save it; the SPI for SAP does *not* check the contents of the configuration file for errors if you use a text editor to modify and save it.

If the SPI for SAP's validation tool finds an error when saving a configuration file, it displays a message describing the error, opens the file containing the error in the configuration-file policy editor, and places the cursor at the point in the configuration file where the error is located. To fix the problem, you will need to have a good understanding of the contents and structure of the configuration files, in particular: which parameters are associated with which commands and what values are allowed for the required parameters. For more information about the contents and the structure of the configuration files for the alert-collector-monitors, see Configuring the SPI for SAP Alert-Collector Monitors on page 97.

Understanding Configuration-File Error Messages

If you use the HPOM for Windows configuration-file policy editor to edit an alert-collector configuration file, you cannot save the file if it contains an error. If the SPI for SAP discovers an error when validating the contents of an alert-collector configuration file, it displays a message describing the error. For more information about the contents of the `r3moncol` configuration file, including what values are allowed and where, see The SPI for SAP Monitor-Configuration File on page 26.

The following list shows the messages that are displayed when an error is found in an alert-collector configuration file and explains what you need to do to fix the problem, which caused the error:

- `Arguments/Parameters are expected but missing in command AlertMonFun; check for arguments after the equals sign '='`

  The number of arguments present in the configuration file does not match the number of arguments required for the AlertMonFun keyword; check that you have not added or removed all or part of a parameter by accident when editing the file.

- `Value for the parameter Enable/Disable in command AlertMonFun must be '0' or '1'`

  The value assigned to the enable/disable parameter in the command AlertMonFun is an invalid number. It must be either 0 (disabled) or 1 (enabled).

- `The second argument in command TraceLevel must be a positive number between '0' and '3'`

  The TraceLevel setting is either missing or not allowed; the value must be one of the following: =0 (disabled), =1 (error messages), =2 (all messages), or =3 (debug).

- `Argument for <command_name> must be a valid number`

  The indicated argument for the command `<command_name>` must be a valid number.

- `Severity status <Status> defined in command DisableMonitoringWithSeverity is not allowed`

  The severity status of the messages you want to use to trigger the disable a monitor is unknown or not allowed. The following severity levels are allowed: Unknown, Normal, Warning, Minor, Major, Critical.

- `Invalid number of arguments in command DisableMonitoringWithSeverity`

  There are either too many or too few arguments defined in the command DisableMonitoringWithSeverity, which means the command is assuming the wrong values for the expected parameters. Check the number of parameters present in the command and their values.

- `Value for Disable/Enable in command DPQueueCheck is not a valid number`

  The value for the enable/disable parameter in the command DPQueueCheck is incorrect; it must be either =0 (disabled) or =1 (enabled).

- `<SeverityLevel> is an invalid Severity`

  The defined severity level is not allowed; check that you have spelled the severity level correctly and that the specified severity level is allowed in this context. The following severity levels are allowed: Unknown, Normal, Warning, Minor, Major, Critical.

- `<WorkProcess> is an invalid work process`

  The name of the work process defined in <WorkProcess> is either not known or not allowed; the names you can use in this context are the three-letter acronyms used in SAP, for example: DIA (dialog), UPD (update), BTC (batch).

- `Value of Workprocess must be either Idle or Queue in command DPQueueCheck.`

  The value defined for the status of the work-processes monitored by the DPQueueCheck command is either missing or invalid; the value must be set to either “Idle” or “Queue”.

- `Threshold value in command DPQueueCheck is not a valid number.`

  The value defined (in percentage terms) for the status of the work-processes queue monitored by the DPQueueCheck command is either missing or invalid; the value must be between 0 (zero) and 100 (one hundred) per cent.

- `Threshold value is out of range in command DPQueueCheck`

  The value defined (in percentage terms) for the status of the work-processes queue monitored by the DPQueueCheck command must be between 0 (zero) and 100 (one hundred) per cent. This value defines how full (or empty) the monitored queue must be as a percentage of the maximum before the dispatch monitor `r3mondisp` generates an alert.

- `Too many or too few arguments in command DPQueueCheck`

  The number of arguments present in the configuration file does not match the number of arguments required for the DPQueueCheck keyword. Check that you have not added or removed a parameter (or part thereof) by accident when editing the file.

- `<Keyword> is an unknown keyword.`

  The keyword specified is invalid; check that you have spelled the keyword correctly and that the specified keyword is allowed in this context.

- `Invalid or missing value <Value> for RFC parameter in configuration item AlertMonFun.`

The value for the defined RFC parameter indicated in <Value> is not allowed or is absent. Check and, if necessary, change or add the value for the specified parameter.

- `Invalid Alert monitor <AlertMonitorName> or Alert type parameter <AlertTypeParameterName>`

  The name of the alert monitor or the type of parameter specified for a given alert type is not allowed in this context. Check the spelling and make sure that the alert type is allowed with the specified alert-collector monitor.

- `Parameter <ParameterName> for Alertmonitor <AlertMonitorName> is not valid.`

  The specified parameter is not allowed in combination with the specified alert-collector monitor.

- `Alertmonitor <AlertMonitorName> and Alerttype <AlertTypeName> requires the parameter USERNAME.`

  You must define the parameter USERNAME if you want to use the alert monitor and alert type indicated.

- `Values specified for HIGH or LOW parameter must be positive numbers.`

  The value(s) defined in the HIGH/LOW parameters for a given alert type are incorrect or not allowed; use a positive number.

- `Values for HIGH or LOW parameter must be between <Number> and <Number>.`

  The HIGH/LOW parameters for a given alert type must be between the numbers indicated.

- `Invalid values specified for parameters LOW or HIGH, see the administrator reference guide for valid values.`

  The *HP Operations Smart Plug-in for SAP On-line Help* describes the contents of each monitor's configuration file in great detail.

- `The value <Value> specified for the SIGN parameter is not allowed; enter the appropriate value as described in the administrators reference.`

  The *HP Operations Smart Plug-in for SAP On-line Help* describes the contents of each monitor's configuration file in great detail.

- `Invalid value <Value> specified for the OPTION parameter.`

  The value used to define the OPTION parameter in the monitor-configuration file is not allowed. Check that the value is valid and that this kind of option it is allowed in the specified context.

- `Low AND High parameter is required if OPTION is <OptionName>.`

  You must specify values for both the HIGH and LOW parameters when using the option indicated in <OptionName>; either one or both of the values is missing or incorrectly defined.

- `No HIGH parameter is required if OPTION is <OptionName>.`

  Remove that value specified for the HIGH parameter; you do not need it when using the option indicated in `<OptionName>`.

- `The number of arguments for keyword <KeyWord> is wrong.`

Different keywords might require a different number or type of parameters. In this case, there are either too many or too few parameters specified for the keyword indicated in <KeyWord>. This could lead to a situation where the monitor assumes an incorrect value for a parameter.

r3monale: The iDOC-Status Monitor

The iDOC-status alert monitor, r3monale, is *time-frame* based and checks the status of existing iDOCs for errors using the transaction **WE02** as the data source. The monitor is application-server independent and available for global (SAP NetWeaver System-wide) use.

Note that, if you use standard SPI for SAP tools to configure r3moncol alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The iDOC-status alert monitor is of type *time frame*. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The iDOC-Status Monitor has the following alert types:

IDOC_CURRENT_STATUS

Defines when to generate an alert concerning the current state of the iDOCs

File Locations

The r3monale alert monitor uses the files listed this table.

Table 23 r3monale Files

File	Description
r3moncol(.exe)	Collector executable for the iDOC-status monitor
r3monale.cfg	Configuration file for iDOC-status monitor
r3monale.log	Trace file for storing trace data

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The r3monale monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert-collector monitors share the same format, the only difference being that the name of the configuration file varies to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The `r3monale` monitor uses the command-line parameters described in Table 22 on page 102. The command-line parameters for all the alert-collector monitors share the same format, the only difference being that the name of the configuration file must vary to match each specific monitor for both the `-cfgfile` and `-trace` parameters as indicated in Table 22 on page 102.

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

The remainder of this section describes the specific configuration requirements for the `r3monale` alert monitor. Alert-Collector Monitor Query Conditions on page 99 describes general configuration query rules which apply to all alert collector monitors. If you use the HPOM for Windows configuration-file policy editor to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the changes you make when you try to save the modified configuration file.

Configuring iDOC-Monitor Alert Types

When configuring the IDOC_CURRENT_STATUS alert type for `r3monale`, the iDOC status monitor, remember that you must define at least one of the parameters listed in Table 24. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

IDOC_CURRENT_STATUS

The IDOC_CURRENT_STATUS alert type defines the current status of iDOCs, which you want to monitor. Use the IDOC_CURRENT_STATUS alert type to configure the iDOC-status alert monitor `r3monale` to generate an alert if the status of an iDOC matches the status defined in the STATUS parameter.

Table 24 on page 114 lists the parameters that you can use to configure the IDOC_CURRENT_STATUS alert type and shows the value assigned to the parameters by default. Note that ‘ ‘ in the `Default Value` column signifies an empty string.

Table 24 IDOC_CURRENT_STATUS Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
DOCNUM	iDOC number, for example: “05” (error during translation)	= Sign: I, E	‘ ‘
		= Opt: GE, GT, LE, LT, BT	‘ ‘
		= Low	‘ ‘
		= High:	‘ ‘

Table 24 IDOC_CURRENT_STATUS Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
DOCTYP	the basic iDOC type, for example: DOCMAS01	= Sign: I	‘‘
		= Opt: CP, EQ	‘‘
		= Low	‘‘
		= High	‘‘
MESCOD	Logical message *code*	= Sign I	‘‘
		= Opt: CP, EQ	‘‘
		= Low	‘‘
		= High	‘‘
MESFCT	Logical message *function*	= Sign: I	‘‘
		= Opt: CP, EQ	‘‘
		= Low	‘‘
		= High	‘‘
MESTYP [a]	Logical message *type*	= Sign: I	‘‘
		= Opt: CP, EQ	‘‘
		= Low	‘‘
		= High	‘‘
RCVPFC	Partner *function* of receiver	= Sign: I	‘‘
		= Opt: CP, EQ	‘‘
		= Low	‘‘
		= High	‘‘
RCVPRN	Partner *number* of receiver	= Sign: I	‘‘
		= Opt: CP, EQ	‘‘
		= Low	‘‘
		= High	‘‘
RCVPRT	Partner *type* of receiver	= Sign: I	‘‘
		= Opt: CP, EQ	‘‘
		= Low	‘‘
		= High	‘‘

Table 24 IDOC_CURRENT_STATUS Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
SNDPFC	Partner *function* of sender	= Sign: I	‘‘
		= Opt: CP, EQ	‘‘
		= Low	‘‘
		= High	‘‘
SNDPRN	Partner *number* of sender	= Sign: I	‘‘
		= Opt: CP, EQ	‘‘
		= Low	‘‘
		= High	‘‘
SNDPRT	Partner *type* of sender	= Sign: I	‘‘
		= Opt: CP, EQ	‘‘
		= Low	‘‘
		= High	‘‘
STATUS [b]	Status of iDOC	= Sign: I, E	‘‘
		= Opt: GE, GT, LE, LT, BT	‘‘
		= Low	‘‘
		= High	‘‘

a. Possible values: ABSENT, MAX_ENTRIES, TIME_LIMIT

b. Possible values: CHECK_INBOUND, CHECK_OUTBOUND, MAX_ENTRIES

In Remote Monitoring, the `r3monale` alert checks the status of inbound iDOCs. An event generating an alert occurs if the number of in-bound iDOCS specified in IDOC_CURRENT_STATUS is greater than (GT) the value 4 (four) defined in MAX_ENTRIES. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

IDOC_CURRENT_STATUS Configuration

```
AlertMonFun  =ALL  =ALL  =ALL  =ALL  =ALL   =1  \
  =WARNING   =ALE =R3_IDOC_STATUS  \
  =IDOC_CURRENT_STATUS =STATUS =I =EQ =CHECK_INBOUND \
                       =MAX_ENTRIES =I =GT =4
```

Checking the iDOC Status

Using the IDOC_CURRENT_STATUS alert type in conjunction with the STATUS parameter allows you to check any one of the different iDOC statuses that are registered in SAP NetWeaver or a range of statuses defined in a group. Table 25 lists all the statuses that the SPI for SAP recognizes.

In addition, the SPI for SAP provides two pre-defined groups that you can use to check for a range of errors relating to incoming or outgoing iDOCs. For example, you can use the values CHECK_INBOUND and CHECK_OUTBOUND to monitor a range of values:

- CHECK_OUTBOUND

  monitors iDOCs with status: 02, 04, 05, 25, 26, 29, 30, 32

- CHECK_INBOUND

  monitors iDOCs with status: 51, 56, 60, 61, 62, 63, 64, 65, 66, 69

If you want to use the r3monale alert monitor to check for a specific iDOC status, replace the value =CHECK_INBOUND shown in IDOC_CURRENT_STATUS Configuration on page 116 with the iDOC status number listed in Table 25 that corresponds to the iDOC status you want to monitor. For example, to monitor the number of existing iDOCS, use =01. Note that it is not currently possible to define your own ranges similar to the pre-defined ranges CHECK_INDOUND and CHECK_OUTBOUND. Instead, you have to define a separate AlertMonFun entry for *each* additional value, which you want to monitor.

Table 25 Possible iDOC Status

iDOC Status	Description	Check Inbound	Check Outbound
00	Not used, only for R/2		
01	IDoc created		
02	Error passing data to port		✓
03	Data passed to port OK		
04	Error within control information of EDI subsystem		✓
05	Error during translation		✓
06	Translation OK		
07	Error during syntax check		
08	Syntax check OK		
09	Error during interchange handling		
10	Interchange handling OK		
11	Error during dispatch		
12	Dispatch OK		
13	Retransmission OK		
14	Interchange Acknowledgement positive		
15	Interchange Acknowledgement negative		
16	Functional Acknowledgement positive		

Table 25 Possible iDOC Status (cont'd)

iDOC Status	Description	Check Inbound	Check Outbound
17	Functional Acknowledgement negative		
18	Triggering EDI subsystem OK		
19	Data transfer for test OK		
20	Error triggering EDI subsystem		
21	Error passing data for test		
22	Dispatch OK, acknowledgement still due		
23	Error during retransmission		
24	Control information of EDI subsystem OK		
25	Processing despite syntax error (outbound)		✓
26	Error during syntax check of IDoc (outbound)		✓
27	Error in dispatch level (ALE service)		
28	Not used		
29	Error in ALE service		✓
30	IDoc ready for dispatch (ALE service)		✓
31	Error - no further processing		
32	IDoc was edited		✓
33	Original of an IDoc which was edited		
34	Error in control record of IDoc		
35	IDoc reloaded from archive		
36	Electronic signature not performed (time-out)		
37	IDoc added incorrectly		
38	IDoc archived		
39	IDoc is in the receiving system (ALE service)		
40	Application document not created in receiving system		

Table 25 Possible iDOC Status (cont'd)

iDOC Status	Description	Check Inbound	Check Outbound
41	Application document created in receiving system		
42	IDoc was created by test transaction		
50	IDoc added		
51	Error: Application document not posted	✓	
52	Application document not fully posted		
53	Application document posted		
54	Error during formal application check		
55	Formal application check OK		
56	IDoc with errors added	✓	
57	Test IDoc: Error during application check		
58	IDoc-Copy from an R/2 connection		
59	Not used		
60	Error during syntax check of IDoc (Inbound)	✓	
61	Processing despite syntax error (Inbound)	✓	
62	IDoc passed to application	✓	
63	Error passing IDoc to application	✓	
64	IDoc ready for transfer to the application	✓	
65	Error in ALE service		
66	IDoc is waiting for predecessor IDoc (serialization)		
67	Not used		
68	Error - no further processing		
69	IDoc was edited	✓	
70	Original of an IDoc which was edited		
71	IDoc reloaded from archive		

Table 25 Possible iDOC Status (cont'd)

iDOC Status	Description	Check Inbound	Check Outbound
72	Not used, only for R/2		
73	IDoc archived		
74	IDoc was created by test transaction		

r3monchg: The System-Change-Option Monitor

The SAP System-change-option alert monitor `r3monchg` double-checks the SAP system change options using the SAP NetWeaver transaction **`SE06`** as a reference.

This section contains information about the following topics:

- Monitor Type on page 120
- Alert Types on page 120
- File Locations on page 121
- Environment Variables on page 121
- Command-Line Parameters on page 121
- Remote Monitoring on page 121

Note that if you use standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The `r3monchg` monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The SPI for SAP monitor for SAP System-change-option alerts has only one alert type:

CHANGE_OPT

Monitors and double-checks the SAP System change options and generates an alert if the option matches the configuration.

File Locations

The r3monchg alert monitor uses the files listed in this table.

Table 26 r3monchg Files

File	Description
r3moncol(.exe)	Collector executable for the system change option monitor
r3monchg.cfg	Configuration file for system change option monitor.
r3monchg.log	Trace file for storing trace data.

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The r3monchg monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert collector monitors share the same format, the only difference being that the name of the configuration file must vary to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The r3monchg monitor uses the command line parameters described in Table 22 on page 102. The command line parameters for all the alert collector monitors share the same format, the only differences being that the name of the configuration file must vary to match each specific monitor for both the -cfgfile and -trace parameters as indicated in Table 22 on page 102.

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99.

Configuring SYSTEM CHANGE OPTION Monitor Alert Types

The general rules repeated below concern the use of exclude and include parameter values: the rules are particularly important for these alert types.

Parameter Values

This section describes how the SPI for SAP interprets *include* and *exclude* parameter values for an alert type entry. The SPI for SAP compares values in *different* parameters using 'and'; the SPI for SAP compares values in the *same* parameter as follows.

- **Include**: use 'or' to compare the parameters

- **Exclude**: use ‘and’ to compare the parameters

Note that the SPI for SAP evaluates *include* values before *exclude* values, as shown in Table 27.

Table 27 Comparing Include and Exclude Conditions for the Same Parameter

Select Options	Alert Type: CHANGE_OPT (SAP 4.6x) Example Configuration of Select Options	Comparison
1	=SYSTEM_CHANGE_OPTION =1 =WARNING =SystemChange =R3_Security = NSP_EDTFLAG =I = CP= /0* =	OR
2	=SYSTEM_CHANGE_OPTION =1 =WARNING =SystemChange = =R3_Security = NSP_EDTFLAG =I =EQ =/SAPQUERY/ =	OR
3	=SYSTEM_CHANGE_OPTION =1 =WARNING =SystemChange =R3_Security = NSP_EDTFLAG =E =EQ =LOCAL =	AND

CHANGE_OPT

The CHANGE_OPT alert type monitors and double-checks the SAP- System change options and generates an alert if the settings for the flag parameters allow the editing you are trying to perform. Table 28 on page 122 lists the parameters that you can use to configure the CHANGE_OPT alert type and shows the value assigned to the parameters by default.

The configuration of all parameters is mandatory. Multiple parameter entries on a single line are *not* allowed; use a new line to specify each one of any multiple configurations. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 28 CHANGE_OPT Configuration Parameters (SAP 4.6/6.x)

Parameter Name	Description	Query Conditions	Default Value
EDTFLAG	Flag indicating if an object can be edited.	= Sign: I	I
		= Opt: EQ	EQ
		= Low: ON, OFF, PATCH (PATCH=set to patch system)	PATCH
		= High:	
NSP_EDTFLAG	Flag indicating which specified name space(s) to set to ON.	= Sign: I	I
		= Opt: EQ, CP	CP
		= Low (See list of name space change options for SAP 4.6. X in Table 30.)	*
		= High:	

Table 28 CHANGE_OPT Configuration Parameters (SAP 4.6/6.x)

Parameter Name	Description	Query Conditions	Default Value
SWC_EDTFLAG	Flag indicating which specified software components to set to ON.	= Sign: I	I
		= Opt: EQ, CP	CP
		= Low: <specified software component> (See list of name space change options for SAP 4.6. X in Table 30.)	*
		= High:	

In The Default CHANGE_OPT Configuration, an event generating an alert occurs when the global system change is OFF or the specified name space is Local Objects (/0LOCAL/), or the specified software component is Local Developments (no automatic transport).

The Default CHANGE_OPT Configuration

```
AlertMonFun =ALL =ALL =ALL =ALL   =SYSTEM_CHANGE_OPTION  =1\
=WARNING    =SystemChange  =R3_Security \
=CHANGE_OPT   =NSP_EDTFLAG  =I =EQ  =/0LOCAL/  =

AlertMonFun  =ALL =ALL =ALL =ALL =SYSTEM_CHANGE_OPTION  =1\
=WARNING    =SystemChange  =R3_Security \
=CHANGE_OPT         =SWC_EDTFLAG  =I    =EQ  = LOCAL    =

AlertMonFun =ALL =ALL =ALL =ALL =SYSTEM_CHANGE_OPTION  =1\
=WARNING    =SystemChange  =R3_Security \
=CHANGE_OPT           =EDTFLAG      =I    =EQ  =OFF  =
```

The Customized CHANGE_OPT Configuration

```
AlertMonFun =ALL =ALL =ALL =SYSTEM_CHANGE_OPTION  =1\
=WARNING    =SystemChange  =R3_Security \
=CHANGE_OPT  =NSP_EDTFLAG  =I    =EQ  =/SAPQUERY/    =

AlertMonFun =ALL =ALL =ALL  =ALL =SYSTEM_CHANGE_OPTION  =1\
=WARNING    =SystemChange  =R3_Security \
=CHANGE_OPT         =SWC_EDTFLAG  =I    =EQ  = SAP_HR =

AlertMonFun =ALL =ALL =ALL =ALL =SYSTEM_CHANGE_OPTION  =1 \
=WARNING    =SystemChange  =R3_Security \
=CHANGE_OPT  =EDTFLAG  =I    =EQ  =OFF  =
```

In The Customized CHANGE_OPT Configuration, an event generating an alert occurs when the global change option is OFF or the system space change option ABAP query /SAP is ON, or the software component change option for Human Resources is ON. For more information about the change options for name system and software components, see Table 29 and Table 30.

Table 29 Software Components Change Options

Technical ID	Description
HOME	Customer developments
LOCAL	Local developments (no automatic transport)
SAP_ABA	Cross-Application Component
SAP_APPL	Logistics and Accounting
SAP_BASIS	SAP Basis Component
SAP_HR	Human Resources

Table 30 Name System Change Options for SAP 4.6/6.x

Technical ID	Description
/0CUST/	Customer name range
/0SAP/	General SAP name range
/1BCABA/	ABAP & GUI tools
/1BCDWB/	Development Workbench
/1BCDWBEN/	Enqueue function groups
/1COPA/	Generated objects in CO-PA
/1ISRWP/	IS-R merchandise and assortment controlling
/1ISU/	Generation namespace for CIC (Customer Interaction Center)
/1PAPA/	Personnel administration
/1PAPAXX/	Personnel administration - general
/1PSIS/	Project Information System - Logical database PSJ
/1PYXXFO/	PY-XX Form tool: Generated objects
/1SAP1/	General SAP generation namespace
/1SDBF12L/	Generation of pricing report
/BI0/	Business Information Warehouse: SAP namespace
/BIC/	Business Information Warehouse: Customer namespace
/SAPQUERY/	ABAP query /SAP

Table 30 Name System Change Options for SAP 4.6/6.x (cont'd)

Technical ID	Description
/SAPRRR/	Ready-to-Run SAP
/SAPSMOSS/	Interface: SAP messages to the SAP Online Service Sy
/SAPTRAIN/	SAP training

r3moncts: The Correction & Transport System Monitor

The correction-and-transport (CTS) alert monitor `r3moncts` identifies and monitors the Correction and Transport System for important transport requests, tasks and objects. Data collection is application-server independent.

The alert monitor `r3moncts` uses the following SAP elements as a reference:

- Transport requests and object lists created using SAP NetWeaver transaction **`SE01`**
- Tasks created using SAP NetWeaver transaction **`SE09`**

Note that, if you use standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The `r3moncts` monitor is of type *time frame*. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The CTS monitor has the following alert types:

- REQUEST_CREATED

  Defines when new requests generate an alert
- REQUEST_RELEASED

  Defines whether to generate an alert for a released request
- TASK_CREATED

  Defines if new tasks should generated an alert
- TASK_RELEASED

  Defines whether to generate an alert for released tasks
- OBJECT_USED

  Defines whether objects used by a task or a request generate an alert
- OBJECT_RELEASED

Defines whether to generate an alert when a request or task releases an object

File Locations

The `r3moncts` monitor uses the files listed in this table.

Table 31 r3moncts Files

File	Description
`r3moncol(.exe)`	Collector executable for the CTS monitor
`r3moncts.cfg`	Configuration file for the CTS monitor.
`r3moncts.log`	Trace file for storing trace data.

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The `r3moncts` monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert collector monitors share the same format, the only difference being that the name of the configuration file must vary to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The `r3moncts` monitor uses the command line parameters described in Table 22 on page 102. The command line parameters for all the alert collector monitors share the same format, the only differences being that the name of the configuration file must vary to match each specific monitor for both the `-cfgfile` and `-trace` parameters as indicated in Table 22 on page 102.

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert-collector monitors, see Alert-Collector Monitor Query Conditions on page 99.

Configuring CTS Monitor Alert Types

You should bear in mind the following the rules when configuring the alert-type parameters for the CTS monitor, `r3moncts`:

- By default, the SPI for SAP selects *all* data for each parameter.
- You can restrict data by specifying some or all of the parameters for the alert type.
- The SPI for SAP only considers the named parameters if you change default values and overrides the default value ALL for the unspecified parameters.

Use the parameter TRFUNCTION to configure the REQUEST_CREATED, REQUEST_RELEASED, TASK CREATED and TASK RELEASED alert types. TRFUNCTION has request functions which you can specify using the letter codes indicated in Table 32.

Table 32 TRFUNCTION Request Functions

Letter Code	Function Description
A	Request: Unclassified request becomes K, L or W with first object
C	Transport with change authorization
D	Patch
K	Request: Change request with destination consolidation layer
L	Request: Local request without transport
R	Task: Repair
S	Task: Development/correction
T	Request: Transport without originals
U	Dummy
W	Request: Customizing request with cons. layer destination
X	Task: Unclassified task becomes S or R with first object
Z	(task without request) SE09 memory usage

In the descriptions of the use of this parameter for each of the CTS alert types, only the letter code is shown. If you do not know what these letter codes represent, consult Table 32.

REQUEST_CREATED

Use the REQUEST_CREATED alert type to configure the correction-and-transport (CTS) alert monitor `r3moncts` to generate a message for any new request created within the last specified time frame. For example, adding a new (or modifying an existing) function module requires a change request. Table 33 on page 128 lists the parameters that you can use to configure the REQUEST_CREATED alert type and shows the value assigned to the

parameters by default. The configuration of any of these parameters is optional. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 33 REQUEST_CREATED Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
TRFUNCTION	The request function.	= Sign: I, E	I
		= Opt: CP, EQ	CP
		= Low: A,K,L,W,C,T, U, D [a]	*
		= High:	
TARGET	The target system for which this request was created. Note: this must be a SID	= Sign I, E	
		= Opt: EQ, CP	
		= Low: <*name of system*>	
		= High	
USERNAME	The login name of the SAP NetWeaver user who created the request.	= Sign I	
		= Opt: EQ, CP	
		= Low: <*username who created this request*>	
		= High	

a. You can only specify the listed functions (* means all).

In The Default REQUEST_CREATED Configuration, the monitor generates a message if a new request occurs within the last time frame.

The Default REQUEST_CREATED Configuration

```
AlertMonFun  =ALL  =ALL  =ALL  =ALL  =CTS  =1\
=WARNING    =Request     =R3_CTS\
=REQUEST_CREATED   =USERNAME   =I    =CP      =*    =
```

REQUEST_RELEASED

Use the REQUEST_RELEASED alert type to configure the correction-and-transport (CTS) alert monitor `r3moncts` to generate a message for any new request released within the last specified time frame. Table 34 on page 129 lists the parameters that you can use to configure the REQUEST_RELEASED alert type and shows the value assigned to the parameters by

default. The configuration of the parameters below is optional. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 34 REQUEST_RELEASED Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
TRKORR	Request ID	= Sign: I, E	
		= Opt: EQ	
		= Low: <Request ID>	
		= High:	
TRFUNCTION	The request function.	= Sign: I, E	
		= Opt: EQ	
		= Low: K,L, W,C,T, U, D. (You can only specify the listed functions (* means all).)	
		= High:	
TARGET	The target system for which this request was created. This must be a SID	= Sign I, E	I
		= Opt: EQ, CP	CP
		= Low: <name of system>	*
		= High	
USERNAME	The login name of the SAP NetWeaver user who created the request.	= Sign I	
		= Opt: EQ,CP	
		= Low: <username who created this request>	
		= High	
CUSTOMIZING	Customizing Requests	= Sign I,E	
		= Opt: EQ	
		= Low (Any entry other than 'X' will be treated as space.)	
		= High	
WORKBENCH	Workbench Requests	= Sign I, E	
		= Opt: EQ	
		= Low (Any entry other than 'X' will be treated as space.)	
		= High	

In The Default REQUEST_RELEASED Configuration, an event generating an alert occurs if any *customizing* request was released in the last time frame.

The Default REQUEST_RELEASED Configuration

```
AlertMonFun     =ALL    =ALL =ALL =ALL =CTS    =1\
  =WARNING     =Request      =R3_CTS\
  =REQUEST_RELEASED   =CUSTOMIZING   =I =EQ   =X
```

TASK_CREATED

Use the TASK_CREATED alert type to configure the correction-and-transport (CTS) alert monitor `r3moncts` to generate a message for any new task *created* within the last specified time frame. Table 35 on page 130 lists the parameters that you can use to configure the TASK_CREATED alert type and shows the value assigned to the parameters by default. The configuration of any of these parameters is optional. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 35 TASK_CREATED Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
TRFUNCTION	The request function.	= Sign: I, E	I
		= Opt: CP, EQ	CP
		= Low: X, S, R, Z [a]	*
		= High:	
USERNAME	The login name of the SAP NetWeaver user who created the request.	= Sign: I	
		= Opt: EQ, CP	
		= Low:<username who created this request>	
		= High:	

a. You can only specify the listed functions (* means all).

In The Default TASK_CREATED Configuration, `r3moncts` generates a message for any new task *created* within the last specified time frame.

The Default TASK_CREATED Configuration

```
AlertMonFun     =ALL    =ALL =ALL   =ALL   =CTS         =1      \
  =WARNING     =Task   =R3_CTS        \
  =TASK_CREATED         =TRFUNCTION     =I     =CP       =*          =
```

TASK_RELEASED

Use the TASK_RELEASED alert type to configure the correction-and-transport (CTS) alert monitor `r3moncts` to generate a message for any new task released within the last time frame. Table 36 on page 131 lists the parameters that you can use to configure the TASK_RELEASED alert type and shows the value assigned to the parameters by default. The

configuration of the parameters below is optional. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 36 TASK_RELEASED Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
TRKORR	Request ID	= Sign: I, E	
		= Opt: EQ	
		= Low: <Request ID>	
		= High:	
TRFUNCTION	The request function.	= Sign: I, E	I
		= Opt: CP, EQ	CP
		= Low: R, S, Z [a]	*
		= High:	
USERNAME	The login name of the SAP NetWeaver user who created the request.	= Sign: I	
		= Opt: EQ, CP	
		= Low: <username who created this request>	
		= High	

a. You can only specify the listed functions (* means all).

In The Default TASK_RELEASED Configuration, `r3moncts` generates a message for any new task *released* in the last time frame.

The Default TASK_RELEASED Configuration

```
AlertMonFun =ALL =ALL =ALL  =ALL  =CTS  =1\
  =WARNING  =Task =R3_CTS\
  =TASK_RELEASED =TRFUNCTION  =I =CP =* =
```

OBJECT_USED

Use the OBJECT_USED alert type to configure the correction-and-transport (CTS) alert monitor `r3moncts` to generate a message if a task or a request uses an object matching the defined configuration within the last time frame. Table 37 on page 132 lists the parameters that you can use to configure the OBJECT_USED alert type and shows the value assigned to the parameters by default.

The configuration of the parameters below is optional. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 37 OBJECT_USED Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
PGMID	Program ID	= Sign: I, E	
		= Opt: EQ, CP	
		= Low: <Program ID>	
		= High:	
OBJECT	Object type of element	= Sign I, E	
		= Opt: EQ, CP	
		= Low: <Object type>	
		= High	
OBJ_NAME	Object Name in object directory	= Sign I, E	I
		= Opt: EQ, CP	CP
		= Low: <Object name>	*
		= High	
OBJ_FUNC	Special function for an object entry: D = Delete, or M = Delete and recreate.	= Sign I, E	
		= Opt: EQ, CP	
		= Low	
		= High	
IN_REQUEST	Alert generated if object container is a request	= Sign I,E	
		= Opt: EQ	
		= Low	
		= High	
IN_TASK	Alert generated if object container is a task.	= Sign I, E	
		= Opt: EQ	
		= Low	
		= High	

In The Default OBJECT_USED Configuration, an event generating an alert occurs if any object with Object Type "LIMU" is used by a task or a request.

The Default OBJECT_USED Configuration

```
AlertMonFun  =ALL  =SD1 =ALL  =ALL   =CTS    =1\
  =WARNING   =Object =R3_CTS\
  =OBJECT_USED =PGMID  =I    =EQ  =LIMU  =
```

OBJECT_RELEASED

Use the OBJECT_RELEASED alert type to configure the correction-and-transport (CTS) alert monitor `r3moncts` to generate a message if a request or a task released the specified object. Table 38 on page 133 lists the parameters that you can use to configure the OBJECT_USED alert type and shows the value assigned to the parameters by default.

The configuration of the parameters below is optional. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 38 OBJECT_RELEASED Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
TRKORR	Request ID	= Sign: I, E	
		= Opt: EQ, CP	
		= Low:<Request ID>	
		= High:	
PGMID	Program ID	= Sign: I, E	
		= Opt: EQ, CP	
		= Low: <Program ID>	
		= High:	
OBJECT	Object type of element	= Sign I, E	
		= Opt: EQ, CP	
		= Low: <Object type>	
		= High	
OBJ_NAME	Object Name in object directory	= Sign I	I
		= Opt: EQ, CP	CP
		= Low: <Object name>	*
		= High	
IN_REQUEST	Alert generated if object container is a request	= Sign I,E	
		= Opt: EQ	
		= Low (Any entry other than 'X' will be treated as space.)	
		= High	

Table 38 OBJECT_RELEASED Configuration Parameters (cont'd)

Parameter Name	Description	Query Conditions	Default Value
IN_TASK	Alert generated if object container is a task.	= Sign I, E	
		= Opt: EQ	
		= Low (Any entry other than 'X' will be treated as space.)	
		= High	

In The Default OBJECT_RELEASED Configuration, an event generating an alert occurs if any object is released by a task.

The Default OBJECT_RELEASED Configuration

```
AlertMonFun =ALL  =ALL     =AL =ALL  =CTS  =1\
  =WARNING  =Object =R3_CTS\
  =IN_TASK   =I =EQ      =X  =
```

r3mondmp: The ABAP-Dump Monitor

The ABAP-dump alert monitor, `r3mondmp`, reports ABAP dumps in the SAP NetWeaver system which have occurred within the last, defined, time frame. The check is performed once per monitor run for all application servers.

Dumps are usually runtime errors and so they cannot always be detected by a static syntax check. They can occur for many reasons and may indicate serious problems. No dumps should occur on a production system.

Here are two examples of actions which cause dumps to occur:

- division by zero
- a called function model is not enabled

Since the system administrator generally has to do something to resolve problems associated with an ABAP dump, the messages generated by the `r3mondmp` alert monitor include an operator-initiated action that calls an ABAP program to display details of the dump.

The alert monitor `r3mondmp` references the SAP NetWeaver transaction **`ST22`**.

Note that, if you use standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The ABAP-dump alert monitor is of type *time frame*. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The ABAP-dump monitor has the following alert types:

- ABAP4_ERROR_EXIST

  Each ABAP dump generates one alert.

File Locations

The `r3mondmp` monitor uses the files listed in this table.

Table 39 r3mondmp Files

File	Description
`r3moncol(.exe)`	Collector executable for ABAP-dump monitor
`r3mondmp.cfg`	Configuration file for monitored application servers.
`r3mondmp.log`	Trace file for storing trace data.

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The `r3mondmp` monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert collector monitors share the same format, the only difference being that the name of the configuration file must vary to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The `r3mondmp` monitor uses the command line parameters described in Table 22 on page 102. The command line parameters for all the alert collector monitors share the same format, the only differences being that the name of the configuration file must vary to match each specific monitor for both the `-cfgfile` and `-trace` parameters as indicated in Table 22 on page 102.

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99.

ABAP4_ERROR_EXIST

Use the ABAP4_ERROR_EXIST alert type to configure the ABAP-dump alert monitor, r3mondmp, to generate an alert for each dump that occurred in the last time frame. The Default ABAP4_ERROR_EXIST Configuration shows how you can use =MAX_ENTRIES to count the number of dumps that have to occur before the SPI for SAP generates a message. In addition, you can specify a period of time in hours (=TIME_LIMIT) within which the defined number of dumps must occur. In this example, the SPI for SAP generates a message if ten dumps occur within twenty four hours.

The Default ABAP4_ERROR_EXIST Configuration

```
AlertMonFun     =ALL  =ALL  =ALL   =ALL =ABAP4 =1\
=WARNING    =ABAP_Dump   =R3_ABAP-4\
=ABAP4_ERROR_EXIST

# New feature in SPI for SAP version 8.0
#AlertMonFun    =ALL   =ALL  =ALL  =ALL  =ABAP4  =1  \
      =WARNING  =ABAP_Dump  =R3_ABAP-4  =ABAP4_ERROR_EXIST\
                =MAX_ENTRIES  =I    =GT   =10   =    \
                =TIME_LIMIT   =I    =LT   =24   =
```

The SPI for SAP's optional test transport includes a program that generates an ABAP dump which you can use to verify that the r3mondmp monitor correctly reports dumps to HPOM for Windows in the form of a message. If the test completes successfully, a message about the test dump appears in the HPOM for Windows console. For more information about SPI for SAP transports, see the transports read-me file \usr\sap\trans\readme on the HPOM for Windows managed node; for more information about importing and applying SPI for SAP transports, see the *HP Operations Smart Plug-in for SAP Configuration Guide*. After importing the transport, you can view the test programs installed by using the SAP transaction **SE80** to open the ABAP object navigator and browsing to the report (or program) /HPOV/YSPI0004.

r3monjob: The Job-Report Monitor

The job-report alert monitor r3monjob identifies and reports on batch jobs for the following conditions:

- A batch job's run time is either less than or has exceeded a specified limit.
- A specified period of time passes between a batch job's scheduled and actual start time (and date).
- A batch job has aborted.

You cannot configure r3monjob to send multiple messages, for example; first send a WARNING message if the run time for a batch job exceeds 5 minutes and then send a CRITICAL message if the run time for the same batch job exceeds 10 minutes.

The alert monitor r3monjob references:

- Reports created using SAP NetWeaver transaction **SM36** or **SM38**
- Job details including ID number using SAP NetWeaver transaction **SM37**

Messages generated by this alert monitor include an operator-initiated action that displays the list of current SAP batch jobs.

Note that, if you use standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The job-report monitor is of type *time frame*. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The Job-report monitor has the following alert types. Note that if you want to use the `r3monjob` monitor, you *must* configure the alert types listed below:

- JOB_MAX_RUN_TIME

  defines the *maximum* allowed run time for a job. `r3monjob` sends an alert if the defined job runs for longer than the maximum defined time, specified in minutes.

- JOB_MIN_RUN_TIME

  defines the *minimum* allowed run time for a job. `r3monjob` sends an alert if the defined job does not run for at least as long as the defined time, specified in minutes.

- START_PASSED

  is the maximum allowed delay between scheduled and actual start time for a defined job. `r3monjob` triggers an alert if the job does not start within the defined time, specified in minutes.

- JOB_ABORTED

  `r3monjob` sends an alert whenever the jobs specified in its configuration fail to complete successfully.

First Time Monitoring

When monitoring batch job alerts for a particular alert type for the first time, the Job-report monitor, `r3monjob` checks for the following conditions in SAP:

- Jobs which are not yet scheduled to run
- Jobs which ended within the previous two days
- Jobs which are still running

Performance Aspects

On a production system the table `tbtco` is usually very big. To speed up the database selection you should specify the job names in as much detail as possible. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

The runtime cost of a job selection grows in the order shown in Table 40.

Table 40 Order of Runtime Cost of Job Selection Criteria

Specified Jobname	Sign	Option	Selection
JOBNAME	I	EQ	Z5_CRITICAL_JOB_1> select via index
JOBNAME	I	CP	Z5_CRITICAL_JOB*> select via index
JOBNAME	E	CP	Z5_CRITICAL_JOB*> sequential scan

Note that exclude options tend to be more expensive than include options in performance terms. Using wild cards such as "*" in general database queries is more expensive than in explicit queries.

File Locations

The `r3monjob` monitor uses the files listed in this table

Table 41 r3monjob Files

File	Description
`r3moncol(.exe)`	Collector executable for the batch job monitor
`r3monjob.cfg`	Configuration file for monitored jobs and job conditions.
`r3monjob.log`	Trace file for storing trace data.

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The `r3monjob` monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert collector monitors share the same format, the only difference being that the name of the configuration file must vary to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The `r3monjob` monitor uses the command-line parameters described in Table 22 on page 102. The command line parameters for all the alert collector monitors share the same format, the only differences being that the name of the configuration file must vary to match each specific monitor for both the `-cfgfile` and `-trace` parameters as indicated in Table 22 on page 102.

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99 in the introduction to this chapter.

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

Configuring Job-Report Monitor Alert Types

You can configure `r3monjob`, the job-report monitor, for each of the listed alert types for a specific job, a combination of jobs, or for *all* jobs. You can also define exceptions for jobs that need different monitoring conditions. For more detailed information, see the alert-type tables which list the parameters and configuration options for each alert type. Note, too, the general rules for using exclude and include parameter values, which are of particular importance for these alert types.

Try to avoid using select option CP with the JOBNAME parameter: CP slows down the selection process. If you do use CP, try to limit its scope, for example; instead of specifying CP *, specify CP SAP*.

Parameter Values

This section describes how the SPI for SAP interprets *include* and *exclude* parameter values for an alert type entry. The SPI for SAP compares values in *different* parameters using 'and'; the SPI for SAP compares values in the *same* parameter as follows.

- **Include**: use 'or' to compare the parameters
- **Exclude**: use 'and' to compare the parameters

The SPI for SAP evaluates *include* values before *exclude* values, as shown in Table 42.

Table 42 Comparing Include and Exclude Conditions for the Same Parameter

Select Options	AlertType:JOB_MAX_RUN_TIME Example Configuration of Select Options	Comparison
1	=JOBNAME =I =CP =ZREP* = =MAX_RUNTIME =I =GT =10 =	OR
2	=JOBNAME =I =CP =SAP* = =MAX_RUNTIME =I =GT =20 =	OR
3	=JOBNAME =E =CP =SAP_ZREP* =	AND

JOB_MAX_RUN_TIME

The JOB_MAX_RUN_TIME alert type defines the maximum allowed run time for a job. Use the JOB_MAX_RUN_TIME alert type to configure the job-report alert monitor `r3monjob` to generate an alert when a job exceeds the value configured in the parameter MAX_RUNTIME. Table 43 on page 140 lists the parameters that you can use to configure the JOB_MAX_RUN_TIME alert type and shows the value assigned to the parameters by default.

The configuration of any of the parameters listed in Table 43 is optional. If both parameters are omitted, `r3monjob` reports all jobs running in the specified time. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 43 JOB_MAX_RUN_TIME Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
JOBNAME	Name of the jobs to monitor	= Sign: I, E	I
		= Opt: EQ, CP, BT	CP
		= Low <Name of job>	*
		= High (Only for use with a range)	
MAX_RUNTIME	Job run time in minutes which, if exceeded, generates an alert.	= Sign I, E	I
		= Opt: EQ, GE, GT, BT	GT
		= Low (Specify this parameter as a number. Otherwise the monitor ends with a dump.)	5
		= High (Only for use with a range)	

The following examples illustrates both the default and a customized configuration for the JOB_MAX_RUN_TIME alert type.

In The Default JOB_MAX_RUN_TIME Configuration, an event generating an alert occurs if any report named <*jobname*>* has a runtime exceeding five minutes.

The Default JOB_MAX_RUN_TIME Configuration

```
AlertMonFun  =ALL =ALL =ALL =ALL =JOBREPORT =1  \
=WARNING    =MaxRunTime   =R3_Jobs\
=JOB_MAX_RUN_TIME =JOBNAME  =I  =CP  =<jobname>*  =\
=MAX_RUNTIME   =I  =GT  =5  =
```

In A Customized JOB_MAX_RUN_TIME Configuration, an event generating an alert occurs if all reports named SAP*, except reports SAPZ*, have a runtime exceeding ten minutes

A Customized JOB_MAX_RUN_TIME Configuration

```
AlertMonFun =ALL  =ALL =ALL =ALL =JOBREPORT =1\
=WARNING    =MaxRunTime   =R3_Jobs  \
=JOB_MAX_RUN_TIME =JOBNAME =I =CP =SAP*  = \
=MAX_RUNTIME   =I  =GT  =10  =
```

```
AlertMonFun =ALL  =ALL =ALL =ALL =JOBREPORT =1\
=WARNING  =MaxRunTime   =R3_Jobs  \
=JOB_MAX_RUN_TIME =JOBNAME  =E =CP =SAPZ*  = \
=MAX_RUNTIME   =I  =GT  =10  =
```

The SPI for SAP's optional test transport includes a program that you can run to start a long-running job. You can use the job to verify that the `r3monjob` monitor is correctly configured to send a message to HPOM for Windows if a job runs for more than a defined amount of time. If the test completes successfully, a message about the test job appears in the HPOM for Windows console. For more information about SPI for SAP transports, see the transports read-me file `\usr\sap\trans\readme` on the HPOM for Windows managed node; for more information about importing and applying SPI for SAP transports, see the *HP Operations Smart Plug-in for SAP Configuration Guide*. After importing the transport, you can view the test programs installed by using the SAP transaction **`SE80`** to open the ABAP object navigator and browsing to the report (or program) `/HPOV/YSPI0002`.

JOB_MIN_RUN_TIME

The JOB_MIN_RUN_TIME alert type defines the minimum allowed run time for a job. Use the JOB_MIN_RUN_TIME alert type to configure the job-report alert monitor `r3monjob` to generate an alert when a job does not run for at least as long as the time specified in the parameter MIN_RUNTIME. Table 44 on page 141 lists the parameters that you can use to configure the JOB_MAX_RUN_TIME alert type and shows the value assigned to the parameters by default.

The configuration of any of the parameters below is optional. If both parameters are omitted, all jobs running in the specified time frame are reported. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 44 JOB_MIN_RUN_TIME Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
JOBNAME	Name of the jobs to monitor	= Sign: I, E	I
		= Opt: EQ, CP, BT	CP
		= Low <Name of job>	*
		= High: [a]	
MIN_RUNTIME	This defines the minimum allowed run time Alerts are triggered for jobs which did not run for at least as long as the time specified (in minutes).	= Sign I, E	I
		= Opt: EQ,LE, LT, BT	LT
		=Low <Min. value in minutes> [b]	1
		= High	

a. Only for use with a range

b. Specify this parameter as a number, otherwise the monitor ends with a dump.

The following examples illustrates both the default and a customized configuration for the JOB_MIN_RUN_TIME alert type.

In The Default JOB_MIN_RUN_TIME Configuration, an event generating an alert occurs if any report named <*jobname*>* has a runtime of less than one minute.

The Default JOB_MIN_RUN_TIME Configuration

```
AlertMonFun =ALL =ALL =ALL  =ALL =JOBREPORT  =1  \
=WARNING      =MinRunTime  =R3_Jobs\
=JOB_MIN_RUN_TIME =JOBNAME   =I  =CP  =<jobname>*  = \
=MIN_RUNTIME =I  =LT  =1   =
```

In Customized JOB_MIN_RUN_TIME Configuration, an event generating an alert occurs if all reports named SAP*, except reports SAPZ*, have a runtime of less than two minutes

Customized JOB_MIN_RUN_TIME Configuration

```
AlertMonFun  =ALL =ALL   =ALL  =ALL  =JOBREPORT =1  \
=WARNING    =MinRunTime   =R3_Jobs  \
=JOB_MIN_RUN_TIME =JOBNAME       =I    =CP     =SAP*  = \
=MIN_RUNTIME  =I =LT =2 =
```

```
AlertMonFun  =ALL =ALL =ALL  =ALL =JOBREPORT =1  \
=WARNING    =MinRunTime   =R3_Jobs  \
=JOB_MIN_RUN_TIME =JOBNAME       =E     =CP     =SAPZ*  = \
=MIN_RUNTIME   =I  =LT  =2  =
```

The SPI for SAP's optional test transport includes a program that you can run to start a short job. You can use the job to verify that the `r3monjob` monitor is correctly configured to send a message to HPOM for Windows if a job runs for less than a defined amount of time. If the test completes successfully, a message about the test job appears in the HPOM for Windows console. For more information about SPI for SAP transports, see the transports read-me file `\usr\sap\trans\readme` on the HPOM for Windows managed node; for more information about importing and applying SPI for SAP transports, see the *HP Operations Smart Plug-in for SAP Configuration Guide*. After importing the transport, you can view the test programs installed by using the SAP transaction **`SE80`** to open the ABAP object navigator and browsing to the report (or program) `/HPOV/YSPI0005`.

START_PASSED

The START_PASSED alert type defines the maximum allowed delay between a job's scheduled and actual start times. Use the START_PASSED alert type to configure the job-report alert monitor `r3monjob` to generate an alert if the specified jobs do not start within the configured TIME_SPAN after the scheduled start time. Table 45 on page 143 lists the parameters that you can use to configure the START_PASSED alert type and shows the value assigned to the parameters by default.

If a job is scheduled but does not have a start time, `r3monjob` cannot monitor it until and unless an assigned start time is visible in the SAP database. SAP associates a start time with a job only when the job assumes a particular status. The following SAP job statuses have a start time which means you can monitor them with `r3monjob`: Released, Ready, Active, Finished, and Canceled.

The configuration of any of the parameters below is optional. If both parameters are omitted all jobs running in the specified time frame are reported. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 45 START_PASSED Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
JOBNAME	Name of the jobs to monitor	= Sign: I, E	I
		= Opt: EQ, CP, BT	CP
		= Low <Name of job>	*
		= High [a]	
TIME_SPAN	The job run time in minutes that specifies when an alert should be raised. Note that it is not necessary to use a time range. You can specify a particular time instead.	= Sign I, E	I
		= Opt: EQ, GT, GE, BT	GT
		=Low [b] <*low_value_of_range_in_minutes_past_scheduled_start_time*>	1
		=High <*high_value_of_range_in_minutes_past_scheduled_start_time*>	

a. Only for use with a range

b. Specify this parameter as a number. Otherwise the monitor ends with a dump.

In The Default START_PASSED Configuration, an event generating an alert occurs if any report named <*jobname*>* does not start more than one minute after the scheduled start time.

The Default START_PASSED Configuration

```
AlertMonFun =ALL  =ALL =ALL   =ALL =JOBREPORT  =1\
=WARNING    =StartPassed  =R3_Jobs  \
=START_PASSED     =JOBNAME    =I  =CP   =<jobname>* =\
 =TIME_SPAN =I =GT  =1     =
```

JOB_ABORTED

The JOB_ABORTED alert type defines the names of the jobs, which fail to complete successfully. Use the JOB_ABORTED alert type to configure the job-report alert monitor `r3monjob` to generate an alert whenever the jobs specified in its configuration file fail to complete successfully. Task 46 on page 144 lists the parameters that you can use to configure the JOB_ABORTED alert type and shows the value assigned to the parameters by default.

The configuration of the parameter below is optional. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 46 JOB_ABORTED Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
JOBNAME	Name of the jobs to monitor	= Sign: I, E	I
		= Opt: EQ, CP, BT	CP
		= Low <Name of job>	*
		= High [a]	

a. Only for use when specifying a range

In The Default JOB_ABORTED Configuration, an event generating an alert occurs if any report named <*jobname*>* aborts.

The Default JOB_ABORTED Configuration

```
AlertMonFun   =ALL =ALL =ALL   =ALL   =JOBREPORT =1\
=WARNING    =Aborted       =R3_Jobs \
 =JOB_ABORTED     =JOBNAME     =I     =CP =  <jobname>*
```

In A Customized JOB_ABORTED Configuration, an event generating an alert occurs if jobs named SAP_REORG_ABAPDUMPS or ITOTEST are aborted.

A Customized JOB_ABORTED Configuration

```
AlertMonFun   =ALL   =ALL   =ALL   =ALL =JOBREPORT =1\
=WARNING    =Aborted =R3_Jobs \
=JOB_ABORTED   =JOBNAME   =I =EQ =SAP_REORG_ABAPDUMPS =
```

```
AlertMonFun   =ALL   =ALL =ALL   =ALL   =JOBREPORT         =1   \
=WARNING    =Aborted   =R3_Jobs\
=JOB_ABORTED =JOBNAME    =I    =EQ   =ITOTEST =
```

The SPI for SAP's optional test transport includes a program that you can run to generate an ABAP dump. You can use the generated dump to verify that the `r3monjob` monitor is correctly configured to send a message to HPOM for Windows if a job aborts. For more information about SPI for SAP transports, see the transports read-me file `\usr\sap\trans\readme` on the HPOM for Windows managed node; for more information about importing and applying SPI for SAP transports, see the *HP Operations Smart Plug-in for SAP Configuration Guide*. After importing the transport, you can view the test programs installed by using the SAP transaction **`SE80`** to open the ABAP object navigator and browsing to the report (or program) `/HPOV/YSPI0004`.

r3monlck: The Lock-Check Monitor

The lock-check alert-collector monitor `r3monlck` references the enqueue process which manages logical locks for SAP NetWeaver transactions and reports on obsolete locks. Obsolete locks are defined as locks which are older than the time period you specify. The check is performed once per monitor run for all application servers.

An object which is locked cannot be changed by anyone other than the user associated with it and can cause severe problems. The operator can check the locks set for a specific instance in **SM12**. Here are two examples of actions which cause locks to occur:

- Users switch off their computers without first logging off the SAP NetWeaver system - this is the most common cause of locked objects.
- An entire SAP instance fails.

The alert monitor `r3monlck` references the SAP NetWeaver transaction **SM12**.

Messages generated by this alert monitor include an operator-initiated action that calls the **SM12** Locks Overview module. The operator can then check the locks set for a specific instance in **SM12**.

Note that, if you use standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The `r3monlck` monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The lock-check monitor has only one alert type:

OLD_LOCKS

Specifies when to define a lock as “old”, using the time period you specify in the parameter LOCK_TIME.

File Locations

The `r3monlck` monitor uses the files listed in this table.

Table 47 r3monlck Files

File	Description
`r3moncol(.exe)`	Collector executable for the lock_check monitor
`r3monlck.cfg`	Configuration file for the lock_check monitor.
`r3monlck.log`	Trace file for storing trace data.

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The `r3monlck` monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert collector monitors share the same format, the only difference being that the name of the configuration file must vary to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The `r3monlck` monitor uses the command-line parameters described in Table 22 on page 102. The command-line parameters for all the alert collector monitors share the same format, the only differences being that the name of the configuration file must vary to match each specific monitor for both the `-cfgfile` and `-trace` parameters as indicated in Table 22 on page 102.

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99.

OLD_LOCKS

The LOCK_TIME alert type specifies when to define a lock as “old”, using the time period you specify in the parameter LOCK_TIME. Use the LOCK_TIME alert type to configure `r3monlck` to generate an alert when a job exceeds the time span defined in the parameter LOCK_TIME. Table 48 on page 146 lists the parameters that you can use to configure the LOCK_TIME alert type and shows the value assigned to the parameters by default.

The configuration of the parameter below is mandatory. Note that you can have more than one configuration in the `.cfg` file. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 48 LOCK_TIME Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
LOCK_TIME	**The time span (in hours) after which a lock is considered old**	**= Sign: I,E**	**I**
		= Opt: EQ, GT, GE, LE, LT, BT	**GT**
		= Low: <time in hours> [a]	
		= High:[b]	

a. Specify this parameter as a number. Otherwise the monitor ends with a dump.

b. Only for use when specifying a range

In The Default OLD_LOCKS Configuration, an event generating an alert occurs if any lock exceeds a time span of 24 hours.

The Default OLD_LOCKS Configuration

```
AlertMonFun  =ALL =ALL =ALL   =ALL =LOCK_CHECK =1\
=WARNING    =Enqueue  =R3_Enqueue\
=OLD_LOCKS  =LOCK_TIME =I    =GT  =24   =
```

r3monoms: The Operation-Mode Monitor

The operation-mode alert monitor `r3monoms` checks each application server for the following conditions:

- A scheduled operation-mode switch occurs later than the time specified
- A scheduled operation-mode switch has not occurred at all

The alert monitor `r3monoms` references the following SAP objects:

- Scheduled operation modes in SAP NetWeaver transaction **SM63**
- Configuration modes in SAP NetWeaver transaction **RZ04**

The operation-mode monitor `r3monoms` does not support the monitoring of WebAS 7.0/ Netweaver04s (kernel 7) environments; changes in SAP mean there are no operation-mode switch errors to monitor.

Operation-mode switch failures influence the performance of the SAP NetWeaver system and can cause problems. Operation-mode switches might occur for a number of reasons, for example; work processes that must be switched are still occupied in a process while the operation-mode switch is running. The system administrator usually needs to intervene to fix the problem, for example; by forcing and testing the operation mode's state.

If an operations-mode switch generates an alarm because the switch is not enabled in time, but then successfully occurs later without any intervention, the SPI for SAP sends a message indicating that the switch, although late, has now gone ahead as planned.

If you use standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The `r3monoms` monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The operation-mode, `r3monoms`, alert monitor has only one alert type:

- OM_SWITCH_OVERDUE

  This defines when an operation mode switch is overdue.

File Locations

The r3monoms monitor uses the files listed in this table

Table 49 r3monoms Files

File	Description
r3moncol(.exe)	Collector executable for the operation mode monitor
r3monoms.cfg	Configuration file for the operation mode monitor.
r3monoms.log	Trace file for storing trace data.

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The r3monoms monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert collector monitors share the same format, the only difference being that the name of the configuration file must vary to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The r3monoms monitor uses the command-line parameters described in Table 22 on page 102. The command-line parameters for all the alert collector monitors share the same format, the only differences being that the name of the configuration file must vary to match each specific monitor for both the -cfgfile and -trace parameters as indicated in Table 22 on page 102.

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99.

OM_SWITCH_OVERDUE

The OM_SWITCH_OVERDUE alert type defines the period of time in which an operation-mode switch must occur. Use the OM_SWITCH_OVERDUE alert type to configure r3monoms to generate an alert if an operation-mode switch does not occur within the defined period of time. Table 50 lists the parameters that you can use to configure the OM_SWITCH_OVERDUE alert type and shows the value assigned to the parameters by default.

The configuration of the parameters in Table 50 is optional. By default, an alert is triggered if an operation-mode switch is more than three minutes late.

The APSERVER parameter allows you to set the application-server- dependent monitors, r3monwpa, r3monusr, and r3monoms to monitor a specific application server. You need to configure APSERVER in the following manner, where *<hostname>* is the name of the application server to monitor as it appears in the list of application servers displayed in transaction **SM51**:

```
=APSERVER  =I =CP =<hostname>_<SID>_<Instance_Number> =
```

It is also recommended that you explicitly define the host name of the SAP NetWeaver central instance whose application server(s) you want to specify with APSERVER, as illustrated in the Specifying an Application Server.

Specifying an Application Server

```
AlertMonFun  =<hostname> =ALL =ALL =ALL =OM =1 \
=WARNING   =OperationMode  =R3_WP   \
=OM_SWITCH_OVERDUE =OVERDUE_TIME   =I  =GT  =15   = \
                  =APSERVER  =I =CP =hpdev01_MP3_00 =
```

The *<hostname>* in Specifying an Application Server is the name of the host where the r3monoms monitor is running. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 50 OM_SWITCH_OVERDUE Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
APSERVER	specifies an application server to monitor	= Sign: I, E	
		= Opt: CP	
		= Low: *<AppServer_ID>*	
		= High:	
OVERDUE_TIME	The time in minutes, after which a scheduled mode switch is considered overdue.	= Sign: I, E	I
		= Opt: GT, GE, LE, LT, BT	GT
		= Low: *<time in minutes>* [a]	3
		= High: [b]	

a. Mandatory; if the query condition is not present, the monitor does not perform any check.

b. Only for use when specifying a range

In The Default OM_SWITCH_OVERDUE Configuration, an event generating an alert occurs if a scheduled operation mode switch is more than three minutes late.

The Default OM_SWITCH_OVERDUE Configuration

```
AlertMonFun  =ALL =ALL =ALL  =ALL=OM  =1\
=WARNING   =OperationMode  =R3_WP\
=OM_SWITCH_OVERDUE   =OVERDUE_TIME  =I   =GT  =3  =
```

r3monrfc: The RFC-Destination Monitor

The RFC-destination monitor `r3monrfc` is application-server independent and checks RFC destinations in an SAP environment. SAP uses RFC destinations to remotely execute function modules, which reside on other SAP Systems. The alert-collector monitor, `r3monrfc`, references the RFC destinations, which you can display, create, and maintain by means of the SAP NetWeaver transaction **`SM59`**.

Note that, if you use standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The `r3monrfc` monitor is of type *snapshot*. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The RFC-destination alert monitor has the following alert type, which uses a snapshot report type:

CHECK

Defines alert conditions for failed SAP-RFC connections

File Locations

The `r3monrfc` monitor uses the files listed in this table.

Table 51 r3monrfc Files

File	Description
`r3moncol(.exe)`	Collector executable for the SAP-RFC monitor
`r3monrfc.cfg`	Configuration file for the SAP-RFC monitor.
`r3monrfc.log`	Trace file for storing trace data.

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The `r3monrfc` monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert collector monitors share the same format, the only difference being that the name of the configuration file must vary to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The `r3monrfc` monitor uses the command-line parameters described in Table 22 on page 102. The command-line parameters for all the alert collector monitors share the same format, the only differences being that the name of the configuration file must vary to match each specific monitor for both the `-cfgfile` and `-trace` parameters as indicated in Table 22 on page 102.

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99.

Limitations

You can use `r3monrfc` to monitor the following RFC destinations as long as they are listed in SAP transaction SM59 (SAP 6.20 and later):

- HTTP Connection to External Server
- HTTP Connection to SAP NetWeaver System

Configuring RFC-destination Alert Types

You must configure the parameters CONNECTION_TYPE and NAME for all alert types for `r3monrfc`, the RFC-destination monitor. Note the general rules below on exclude and include parameters for `r3monrfc`.

Parameter Values

This section describes how the SPI for SAP interprets *include* and *exclude* parameter values for an alert type entry. The SPI for SAP compares values in *different* parameters using 'and'; the SPI for SAP compares values in the *same* parameter as follows.

- **Include**: use 'or' to compare the parameters
- **Exclude**: use 'and' to compare the parameters

The SPI for SAP evaluates *include* values before *exclude* values.

CHECK

CHECK is a snapshot alert type for `r3monrfc`, the SPI for SAP's RFC-destination monitor. Snapshot alert types take a picture of the SAP System at the moment the monitor runs.

The CHECK alert type defines alert conditions for failed SAP-RFC connections. Use the CHECK alert type to configure `r3monrfc` to generate an alert if the RFC connection test for the target system fails. Table 52 on page 152 lists the parameters that you can use to configure the CHECK alert type and shows the value assigned to the parameters by default.

The parameter CHECK is required. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 52.

Table 52 CHECK Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
CONNECTION_TYPE	Type of SAP RFC connection to monitor, for example: 1, 3, M, T... Type 1= App. Server, 3= SAP NetWeaver System, M= CMC, T =TCP/IP, G= HTTP connection to external server, H= HTTP connections to SAP NetWeaver system.	= Sign I, E	I
		= Opt: EQ	EQ
		= Low	3
		= High	
NAME	Name you assigned to the SAP-RFC connection as shown in the transaction /NSM59.	= Sign: I, E	I
		= Opt: EQ, CP	EQ
		= Low: <SID>	' '
		= High:	

In The Default Check-RFC_DESTINATION Configuration, an event generating an alert occurs whenever the RFC_DESTINATION test fails for any *one* of the type 3 SAP-RFC destinations.

The Default Check-RFC_DESTINATION Configuration

```
AlertMonFun  =ALL  =ALL  =ALL  =ALL  =RFC_DESTINATION  =1 \
             =WARNING  =RFC_Destinations  =R3_RFC  \
              =CHECK  =CONNECTION_TYPE  =I  =EQ  =3  =
```

In An Example Check-RFC_DESTINATION Configuration, an event generating an alert occurs whenever RFC_DESTINATION test fails for the single SAP-RFC destination named OV_C01_099.

An Example Check-RFC_DESTINATION Configuration

```
AlertMonFun  =ALL  =ALL  =ALL  =ALL  =RFC_DESTINATION  =1 \
             =WARNING  =RFC_Destinations  =R3_RFC  \
              =CHECK  =NAME  =I  =CP  =OV_C01_099  =
```

r3monspl: The Spooler Monitor

The spooler alert monitor `r3monspl` is application-server independent and monitors spooler entries for the following conditions:

- The number of spool requests which would generate an alert
- The number of error-generating spool requests that would generate an alert
- A specified printer has received erroneous spool requests.

The alert monitor `r3monspl` references output tasks in SAP NetWeaver transaction **`SP01`** and report sources in SAP NetWeaver transaction **`SE38`**.

Note that, if you use standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The `r3monspl` alert monitor is of type *snapshot*. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The spooler alert monitor has the following alert types:

- SPOOL_ENTRIES_RANGE

  This defines the number of spool requests which, if exceeded, would cause an alert.

- SPOOL_ERROR_RANGE

  This defines the number of error-generating spool requests which, if exceeded, would cause an alert.

- PRINT_ERROR_EXISTS

  This specifies the name(s) of printers for which an alert would be generated if a spool error exists.

File Locations

The `r3monspl` monitor uses the files listed in this table.

Table 53 r3monspl Files

File	Description
`r3moncol(.exe)`	Collector executable for the spooler monitor
`r3monspl.cfg`	Configuration file for the spooler monitor.
r3monspl.log	Trace file for storing trace data.

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The `r3monspl` monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert collector monitors share the same format, the only difference being that the name of the configuration file must vary to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The `r3monspl` monitor uses the command line parameters described in Table 22 on page 102. The command line parameters for all the alert collector monitors share the same format, the only differences being that the name of the configuration file must vary to match each specific monitor for both the `-cfgfile` and `-trace` parameters as indicated in Table 22 on page 102.

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99.

Configuring Spooler-Monitor Alert Types

You can configure `r3monspl`, the spooler monitor, for each of the alert types and then define exceptions for different monitoring conditions. For more detailed information, see the alert-type tables which give the parameters and configuration for each alert type.

SPOOL_ENTRIES_RANGE

The SPOOL_ENTRIES_RANGE alert type defines the number of spool requests which, if exceeded, would generate an alert. Use the SPOOL_ENTRIES_RANGE alert type to configure `r3monspl` to generate an alert if the number of spool entries exceeds the range specified. Table 54 lists the parameters that you can use to configure the SPOOL_ENTRIES_RANGE alert type and shows the value assigned to the parameters by default.

The configuration of the RANGE parameter is mandatory. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 54 SPOOL_ENTRIES_RANGE Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
RANGE	The number of spool entries outside of which an alert will be generated. Note that, despite its name, you do not need to specify this parameter as a select-option range.	= Sign: I, E	I
		= Opt: EQ, GT, GE, LE, LT, BT	GT
		= Low: [a]	50
		= High:	

a. Specify this parameter as a number. Otherwise the monitor ends with a dump.

In The Default SPOOL_ENTRIES_RANGE Configuration, an event generating an alert occurs if there are more than 50 spooler entries.

The Default SPOOL_ENTRIES_RANGE Configuration

```
AlertMonFun  =ALL   =ALL =ALL =ALL =SPOOLER  =1\
=CRITICAL     =Spool   =R3_Spooler \
=SPOOL_ENTRIES_RANGE    =RANGE  =I  =GT  =50   =
```

SPOOL_ERROR_RANGE

The SPOOL_ERROR_RANGE alert type defines the number of *erroneous* spool requests which, if exceeded, would generate an alert. Use the SPOOL_ERROR_RANGE alert type to configure `r3monspl` to generate an alert if the number of *erroneous* spool entries exceeds the range specified. Table 55 lists the parameters that you can use to configure the SPOOL_ERROR_RANGE alert type and shows the value assigned to the parameters by default.

The configuration of the RANGE parameter is mandatory. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 55 SPOOL_ERROR_RANGE Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
RANGE	The number of erroneous spool requests outside of which an alert will be generated. Note that, despite its name, you do not need to specify this parameter as a select option range.	= Sign: I, E	I
		= Opt: EQ, GT, GE,LE, LT, BT	GT
		= Low: [a]	50
		= High:	

a. Specify this parameter as a number; otherwise the monitor ends with a dump.

In The Default SPOOL_ERROR_RANGE Configuration, an event generating an alert occurs if there are more than 50 erroneous spool requests.

The Default SPOOL_ERROR_RANGE Configuration

```
AlertMonFun  =ALL =ALL =ALL =ALL  =SPOOLER  =1\
=CRITICAL =Spool  =R3_Spooler \
=SPOOL_ERROR_RANGE  =RANGE  =I  =GT  =50    =
```

PRINT_ERROR_EXISTS

The PRINT_ERROR_EXISTS alert type defines the printers to monitor for spool errors. Use the PRINT_ERROR_EXISTS alert type to configure `r3monspl` to generate an alert if a spool error exists for the specified printer. Table 56 lists the parameters that you can use to configure the PRINT_ERROR_EXISTS alert type and shows the value assigned to the parameters by default.

r3monspl generates an alert if a spool error exists for a specified printer. The configuration of the PRINTER parameters is mandatory. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 56 PRINT_ERROR_EXISTS Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
PRINTER	The printer(s) which should be checked for spool entries of state error.	= Sign: I, E	I
		= Opt:	CP
		= Low:	*
		= High:	

In The Default PRINT_ERROR_EXISTS Configuration, r3monspl generates an alert if any printer has a spool entry-state error.

The Default PRINT_ERROR_EXISTS Configuration

```
AlertMonFun  =ALL  =ALL =ALL  =ALL  =SPOOLER  =1\
=WARNING  =Spool  =R3_Spooler \
=PRINT_ERROR_EXISTS =PRINTER   =I  =CP      =*   =
```

r3montra: The Transport Monitor

The transport monitor r3montra is application-server independent and is used to check the following parts of the transport system:

- Successful or failed imports and exports for the monitored system
- The presence of confirmed and unconfirmed repairs in the monitored system
- Connections that use a connection test (PING) to the configured systems
- TP-Tests of the configured systems

The alert monitor r3montra references transport routes in SAP NetWeaver transactions **STMS** and **SE01**.

If you use standard SPI for SAP tools to configure r3moncol alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The r3montra monitor is of type *snapshot*. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The transport alert monitor has the following alert types, which use a mixture of snapshot and time-frame report types:

- TRANS

  Defines alert conditions for successful and failed transport exports and imports

- REPAIR

  Defines alert conditions for confirmed and unconfirmed repairs

- RFCONNECT

  Defines alert conditions for the RFC connections between the systems

- TPTEST

  Defines alert conditions concerning the TP interface with the database. It includes a connection test (PING), a TP call to the connected database, a check of the TP interface (version, transport directory, TPPARAM path, a file check and a TPLOG check).

File Locations

The `r3montra` monitor uses the files listed in this table.

Table 57 r3montra Files

File	Description
`r3moncol(.exe)`	Collector executable for the transport monitor
`r3montra.cfg`	Configuration file for the transport monitor.
r3montra.log	Trace file for storing trace data.

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The `r3montra` monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert collector monitors share the same format, the only difference being that the name of the configuration file must vary to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The `r3montra` monitor uses the command-line parameters described in Table 22 on page 102. The command-line parameters for all the alert collector monitors share the same format, the only differences being that the name of the configuration file must vary to match each specific monitor for both the `-cfgfile` and `-trace` parameters as indicated in Table 22 on page 102.

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99.

Configuring Transport-Monitor Alert Types

You must configure the parameter ALERT_THRESHOLD for all alert types for `r3montra`, the transport monitor. All other parameters are optional. Note the general rules below on exclude and include parameters for `r3montra`.

Parameter Values

This section describes how the SPI for SAP interprets include and exclude parameter values for an alert type entry. the SPI for SAP compares values in different parameters using 'and;' the SPI for SAP compares values in the same parameter as follows.

- **Include:** Use 'or' to compare the parameters
- **Exclude:** Use 'and' to compare the parameters

The SPI for SAP evaluates *include* values before *exclude* values.

TRANS

`TRANS` is a time-frame based alert type for `r3montra`, the SPI for SAP's transport monitor. `r3montra` generates an alert if the number of failed or successful transport imports and exports exceeds a defined threshold. Note that the parameter USERNAME is mandatory for the TRANS alert type.

Table 58 on page 158 lists the parameters that you can use to configure the TRANS alert type and shows the value assigned to the parameters by default. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 58 TRANS Configuration Parameters

Parameter Name	Description	query conditions	Default Value
ALERT_THRESHOLD	The return code of the transport state above which an alert occurs for example; 4 (warning).	= Sign: I, E	I
		= Opt: GT, GE, LT, LE	GT
		= Low: [a]	4
		= High:	

Table 58 TRANS Configuration Parameters (cont'd)

Parameter Name	Description	query conditions	Default Value
E_SUCCESS	Filtering option to include all *successfully* exported transports	= Sign: I, E	I
		= Opt: EQ	EQ
		= Low: [b]	X
		= High:	
E_FAILURE	Filtering option to include all failed *exported* transports	= Sign: I, E	I
		= Opt: EQ	EQ
		= Low: [b]	X
		= High:	
I_SUCCESS	Filtering option to include all *successfully* imported transports	= Sign: I, E	I
		= Opt: EQ	EQ
		= Low: [b]	X
		= High:	
I_FAILURE	Filtering option to include all *failed* imported transports	= Sign: I, E	I
		= Opt: EQ	EQ
		= Low [b]	X
		= High:	
USERNAME	The login name of the SAP NetWeaver user [c]. This parameter is mandatory.	= Sign I, E	I
		= Opt: EQ,CP	EQ
		= Low: <username>	ddic [d]
		= High:	

a. Specify as a number, otherwise the monitor ends with a dump

b. Any entry other than the default is treated as space

c. Since requests/tasks are user dependent, you can use it to restrict data.

d. SAP user name for database-administration tasks

In The Default TRANS Configuration, an event generating an alert occurs if the threshold for imported or exported transports is greater than four (4). Note that the number "4" defined in the threshold for the parameter ALERT_THRESHOLD does not refer to the total number of imports: it refers to the SAP return code associated with the import. In this example, transport imports with return codes of 4 (warning) and above (GT =4) would generate an alert. For more information about import return codes, refer to the SAP product documentation.

The Default TRANS Configuration

```
AlertMonFun =ALL =ALL =ALL =ALL =TRANSPORT =1\
=WARNING =Trans =R3_Transport\
=TRANS =I_FAILURE =I =EQ =X =\
=USERNAME =I =EQ =ITOUSER =\
=ALERT_THRESHOLD =I =GT =4 =

AlertMonFun =ALL =ALL =ALL =ALL =TRANSPORT =1\
=WARNING =Trans =R3_Transport\
=TRANS =I_SUCCESS =I =EQ =X =\
=USERNAME =I =EQ =ITOUSER =\
=ALERT_THRESHOLD =I =GE =4 =

AlertMonFun =ALL =ALL =ALL =ALL =TRANSPORT =1\
=WARNING =Trans =R3_Transport\
=TRANS =E_FAILURE =I =EQ =X =\
=USERNAME =I =EQ =ITOUSER =\
=ALERT_THRESHOLD =I =GT =4

AlertMonFun =ALL =ALL =ALL =ALL =TRANSPORT =1\
=WARNING =Trans =R3_Transport\
=TRANS =E_SUCCESS =I =EQ =X =\
=USERNAME =I =EQ =ITOUSER =\
=ALERT_THRESHOLD = I = GT = 4 =
```

REPAIR

REPAIR is a time-frame based alert type for `r3montra`, the SPI for SAP's Transport Monitor. `r3montra` generates an alert if the number of confirmed or unconfirmed repairs exceeds a specified threshold.

Table 59 on page 160 lists the parameters that you can use to configure the REPAIR alert type and shows the value assigned to the parameters by default. Note that the parameter ALERT_THRESHOLD is mandatory. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 59 REPAIR Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
R_CONFIRM	Filtering option to include all confirmed repairs.	= Sign: I, E	I
		= Opt: EQ	EQ
		= Low: [a]	X
		= High:	
R_UNCONFIR	Filtering option to include all unconfirmed repairs.	= Sign: I, E	I
		= Opt:	EQ
		= Low: [a]	X
		= High:	

Table 59 REPAIR Configuration Parameters (cont'd)

Parameter Name	Description	Query Conditions	Default Value
USERNAME	The login name of the SAP NetWeaver user[b]. This parameter is mandatory.	= Sign I, E	I
		= Opt: EQ,CP	EQ
		= Low: <username>	ddic [c]
		= High:	
ALERT_THRESHOLD	The number of the allowed repair state above which an alert occurs	= Sign I, E	I
		= Opt: GT, GE, LT, LE	GT
		= Low: [d]	4
		= High:	

a. Any entry other than the default is treated as space

b. Since requests/tasks are user dependent, you can use it to restrict the data.

c. SAP user name for database-administration tasks

d. Specify the parameter as a number or the monitor ends with a dump

In The Default REPAIR Configuration, an event generating an alert occurs if the alert threshold of four (=GT =4) R_CONFIRM or R_UNCONFIR errors is exceeded for the specified target System.

The Default REPAIR Configuration

```
AlertMonFun  =ALL  =ALL  =ALL =ALL =TRANSPORT =1  \
=WARNING    =Repair =R3_Transport  \
=REPAIR =R_CONFIRM =I  =EQ =X =  \
=ALERT_THRESHOLD  =I      =GT      =4          =

AlertMonFun  =ALL  =ALL  =ALL =ALL =TRANSPORT =1  \
=WARNING    =Repair =R3_Transport  \
=REPAIR =R_UNCONFIR =I  =EQ =X =  \
=ALERT_THRESHOLD  =I      =GT      =4          =

AlertMonFun  =ALL  =ALL  =ALL =ALL =TRANSPORT =1  \
=WARNING    =Repair =R3_Transport   \
=REPAIR =USERNAME =I  =CP =* =\
=ALERT_THRESHOLD  =I   =GT   =4    = =
```

RFCONNECT

RFCONNECT is a snapshot alert type for `r3montra`, the SPI for SAP's Transport Monitor. Snapshot alert types take a picture of the System at the moment the monitor runs. `r3montra` generates an alert if the number of RFC-connect errors to the target system exceeds the specified alert threshold.

Table 60 on page 162 lists the parameters that you can use to configure the RFCONNECT alert type and shows the value assigned to the parameters by default. Note that the parameter ALERT_THRESHOLD is mandatory. All other parameters are optional. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 60 RFCONNECT Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
ALERT_THRESHOLD	Number of reconnect errors above which an alert occurs	= Sign I, E	I
		= Opt: GT, GE, LT, LE	GT
		= Low: [a]	4
		= High:	
CHECKSYSTEM	System ID of the systems you are monitoring.	= Sign: I, E	I
		= Opt: EQ, CP	EQ
		= Low: <SID>	’ *’
		= High:	

a. Specify this parameter as a number; otherwise the monitor ends with a dump.

In The Default RFCONNECT Configuration, an event generating an alert occurs if the alert threshold of four RFC-connect errors is exceeded for the specified target system.

The Default RFCONNECT Configuration

```
AlertMonFun =ALL =ALL  =ALL =ALL =TRANSPORT =1\
=WARNING    =RfcConnect  =R3_Transport\
=RFCCONNECT  =CHECKSYSTEM =I =CP =* =\
=ALERT_THRESHOLD  =I =GT =4 =
```

TPTEST

TPTEST is a snapshot alert type for `r3montra`, the SPI for SAP’s Transport Monitor. Snapshot alert types take a picture of the System at the moment the monitor runs. `r3montra` generates an alert if the number of TPTEST errors to the target system exceeds a defined threshold.

Table 61 on page 163 lists the parameters that you can use to configure the TPTEST alert type and shows the value assigned to the parameters by default. Note that the parameter ALERT_THRESHOLD is mandatory. All other parameters are optional. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 61 TPTEST Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
ALERT_THRESHOLD	Number of TPTEST errors above which an alert occurs	= Sign I, E	I
		= Opt: GT, GE, LT, LE	GT
		= Low: [a]	4
		= High:	
CHECKSYSTEM	ID of the System which you are testing or monitoring.	= Sign: I, E	I
		= Opt: EQ, CP	EQ
		= Low: <SID>	' '
		= High:	

a. Specify this parameter as a number; otherwise the monitor ends with a dump.

In The Default TPTEST Configuration, an event generating an alert occurs if the alert threshold of four TPTEST errors is exceeded for the specified target system.

The Default TPTEST Configuration

```
AlertMonFun  =ALL  =ALL  =ALL =ALL =TRANSPORT =1\
=WARNING    =TpTest      =R3_Transport\
=TPTEST    =CHECKSYSTEM    =I  =EQ =<SID> =\
=ALERT_THRESHOLD=I  =GT  =4  =
```

r3monupd: The Update Monitor

The update alert monitor identifies and reports the following update conditions:

- The update process is *in*active
- Update-process errors

`r3monupd` monitors the status of both active updates and updates that have been stopped by a SAP user or by the System. The alert monitor `r3monupd` references update errors and update status in SAP NetWeaver transaction **`SM13`**.

Note that, if you use standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The `r3monupd` monitor is of type *snapshot*. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The update monitor has the following alert types.

- UPDATE_ACTIVE

  Get information about the status of update processes and sends an alert if a process is not active.

- UPDATE_ERRORS_EXIST

  Get information about update processes that have errors.

File Locations

The `r3monupd` monitor uses the files listed in this table.

Table 62 r3monupd Files

File	Description
`r3moncol(.exe)`	Collector executable for the update monitor
`r3monupd.cfg`	Configuration file for the update monitor.
r3monupd.log	Trace file for storing trace data.

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The `r3monupd` monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert collector monitors share the same format; the only difference is that the name of the configuration file must vary to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The `r3monupd` monitor uses the command-line parameters described in Table 22 on page 102. The command-line parameters for all the alert collector monitors share the same format: the only difference is that the name of the configuration file must vary to match each specific monitor for both the `-cfgfile` and `-trace` parameters as indicated in Table 22 on page 102.

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99.

Configuring Update-Monitor Alert Types

No parameters are used to configure alert types for `r3monupd`, the SPI for SAP's update monitor. You do not need to edit or customize the configuration file.

UPDATE_ACTIVE

UPDATE_ACTIVE is an alert type for `r3monupd`, the SPI for SAP's Update Monitor. `r3monupd` generates an alert if the UPDATE task is inactive. The following example illustrates the default configuration for the UPDATE_ACTIVE alert type.

In The Default UPDATE_ACTIVE Configuration, an event generating an alert occurs if any update is stopped.

The Default UPDATE_ACTIVE Configuration

```
AlertMonFun    =ALL =ALL =ALL =ALL =UPDATE   =1\
=CRITICAL    =UpdActive      =R3_Update  =UPDATE_ACTIVE
```

UPDATE_ERRORS_EXIST

UPDATE_ERRORS_EXIST is an alert type for `r3monupd`, the SPI for SAP's Update Monitor. `r3monupd` generates an alert if any update errors exist. The following example illustrates the default configuration for the UPDATE_ERRORS_EXIST alert type.

In The Default UPDATE_ERRORS_EXIST Configuration on page 165, an event generating an alert occurs if any update error occurs.

The Default UPDATE_ERRORS_EXIST Configuration

```
AlertMonFun    =ALL =ALL =ALL  =ALL =UPDATE =1\
=CRITICAL  =UpdError  =R3_Update  =UPDATE_ERRORS_EXIST
```

r3monusr: The SAP-User Monitor

The SAP-user alert monitor `r3monusr` identifies and reports the number of logged-in users. The check is performed for each application server. A very high number of users could indicate that performance problems might occur. The alert can then be used to decide whether it is necessary to ask or even force users to log out.

The alert monitor `r3monusr` references the SAP NetWeaver transaction **`SM04`**.

Note that, if you use standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The `r3monusr` monitor is of type *snapshot*. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The SAP-user monitor has only one alert type:

USER_LOGGEDIN_MAX

Define the maximum number of logged in users.

File Locations

The `r3monusr` monitor uses the files listed in this table.

Table 63 r3monusr Files

File	Description
`r3moncol(.exe)`	Collector executable for the user monitor
`r3monusr.cfg`	Configuration file for the user monitor.
r3monusr.log	Trace file for storing trace data.

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The `r3monusr` monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert collector monitors share the same format, the only difference being that the name of the configuration file must vary to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The `r3monusr` monitor uses the command-line parameters described in Table 22 on page 102. The command-line parameters for all the alert collector monitors share the same format: the only difference is that the name of the configuration file must vary to match each specific monitor for both the `-cfgfile` and `-trace` parameters as indicated in Table 22 on page 102.

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

USER_LOGGEDIN_MAX

USER_LOGGEDIN_MAX is an alert type for `r3monusr`, the SPI for SAP's SAP-user monitor. `r3monusr` generates an alert if the maximum number of SAP users exceeds a defined threshold. Table 64 on page 167 lists the parameters that you can use to configure the USER_LOGGEDIN_MAX alert type and shows the value assigned to the parameters by default. The configuration of the parameter MAX is mandatory.

The APSERVER parameter allows you to set the application-server- dependent monitors, r3monwpa, r3monusr, and r3monoms to monitor a specific application server. You need to configure APSERVER in the following manner, where *<hostname>* is the name of the application server you are monitoring as it appears in the list of application servers displayed in transaction **SM51**:

```
=APSERVER  =I =CP =<hostname>_<SID>_<Instance_Number> =
```

We also recommend that you explicitly define the host name of the SAP NetWeaver central instance whose application server(s) you want to specify with APSERVER, as illustrated in Specifying an Application Server on page 149.

Specifying an Application Server

```
AlertMonFun =<Central_Inst_Hostname> =ALL =ALL =ALL =USER =1 \
=WARNING =Login =R3_WP \
=USER_LOGGEDIN_MAX =MAX =I =GT =30 = \
=APSERVER =I =CP =hpdev01_MP3_00 =
```

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 64 USER_LOGGEDIN_MAX Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
APSERVER	Specifies the application server to monitor	= Sign: I, E	
		= Opt: CP	
		= Low : <*AppServer_ID*>	
		= High:	
MAX	The number of logged in users before an alert occurs. [a]	= Sign: I, E	I
		= Opt: GT, GE	GT
		= Low:	5
		= High:	

a. You must specify the parameter value as a number, otherwise the monitor ends with a dump.

In The Default USER_LOGGEDIN_MAX Configuration, an event generating an alert occurs if the number of users logged in exceeds thirty.

The Default USER_LOGGEDIN_MAX Configuration

```
AlertMonFun  =ALL =ALL =ALL =ALL =USER =1\
=WARNING    =Login   =R3_User\
=USER_LOGGEDIN_MAX =MAX =I   =GT  =30  =
```

r3monwpa: The Work-Process Monitor

The work-process alert monitor `r3monwpa` references the SAP NetWeaver transaction **`SM50`** and reports the following conditions for work processes running on each of the application servers, which the SPI for SAP is monitoring:

- Reports the number of *running* work processes for each work-process type configured in the profile of the current operation mode
- Reports the number of *waiting* work processes for each work-process type configured in the profile of the current operation mode
- Compares the number of *active* work processes with the number of *configured* work processes (of the same work process type) in the profile of the current operation mode.
- Checks the status of the work processes, as follows:
  - **D (Debug)**

    No processes run on live systems
  - **P (Private)**

    Processes run using maximum available system resources.
  - **R (No Restart)**

    Failed processes do not restart, which means that dependent jobs also fail.

The work-process monitor `r3monwpa` can only monitor alerts from an `enqueue` work process that is part of a central instance; it cannot monitor the alerts from an `enqueue` work process belonging to a stand-alone `enqueue` server. To monitor stand-alone `enqueue` work processes, use the `r3monal` monitor to check for SAP CCMS alerts generated by the `enqueue` server. For more information about using `r3monal` to monitor a stand-alone `enqueue` server, see r3monal: Monitoring Stand-alone Enqueue Servers on page 59.

Note that, if you use standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration and will not allow you to save a file, which contains configuration errors. For more information about the validation tool and the messages it generates when it encounters a problem, see Validating the Alert-Collector Configuration Files on page 110 and Understanding Configuration-File Error Messages on page 110.

Monitor Type

The `r3monwpa` monitor is of type *snapshot*. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Alert Types

The work-process alert monitor has the following alert types.

- WP_AVAILABLE

  The WP_AVAILABLE alert type defines alert conditions for the number of expected work processes running.
- WP_IDLE

  The WP_IDLE alert type defines alert conditions for the number of idle work processes waiting.

- WP_CHECK_CONFIGURED

  The WP_CHECK_CONFIGURED alert type defines alert conditions for comparing the actual number of running work processes with the number of configured work processes in the profile of the current operation mode. The monitor check only compares work processes of the same type.

- WP_STATUS

  The WP_STATUS alert type defines alert conditions for work processes which the monitor finds in a problematic state, for example: D (Debug), P (Private) or R (No Restart).

File Locations

The `r3monwpa` monitor has the files listed in this table.

Table 65 r3monwpa Files

File	Description
`r3moncol(.exe)`	Collector executable for the WorkProcess monitor
`r3monwpa.cfg`	Configuration file for the WorkProcess monitor.
r3monwpa.log	Trace file for storing trace data.

The alert-collector monitors do not write history information to a specific history file. For more information, see Alert-Collector Monitor History on page 98.

Environment Variables

The `r3monwpa` monitor uses the environment variables described in Table 21 on page 102. The environment variables for all the alert collector monitors share the same format: the only difference is that the name of the configuration file must vary to match each specific monitor as indicated in Table 21 on page 102.

Command-Line Parameters

The `r3monwpa` monitor uses the command-line parameters described in Table 22 on page 102. The command-line parameters for all the alert collector monitors share the same format, the only differences being that the name of the configuration file must vary to match each specific monitor for both the `-cfgfile` and `-trace` parameters as indicated in Table 22 on page 102

Remote Monitoring

For more information about configuring the alert-collector monitors to monitor another SAP System remotely, see Remote Monitoring with the Alert-Collector Monitors on page 103.

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99.

Configuring Work-Process Monitor Alert Types

This section helps you to configure alert types for `r3monwpa`, the SPI for SAP's work-process monitor. Note the general rules below concerning the use of the *exclude* and *include* parameter values; the rules are of particular importance for these alert types.

Parameter Values

This section describes how the SPI for SAP interprets *include* and *exclude* parameter values for an alert type entry. The SPI for SAP compares values in *different* parameters using 'and'; the SPI for SAP compares values in the *same* parameter as follows.

- **Include:** use 'or' to compare the parameters
- **Exclude:** use 'and' to compare the parameters

The SPI for SAP evaluates include values before exclude values, as shown in the Table 66.

Table 66 Comparing Include and Exclude Conditions for the Same Parameter

Select Options	Alert Type: WP_AVAILABLE Example Configuration of Select Options	Comparison
1	=DIA =I =BT =50 =100 =OPMODE =I =CP =DAY	OR
2	=DIA =I =GT =5 =OPMODE =I =CP =NIGHT	OR
3	=DIA = E =LT =60	AND

WP_AVAILABLE

WP_AVAILABLE is an alert type for `r3monwpa`, the SPI for SAP's work-process monitor. `r3monwpa` generates an alert if the number of running work processes for each, selected work-process type is outside the specified maximum (or minimum) threshold.

Table 67 on page 171 lists the parameters that you can use to configure the WP_AVAILABLE alert type and shows the value assigned to the parameters by default. The configuration of the parameters listed for the WP_AVAILABLE alert type is mandatory. You must specify all threshold parameters as a number otherwise the monitor ends with a dump.

The APSERVER parameter allows you to set the application-server- dependent monitors, `r3monwpa`, `r3monusr`, and `r3monoms` to monitor a specific application server. You need to configure APSERVER in the following manner, where *<hostname>* is the name of the application server to monitor as it appears in the list of application servers displayed in transaction `SM51`:

```
=APSERVER  =I =CP =<hostname>_<SID>_<Instance_Number> =
```

We also recommend that you explicitly define the host name of the SAP NetWeaver central instance whose application server(s) you want to specify with APSERVER, as illustrated in the Specifying an Application Server.

Specifying an Application Server

```
AlertMonFun =<Centr_Instance_Hostname> =ALL =ALL =ALL =WP =1 \
=WARNING   =Availability  =R3_WP   \
=WP_AVAILABLE =DIA   =I  =GT  =50   = \
              =APSERVER  =I =CP =hpdev01_MP3_00 =
```

The remainder of this section describes the specific configuration requirements for this alert monitor. If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 67 WP_AVAILABLE Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
APSERVER	specifies an application server to monitor	= Sign: I, E	
		= Opt: CP	
		= Low : <*AppServer_ID*>	
		= High:	
BTC	Threshold for batch work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low: <*number*>	
		= High:	
DIA	Threshold for dialog work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low: <*number*>	
		= High:	
ENQ	Threshold for enqueue work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low: <*number*>	
		= High:	
OPMODE	Defines the operation mode for this parameter [a]	= Sign I, E	I
		= Opt: CP, EQ	EQ
		= Low: <operation_ mode>	current
		= High:	
SPO	Threshold for spool work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low: <*number*>	
		= High:	

Table 67 WP_AVAILABLE Configuration Parameters (cont'd)

Parameter Name	Description	Query Conditions	Default Value
UPD	Threshold for update work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low: <*number*>	
		= High:	
UP2	Threshold for update2 work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low: <*number*>	
		= High:	

a. A critical alert occurs if you specify a non-existent mode.

In The Default WP_AVAILABLE Configuration, an event generating an alert occurs if the number of available Dialog work processes is less than fifty.

The Default WP_AVAILABLE Configuration

```
AlertMonFun   =ALL   =ALL  =ALL  =ALL =WP  =1\
=WARNING   =Availability  =R3_WP\
=WP_AVAILABLE    =DIA   =I    =LT  =50   =
```

Check that the work-process types you want to monitor with `r3monwpa` are correctly configured in the SAP instance profile.

The `r3monwpa` monitor can only monitor work-process types that are configured in the SAP instance profile. If the DIA work-process type is not configured in the SAP instance profile (or "`rdisp/wp_no_dia = 0`"), then *no* DIA work processes are started. Since zero (0) DIA work processes is clearly less than the minimum allowed (50) specified in the default configuration for the WP_AVAILABLE alert type shown in The Default WP_AVAILABLE Configuration, this would, under normal circumstances, generate an alert.

However, if the DIA work-process type is not configured in the SAP instance profile, `r3monwpa` cannot monitor the number of DIA work processes that are running at any given point in time and, as a consequence, does not generate an alert. You can check discrepancies between the SAP instance profile and the `r3monwpa` configuration file with the alert type WP_CHECK_CONFIGURED on page 175.

WP_IDLE

WP_IDLE is an alert type for `r3monwpa`, the SPI for SAP's work-process monitor. `r3monwpa` generates an alert if the number of waiting work processes for each, selected work-process type is outside the specified max (or min) threshold.

Table 68 on page 173 lists the parameters that you can use to configure the WP_IDLE alert type and shows the value assigned to the parameters by default. The configuration of the parameters for the WP_IDLE alert type is mandatory. You must specify all threshold parameters as a number otherwise the monitor ends with a dump.

The APSERVER parameter allows you to set the application-server- dependent monitors, r3monwpa, r3monusr, and r3monoms to monitor a specific application server. You need to configure APSERVER in the following manner, where *<hostname>* is the name of the application server to monitor as it appears in the list of application servers displayed in transaction SM51:

```
=APSERVER  =I =CP =<hostname>_<SID>_<Instance_Number> =
```

It is also recommended to define explicitly the host name of the SAP NetWeaver central instance whose application server(s) you want to specify with APSERVER, as illustrated in the Specifying an Application Server.

Specifying an Application Server

```
AlertMonFun =<Centr_Instance_Hostname> =ALL =ALL =ALL =WP =1 \
=WARNING   =Idle  =R3_WP   \
=WP_IDLE   =BTC   =I  =GT  =20   = \
          =APSERVER  =I =CP =hpdev01_MP3_00 =
```

If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 68 WP_IDLE Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
APSERVER	specifies an application server to monitor	= Sign: I, E	
		= Opt: CP	
		= Low : <*AppServer_ID*>	
		= High:	
BTC	Threshold for batch work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low: <*number*>	
		= High:	
DIA	Threshold for dialog work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low: <*number*>	
		= High:	
ENQ	Threshold for enqueue work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low:	
		= High:	

Table 68 WP_IDLE Configuration Parameters (cont'd)

Parameter Name	Description	Query Conditions	Default Value
OPMODE	Defines the operation mode for this parameter.[a]	= Sign I, E	I
		= Opt: CP, EQ	EQ
		= Low: <*operation_mode*>	current
		= High:	
SPO	Threshold for spool work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low: <*number*>	
		= High:	
UPD	Threshold for update work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low: <*number*>	
		= High:	
UP2	Threshold for update 2 work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low: <*number*>	
		= High:	

a. If a non-existent mode is specified, a critical alert occurs.

In The Default WP_IDLE Configuration, an event generating an alert occurs if the number of idle Dialog work processes is less than ten.

The Default WP_IDLE Configuration

```
AlertMonFun   =ALL =ALL =ALL  =ALL =WP =1\
=WARNING   =Idle  =R3_WP\
=WP_IDLE  =DIA  =I  =LT =10  =
```

Check that the work-process types you want to monitor with `r3monwpa` are correctly configured in the SAP instance profile.

The `r3monwpa` monitor can only monitor work-process types that are configured in the SAP instance profile. If the DIA work-process type is not configured in the SAP instance profile (or "`rdisp/wp_no_dia = 0`"), then *no* DIA work processes are started. Since zero (0) DIA work processes is clearly less than the minimum allowed (10) specified in the default configuration for the WP_IDLE alert type shown in The Default WP_IDLE Configuration, this would, under normal circumstances, generate an alert.

However, if the DIA work-process type is not configured in the SAP instance profile, r3monwpa cannot monitor the number of DIA work processes that are running at any given point in time and, as a consequence, does not generate an alert. You can check discrepancies between the SAP instance profile and the r3monwpa configuration file with the alert type WP_CHECK_CONFIGURED on page 175.

WP_CHECK_CONFIGURED

WP_CHECK_CONFIGURED is an alert type for r3monwpa, the SPI for SAP's work-process monitor. The WP_CHECK_CONFIGURED alert type makes a comparison between the actual number of running work processes and the number of configured work processes in the profile of the current operation mode. Note that the monitor only compares work processes of the same type, for example: DIA, BTC. Table 69 on page 175 lists the parameters that you can use to configure the WP_CHECK_CONFIGURED alert type and shows the value assigned to the parameters by default.

The APSERVER parameter allows you to set the monitors, r3monwpa, r3monusr, and r3monoms to monitor a specific application server. You need to configure APSERVER in the following manner, where *<hostname>* is the name of the application server to monitor as it appears in the list of application servers displayed in transaction SM51:

```
=APSERVER  =I =CP =<hostname>_<SID>_<Instance_Number> =
```

We also recommend that you explicitly define the host name of the SAP NetWeaver central instance whose application server(s) you want to specify with APSERVER, as illustrated in the Specifying an Application Server.

Specifying an Application Server

```
AlertMonFun =<Centr_Instance_Hostname> =ALL =ALL =ALL =WP =1 \
=WARNING   =Check  =R3_WP   \
=WP_CHECK_CONFIGURED \
              =APSERVER  =I =CP =hpdev01_MP3_00 =
```

If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 69 WP_CHECK_CONFIGURED Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
APSERVER	specifies an application server to monitor	= Sign: I, E	
		= Opt: CP	
		= Low: <*AppServer_ID*>	
		= High:	

In Default WP_CHECK_CONFIGURED Configuration, r3monwpa generates an alert if the number of running work processes does not match the number of configured work processes for a given work-process type.

Default WP_CHECK_CONFIGURED Configuration

```
AlertMonFun =ALL    =ALL  =ALL =ALL =WP =1\
=WARNING  =Check  =R3_WP\
=WP_CHECK_CONFIGURED  \
              =APSERVER  =I =CP =ALL =
```

WP_STATUS

WP_STATUS is an alert type for `r3monwpa`, the SPI for SAP's work-process monitor. WP_STATUS defines alert conditions for work processes which the monitor finds in a problematic state, for example: D (Debug), P (Private), or R (No Restart). `r3monwpa` generates an alert if the work processes running in the SAP Systems you are monitoring with the SPI for SAP match the conditions defined in the parameters below. The configuration of the parameter below is optional.

The APSERVER parameter allows you to set the application-server- dependent monitors, `r3monwpa`, `r3monusr`, and `r3monoms` to monitor a specific application server. You need to configure APSERVER in the following manner, where *<hostname>* is the name of the application server to monitor as it appears in the list of application servers displayed in transaction `SM51`:

```
=APSERVER  =I =CP =<hostname>_<SID>_<Instance_Number> =
```

We also recommend that you explicitly define the host name of the SAP NetWeaver central instance whose application server(s) you want to specify with APSERVER, as illustrated in the Specifying an Application Server.

Specifying an Application Server

```
AlertMonFun =<Centr_Instance_Hostname> =ALL =ALL =ALL =WP =1 \
=WARNING   =WP_Status  =R3_WP   \
=WP_STATUS =STATUS   =I  =GT  =30   = \
           =APSERVER  =I =CP =hpdev01_MP3_00 =
```

If you are unsure about the general configuration query rules which apply to all alert collector monitors, see Alert-Collector Monitor Query Conditions on page 99. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 19 on page 100.

Table 70 Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
APSERVER	Specifies an application server to monitor	= Sign: I, E	
		= Opt: CP	
		= Low: <*AppServer_ID*>	
		= High:	
STATUS [a]	The status which is monitored	= Sign: I, E	
		= Opt:	
		= Low: [b]	
		= High:	

a. Possible additional values: MAX_ENTRIES

b. Possible values: D=Debug, P=Private, R=Restart (no alert).

In The Default WP_STATUS Configuration, an event generating an alert occurs if the status of a running workprocess is *critical*. The Default WP_STATUS Configuration also shows how you can use `=MAX_ENTRIES` to define the number of work processes with a defined status that have to exist before the SPI for SAP generates a message.

The Default WP_STATUS Configuration

```
AlertMonFun     =ALL =ALL =ALL  =ALL =WP   =1\
                =CRITICAL   =WP_Status  =R3_WP\
                =WP_STATUS     =STATUS =I  =CP  =*   =
```

Monitoring the TemSe file

To save runtime costs, the SPI for SAP monitors the consistency of SAP's Temporary Sequential file (TemSe) not by means of one of the SPI for SAP alert monitors, but rather by means of a report you set up in SAP. However, you still need to assign the SPI for SAP `r3monaco` monitor to the managed nodes.

Monitor Type

The TemSe monitor is of type *snapshot*. One monitor run gathers only one value set. For more information, see Report Types for the Alert-Collector Monitors on page 97.

Report Description

The TemSe report references the SAP NetWeaver transaction **`SP12`**. Any inconsistency found in the TEMSE database is serious; you must use the log in **`SP12`** to correct the cause of the inconsistency, for example a disk failure.

Running the TemSe Monitor

To run the TemSe monitor, you need to set up a job in SAP NetWeaver which references a report named `/HPOV/ZHPSPIT1`. Note that you can only use the report with SAP version 4.6 and later.

To set up the report:

1. Login to SAP NetWeaver
2. Set up a job using transaction **`SM36`**
3. In the job, specify the following details:
   - the date on which the report should start
   - the frequency with which the report should run

5 Understanding Message Flow

This section describes how to use HPOMHPOM for Windows functionality and CCMS to control the flow of messages between SAP NetWeaver and HPOMHPOM for Windows.

In this Section

The information in this section describes how to control message flow between SAP NetWeaver and HPOM for Windows and includes the following topics:

- HPOM Message Customization on page 179

  Customize HPOM for Windows message policy conditions.

- Customizing CCMS Message Flow in SAP on page 182

  Use SAP NetWeaver features to control how CCMS alert monitors generate specific messages.

- SAP Solution-Manager Integration on page 186

  Use the `r3ovo2ccms` command to write HPOM for Windows messages directly into the CCMS tree, where they can be viewed and used by the SAP Solution Manager in the same way as any other SAP message alert. You can also use `r3monal` to forward messages directly from CCMS to HPOM for Windows.

- Monitoring CCMS Alerts in the CEN on page 193

  Monitor alerts and analyze data collected by the SAP central monitoring system (CEN).

The methods for setting thresholds in the CCMS monitor do not apply if you are using the new CCMS monitoring architecture, where thresholds can be set globally within SAP NetWeaver.

For details about the procedures outlined in these sections, refer to your SAP NetWeaver documentation and to the manuals supplied with HPOM for Windows.

HPOM Message Customization

With the aid of standard HPOM for Windows functionality, you can modify important aspects of the messages generated by the SPI for SAP monitors and, in addition, specify which of the generated messages you want displayed. This section provides information about the following tasks:

- **Setting up message views**

Use message filters to set up views that show you only those messages which fit specified criteria, for example; messages with the severity level “critical”. For more information, see Setting Up the Message Filters on page 180.

- **Changing severity levels**

  Change the severity level of messages. For more information, see Changing the Message Severity on page 181.

- **Suppressing messages**

  Suppress specific messages by setting a suppress condition in the `opcmsg` template. For more information, see the *HP Operations Manager Smart Plug-in for SAP Configuration Guide*.

Setting Up the Message Filters

By default, the HPOM for Windows console displays *active* messages generated on your managed nodes. However, you can modify the number and type of messages that are displayed so that only the most important messages appear. For example, you can filter messages by using any one or combination of the following criteria:

- **Application:**

  Filter messages according to the *application* message attribute, that is: the application responsible for sending the message

- **Message text:**

  Filter messages containing specific text

- **Object:**

  Filter messages according to the *object* message attribute that is: the HPOM for Windows object responsible for sending the message

- **Ownership:**

  Filter messages according to message ownership

- **Severity:**

  Filter messages according to the selected severity

- **Time:**

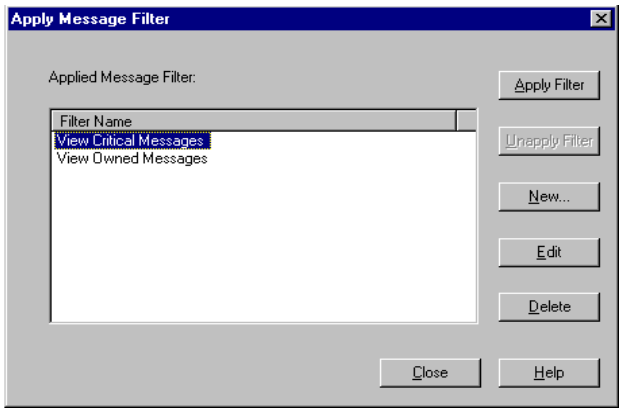
  Filter messages created at/before/since particular dates and times

- **Unmatched:**

  Filter messages that either do or do not match any of the message conditions or suppressed conditions defined in the policies deployed on the managed nodes.

Using message filters, you can set up simple or complex views which display specific messages. For example, if you want to display messages with a severity level of critical, you can define a filter that prevents HPOM for Windows displaying messages with all other severity levels.

Figure 10 Applying Message Filters



To define your customized message filter:

1 Select the managed node.

In the HPOM for Windows console, locate and right-click the managed node whose messages you want to filter, and select the following option from the menu that pops up:

Configure > Message Filter

2 Create a new message filter.

In the Apply Message Filter window which appears, click **New...**. The Filter Properties window appears.

3 Define the new message filter.

Use the Filter Properties window to define the filtering patterns to use. For example, if you want to filter the messages to display on the basis of message severity, use the Severity field in the General property sheet.

Click **OK** to save your filtering pattern(s).

4 Save and apply the filter.

In the Apply Message Filter window, click **Apply Filter**, and then click **Close**.

Changing the Message Severity

To change the severity of specific SAP NetWeaver-generated messages in the HPOM for Windows console:

1 Log on to HPOM for Windows as administrator.

2 In the details pane, locate and right-click the message whose severity attribute you want to change, and select the following option from the menu which pops up:

Change Severity >

3 Select the severity level you want from the pop-up menu, for example, Major. The message severity is immediately updated in the active-messages browser.

The user who changes a message's severity automatically becomes the message's owner: message ownership is indicated by a flag in the **S** column in the HPOM for Windows console.

Customizing CCMS Message Flow in SAP

SAP CCMS provides a range of features enabling you to allow or prevent the inclusion of specific messages in its alert monitor. This section includes information about the following topics:

Disabling Messages

To disable messages in SAP NetWeaver:

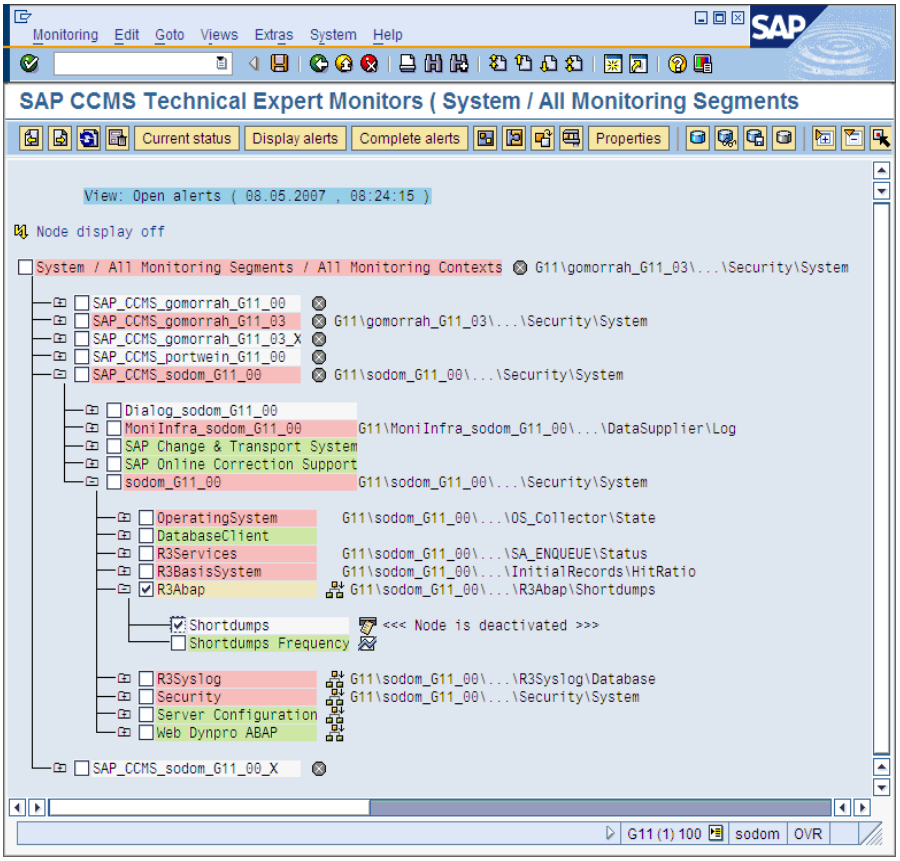
1. Browse to the following location using the SAP Easy-Access menu:

   Tools > CCMS > Control/Monitoring > Control Panel

   Alternatively, enter the following transaction code in the command field: **`RZ03`**
2. Select your SAP instance.
3. Click the Alert Monitor button in the menu bar to display the CCMS alert-monitor dialog. Alternatively, enter the following transaction code in the command field: **`RZ20`**
4. Select the following menu items from the SAP NetWeaver menu bar:

   Extras > activate maintenance function
5. In the list of monitors displayed, select the node or monitor-tree element whose messages you want to disable, for example: short- dump messages.

Figure 11 Deactivate Monitor Messages



6 To disable, for example, short-dump messages from the R3Abap monitor:

   a Click: **SAP CCMS Technical Expert Monitors -> System / All monitoring segments / all monitoring contexts -> SAP_CCMS_<host>_<SID>_<Instance number> -> <Host>_<SID>_<Instance number> -> R3Abap**

   b In the SAP NetWeaver menu bar, select the following menu items:

   Edit > Nodes(MTE) > Deactivate

   The selected item and the suppressed message type are now marked as “deactivated” in the SAP GUI.

7 Save your settings and return to the CCMS Monitor Sets screen.

8 Check the HPOM for Windows console. You should not receive any more short-dump messages.

Since disabling messages will result in inconsistencies with the settings previously defined in the SPI for SAP configuration file, you must only perform this operation if you do *not* want to have a central configuration.

Setting Thresholds for SAP CCMS Alert Monitor Messages

To set thresholds for SAP NetWeaver CCMS alert monitor messages:

1 Browse to the following location using the SAP Easy-Access menu:

Tools > CCMS > Control/Monitoring > Control Panel

Alternatively, enter the following transaction code in the command field: **RZ03**

2 Select the SAP NetWeaver instance (under Server name) for which you want to define a performance limit value.

Click the Alert Monitor button in the menu bar to display the CCMS alert-monitor dialog. Alternatively, enter the following transaction code in the command field: **RZ20**

3 Browse to the CCMS monitor set which contains the monitor whose alert thresholds you want to modify:

SAP CCMS Technical Expert Monitors > System / All monitoring segments / all monitoring contexts

4 To display alert details for a selected monitor:

a Click **Open alerts** in the tool bar

b Click **Display alerts** in the tool bar

Note that you can display alerts for a desired SAP instance or for all monitored instances.

c Select the alert whose details you want to display and click **Properties** in the tool bar

5 Click the **Performance Attribute** tab to display the threshold values for the selected CCMS alert.

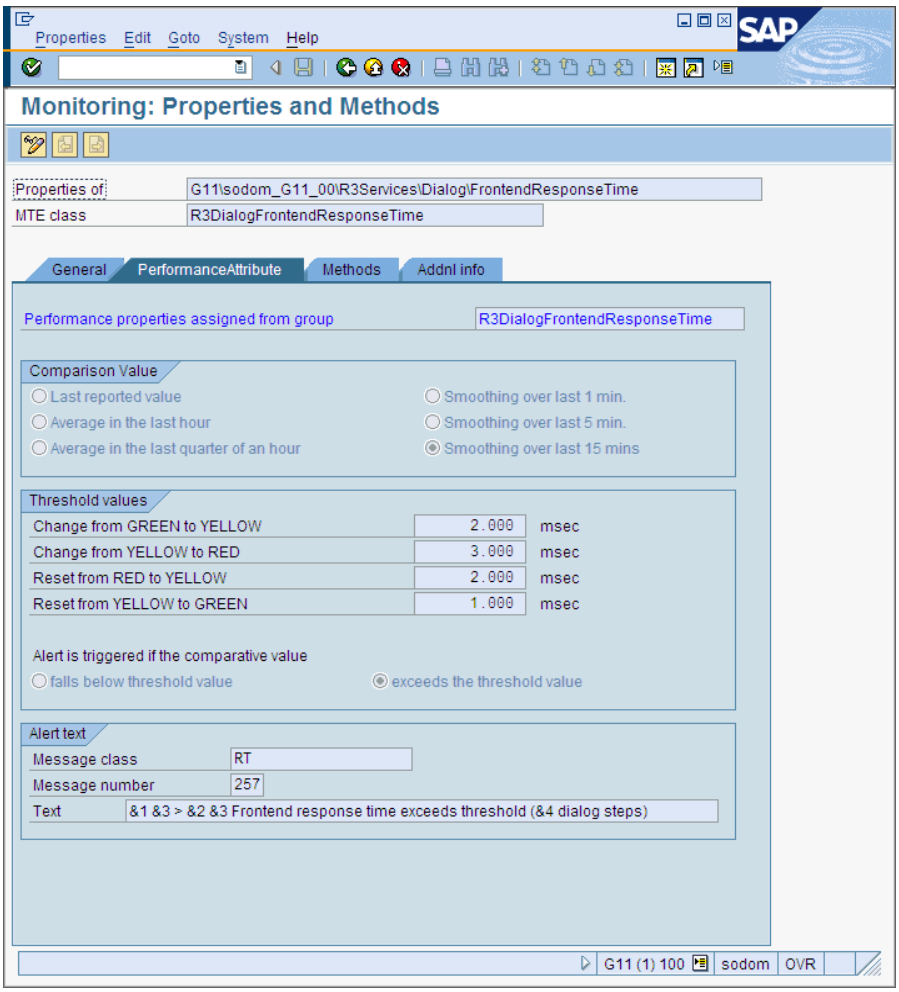
6 Click the **Display/Change** button (or the keyboard combination Shift+F6) and enter edit mode and change the threshold values as appropriate.

7 Save the changes to the threshold values; click the Save button in the menu bar, or use the following menu option:

Properties > Save

When the new threshold is reached, the SPI for SAP sends a warning or a critical Dialog Performance message (similar to Figure 12).

Figure 12 Performance Alert Thresholds



Obtaining a Message ID from the SAP NetWeaver Syslog File

Any messages recorded in the SAP NetWeaver system log file can be defined to trigger an alert in CCMS. This alert can be picked up and used to display an associated message in the HPOM for Windows console with instructions for any appropriate actions, which are required.

To obtain the message ID of a critical message:

1 Browse to the following location using the SAP Easy-Access menu to read the system log file:

Tools > Administration > Monitor > System Log

Alternatively, you can enter the following transaction code into the SAP NetWeaver command field: **SM21**

2 Double-click **System Log** to display system-log details in the System Log:Local Analysis screen.

You can apply time restrictions to limit the contents of the `syslog` file to the currently relevant entries.

3 Click **Reread System Log** to display the system log file of your SAP NetWeaver system.

4 Double-click the message that you want to use to trigger an alert. The system displays details of the selected message.

5 Make note of the message ID including group (for example: AB) and number (for example: 0); AB0 indicates a run-time error (RFC_NO_AUTHORITY).

6 To display the ID numbers of all SAP NetWeaver syslog messages, enter the transaction code **SE92** into the SAP NetWeaver command field and click **All numbers**.

7 Use the ID number to set up a filter in the SPI for SAP `r3monal.cfg` configuration file, for example:

```
# Syslog filtering
#-------------------------------------------------------
# Alert Classes  SAP     SAP      SyslogId     Enabled=1
#                System  Number   From    To   Disabled=0

AlerMonSyslog    =ALL    =ALL    =AB0   =AB1    =1
-------------------------------------------------------
```

SAP Solution-Manager Integration

The information in this section explains how you can set up the SPI for SAP to enable bi-directional communication between the SAP Solution Manager and HPOM for Windows. With the SPI for SAP's Solution-Manager integration, you can configure the SPI for SAP to inform HPOM for Windows when a Solution Manager business process fails: you can also set up the SPI for SAP in such a way as to enable it to populate the CCMS tree with managed objects from HPOM for Windows, for example; by means of an automatic or operator-initiated action attached to a message condition in a policy. The information in this section is split into the following topics:

Pre-requisites

If you want to take advantage of the SPI for SAP's Solution-manager integration, note that the target system, that is; the SAP server to which the SPI for SAP writes the CCMS alerts, must meet the following pre-requisites:

- Satellite Systems that are monitored by the Solution Manager must have SAP Version 4.6 or higher
- The SPI for SAP supports the BC-XMW interface for releases 6.20 and 6.40 of the SAP_BASIS package.
  - Release 6.40:

    The BC-XMW interface is available and fully supported with the initial support package; no additional support packages are required.

— Release 6.20:

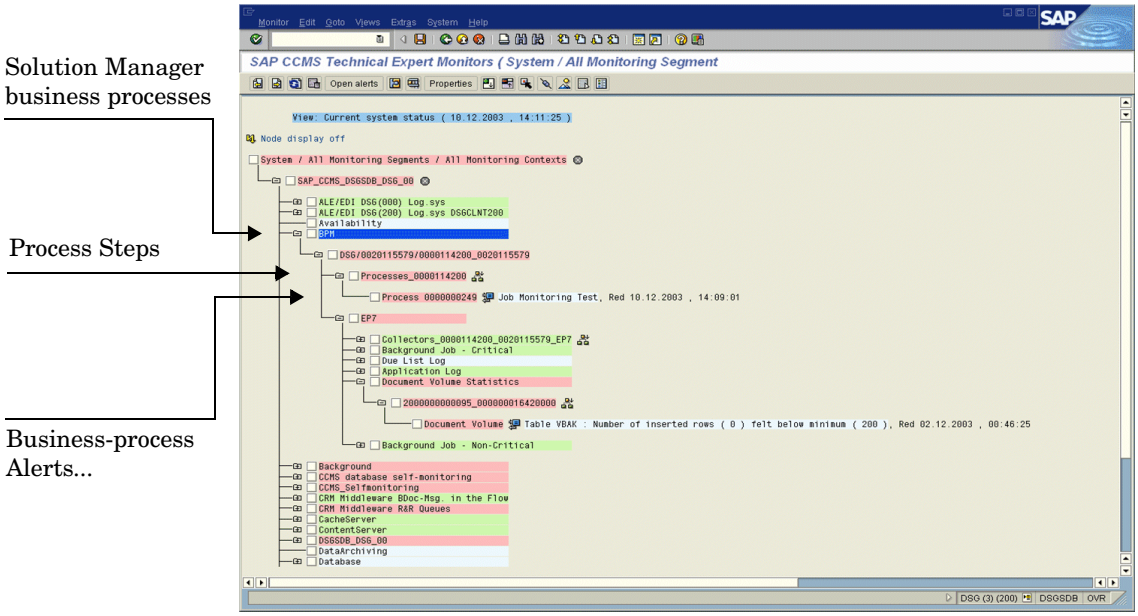
Support package 29 is required for full support of the BC-XMW interface. According to SAP, earlier SP levels will work, but the XMW interface designation will not be recognized.

- Have a look at SAP notes 645353 and 608384, too.

Integration Overview

The SPI for SAP's Solution-manager integration uses the CCMS XMW and XAL interfaces to improve communication between SAP and HPOM for Windows. Using the CCMS interfaces, the SPI for SAP ensures that the power of both SAP and HPOM for Windows can be used to enhance and improve the information available to system administrators in both areas.

Figure 13 Choosing CCMS Alerts to Monitor



For example, you can now configure the SPI for SAP to write directly to CCMS and populate the CCMS tree with messages and alerts, which are discovered by HPOM for Windows and relate to problems not normally of particular interest to SAP, such as hardware and network performance. Conversely, Figure 13 on page 187 shows how you can use the Solution-manager integration to monitor specific CCMS alerts and, by linking the generated HPOM for Windows messages to a defined service ID, monitor the status of specific services. In this way, it is possible to ensure not only that HPOM for Windows knows as soon as a Solution-manager business process fails but also that the status of the service associated with the business process you are monitoring is immediately reflected in the service map in the HP Service Navigator.

To summarize how the SPI for SAP's Solution-manager integration enhances communication in both directions between SAP and HPOM for Windows:

- **SAP -> HPOM for Windows**

  By defining message conditions for `r3monal`, the SPI for SAP's CCMS alert monitor, you can keep an eye on specific CCMS alerts, for example; the alerts you have assigned to Business Processes. For more information about setting up `r3monal`, the CCMS alert monitor, see Sending Messages from SAP to HPOM on page 188.

- **HPOM for Windows -> SAP**

You can attach an action to an HPOM for Windows message condition, which calls the `r3ovo2ccms` command and uses it to populate the CCMS tree with messages and objects monitored by HPOM for Windows. For more information about using the `r3ovo2ccms` command, see The r3ovo2ccms Command on page 191.

Sending Messages from SAP to HPOM

By defining message conditions for `r3monal`, the SPI for SAP's CCMS alert monitor, you can keep an eye on specific alerts in the CCMS tree. When the message condition for the specified CCMS alert matches, you can associate the HPOM for Windows message the condition generates with a known Service ID and, in this way, link the message directly to a service in the HPOM for Windows service tree. For more information about setting up `r3monal`, the CCMS alert monitor, see r3monal: the CCMS 4.x Alert Monitor on page 48.

To set up communication between the SAP Solution Manager and HPOM for Windows, you need to carry out the following high-level steps:

1. In SAP, open up the CCMS alert tree for the Solution-manager business process which you want to monitor.
2. Expand the CCMS alert tree and browse to the alerts associated with individual steps in the selected business process.

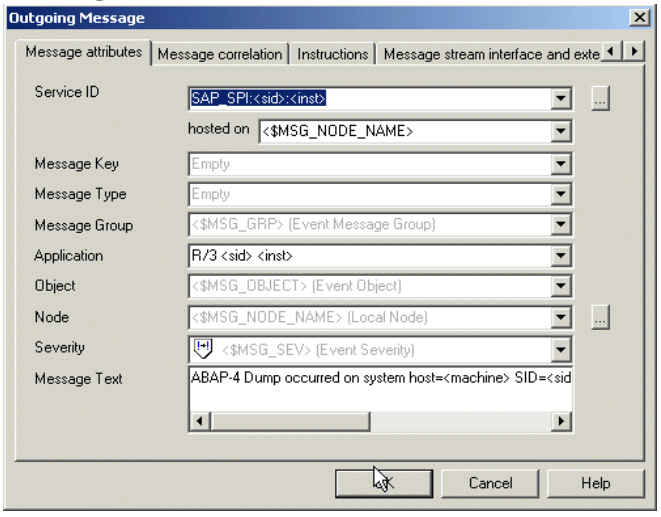
   If CCMS alerts are not already assigned to individual steps in the business process you want to monitor, you will have to use SAP to locate the CCMS monitor which generates the alerts you require (transaction RZ20) and then assign the alert(s) to the business-process step.

3. Assign the desired CCMS alert(s) to the step in the business process, which you want to link to service objects in HPOM for Windows.
4. If you want to link the HPOM for Windows messages to services in HPOM for Windows, you will need to assign a service ID at this point, too. The service ID must match the service name defined in the service-configuration file and take the following form:

   `SAP_SPI:<SID>:<service_instance_name>`

5. Remember to (re)deploy the SPI for SAP `opcmsg` policy with the new (or modified) conditions.

Figure 14 Linking Messages to Service IDs



Sending Messages from HPOM to SAP

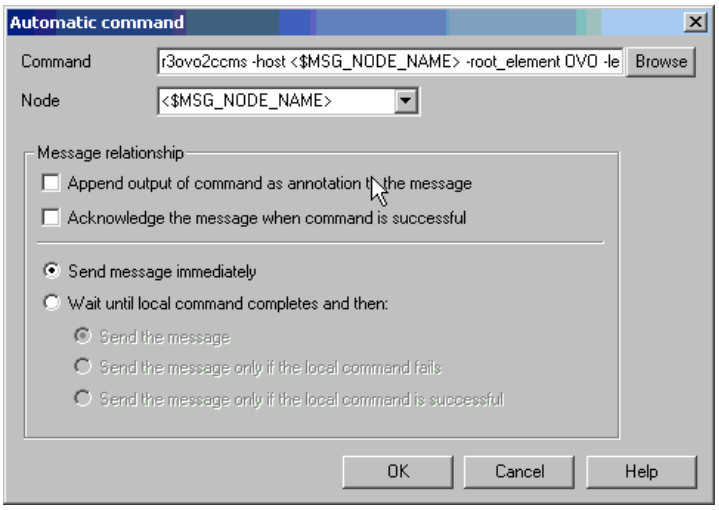
The first and most important thing you need to do is to inform HPOM for Windows which of the incoming HPOM for Windows messages it should forward to SAP and write into the CCMS tree. The message-forwarding task is triggered by means of an action attached to the policy rule, which generates the original message. The action you configure can be either automatic or operator-initiated. For more information about the command you use and the parameters and options that are allowed, see The r3ovo2ccms Command on page 191.

To set up an automatic action in an HPOM for Windows policy, follow the instructions below. Note that the names and titles of the windows, tabs, and property sheets can sometimes vary according to the type of policy you select. The example described here uses a performance-threshold policy.

1. In the console tree, locate and double-click the policy which generates the HPOM for Windows message you want to forward to SAP and write into the CCMS tree. In this example, we have chosen a performance monitor monitoring CPU load on the SAP server.
2. In the Measurement-threshold window which appears, click the **Threshold Levels** tab.
3. In the Threshold-levels tab, locate and double-click the rule which generates the message you want to forward to SAP. Note that you do not need to forward all messages. For example; the rule which generates a critical message is probably of more interest than the rules which generate messages with severity “warning” or “normal”.
4. In the Threshold-level window which appears, click the **Start Actions** tab.
5. In the Start Actions window, click the **Automatic Action** button.
6. In the Automatic Action window which appears, enter the `r3ovo2ccms` command in the command box along with the parameters and options you need to perform the desired action, including the location in the CCMS tree, where you want the message to appear. If the location you specify in the CCMS tree does not already exist, `r3ovo2ccms` creates it for you when it forwards the message to SAP. The default name for the root HPOM for Windows monitor tree is ZSAPSPI. Note that provided you do not alter the default settings, you do not need to supply an absolute path with the command. For more information about the `r3ovo2ccms` command, see The r3ovo2ccms Command on page 191.

   The Node text box defines the name of the node where the policy you are modifying is deployed and the `r3ovo2ccms` command runs. If you use the $MSG_NODE_NAME variable in conjunction with the `-host` option in the Command text box, the SPI for SAP assumes the name of the node associated with the original message. Assuming the RemoteMonitoring feature is enabled, this is true even for nodes, which the SPI for SAP is monitoring remotely.

Figure 15 Configuring an Automatic Action



7 The CCMS alert (Monitor-tree element or MTE) that `r3ovo2ccms` writes to the CCMS monitor tree must be assigned to a specific step in the business process, for example; “Create Invoice”, which you have defined in SAP Solution Manager.

a In SAP, enter the following transaction: **`/dswp`**

The `/dswp` transaction displays the following page:

Change Mode: Setup Business Process Monitoring

b Select the process step to which you want to assign the HPOM for Windows alert

c Manually enter the name of the CCMS monitor, which you want to assign to the business-process step.

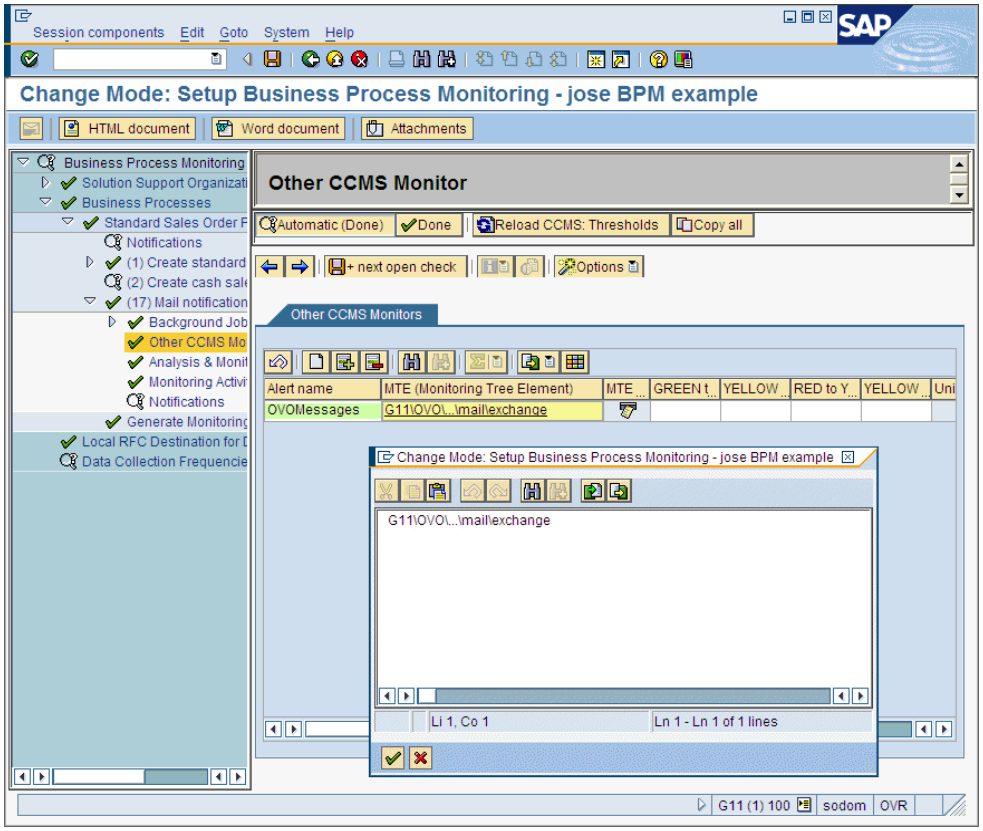
➤ The name of the monitor element that you enter must match the entry created by the `r3ovo2ccms` command, as it appears in the CCMS monitor tree. You do *not* need to include either the monitor context (ZSAPSPI) or the name of the CCMS Monitor *Set*, to which the monitor belongs.

8 Next, you need to create a CCMS monitor set, for example; HPOM, and generate a CCMS monitor, for example; SAPSPI, to host the alerts sent by the `r3ovo2ccms` command and make them visible to SAP users.

Then you can select the new monitor and, using the Change button, display a list of the CCMS alerts and alert groups, which you want to associate with the new monitor (SAPSPI) to make them visible to the Solution Manager. Scroll down the list of contexts displayed and select “ZSAPSPI”.

➤ The context ZSAPSPI is only visible for selection in the list of contexts displayed after the first HPOM for Windows message sent by the `r3ovo2ccms` command appears in the CCMS tree.

Figure 16 Assigning CCMS MTEs to Business Process Steps



The r3ovo2ccms Command

The mechanism which the SPI for SAP uses to forward HPOM for Windows messages to SAP and write them directly into the CCMS tree is the `r3ovo2ccms` command, which the SPI for SAP installs in the default HPOM for Windows actions directory on the HPOM for Windows managed node.

You can use the `r3ovo2ccms` command directly on the command line or start it either automatically (as an automatic action) or manually (as an operator-initiated action). If you want to use the `r3ovo2ccms` command in a configured action, you need to modify each policy that generates an HPOM for Windows message, which you want to forward to CCMS. The SPI for SAP uses the configured action to forward the HPOM for Windows message to SAP, where it will appear in the CCMS tree in the location defined by the parameters and options you specify.

The `r3ovo2ccms` command accepts the following parameters and parameter options, which are displayed in the command shell if no parameters are specified:

r3ovo2ccms -level1_element <*level1_element*> -level2_element <*level2_element*> -text <*text*> -host <*SAP_hostname*> [-root_element <*root element*>] [-sid <*SID*>] [-number <*SAP_instance_number*>] [-severity <*NORMAL* | *WARNING* | *CRITICAL*>]

Command Parameters

The `r3ovo2ccms` command accepts the following command parameters:

- `-level1_element <level1_element>`

This parameter identifies first-level branch in the CCMS tree structure

- `-level2_element <level2_element>`

  This parameter identifies the second-level branch in the CCMS tree structure

- `-text <text>`

  Descriptive text explaining the event/problem in more details.

- `-host <SAP_hostname>`

  The name of the SAP System on which the event/problem was originally detected by HPOM for Windows.

Optional Parameters

The following optional parameters can be used with the `r3ovo2ccms` command:

- `-root_element <root_element>`

  The name of the root element of the branch of the CCMS tree into which you want to insert the message. The default value is "ZSAPSPI".

- `-sid <SID>`

  The System ID (SID) of the SAP System, where the original event/problem was detected when found by HPOM for Windows.

- `-number <SAP_instance_number>`

  The instance number of the SAP System, where the original event/problem was detected by HPOM for Windows.

- `-severity <NORMAL|WARNING|CRITICAL>`

  The severity of the CCMS alert message. The default value is "CRITICAL"

Examples

The following example shows how you can use the `r3ovo2ccms` command to forward to SAP an HPOM for Windows message relating to a problem with CPU load on the SAP server “example” and write it directly into a defined location in the CCMS tree. You can configure the HPOM for Windows policy which generates the message to execute the command either automatically by means of an automatic action or manually by means of an operator-initiated action.

Writing HPOM for Windows Messages into the CCMS Tree

```
r3ovo2ccms -root_element  -level1_element Performance -level2_element CPU
-text "CPU load: bottleneck situation 90%" -host example
```

In the example above, the HPOM for Windows message will appear in the **`HPOM > Performance > CPU`** branch of the SAP CCMS tree when a critical problem with the CPU load occurs and is reported by the SPI for SAP. The problem to which the message relates was originally reported on the SAP server, “example”.

Monitoring CCMS Alerts in the CEN

If your SAP landscape includes multiple systems and numerous instances, you can reduce management overheads by using the SAP Computing Center Management System (CCMS) to monitor the entire landscape from one system, which SAP calls the central monitoring system (CEN), and then configuring the SPI for SAP to monitor the CEN. The SPI for SAP can then map alerts identified in the CCMS subsystem to messages that it sends to the HPOM for Windows console.

This section provides a brief overview of the things you need to look out for when considering the idea of using the SPI for SAP to monitor CCMS alerts in a SAP central monitoring system.

CEN-Integration Overview

The central monitoring system (CEN) is a single SAP system that you designate as the central point of control for CCMS alerts originating from all over the monitored SAP landscape. The CEN concept allows you to reduce the overhead of monitoring and managing multiple SAP systems by making essential information concerning problem alerts available in one, central location.

After you configure SAP to use the CEN for the central management of CCMS alerts, you can use the SPI for SAP's `r3monal` monitor to intercept the CCMS alerts destined for the CEN and use the alerts to generate messages, which it forwards to the HPOM for Windows console.

For more information about configuring SAP to use a central monitoring system (CEN) to manage CCMS alerts for a complete SAP landscape, see the SAP documentation; for more information about setting up the SPI for SAP to monitor CCMS alerts, see r3monal: the CCMS 4.x Alert Monitor on page 48.

Configuring the SAP CEN

The SPI for SAP supports the monitoring of CCMS alerts in a CEN provided you configure SAP to use the CEN as a central alert-monitoring location. Setting up the CEN as the central location for the collection and monitoring of alerts is straight forward but involves a number of steps. For example, you need to ensure (among other things) that you configure the required users, register and start the appropriate agents, and define the type of information you want to collect, such as: performance, statistical, or availability. The information in this section provides some pointers to what you need to consider when setting up the CEN for monitoring with the SPI for SAP.

For more information about configuring SAP to use a central monitoring system (CEN) to manage CCMS alerts for a complete SAP landscape, see the SAP documentation; you will need to find out in particular about the following high-level topics:

- SAP Central Monitoring System on page 193
- SAP ABAP Instances on page 195
- J2EE Instances on page 196

SAP Central Monitoring System

When you are setting up the SAP central monitoring system to collect, monitor, and analyze alert data, you need to consider the following important points:

- **Background Dispatching in the CEN**

To ensure the correct and timely startup of all data collection methods by the background process, you have to enable the monitoring architecture. Enable background dispatching both in the CEN and in all monitored ABAP systems, as illustrated in Figure 17 on page 195.

- **The CSMREG User**

  You need to create the CSMREG user both in the CEN and in all the ABAP systems you want the CEN to monitor remotely. CSMREG is a user with specific authorizations, which SAP uses to collect data from the remote systems and send it to the CEN. For more information about the configuring the CSMREG user, see the SAP documentation.

- **The CSMCONF file**

  The CSMCONF file is mandatory for the registration and startup of the CCMS agents; it contains all the connection data that you would otherwise have to supply during the normal registration process, for example: the system ID of the CEN, the client number, user name, and so on.

- **Data Collection and Analysis**

  If you want to use the CEN to collect, monitor, and analyze data from remote ABAP systems, you need to create two RFC destinations for each monitored ABAP system. CEN requires an entry in the CCMS alert monitor for each SAP system it monitors remotely.

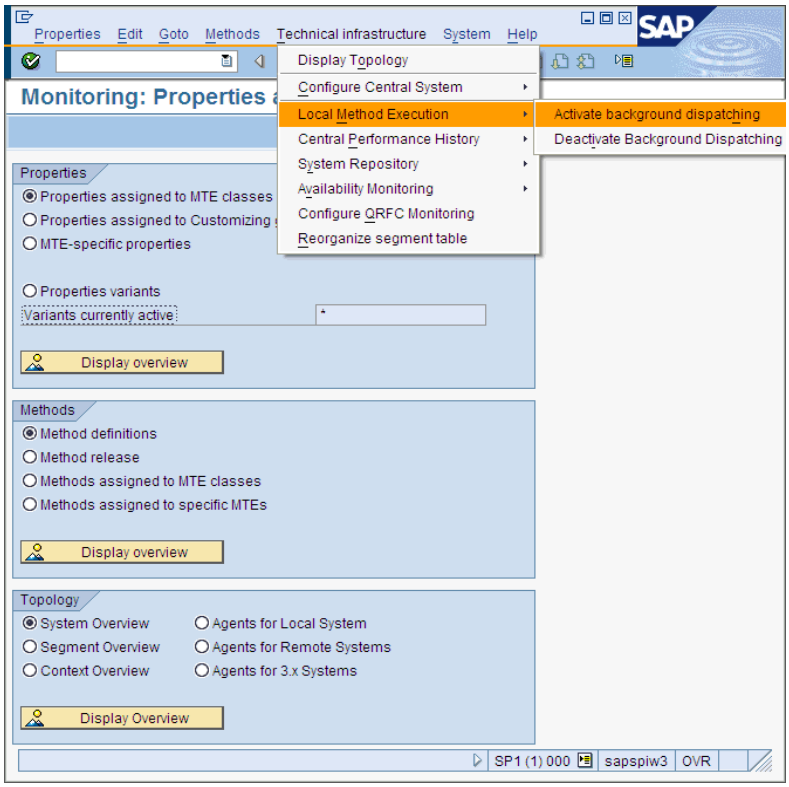
- **Statistical Workload Data**

  If you want to monitor the work-load statistics from the ABAP system in the CEN, use transaction **`ST03G`** (Global System Workload Analysis) to enter the RFC destination of each ABAP system in the workload monitor, as illustrated in Figure 18 on page 196.

- **The CCMSPING Availability Agent**

  Make sure the CCMS availability agent, CCMSPING, is available so that CCMS can monitor the status and availability of remote SAP systems. See the SAP documentation for more information about the pre-requisites for (and configuration of) the CCMSPING agent.

Figure 17 Enabling Background Dispatching



SAP ABAP Instances

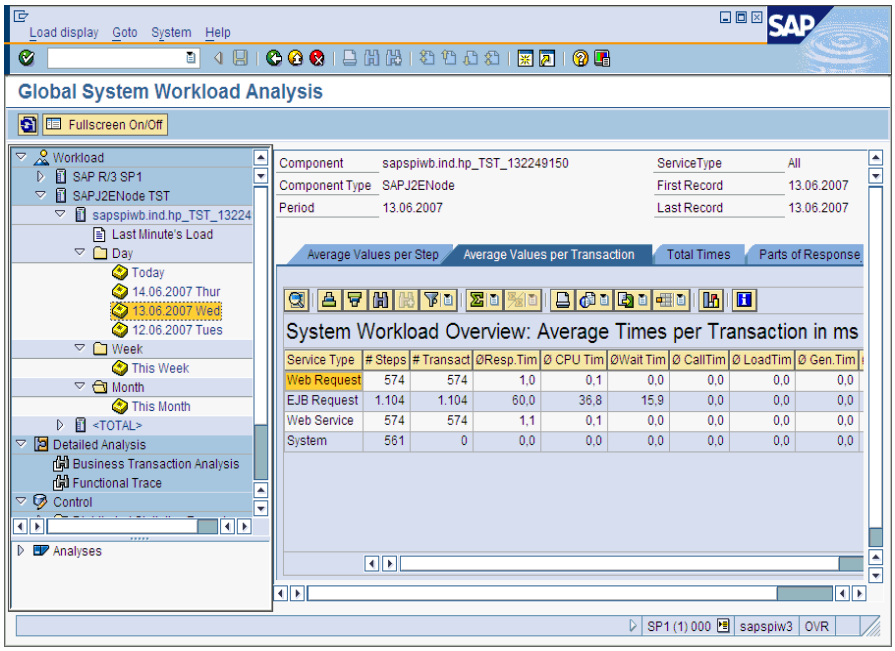
When you are setting up the SAP central monitoring system to collect, monitor, and analyze alert ABAP data, you need to consider the following important points for each monitored ABAP instance:

- **The SAPCCM4X Agent**

  To avoid communication problems when using the CEN to monitor an ABAP instance, you need to register the CCMS agent SAPCCM4X; registering the SAPCCM4X agent establishes a communication channel between the CEN and the monitored ABAP instances. Since the SAPCCM4X agent does not requires a free work process, it is not affected by any error states in any of the monitored ABAP instances.

  Note that you need to register the SAPCCM4X agent on each of the ABAP instances monitored with the CEN.

Figure 18 Monitoring ABAP Statistics in the CEN



J2EE Instances

When you are setting up the SAP central monitoring system to collect, monitor, and analyze alert data from SAP Java instances, you need to consider the following important points for each monitored J2EE instance:

- **The SAPCCMSR Agent**

  If you want to use CCMS to monitor J2EE instances with the CEN, you need to register the CCMS agent SAPCCMSR in the CEN since monitored data from the Java instances are transferred through the CCMS agent. Note that the installation of the J2EE engine configures the SAPCCMSR by default; you just need to register the SAPCCMSR agent with CEN for each J2EE instance and start the agent.

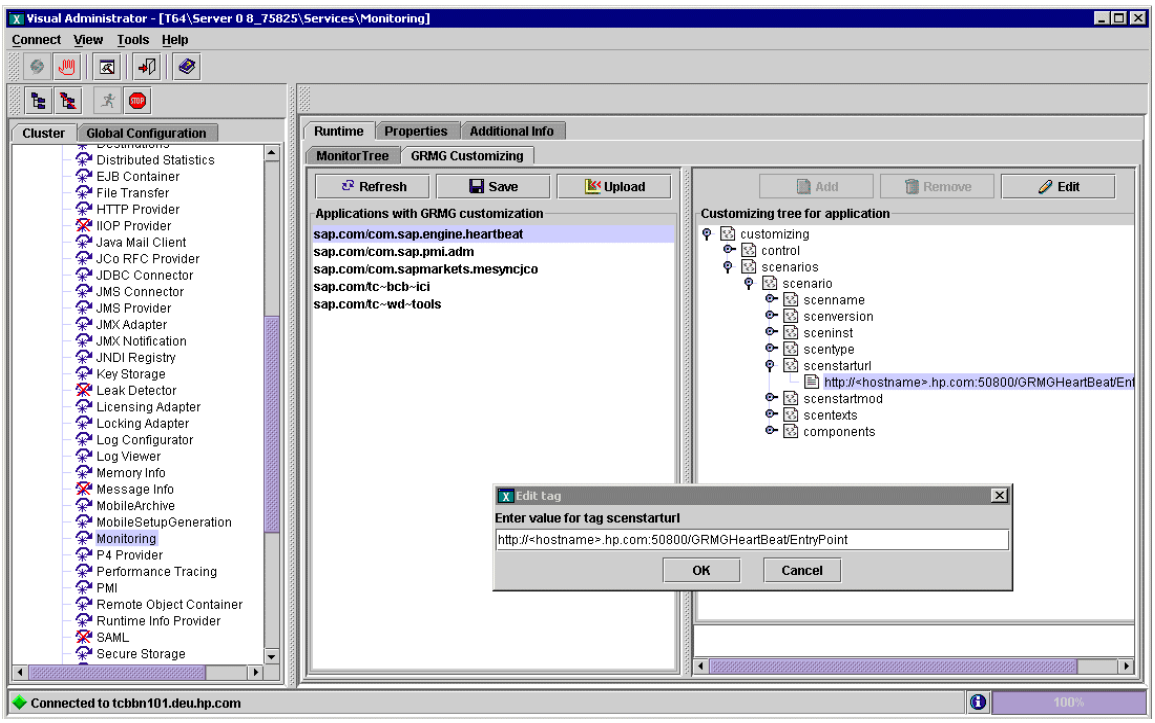
- **Java DSRs in the CEN**

  You can configure the global workload monitor to display distributed statistical records (DSR) for Java instances in the CEN. Figure 18 on page 196 shows the output for the Global System Workload Analysis transaction.

- **Availability monitoring with GRMG**

  To monitor the availability of a J2EE instance in SAP, you need to customize the configuration files for the General Request and Message Generator (GRMG) and upload the modified configuration files to the CCMS agent; the J2EE engine's Visual Administrator displays example XML files that are available for modification and upload to CCMS, as illustrated in Figure 19 on page 197. You can also use the transaction GRMG to display a list of active GRMG configuration scenarios that are available in the SAP central monitoring system.

Figure 19 Uploading the GRMG Configuration File to CCMS



Configuring the SPI for SAP

After you configure SAP to use the CEN for the central management of CCMS alerts, you can use the SPI for SAP's `r3monal` monitor to intercept the CCMS alerts destined for the CEN and generate a message that it forwards to the HPOM for Windows console.

For more information about configuring SAP to use a central monitoring system (CEN) to manage CCMS alerts for a complete SAP landscape, see the SAP documentation; for more information about setting up the SPI for SAP to monitor CCMS alerts, see r3monal: the CCMS 4.x Alert Monitor on page 48.

The following list provides a high-level overview of the steps you need to perform to configure the SPI for SAP to monitor CCMS alerts in the CEN:

1. Install the SPI for SAP on the SAP system you assign as the central monitoring system (CEN).

   Note that if you are already using the SPI for SAP to monitor the SAP System nominated as the CEN, you do not have to perform this step.

2. Import the SPI for SAP transports for CCMS into the SAP system nominated as the central monitoring system (CEN):

   The SPI for SAP's CCMS transport (`SAPSPI_CCMS_Monitors.car`) provides a CCMS monitor set (HP OV SAP-SPI) that includes monitors for the following SAP components: the J2EE engine, SAP security, stand-alone enqueue servers, enterprise-portal performance and availability, and XI monitoring.

   You can define new (or expand existing) monitor sets to include new CCMS monitors, whose alerts you want to display. For more information about defining CCMS monitor sets in the context of the SPI for SAP, see r3monal: CCMS Monitor Sets on page 49 and r3monal: CCMS Alert Monitors on page 51.

3 Import the SPI for SAP monitor transports:

   The SPI for SAP monitor transport (`R3Trans.car`) contains all the SPI for SAP's ABAP monitors and their default configuration settings. You must import the monitor transport into each ABAP or ABAP/JAVA(Dual stack) instance that you want the SPI for SAP to monitor through the central monitoring system.

4 Register and start the appropriate CCMS agent on each instance of the J2EE engine and ABAP that you want to monitor with the SPI for SAP through the CEN.

   For a brief description of the SAPCCMSR agent (for J2EE) and the SAPCCM4X agent (for ABAP) in the context of the SPI for SAP, see J2EE Instances on page 196 and SAP ABAP Instances on page 195 respectively. For more detailed information about installing, registering, and starting the agents, see the SAP product documenting.

5 If not already present, deploy the SPI for SAP's CCMS-alert monitor `r3monal` to the system hosting the CEN and modify the `r3monal.cfg` configuration file to enable the monitoring of CCMS monitor sets. For more information about enabling CCMS monitor sets in the `r3monal.cfg` configuration file, see CCMS Monitor Set on page 32.

6 Make sure the SPI for SAP is aware of the CEN.

   If not already present, add an entry for the CEN to the SPI for SAP's central configuration file, `r3itosap.cfg`, on the system hosting the CEN instance.

   For more information about the contents of the `r3itosap.cfg` file and an explanation of the syntax required with the HostSapAssign keyword used to define a new SAP instance to monitor, see the *HP Operations Smart Plug-in for SAP Installation Guide*.

7 If you previously used the SPI for SAP to monitor individual SAP Systems locally (and independently) and now want to change the configuration so that you can monitor all the individual SAP Systems remotely in the CEN, you will have to take note of the following points:

   a The `r3monal` monitor must not run on both the local SAP System and on the CEN System, too; this will lead to the duplication of messages.

      To avoid message duplication, disable both the `r3monal` monitor and the `r3itosap.cfg` file on each of the individual SAP Systems whose CCMS alerts you were previously monitoring independently with the SPI for SAP.

   b Configure the CEN to monitor CCMS alerts remotely from all the individual SAP Systems that you were monitoring locally.

   c Configure `r3monal` on the CEN to intercept CCMS alerts arriving on the CEN from all the individual SAP Systems that you were monitoring locally.

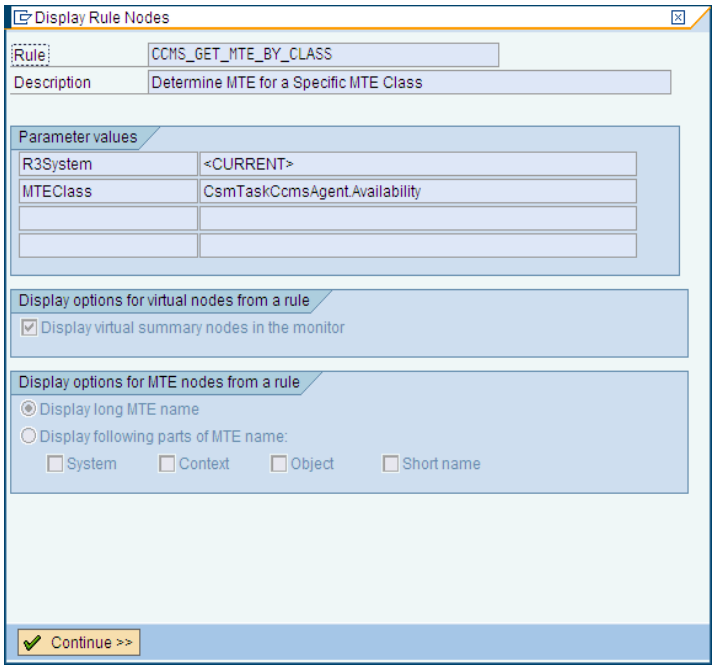
      To ensure that the CCMS alerts from the individual, remote SAP Systems now appear in the Solution Manager on the CEN, use transaction **`RZ20`** to set up a CCMS monitor tree (on the CEN) for each SAP System ID that you previously monitored locally. The new monitor trees should specify which CCMS alerts you want to monitor and intercept with the SPI for SAP.

   In this way, one instance of `r3monal` on the CEN can monitor CCMS alerts from all the SAP Systems monitored remotely by the CEN.

8 By default, the MTE rule nodes for J2EE monitoring installed with the SPI for SAP CCMS transport are set to monitor the "Current" System on which the transport is imported. This setting should be changed to "all" when imported into a CEN, so that alerts from remote Systems reporting to the CEN are monitored, as illustrated in Figure 20 on page 199.

9 If you were *not* already monitoring the CEN with the SPI for SAP, add the system hosting the CEN to the HPOM for Windows console so that messages generated by the SPI for SAP are visible in the HPOM for Windows console.

Figure 20 MTE Rule-Node Settings for CEN Monitoring



6 The SPI for SAP Performance Monitors

This section describes in detail how to install, set up, and use the SPI for SAP performance subagent (SAP/Performance subagent). It also provides information about how to put the performance monitors included in the SAP/Performance subagent to best use and supplement the information collected by the SPI for SAP performance monitors with information supplied by the HP Performance Agent.

Performance Monitors Overview

The SPI for SAP performance subagent (SAP/Performance subagent) uses a selection of performance monitors to collect SAP performance data and store them either in the HP Software Embedded Performance Component (CODA) or the Performance Agent (Unix/Windows). You can use the Performance Manager to monitor, manage, and correlate these data, together with data collected by any other application, database, system and network Performance Agent. The data can then be used to compare trends between SAP business transactions and other system metrics. This section provides information about the following topics:

- Performance monitoring with the SPI for SAP
- Using HPOM for Windows to install the SAP/Performance subagent
- Configuring the performance monitors

Implemented ABAP-function modules inside SAP NetWeaver are accessed by means of an RFC-call. The performance monitors gather a snapshot of SAP-runtime performance data.

The SPI for SAP SAP/Performance subagent can collect more than 130 metrics in *addition* to those collected by the SAP NetWeaver Performance alert monitor (**`ST03`**), which is part of the SAP NetWeaver CCMS subsystem.

You can configure the SAP/Performance subagent to specify which monitors should be run on specified SAP NetWeaver instances and how frequently. For more information, see Configuring the SAP/Performance Subagent on page 209.

The Performance Agent runs in Windows operating systems as a service and in UNIX operating systems as a daemon (background) process that runs independently of the HPOM for Windows agent processes. To start or stop the SAP/Performance subagent processes, use the appropriate HPOM for Windows tool in the SPI for SAP tools group in the HPOM for Windows console. For more information, see Managing the SAP/Performance Subagent on page 220.

Upgrading the SAP/Performance Subagent

You cannot always use the data sources you defined in previous versions of the SAP/Performance subagent with the latest version of the SPI for SAP SAP/Performance subagent. The upgrade strategy you adopt depends on the version of the SAP/Performance subagent you want to upgrade.

If you are upgrading a recent version of the SAP/Performance subagent such as 10.70, 10.50, or 09.01, you can continue to use all existing data and data sources. If you are using an older version such as 08.70 you can re-use the data and data sources, but you have to migrate the data to the new format required by the latest SAP/Performance subagent. If you are using a version of the SAP/Performance subagent such as 08.11 or earlier, you will not be able to reuse any of the existing data and data sources.

To upgrade the SAP/Performance subagent, perform the following high-level steps:

1. **Remove the existing SAP/Performance subagent**

   For more information about removing the SAP/Performance subagent, see Removing the SAP/Performance Subagent on page 243.

2. **Remove existing SAP/Performance subagent data and data sources**

   - SPI for SAP 10.70, 10.50, or 09.01

     If you are upgrading from versions 10.70, 10.50, or 09.01 to the current version of the SPI for SAP, you do not need to perform this step; you can continue to use existing data and data sources.

   - SPI for SAP 08.70

     If you are upgrading from versions 08.70 to the current version of the SPI for SAP, you do not need to perform this step: you can continue to use existing data and data sources with the new SPI for SAP performance agent. However, you need to migrate the data sources to the new format, first. The configuration of the new SPI for SAP performance agent walks you through the migration process and locates and updates the old data to the new format for you.

   - SPI for SAP 08.11 or earlier

     If you are upgrading from version 08.11 or earlier of the SPI for SAP, see Migrating the SAP/Performance Subagent with the HP Performance Agent on page 203 or Upgrading the SAP/Performance subagent with CODA on page 204 for more information about cleaning up old data sources.

3. **Upgrade the SPI for SAP**

   For more information, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.

4. **Install the new SAP/Performance subagent**

   For more information about installing the SAP/Performance subagent, see Installing the SAP/Performance Subagent on page 206.

5. **Configure the new SAP/Performance subagent**

   For more information about installing the SAP/Performance subagent, see Configuring the SAP/Performance Subagent on page 209.

6. **Upgrade the SPI for SAP/Reporter Integration**

   For more information about upgrading the SPI for SAP Reporter integration, see Upgrading the SPI for SAP Reports on page 356.

Migrating the SAP/Performance Subagent with the HP Performance Agent

If you are using the HP Performance Agent as your performance data source and want to upgrade the SAP/Performance subagent from a previous to the most recent version, it is extremely important that you migrate (or in some cases remove) cleanly and completely the data and data sources associated with the old version of the SAP/Performance subagent before you start the installation of the new version.

To migrate the SAP/Performance subagent, you need to perform the following steps:

1. **Stop the Performance Agent**

   On the node where you perform the upgrade, stop the Performance Agent:

   - AIX operating systems:

     `/usr/lpp/perf/bin/mwa stop`

   - HP-UX/Solaris operating systems:

     `/opt/perf/bin/mwa stop`

   - Windows operating systems:

     `mwacmd stop`

2. **Remove the old SAP/Performance subagent**

   Remove the old version of the SPI for SAP SAP/Performance subagent from the managed node as described in Removing the SAP/Performance Subagent on page 243.

3. **Clean up data sources**

   If you are upgrading from versions 08.70 or later to the current version of the SPI for SAP, you do not need to perform this step: you can continue to use existing data and data sources with the new SPI for SAP performance agent.

   The configuration of the new SPI for SAP performance agent walks you through the migration process and locates and updates the old data to the new format for you. For more information, see Configure the SAP/Performance Subagent on page 211.

   If you are upgrading from version 08.11 or earlier of the SPI for SAP, you need to remove all existing SAP/Performance subagent performance data sources from the managed nodes as follows:

   a. On the HPOM for Windows managed node, locate and, using your favorite text editor, open the following file, whose location differs according to operating system:

      – AIX operating systems:

        `/usr/lpp/perf/data/perflbd.rc`

      – HP-UX/Solaris operating systems:

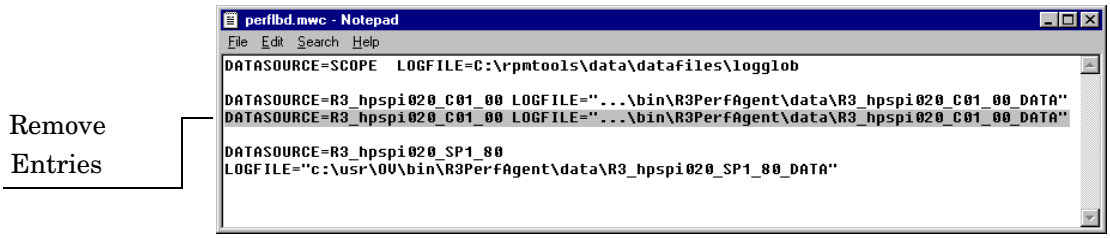
        `/var/opt/perf/data/perflbd.rc`

      – Windows operating systems:

        `<OvPerfAgtInstallDir>\data\perflbd.mwc`

   b. Remove by hand any entries relating to the SAP/Performance subagent present in the `perflbd` file, as illustrated in Figure 21 on page 204. Entries in the `perflbd` file relating to the SAP/Performance subagent start with: `DATASOURCE=R3_*`.

Figure 21 Cleaning up the perflbd file



c Remove by hand the data-source files from the following directories:

- AIX operating systems:

  `/var/lpp/OV/bin/R3PerfAgent/data`

- HP-UX/Solaris operating systems:

  `/var/opt/OV/bin/R3PerfAgent/data`

- Windows operating systems:

  `%OvDataDir%\bin\R3PerfAgent\data`

4 **Remove the old version of the SPI for SAP**

If you have not already done so, remove the old version of the SPI for SAP from the management server. For more information see *Deinstalling the SPI for SAP* in the *HP Operations Smart Plug-in for SAP Configuration Guide*.

5 **Install the new version of the SPI for SAP**

Install the new version of the SPI for SAP on the HPOM for Windows management server. For more information, see *Installing the SPI for SAP* in the *HP Operations Smart Plug-in for SAP Configuration Guide*.

6 **Install the new SAP/Performance subagent**

Install the new version of the SPI for SAP SAP/Performance subagent as described in Installing the SAP/Performance Subagent on page 206.

7 **Configure the new SAP/Performance subagent**

Configure the SPI for SAP SAP/Performance subagent. For more information, see Configuring the SAP/Performance Subagent on page 209.

Note that after finishing the migration described here, you do not need to execute steps 1 and 2 specified in Configure the SAP/Performance Subagent on page 211. You can proceed directly to step 3 and adapt the configuration file before starting the SAP/Performance subagent in steps 4 and 5.

Upgrading the SAP/Performance subagent with CODA

If you are using the HP Software Embedded Performance Component (CODA) as your performance data source and want to upgrade the SAP/Performance subagent from a previous to the most recent version, it is extremely important that you migrate (or in some cases remove) cleanly and completely the data and data sources associated with the old version of the SAP/Performance subagent before you start the installation of the new version.

To migrate the SAP/Performance subagent, you need to perform the following steps:

1 **Remove the old SPI for SAP SAP/Performance subagent**

Remove the old version of the SPI for SAP SAP/Performance subagent from the managed node as described in Removing the SAP/Performance Subagent on page 243.

2 **Clean up SAP/Performance subagent data sources**

If you are upgrading from version 08.70 or later to the current version of the SPI for SAP, you do not need to perform this step: you can continue to use existing data and data sources with the new SPI for SAP performance agent. The configuration of the new SPI for SAP performance agent walks you through the migration process and locates and updates the old data to the new format for you. For more information, see Configure the SAP/Performance Subagent on page 211.

If you are upgrading from version 08.11 or earlier of the SPI for SAP, you need to check for (and delete) entries relating to the old SAP/Performance subagent present in the `ddflbd` file. Note that the location of the `ddflbd` file and the file extension differ according to platform, namely:

- AIX operating systems:

  `/var/lpp/OV/conf/dsi2ddf/ddflbd.rc`

- HP-UX/Solaris operating systems:

  `/var/opt/OV/conf/dsi2ddf/ddflbd.rc`

- Windows operating systems:

  `%OvAgentDir%\conf\dsi2ddf\ddflbd.mwc`

Entries in the `ddflbd` file relating to the SAP/Performance subagent typically start with the following string: `DATASOURCE=R3_*` as illustrated in Figure 22 on page 206. The value of `LOGFILE=` defined for the SAP/Performance subagent entries is important: you use it (including the complete path) as an argument with the command-line utility `ddfutil -rm all` to remove the entries one by one, as follows:

After you remove from the `ddflbd` file all the entries you can find relating to the SAP/Performance subagent, check that the entries are no longer present by closing the `ddflbd` file and opening it again.

3 **Remove the old version of the SPI for SAP**

If you have not already done so, remove the old version of the SPI for SAP from the management server. For more information see “Removing the SPI for SAP” in the *HP Operations Smart Plug-in for SAP Configuration Guide*.

4 **Install the new version of the SPI for SAP**

Install the new version of the SPI for SAP on the HPOM for Windows management server. From more information, see *Installing the SPI for SAP* in the *Configuration Guide*.

5 **Install the new SPI for SAP SAP/Performance subagent**

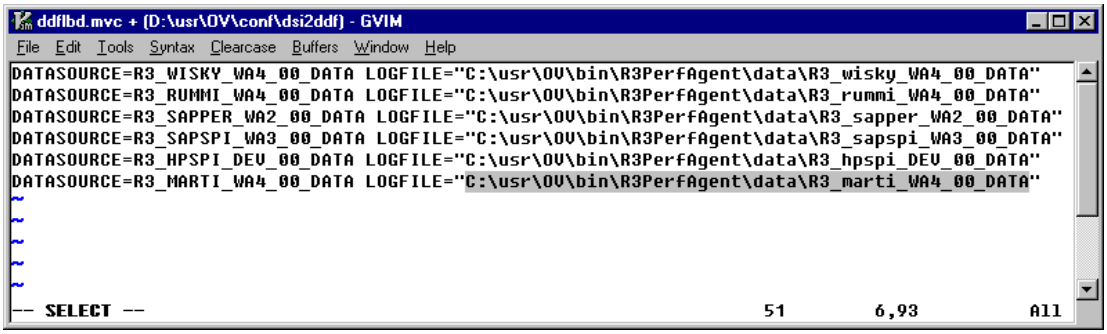
Install the new version of the SAP/Performance subagent as described in Installing the SAP/Performance Subagent on page 206.

6 **Configure the new SPI for SAP SAP/Performance subagent**

Configure the SAP/Performance subagent. For more information, see Configuring the SAP/Performance Subagent on page 209.

Note that after finishing the migration described here, you do not need to execute steps 1 and 2 specified in Configure the SAP/Performance Subagent on page 211. You can proceed directly to step 3 and adapt the configuration file before starting the SAP/Performance subagent in steps 4 and 5.

Figure 22 The ddflbd.mwc File



Installing the SAP/Performance Subagent

This section describes how to use the HPOM for Windows console to install the SPI for SAP functionality for the performance-agent on the SAP servers you want to manage with HPOM for Windows and the SPI for SAP. Note that the instructions in this section assume the following is true:

- The HP Operations agent is already installed and running on the selected SAP servers.
- Either the HP Performance Agent or the HP Software Embedded Performance Component (CODA) is running on the selected SAP servers. For information about which versions of the Performance Agent are compatible with the SPI for SAP 11.10, refer to the support matrix (**http://h20230.www2.hp.com/sc/support_matrices.jsp**).

To install the SAP/Performance package, follow these steps:

1 **Deploy the Performance-Monitor Instrumentation:**

   a From the HPOM for Windows console, select and right-click the node(s) where you want to deploy the instrumentation.

   b Browse to the following menu option:

   All tasks > Deploy instrumentation

   c In the Deploy Instrumentation window, select the following items:

   – **SPI Data Collector**

   – **SPI for SAP Performance Package**

   d Select **OK**.

2 **Install the Performance-Monitor Package:**

   a In the HPOM for Windows console, browse to the following tools folder:

   Tools > SPI for SAP > SAP R/3 Admin

   b Select and right-click the Performance Package tool which corresponds to the operating system for the SAP System environment you want to monitor. The choices are:

   – **Install Performance Package (UNIX)**

   – **Install Performance Package (Windows)**

   c Start the Install Performance Package tool for the appropriate operation system using the following option in the menu, which pops up:

All tasks > Launch Tool...

d In the window which pops up, select the SAP managed node(s) where you want to start the Performance Package installation. Remember to ensure that the nodes you select correspond to the operating system of the chosen tool, for example; UNIX or Microsoft Windows.

e Click **Launch...** to start the installation.

➤ After installation, neither the SPI Data Collector nor the SPI for SAP Performance Package appears in the list of packages installed on the managed node.

Locating the SAP/Performance Subagent Files

The information in this section describes the location of the files which the SPI for SAP installs as part of the SAP/Performance subagent package for the following platforms:

- SAP/Performance Subagent Files: AIX
- SAP/Performance Subagent Files: HP-UX, Solaris, and Linux
- SAP/Performance Subagent Files: Windows

The performance-related files listed in this section belong to the following categories: binaries and executable, configuration files, the `dsilog` files required by the HP Performance Agent, and templates.

➤ The `dsilog` files are only required by the HP Performance Agent; the HP Software Embedded Performance Component does not require or make use of the `dsilog` files.

SAP/Performance Subagent Files: AIX

This section lists the files which the SPI for SAP installs as part of the SAP/Performance subagent package for AIX.

- Binaries: `/var/[lpp | opt]/OV/bin/R3PerfAgent/bin`
  - `r3perfconfig`

    SPI for SAP performance-monitor configuration tool

  - `r3perfagent`

    SPI for SAP performance-monitor agent
- Configuration files: `/var/[lpp | opt]/OV/conf/sapspi/[global | local]`
  - `r3perfagent.cfg`

    Configuration file for the various global and local performance monitors. Note that the SPI for SAP creates this directory *after* you deploy the SPI for SAP performance-agent policies for the first time.
- `Dsilog` files: `/var/[lpp |opt]/OV/bin/R3PerfAgent/data`
  - `R3_<HOSTNAME>_<SID>_...`

Immediately after installation, this directory is empty; the SPI for SAP uses the directory to store the `dsilog` files, which `r3perfconfig` and `compdsifile.sh` compile for the HP Performance Agent.

- Templates: `/var/[lpp | opt]/OV/bin/R3PerfAgent/template`
  - `R3statistics.<PERF-MONITOR>`

    Files the SPI for SAP uses to compile the `dsilog` files
  - `Parm.UX`

    Template for the performance-agent parameter file.

SAP/Performance Subagent Files: HP-UX, Solaris, and Linux

This section lists the files which the SPI for SAP installs as part of the SAP/Performance subagent package for HP-UX, Solaris, and Linux:

- Binaries: `/var/opt/OV/bin/R3PerfAgent/bin`
  - `r3perfconfig`

    SPI for SAP performance-monitor configuration tool
  - `r3perfagent`

    SPI for SAP performance-monitor agent
- Configuration files: `/var/opt/OV/conf/sapspi/[global | local]`
  - `r3perfagent.cfg`

    Configuration file for the various performance monitors. Note that the SPI for SAP creates this directory *after* you deploy the SPI for SAP performance-agent policies for the first time.
- `Dsilog` files: `/var/opt/OV/bin/R3PerfAgent/data`
  - `R3_<HOSTNAME>_<SID>_...`

    Immediately after installation, this directory is empty; the SPI for SAP uses the directory to store the `dsilog` files, which `r3perfconfig` and `compdsifile.sh` compile for the HP Performance Agent.
- Templates: `/var/opt/OV/bin/R3PerfAgent/template`

  `R3statistics.<PERF-MONITOR>`

  Files the SPI for SAP uses to compile the `dsilog` files
  - `parm.UX`

    Template for the performance-agent parameter file.

SAP/Performance Subagent Files: Windows

This section lists the files which the SPI for SAP installs as part of the SAP/Performance subagent package for Windows:

- Binaries: `%OvDataDir%\bin\R3PerfAgent\bin`
  - `r3perfconfig`

    SPI for SAP performance-monitor configuration tool

  - — `r3perfagent`

    SPI for SAP performance-monitor agent

  - — `r3perfagent_service`

    Starts the performance-monitor agent as a service under Windows

- Configuration files: `%OvAgentDir%\conf\sapspi\[global| local]`
  - — `r3perfagent.cfg`

    Configuration file for the various performance monitors. Note that the SPI for SAP creates this directory *after* you deploy the SPI for SAP performance-agent policies for the first time.

- `Dsilog` files: `%OvDataDir%\bin\R3PerfAgent\data`
  - — `R3_<HOSTNAME>_<SID>_...`

    Immediately after installation, this directory is empty; the SPI for SAP uses the directory to store the `dsilog` files, which `r3perfconfig.bat` and `compdsifile.bat` compile for the HP Performance Agent.

- Templates: `%OvDataDir%\bin\R3PerfAgent\template`
  - — `R3statistics.<PERF-MONITOR>`

    Files the SPI for SAP uses to compile the `dsilog` files

  - — `parm.UX`

    Template for the performance-agent parameter file.

Configuring the SAP/Performance Subagent

The information in this section takes you through the process of setting up and configuring the SAP/Performance Agent.

Selecting the Performance-data Source

The HP Software Embedded Performance Component is, as the name suggests, embedded in the HPOM for Windows software and available, by default, in any HPOM for Windows installation. However, you can use the HPOM for Windows console to deploy the HP Performance Agent to the managed nodes, too.

If you prefer to use the HP Performance Agent as the source for performance data for newly installed HP Software products rather than the HP Software Embedded Performance Component, for example; to feed the data into the Performance Manager, you can set up a small text file, `nocoda.opt`, which instructs the SPI for SAP to ignore the default data source, the HP Software Embedded Performance Component, and switch to the HP Performance Agent. After you configure the `nocoda.opt` file, you must store it in the following location on each managed node, whose performance-data source you want to change:

- AIX [DCE | HTTPS]:

  `/var/[lpp | opt]/OV/conf/dsi2ddf/nocoda.opt`

- HP-UX/Solaris:

  `/var/opt/OV/conf/dsi2ddf/nocoda.opt`

- Microsoft Windows:
- `%OvAgentDir%\conf\dsi2ddf\nocoda.opt`

To change the performance-data source, follow these steps:

1 **Open the nocoda.opt file**

Open the (or create a new) `nocoda.opt` file in a text editor and manually enter the appropriate information using the format and syntax illustrated in An Example of the nocoda.opt File on page 210.

2 **Specify a generic data source**

To designate the HP Performance Agent as the agent for all data sources on the managed node, enter (or enable) the key word ALL at the top of the `nocoda.opt` file.

> Using the ALL keyword in the `nocoda.opt` file to enable all SAP NetWeaver and SAP ITS instances on the managed node as data sources for the Performance Agent overrides any references to explicit data sources, which are still present in the `nocoda.opt` file.

3 **Specify individual data sources**

To designate the HP Performance Agent as the data source tied to a specific SAP NetWeaver (or SAP ITS) instance, remove (or disable) the key word ALL at the top of the `nocoda.opt` file and include a reference to each SAP (or SAP ITS) instance on a separate line of the `nocoda.opt` file, as illustrated in An Example of the nocoda.opt File, using the following format:

```
R3ITS_<Virtual_SAPITS_Instance_Name>_ <SAPITS_Hostname>_DATA
```

> Any SAP NetWeaver and SAP ITS instances on the managed node which are not explicitly listed in the `nocoda.opt` file, will continue to use the default data source, namely; the HP Software Embedded Performance Component (CODA).

4 **Save the changes to the nocoda.opt file**

Save the changes to the `nocoda.opt` file

5 **Restart the HP Operations agent**

Restart the HP Operation agent on the managed node where the `nocoda.opt` file has been modified.

An Example of the nocoda.opt File

```
#-------------------------------------------------------------
# Add to (or modify) the contents of this file to change the
# data-source from the default CODA to the Performance Agent
#-------------------------------------------------------------
# All hosts:
# ALL
# SAP R/3 hosts/instances:
R3_ovsdsap_DEV_00_DATA
# SAP R/3 ITS hosts/instances:
R3ITS_SP6_00_ovspi_DATA
```

Configure the SAP/Performance Subagent

You need to complete the following steps to configure the SAP/Performance subagent:

Make sure that the `OVDATADIR` environment variable is set for all UNIX nodes.

1 **Start the SAP/performance subagent configuration**

On the node where you installed the SAP/performance subagent, switch to the appropriate directory and enter the following command to run the SAP/performance-subagent configuration scripts:

— Windows operating systems: **`r3perfconfig`**

— UNIX operating systems: **`../r3perfconfig`**

Follow the instructions which appear on screen. The script lists the SIDs that it finds and prompts you to choose one of the associated numbers to indicate which SAP NetWeaver instance you want to configure. For example:

```
Installed SAP Instances:

       SID    SapNr    HostName
------------------------------

(0)    AST    45       sapper
(1)    DEV    50       sapper
(2)    SP1    80       sapper

Choose:
(x) to configure shown system
888 to manually configure a SAP system
999 to quit
```

Enter the appropriate SAP-SID identification number, for example; **`0`** for AST, **`1`** for DEV, **`2`** for SP1, or **`888`** to configure a new SAP System:

a If *no* data source exists for the given SAP System ID, `r3perfconfig` creates one and configures it, as follows:

```
Choose:
(x) to configure shown system
888 to manually configure a SAP system
999 to quit
0
Creating new datasource: R3_sapper_AST_45_DATA
...Datasource successfully created
```

b If a valid data source already exists for the given SAP System ID, `r3perfconfig` lists the data source and prompts you to continue, as follows:

```
Choose:
(x) to configure shown system
888 to manually configure a SAP system
999 to quit
0
Valid datasource already exists: R3_sapper_AST_45_DATA
```

c If `r3perfconfig` finds an existing data source, which it can migrate to the required *new* format, it lists the old data source and asks you what to do:

```
Choose:
(x) to configure shown system
888 to manually configure a SAP system
999 to quit
1
Found an old datasource: R3_sapper_DEV_50_DATA
Should the existing datasource be migrated <yes/no>?
```

Bear in mind the following before you respond:

– **yes**

automatically migrates the old data source to the format required by the new version of the SPI for SAP SAP/Performance subagent

– **no**

leaves the existing data source unchanged: the old data source *cannot* be used with the new version of the SPI for SAP SAP/Performance subagent

d If `r3perfconfig` finds an existing data source, which *cannot* be migrated to the new format, for example; because it belongs to a version of the SPI for SAP that is older than 08.70, it lists the old, *invalid* data source and prompts you to continue, as follows:

```
Choose:
(x) to configure shown system
888 to manually configure a SAP system
999 to quit
2
Found an invalid datasource: R3_sapper_SP1_80_DATA
Existing datasource cannot be migrated
```

e If you choose **888** to configure a SAP SID from scratch, you are required to answer a series of questions concerning the SAP SID you want to configure.

Since `r3perfagent` will always use the physical hostname in a cluster environment, you must specify the clustered SAP-system details by configuring `r3perfagent` with the manual mode (**888**). If you are configuring `r3perfagent` on a physical cluster node, `r3perfconfig` *may* offer you the option (**x**) on the SAP system with the virtual node. In this case, use the manual configuration (**888**) by specifying the physical cluster node name.

When you are finished, the data sources are created and added to the following file, which differs according to whether you are using HP Performance Agent or the HP Software Embedded Performance Component:

— Windows operating systems:

`perflbd.mwc / ddflbd.mwc`

— UNIX operating systems:

`perflbd.rc / ddflbd.rc`

It is a good idea to update the `parm.mwc` file as described in the next step before you restart the performance agent.

2 **Update the performance-agent parameter file**

This step does not apply to the HP Software Embedded Performance Component.

If you are using the performance agent, append the template file `parm.NT` (or `Parm.UX`, depending on the installed operating system on the managed node) to the `parm` file of the performance agent, as follows:

— UNIX operating systems:

```
cat parm.UX >> parm
```

In UNIX operating systems, the `parm` file is located in: `/var/opt/perf/parm`

— Windows operating systems:

```
type parm.NT >> parm.mwc
```

The `parm.mwc` file is located in the following directory:
`<drive_letter>\rpmtools\data\parm.mwc`

You can represent several SAP NetWeaver instances in the `parm` file by using the asterisk (*) wild card.

3 **Configure the performance monitors**

Configure the monitors in the `r3perfagent.cfg` file. If you do not do this, all monitors will run with the default settings as illustrated in the following example. There are two possible configurations:

— **Global:** `global_r3perfagent.cfg`

Global SAP/performance subagent settings for *all* SAP managed nodes

— **Local:** `local_r3perfagent.cfg`

Local SAP/performance subagent settings for *individual* SAP managed nodes.

To open the `r3perfagent.cfg` file with the configuration-file policy editor, double-click the **global_r3perfagent** policy, which resides in the policy group:

Policy Management > Policy Groups > SPI for SAP

The settings in the *global* configuration files are used for all nodes which do not have *local* configuration settings. Where both files are present, local settings override global ones.

The default configuration is:

— All performance monitors are enabled for all SAP host names, systems, numbers and clients.

— The default polling intervals are set for each performance monitor in minutes.

— `Hold Connections` is disabled.

Change any values as required and save the file. You will have to restart the HP Performance Agent to upload the latest configurations.

4 **Deploy the policies**

To deploy the new or modified policies to the managed nodes, right-click the new or modified policies and use the following option from the menu which appears:

All Tasks > Deploy on...

5 **Start the HP Performance Agent**

Start the HP Performance Agent on the managed node by entering the following command in a shell:

— UNIX operating systems: **`mwa start`**

— Windows operating systems: **`mwacmd start`**

6 **Start the SAP/performance subagent**

On the managed node, switch to the directory in which the `r3perfagent` command resides and start the SAP/performance subagent by entering the following command in a shell:

— UNIX operating systems:

```
./r3perfagent [stop | start]
```

— Windows operating systems:

```
r3perfagent_service [-e | -s]
```

Or, alternatively, in the HPOM for Windows console, use the following SPI for SAP tool:

— UNIX operating systems:

Tools > SPI for SAP > SAP R/3 UN*X > PerfAgt START

— Windows operating systems:

Tools > SPI for SAP > SAP R/3 NT > PerfAgt START

Remote Performance Monitoring

The current version of the SPI for SAP includes a feature which allows you to extend the scope of the performance monitor to remotely monitor the health of an additional SAP server (which is *not* a managed node) from an SAP server, which *is* already configured as an HPOM for Windows managed node.

Although the remote host is not an HPOM for Windows managed node, it must nonetheless be present in the HPOM for Windows node list. If you do not add the remote host to the HPOM for Windows node list, HPOM for Windows cannot resolve the host name associated with the remote host and, as a consequence, any messages from the remote host will not appear in the HPOM for Windows console.

In addition, the SAP Server defined in RemoteHost must appear in the `r3itosap.cfg` file to ensure that the SPI for SAP can login to and extract information from the SAP instances it is monitoring on the remote host. For more information about the `r3itosap.cfg` file, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.

SPI for SAP tools cannot start a SAP GUI on an SAP System, which the SPI for SAP is monitoring remotely from an HPOM for Windows managed node.

To make use of the remote-monitoring feature provided by the SPI for SAP, for example; to collect SAP performance metrics from a SAP System running an operating system that is not supported by the SPI for SAP, you need to use the `r3perfconfig` command to manually add an additional data source for each system you plan to monitor remotely and then enable the new RemoteMonitoring keyword (by removing the leading hash symbol “#”) in the *global* `r3perfagent.cfg` file.

On the same line in the *global* `r3perfagent.cfg` file, tell the SPI for SAP performance agent the name of the local SAP server which you want to perform the monitoring and, in addition, the name of the remote SAP server, which you want to monitor. Note that you must add a new line for each *additional* server that you want to monitor remotely. Specifying Remotely Monitored Hosts in the r3perfagent.cfg File on page 215, shows an excerpt from the *global*

r3perfagent.cfg file with the remote-monitoring feature enabled; the *local* r3perfagent.cfg file, if present, would only contain references to the managed node on which the local configuration file is located.

The performance-monitoring conditions defined in the *Perfmon* section at the end of the r3perfagent.cfg file apply by default to all SAP instances running on all the servers listed in the configuration file, that is: all SAP instances running on both the local and remote servers defined in the RemoteMonitoring section. For more information about the keywords and parameters used to define remote monitoring in the r3perfagent.cfg file, see The r3perfagent.cfg Configuration File on page 216.

Specifying Remotely Monitored Hosts in the r3perfagent.cfg File

```
#-----------------------------------------------------------
# Remote            LocalHost    RemoteHost
# Monitoring

RemoteMonitoring    =sapwolf2    =sapprod1
RemoteMonitoring    =sapwolf3    =sapprod2
RemoteMonitoring    =sapper      =sapprod3
#-----------------------------------------------------------
```

The Performance-Monitor Scheduler

An internal scheduler ensures that the performance monitors run according to the desired schedule. The scheduler keeps track of time and the number of runs that have been completed and uses this information to ensure that the performance monitors run at the correct time and collect the appropriate performance-related data.

If the performance monitor encounters any problems during its run and cannot complete its task before the start of the next scheduled run, it does not stop and leave tasks incomplete; the performance monitor continues to run until it has completed its task. However, the scheduler tracks the progress of the performance monitor and tries to synchronize the run schedules so that the time lost can be regained without affecting the collection of the performance data.

If the performance-monitor scheduler falls ten minutes behind schedule, it sends a message to the HPOM for Windows management server with the warning that the scheduler is out of synchronization. If the performance-monitor scheduler falls thirteen minutes behind schedule, it resets—ignoring all outstanding jobs. For more information about the keywords you can use to control the performance-monitor scheduler and the messages it generates, see The r3perfagent.cfg Configuration File on page 216.

The performance monitor has problems with synchronization if it is not able to complete all its scheduled tasks in the allowed time between each monitor run. To troubleshoot scheduler-synchronization problems:

1. **Check the Polling Interval**

   Check that the polling interval for the individual r3perfagent monitors has not been changed in the r3perfagent.cfg file to a value that is too small. You can define the polling interval for individual monitors in the “Polling Interval” column of the r3perfagent.cfg file, as shown in Specifying Remotely Monitored Hosts in the r3perfagent.cfg File on page 215. The default polling intervals for the performance monitors are, with one or two exceptions, between 15 and 60 minutes.

For example, if you reduce the polling interval of *all* the performance monitors to one (1) minute, the performance-monitor scheduler tries to start *all* the performance monitors *each* time it runs. If there are ten monitors and each monitor takes ten seconds to respond, then the scheduler will already be out of synchronization by the time the scheduler starts its second run. You will have to increase the polling interval for the various performance monitors accordingly.

2 **Disable Remote Monitoring**

If you have enabled remote monitoring for the `r3perfagent` performance monitor, network problems could mean that requests for information from the remote server are not being answered in a timely fashion. Try disabling remote monitoring for a short while to test if this is the reason the `r3perfagent` performance monitor is having problems. You can do this for one individual remote host, or all remote hosts (if there are more than one). For more information about remote monitoring with the SPI for SAP performance monitor, see Remote Performance Monitoring on page 214.

The r3perfagent.cfg Configuration File

The SPI for SAP provides a default configuration for the `r3perfagent` monitor; the default file works without modification immediately after installation. However, if you want to set up the `r3perfagent` monitor for your particular SAP environment, you can modify the `r3perfagent.cfg` file by enabling or disabling the keywords in the following list and, where necessary, setting or modifying the appropriate parameters:

- **TraceLevel**

  The TraceLevel keyword accepts the following parameters:

  ```
  TraceLevel =<Hostname> =<TraceLevel>
  ```

  — **Hostname:**

=ALL	Monitor all hosts with the SPI for SAP. This is the default setting.
=<SAP_host>	The name of an SAP server, where you want to specify a trace level. Use a new line for each individual host.

  — **TraceLevel:**

=0	Disable. This is the default setting.
=1	Log only error messages
=2	Log all messages
=3	Log only debug messages. Note that this trace level logs a lot of information and could very quickly lead to a very large trace file.

- **TraceFile:**

  The TraceFile keyword accepts the following parameters:

  ```
  Tracefile =<Hostname> =<Filename>
  ```

— **Hostname:**

=ALL Monitor all SAP servers with the SPI for SAP. This is the default setting

=<*SAP_host*> The name of a specific host where tracing is enabled and you want to specify a trace level.

— **Filename:**

`=r3perfmon.log` – This is the default setting, which writes the log file to the working directory of the process, which started the `r3perfagent`. Alternatively, you can specify the name of the file to which you want to write the trace log and, if necessary, the path. The path can be either absolute or relative to the working directory.

If you use standard SPI for SAP tools to start the `r3perfagent`, the working directory is the directory where the `r3perfagent` binary resides, for example in UNIX operating systems: `/var/opt/OV/bin/R3PerfAgent/bin`. For more information about the location of the `r3perfagent` binaries, see Locating the SAP/Performance Subagent Files.

- **AgentHostname**

  Make sure that the `AgentHostname` keyword set to `ALL`.

- **SyncBack**

  The SyncBack keyword accepts the following parameters:

  ```
  SyncBack =<Enable|Disable> =<SyncBack Threshold>
  ```

  — **Enable/Disable:**

  =0 Disable the scheduler synchronization

  =1 Enable the scheduler synchronization. This is the default setting.

  — **SyncBack Threshold:**

  =<*n*> mins The difference in minutes between defined and actual schedules. If the SyncBack threshold is reached, for example; when the scheduler is “n” minutes behind schedule, the scheduler restarts to return to the defined schedule. The SyncBack threshold should be *higher* than the `Message Threshold` value set in association with the `BehindSyncMessage` keyword so that you receive a message warning about schedule problems *before* the scheduler restarts.

- **BehindSyncMessage**

  The BehindSyncMessage keyword accepts the following parameters:

  ```
  BehindSyncMessage =<Enable|Disable> =<OpC Severity>
  =<OpC Object> =<OpC MsgGroup> =<Message Threshold>
  ```

  — **Enable/Disable:**

  =0 Disable the sending of a behind-schedule message.

  =1 Enable the sending of a behind-schedule message. This is the default setting.

— **OpC Severity:**

=WARNING The severity of the behind-schedule message sent. This is the default value.

— **OpC Object:**

=r3perfagent The HPOM for Windows object to associate with the behind-schedule message. This is the default value.

— **OpC MsgGroup:**

=R3_General The HPOM for Windows message group to which the behind-schedule message belongs. This is the default value.

— **Message Threshold:**

=<*n*> mins The elapsed time in minutes before a behind-schedule message is sent to the HPOM for Windows management server. The message-threshold value should be *less* than the `SyncBack Threshold` value set in association with the `SyncBack` keyword so that you receive a message warning about schedule problems *before* the scheduler restarts.

- **RemoteMonitoring**

  The RemoteMonitoring keyword accepts the following parameters:

  ```
  RemoteMonitoring =<LocalHost> =<RemoteHost>
  ```

  — **LocalHost**

  This is the name of the host where the SPI for SAP software is running and whose performance agent will be used to remotely monitor the SAP server defined in “Remotehost”.

  — **RemoteHost**

  This is the name of the *remote* SAP server that you want to monitor using the SPI for SAP on the SAP server defined in “Localhost”. Although the remote host does not have the SPI for SAP software installed and is *not usually* an HPOM for Windows managed node, it must appear in the HPOM for Windows node list.

  For more information, see Remote Performance Monitoring on page 214.

- **PerfMon**

  The Perfmon keyword *requires* a value for the following parameters:

  ```
  PerfMon =<SAP Hostname> =<SAP System> =<SAP Number> \
  =<SAP Client> =<RFC FUNCTION> =<Enable|Disable> \
  =<Polling Interval> =<Hold Connection>
  ```

  — **SAP Hostname:**

  =ALL Monitor all SAP hosts with the SPI for SAP. This is the default setting.

  =<*SAP_host*> The host name of a specific SAP server whose performance you want to monitor. Use a new line for each individual host

— **SAP System:**

=ALL	Monitor all SAP Systems with the SPI for SAP. This is the default setting.
=<*SAP_SID*>	The ID of a SAP System whose performance you want to monitor, for example; DEV. Use a new line for each individual SID.

— **SAP Number:**

=ALL	Monitor all SAP numbers with the SPI for SAP. This is the default setting.
=<*Instance*>	The number of a specific SAP *instance* whose performance you want to monitor, for example; 00, 99. Use a new line for each new SAP number.

— **SAP Client:**

=ALL	Monitor all SAP clients with the SPI for SAP. This is the default setting.
=<*ClientID*>	The number of a specific SAP client whose performance you want to monitor, for example; 099. Use a new line for each SAP client.

— **RFC FUNCTION**:

=<*metricname*>_PERF, where *metricname* refers to the specific metric list you want the performance monitor to use, for example; DBINFO_PERF or SAPMEMORY_PERF. For more information about the possible values you can use, see The SPI for SAP Performance Monitors on page 222.

— **Enable/Disable:**

=0	Disable the performance monitor
=1	Enable the performance monitor. This is the default setting.

— **Polling Interval:**

=*nn*	*nn* is the time in minutes between each run of the performance monitor

— **Hold Connection:**

=0	*Disable*: close the RFC connection after the call has completed. This is the default setting.
=1	*Enable*: keep the RFC connection open after the call has completed

Managing the SAP/Performance Subagent

You can control the SPI for SAP SAP/Performance subagent using command-line options, which differ according to the platform and operating system. You can manage the SPI for SAP SAP/Performance subagent either by using command-line options or the tools that are installed by the SPI for SAP.

SAP/Performance agent Command Line Syntax

You an use the following options with the `r3perfagent` command on UNIX managed nodes to control the SPI for SAP SAP/Performance subagent from the command line:

- **`r3perfagent start`**
- **`r3perfagent stop`**
- **`r3perfagent status`**

You can use the following syntax with the `r3perfagent` command on Windows managed nodes to control the SPI for SAP SAP/Performance subagent from the command line:

- **`r3perfagent_service -i`**

  registers the `r3perfagent` service
- **`r3perfagent_service -u`**

  *de*registers the `r3perfagent` service
- **`r3perfagent_service -s`**

  starts the `r3perfagent` service
- **`r3perfagent_service -e`**

  stops the `r3perfagent` service

You can also use the `Services` option in the Windows Control Panel to control Windows services.

SAP Logins for the SAP/Performance Agent

The SPI for SAP SAP/Performance subagent requires access to SAP to collect SAP-related metrics, which it then uses to generate reports and graphs. You define the SAP login for the SAP/Performance subagent during the installation and configuration of the SPI for SAP. You also need to copy the combination of SAP user-name and password to the central SPI for SAP configuration file, `r3itosap.cfg`, which the SPI for SAP monitors and agents use to login to SAP.

This is particularly important for the SPI for SAP's SAP/Performance subagent, which reads the SAP log-in information in the `r3itosap.cfg` *once only*, on startup, and will not start if it cannot log in to SAP. The SPI for SAP SAP/Performance subagent attempts to log in to SAP and, if it fails, sends a message to HPOM for Windows indicating that it was unable to start as a result of authorization problems.

Note that SAP has a security mechanism which blocks further logins from a user who tries (and fails) to login to SAP a given number of times. This number of failed logins could quickly be reached by the SAP/Performance subagent if the SAP username/password for the SPI for SAP is changed in SAP but the changes to the SAP log-in details are not updated in the `r3itosap.cfg` file.

If you change the SAP user name-password combination that the SPI for SAP uses to log in to SAP, you need to make sure that the changes are reflected in the `r3itosap.cfg` file and, in addition, that the SPI for SAP components which use the information in the `r3itosap.cfg` are restarted to make them aware of the changes.

Best of all, stop the SPI for SAP SAP/Performance Agent *before* you change the SAP user/password which the SPI for SAP needs for access to SAP, as follows:

1. **Stop the SAP/Performance Agent**

   Stop the SAP/Performance Agent on all HPOM for Windows managed nodes where it is running. On each managed node, enter:

   ```
   r3perfagent stop
   ```

2. **Login to SAP**

   Login to SAP as the administrator and change the user-password combination that SPI for SAP uses to log in to SAP, as required.

   Note that SAP requires you to change the password for dialog users more frequently than other types of SAP users.

3. **Update the configuration file**

   Update the SPI for SAP configuration file, `r3itosap.cfg`, with the changes you have made to the SAP user and password and re-deploy to the managed nodes.

4. **Restart the SAP/Performance Agent**

   Restart the SPI for SAP SAP/Performance Agent on each of the HPOM for Windows managed nodes where the SAP/Performance Agent is running. On each managed node, enter:

   ```
   r3perfagent start
   ```

The SPI for SAP cannot collect performance metrics during the period when the SAP/Performance Agent is not running.

SAP/Performance agent Tools

Table 71 shows which HPOM for Windows tools are available for the SAP/Performance subagent in the appropriate SPI for SAP tool group—SAP R/3 NT or SAP R/3 UN*X.

Table 71 Performance Agent Tools

Tool Name	SAP R/3 NT	SAP R/3 UN*X
PerfAgt START	✓	✓
PerfAgt STOP	✓	✓
PerfAgt STATUS		✓

The SPI for SAP Performance Monitors

The SPI for SAP performance monitors can be one of two types: **snapshot** or **time-frame**. A snapshot monitor runs once and gathers only one set of values. Snapshot monitors need to run on a regular basis to create a comprehensive picture of the performance of the SAP NetWeaver environment. Time-frame monitors run, as the name suggests, over a period of time. Most SPI for SAP performance monitors do not make use of alert types or parameters.

The following SPI for SAP performance monitors are available with the SPI for SAP and are explained in greater detail in the individual sections that follow:

- DBINFO_PERF

  Monitors database-performance analysis values
- DOCSTAT_PERF

  Collects the document volume statistics for the last full hour
- EP_PERF

  Monitors the status and performance of the SAP Enterprise Portal
- ICMSTAT_PERF

  Monitors the status and performance of the SAP Internet Communication Manager
- JOBREP_PERF

  Counts the number of jobs per state (scheduled, running)
- SAPBUFFER_PERF

  Returns values for the use of SAP *buffers* for an SAP instance
- SAPMEMORY_PERF

  Monitors SAP memory use by SAP users for an SAP instance
- SPOOL_PERF

  Counts the number of spool requests in different states
- STATRECS_PERF

  Returns the response/net times of defined transactions
- SYSUP_PERF

Monitors the status of the SAP NetWeaver instances

- UPDATE_PERF

  Monitors the number of update processes

- USER_PERF

  Monitors the number of users and user sessions per SAP client

- WLSUM_PERF

  Collects the performance-workload statistics hourly

- WP_PERF

  Monitors the number of users/sessions per SAP client for an SAP application server

The name of the SPI for SAP performance monitor is often the same as the name of the metric list that the monitor uses to gather data for reports. For example: the SPI for SAP performance monitor DBINFO_PERF uses the metric list DBINFO_PERF. However, the names of some performance metrics have the prefix "SAP_". For example, the SPI for SAP performance monitor ICMSTAT_PERF uses the metric list SAP_ICMSTAT_PERF. For more information about SPI for SAP metric lists, see SPI for SAP Report Metrics on page 367.

DBINFO_PERF

The DBINFO_PERF performance monitor returns a set of values as they are displayed in the SAP database-performance analysis page. This information can be used to detect database performance problems and assess whether database tuning could improve database performance.

The DBINFO_PERF performance monitor works *only* with Oracle database data structures. It does *not* work with data structures from other database products.

Type

The DBINFO_PERF performance monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set. The DBINFO_PERF performance monitor collects SID-related metrics and should run only once per monitored SID, that is: either on the SAP central instance or on *one* application server.

Frequency

It is recommended to run the DBINFO_PERF performance monitor once every 15 minutes.

Datasource

The DBINFO_PERF performance monitor uses the SAP transaction **ST04** (DB performance overview) as its data source.

Metrics

Table 72 shows the values in the performance table returned by the DBINFO_PERF performance monitor.

Table 72 DBINFO_PERF Performance Monitor Metrics

Order	Metric Name	Description	% Value	Cumul-ation
1	CPUUSAGE	Database CPU usage		No
2	BUFPREADS	Physical reads		Yes
3	BUFPWRITES	Physical writes		Yes
4	BUFQUAL	Quality of data base buffer pool	%	No
5	BUFSIZE	Database buffer pool size		Static
6	BUFWAITS	Buffer busy waits		Yes
7	BUFWTIME	Buffer busy wait time		Yes
8	DICTSIZE	Dictionary cache size		Static
9	DDQUAL	Quality of Data Dictionary cache	%	No
10	LOGBLOCKS	Redo log blocks written		Yes
11	LOGENTRIES	Redo log buffer entries		Yes
12	LOGSIZE	Redo log buffer size		Static
13	LOGFAULT	Allocation error rate of redo log buffer	%	No
14	LOGALLOC	Redo log buffer allocation retries		Yes
15	ROLLBACKS	Rollbacks		Yes
16	SCANLONG	Long table scans		Yes
17	SORTDISK	Sort disk		Yes
18	SORTMEM	Sort memory		Yes
19	SORTROWS	Sort rows		Yes

DOCSTAT_PERF

The performance monitor, DOCSTAT_PERF, collects statistics relating to the volume of documents generated and processed for the last full hour. You can only configure this monitor once for every SAP NetWeaver System that you want to monitor.

Type

The DOCSTAT_PERF performance monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set. The DOCSTAT_PERF performance monitor collects SID-related metrics and should run only once per monitored SID, that is: either on the SAP central instance or on *one* application server.

Frequency

It is recommended to run the DOCSTAT_PERF performance monitor hourly.

Data Source

The DOCSTAT_PERF performance monitor uses the SAP transaction **ST07** (quantity structure) as its data source.

Metrics

Table 73 shows the values in the performance table returned by the DOCSTAT_PERF performance monitor.

Table 73 DOCSTAT_PERF Performance Monitor Metrics

Order	Metric Name	Description
1	SID	The SAP System ID
2	DESCRIPTION	Description of an application-monitor object
3	CNTHEADER	Document headers
4	CNTITEM	Document items
5	CNTDIV	Document Division
6	CNTTOTAL	Total number of records
7	CNTLINE	Number of line items
8	CNTCHGDOC	The number of changed documents
9	CNTTEXT	Text

EP_PERF

The performance monitor, EP_PERF, monitors the status and performance of the SAP Enterprise Portal (EP) including (but not limited to) all the J2EE components on which it relies. For more information about the SPI for SAP's dedicated monitor for the SAP Enterprise Portal, see The SAP Enterprise-Portal Monitor on page 86.

Type

The EP_PERF performance monitor is of type *time-frame* and does not make use of alert types or parameters. One monitor run gathers only one value set. The EP_PERF performance monitor collects SID-related metrics and should run only once per monitored SID, that is: either on the SAP central instance or on *one* application server.

Frequency

It is recommended to run the EP_PERF performance monitor approximately once every fifteen minutes.

Datasource

The EP_PERF monitor uses the SAP function **`/HPOV/OV_EP_PERF_MONITOR_2`** as its data source.

Metrics

Table 74 shows the values in the performance table returned by the EP_PERF performance monitor.

Table 74 EP_PERF Performance Monitor Metrics

Order	Metric Name	Description
1	SID_EP	ID of the SAP System hosting the Enterprise Portal
2	HOSTNAME_EP	Name of the system hosting the Enterprise Portal
3	START_TIME_EP	The time at which the EP-monitor run starts
4	NO_REQ_EP	Number of requests to the Enterprise Portal
5	AVG_RESP_TIME_EP	Average time to respond to requests to the Enterprise Portal
6	AVG_CPU_TIME_EP [a]	Average CPU time required to respond to requests to the Enterprise Portal
7	REQ_PER_SEC_EP	Number of requests per second to the Enterprise Portal
8	AVG_OUTBND_DATA_EP	Average amount of out-bound data per request to the Enterprise Portal
9	ACC_RESP_TIME_EP	Accumulated response time of requests to the Enterprise Portal
10	ACC_CPU_TIME_EP (a)	Accumulated CPU time required to respond to EP requests
11	OUTBND_DATA_REQ_EP	Requests providing outbound data

Table 74 EP_PERF Performance Monitor Metrics (cont'd)

Order	Metric Name	Description
12	ACC_OUTBND_DATA_EP	Amount of accumulated outbound data (in bytes)
13	NO_COMPCALLS_REQ_EP	Number of component calls by all requests to the Enterprise Portal
14	AVG_CMPCALLPERREQ_EP	Average number of component calls per EP request
15	VALID_MONDATA_REQ_EP	EP requests providing correct monitor data
16	REQ_NOT_CORR_CLSD_EP	EP requests with components that were not correctly closed
17	REQCLSD_TOOMNYCMP_EP	Number of EP requests that were closed because of too many components
18	REQS_RUNLEVEL_0_EP	EP requests running with level 0
19	REQS_RUNLEVEL_1_EP	EP requests running with level 1
20	REQS_RUNLEVEL_2_EP	EP requests running with level 2
21	USRS_SINCE_1_REQ_EP	Number of users making EP requests since the first request
22	USRS_SINCE_LSTRST_EP	Number of users making EP requests since the last user reset
23	LST_REQ_RST_TSTMP_EP	Time of the last EP-request reset
24	LST_CMPREQ_TSTMP_EP	Time of the last component reset
25	LST_USRREQ_TSTMP_EP	Time of the last EP-user reset

a. Only for SAP NetWeaver portal version 7.0

If the performance monitor EP_PERF cannot find any data or it encounters a null string in SAP CCMS, it logs some performance metrics as '0' (zero); this behavior is expected.

ICMSTAT_PERF

The performance monitor, ICMSTAT_PERF, monitors the status and performance of the SAP Internet Communication Manager (ICM).

Type

The ICMSTAT_PERF performance monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set. The ICMSTAT_PERF performance monitor collects application-server-specific metrics; it should run on each application server whose performance you want to monitor.

Frequency

It is recommended to run the ICMSTAT_PERF performance monitor approximately once every fifteen minutes.

Datasource

The ICMSTAT_PERF monitor uses the SAP transaction **SMICM** (ICM monitor) as its data source.

Metrics

Table 75 shows the values in the performance table returned by the ICMSTAT_PERF performance monitor.

Table 75 ICMSTAT_PERF Performance Monitor Metrics

Order	Metric Name	Description
1	ICM_Status	The status of the Internet Communication Manager
2	Max_Threads	The defined max. number of open threads allowed by the ICM
3	Peak_Threads	Peak number of open threads in the ICM in a given period
4	Cur_Threads	Number of currently open threads in the ICM
5	Max_Connections	The defined max. number of open connections allowed by the ICM
6	Peak_Connections	Peak number of connections in the ICM in a given period
7	Cur_Connections	Number of current connections in the ICM
8	Max_QueueEntries	The max. number of queued requests allowed by the ICM defined in: `icm/req_queue_len`
9	Peak_QueueEntries	Peak number of queued requests in the ICM in a given period
10	Cur_QueueEntries	Number of currently queued requests in the ICM
11	Running_Threads	Number of work threads waiting for a request (*idle*)
12	Dead_Threads	Number of work threads in a problematic state, for example; dead or hanging
13	Processed_Threads	Number of work threads currently processing a request

JOBREP_PERF

The JOBREF_PERF performance monitor counts the jobs per state in the time period between the end date and time of the last monitor run and the start date and time of the actual monitor run.

Type

The JOBREF_PERF monitor is of type *time-frame* and does not make use of alert types or parameters. One monitor run gathers only one value set. The JOBREF_PERF performance monitor collects SID-related metrics and should run only once per monitored SID, that is: either on the SAP central instance or on *one* application server.

Frequency

It is recommended to run the JOBREF_PERF performance monitor between once an hour and once a day.

Datasource

The JOBREF_PERF monitor uses the SAP transaction **SM37** (background job overview) as its data source.

Metrics

Table 76 shows the values in the performance table returned by the JOBREF_PERF performance monitor.

Table 76 JOBREF_PERF Performance Monitor Metrics

Order	Metric Name	Description
1	RUNNING	The number of jobs with status *running* since the last monitor run
2	READY	The number of jobs with status *ready* since the last monitor run
3	SCHEDULED	The number of jobs with status *scheduled* since the last monitor run
4	RELEASED	The number of jobs with status *released* since the last monitor run
5	ABORTED	The number of jobs with status *aborted* since the last monitor run
6	FINISHED	The number of jobs with status *finished* since the last monitor run
7	PUT_ACTIVE	The number of jobs with status *put_active* since the last monitor run
8	UNKNOWN_STATE	The number of jobs with status *unknown* since the last monitor run

SAPBUFFER_PERF

The SAPBUFFER_PERF performance monitor returns values for the use of SAP memory *buffers* by SAP users for a given instance, for example; hit ratios, buffer quality, free space available and so on in the NetWeaver repository, programs, and database tables.

Use the SAPBUFFER_PERF and SAPMEMORY_PERF performance monitors to collect data previously collected by the SYSBUF_PERF Monitor.

Type

The SAPBUFFER_PERF monitor is of type *time frame*. The SAPBUFFER_PERF performance monitor collects application-server-specific metrics; it should run on each application server whose performance you want to monitor.

Frequency

It is recommended to run the SAPBUFFER_PERF performance monitor once every fifteen minutes.

Data Source

The SAPBUFFER_PERF monitor reads information from the SAP- buffers transaction **ST02**.

Metrics

Table 77 shows the values in the performance table returned by the SAPBUFFER_PERF performance monitor.

Table 77 SAPBUFFER_PERF Performance Monitor Metrics

Order	Metric Name	Description
1	BUFFER_NAME	The name of the buffer
2	HITRATIO	Buffer object reads / logical requests. The buffer hit ratio appears as a percentage.
3	ALLOCATED_SIZE	The amount of space allocated to the buffers [a]
4	FREE_SPACE	The amount of free space (KB) available in the buffer
5	FREE_SPACE_PERCENT	Available free buffer space as a percentage of total
6	MAXDIR_ENTR	The number of directories available for the buffer [b]
7	FREEDIR_ENTR	Number of free directories available for the buffer
8	FDIR_ENTR_PERCENT	Free directories available for the buffer as a percentage

Table 77 SAPBUFFER_PERF Performance Monitor Metrics (cont'd)

Order	Metric Name	Description
9	BUFFER_SWAPS	Swap activity both inwards and outwards since System start [c]
10	BUFFER_SWAPS_DELTA	Difference between the number of buffer swaps measured in the current and previous monitor runs
11	DB_ACCESSES	The number of database accesses since System start [d]
12	DB_ACCESSES_DELTA	Difference between the number of database accesses measured in the current and previous monitor runs

a. Buffer size and "available buffer size" differ because part of the buffer space is used for buffer management.

b. The buffer directories point to the location of the objects stored in the buffer.

c. Buffers swap objects *out* of the buffer to load a new object *in*, if insufficient free space or free directories exist.

d. Database access occurs when an object cannot be read from the buffer.

SAPMEMORY_PERF

The SAPMEMORY_PERF performance monitor returns values for SAP memory use by SAP users for a given instance, for example; roll and paging areas, and extended memory.

Use the SAPBUFFER_PERF and SAPMEMORY_PERF performance monitors to collect data previously collected by the SYSBUF_PERF Monitor.

Type

The SAPMEMORY_PERF monitor is of type *snapshot*: one monitor run gathers one value set. The SAPMEMORY_PERF performance monitor collects application-server-specific metrics; it should run on each application server whose performance you want to monitor.

Frequency

It is recommended to run the SAPMEMORY_PERF performance monitor once every fifteen minutes.

Data source

The SAPMEMORY_PERF monitor reads information from the SAP- buffers transaction **`ST02`**.

Metrics

Table 78 shows the values in the performance table returned by the SAPMEMORY_PERF performance monitor.

Table 78 SAPMEMORY_PERF Performance Monitor Metrics

Order	Metric Name	Description
1	MEMORY_AREA	The type of memory buffer
2	CURRENT_USE_PERCENT	The amount of space currently used expressed as a percentage of the total available
3	CURRENT_USE	The amount of space currently used in KB
4	MAX_USE	The maximum value (max. use) since system startup
5	IN_MEMORY	The amount of space used in shared memory
6	ON_DISK	The amount of space used on the disk

SPOOL_PERF

The SPOOL_PERF performance monitor counts the number of spool requests present in different states.

Type

The SPOOL_PERF performance monitor is of type *time frame* and does not make use of alert types or parameters. One monitor run gathers only one value set. The SPOOL_PERF performance monitor collects SID-related metrics and should run only once per monitored SID, that is: either on the SAP central instance or on *one* application server.

Frequency

It is recommended to run the SPOOL_PERF performance monitor once every 10 to 30 minutes.

Data Source

The SPOOL_PERF performance monitor uses the SAP transaction **`SP01`** (output controller) as its data source.

Metrics

Table 79 shows the values in the performance table returned by the SPOOL_PERF performance monitor.

Table 79 SPOOL_PERF Performance Monitor Metrics

Order	Metric Name	Description
1	ALL_SJ	Total number of spool jobs
2	SJ_ARCHIVE	Number of spool jobs in status archive
3	PRINT_REQ	Total number of print requests
4	OPEN_PR	Number of open print requests
5	SUCCESS_PR	Number of successfully processed print requests
6	ERROR_PR	Number of Print requests with errors
7	FAILED_PR	Number of failed print requests

STATRECS_PERF

The STATRECS_PERF performance monitor reads the statistical records and returns the average response time per transaction.

The STATRECS_PERF performance monitor uses the alert types RESPONSE_TIME and the parameter TRANSACTION to restrict the data selected. The transactions monitored are specified in the parameter TRANSACTION. If this parameter is not specified, the average response time is reported for each transaction in the local statistics file for the specified time frame.

Type

The STATRECS_PERF performance monitor is *time-frame* based. Each run gathers only one value set. To collect a set of values, the monitor must be scheduled on a regular basis. Since the various monitors have different requirements, you have to specify the interval for each monitor individually. This monitor uses the time frame between the last start and the current start times and considers only those transactions which complete within the specified time-frame.

The STATRECS_PERF performance monitor collects application-server-specific metrics; it should run on each application server whose performance you want to monitor.

Frequency

It is recommended that you configure the STATRECS_PERF performance monitor to run once a minute.

Data Source

The STATRECS_PERF performance monitor uses the following SAP transaction as its data source:

- For SAP 7.0 and higher: STAD
- For other supported SAP versions:STAT

Metrics

Table 80 shows the values in the performance table returned by the STATRECS_PERF performance monitor.

Table 80 STATRECS_PERF Performance Monitor Metrics

Order	Metric Name	Description
1	SAP_TCODE	Transaction code associated with the measured transaction. This metric is only visible with the HP Performance Manager.
2	SAP_RESPONSE_TIME	Time SAP takes to respond
3	SAP_NET_TIME	Net Time
4	SAP_REC_COUNT	The number of times the measured transaction occurs

Configuring and Uploading STATRECS_PERF

To enable the STATRECS_PERF monitor, you must configure the `r3perfstat.cfg` file and upload the results into SAP. There are two possible configurations:

- Global: `global_r3perfstat.cfg`
- Local: `local_r3perfstat.cfg`

To set and upload the STATRECS_PERF configurations:

1 **Open and edit the r3perfstat.cfg configuration file**

Use the configuration-file policy editor to modify the `global_r3perfstat` policy to suit the needs of your environment:

a In the details pane of the HPOM for Windows console, select and right-click the configuration-file policy `global_r3perfstat`. The `global_r3perfstat` policy is located in the folder:

Policy Management > SPI for SAP > ConfigFile

b Click the following option in the menu which pops up:

All Tasks > Edit...

HPOM for Windows displays the `global_r3perfstat` policy shown in Figure 23 on page 236.

2 **Modify and save the r3perfstat.cfg configuration file**

Change any values as required and save the file. The `global_r3perfstat` configuration-file policy resides on the HPOM for Windows management server; you must deploy it to the managed nodes whose statistical records you want to monitor and, in addition, upload it to SAP NetWeaver.

For local configuration files, we suggest you include the name of the machine for which the local configuration is intended in the local-configuration file name, for example; `<machine_name>_r3perfstat.cfg`. Note that local configuration settings override global ones.

3 **Deploy the r3perfstat.cfg file to the managed node**

You need to deploy the modified `r3perfstat.cfg` file to the SAP NetWeaver servers, whose statistical records you want to monitor with the SPI for SAP, as follows:

a Locate and right-click the configuration file `r3perfstat.cfg` and browse to the following option in the menu which pops up:

All Tasks > Deploy on...

b In the Deploy Policies on... dialog which appears, select the managed nodes to which you want to deploy the new `r3perfstat.cfg` file, and then click **OK**.

c Verify that the deployment completes successfully by monitoring progress in the Deployment Jobs pane at the bottom of the HPOM for Windows console.

4 **Upload the new configuration to SAP NetWeaver**

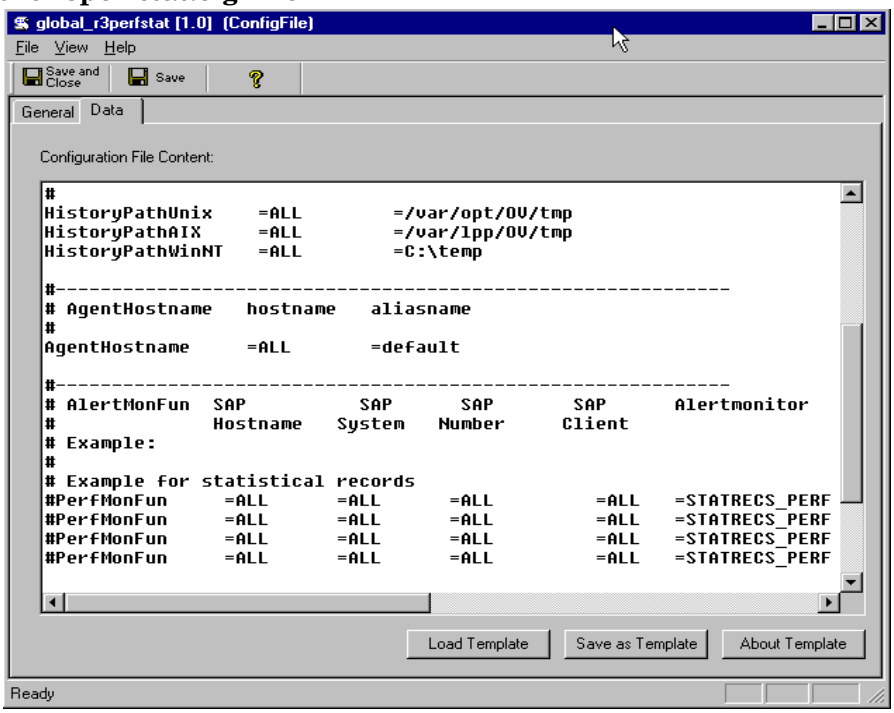
Upload the `global_r3perfstat` configuration to SAP NetWeaver using the Write Statistical Records tool, which you can find in the SAP R/3 Admin tools group.

a Locate and right-click the Write Statistical Records tool and browse to the following option in the menu which pops up:

All Tasks > Launch Tool...

b In the Edit Parameters... dialog which appears, select the managed nodes where you want to launch the tool, and then click **OK**.

Figure 23 Editing the r3perfstat.cfg File



SYSUP_PERF

The SYSUP_PERF performance monitor is used to determine whether the SAP NetWeaver system is available or not.

Type

The SYSBUF_PERF performance monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set.

Frequency

The SYSBUF_PERF performance monitor runs once a minute; the run frequency cannot be modified.

Data Source

The SYSUP_PERF performance monitor uses internal SAP RFC calls as its data source.

Metrics

Table 81 shows the values in the performance table returned by the SYSUP_PERF performance monitor.

Table 81 SYSUP_PERF Performance Monitor Metrics

Metric Name	Description
SYSTEM_STATUS	Status of the System (UP/DOWN) on the basis of the following values: • SAP System available • SAP System logon failure • SAP System communication problems • SAP System unknown Indicates that the performance agent was not running and could not collect any data.

UPDATE_PERF

The UPDATE_PERF performance monitor is used to determine whether update errors are occurring.

When the SAP NetWeaver system is behaving well, no update errors should occur. However, an update error can occur, if an update is performed on a database table record that has previously been deleted. A normal update process should not have to wait in status INIT for more than 5 minutes for an update task. If a greater number of work processes exist with the status INIT the reason could be that a table space is full.

Type

The UPDATE_PERF monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set. The UPDATE_PERF performance monitor collects SID-related metrics and should run only once per monitored SID, that is: either on the SAP central instance or on *one* application server.

Frequency

It is recommended you configure the UPDATE_PERF performance monitor to run once a minute.

Data Source

The UPDATE_PERF monitor uses the SAP transaction **`SM13`** (update records) as its data source.

Metrics

Table 82 shows the values in the performance table returned by the UPDATE_PERF performance monitor.

Table 82 UPDATE_PERF Performance Monitor Metrics

Order	Metric Name	Description
1	ALL	Number of all VB-update tasks
2	INITIAL	Number of initial VB-update tasks
3	ERRONEOUS	Number of erroneous VB-update tasks
4	VB1	Number of update tasks having V1 executed
5	VB2	Number of update tasks having V2 executed

USER_PERF

The USER_PERF performance monitor provides important information about the number of users and user sessions per SAP client for a given SAP application server.

Type

The USER_PERF monitor is of type *snapshot*: one monitor run gathers one value set. The USER_PERF performance monitor collects application-server-specific metrics; it should run on each application server whose performance you want to monitor.

Frequency

It is recommended to run the USER_PERF performance monitor once every five minutes.

Data source

The USER_PERF performance monitor the SAP transaction **SM04** (overview of users) as its data source.

Metrics

Table 83 shows the values in the performance table returned by the USER_PERF performance monitor.

Table 83 USER_PERF Performance-Monitor Metrics

Order	Metric Name	Description
1	USER_CLIENT	The SAP client number associated with the users
2	USER_CNT	The number of users logged in per client
3	SESSION_CNT	The total number of user sessions per client

WLSUM_PERF

The performance monitor, WLSUM_PERF, collects the performance workload statistics for the last full hour. You can display the workload statistics for all task types, for example; dialog, background, RFC, ALE, or update. The WLSUM_PERF performance monitor is mandatory; you must configure it for every application server that you want to monitor.

The data collection for the `WLSUM` monitor is based on the internal SAP job `COLLECTOR_FOR_PERFORMANCEMONITOR`. This job must run with the same frequency as specified for `WLSUM_PERF` in `r3perfagent.cfg`. `WLSUM_PERF` will then pick up the data collected by the last run of `COLLECTOR_FOR_PERFORMANCEMONITOR`.

Type

The WLSUM_PERF performance monitor is of type *time-frame* and does not make use of alert types or parameters. One monitor run gathers only one value set. The WLSUM_PERF performance monitor collects application-server-specific metrics; it should run on each application server whose performance you want to monitor.

Frequency

Due to the way in which the performance monitor, WLSUM_PERF, measures and records time, it is *mandatory* to configure the WLSUM_PERF performance monitor to run once an hour.

Data source

The WLSUM_PERF performance monitor uses the SAP transaction **`ST03`** (workload analysis) as its data source.

Metrics

Table 84 shows the values in the performance table returned by the WLSUM_PERF performance monitor.

Table 84 WLSUM_PERF Performance Monitor Metrics

Order	Metric Name	Description
1	Hostname	The SAP System hostname
2	SID	The SAP System ID
3	INSTANCE	The SAP instance number, if SAP version < 4.6x
4	TASKTYPE	Type of SAP NetWeaver task (RFC, dialog)
5	CNT	The number of dialog steps
6	DBACTIVCNT	Counter for database-active dialog steps
7	RESPTI	Time that elapses between a dialog sending a request to the dispatcher and receiving a response
8	CPUTI	CPU time used in the work process
9	QUEUETI	The time an unprocessed dialog step waits in the dispatcher queue for a free work process
10	LOADGENTI	Time taken loading and generating objects such as ABAP source code and screen information from the database
11	COMMITTI	Time required for commit to complete
12	DDICTI	Time required for Data Dictionary
13	QUETI	Time required for batch-input queue
14	CPICTI	Time required for RFC and CPI-C
15	ROLLINCNT	Number of roll-ins (rolled-in user contexts)
16	ROLLINTI	Processing time for roll-ins
17	ROLLOUTCNT	Number of roll-outs (rolled-out user contexts)
18	ROLLOUTTI	Processing time for roll-outs
19	READDIRCNT	Number of direct read accesses
20	READDIRTI	Time for direct read access
21	READSEQCNT	Number of sequential read attempts
22	READSEQTI	Time for sequential read accesses

Table 84 WLSUM_PERF Performance Monitor Metrics (cont'd)

Order	Metric Name	Description
23	CHNGCNT	Number of modified database accesses
24	CHNGTI	Time for modified database accesses
25	BYTES	Number of bytes
26	GUITIME	Total time taken for the dispatcher to execute a GUI request
27	GUICNT	Count of GUI steps
28	GUINETTIME	Time taken for the application server to respond to a request from the SAP GUI

WP_PERF

The SPI for SAP performance agent uses the WP_PERF monitor to detect performance problems concerning SAP work processes. For example, WP_PERF can detect and report on the following situations:

- Work processes need to wait for semaphores
- Work processes are in *private* mode
- A dialog work-process does not return to idle after use/release

Type

The WP_PERF monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set. The WP_PERF performance monitor collects application-server-specific metrics; it should run on each application server whose performance you want to monitor.

Frequency

It is recommended you configure the WP_PERF performance monitor to run once every 15 minutes.

Data Source

The WP_PERF performance monitor uses SAP transaction **`SM50`** (work- process overview) as its data source.

Metrics

Table 85 shows the values in the performance table returned by the performance monitor.

Table 85 WP_PERF Performance Monitor Metrics

Order	Metric Name	Description
1	ALL_WP	Number of all work processes
2	SEMAPHORE_WP	Number of work processes waiting on a semaphore
3	DEBUG_WP	Number of work processes in debug mode
4	LONG_RUNNING	Number of long running dialog wp
5	PRIVAT_WP	Number of dialog `wp` in private mode
6	NOSTART_WP	Number of dialog `wp` with no restart capability
7	DIA_IDLE	Number of idle dialog work processes
8	DIA_ALL	Number of dialog work processes
9	DIA_RUNNING	Number of running dialog `wp`
10	BTC_IDLE	Number of idle batch work processes
11	BT_ALL	Number of batch work processes
12	BTC_RUNNING	Number of running batch `wp`
13	SPO_IDLE	Number of idle spool work processes
14	SPO_ALL	Number of spool work processes
15	SPO_RUNNING	Number of running spool `wp`
16	ENQ_IDLE	Number of idle enqueue work processes
17	ENQ_ALL	Number of enqueue work processes
18	ENQ_RUNNING	Number of running enqueue `wp`
19	UPD_IDLE	Number of idle update work processes
20	UPD_ALL	Number of update work processes
21	UPD_RUNNING	Number of running update `wp`
22	UPD2_IDLE	Number of idle update2 work processes
23	UPD2_ALL	Number of update2 work processes
24	UPD2_RUNNING	Number of running update2 work processes

Removing the SAP/Performance Subagent

To remove the SAP/Performance subagent from the managed node, you need to perform the following steps in the order indicated:

1. Before starting the process of removing the SPI for SAP SAP/Performance subagent from the managed node, make sure that you *stop* the SPI for SAP SAP/Performance subagent, for example;
   - Use the SPI for SAP application, `PerfAgt Stop`, which resides in the `SAP R/3 UN*X` or `SAP R/3 NT` Tools Group.
   - Login to the SAP managed node and use the following command on the command line:

     `r3perfagent stop`
2. In the HPOM for Windows console, browse to the following tools folder:

   Tools > SPI for SAP > SAP R/3 Admin
3. Select and right-click the appropriate Performance Package tool (according to the operating system) for the SAP System environment as illustrated below:
   - **Remove Performance Package (UNIX)**
   - **Remove Performance Package (Windows)**
4. Start the Remove Performance Package tool you have selected using the following menu option:

   All tasks > Launch Tool...
5. Select the SAP managed node(s) from which you want to remove the Performance Package. Remember to ensure that the nodes you select correspond to the operating system for the chosen tool (UNIX or Microsoft Windows).
6. Click **Launch...** to start the removal process.

7 The SAP ITS Monitor

This section describes how to install, configure, use, and remove the SPI for SAP monitor for SAP ITS 6.20.

In this Section

The information in this section introduces you to the SPI for SAP's ITS monitor and explains how to use it to expand the monitoring capability of the SPI for SAP in such as way as to manage SAP ITS instances, too. In this section, you can find information about the following topics:

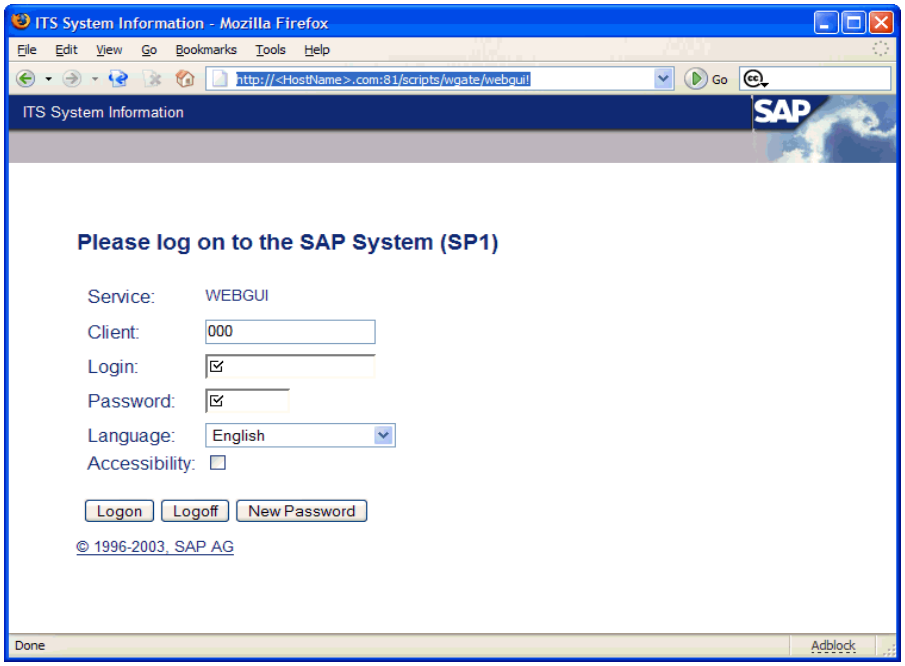
What is ITS?

The SAP **Internet Transaction Server** (ITS) provides the SAP user with an SAP transaction interface in a web browser. With this transaction interface, the SAP user can perform the following tasks:

- Use a web browser to log on to the SAP System
- Make requests for information by entering transactions directly in the SAP system
- Immediately see the results of the transaction request in a web browser by means of the transaction interface provided by ITS

The SAP ITS is only available for Linux and Microsoft Windows operating systems.

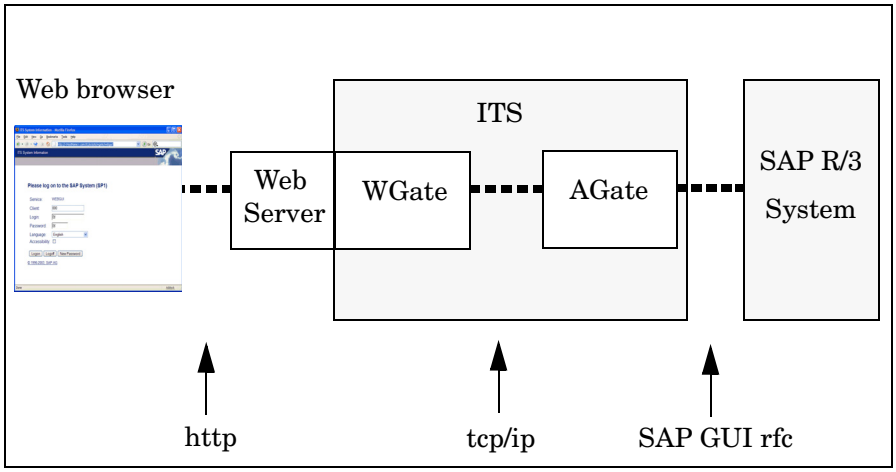
Figure 24 Logging in to SAP with ITS



ITS Installation Scenarios

The ITS server consists of two main components, the **Application Gateway** (AGate) and the **Web Gateway** (WGate). You can monitor both these components with the ITS performance monitor, which the SPI for SAP installs during setup and configuration.

Figure 25 ITS Architecture



Application Gateway

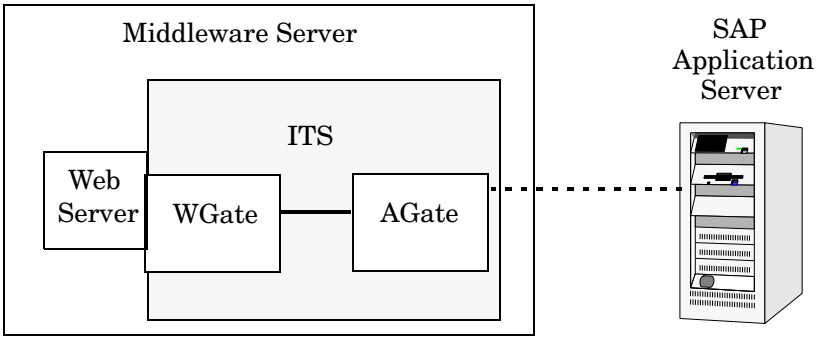
The application gateway links the ITS server to the SAP application server. The AGate is the core processing component of the ITS: it receives web browser requests from the WGate and communicates with the SAP application server by means of either the DIAG or the RFC protocol.

Web Gateway

The Web Gateway connects the ITS server to the Web server. The WGate component is always located on the same host as the Web server. The WGate receives requests from the Web server and then establishes a connection *with* and forwards the requests *to* the AGate.

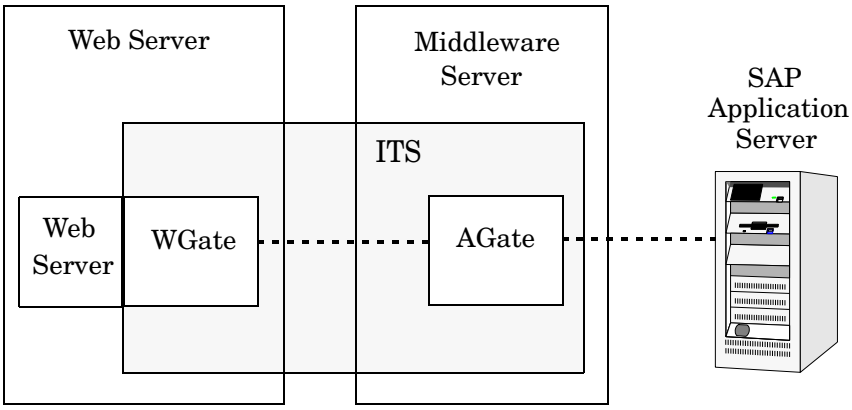
You can either install both components of the ITS, the AGate and the WGate, on a **single-host** or on two *separate* hosts (**dual-host** installation). The single-host installation illustrated in Figure 26 is appropriate for test or development purposes, where small loads are present: the dual-host configuration shown in Figure 27 tends to work better in a production environment, where higher loads are tend to occur.

Figure 26 ITS Single-Host Configuration



In a dual-host installation, the Web server and the WGate run on one host, which must be connected to the client-access network (Internet or intranet) and the AGate runs on the second host, which is connected to the WGate through the TCP/IP network and handles all communication with the SAP System by means of SAP remote function calls.

Figure 27 ITS Dual-Host Configuration



ITS also allows the configuration of multiple AGate and WGate instances, which can share the increased load generated by large numbers of remote users logging on. The scalability feature allows individual AGate instances to communicate with multiple WGate instances and multiple application servers, too. Similarly, to balance overall load, individual WGate instances can communicate with multiple AGate instances.

The ITS 6.20 Monitor

The SPI for SAP includes a dedicated monitor for SAP ITS 6.20 (Internet Transaction Server); the monitor allows you to perform the following actions:

- **Check ITS 6.20 availability**

  You can check the availability of the various components of the ITS 6.20 server, including; AGate, WGate, and Web Server

- **Pinpoint communication problems**

  You can now pinpoint communication problems between the ITS 6.20 components even in an environment with multiple ITS 6.20 instances and complex load sharing

The ITS 6.20 monitor collects data by parsing ITS log files and regularly sending `http` requests for specific information from the ITS server instances.

The ITS 6.20 monitor saves the data it collects along with the data collected by HP Performance Agent or the HP Software Embedded Performance Component (CODA). HP Software performance tools such as the HP Reporter or Performance Manager can then use the correlated data to generate reports and graphs, which can be used to investigate problems, performance issues, and general trends relating to ITS.

The ITS 6.20 monitor allows you to monitor the following aspects of the ITS Application Gateway:

- the status of both local *and* remote AGate instances in one AGate cluster
- the status of each AGate process and AGate-process work thread

Together with HP Internet Services, the `r3monits` monitor allows you to monitor the ITS Web Gateway, too. However, since the ITS Web Gateway's main tasks involve passing requests to and from the internet, whose performance is outside your control, the information you glean from such monitoring is probably not very useful.In this section, you can also find information about the following topics:

- Installing the ITS 6.20 Monitor on page 248
- Verifying the ITS 6.20 Monitor Installation on page 251
- Configuring the ITS 6.20 Monitor on page 251
- ITS 6.20 Status and Availability on page 261

ITS 6.20 Service Reports on page 261

Installing the ITS 6.20 Monitor

The instructions in this section assume that either the HP Software Embedded Performance Component (CODA) or the HP Performance Agent is already running on all HPOM for Windows managed nodes, which you want to monitor with the ITS 6.20 monitor. To install the ITS 6.20 monitor on an HPOM for Windows managed node, you need to perform the steps indicated below. For detailed information about the individual steps, see the appropriate subsections that follow:

- ITS 6.20 Monitor: Installation Pre-requisites on page 249
- ITS 6.20 Monitor Deployment Tasks on page 250

You cannot remove the ITS 6.20 monitor components from the HPOM for Windows managed node in isolation; you can only remove the ITS 6.20 monitor components from the managed node as part of the removal of the SPI for SAP.

ITS 6.20 Monitor: Installation Pre-requisites

Before you start the installation of the ITS 6.20 monitor, make sure that the SAP ITS 6.20 AGate servers on which you have chosen to install the SPI for SAP ITS 6.20 monitor meet the following requirements:

- Your SAP ITS instance must be running on one of the following operating systems:
  - Windows 2003
  - SuSE Linux Enterprise Server (SLES) 8 or 9
  - Red Hat Enterprise Linux (RHEL) 3 or 4
- The installed HPOM for Windows agent must be running.
- Either the HP Performance Agent or the HP Software Embedded Performance Component must be running on the SAP ITS 6.20 server
- SAP ITS 6.20 must be available and appropriately configured.

  The ITS monitor `r3monits` was designed to monitor ITS 6.20 AGate servers *only*; from SAP 6.40 onwards, the SAP design has changed, and the ITS monitor can no longer be used.
- *Optional* - HP Performance Manager must be available (but not necessarily on the ITS 6.20 server machine) if you want to generate and view performance graphs.
- *Optional* - HP Reporter must be available (but not necessarily on the ITS 6.20 server machine) if you want to generate and view service reports. For more information about supported software versions, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.
- The SPI Data Collector instrumentation must be available on the HPOM for Windows management server and deployed to the ITS 6.20 server; for more information about required product versions, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.

Use the ITS 6.20 monitor to monitor the ITS AGate server. If your environment has the AGate and WGate servers running on separate hosts, make sure you install the ITS 6.20 monitor on the host where the AGate instance is running.

If you do not want to use the default settings for the SPI for SAP monitor for ITS 6.20, you need to specify the source you want the ITS 6.20 monitor to use to gather status metrics. For more information about installation pre-requisites and selecting the performance-data source, refer to the *HP Operations Smart Plug-in for SAP Configuration Guide*.

ITS 6.20 Monitor Deployment Tasks

To deploy the ITS 6.20 monitor to the ITS 6.20 servers, which you want to monitor with the SPI for SAP, you need to perform the following steps in the order indicated:

- Deploying the ITS 6.20 Monitor Instrumentation on page 250
- Deploying the Configuration-file Policies for ITS 6.20 on page 250
- Deploying the ITS 6.20 Policies to the Managed Nodes on page 251

Deploying the ITS 6.20 Monitor Instrumentation

To deploy the ITS 6.20 monitor instrumentation to the ITS 6.20 server which you want to monitor:

1. In the HPOM for Windows console, select and right-click the SAP (managed node) where you want to deploy the ITS 6.20 components.
2. Browse to the following menu option:

   All Tasks > Deploy instrumentation
3. In the Deploy Instrumentation... window, select the following items:
   - SPI Data Collector
   - SPI for SAP Instrumentation
4. Click **OK**.

You can monitor the deployment in real time in the Deployment Jobs pane at the bottom of the HPOM for Windows console.

Deploying the Configuration-file Policies for ITS 6.20

To deploy the configuration-file policies to the ITS 6.20 server which you want to monitor:

1. In the HPOM for Windows console, browse to the following folder:

   Policy management > Policy groups > SPI for SAP
2. Select `global_r3itosap` and all policies beginning with `global_r3monits`
3. Right-click and browse to the following option in the menu, which pops up:

   All Tasks > Deploy on...
4. In the Deploy Polices on... window which appears, select the managed nodes where you want to deploy the configuration-file policies.
5. Click **OK**.

You can monitor the deployment in real time in the Deployment Jobs pane at the bottom of the HPOM for Windows console window.

Deploying the ITS 6.20 Policies to the Managed Nodes

To deploy the ITS 6.20 policies on the ITS 6.20 servers, which you want to monitor with the SPI for SAP:

1 In the HPOM for Windows console, browse to the following folder:

Policy management > Policy groups > SPI for SAP > SAP ITS 6.20

2 Select and right-click the following files:

- `r3monits` (Scheduled Task)
- `SAP R3 opcmsg` (Open Message Interface)

3 Browse to the following option in the menu, which pops up:

All Tasks > Deploy on...

4 In the Deploy Polices on... window which appears, select the managed nodes where you want to deploy the ITS 6.20 policies.

5 Click **OK**

You can monitor the deployment in real time in the Deployment Jobs pane at the bottom of the HPOM for Windows console.

Verifying the ITS 6.20 Monitor Installation

This section describes how to verify that the installation of the ITS 6.20 monitor completes successfully:

1 In the HPOM for Windows console, select and right-click the ITS 6.20 node and browse to the following option in the menu which pops up:

View > Policy Inventory

2 In the right-hand (details) pane of the HPOM for Windows console, check for the presence of the items displayed in the list below:

- `r3monits` (scheduled task)
- `r3itosap` (central configuration file)
- `global_r3monits` (configuration file)
- `SAP R/3 opcmsg` (OpC message Interface)

Configuring the ITS 6.20 Monitor

This section describes how to configure the ITS 6.20 monitor. To carry out the tasks described in this section, you must first install the ITS 6.20 monitor and, in addition, verify that the installation completes successfully.

The ITS 6.20 monitor collects availability data from ITS 6.20 using HTTP commands. The HTTP commands request status information from the ITS 6.20 components, which are configured and running. This section provides detailed information about the following topics:

- ITS 6.20 Monitor: Selecting the Performance-Data Source on page 252

ITS 6.20 Monitor: Selecting the Performance-Data Source

HPOM Smart Plug-ins can use either the HP Performance Agent or the HP Software Embedded Performance Component (CODA) as the default source for the performance data required for graphing in HP Performance Manager and HP Reporter. For more information about selecting performance-data sources, see Selecting the Performance-data Source on page 209.

ITS 6.20 Monitor: Configuration Tasks

Although the ITS 6.20 monitor uses information in the ITS 6.20 `global.srvc` configuration file to provide a default configuration automatically, you still need to set up the ITS 6.20 monitor to collect information on the managed node. For example, you need to configure some environment variables and ensure that ITS 6.20 commands work correctly.

To configure the SPI for SAP monitor for ITS 6.20:

1 Set the SAP_REGISTRY_PATH environment variable

To find the installation location of the ITS 6.20 on the AGate node, the `r3monits` monitor needs the environment variable SAP_REGISTRY_PATH to point to the ITS 6.20 XML registry. This variable must be visible to the HPOM agent. On Windows operating systems, the variable is set during the installation of ITS 6.20. On Linux operating systems, you have to set the variable manually.

If you do not change the suggested installation directories, the default values for the SAP_REGISTRY_PATH environment variable are as follows:

- **Linux operating systems:**

  `/usr/sap/its/6.20/config`

- **Windows operating systems:**

  `C:\Program Files\SAP\ITS\6.20\config`

2 Configure the `its_ping` service.

The `r3monits` monitor uses information in the ITS 6.20 `global.srvc` configuration file to provide a default configuration automatically. However, since the `r3monits` monitor uses the `its_ping` service to determine the status of the system, you must configure the `its_ping` service by using the ITS 6.20-administrator web console to add the following entries together with the appropriate values to the file `its_ping.srvc`:

- `~client`, for example: `000`
- `~language`, for example: `EN`
- `~login`, for example: *`<valid_SAP_user>`*
- `~password`, for example: *`<password_for_valid_SAP_user>`*

3 Check that the configuration of the `its_ping` service completes successfully.

Open a web browser and enter the following URL:

http://<WGateHost>:<WGatePort>/scripts/wgate/its_ping/!?~agate_routing=<AGateHost>:0

If you configure the `its_ping` service correctly, the browser displays a page indicating the status of the SAP System you want to access.

Figure 28 Configuring its_ping with the ITS 6.20 Administrator GUI

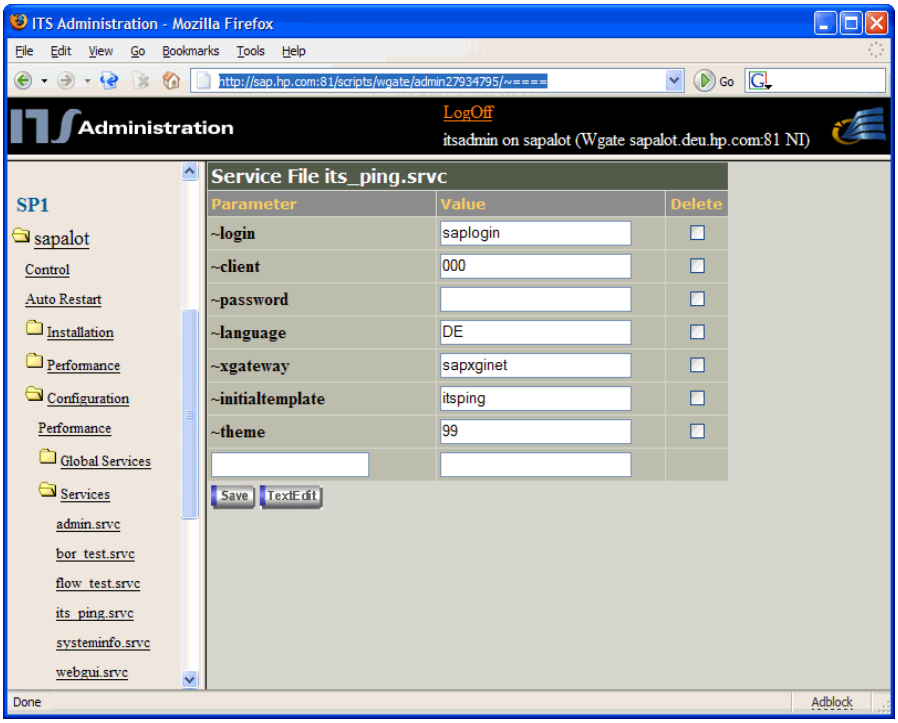


Figure 28 shows you how to set up the `its_ping` service using the ITS 6.20 administrator GUI.

ITS 6.20 Monitor: Default Configuration

The ITS 6.20 monitor stores configuration details in the file, `r3monits.cfg`. After installation, the ITS 6.20 monitor uses the default version of the configuration file shown in The ITS 6.20 Monitor Configuration File. For more information about where to find the configuration file for the ITS 6.20 monitor, see ITS 6.20 Monitor: File Locations on page 254.

The ITS 6.20 Monitor Configuration File

```
# The r3monits.cfg file
# TraceLevel   hostname    only error messages =  1
#                          info messages       =  2
#                          debug messages      =  3
#                          Disable             =  0
TraceLevel     =ALL        =0
#-------------------------------------------------------------
# TraceFile  hostname    filename
TraceFile    =ALL        =r3monits.log
#-------------------------------------------------------------
# History          hostname    path
# Path
HistoryPathWinNT   =ALL        =default
```

```
HistoryPathUnix    =ALL        =default
#-------------------------------------------------------------
# Datafiles    hostname    path
# location
DatafilesLocation  =ALL        =default
#-------------------------------------------------------------
# RemoteMonitoring  LocalHost     RemoteHost  ITS     ITS        min   \
#                                             System  SystemNr   AGates\
# ITS        ITS          SAP     SAP         SAP
# WGatehost  WGateport    System  appserver   Number
#
#RemoteMonitoring     =local        =remote     =SID    =00        =1  \
# =wgate     =00          =SID    =appserv   =00
#-------------------------------------------------------------
# WebServer   ITS         ITS         hostname      port
#             hostname    System ID
WebServer     =ALL        =ALL        =default      =default
#-------------------------------------------------------------
# AGate       ITS         ITS         Alias
#             hostname    System ID   hostname
AGate         =ALL        =ALL        =default
#-------------------------------------------------------------
# ITSPerfMon ITS         ITS          Threshold   Enable/   \
#            hostname    System ID                Disable   \
#            OpC         OpC         OpC
#            Severity    Object      MessageGroup
ITSPerfMon   =ALL         =ALL        =default    =1       \
             =WARNING    =ITS        =R3_ITS
ITSPerfMon   =ALL         =ALL        =1          =1       \
             =CRITICAL   =ITS        =R3_ITS
#-------------------------------------------------------------------------------
---
```

ITS 6.20 Monitor: File Locations

The ITS 6.20 monitor installs the configuration files it reads and the trace files it writes in the following location on the HPOM for Windows managed node (ITS 6.20 server):

- **Linux Operating Systems:**
  - Binaries: `<OvDataDir>/bin/instrumentation/`
  - Configuration files: `<OvDataDir>/conf/sapspi/[global|local]`
  - Trace files: `<OvDataDir>/log/`
- **Windows Operating Systems:**
  - Binaries: `%OvDataDir%\bin\instrumentation`
  - Configuration files: `%OvDataDir%\conf\sapspi\[global|local]`
  - Trace files: `%OvDataDir%\log`

Table 86 lists the files the r3monits monitor uses.

Table 86 r3monits Files

File	Description
`r3monits(.exe)`	Executable for the SAP R/3 ITS 6.20 monitor
`r3monits.cfg`	Configuration file for the SAP R/3 ITS 6.20 monitor. See The ITS 6.20 Monitor Configuration File.
`r3monits.his`	Monitor history file created during the first monitor run of the SAP R/3 ITS 6.20 monitor
`r3monits.log`	File used to store information when tracing is enabled for the SAP R/3 ITS 6.20 monitor

ITS 6.20 Monitor: Configuration-File Key Words

The SPI for SAP provides a default configuration for the ITS 6.20 monitor, which works without modification immediately after installation. However, if you want to set up the ITS 6.20 monitor for the particular demands of your SAP environment, you can modify the `r3monits.cfg` file by enabling or disabling the key words in the following list and, where necessary, setting the appropriate parameters. This section provides detailed information about the following keywords:

- TraceLevel
- TraceFile
- HistoryPath
- DatafilesLocation
- RemoteMonitoring
- WebServer
- AGate
- ITSPerfMon

TraceLevel

The TraceLevel keyword accepts the following parameters:

```
TraceLevel =<Hostname> =<TraceLevel>
```

- **Hostname:**

=ALL	Monitor all SAP ITS 6.20 servers with the SPI for SAP ITS 6.20 monitor. This is the default setting.
=<*ITS_host*>	The name of the SAP ITS 6.20 server, where you want to specify a trace level. Use a new line for each individual SAP ITS 6.20 server.

- **TraceLevel:**

=0	Disable; this is the default setting.
=1	Log only error messages
=2	Log only informational messages
=3	Log everything, including debug messages
=-1	Test output

TraceFile

The TraceFile keyword accepts the following parameters:

```
TraceFile =<Hostname> =<Filename>
```

- **Hostname:**

=ALL	Monitor all SAP ITS 6.20 servers with the SPI for SAP ITS 6.20 monitor. This is the default setting.
=<*ITS_host*>	The name of a specific SAP ITS 6.20 server where you want to enable tracing and where you want the monitor to write the trace file. Use a new line for each individual SAP ITS 6.20 server.

- **Filename:**

  =`r3monits.log` - which is the default setting or, alternatively, the name of the file to which you want to write the trace log and, if necessary, the path. For more information about the location of the `r3monits` binaries, see ITS 6.20 Monitor: File Locations on page 254.

HistoryPath

The HistoryPathUnix and HistoryPathWinNT keywords accept the following parameters:

```
HistoryPathUnix =<Hostname> =<Path>
HistoryPathWinNT =<Hostname> =<Path>
```

- **Hostname:**

=ALL	All SAP ITS 6.20 servers, which the SPI for SAP monitors. This is the default setting.
=<*ITS_host*>	The name of the SAP ITS 6.20 server where you want to specify the path to the monitor history file. Use a new line for each individual SAP ITS server.

- **Path:**

=default	Path to (and name of) the file containing information about monitor runs. The default is: `<`*`OvDataDir`*`>/conf/sapspi` or `%`*`OvDataDir`*`%\conf\sapspi` for Linux and Windows operating systems respectively.

DatafilesLocation

The default location of the files containing the data, which the Performance Manager and HP Reporter use; the DatafilesLocation keyword accepts the following parameters:

```
DatafilesLocation =<Hostname> =<Path>
```

- **Hostname:**

=ALL	All SAP ITS 6.20 servers, which the SPI for SAP monitors. This is the default setting.
=<*ITS_host*>	The name of the SAP ITS 6.20, where you want to specify the path to the monitor history file. Use a new line for each individual SAP ITS server.

- **Path:**

=default	Defines the path to location of the datafiles; the default values are as follows:
	• **Linux Operating Systems:**
	`<OvDataDir>/datafiles`
	• **Windows Operating Systems:**
	`%OvDataDir%\datafiles`

The HP Performance Agent uses the directory specified in DatafilesLocation to store its datafiles; datafiles contain performance and availability data, which reports and graphs display. If you are using the HP Software Embedded Performance Component, which uses an internal data store, you still need to specify a valid datafiles location, since the location is required for internal use.

RemoteMonitoring

Configures the remote-monitoring feature of the ITS 6.20 monitor, `r3monits`, and requires a value for the following parameters:

```
RemoteMonitoring =<LocalHost> =<RemoteHost> =<ITS SystemID> =<ITS SystemNr>
=<Min Agates> =<ITS WgateHost> =<ITS WGatePort> =<SAP System> =<SAP appserver>
=<SAP Number>
```

- **LocalHost:**

  The name of the managed node that performs the remote monitoring

- **RemoteHost**

  The name of the ITS 6.20 AGate host you want to monitor remotely

- **ITS SystemID:**

  The System ID <*SID*> of the ITS 6.20 system you want to monitor on the remote host, for example: "IT1"

- **ITS SystemNr:**

  The number of the monitored ITS 6.20 System running on the remote host, for example: "00"

- **Min AGates:**

  The configured minimum number of running AGate processes allowed on the remote ITS 6.20 AGate

- **ITS WGatehost:**

  The WGate of the monitored ITS 6.20 AGate host

- **ITS WGateport:**

  The port of the WGate's web-server, for example: "80"

- **SAP System:**

  <SID> of the SAP System connected to the monitored ITS 6.20 instance, for example: "SP1"

- **SAP appserver:**

  The SAP application server used by the monitored ITS 6.20 instance

- **SAP Number:**

  The instance number of the SAP System connected to the monitored ITS 6.20 instance

WebServer

The WebServer keyword accepts the following parameters:

```
WebServer =<ITSHostName> =<ITSSystemID> =<HostName> =<Port>
```

- **ITS Hostname:**

=ALL	Monitor all SAP ITS 6.20 servers with the SPI for SAP. This is the default setting.
=<*ITS_host*>	The host name of a specific SAP ITS 6.20 server which you want to monitor. Use a new line for each individual SAP ITS 6.20 Server.

- **ITS System ID:**

=ALL	Monitor all SAP ITS 6.20 Systems with the SPI for SAP. This is the default setting.
=<*ITS_SID*>	The ID of a specific SAP ITS 6.20 System which you want to monitor, for example; "DEV". Use a new line for each individual SAP ITS 6.20 SID.

  — **Hostname:**

  The hostname of the WGate, whose status you want to probe:

=default	The default host name is the value of `~hostunsecure` configured in the `global.srvc` file for the corresponding ITS 6.20 instance.
=<*HostName*>	The name of the host on which the WGate web server is running.

- **Port:**

  The port on which the WGate web server is listening on the configured host:

=default	The default port is the value of `~portunsecure` configured in the `global.srvc` file for the corresponding ITS 6.20 instance.
=<*PortNumber*>	The number of the port on which the WGate web server is listening if different from the default value.

AGate

Specifies a different hostname for the AGate host. The AGate keyword accepts the following parameters:

```
Agate =<ITSHostName> =<ITSSystemID> =<AliasHostname>
```

- **ITS Hostname:**

=ALL	Monitor all SAP ITS 6.20 AGate servers with the SPI for SAP. This is the default setting.
=<*ITS_host*>	The host name of a specific SAP ITS 6.20 AGate server which you want to monitor. Use a new line for each individual SAP ITS 6.20 AGate Server.

- **ITS System ID:**

=ALL	Monitor all SAP ITS 6.20 Systems with the SPI for SAP. This is the default setting.
=<*ITS_SID*>	The ID of the SAP ITS 6.20 System which you want to monitor, for example; “DEV”. Use a new line for each individual SAP ITS 6.20 SID.

  - **Alias Hostname:**

    An alias for the ITS 6.20 AGate host as defined in the `ItsRegistryWGATE.xml` of the selected WGate host:

=default	The default alias is the short host name of the AGate where the ITS 6.20 monitor is running.
=<*HostName*>	The name of the host on which the AGate is running. It is essential that the host name defined here is the same as the hostname specified in the `ItsRegistryWGATE.xml` on the WGate host.

ITSPerfMon

The ITSPerfMon keyword configures the web server of the routing path and *requires* a value for the following parameters:

```
ITSPerfMon =<ITSHostName> =<ITSSystemID> =<Threshold> =<OpCSeverity>
=<OpCObject> =<OpCMessageGroup>
```

- **ITS Hostname:**

=ALL	Monitor all SAP ITS 6.20 servers with the SPI for SAP. This is the default setting.
=<*ITS_host*>	The host name of a specific SAP ITS 6.20 server where you want to enable monitoring. Use a new line for each individual SAP ITS 6.20 Server.

- **ITS System ID:**

=ALL	Monitor all SAP ITS 6.20 Systems with the SPI for SAP. This is the default setting.
=<*ITS_SID*>	The SAP ITS 6.20 System ID (SID) which you want to monitor, for example; “DEV”. Use a new line for each individual SAP ITS 6.20 SID.

- **Enable/Disable:**

=0	Disable the ITS 6.20 monitor
=1	Enable the ITS 6.20 monitor. This is the default setting.

  - **Threshold:**

=default	The minimum number of processes allowed. The default threshold is the value of "MinAGates" as configured in the ITS 6.20 XML registry and represents the number of AGate processes usually running during normal usage of ITS 6.20.
=<*integer*>	<*integer*> is the minimum number of AGate processes that are allowed during normal ITS 6.20 usage. If <*integer*> is 5, and 3 AGate processes are running, an alert is sent to the management server.

  - **OpC Severity:**

=<*Severity*>	The severity status of the HPOM message that the `r3monits` monitor sends when a threshold rule is violated. Possible values are CRITICAL, WARNING, MAJOR, MINOR, NORMAL, UNKNOWN.

- **OpC Object:**

=<*object*>	The object of the HPOM message that is sent when the threshold rule is violated.

- **OpC Message Group:**

=<*object*>	The message group assigned to the HPOM message that the SPI for SAP sends when the threshold rule is violated.

ITS 6.20 Status and Availability

The ITS 6.20 monitor checks the availability of the various critical components of the ITS server, including; the Application Gateway, the Web Gateway, and the Web Server itself. The ITS 6.20 monitor also monitors the connections between the critical components so that it can pinpoint potential and existing communication problems. This capability is particularly important in an environment which has multiple ITS instances and complex load sharing.

This section describes the messages which the ITS 6.20 monitor sends to HPOM for Windows if it discovers a problem when checking the availability of SAP ITS on the managed nodes you have asked it to monitor:

- **The connection between AGate and WGate is down**

  `The connection between the ITS Instance: <Instance Name> on host: <Hostname> and the Web server: <Webserver-Hostname>:<Portnumber> is down.`

- **The WGate does not recognize the configured AGate host**

  `Bad monitor configuration: WGate <hostname>:<port> does not recognize configured AGate <hostname>`

- **Unexpected response from WGate**

  `Unexpected response from WGate <hostname>:<port> while trying to reach AGate <hostname>.`

- **AGate cannot login to R/3**

  `The AGate <hostname> of ITS SID <SID> cannot login to the R/3 system <R/3Connection> - <SAPSID> [Reason: <details>]`

- **Process threshold violation**

  `Number of running AGate processes (<nr>) on host <hostname> is below the configured threshold of <nr> for ITS SID <SID>.`

- **Error during performance Agent configuration**

  `The r3monits is unable to configure the performance agent datasource.`

ITS 6.20 Service Reports

This section describes how to use the HP Reporter to examine the data collected by the SPI for SAP monitor for ITS 6.20. For a complete list of the ITS reports available with the SPI for SAP, see Table 90 on page 365. This section covers the following topics:

ITS 6.20 Service Reports: Installation Pre-requisites

You will need to ensure that the following products are installed and configured before you can use the HP Reporter to generate and view reports relating to information collected by the ITS 6.20 monitor:

- HP Reporter
- SPI for SAP ITS 6.20 monitor Reports Snap-In

ITS 6.20 Service Reports: Configuring the HP Reporter

The installation of the SPI for SAP service reports described in Installing the SPI for SAP Reports on page 356 automatically completes most of the installation and configuration of the ITS 6.20 service reports. However, you should perform the following steps:

1. **Add managed nodes to the Reporter**

   Check that the individual SAP ITS systems you want to monitor with the ITS 6.20 monitor have been added to (and discovered by) the HP Reporter. The Reporter automatically attempts to discover all the new systems you add to it. If it cannot find a node, Reporter will not be able to generate any reports for that node.

2. **Schedule the report generation**

   Remember to schedule a job to generate reports for the ITS 6.20 systems

Viewing ITS 6.20 Service Reports

To view the complete list of the ITS 6.20 monitor reports, you can use one of several options:

- Click the **`View Reports`** button in the Reporter window
- Browse to the following file/directory on the Reporter machine, *`host.name.com`*:

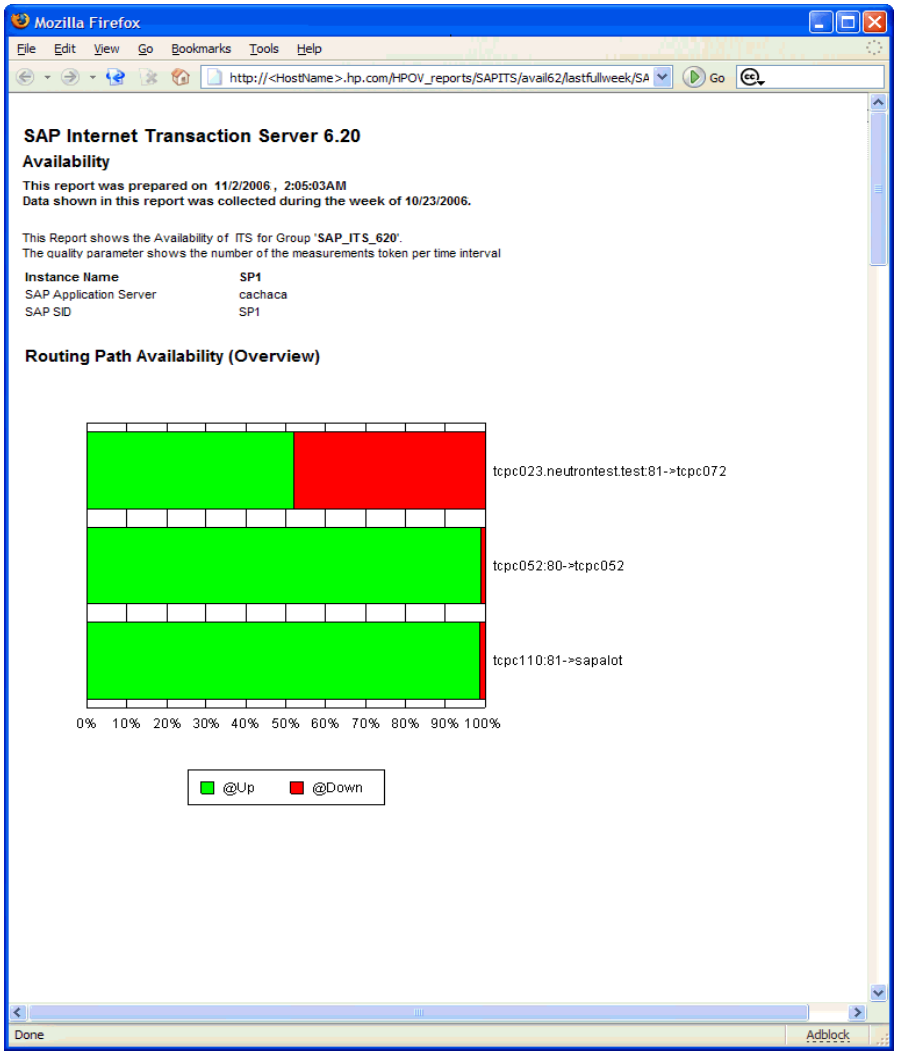
  `\\<`*`host.name.com`*`>\rpmtools\Data\Webpages\reports.htm`
- open a (remote) Web-browser window and enter the following URL:

  http://<host.name.com>/HPOV_reports/reports.htm

  Note that this assumes that a Web server is running on the Reporter machine *`host.name.com`*.

In the page that appears, browse to the group of reports that you want to examine, for example: SAP ITS 620 Last Full Week. Next, you can select an individual report from the list of reports displayed; the report in Figure 29 shows an overview of the availability of the routing path in a SAP ITS 6.20 instance over the last full week.

Figure 29 ITS 6.20 Reports



8 Monitoring SAP NetWeaver Web Application Server (J2EE)

The SPI for SAP helps you monitor the health of the J2EE engine of the SAP NetWeaver Web Application Server. With the help of a series of policies, you can collect metrics indicating the health, availability, and performance of the J2EE engine of an SAP NetWeaver Web Application Server. All the policies, necessary for monitoring the J2EE engine of SAP NetWeaver, are grouped under the SAP NetWeaver Java Monitoring policy group.

You cannot use the policies under the SAP NetWeaver Java Monitoring policy group to monitor the Web AS (Java) environment of an SAP R/3 environment. For an SAP R/3 deployment, you can use the `SAPSPI_CCMS_Monitors.car` transport, which is distributed with the SPI for SAP, to monitor the Web AS (Java) environment.

This version of the SPI for SAP helps you monitor the SAP NetWeaver Web Application Server (J2EE) for SAP NetWeaver 6.40 and 7.00 only.

Before You Begin

Before you start monitoring the SAP NetWeaver Web Application Server (J2EE) environment, follow these steps:

1 **Deploy instrumentation.**

Deploy the *SPI for JMX Application Server* instrumentation group (along with the *SPI for SAP* instrumentation group) on all the nodes where you want to monitor the SAP NetWeaver Web Application Server (J2EE) metrics.

Before deploying the instrumentation, make sure that the Generic JMX Component is installed on the HPOM management server.

2 **Verify the location of necessary JAR files.**

Make sure that the following JAR files are included in the specified locations on the SAP NetWeaver system:

These JAR file are placed in these locations by your SAP installation.

- `logging.jar` (in the <*SAP_home*>`\j2ee\admin\lib` directory)
- `exception.jar` (in the <*SAP_home*>`\j2ee\admin\lib` directory)
- `com_sap_pj_jmx.jar` (in the <*SAP_home*>`\j2ee\admin\lib` directory)
- `sapj2eeclient.jar` (in the <*SAP_home*>`\j2ee\j2eeclient` directory)
- `jmx.jar` (in the <*SAP_home*>`\j2ee\admin\logviewer_standalone\lib` directory)

3 **Provide access-related details.**

You must provide the SPI for SAP with the details to access SAP NetWeaver Web Application Servers. With the help of the `global_SiteConfig` policy (which uses the `SiteConfig` configuration file), you can provide the SPI for SAP with the access details of an SAP NetWeaver Web Application Server and enable the SPI for SAP to collect necessary metrics. To provide the SPI with all the access-related information, follow these steps:

The `SiteConfig` file does not store the password in an encrypted format.

a. In the HPOM console, open the policy dialog of the `global_SiteConfig` policy from **Policy groups > SPI for SAP > en > SAP NetWeaver Java Monitoring > Configure**.

b. Specify the value for every attribute of the SAP NetWeaver server that you want to monitor. See The SiteConfig File on page 267 for information on all the attributes.

c. Repeat step b for all the nodes that you want to monitor.

The `global_SiteConfig` policy enables you to add the access details of all the SAP NetWeaver nodes that you want to monitor into the same file (see The SiteConfig File on page 267).

d. Click **Save and Close**.

e. Deploy the `global_SiteConfig` policy on the node.

4 **Create necessary configurations on nodes.**

Run the Create SPI SAP NetWeaver Config tool to create necessary configurations on nodes. Run this tool on all the SAP NetWeaver Web Application Servers. This tool is available in the **SPI for SAP > SAP R/3 Admin** group in the HPOM console.

5 **Test the monitoring setup.**

The setup that you have prepared, by performing step 1 through step 3, can be tested with the help of the Check the SAP NetWeaver Connection tool. From the HPOM console, run the Check the SAP NetWeaver Connection tool (**SPI for SAP > SAP R/3 Admin**) on all the nodes that you want to monitor.

6 **Deploy the collection definition.**

The `SPISAP-UpdateNWMetricConfig -1d` policy (included in the **SPI for SAP > en > SAP NetWeaver Java Monitoring > Configure** policy group) contains the mechanism to collect data from the SAP NetWeaver Web Application Servers. The policy provides the SPI with the following details:

— Types of information to be collected

— Types of information to be stored into the data store

— Types of information to be compared with preset thresholds

You must deploy the `SPISAP-UpdateNWMetricConfig -1d` policy on all the SAP NetWeaver Web Application Server nodes.

7 **Create data sources.**

Before the SPI for SAP starts logging the collected data into the data store on the node, necessary data tables must be created. The SPI for SAP and HP Operations environment use these data tables as the source of data to perform analysis, report building, and graph generation. When you install and configure the SAP Performance/subagent on nodes, these data sources (data tables) are automatically created into the data store. Install and

configure the SAP Performance/subagent on the SAP NetWeaver Web Application Server nodes as described in Installing the SAP/Performance Subagent on page 206 and Configuring the SAP/Performance Subagent on page 209.

The SiteConfig File

The `SiteConfig.cfg` file contains the access-related details of an SAP NetWeaver Web Application Server. You can modify the contents of this file from the `global_SiteConfig` policy. You must specify values of the following attributes in this file:

- `NODE`: The fully-qualified domain name of the SAP NetWeaver server that you want to monitor.
- `NUM_SERVERS`: The number of Web Application Server instances that you want to monitor on the node.

  > You can monitor only one instance of Web Application Server for every SAP NetWeaver node. Always set this property to **`1`**.

- `SERVER1_NAME`: The fully-qualified domain name of the SAP NetWeaver Web Application Server.
- `SERVER1_LOGIN`: The user name to log on to the server.
- `SERVER1_PASSWORD`: The password for the above-mentioned user.
- `SERVER1_PORT`: The port number for the Web Application Server.
- `SERVER1_VERSION`: The version of SAP NetWeaver on the node.
- `SERVER1_HOME`: The SAP home directory on the node.
- `SERVER1_JAVA_HOME`: The `JAVA_HOME` location on the node.

  > Always use the forward slash character (**`/`**) while specifying location-related details in the `SiteConfig` file.

After you specify the values for the aforementioned attributes for all the SAP NetWeaver nodes that you want to monitor, you must place the `SiteConfig` file on the node by deploying the `global_SiteConfig` policy on the node.

Example SiteConfig File

```
NODE = sapspiw1.example.com

{

NUM_SERVERS=1

SERVER1_NAME=sapspiw2

SERVER1_LOGIN=j2ee_admin

SERVER1_PASSWORD=password

SERVER1_PORT=50104

SERVER1_VERSION=7.0

SERVER1_HOME=/usr/sap/GBR/DVEBMGS00

SERVER1_JAVA_HOME=/opt/java1.4

}

NODE = sapspiw2.example.com
```

```
{
NUM_SERVERS=1
SERVER1_NAME=sapspiw2
SERVER1_LOGIN=j2ee_admin
SERVER1_PASSWORD=password
SERVER1_PORT=50104
SERVER1_VERSION=7.0
SERVER1_HOME=/usr/sap/GBR/DVEBMGS00
SERVER1_JAVA_HOME=/opt/java1.4
}
```

Monitoring the J2EE Engine

After performing all the prerequisite tasks on the SAP NetWeaver Web AS node, you can start deploying the necessary policies to initiate monitoring. The SPI for SAP introduces three new policies to invoke the collector and analyzer programs on the SAP NetWeaver Web Application Server nodes.

Deploy the Scheduled Task Policies

Scheduled task policies help the collectors run on the node at a regular interval to collect metric data that can be stored or compared by the SPI for SAP against preset thresholds to generate alarms. These policies are:

- **SPISAP-70-High-10m:** Runs every 10 minutes.
- **SPISAP-70-High-30m:** Runs every 30 minutes.
- **SPISAP-70-High-1h:** Runs every hour.
- **SPISAP-70-perf-30m:** Runs every 30 minutes.
- **SPISAP-NWSTATUS-02m:** Runs every 2 minutes. This policy sends an alert to the message browser if the SAP NetWeaver Web Application Server is found to be down.

These policies are grouped under the **SPI for SAP > en >SAP NetWeaver Java Monitoring > Monitors** group.

Deploy the Measurement Threshold Policies

The measurement threshold policies help the SPI generate alarms in the event of threshold violation. The collectors and analyzers collect a variety of metrics on the node that indicate the availability, health, and performance of the J2EE engine of the Web AS. You must deploy the policies under the following groups to receive alerts and messages on your HPOM console.

- **J2EE Engine - Kernel:** Includes the policies to monitor the Kernel of the J2EE engine.
- **J2EE Engine - Performance:** Includes the policies to monitor the performance of the J2EE engine.

- **J2EE Engine - Services:** Includes the policies to monitor the various services on the SAP NetWeaver Web Application Server.

For information on these policies, see Reference Information on SAP NetWeaver Java Monitoring Policies.

Reference Information on SAP NetWeaver Java Monitoring Policies

This section includes the reference information on all the policies required to monitor the SAP NetWeaver Web Application Server's J2EE engine. The SPI for SAP primarily collects metric data from the **managers** and **services** that run on the J2EE engine.

Policies: the J2EE Engine - Kernel Group

The policies under the J2EE Engine - Kernel group collect data from the managers available on the J2EE engine. The SPI for SAP monitors metrics indicating the health and performance of the J2EE engine kernel from the data collected from several monitored units on SAP nodes.

Policies to Monitor the Configuration Manager Data

The SPI for SAP collects and monitors values of monitored units of Configuration Manager from SAP nodes.

SPISAP_0001

Policy name	SPISAP_0001
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the *Cache hit rate* monitored unit of the Configuration Manager.
Default threshold	• 110: The SPI for SAP sends an alert with the severity Warning when the cache hit rate exceeds 110. • 120: The SPI for SAP sends an alert with the severity Major when the cache hit rate exceeds 120.

SPISAP_0002

Policy name	SPISAP_0002
Policy type	Measurement Threshold

Policy name	SPISAP_0002
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	Commit duration of the J2EE engine.
Default threshold	• 30: The SPI for SAP sends an alert with the severity Warning when the commit duration is above or equal to 30. • 120: The SPI for SAP sends an alert with the severity Major when the commit duration is above or equal to 120.

SPISAP_0012

Policy name	SPISAP_0012
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	ClassLoader count of the J2EE engine.
Default threshold	0: The SPI for SAP sends an alert with the severity Major when the ClassLoader count is equal to 0.

SPISAP_0013

Policy name	SPISAP_0013
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	Total connection count of the J2EE engine.
Default threshold	0: The SPI for SAP sends an alert with the severity Major when the total connection count is equal to 0.

Policies to Monitor the Cluster Manager Data

The SPI for SAP collects and monitors values of monitored units of Cluster Manager from SAP nodes.

SPISAP_0038

Policy name	SPISAP_0038
Policy type	Measurement Threshold

Policy name	SPISAP_0038
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the value of the message context pool size of cluster management.
Default threshold	0: The SPI for SAP sends an alert with the severity Major when the value falls below the threshold.

SPISAP_0039

Policy name	SPISAP_0039
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the average message context pool size of cluster management.
Default threshold	0: The SPI for SAP sends an alert with the severity Major when the value falls below the threshold.

SPISAP_0040

Policy name	SPISAP_0040
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for configuration manager.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0041

Policy name	SPISAP_0041
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for cache manager.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0042

Policy name	SPISAP_0042
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for service manager deploy distributor.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0043

Policy name	SPISAP_0043
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for service manager internal connection.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0044

Policy name	SPISAP_0044
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for P4.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0045

Policy name	SPISAP_0045
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for iiop.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0046

Policy name	SPISAP_0046
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for sld.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0047

Policy name	SPISAP_0047
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for shell.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0048

Policy name	SPISAP_0048
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for web services.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0049

Policy name	SPISAP_0049
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for log configurator.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0050

Policy name	SPISAP_0050
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for jmx notification.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0051

Policy name	SPISAP_0051
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for telnet.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0052

Policy name	SPISAP_0052
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for jmx.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0053

Policy name	SPISAP_0053
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for jms provider.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0054

Policy name	SPISAP_0054
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for http.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0055

Policy name	SPISAP_0055
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for deploy.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0056

Policy name	SPISAP_0056
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for naming.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0057

Policy name	SPISAP_0057
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for connector.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0058

Policy name	SPISAP_0058
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for BI MMR deployer.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0059

Policy name	SPISAP_0059
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for com.sap.security.core.ume.service.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0060

Policy name	SPISAP_0060
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for security.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0061

Policy name	SPISAP_0061
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for web dynpro.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0062

Policy name	SPISAP_0062
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for servlet jsp.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0063

Policy name	SPISAP_0063
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for rfcengine.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0064

Policy name	SPISAP_0064
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for apptracing.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0065

Policy name	SPISAP_0065
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte sent for prtbridge.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0066

Policy name	SPISAP_0066
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for configuration manager.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0067

Policy name	SPISAP_0067
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for cache manager.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0068

Policy name	SPISAP_0068
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for service manager deploy distributor.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0069

Policy name	SPISAP_0069
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for service manager (internal connection).
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0070

Policy name	SPISAP_0070
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for P4.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0071

Policy name	SPISAP_0071
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for iiop.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0072

Policy name	SPISAP_0072
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for sld.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0073

Policy name	SPISAP_0073
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for Shell.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0074

Policy name	SPISAP_0074
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for Web Services.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0075

Policy name	SPISAP_0075
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for Log Configurator.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0076

Policy name	SPISAP_0076
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for jmx_notification.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0077

Policy name	SPISAP_0077
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for jmx_notification.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0078

Policy name	SPISAP_0078
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for jmx.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0079

Policy name	SPISAP_0079
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for jms_provider.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0080

Policy name	SPISAP_0080
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for http.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0081

Policy name	SPISAP_0081
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for deploy.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0082

Policy name	SPISAP_0082
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for naming.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0083

Policy name	SPISAP_0083
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for connector.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0084

Policy name	SPISAP_0084
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for bi~mmr~deployer.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0085

Policy name	SPISAP_0085
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for com.sap.security.core.ume.service.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0086

Policy name	SPISAP_0086
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for security.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0087

Policy name	SPISAP_0087
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for web dynpro.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0088

Policy name	SPISAP_0088
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for servlet_jsp.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0089

Policy name	SPISAP_0089
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for rfcengine.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0090

Policy name	SPISAP_0090
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for apptracing.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0091

Policy name	SPISAP_0091
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the total message byte received for prtbridge.
Default threshold	**10000000:** The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_0092

Policy name	SPISAP_0092
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the maximum session queue size.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0093

Policy name	SPISAP_0093
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the P4 current session queue size.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0094

Policy name	SPISAP_0094
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the internal current session queue size.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0095

Policy name	SPISAP_0095
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the telnet current session queue size.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0096

Policy name	SPISAP_0096
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the http current session queue size.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0097

Policy name	SPISAP_0097
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the jms_provider current session queue size.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0098

Policy name	SPISAP_0098
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the web services current session queue size.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0099

Policy name	SPISAP_0099
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors the iiop current session queue size.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0100

Policy name	SPISAP_0100
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session bytes sent for the P4 processor.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0101

Policy name	SPISAP_0101
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session bytes sent for the internal processor.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0102

Policy name	SPISAP_0102
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session bytes sent for the telnet processor.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0103

Policy name	SPISAP_0103
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session bytes sent for the http processor.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0104

Policy name	SPISAP_0104
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session bytes sent for the jms_provider processor.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0105

Policy name	SPISAP_0105
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session bytes sent for the web services processor.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0106

Policy name	SPISAP_0106
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session bytes sent for the iiop processor.
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0107

Policy name	SPISAP_0107
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session byte received for the P4 processor(
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0108

Policy name	SPISAP_0108
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session byte received for the internal processor(
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0109

Policy name	SPISAP_0109
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session byte received for the telnet processor(
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0110

Policy name	SPISAP_0110
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session byte received for the http processor(
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0111

Policy name	SPISAP_0111
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session byte received for the jms_provider processor(
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0112

Policy name	SPISAP_0112
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session byte received for the web services processor(
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

SPISAP_0113

Policy name	SPISAP_0113
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Kernel**
Description	This policy monitors total session byte received for the iiop processor(
Default threshold	**0:** The SPI for SAP sends an alert with the severity Major when the value reaches the threshold.

Policies: the J2EE Engine - Services Group

The policies under the J2EE Engine - Services group collect data from the services available on the J2EE engine.

This group monitors states and conditions of the services that are necessary for the J2EE engine. Policies under this group monitor the following services and send alert messages to the message appropriate in the events of threshold violation:

- JMX Adapter Service
- HTTP Provider Service
- Connector Container Service: SAPSR3DB
- Connector Container Service: SAP/EP_PRT
- Connector Container Service: SAP/BC_MIGSERVICE
- Connector Container Service: SAP/CAF_EUF_GP
- Connector Container Service: SAP/BC_WDRR
- Connector Container Service: SAP/CAF_RT
- Connector Container Service: SAP/BW_MMR
- Connector Container Service: SAP/EP_DQE
- Connector Container Service: SAP/CAF/EUP_GP/MAIL_CF
- Connector Container Service: SAP/BC_UME
- Connector Container Service: SAP/BC_JMS
- Connector Container Service: SAP/BC_FO
- Connector Container Service: SAP/BC_XMLA
- Connector Container Service: SAP/BC_MON
- Connector Container Service: SAP/CAF_EUP_ER
- Connector Container Service: SAP/EP_PCD
- Connector Container Service: SAP/CAF_BW_RD
- Connector Container Service: SAP/BC_SLM
- Connector Container Service: SAP/LOCAL_MAINFRAME_POOL
- Connector Container Service: SAP/BC_SLD
- Connector Container Service: SAP/BC_JDO
- Connector Container Service: SAP/BC_UDDI
- Connector Container Service: utdb
- Connector Container Service: ADS
- Connector Container Service: SDK_JDBC
- Connector Container Service: SDK_CAF
- Connector Container Service: SDK_SAPQ
- Connector Container Service: SDK_XMLA
- Connector Container Service: SDK_ODBO

- EJB Container Service: Session stateful beans
- EJB Container Service: Session stateless beans
- EJB Container Service: Message driven beans.
- EJB Container Service: Entity beans
- Web Services Container Service
- Web Container Service

Policies to Monitor the JMX Adapter Service

These policies monitor the *JMX Adapter Service*.

SPISAP_2001

Policy name	SPISAP_2001
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en > SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the maximum entries of the JMX adapter service.
Default threshold	10000: The SPI for SAP sends an alert with the severity Warning when the maximum entries of the JMX adapter service exceeds 10000. 50000: The SPI for SAP sends an alert with the severity Major when the maximum entries of the JMX adapter service exceeds 50000.

SPISAP_2002

Policy name	SPISAP_2002
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en > SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the current entries of the JMX adapter service.
Default threshold	**10000**: The SPI for SAP sends an alert with the severity Warning when the current entries of the JMX adapter service exceeds 10000. **50000**: The SPI for SAP sends an alert with the severity Major when the current entries of the JMX adapter service exceeds 50000.

SPISAP_2003

Policy name	SPISAP_2003
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the replaced entries of the JMX adapter v.
Default threshold	**10000**: The SPI for SAP sends an alert with the severity Warning when the replaced entries of the JMX adapter service exceeds 10000. **50000**: The SPI for SAP sends an alert with the severity Major when the replaced entries of the JMX adapter service exceeds 50000.

SPISAP_2004

Policy name	SPISAP_2004
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en > SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the hit rate of the JMX adapter v.
Default threshold	**500**: The SPI for SAP sends an alert with the severity Warning when the hit rate of the JMX adapter service exceeds 500. **1000**: The SPI for SAP sends an alert with the severity Major when the hit rate of the JMX adapter service exceeds 1000.

SPISAP_2005

Policy name	SPISAP_2005
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en > SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the notification queue size of the JMX adapter service.
Default threshold	**10**: The SPI for SAP sends an alert with the severity Warning when the queue size of the JMX adapter service exceeds 10. **100**: The SPI for SAP sends an alert with the severity Major when the queue size of the JMX adapter service exceeds 100.

SPISAP_2006

Policy name	SPISAP_2006
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en > SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the number of active threads of the JMX adapter service.
Default threshold	**3**: The SPI for SAP sends an alert with the severity Major when the number of active threads of the JMX adapter service exceeds 3.

SPISAP_2007

Policy name	SPISAP_2007
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en > SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the log size on the SAP node.
Default threshold	**524288 (KB)**: The SPI for SAP sends an alert with the severity Major when the log size of the monitored node exceeds 524288 kb.

Policies to Monitor the HTTP Provider Service

These policies monitor the *HTTP Provider Service*.

SPISAP_2011

Policy name	SPISAP_2011
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en > SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Current open connections: Total count* monitored unit of the HTTP Provider Service.
Default threshold	**100**: The SPI for SAP sends an alert with the severity Major when the value of the *Current open connections: Total count* monitored unit exceeds 100.

SPISAP_2012

Policy name	SPISAP_2012
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Current open connections: Reading request* monitored unit of the HTTP Provider Service.
Default threshold	**100**: The SPI for SAP sends an alert with the severity Major when the value of the *Current open connections: Reading request* monitored unit exceeds 100.

SPISAP_20013

Policy name	SPISAP_2013
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Current open connections: Reading response* monitored unit of the HTTP Provider Service.
Default threshold	**100**: The SPI for SAP sends an alert with the severity Major when the value of the *Current open connections: Reading response* monitored unit exceeds 100.

SPISAP_2014

Policy name	SPISAP_2014
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Current open connections: Skipping requests* monitored unit of the HTTP Provider Service.
Default threshold	**100**: The SPI for SAP sends an alert with the severity Major when the value of the *Current open connections: Skipping requests* monitored unit exceeds 100.

SPISAP_2015

Policy name	SPISAP_2015
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Current open connections: Keep-Alive waiting* monitored unit of the HTTP Provider Service.
Default threshold	**100**: The SPI for SAP sends an alert with the severity Major when the value of the *Current open connections: Keep-Alive waiting* monitored unit exceeds 100.

SPISAP_2016

Policy name	SPISAP_2016
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Total requests: Avg requests per connection rate* monitored unit of the HTTP Provider Service.
Default threshold	**100000**: The SPI for SAP sends an alert with the severity Major when the value of the *Total requests: Avg requests per connection rate* monitored unit exceeds 100000.

SPISAP_2018

Policy name	SPISAP_2018
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Total requests: Avg request-response time* monitored unit of the HTTP Provider Service.
Default threshold	• **120**: The SPI for SAP sends an alert with the severity Major when the value of the *Total requests: Avg request-response time* monitored unit exceeds 120. • **60**: The SPI for SAP sends an alert with the severity Warning when the value of the *Total requests: Avg request-response time* monitored unit exceeds 60.

Policies to Monitor the SAPSR3DB Connector Container Service

These policies monitor the *SAPSR3DB Connector Container Service*.

SPISAP_2019

Policy name	SPISAP_2019
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAPSR3DB Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2020

Policy name	SPISAP_2020
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAPSR3DB Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2021

Policy name	SPISAP_2021
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAPSR3DB Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2022

Policy name	SPISAP_2022
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAPSR3DB Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/EP_PRT Connector Container Service

These policies monitor the *SAP/EP_PRT Connector Container Service*.

SPISAP_2023

Policy name	SPISAP_2023
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/EP_PRT Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2024

Policy name	SPISAP_2024
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/EP_PRT Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2025

Policy name	SPISAP_2025
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/EP_PRT Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2026

Policy name	SPISAP_2026
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/EP_PRT Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BC_MIGSERVICE Connector Container Service

These policies monitor the *SAP/BC_MIGSERVICE Connector Container Service*.

SPISAP_2027

Policy name	SPISAP_2027
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BC_MIGSERVICE Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2028

Policy name	SPISAP_2028
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BC_MIGSERVICE Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2029

Policy name	SPISAP_2029
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BC_MIGSERVICE Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2030

Policy name	SPISAP_2030
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BC_MIGSERVICE Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/CAF_EUP_GP Connector Container Service

These policies monitor the *SAP/CAF_EUP_GP Connector Container Service*.

SPISAP_2031

Policy name	SPISAP_2031
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/CAF_EUP_GP Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2032

Policy name	SPISAP_2032
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/CAF_EUP_GP Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2033

Policy name	SPISAP_2033
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/CAF_EUP_GP Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2034

Policy name	SPISAP_2034
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/CAF_EUP_GP Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BC_WDRR Connector Container Service

These policies monitor the *SAP/BC_WDRR Connector Container Service*.

SPISAP_2035

Policy name	SPISAP_2035
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BC_WDRR Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2036

Policy name	SPISAP_2036
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BC_WDRR Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2037

Policy name	SPISAP_2037
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BC_WDRR Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2038

Policy name	SPISAP_2038
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BC_WDRR Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/CAF_RT Connector Container Service

These policies monitor the *SAP/CAF_RT Connector Container Service*.

SPISAP_2039

Policy name	SPISAP_2039
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/CAF_RT.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2040

Policy name	SPISAP_2040
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/CAF_RT.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2041

Policy name	SPISAP_2041
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/CAF_RT.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2042

Policy name	SPISAP_2042
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/CAF_RT Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BW_MMR Connector Container Service

These policies monitor the *SAP/BW_MMR Connector Container Service*.

SPISAP_2043

Policy name	SPISAP_2043
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BW_MMR Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2044

Policy name	SPISAP_2044
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BW_MMR Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2045

Policy name	SPISAP_2045
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BW_MMR Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2046

Policy name	SPISAP_2046
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BW_MMR Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/EP_DQE Connector Container Service

These policies monitor the *SAP/EP_DQE Connector Container Service*.

SPISAP_2047

Policy name	SPISAP_2047
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/EP_DQE Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2048

Policy name	SPISAP_2048
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/EP_DQE Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2049

Policy name	SPISAP_2049
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/EP_DQE Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2050

Policy name	SPISAP_2050
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/EP_DQE Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/CAF/EUP_GP/MAIL_CF Connector Container Service

These policies monitor the *SAP/CAF/EUP_GP/MAIL_CF Connector Container Service*.

SPISAP_2051

Policy name	SPISAP_2051
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/CAF/EUP_GP/MAIL_CF Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2052

Policy name	SPISAP_2052
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/CAF/EUP_GP/MAIL_CF Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2053

Policy name	SPISAP_2053
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/CAF/EUP_GP/MAIL_CF Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2054

Policy name	SPISAP_2054
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/CAF/EUP_GP/MAIL_CF Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BC_UME Connector Container Service

These policies monitor the *SAP/BC_UME Connector Container Service*.

SPISAP_2055

Policy name	SPISAP_2055
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BC_UME Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2056

Policy name	SPISAP_2056
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BC_UME Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2057

Policy name	SPISAP_2057
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BC_UME Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2058

Policy name	SPISAP_2058
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BC_UME Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BC_JMS Connector Container Service

These policies monitor the *SAP/BC_JMS Connector Container Service*.

SPISAP_2059

Policy name	SPISAP_2059
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BC_JMS Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2060

Policy name	SPISAP_2060
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BC_JMS Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2061

Policy name	SPISAP_2061
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BC_JMS Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2062

Policy name	SPISAP_2062
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BC_JMS Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BC_FO Connector Container Service

These policies monitor the *SAP/BC_FO Connector Container Service*.

SPISAP_2063

Policy name	SPISAP_2063
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BC_FO Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2064

Policy name	SPISAP_2064
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BC_FO Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2065

Policy name	SPISAP_2065
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BC_FO Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2066

Policy name	SPISAP_2066
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BC_FO Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BC_XMLA Container Service

These policies monitor the *SAP/BC_XMLA Connector Container Service*.

SPISAP_2067

Policy name	SPISAP_2067
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BC_XMLA Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2068

Policy name	SPISAP_2068
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BC_XMLA Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2069

Policy name	SPISAP_2069
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BC_XMLA Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2070

Policy name	SPISAP_2070
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BC_XMLA Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BC_MON Connector Container Service

These policies monitor the *SAP/BC_MON Connector Container Service*.

SPISAP_2071

Policy name	SPISAP_2071
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BC_MON Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2072

Policy name	SPISAP_2072
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BC_MON Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2073

Policy name	SPISAP_2073
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BC_MON Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2074

Policy name	SPISAP_2074
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BC_MON Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/CAF_EUP_ER Connector Container Service

These policies monitor the *SAP/CAF_EUP_ER Connector Container Service*.

SPISAP_2075

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/CAF_EUP_ER Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2076

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/CAF_EUP_ER Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2077

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/CAF_EUP_ER Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2078

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/CAF_EUP_ER Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/EP_PCD Connector Container Service

These policies monitor the *SAP/EP_PCD Connector Container Service*.

SPISAP_2079

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/EP_PCD Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2080

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/EP_PCD Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2081

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/EP_PCD Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2082

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/EP_PCD Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BC_ADM Connector Container Service

These policies monitor the *SAP/BC_ADM Connector Container Service*.

SPISAP_2083

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BC_ADM Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2084

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BC_ADM Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2085

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BC_ADM Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2086

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BC_ADM Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/CAF_BW_RT Connector Container Service

These policies monitor the *SAP/CAF_BW_RT Connector Container Service*.

SPISAP_2087

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/CAF_BW_RT Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2088

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/CAF_BW_RT Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2089

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/CAF_BW_RT Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2090

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/CAF_BW_RT Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BC_SLM Connector Container Service

These policies monitor the *SAP/BC_SLM Connector Container Service*.

SPISAP_2091

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BC_SLM Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2092

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BC_SLM Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2093

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BC_SLM Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2094

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BC_SLM Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/LOCAL_MAINFRAME_POOL Connector Container Service

These policies monitor the *SAP/LOCAL_MAINFRAME_POOL Connector Container Service*.

SPISAP_2095

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/LOCAL_MAINFRAME_POOL Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2096

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/ LOCAL_MAINFRAME_POOL Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2097

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/ LOCAL_MAINFRAME_POOL Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2098

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/LOCAL_MAINFRAME_POOL Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BC_SLD Connector Container Service

These policies monitor the *SAP/BC_SLD Connector Container Service*.

SPISAP_2099

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BC_SLD Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2100

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BC_SLD Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2101

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BC_SLD Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2102

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BC_SLD Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BC_JDO Connector Container Service

These policies monitor the *SAP/BC_JDO Connector Container Service*.

SPISAP_2103

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BC_JDO Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2104

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BC_JDO Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2105

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BC_JDO Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2106

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BC_JDO Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SAP/BC_UDDI Connector Container Service

These policies monitor the *SAP/BC_UDDI Connector Container Service*.

SPISAP_2107

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SAP/BC_UDDI Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2108

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SAP/BC_UDDI Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2109

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SAP/BC_UDDI Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2110

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SAP/BC_UDDI Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the utdb Connector Container Service

These policies monitor the *SAP/utdb Connector Container Service*.

SPISAP_2111

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the utdb Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2112

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the utdb Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2113

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the utdb Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2114

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the utdb Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the ADS Connector Container Service

These policies monitor the *ADS Connector Container Service*.

SPISAP_2115

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the ADS Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2116

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the ADS Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2117

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the ADS Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2118

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the ADS Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SDK_JDBC Connector Container Service

These policies monitor the *SDK_JDBC Connector Container Service*.

SPISAP_2119

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SDK_JDBC Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2120

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SDK_JDBC Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2121

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SDK_JDBC Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2122

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SDK_JDBC Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SDK_CAF Connector Container Service

These policies monitor the *SDK_CAF Connector Container Service*.

SPISAP_2123

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SDK_CAF Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2124

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SDK_CAF Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2125

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SDK_CAF Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2126

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SDK_CAF Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SDK_SAPQ Connector Container Service

These policies monitor the *SDK_SAPQ Connector Container Service*.

SPISAP_2127

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SDK_SAPQ Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2128

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SDK_SAPQ Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2129

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SDK_SAPQ Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2130

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SDK_SAPQ Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SDK_XMLA Connector Container Service

These policies monitor the *SDK_XMLA Connector Container Service*.

SPISAP_2131

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SDK_XMLA Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2132

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SDK_XMLA Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2133

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SDK_XMLA Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2134

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SDK_XMLA Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the SDK_ODBO Connector Container Service

These policies monitor the *SDK_ODBO Connector Container Service*.

SPISAP_2135

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Maximum connections number* monitored unit of the SDK_ODBO Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Maximum connections number* monitored unit exceeds 10000000.

SPISAP_2136

Policy type	Measurement Threshold

Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Free managed connections number* monitored unit of the SDK_ODBO Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Free managed connections number* monitored unit exceeds 10000000.

SPISAP_2137

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Used managed connections number* monitored unit of the SDK_ODBO Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Used managed connections number* monitored unit exceeds 10000000.

SPISAP_2138

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Waiting for connections number* monitored unit of the SDK_ODBO Connector Container Service.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value of the *Waiting for connections number* monitored unit exceeds 10000000.

Policies to Monitor the EJB Container Services

These policies monitor the EJB container services.

SPISAP_2139

Policy name	SPISAP_2139
Policy type	Measurement Threshold

Policy name	SPISAP_2139
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the ActiveSessionTimeout monitoring unit of the Stateful Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2140

Policy name	SPISAP_2140
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the PassiveSessionTimeout monitoring unit of the Stateful Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2141

Policy name	SPISAP_2141
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the ActiveSessionCount monitoring unit of the Stateful Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2142

Policy name	SPISAP_2142
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the PassiveSessionCount monitoring unit of the Stateful Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2143

Policy name	SPISAP_2143
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the CompletedSessions monitoring unit of the Stateful Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2144

Policy name	SPISAP_2144
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the CreationsNumber monitoring unit of the Stateful Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2145

Policy name	SPISAP_2145
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the RemovalsNumber monitoring unit of the Stateful Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2146

Policy name	SPISAP_2146
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the PassivationsNumber monitoring unit of the Stateful Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2147

Policy name	SPISAP_2147
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the ActivationsNumber monitoring unit of the Stateful Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2148

Policy name	SPISAP_2148
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the CreationsNumber monitoring unit of the Stateful Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2149

Policy name	SPISAP_2149
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the RemovalsNumber monitoring unit of the Stateful Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2150

Policy name	SPISAP_2150
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the CurrentPoolSize monitoring unit of the Stateless Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2151

Policy name	SPISAP_2151
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the MaxPoolSize monitoring unit of the Stateless Session beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2152

Policy name	SPISAP_2152
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the InitialPoolSize monitoring unit of the Stateless Session beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2153

Policy name	SPISAP_2153
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the PoolIncrementSize monitoring unit of the Stateless Session beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2154

Policy name	SPISAP_2154
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the PoolCurrentlyUsedObject monitoring unit of the Stateless Session beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2155

Policy name	SPISAP_2155
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the CreationsNumber monitoring unit of the Message-Driven beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2156

Policy name	SPISAP_2156
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the RemovalsNumber monitoring unit of the Message-Driven beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2157

Policy name	SPISAP_2157
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the CurrentPoolSize monitoring unit of the Message-Driven beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2158

Policy name	SPISAP_2158
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the MaxPoolSize monitoring unit of the Message-Driven beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2159

Policy name	SPISAP_2159
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the InitialPoolSize monitoring unit of the Message-Driven beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2160

Policy name	SPISAP_2160
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the PoolIncrementSize monitoring unit of the Message-Driven beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2161

Policy name	SPISAP_2161
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the PoolCurrentlyUsedObject monitoring unit of the Message-Driven beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2162

Policy name	SPISAP_2162
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the CreationsNumber monitoring unit of the Entity beans.
Default threshold	**10000000**: The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2163

Policy name	SPISAP_2163
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the RemovalsNumber monitoring unit of the Entity beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2164

Policy name	SPISAP_2164
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the CurrentPoolSize monitoring unit of the Entity beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2165

Policy name	SPISAP_2165
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the MaxPoolSize monitoring unit of the Entity beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2166

Policy name	SPISAP_2166
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the InitialPoolSize monitoring unit of the Entity beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2167

Policy name	SPISAP_2167
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the PoolIncrementSize monitoring unit of the Entity beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2168

Policy name	SPISAP_2168
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the PoolCurrentlyUsedObject monitoring unit of the Entity beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2169

Policy name	SPISAP_2169
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the PassivationsNumber monitoring unit of the Entity beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

SPISAP_2170

Policy name	SPISAP_2170
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the ActivationsNumber monitoring unit of the Entity beans.
Default threshold	**10000000** : The SPI for SAP sends an alert with the severity Major when the value exceeds the threshold.

Policies to Monitor the Web Container Service

These policies monitor the *Web Container Service*.

SPISAP_2187

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Current Http sessions* monitored unit of the Web Container Service.
Default threshold	**500**: The SPI for SAP sends an alert with the severity Major when the value of the *Current Http sessions* monitored unit exceeds 500.

SPISAP_2188

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Current security sessions* monitored unit of the Web Container Service.
Default threshold	**500**: The SPI for SAP sends an alert with the severity Major when the value of the *Current security sessions* monitored unit exceeds 500.

SPISAP_2189

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Number of timed out http sessions* monitored unit of the Web Container Service.
Default threshold	**100000**: The SPI for SAP sends an alert with the severity Major when the value of the *Number of timed out http sessions* monitored unit exceeds 100000.

SPISAP_2190

Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Services**
Description	This policy monitors the *Number of timed out security sessions* monitored unit of the Web Container Service.
Default threshold	**100000**: The SPI for SAP sends an alert with the severity Major when the value of the *Number of timed out security sessions* monitored unit exceeds 100000.

Policies: the J2EE Engine - Performance Group

The J2EE Engine - Performance group of policies collects the performance monitor data of the J2EE engine. This group collects the data from the *Request performance* monitor group.

SPISAP_4001

Policy name	SPISAP_4001
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Performance**
Description	The SPISAP_4001 policy collects data from the *Number of requests* monitored unit.
Default threshold	1000000: The SPI for SAP sends an alert with the severity Major when the total number of JARM requests equals or exceeds 1000000.

SPISAP_4002

Policy name	SPISAP_4002
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Performance**
Description	The SPISAP_4002 policy collects data from the *Requests per second* monitored unit.
Default threshold	1000000: The SPI for SAP sends an alert with the severity Major when the number of JARM requests per second equals or exceeds 1000000.

SPISAP_4003

Policy name	SPISAP_4003
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Performance**
Description	The SPISAP_4003 policy collects data from the *Component calls* monitored unit.
Default threshold	1000000: The SPI for SAP sends an alert with the severity Major when the total number of component calls made by all JARM requests equals or exceeds 1000000.

SPISAP_4004

Policy name	SPISAP_4004
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Performance**
Description	The SPISAP_4004 policy collects data from the *Average response time* monitored unit.
Default threshold	1000000: The SPI for SAP sends an alert with the severity Major when the total number of component calls made by all JARM requests equals or exceeds 1000000.

SPISAP_4005

Policy name	SPISAP_4006
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Performance**
Description	The SPISAP_4006 policy collects data from the *Average CPU Time* monitored unit.
Default threshold	1000000: The SPI for SAP sends an alert with the severity Major when the average CPU time equals or exceeds 1000000.

SPISAP_4006

Policy name	SPISAP_4006
Policy type	Measurement Threshold
Policy group	**SPI for SAP > en >SAP NetWeaver Java Monitoring > J2EE Engine - Performance**
Description	The SPISAP_4006 policy collects data from the *Average outbound data* monitored unit.
Default threshold	1000000: The SPI for SAP sends an alert with the severity Major when the average outbound data equals or exceeds 1000000.

9 Service Views

This section describes how to install, set up, and use the service views provided with the SPI for SAP.

In this Section

The information in this section introduces you to the concept of Service Views and explains how they are used by both the SPI for SAP and HPOM for Windows to provide you with information that is specifically designed to help you manage your SAP NetWeaver landscape in a more efficient and more convenient way. You can find detailed information about the following topics:

What are Service Views?

Service views provide you with a way of viewing the objects that make up your environment so that you can better determine the effect of current problems or predict potential problems.

Use the capabilities of HPOM for Windows to perform the following tasks:

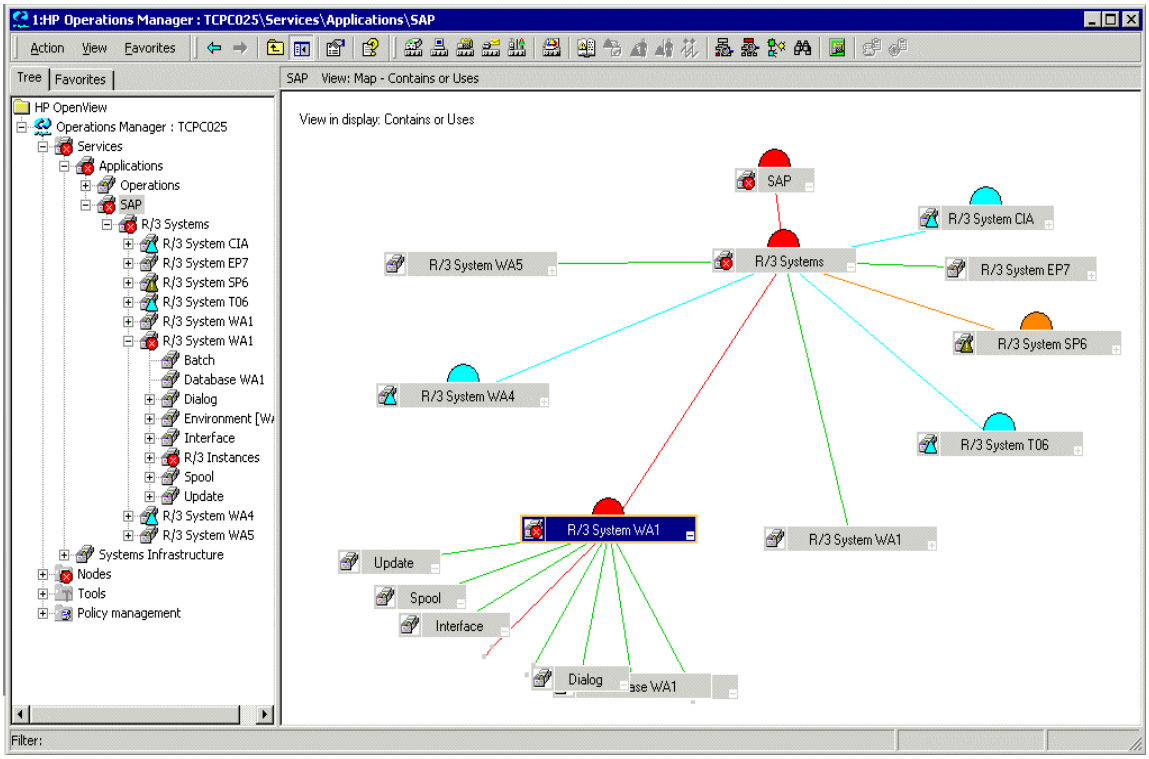
- Map messages to the services that they directly affect
- Generate a service model of your environment, which includes all relationships and dependencies between component objects
- Identify and select actions available for each object
- Define propagation rules, which can identify potential or present problems on objects and on related services

The scoping pane of the main window shows discovered services in addition to the usual HPOM for Windows managed nodes and applications. Click a service to expand the display the navigation tree for the selected service in the scoping pane. In the tree, you can select any service or subservice and display a service graph.

In both the navigation tree and the service graph, the component services are color-coded according to status. This color-coding of the tree elements matches the color-coding of messages in the console, which is determined by message severity level.

For instance, a service displayed in red indicates that a condition exists that has a critical effect on that service or on a related service. The action Get Root Cause traces the origin of a condition that has affected the status of a selected service.

The Service Map



Service Views in the SPI for SAP

The SPI for SAP provides a Service Auto-Discovery policy, which you can deploy on each managed node to analyze the SAP environment and generate a service view. The service view represents all existing ownership and dependency relationships between objects on the nodes, message-propagation rules, and any actions that are available for objects.

The service view reflects your individual setup. Each service view is a unique representation of the environment from which it is taken. In general, the SAP service view consists of several levels.

The first level is an accumulation object including all SAP systems. When you expand a first-level object, you see an object for each SAP NetWeaver system in your environment. The SAP Systems object changes status in response to a change of status in any of the objects that make up the instances that it contains.

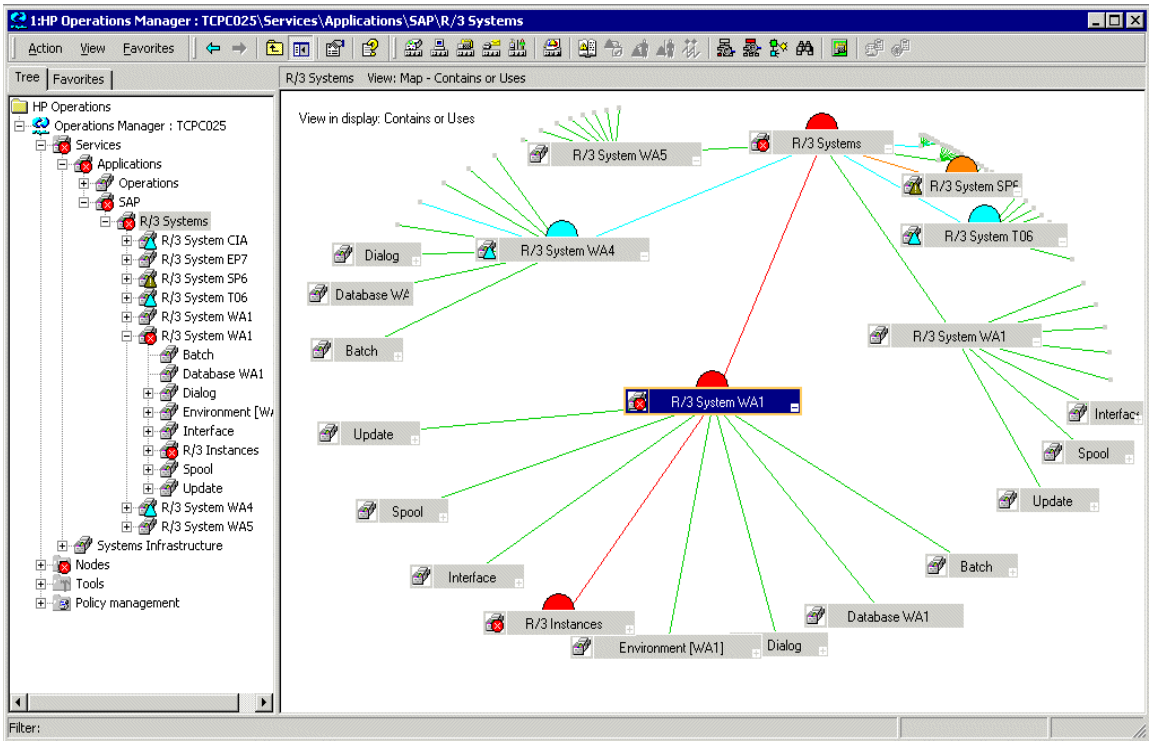
The second level includes logical objects within each SAP system. Notice that none of the objects shown at this level have any messages mapped directly to them. They are logical objects, used to give a general overview of the status of the services provided by the SAP NetWeaver system. Expand an SAP NetWeaver system object to display the following logical objects:

- SAP NetWeaver Instances

- Database (<*SID*>)
- Environment (<*SID*>)
- Interface
- Batch
- Dialog
- Spool
- Update

Figure 30 shows an example SAP service view expanded to the logical object level.

Figure 30 Service Map of SAP Systems

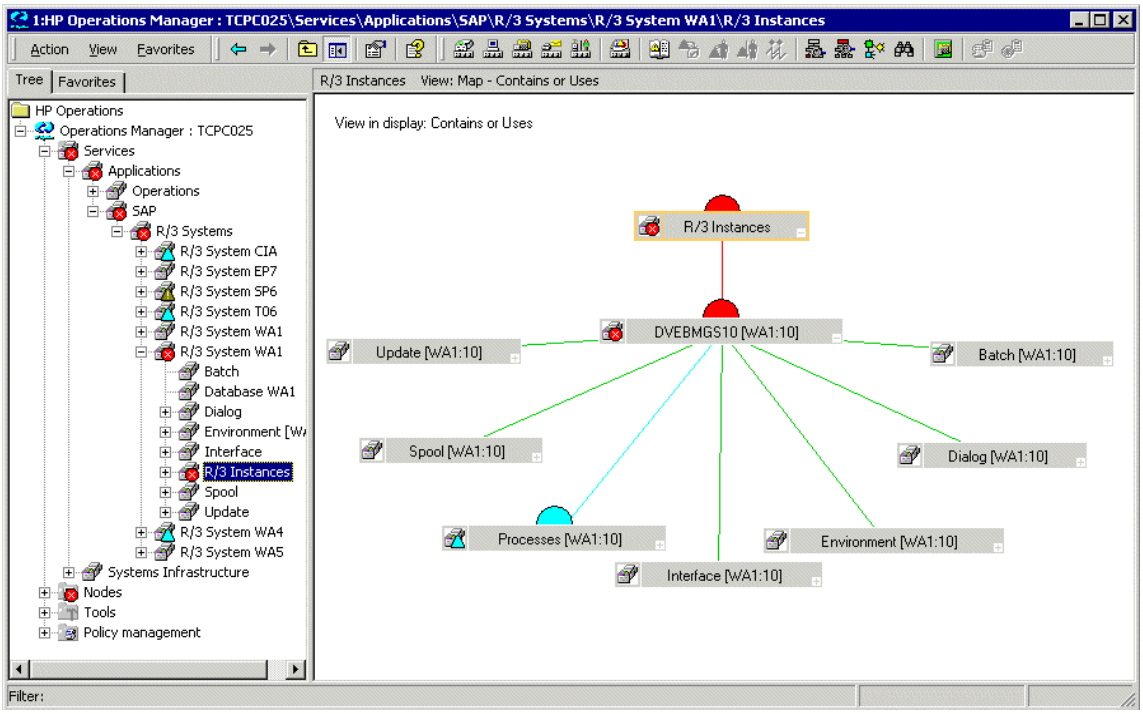


When you expand the SAP NetWeaver Instance object, each SAP NetWeaver instance appears as an object in the tree. When you expand the environment object, you will see displayed three further objects:

- Operating System
- Network
- Memory Management

These objects have messages mapped to them which would then be propagated to the environment object. The other objects have **use** relationships with objects contained within the processes object; an event that affects a related process would cause a change in status in these objects.

Figure 31 Service Map of an SAP Instance



The processes object can be expanded to show the following objects:

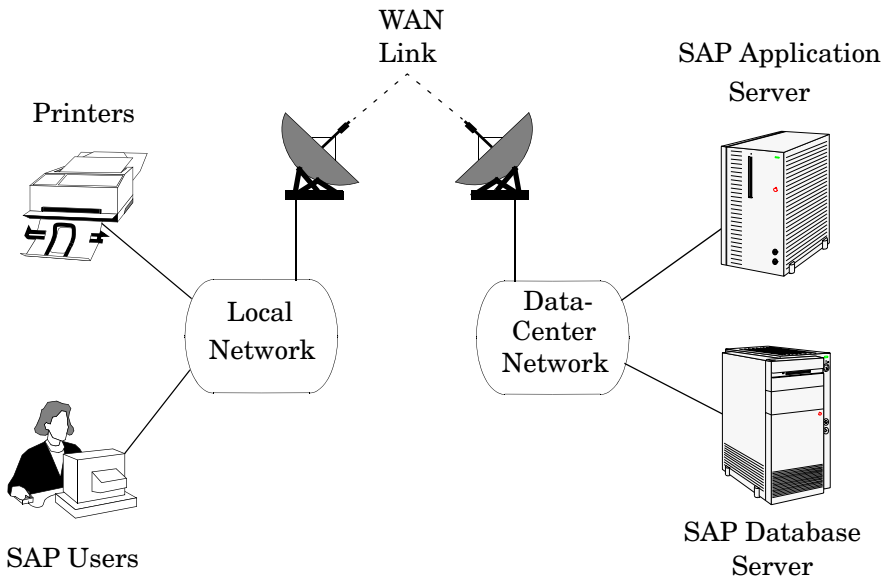
- Gateway
- Message
- Dialog work process
- Batch work process
- Spool work process
- Update work process

Line of Business Views

The SAP NetWeaver service view and the other service views available with HPOM for Windows provide graphical representations of the individual areas you are monitoring, for example SAP NetWeaver, a WAN or a LAN, or printer services. Business processes are not typically confined to any one of these areas and each business process depends on the services of several areas and is specific to the customer's defined processes.

For example, for an operator to enter orders and print acknowledgments, the printer, the network, and SAP NetWeaver Dialog Spool Service must all be available. To monitor order entry and printing at a particular location, you could set up a view that includes the WAN, the LAN at that location, the printer being used for the order acknowledgments, and the SAP NetWeaver dispatch, dialog, and spooling processes for the specific SAP NetWeaver instance.

Figure 32 Service Areas Affecting Order Entry



To create a line-of-business service view, you must first define the structure you want to see by generating a custom service view, in which you must define one or more logical objects (for example, Order Entry) to which messages will be propagated by the objects you include in the view.

Using the Service Editor (which you can start by right-clicking a service object and browsing to the option; **`Configure > Services`** in the menu that pops up) obtain the service names of the objects you want to include and add use references and dependencies to them from your custom service view.

Be aware that the services should only be built on top of logical (not physical) service objects. For example, use the SAP Spool-Service object in a reference but not the underlying physical objects such as Spool Work Process. This ensures that your customization and Business Service Views remain working, even if new releases of SAP or the SPI for SAP change the dependencies between physical components, for example as a result of architectural changes.

Configuring Service Views for SAP

To use the service-views feature of the SPI for SAP, you need to find out which services are running on the SAP servers you are monitoring and upload the discovered information to the HPOM for Windows database, as follows:

1. Ensure that the `r3itosap.cfg` file is available on all the managed nodes for which you want to generate a service view: typically, the managed nodes are the SAP servers, which you want to manage with the SPI for SAP. The service-discovery policy requires the information in the `r3itosap.cfg` file to complete its task successfully.
2. In the HP Operations Manager for Windows console, browse to the following folder:

   Policy management > Policy groups > SPI for SAP
3. Select and right-click the following policy:

   `r3sdisc` (Service auto-discovery)
4. Browse to the following option in the menu, which pops up:

   All Tasks > Deploy on...

5 In the Deploy Polices on... window which appears, select the managed nodes (SAP servers) where you want to run the automatic discovery of SAP services.

Click **OK**.

➤ You can monitor the deployment in real time in the Deployment Jobs pane at the bottom of the HPOM for Windows console.

6 The service discovery starts as soon as the policy is successfully deployed to the managed node and, in addition, according to the schedule defined in the policy. The default schedule is once a day.

You can verify that the service discovery has completed successfully, by browsing to the Services folder in the HPOM for Windows console and checking for the presence of the SAP servers (where you ran the service discovery) and the associated services.

Troubleshooting Service Discovery

In normal circumstances, the SPI for SAP discovers SAP services automatically and without any problem. However, if for any reason the information the SPI for SAP is looking for is not present in the default locations, then the service-discovery process fails.

For example, the SPI for SAP needs to know the names of the hosts on which SAP instances are running and, in addition, the location of the SAP profile directory, which contains the SAP **default**, **instance**, and **startup** profiles. The SAP default and instance profiles are of particular interest as they contain SAP System- and instance-specific information, which the SPI for SAP uses to determine the SAP System IDs (SID) and SAP instance names as well as the SAP instance numbers, whose services it attempts to discover.

In the event that the service discovery fails, you can use the environment variables in Table 87 on the managed node to help the SPI for SAP find the information it needs to discover SAP services successfully. The SPI for SAP Service discovery tool looks for SAP profiles in the following locations on the SAP application servers:

- **UNIX operating systems**

  `/sapmnt/<SID>/profile/`

- **Microsoft Windows operating systems**

  `\\<central_instance_host>\sapmnt\<SID>\SYS\profile\`

On SAP application servers running Microsoft Windows operating systems, the path to the SAP profile includes the name of the host on which the SAP central instance is running, for example: <*central_instance_host*>. Note that you can use the long or short hostname, the IP address of the hostname, or the UNC notation.

Table 87 Service-discovery Environment Variables

Environment Variable	Description
SAPOPC_SAPPROFILEDIR	the path to the location of the SAP profiles. Like the PATH environment variable, it may contain a list of directories where the profiles could reside
SAPOPC_HOSTNAMES	Use on managed nodes in a high-availability cluster to define the list of physical and virtual hostnames (each separated by a space) to process with service- discovery

10 Service Reports

This section describes how to install, set up, and use the service reports provided with the SPI for SAP.

In this Section

The information in this section introduces you to the concept of Service Reports and explains how you can use them in conjunction with both the SPI for SAP and HPOM for Windows to provide you with information that is specifically designed to help you manage your SAP NetWeaver landscape in a more efficient and more convenient way. You can find detailed information about the following topics:

What Are Service Reports?

Service reports are web-based reports that are produced by HP Reporter (Reporter) using default templates and viewed using a web browser. Reporter allows you to request both scheduled and on-demand versions of reports.

SPI for SAP service reports correlate the data extracted from either the HP Software Embedded Performance Component or the HP Performance Agent. You can use the correlated data to generate reports which display short-, medium-, or long-term views of your IT environment and supplement the detailed, real-time graphs available with Performance Manager. The combination of reports and graphs is a powerful tool for trend analysis. For example, you can perform the following tasks:

- Identify potential bottlenecks in your IT system, so that you can take action before problems become acute.
- Use the information presented in the reports to help you to make accurate predictions for future upgrades.
- Collect accurate information to use in measuring service levels.

Upgrading the SPI for SAP Reports

This section describes what you have to do if you upgrade the SPI for SAP software and the SAP/Performance subagent and want to continue using the service-reporter functionality. Note that upgrading the SPI for SAP Service Reports is not the same as upgrading the HP Reporter software. For more information about supported software versions, refer to *HP Operations Smart Plug-in for SAP Configuration Guide*.

For more information about upgrading the SAP/Performance subagent, which gathers performance data for the Service Reports, see Upgrading the SAP/Performance Subagent on page 202. For more information about upgrading the SPI for SAP itself, see "Upgrading the SPI for SAP" in the *HP Operations Smart Plug-in for SAP Configuration Guide*.

The SPI for SAP comes with a Reporter-integration package containing improved and enhanced reports, some of which make use of new metrics lists. To upgrade the SPI for SAP reporter-integration, you have to remove the old Reporter-integration package and install the new one in its place, as follows:

1. Remove the old SPI for SAP reporter-integration package using the standard Windows method:

   Start: Settings > Control Panel > Add/Remove Software

2. Install the new SPI for SAP reporter integration as described in Installing the SPI for SAP Reports on page 356.
3. Schedule and generate the new service reports as described in Generating SPI for SAP Reports on page 366.

Installing the SPI for SAP Reports

This section explains how to install the SAP NetWeaver service reports which come with the SPI for SAP and, in addition, provides information designed to help you prepare for the installation. The section covers the following topics:

Before You Begin

Before you install and set-up for the SAP NetWeaver Service Reports, you must ensure that the following tasks have been completed:

1. **Performance Agent**

   Either the HP Software Embedded Performance Component or the HP Performance Agent agent must be available on all SAP NetWeaver managed nodes for which you want to produce service reports.

   The HP Performance Agent agent must also have been configured according to the instructions given in The SPI for SAP Performance Monitors on page 222.

2. **Service Reports**

The HP Reporter instance must be available. For more detailed information about the platforms the Reporter supports, see the Reporter product documentation.

HP Reporter light is no longer bundled with HPOM for Windows. You have to install and use the *full* version of the HP Reporter to view SPI for SAP reports.

If you want to edit existing (or create new) Service Reports for the SPI for SAP, make sure that Crystal Reports is running on the machine hosting the HP Reporter. For more information about required or supported software versions, see the *HP Operations Smart Plug-in for SAP Configuration Guide*.

To Install SAP Service Reports

The service reports for SAP NetWeaver are installed into the HP Reporter product as a snap-in using InstallShield on the HP Reporter system. During set-up you will be asked to select the common application path of HP Reporter. This is the folder where you installed HP Reporter. Setup attempts to discover this path automatically and indicate to you what it finds. In most circumstances you should avoid changing it and accept the suggested settings.

The set-up copies components to the directories as summarized in Table 88. All directory paths are relative to the HP Reporter common application path.

Table 88 Locations of SAP Service Report Components

Component	Directory
Configuration files	\newconfig\
Installation script	\newconfig\
Report template files	\data\reports\Sap\
Executables	\bin\

To install the SPI for SAP Service Reports:

1. Insert the product media and browse to the following directory:

   `\Disk2\SAP SPI Reporter Package`

   Double-click the `sapspi_reporter.msi` file, and select the **`Custom Setup`** option.

2. Follow the installation-wizard's instructions. During set-up of the SPI for SAP service reports you will be asked to confirm or specify the common application path for the HP Reporter. Accept the default to ensure that all automatic configuration steps are correctly executed without the need for manual re-configuration.

   If you change the common application path, set-up will not be able to find its executables and will generate warning messages.

3. Set-up automatically performs the following tasks:

   - Creates SAP-specific report groups: SAP_R3 and SAP_ITS_620
   - Assigns metric lists to the SAP_R3 and SAP_ITS_620 report groups
   - Assigns group reports to the SAP_R3 and SAP_ITS_620 report groups
   - Assigns system reports to the SAP_R3 and SAP_ITS_620 report groups

4 Verify that the installation of the SPI for SAP service reports completed successfully by confirming that setup created the report and metrics groups mentioned in the previous step and listed in full in SPI for SAP Report Metrics on page 367. The installation should look similar to the example illustrated in Figure 33.

5 If you choose to add your SAP NetWeaver or SAP ITS systems to HP Reporter manually, you can use the following values in the Add System window replacing the example "host.name.com" with the real name of the system you want to add:

- System: **`host.name.com`**
- Replace "host.name.com" with the real name of the system you want to add to HP Reporter.
- Network: **`SAP`**
- Domain: either **`SAP`** or **`ITS`**, as appropriate

Check that your SAP NetWeaver and SAP ITS 6.20 hosts have been added to the appropriate HP Reporter group, namely; SAP_R3 or SAP_ITS_620. Hosts are automatically assigned to a report group according to the kind of data source (SAP NetWeaver or SAP ITS 6.20) discovered on the monitored host.

6 Click **`OK`** to display the newly added systems in the Reporter's Details Pane.

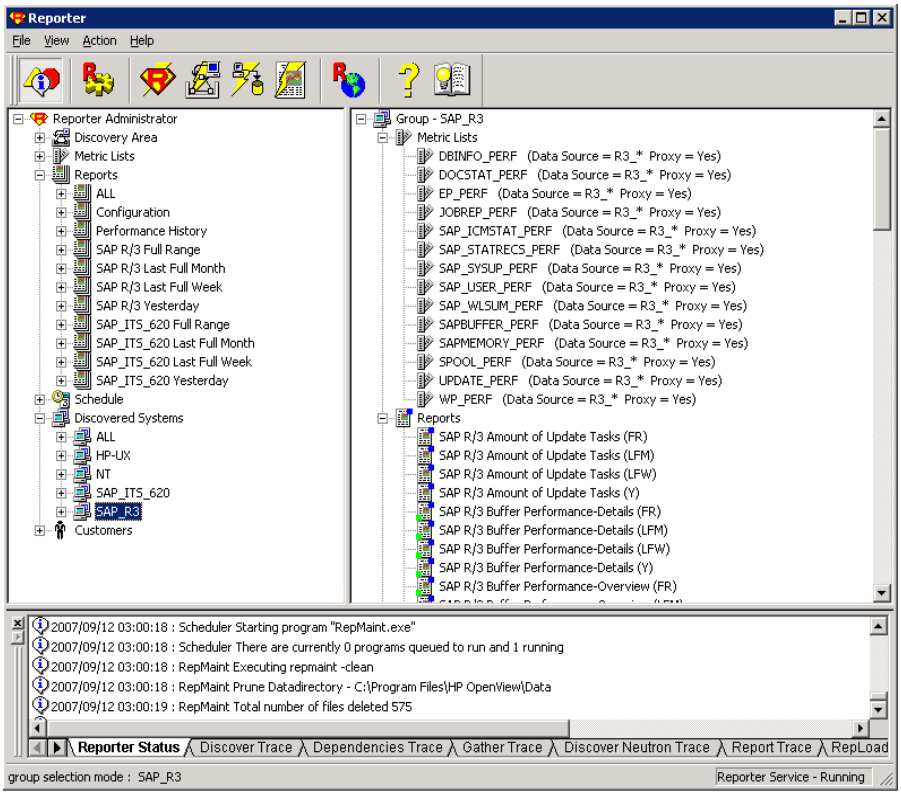
7 Use the Reporter GUI to schedule the generation of the SPI for SAP reports or generate them now using the following option:

Actions > Run > Generate Reports

Make sure you allow enough time for HP Reporter to gather the report data and store it in the HP Reporter database before you start generating reports. For more information, see Generating SPI for SAP Reports on page 366.

8 After you have successfully generated the SPI for SAP reports, you can view them with any standard web browser. For more information about how to view the SPI for SAP reports, see Viewing SPI for SAP Reports on page 367.

Figure 33 SPI for SAP Reports and Metrics



Service Reports in the SPI for SAP

The Smart Plug-in for SAP includes a package of service reports that use the data collected by the HP Software Embedded Performance Component and HP Performance Agent to generate reports, which display vital information about the health and availability of the Systems in your SAP landscape. The reports provided in the Smart Plug-in for SAP report package cover a wide variety of system- and business-critical areas.

The information in this section describes in detail the service reports, which are supplied with the SPI for SAP. You can find information about the following topics:

- SAP Reports on page 360

  A complete list of all the SAP-related reports provided with the SPI for SAP including the metrics used

- SAP ITS 6.20 Service Reports on page 365

  A complete list of the reports which the SPI for SAP provides for SAP ITS 6.20, including the metrics used

- Defining the Scope of SAP Service Reports on page 366

  Hints to help you target more accurately the information you want to display in a report

- Generating SPI for SAP Reports on page 366

  Instructions for starting the generation of the SPI for SAP reports

- Viewing SPI for SAP Reports on page 367

Instructions for viewing the SPI for SAP reports you have generated

The SPI for SAP service-report integration supports the remote-monitoring functionality, where SAP servers which are *not* HPOM for Windows managed nodes and do *not* have the SPI for SAP software installed, are monitored remotely from an HPOM for Windows managed node, where the SPI for SAP monitors are installed, configured, and running. You can generate service reports for SAP servers, which are managed remotely. For more information about remote monitoring feature, see Remote Monitoring with the Alert Monitors on page 24, and Remote Performance Monitoring on page 214.

SAP Reports

Table 89 lists the SAP reports available with the Smart Plug-in for SAP. You can also find in the table details about the information displayed in the reports and the individual metrics used to generate the reports. For more information about the SPI for SAP performance monitors, see The SPI for SAP Performance Monitors on page 222.

Table 89 SAP Performance Reports

Report	Purpose	Metrics
Database Performance	Correlates and displays the most important database performance metrics	• Physical reads/writes • Disk Physical IO • Long Table Scans • Sort Rows • Sort in Memory • Sort on Disk • Redo block Written • Redo Buffer Size
Database Quality	Shows important metrics, which taken together give a detailed picture of the quality of the database configuration	• Quality of data base buffer pool • Quality of Data Dictionary cache • Redo-Log faults • Buffer Pool Size • Dictionary Cache Size • Redo log buffer size • Buffer busy waits • Buffer busy wait time
Enterprise Portal Performance	Correlates and displays the most important status and performance metrics for the SAP Enterprise Portal	• Average response time • Average CPU time • Average Outbound data • Average number of component calls per request • Number of users making requests • Requests running in different levels • Percentage of requests not serviced
Enterprise Portal Availability		

Table 89 SAP Performance Reports (cont'd)

Report	Purpose	Metrics
E2E Time	Shows the E2E Transaction Time of the configured transactions, divided into Response and Network Time	• Response time • Network time
ICM Statistics - Overview	Shows an overview of the status of the Internet Communication Manager plus general information about queues, threads, and connections	• ICM Status • Max. number of threads • Peak number of threads • Current number of threads • Max. number of connections • Peak number of connections • Current number of connections • Max. number of queue entries • Peak number of queue entries • Current number of queue entries • Number of running work threads • Number of dead work threads • Number of processed work threads
ICM Statistics - Details	Shows a much more detailed view of the status of the Internet Communication Manager including up-time and down-time periods, plus statistics for request queues, work threads, and open connections	
Job Overview	Shows the number of jobs for the SAP instances in the different, specified states (running, ready, released)	Number of Jobs in the status: • Running • Ready • Scheduled • Released • Aborted • Finished
Number of Spool Jobs	Shows the number of spool jobs and print requests in different status	• Total Number of Spool Jobs • Number of Spool Jobs in status Archive • Number of open print Requests • Number of print Requests with errors • Number of failed print requests
Amount of Update Tasks	Shows the amount of Update tasks	• total VB-update tasks • initial VB-update tasks • erroneous VB-update tasks • update tasks having V1 executed • update tasks having V2 executed

Table 89 SAP Performance Reports (cont'd)

Report	Purpose	Metrics
Work Process Overview	Compares the total number of the different work processes with the number of in use processes	• Dialog processes/processes in Use • Batch processes/processes in Use • Spool processes/processes in Use • Update processes/processes in Use • Update2 processes/processes in Use
Document Volume	Shows the total document volumes per module (BW, FA, QA) correlated with business-transaction metrics	• GUI net time • Response time • CPU time • DB Request time
Document & Lines	Shows the number of documents and the lines created per document, sorted by SAP application module	• Head - generic doc. information • Detail - the average number of lines in the document. The larger the file, the longer it takes to commit to the database.
Document Volume by Module	Shows the volume of documents per application module	Number of documents
Workload Overview Count	Shows the number of steps for all task types in an SAP NetWeaver System, for example: Batch, Dialog, Spool, Update)	• GUI net time • Response time • CPU time • DB Request time
Workload Overview Response Time	Shows the average number of steps and response time (in seconds) for each SAP NetWeaver instance	• CPU Time • Load Time • Queue Time • DB Read Time • DB Update Time
Workload Overview Task Type	Shows the average number of steps and response time (in seconds) for each task type (AUTOABA, BCKGRD)	

Table 89 SAP Performance Reports (cont'd)

Report	Purpose	Metrics
Workload Overview DB Overview	Shows the work-load metrics based on database activity for a defined SAP NetWeaver system	• Change Count • Change Time • DB Calls • DB Requests • DB Time per Req. • Read-Dir Count • Read-Dir Time • Read-Seq. Count • Read-Seq. Time • Requested Bytes
Workload Overview DB Task Type	Shows the work-load metrics per task type and based on database activity for a defined SAP NetWeaver system	
SAP R/3 Memory	Shows SAP memory use for the defined System	• Extended Memory • Paging Area • Roll Area
SAP R/3 Users - Overview	Shows the number of users and user sessions per SAP client for a given SAP application server	• Average Users • Average Sessions
SAP R/3 Users - Workload	Shows the load for named SAP work process of users and user sessions (per SAP client/application server)	• Average Users • Average Sessions • Average Response Time • CPU Time • Dialog, Update, Spool, Batch steps
SAP R/3 Users - Document Statistics	Shows the document statistics per SAP module for users and user sessions (per SAP client/application server)	• Average Sessions • Average Users • SAP Module (FA, MM, SD)
SAP R/3 Buffer Performance - Overview	Shows general and detailed analyses of the use of SAP memory buffers by SAP users for a given instance and client.	• Buffer Name • Hit Ration • Allocated Size • Free Space • Free Space Percent • Max. Dir Entry • Free Dir Entry • Free Dir Entry (Percent) • Buffer Swaps • Buffer Swaps (Delta) • Database Accesses • Database Accesses (Delta)
SAP R/3 Buffer Performance - Detailed Analysis		

Table 89 SAP Performance Reports (cont'd)

Report	Purpose	Metrics
Threads usage rate for different ports	Shows the usage rate of different ports in the form of a bar graph.	• http • http|ssl • iiop • iiop|ssl • p4 • p4 http tunneling • p4 ssl • telnet • jms provider
Connections count	Shows the sum of connections of all types in the form of a bar graph.	• http connections • p4 connections • iiop connections • jms connections • telnet connections • Other connections • Free connections • Maximum connections
Memory Consumption	Shows the average memory consumption in the form of a bar graph.	• Allocated memory • Available memory • Used memory
Sessions view	Shows the sum of the sessions of all types in the form of a line graph.	• Active sessions • Total sessions • Timed-out sessions • Invalid sessions • Logged-off sessions

Table 89 SAP Performance Reports (cont'd)

Report	Purpose	Metrics
Requests view	Shows the sum of the requests of all types in the form of a bar graph.	• Web container all requests • p4 provider all requests • http provider all requests
Comparison of application and system threads	Shows the sum of sizes of application threads of all types in the form of a line graph.	• Minimum Application thread pool size threads • Maximum application thread pool size threads • Initial application thread pool size threads • Current application thread pool size threads • Active applications threads • Minimum system thread pool size threads • Maximum system thread pool size threads • Initial system thread pool size threads • Current system thread pool size threads • Active system threads
Comparison of application and system waiting tasks	Shows the states of the waiting task details between the application thread pool and system thread pool in the form of a line graph.	• Waiting application tasks • Waiting application queue size tasks • Waiting application queue overflow tasks • Waiting system tasks • Waiting system queue size tasks • Waiting system queue overflow tasks

SAP ITS 6.20 Service Reports

Table 90 lists the Internet-Transaction-Server (ITS 6.20) reports available with the Smart Plug-in for SAP. The table also shows details of the information displayed in the reports and the individual metrics used to generate the reports. Note that the ITS 6.20 availability report makes a distinction between single and multiple instances. For example, a system with multiple web servers configured is considered up (and available) as long as at least one of the web servers is running.

Table 90 Internet Transaction Server ITS 6.20 Reports

Report	Purpose	Metric
Availability	shows the overall availability of the ITS 6.20 systems	• Up • Down • Unknown

Defining the Scope of SAP Service Reports

You can limit the scope of any service report by using the following criteria:

- Specify which systems to include, by using one of the following possible values:
  - *all* systems
  - a selected *group* of systems
  - a selected *system*
- Specify the period for which you want to include report data by using one of the following possible values:
  - a full *range* (up to the last 180 days)
  - last full *month*
  - last full *week*
  - yesterday

Generating SPI for SAP Reports

You can use the Reporter GUI either to schedule the generation of the SPI for SAP reports or manually generate them on demand. You should consider using the schedule option, if you need to generate a lot of reports and the reports involve collecting and processing data from multiple SAP Systems. To generate single reports or multiple reports, follow the steps described below:

1 Make sure you complete the installation and configuration steps described in To Install SAP Service Reports on page 357 before you start generating reports.

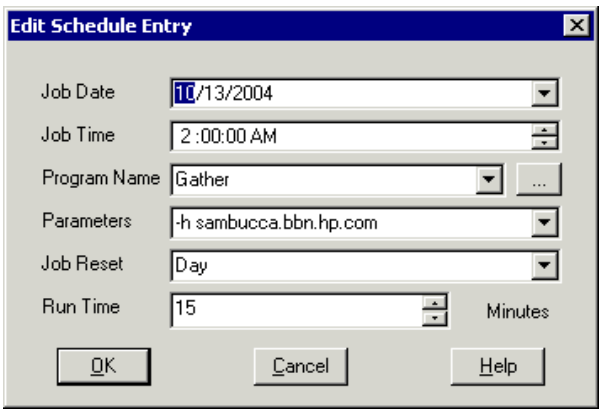
2 Use the Reporter GUI to schedule data collection for the SPI for SAP reports using the following menu option:

Report Administrator> Schedule > Gather

In the right pane, select and right-click the job whose schedule you want to view or change. To ensure that *all* data up to the current hour are included in the collection for the given host, use the `-h` option before the host name in the `Parameters` box of the `Edit Schedule Entry` window.

Due to differences between the way SAP and the SPI for SAP's performance-data sources (HP Software Embedded Performance Component and HP Performance Agent) handle time, avoid scheduling data collection to start between midnight (00:00) and 2 a.m. (02:00). Run data collection *after* 02:00 instead, as illustrated in Figure 34 on page 367.

Figure 34 Setting up Data Collection for Reports



3 Use the Reporter GUI to start the generation of the SPI for SAP reports using the following option:

Actions > Run > Generate Reports

Remember to allow enough time for the data-collection process to complete to ensure you have all the latest data for the reports.

Viewing SPI for SAP Reports

To view the SPI for SAP reports:

1 First, ensure that the reports have been successfully generated. For more information about generating reports, see To Install SAP Service Reports on page 357.

2 Open a web browser

3 Enter the following string in the location bar:

```
http://<machine.name.com>/HPOV_reports/reports.htm
```

4 Navigate through the displayed reports to the report, which you want to examine more closely.

SPI for SAP Report Metrics

This section lists the metrics used by the reports for SAP R/3 and SAP ITS 6.20, which are installed as part of the SPI for SAP reporter package. For more information about the metrics listed in the section below, see The SPI for SAP Performance Monitors on page 222. For more information about the SPI for SAP reports, see Service Reports in the SPI for SAP on page 359.

SAP NetWeaver Report Metrics

The information in this section shows which performance metrics are used to gather the data that is used in the preparation of the performance-related reports for the SPI for SAP. Note that the name of the performance metric is often (but not always) the same as the monitor

that collects the performance data. For example, the SPI for SAP performance monitor DBINFO_PERF uses the metrics list DBINFO_PERF; the performance monitor USER_PERF uses the metrics list SAP_USER_PERF.

Table 91 lists the metrics that are available to the SPI for SAP and shows which performance monitor uses the metric.

Table 91 SPI for SAP Performance-report Metrics

Report-metric Name	Referenced Monitor	Description
DBINFO_PERF	DBINFO_PERF	Collects database-performance analysis values
DOCSTAT_PERF	DOCSTAT_PERF	Collects the quantity-structure statistics (the document volume) for the last full hour
EP_PERF	EP_PERF	Monitors the status and performance of the SAP Enterprise Portal
JOBREP_PERF	ICMSTAT_PERF	Counts the number of jobs per state (scheduled, running, etc.)
SAPBUFFER_PERF	SAPBUFFER_PERF	Returns values for the use of SAP memory *buffers* for an SAP instance
SAPMEMORY_PERF	SAPMEMORY_PERF	SAP memory used by SAP users for an SAP instance
SAP_ICMSTAT_PERF	ICMSTAT_PERF	Monitors the status and performance of the SAP Internet Communication Manager
SAP_STATRECS_PERF	STATRECS_PERF	Returns the response/net times of defined transactions
SAP_SYSUP_PERF	SYSUP_PERF	Shows the status of the SAP NetWeaver instances
SAP_USER_PERF	USER_PERF	Monitors the number of users and user sessions per SAP client for a given SAP application server
SAP_WLSUM_PERF	WLSUM_PERF	Collects the performance-workload statistics
SPOOL_PERF	SPOOL_PERF	Counts the number of spool requests in different states
UPDATE_PERF	UPDATE_PERF	The number of update processes
WP_PERF	WP_PERF	Number of users/sessions per SAP client for an SAP application server

SAP ITS 6.20 Report Metrics

The following list shows which performance metrics are used to gather the data that is used in the preparation of the performance-related reports for the SPI for SAP's ITS 6.20 monitor:

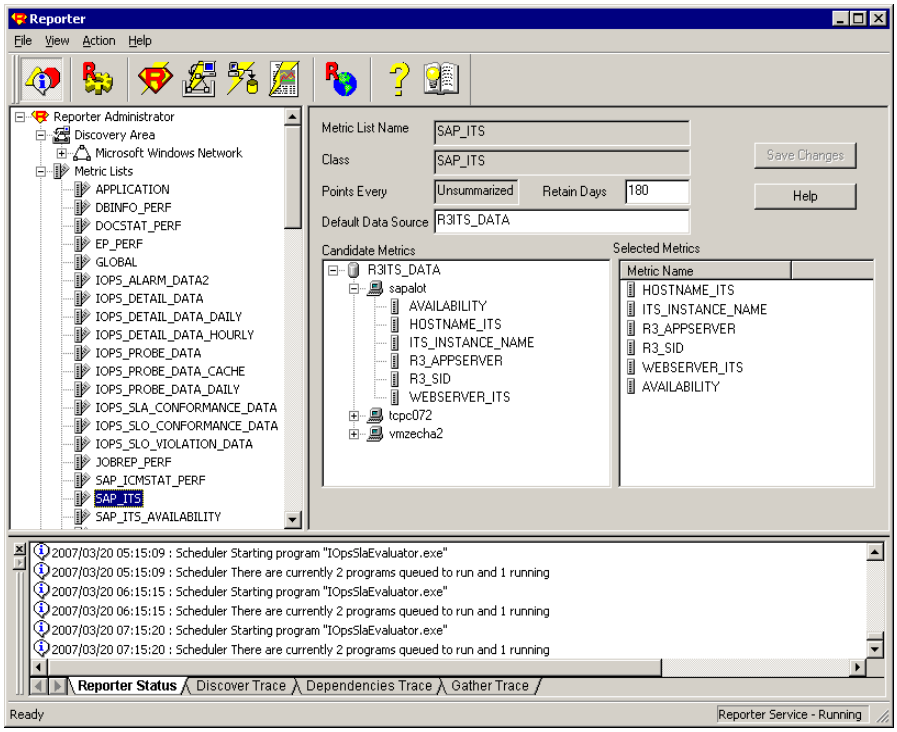
- SAP_ITS

  Uses the data source “R3ITS_DATA” to gather data relating to the named ITS 6.20 instances.

- SAP_ITS_AVAILABILITY

  Uses the data source “gatherSAPITS” to gather data relating to the named ITS 6.20 instances.

Figure 35 SAP ITS 6.20 Report Metrics



Removing the SPI for SAP Reports

To completely remove the SPI for SAP reports and the integration with the HP Reporter, you need to perform the following steps described in this section in the order specified. This section covers the following topics:

- To Remove HP Reporter Snap-in Packages on page 369
- To Remove the SPI for SAP from the Reporter System on page 370

To Remove HP Reporter Snap-in Packages

Use the following instructions to help you remove the SPI for SAP snap-in package for the HP Reporter quickly and easily from the HP Reporter system:

1 In Reporter, browse to:

File > Configure > Reporter Packages

2 Select the following files from the Installed Packages window located in the right pane of the Configure Report Packages window:

- SPI for SAP - ITS Reports
- SPI for SAP

3 Double-click the left arrow button **[<-]** in the `Available Packages` window located in the left pane of the `Configure Report Packages` window.

4 Click **OK** to finish

To Remove the SPI for SAP from the Reporter System

To remove the SPI for SAP binaries from the HP Reporter system, you need to carry out the following steps on the HP Reporter system as the system administrator:

1 Go to the HP Reporter system.

2 Insert the HP Operations SMart Plug-in DVD in the DVD drive.

3 Chose to remove program.

4 Follow the on-screen instructions and select Reports under SAP SPI.

5 Follow the on-screen instructions to complete the removal process.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

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: