HP OpenView Operations Smart Plug-in for SAP

Administrator's Reference

Software Version: 10.20

For HP-UX and Sun Solaris operating systems

Manufacturing Part Number: None
Document Release Date: December 2006
Software Release Date: December 2006

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.

Linux® is a U.S. registered trademark of Linus Torvalds.

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.

X/Open® is a registered trademark, and the X device is a trademark of X/Open Company Ltd. in the UK and other countries.

4. The SPI for SAP Alert-Collector Monitors

5. Understanding Message Flow

6. The SPI for SAP Performance Monitors

10. Troubleshooting the SPI for SAP

Support

Please visit the HP OpenView web site at:

http://www.hp.com/managementsoftware/support/

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

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

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. To find more information about access levels, go to the following URL:

http://support.openview.hp.com/access_level

To register for an HP Passport ID, go to the following URL:

http://www.managementsoftware.hp.com/passport-registration.html

1 Introducing the Smart Plug-in for SAP

This section describes what information is in the *HP OpenView Smart Plug-in for SAP Administrator's Reference* and where you can find it.

Overview

The *HP OpenView Smart Plug-in for SAP Administrator's Reference* provides information designed to help the administrators of both OVO and SAP R/3 to configure the SPI for SAP to suit the needs and requirements of the SAP R/3 landscape which they plan to manage with OVO. This book also explains how to install and configure the various, additional sub-agents that come with the SPI for SAP. Finally, the *HP OpenView Smart Plug-in for SAP Administrator's Reference* describes how to integrate the SPI for SAP with performance-related products that are available as part of HP OpenView.

The *HP OpenView Smart Plug-in for SAP Administrator's Reference* consists of the following sections:

- "Customizing the SPI for SAP Monitors" on page 17

  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 57

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

- "The SPI for SAP Alert-Collector Monitors" on page 123

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

- "Understanding Message Flow" on page 241

  This section describes how to use both OVO functionality and CCMS to control the flow of messages between SAP R/3 and OVO.

- "The SPI for SAP Performance Monitors" on page 263

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

- "The SAP ITS Monitor" on page 325

  This section describes how to install and configure the ITS Monitor. The **Internet Transaction Server** (ITS) provides the SAP R/3 user with an SAP R/3 transaction interface in a web browser.

- "Service Views" on page 355

  This section introduces the concept of service views and explains how to use service views to improve the management of your SAP R/3 landscape.

- "Service Reports" on page 371

  This section describes how to install the SPI for SAP service reports, configure the OpenView Reporter to generate the reports, and use the reports to monitor and manage your SAP R/3 landscape.

- "Troubleshooting the SPI for SAP" on page 395

  This section provides information that is designed to help troubleshoot the problems you encounter when working with the SPI for SAP.

2 Customizing the SPI for SAP Monitors

This section describes how to set up the SPI for SAP monitors and distribute them to the SAP R/3 servers in your SAP R/3 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 OVO administrators, working from the OVO desktop, distribute the appropriate SPI for SAP message-source templates to the SAP R/3 servers which they want to manage and monitor with OVO. Monitor distribution 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 R/3 users and their associated logons as described in the *HP OpenView Smart Plug-in for SAP Installation 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 OpenView Smart Plug-in for SAP Installation Guide*)

  or,

  — at any time, using the `Config SAP R/3 GUI` function in the `SAP R/3 Admin` application group

NOTE

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 "Specifying SAP R/3 Systems to Monitor" in the *HP OpenView Smart Plug-in for SAP Installation Guide*.

The SPI for SAP Monitors

Table 2-1 provides an overview of SPI for SAP alert-monitors.

Table 2-1 The Alert Monitors

Alert Monitor	Monitor Function
`r3monal` [a]	Monitors SAP R/3 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 2-2 provides an overview of the alert-collector monitors used by `r3moncol`, the SPI for SAP alert collector.

Table 2-2 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 239.; see "Monitoring the TemSe file" on page 239.

Table 2-2 The r3moncol Alert-Collector Monitors (Continued)

Alert-Collector Monitor	Monitor Function
r3monale	Monitors the status of iDOCs in the SAP R/3 System
r3monchg	Monitors the SAP R/3 system change options.
r3moncts	Monitors the correction-and-transport system.
r3mondmp	Monitors ABAP/4 Dumps.
r3monjob	Monitors SAP R/3 batch jobs.
r3monlck	Monitors the Enqueue process, which manages logical locks for SAP R/3 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 R/3.

Table 2-2 The r3moncol Alert-Collector Monitors (Continued)

Alert-Collector Monitor	Monitor Function
`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 usable 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 29

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

- "The Alert-Monitor Configuration Files" on page 60

  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 106

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

- "The r3status Configuration File" on page 90
- "The Alert-Collector Monitor Configuration Files" on page 138

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

Configuration files can be distributed to the managed nodes either globally or locally, as follows:

- **Globally**

  Globally using the `Install Config` function in the `SAP R/3 Admin` application group, which distributes copies of each configuration file to all selected managed nodes.

- **Locally**

  Locally using the `Distribute Local Config` function in the `SAP R/3 Admin Local` application group.

For more information about when to use each of these distribution methods and for instructions on editing the configuration files, see "The SPI for SAP Monitor-Configuration File" on page 29.

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 50.

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 83.
2. On UNIX managed nodes:
   a. Local configuration file

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

      `<OvDataDir>/conf/sapspi/local`

   b. Global configuration file

      If the monitor does not find an OVO 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 MS Windows managed nodes:
   a. Local configuration file

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

      `%OvAgentDir%\conf\sapspi\local`

   b. Global configuration file

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

      `%OvAgentDir%\conf\sapspi\global`

In Example 2-1, the first line relates only to instance 01 on SAP system LPO. Therefore, for SAP instance 01, the monitor applies the rules as defined on this line *only*. The second line of the example refers to all other instances on LPO. The final line refers to all instances on all systems except for LPO

Example 2-1 Order of Precedence for Configuration Files

```
Order of        SAP        SAP
Precedence      System     Number
1               =LPO       =01      =<monitor-spec conf>
2               =LPO       =ALL     =<monitor-spec conf>
3               =ALL       =ALL     =<monitor-spec conf>
```

Remote Monitoring with the Alert Monitors

The current version of 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* OVO managed nodes and where the SPI for SAP is *not* installed. You set up and perform the remote monitoring from an OVO managed node, where the SPI for SAP software is running.

NOTE

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

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 RemoteHost. For more information about the `r3itosap.cfg` file, refer to the *HP OpenView Smart Plug-in for SAP Installation Guide*.

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. Example 2-2 on page 27 shows how a new line is required for each *additional* SAP server, which you want to monitor remotely.

- Enable the new **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 OVO node bank.

The RemoteMonitoring keyword accepts the following parameters:

- **LocalHost**

  This is the name of the local OVO managed node where the SPI for SAP software is running and whose OVO 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 OVO managed node, it must be present in the OVO node bank 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 29 and "The Alert-Monitor Configuration Files" on page 60.

Example 2-2 Specifying Individual Remote Servers to Monitor

```
#------------------------------------------------------------
# Remote                Local       Remote
# Monitoring            Host        Host
```

```
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 29.

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 by alert type and distribute the modified configuration files to the managed nodes.

Each configuration file provided with the SPI for SAP defines particular default settings by means of keywords. This section indicates which keywords you can use with which monitors and, where appropriate, shows permitted values for keyword parameters. This section provides detailed information about the following keywords:

Alert Classes

You use the alert-classes section at the end of the monitor-configuration file to define conditions that, when met, generate messages about the SAP alerts you are monitoring. The contents of the alert-classes section changes according to the parameters that are allowed or required for a given monitor. For example, the parameters `SAP Hostname`, `SAP system`, and `SAP number` tend to be present in all the monitor-configuration files; the `=CHANGE_OPT` alert type can only be used with `r3monchg`, the System Change Monitor.

For more information about which alert types and parameters are allowed with which monitor-specific Alert Classes, see the information in this section and, in addition, the section which corresponds to the individual monitor you want to configure.

NOTE

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 R/3 and, in addition, the local SAP R/3 landscape, which you want to manage with the SPI for SAP.

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

- **Alerttype**:

  `=<`*`Alerttype`*`>` For more information about the values an alert-collector monitor accepts, see the alert types section for a given monitor, for example; "r3monale: The iDOC-Status Monitor" on page 149 refers to the alert type "IDOC_CURRENT_STATUS".

- **AlertMonitor**:

  `=<`*`Monitor_Name`*`>`

  where `<`*`Monitor_Name`*`>` is 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.

- **Filemask** (`r3mondev` only):

  =*<File_Name>*

  where *<File_Name>* is 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>* where *<mode_value>* is the way 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 82.

- **OPC MsgGroup**:

  =*<OVO_Msg_Group>*

  where *<OVO_Msg_Group>* is the name of the OVO 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 OVO 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**:

  =*<OVO_Object>* where *<OVO_Object>* is the OVO 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 OVO 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 Class described below.

- **OPC Severity**:

  =<*OVO_Msg_Severity*>

  where <*OVO_Msg_Severity*> is the severity level of the OVO message you want to map the CCMS alert to, for example: Normal, Warning, Major, Critical.

- **ProcessName** (`r3monpro` only):

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

- **ProcessNumber** (`r3monpro` only):

  =<*nn*> where <*nn*> is the number 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 82.

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

  =<*RFC_Param*> where *RFC_Param* is 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 130. For more information about monitor-specific, alert-type parameters, see the appropriate monitor description, for example: Table 4-7, "IDOC_CURRENT_STATUS Configuration Parameters," on page 151 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.

AlerMonSyslog

Syslog filtering can be used *only* with the `r3monal` alert monitor. You use it to configure syslog filtering 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 46. The AlerMonSyslog keyword requires a value for the following parameters:

```
AlertMonSyslog =<SAP System> =<SAP Number> =<SyslogId> \
=<Enabled/Disabled>
```

- **SAP System**

  The SAP System ID whose CCMS alerts or system logs you want to monitor

- **SAP Number**

  This SAP *instance* number associated with the SAP System whose CCMS alerts or system logs you want to monitor

- **SyslogId**:

=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.

- **Enable/Disable**:

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

CCMS Acknowledge Message

Only with `r3monal` with SAP 4.6 (and later) and the XMI/XAL interface

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 OVOThis keyword requires a value for the following parameters:

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

- **SAP System** (`r3monal` with SAP 4.6 and later *only*):

  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 OVO.

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

- **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 *Only* with `r3monal` with SAP 4.6 (and later) and the XMI/XAL interface

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”

- **Instance Nr**:

  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. 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

- **OVO Msg Group**:

  The name of the OVO message group to which the message generated by `r3mondisp` should be assigned

- **OVO Msg Object**:

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

- **OVO Msg Severity**:

  The severity assigned to the OVO 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 message browser 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 103.

The EnableDPQueueCheck keyword requires the following parameters:

```
EnableDPQueueCheck =<hostname> =<SAP System> =<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.

- **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"

- **Instance Nr**:

  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 of the message sent to OVO 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`

  MS Windows: `=default`

The `=default` value here is associated with the default path to the history files which the SPI for SAP monitors write. UNIX managed nodes generally use `/var/opt/OV/conf/sapspi/`. AIX uses `/var/lpp/OV/conf/sapspi/` for DCE agents. MS Windows managed nodes use `\usr\OV\conf\sapspi\` for DCE agents and `\Program Files\HP OpenView\data\conf\sapspi\` for https agents.

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`

Monitoring Conditions

The monitors use the monitoring conditions specified in the monitor-configuration file to determine which alert-collection functions to call when the monitor runs, as well as any limiting parameters for these functions. The conditions also define rules for any messages that the alert collectors generate during their run. You can define default conditions that apply to all SAP systems and instances, and exceptions that apply only to specific systems and instances.

Note that the keywords you use to define the conditions associated with a particular monitor differ according to the scope of the monitor and the specific area of SAP, which the monitor manages. For example, you can only use the `AlertDevMon` keyword in the configuration file for the `r3mondev` monitor. Similarly, the `AlertMonPro` and `AlertInstMonPro` keywords only appear in the `r3monpro` monitor's configuration file. For more information about which keywords you can use with a particular monitor, see the section that describes the monitor you are configuring, for example; `r3mondmp`, the ABAP dump monitor.

Try to avoid ambiguous definitions if at all possible. For example, in the configuration below, the final two lines cause a logical clash because both `msg4` and `msg5` define OVO objects for roll paging messages from the same SAP instance of the same SAP system. The result could be a lot of unwanted or confusing messages.

```
AlertClassRollpag  =ALL  =ALL  =1  =RollPag  =R3_Roll-Paging
AlertClassRollpag  =ALL  =01   =1  =msg2     =R3_Roll-Paging
AlertClassRollpag  =LPO  =ALL  =1  =cwmsg3   =R3_Roll-Paging
AlertClassRollpag  =LPO  =01   =1  =msg4     =R3_Roll-Paging
AlertClassRollpag  =LPO  =01   =1  =msg5     =R3_Roll-Paging
```

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 OVO managed node where the SPI for SAP is running and whose OVO 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 OVO 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.

Example 2-3 Setting up Remote Monitoring for r3monal

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

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

- "Remote Monitoring with the Alert Monitors" on page 26
- "r3status: Monitoring SAP Remotely" on page 92
- "Remote Monitoring with the Alert-Collector Monitors" on page 135
- "Remote Performance Monitoring" on page 286

RFC Time Out

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

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

The SeverityValue keyword enables the `r3monal` monitor to map the severity of CCMS alerts (for example; SeverityCritical) in the SAP subsystem to messages in OVO (for example; CRITICAL) and accepts the following values:

```
<SAPSeverityLevel> =<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 OVO:

=Enabled	Consider CCMS alerts with the severity <SAPSeverityLevel> and send a message to OVO with the severity <OpcSeverity>.
=Disabled	Ignore CCMS alerts with the severity <SAPSeverityLevel> and do *not* send a message to OVO.

Table 2-3 Mapping Severity Levels

CCMS Alert Severity	OVO Message Severity
SeverityCritical (red)	= CRITICAL
SeverityWarning (yellow)	= WARNING
SeverityNormal (green)	= NORMAL

Table 2-3 Mapping Severity Levels (Continued)

CCMS Alert Severity	OVO Message Severity
SeverityNull	= UNKNOWN

Note that the alert-*collector* monitors (`r3moncol`) have two *additional* OVO 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: `/var/lpp/OV/log`

  — HTTPS: `/var/opt/OV/log`

  — **MS Windows:**

  — DCE: `\usr\OV\log`

  — HTTPS: `\Program Files\HP OpenView\log`

  For more information about changing the path, see the environment variable SAPOPC_TRACEPATH in "Alert-Collector Monitor Environment Variables" on page 134.

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; this is the default setting for all configuration files.
=1	`r3monal`, `r3mondev`, `r3monpro`: Enable 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 73.

To Configure the SPI for SAP Alert Monitors

1. In the application desktop, double-click the appropriate application group icon. There are two application groups that include monitor configuration icons:

`SAP R/3 Admin`	For global configurations
`SAP R/3 Admin Local`	For local configurations

2. In the `Application Group` window, double-click the icon that corresponds to the alert monitor to be changed. The selected alert monitor's configuration file opens.

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 46.

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 2-4

Table 2-4 Default Trace File Names

Tracefile Name	Monitor Alert Type
`r3monaco.log`	Alert Calls
`r3monal.log`	Alerts (SAP R/3 4.x)
`r3monale.log`	iDOC alerts
`r3monchg.log`	System Change
`r3moncts.log`	Correction and Transport System
`r3mondev.log`	Trace and Log Files

Table 2-4 Default Trace File Names (Continued)

Tracefile Name	Monitor Alert Type
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 MS Windows servers:

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

NOTE

You can tell the alert monitors to use a specific history path on MS 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 40.

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.

IMPORTANT

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 "Monitoring Conditions" on page 42 and "Alert Classes" on page 30 for general information about the keywords and parameters that are allowed with each monitor.

NOTE

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 can distribute the alert-monitor configuration files to the managed nodes in any one of the following ways:

1. The `.Install Config` application

   Use the `.Install Config` application located in the `SAP R/3 Admin` application group. The `.Install Config` application distributes copies of each *global* monitor-configuration file to all selected managed nodes. This method can be used by any OVO user with the necessary access permissions.

2. The `Distribute Local Config` application

   Use the `Distribute Local Config` application located in the `SAP R/3 Admin Local` application group. The `Distribute Local Config` application distributes a copy of the *local* monitor-configuration file to the selected managed node *only*. Distributing monitors does *not* ensure the availability of monitor-configuration files on managed nodes. This method can be used by any OVO user with the necessary access permissions.

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 25.

Global configuration files are installed in the following directories on the OVO managed node:

- UNIX: `/var/opt/OV/conf/sapspi/global`
- AIX (DCE): `/var/lpp/OV/conf/sapspi/global`

  AIX (HTTPS): `/var/opt/OV/conf/sapspi/global`
- MS Windows (DCE): `\usr\OV\conf\sapspi\global`

  MS Windows (HTTPS): `\Program Files\HP OpenView\data\conf\sapspi\global`

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

- UNIX: `/var/opt/OV/conf/sapspi/local`
- AIX (DCE): `/var/lpp/OV/conf/sapspi/local`

  AIX (HTTPS): `/var/opt/OV/conf/sapspi/local`
- MS Windows (DCE): `\usr\OV\conf\sapspi\local`

  MS Windows (HTTPS):
  `\Program Files\HP OpenView\data\conf\sapspi\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 applied and distributed. This section provides instructions for the following tasks:

- "To Apply a Global Configuration" on page 52
- "To Apply a Local Configuration" on page 53
- "To Delete Selected Local Configurations on a Node" on page 55

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 25.

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

To Apply a Global Configuration

1. In the application group `SAP R/3 Admin`, double-click the icon associated with the alert monitor, which you want to configure.
2. Edit the configuration file of the alert monitor as required. For a detailed description of file parameters, see "To Configure the SPI for SAP Alert Monitors" on page 47.
3. Save the modified configuration file.

NOTE

If you use the standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration file 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 143 and "Understanding Configuration-File Error Messages" on page 143.

4. Double-click the icon `Install Config` to include the monitor configurations in the SPI for SAP R/3 database.
5. Repeat steps 1 through 3 for each alert type you wish to monitor, making sure to make all required changes in each corresponding alert monitor configuration file.
6. In the `Node Bank` window, select the managed nodes to which you want to distribute updated configurations.
7. Double-click the icon `.Install Config`

   The *global* configuration files are copied to one of the following directories on each of the selected managed nodes:

   - UNIX: `/var/opt/OV/conf/sapspi/global`
   - AIX (DCE): `/var/lpp/OV/conf/sapspi/global`

     AIX (HTTPS): `/var/opt/OV/conf/sapspi/global`
   - MS Windows (DCE): `\usr\OV\conf\sapspi\global`

     MS Windows (HTTPS):
     `\Program Files\HP OpenView\data\conf\sapspi\global`

To Apply a Local Configuration

1. In the `Node Bank` window, select the managed node(s) on which you want to create or update a local configuration.
2. On the management server in the application group `SAP R/3 Admin Local`, double-click the icon associated with the alert monitor you want to configure.
3. Edit the configuration file of the alert monitor as required. For more information, see "To Configure the SPI for SAP Alert Monitors" on page 47

IMPORTANT

If this is the first local configuration for the selected alert monitor and node, opening the configuration file automatically places a copy of the dedicated global-configuration file in the local-configuration directory on the managed node.

If you do not want to have a local configuration for this alert monitor, you must delete this file from the directory before the next distribution of local-configuration files.

4. Save the modified configuration file.

NOTE

If you use the standard SPI for SAP tools to configure `r3moncol` alert collectors, the SPI for SAP checks the validity of the new configuration file 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 143 and "Understanding Configuration-File Error Messages" on page 143.

5. Repeat steps 1 through 3 for each alert type you wish to monitor locally, ensuring you make all required changes in *each* corresponding alert-monitor configuration file.
6. In the `Node Bank` window, select the managed nodes to which you want to distribute updated local configurations.
7. In the application group `SAP R/3 Admin Local`, double-click the `Distribute Local Config` icon.

   The *local* configuration files are copied to one of the following directories on each of the selected managed nodes:

   - UNIX: `/var/opt/OV/conf/sapspi/local`
   - AIX (DCE): `/var/lpp/OV/conf/sapspi/local`

     AIX (HTTPS): `/var/opt/OV/conf/sapspi/local`
   - MS Windows (DCE): `\usr\OV\conf\sapspi\local`

     MS Windows (HTTPS): `\Program Files\HP OpenView\data\conf\sapspi\local`

To Delete All Local Configurations on a Node

1. In the `Node Bank` window, select the managed node(s) for which you want to delete the local configuration.

2. On the management server, in the application group `SAP R/3 Admin Local`, double-click the icon `Delete Local Config`.

   On the management server, the local-configuration directories for the selected managed nodes are deleted and the updated configurations are distributed to the managed nodes.

To Delete Selected Local Configurations on a Node

1. On the OVO management server, change to the local-configuration directory for the node:

   `cd /var/opt/OV/share/conf/sapspi/local/<node_name>`

2. Remove the configuration file that is no longer required:

   `rm <filename>.cfg`

3. In the `Node Bank` window, select the managed node whose local configuration you want to delete.

4. In the application group SAP R/3 `Admin Local`, double-click the icon `Distribute Local Config`.

   The existing local configuration is removed and replaced by the new configuration, which does not include the configuration file you have removed.

IMPORTANT

Even if it is empty, do not manually remove the `directory /var/opt/OV/share/conf/sapspi/local/<node_name>` on the management server.

If you accidentally remove this directory, or this directory is otherwise not present, the `Distribute Local Config` function is not able to redistribute the configuration, which means that the local configuration on the managed node cannot be updated.

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 R/3 servers, which you want to manage and monitor with OVO. Monitor distribution is part of the SPI for SAP installation and configuration process. Before distributing a monitor, the OVO administrator, working from the OVO desktop, first assigns and distributes the appropriate SPI for SAP message-source templates.

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. For more information about the default polling rates for each alert monitor, see Table 3-1, which shows the rates in days, hours, and minutes.

Table 3-1 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 OVO message-source template and in several files, including an executable file and a configuration file.

The message-source template defines the rules for generating messages that appear in the OVO message browser. The message-source template also controls the frequency with which the associated executable file runs. If you want to customize a message-source template, follow the instructions given in the online help for OVO administrators.

The monitor executable file runs at the regular interval defined in the message-source template. It checks for and reports conditions according to monitoring 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 templates, refer to the *HP OpenView Smart Plug-in for SAP Installation 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 90. Example 3-1 on page 61 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`".

Example 3-1 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      MsgGroup
#AlertDevMon    =ALL  =ALL    =1        =dev_*     =WARNING  =r3mondev  =R3_Trace
#AlertDevMon    =ALL  =ALL    =1        =std*      =CRITICAL =r3mondev  =R3_Trace
#Dispatcher trace file
AlertDevMon     =ALL  =ALL    =1        =dev_disp  =WARNING  =r3mondev  =R3_Trace
#Workprocess trace file for workprocess with number 0
AlertDevMon     =ALL  =ALL    =1        =dev_w0    =WARNING  =r3mondev  =R3_Trace
#message server trace file
AlertDevMon     =ALL  =ALL    =1        =dev_ms    =WARNING  =r3mondev  =R3_Trace
#screen processor trace file
AlertDevMon     =ALL  =ALL    =1        =dev_dy0   =WARNING  =r3mondev  =R3_Trace
#tp process trace file
AlertDevMon     =ALL  =ALL    =1        =dev_tp    =WARNING  =r3mondev  =R3_Trace
--------------------------------------------------------------------------------
```

r3monal: the CCMS 4.x Alert Monitor

The `r3monal` monitor uses the SAP R/3 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 OVO messages, which you can view in the OVO message browser.

NOTE 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 levels, RFCTimeOut, CCMSMonitorSet, and CCMSAcknowledgeMessage; all other keywords in the `r3monal.cfg` configuration file are optional.

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 OVO. Figure 3-1 on page 64 shows how the application servers `bounty` and `hpspi003` appear in the Monitor-tree when you select and expand the central-instance item `WA1`.

NOTE

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:

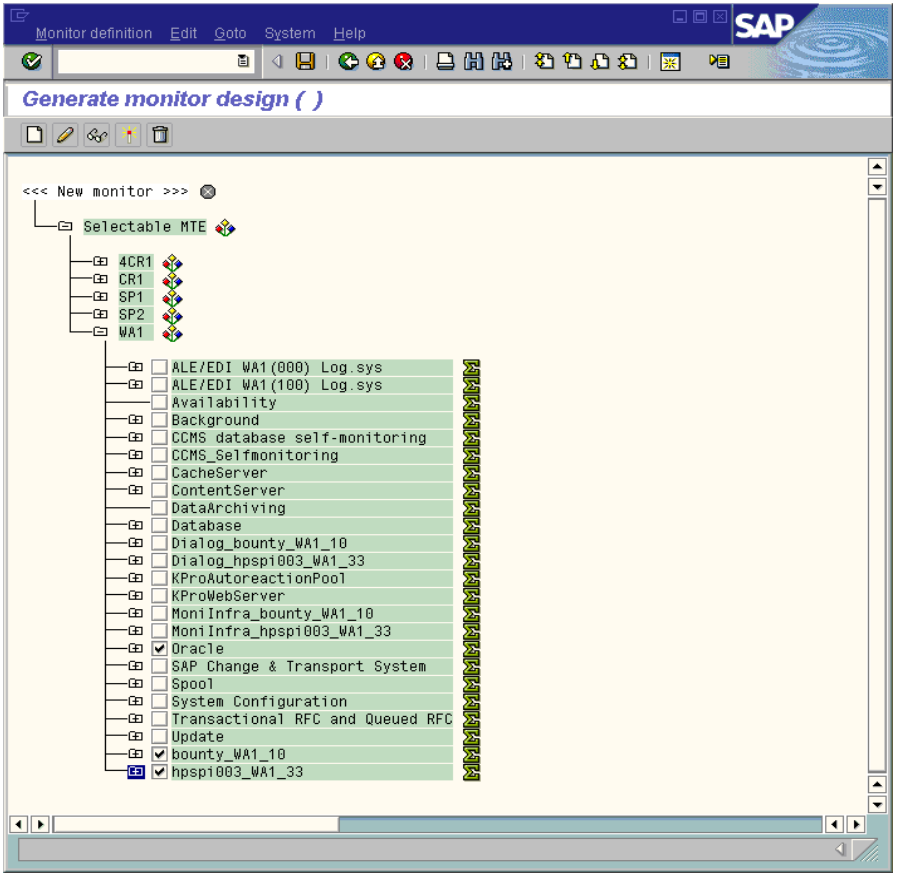
```
Extras > Activate Maintenance Function
```

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 OVO. In the example configuration shown in Figure 3-1, we have also selected the `Oracle` item so that we hear about problems with the database, too.

Make sure that the new monitor sets you define for the SPI for SAP are visible to and usable by the OVO user, which you have defined for the SPI for SAP. If you are logged into SAP as the defined OVO user, then you can see only the CCMS monitor sets defined for the defined OVO 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 OVO 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.

Figure 3-1 Defining a Monitor Set



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 Example 3-2. 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 Example 3-2.

Note that the combination of traditional long SAP names and the line break in the example configuration file shown in Example 3-2 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 Example 3-2, where the **SPISAP** monitor set has two Monitors; **System** and **DB_ALERT**.

Example 3-2 Configuring Multiple Monitor Sets

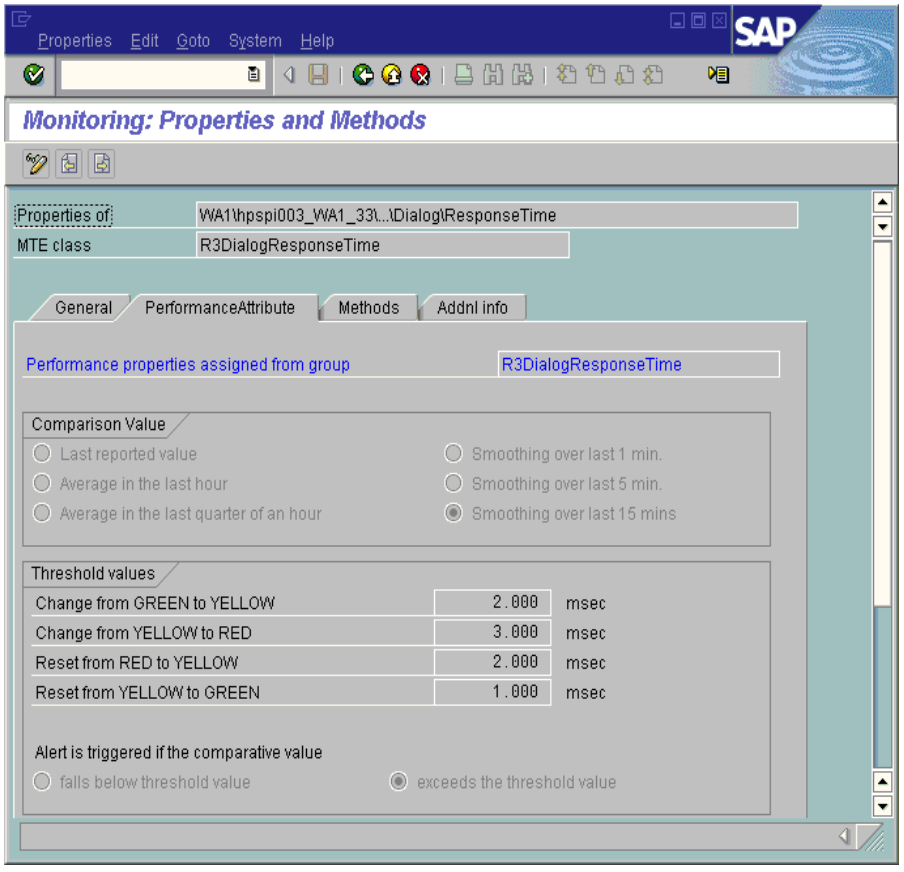
```
#-------------------------------------------------------------------------
# Monitor Set    SAP     SAP     Monitor Set                          Monitor
#                System  Number
CCMSMonitorSet   =WA1    =33     =SPISAP                              =System
CCMSMonitorSet   =WA1    =33     =SPISAP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

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 3-2 on page 66. You need to:

- ensure that the severity level of the CCMS Alerts matches the severity level of the OVO messages, which are generated by the CCMS Alerts.
- ensure that severity-level thresholds configured for a given CCMS alert monitor are appropriate for your needs.

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.

Figure 3-2 **Checking and Modifying CCMS Alert-Monitor Thresholds**

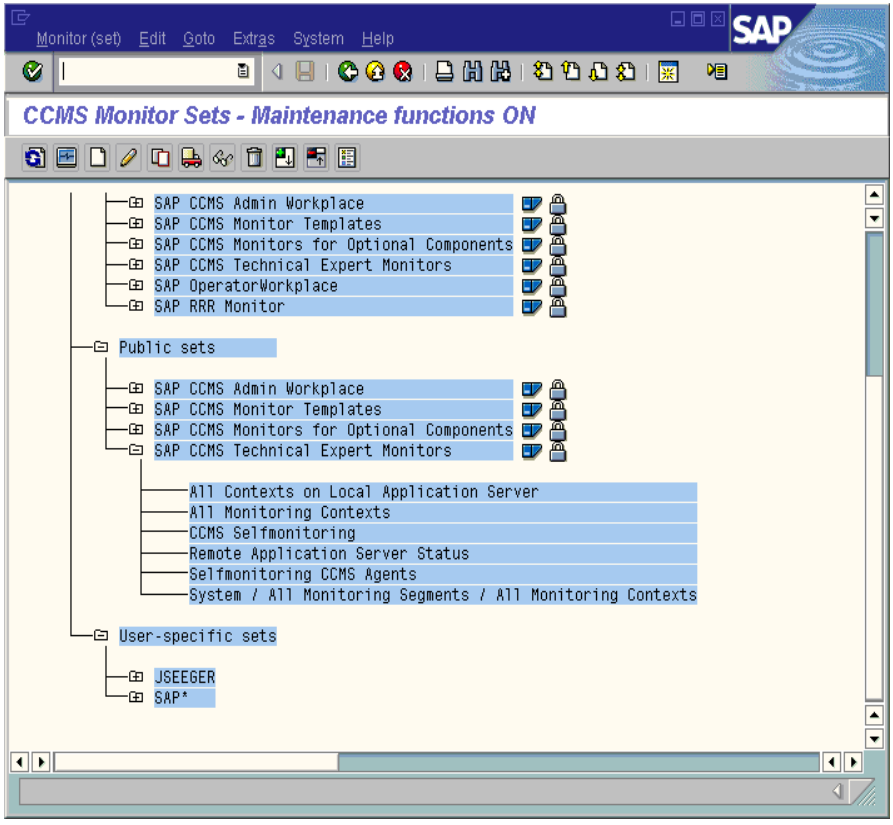


r3monal: CCMS Alert Monitors

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 R/3 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 3-3. Note that *public* Monitor sets are visible to (and usable by) all SAP users.

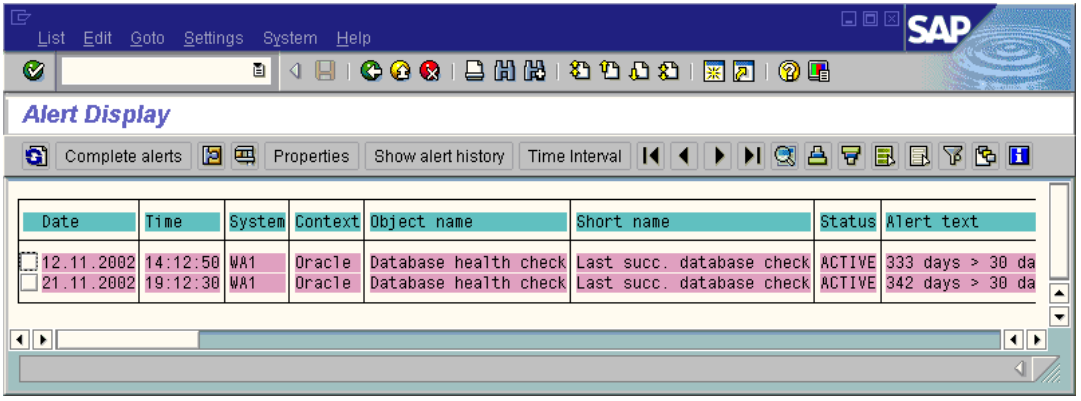
Figure 3-3 **CCMS Monitor Sets**



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. 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 3-4 CCMS Alert Properties



When a condition is reported in the SAP R/3 CCMS monitor, the monitoring object and its attributes are included in the resulting alert as shown in Figure 3-4.

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.

Example 3-3 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.

Note that, if you enable the CCMSAcknowledgeMessages keyword, you also need to make sure that you enable the SeverityValue keyword, too; the SeverityValue keyword allows you to filter CCMS alerts according to severity. For more information, see "r3monal: Severity Levels" on page 71.

r3monal: Environment Variables

Table 3-2 lists the environment variables, which you can use to configure the `r3monal` monitor.

Table 3-2 r3monal Environment Variables

Environment Variable	Description
SAPOPC_DRIVE	The Windows drive where the OVO agent is running, for example; `E:\usr\...`
SAPOPC_HISTORYPATH	Path to the `r3monal` history file
SAPOPC_R3MONAL_CONFIGFILE	Name of the `r3monal` configuration file
SAPOPC_SAPDIR	The Windows drive where SAP R/3 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 3-3. 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 29.

Table 3-3 r3monal File

File Name	Description
`r3monal(.exe)`	Executable for the SAP R/3 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 26. Note that SAP System and SAP Number are only required by `r3monal`.

Example 3-4 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.

Example 3-5 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 Levels” 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 OVO 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 68. For more information about the SPI for SAP configuration files in general, see “The SPI for SAP Monitor-Configuration File” on page 29.

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 OVO messages to a specific SAP System ID and SAP Number. Example 3-6 shows the default settings for severity levels in the `r3monal.cfg` file.

Example 3-6 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) 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 CCMS severity levels are mapped to OVO severity levels**

   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
   ```

Example 3-7 Excerpt from the r3monal Configuration File

```
# A Monitor Set defines the messages you want to forward to OVO.
#--------------------------------------------------------------------------
# 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 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 10.01, 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).

Example 3-8 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 74.

r3monal: Alert Classes

In the alert-classes section of the `r3monal.cfg` file, you define how the monitor should filter syslog events in the SAP System to extract and display only those 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 Example 3-9 on page 74, `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.

Example 3-9 Syslog events in the r3monal.cfg file

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

NOTE 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 R/3 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 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.

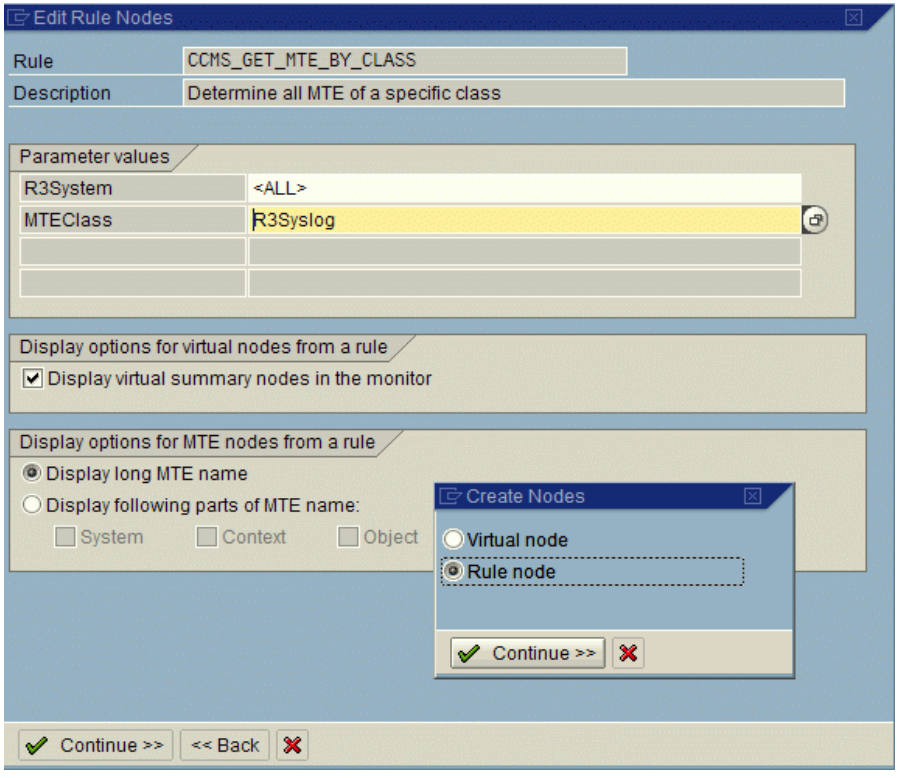
4. Set up the system-log filters

   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 AlertMonSysLog 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 3-5 on page 76 shows you how the CCMS rule node for SAP syslog elements should look when you complete the configuration successfully.

Figure 3-5 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 109.

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 113.

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 OVO message browser.

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 116.

r3monal: Testing the Configuration

The SPI for SAP's optional test transport includes a program that you can use to generate an ABAP dump in order to verify that the `r3monal` monitor checks the syslog and sends a message to OVO if a dump occurs in the SAP System. If the test completes successfully, a message about the test dump appears in the OVO message browser. Note that this test works only if you have configured `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 OVO managed node; for more information about importing and applying SPI for SAP transports, see the *HP OpenView Smart Plug-in for SAP Installation 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/
- **AIX:** /usr/sap/<*SID*>/<*InstanceNumber*>/work/
- **Win**: <*drive*:>\usr\sap\<SID>\<*InstanceNumber*>\work

Messages generated by this monitor include an operated-initiated action, which calls the vi editor. vi then displays a list of all trace files and log files and prompts you to select a file from the list and display its contents.

This section contains information about the following topics:

- "r3mondev: File Locations" on page 79
- "r3mondev: Environment Variables" on page 80
- "r3mondev: Monitoring Conditions" on page 80
- "r3mondev: Editing the Configuration File" on page 81

r3mondev: File Locations

The file monitor, r3mondev, includes the files listed in Table 3-4. 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 29

Table 3-4 r3mondev Files

File	Description
r3mondev(.exe)	Executable for the file monitor
r3mondev.cfg	Configuration file for monitored files

Table 3-4 r3mondev Files (Continued)

File	Description
r3mondev.his	History file that stores data for each monitor run

r3mondev: Environment Variables

The file monitor uses environment variables listed in Table 3-5.

Table 3-5 r3mondev Environment Variables

Environment Variable	Description
SAPOPC_DRIVE	The Windows drive where the OVO 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 MS Windows drive where SAP R/3 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 R/3.

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 60.

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      MsgGroup
AlertDevMon     =ALL   =ALL      =1      =dev_*   =WARNING  =r3mondev  =R3_Trace
AlertDevMon     =ALL   =ALL      =1      =std*    =CRITICAL =r3mondev  =R3_Trace
```

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_Trace
  ```

- **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
  ```

NOTE 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 3-6. 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 29

Table 3-6 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 3-7.

Table 3-7 r3monpro Environment Variables

Environment Variable	Description
SAPOPC_DRIVE	The MS Windows drive where the OVO 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 MS Windows drive where SAP R/3 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 60.

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 OVO object `saposcol`. The associated OVO 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 OVO object `dw.sap` and OVO 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_State
AlertInstMonPro  =C01 =00  =explorer  =1 =Max  =1 =CRITICAL =explorer =R3_State
AlertInstMonPro  =T11 =00  =dw.sapSID =1 =Min  =8 =WARNING  =dw.sap   =R3_State
```

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.

NOTE

On servers running the HP-UX or Linux operating systems, `r3monpro` can identify processes at the instance level. On servers running the MS 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 or Linux 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:

- Example 3-10 on page 86

  Monitoring SAP-Gateway Read Processes per SAP SID

- Example 3-11 on page 86

  Monitoring SAP-Gateway Read Processes per SAP Instance

Example 3-10 on page 86 shows how to configure r3monpro to monitor the individual gwrd processes associated with specific SIDs on a SAP server hosting multiple SAP SIDs.

Example 3-10 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
```

Example 3-11 on page 86 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.

Example 3-11 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 R/3 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 R/3 function module RFC_SYSTEM_INFO, the `r3status` monitor provides the following features:

- Reports about local SAP R/3 system-availability
- Recognition and monitoring of each individual SAP R/3 instance
- SAP R/3 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 128.

NOTE

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 91.

This section contains information about the following topics:

r3status: File Locations

Table 3-8 lists the files used by the `r3status` monitor.

Table 3-8 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 OVO 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 89.

r3status: Environment Variables

Table 3-9 lists the environment variables used by the `r3status` monitor.

Table 3-9 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]

Table 3-9 r3status Environment Variables (Continued)

Environment Variable	Description
SAPOPC_R3STATUS_CONFIGFILE	Name of the configuration file, which the `r3status` monitor uses
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 89

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 OVO 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 29.

Note that the `r3status` monitor does not add entries to the `r3status.his` history file each time it runs: it only writes to the file if it discovers that a change of status has taken place. In addition, if a change of status has occurred, `r3status` overwrites the existing information in the history file with the latest available status information, which includes a timestamp indicating when the change of status was discovered.

The information in the `r3status.his` history file reflects the last *change* in status of the SAP instances, which you are managing with the SPI for SAP. If the most recent run of the `r3status` monitor discovers that no change in status has occurred since the last time it ran, it does not update the information in the `r3status.his` file. Example 3-12 shows the format and contents of the `r3status.his` file.

Example 3-12 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. Example 3-13 on page 93 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 29:

- **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 message browser 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 DisableMonitorWithSeverity 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 103.

  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 92.

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* OVO managed nodes) from a host, which *is* already configured as an OVO 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. Example 3-13 on page 93 shows how a new line is required for each *additional* SAP server, which you want to monitor remotely.

NOTE You can associate multiple remote SAP servers with one, single local host or you can associate single remote hosts with individual, different local hosts. Example 3-13 on page 93 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 90.

Example 3-13 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 OVO 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 96
- "r3monsec: Alert Types" on page 96
- "r3monsec: Monitoring Security Remotely" on page 101

NOTE

If you use the SPI for SAP tools located in the application bank 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 143 and "Understanding Configuration-File Error Messages" on page 143.

r3monsec: File Locations

The SAP System-security monitor `r3monsec` uses the files listed in Table 3-10.

Table 3-10 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 97

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

- "r3monsec: DEFAULT_USERS" on page 99

  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 100

  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 or 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 *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.

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

“Example SAP_PARAMETERS settings” on page 97 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 OVO message group R3_Security.

Example 3-14 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 3-11 on page 98 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 message browser.

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 message browser

Table 3-11 Default Settings for SAP_PARAMETERS

Parameter	Default Value
login/failed_user_auto_unlock	0 [a]
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
login/password_max_reset_valid	2
login/password_expiration_time	30

Table 3-11 Default Settings for SAP_PARAMETERS (Continued)

Parameter	Default Value
login/disable_password_logon	0 [a]
login/disable_multi_gui_login	0 [a]
login/disable_cpic	0 [a]
login/system_client	100
login/disable_multi_rfc_login	0 [a]
rdisp/gui_auto_logout	1800

a. 0=disabled; 1=enabled

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.

Example 3-15 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.

NOTE 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 100. 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 100 shows how to exclude SAP user KWAME from the check to determine which users have permission to execute external operating-system commands.

Example 3-16 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 message browser. 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 need to add a new line for each *additional* SAP server, which you want to monitor remotely.

Example 3-17 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 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 message browser. `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 Example 3-18 on page 104, you can configure and use the `r3mondisp` monitor.

Example 3-18 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 MS 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 MS 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 106.

r3mondisp: File Locations

The SAP System-security monitor `r3mondisp` uses the files listed in Table 3-12.

Table 3-12 r3mondisp Files

File	Description
`r3mondisp(.exe)`	Executable for the ABAP Dispatcher-queue monitor

Table 3-12 r3mondisp Files (Continued)

File	Description
`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 `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 Example 3-19 on page 106. 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 message browser 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.

NOTE `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.

Example 3-19 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 39.

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. Example 3-20 on page 108 shows an excerpt from the `r3mondisp` monitor's default configuration file.

NOTE 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 29.

- **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 29.

- **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 29.

  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 39.

- **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 29.

Example 3-20 on page 108 shows how to configure `r3mondisp` to send a warning message to the message browser 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.

Example 3-20 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
```

Example 3-20 on page 108 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 39.

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. Example 3-21 on page 109 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 OVO

Example 3-21 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 Example 3-21 on page 109 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 OVO management server after the installation of the SPI for SAP bits:

`/opt/OV/lbin/sapspi/trans/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.

  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 message browser.

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 OpenView Smart Plug-in for SAP Installation Guide*.

- **SPI for SAP Monitors**

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

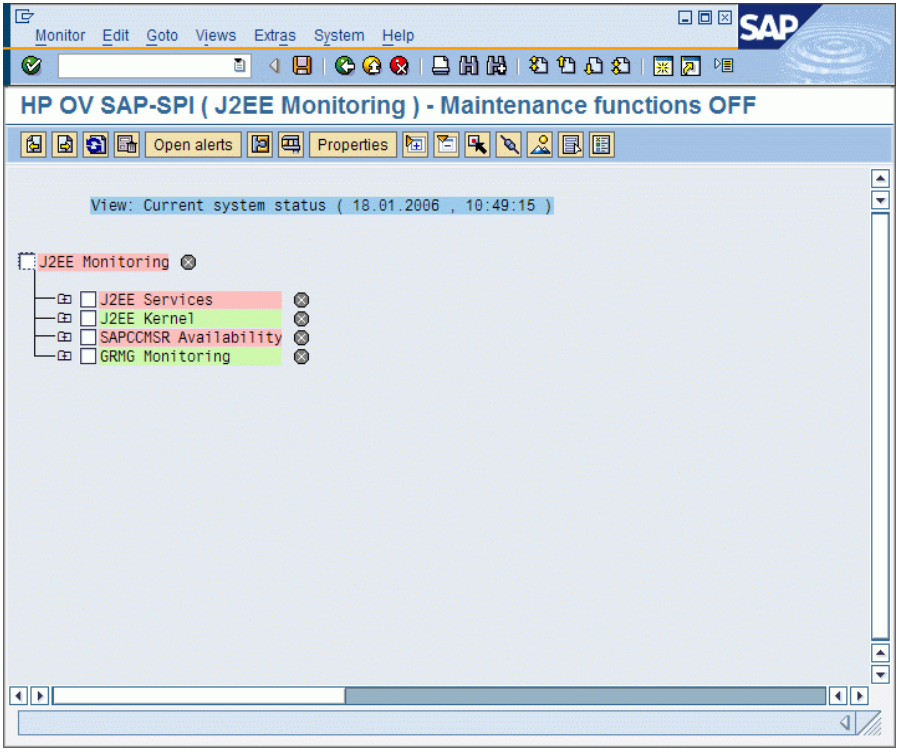
Configuring the SPI for SAP J2EE Monitor

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 109.
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 Figure 3-6 on page 112. For more information about which CCMS alerts you need to enable for J2EE, see "J2EE Monitor: Enabling CCMS Alerts" on page 109.

Figure 3-6 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 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 OVO message browser when problems occur that require urgent attention. This section contains information about the following topics:

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`. Example 3-22 on page 113 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 OVO

Example 3-22 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 OpenView Smart Plug-in for SAP Installation Guide*.

- **CCMS Agents**

  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**

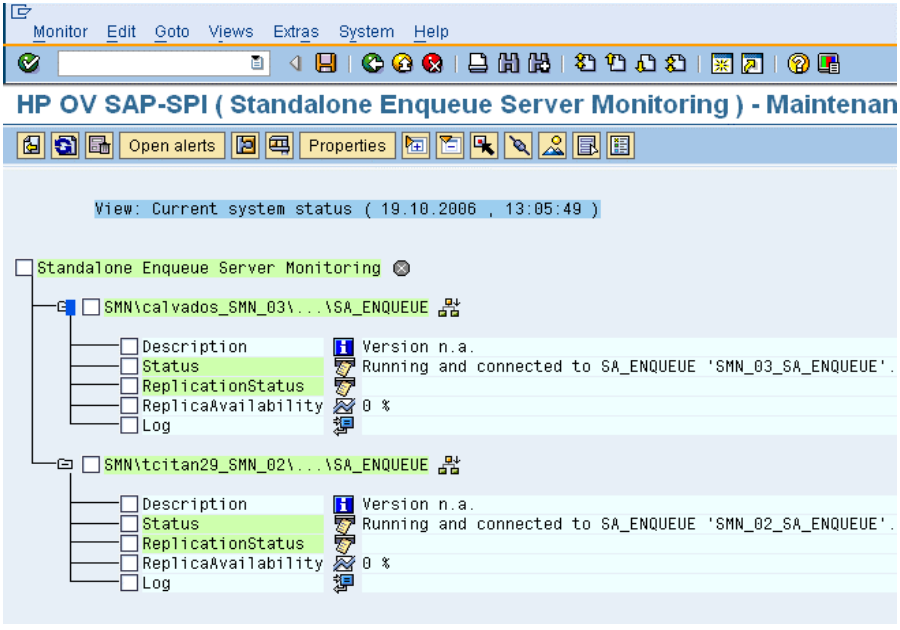
  The SPI for SAP monitors and their configuration files must be available for distribution to the SAP Systems, whose stand-alone enqueue server you want to monitor.

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 is configured to run 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 Monitor as illustrated in "Monitoring Enqueue Alerts in CCMS" on page 113.
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 3-7 on page 115.

Figure 3-7 **Enabling CCMS alerts for the Enqueue Server 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 116
- "Configuring the Security-Audit Monitor" on page 117

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 OVO message browser. Table 3-13 on page 117 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.

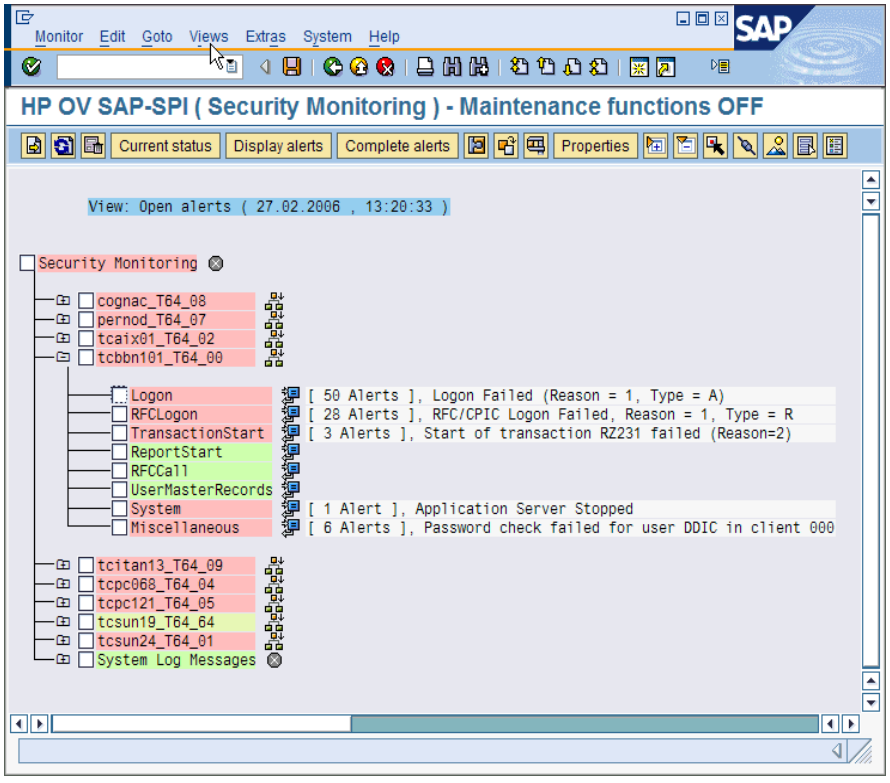
Table 3-13 SAP Security-Audit Classes

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 OVO; 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 3-8 on page 118 shows what the CCMS monitor tree looks like when you complete the configuration on the SAP side successfully.

Figure 3-8 **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 118
2. “Configuring the SAP Security Audit” on page 119
3. “Enabling CCMS Security Monitoring” on page 120

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, 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 116.

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.

NOTE 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.

NOTE 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.

NOTE

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, 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.

Example 3-23 on page 121 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".

Example 3-23 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 63.

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 R/3 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 128
- "The Alert-Collector Monitor Configuration Files" on page 138

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 239

  To save runtime costs, a report now replaces the Temporary Sequential File (TEMSE) monitor. See "Monitoring the TemSe file" on page 239 for more details.

- "r3monale: The iDOC-Status Monitor" on page 149

  The IDOC Status monitor checks the status of the iDOCs present in the SAP R/3 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 159

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

- "r3moncts: The Correction & Transport System Monitor" on page 165

  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 178

  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 181

  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 193

  The LOCK_CHECK monitor references the SAP R/3 Enqueue process which manages logical locks for SAP R/3 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 196

  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

NOTE 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 200

  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 204

  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 209

  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 219

  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 222

  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 225

  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 R/3, for example; checks on SAP R/3 processing modes, SAP R/3 dumps, or the availability of SAP R/3 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. This section covers the following topics:

For more information about the contents of the individual alert-collector monitor configuration files, see "The Alert-Collector Monitor Configuration Files" on page 138.

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. For more information about the default polling rates for alert-collector monitors, see Table 4-1, which shows the rates in days, hours, and minutes.

Table 4-1 Default Polling Rates for Alert-Collector Monitors

Alert-Monitor Name	Polling Rate		
	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 239.

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 OVO management server has already been notified about and whether to generate further messages or not.

Note that in versions up to and including SPI for SAP A.08.x, the alert collector `r3moncol` used shared memory to determine the status of any given SAP instances and wrote the information to the history file, `r3monup.his`. In later versions of the product, the `r3status` monitor provides a more convenient and, by means of a wider range of statuses, a more accurate way to determine the status of the SAP instances, which the SPI for SAP is monitoring.

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 R/3 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 R/3 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 OVO 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 4-2)

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 OVO message browser.
- 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 4-2, 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 4-2 Description of Parameter Delimiters

Parameter Delimiters	Description
SIGN	**I**: Inclusive **E**: Exclusive
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 4-3.

Table 4-3 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:

  1. Within each specified configuration between:

     a. the general alert class configuration (SAP hostname, system, number and client)

b. the OVO configurations (severity level, object and message group)

c. the monitoring query conditions (parameter name and the SIGN, OPT, LOW and HIGH parameter delimiters).

2. 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 4-4 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 R/3 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 4-5 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* OVO managed nodes) from an SAP server, which *is* already configured as an OVO managed node.

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

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 OpenView Smart Plug-in for SAP Installation 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. Example 4-2 on page 142 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 OVO 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 OVO managed node.

For more information about the contents of the alert-collector monitor configuration file, see "The Alert-Collector Monitor Configuration Files" on page 138.

Example 4-1 on page 137 shows a hypothetical example of how to configure the SPI for SAP on two different OVO 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 Example 4-1 is the *production* system, it has the monitor enabled (=1) and associates the OVO message severity CRITICAL with alerts generated by the =REQUEST_CREATED alert type.

- **Development System**

  The remote server `ovsdsap2` in Example 4-1 is the *development* system, it has the monitor enabled (=1) and associates the OVO message severity MAJOR with alerts generated by the =REQUEST_CREATED alert type.

- **Test System**

  The remote server `ovsdsap3` in Example 4-1 is the test system whose configuration is unchanged from the default which has the monitor disabled (=0) and associates the OVO message severity WARNING with alerts generated by the =REQUEST_CREATED alert type.

Example 4-1 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. Example 4-2 on page 142 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 143:

- **TraceLevel**

  For more information, see "The SPI for SAP Monitor-Configuration File" on page 29.

- **TraceFile**

  For more information, see "The SPI for SAP Monitor-Configuration File" on page 29.

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

  For more information, see "The SPI for SAP Monitor-Configuration File" on page 29.

- **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 135.

- **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*> For more information about the values an alert-collector monitor accepts, see the alert types section for a given monitor, for example; "r3monale: The iDOC-Status Monitor" on page 149 refers to the alert type "IDOC_CURRENT_STATUS".

  — **AlertMonitor**:

  =<*Monitor_Name*>

  where <*Monitor_Name*> is 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**:

  =<*OVO_Msg_Severity*>

  where <*OVO_Msg_Severity*> is the severity level of the OVO message you want to map the CCMS alert to, for example: Normal, Warning, Major, Critical.

— **OPC Object**:

=*<OpC_Object>* where *<OpC_Object>* is the OVO 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 OVO 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**:

=*<OVO_Msg_Group>*

where *<OVO_Msg_Group>* is the name of the OVO 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 OVO 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>* where *RFC_Param* is 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 130. For more information about monitor- specific alert-type parameters, see the

monitor descriptions. For example, for the `r3moncts` alert type REQUEST_CREATED, see: Table 4-16, "REQUEST_CREATED Configuration Parameters," on page 169.

— **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 OVO. For example, SAP alerts with the severity level *SeverityCritical* are mapped by default to the OVO message severity *Critical*. The OVO-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.

Example 4-2 Example 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          Server      Remotely
# Monitoring      Node        monitored Node
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 "Example Default Configuration for the CTS Monitor (r3moncts)" on page 142. 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.

NOTE

The SPI for SAP checks the contents of an alert-collector's configuration file only if you use OVO for UNIX tools 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 vi text 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 128.

Understanding Configuration-File Error Messages

If you use OVO for UNIX tools 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 29.

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:

1. `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.

2. `No value found for the parameter Enable/Disable in command AlertMonFun; setting to '0'`

   The command AlertMonFun is incomplete; an expected parameter to define enabling (=1) or disabling (=0) is missing. Assume disable (=0), which is the default.

   OVO for UNIX only. This is a warning, not an error, so the configuration file can be saved.

3. `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).

4. `Enable/Disable for the command AlertMonFun is not set; setting to '0'`

   The enable/disable parameter in the command AlertMonFun is missing or incorrectly defined; the default value of 0 (disabled) is assumed and set.

   OVO for UNIX only. This is a warning, not an error, so the configuration file can be saved.

5. `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).

6. `Argument for <command_name> must be a valid number`

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

7. `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.

8. `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.

9. `Value for Disable/Enable in command DPQueueCheck must be either '0' or '1'; setting to '0' (disable)`

   The enable/disable parameter for the command DPQueueCheck is missing or incorrectly defined; the default value of 0 (disabled) is assumed and set.

   OVO for UNIX only. This is a warning, not an error, so the configuration file can be saved.

10. `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).

11. `<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.

12. `<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).

13. `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”.

14. `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.

15. `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.

16. `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.

17. `<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.

18. `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.

19. `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.

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

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

21. `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.

22. `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.

23. `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.

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

    The *HP OpenView Smart Plug-in for SAP Administrator's Reference* describes the contents of each monitor's configuration file in great detail.

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

The *HP OpenView Smart Plug-in for SAP Administrator's Reference* describes the contents of each monitor's configuration file in great detail.

26. `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.

27. `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.

28. `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>`.

29. `Note: The character '*' in LOW parameter of OPTION 'EQ' will be interpreted literally; that is as '*' and NOT as a wildcard.`

    The asterisk character will be interpreted as the asterisk character and not as a wild card in the context of the EQ (equals) option.

30. `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 R/3 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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

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 in Table 4-6.

Table 4-6 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 130.

Environment Variables

The `r3monale` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3monale` monitor uses the command-line parameters described in Table 4-5 on page 135. 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 4-5 on page 135.

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 135.

NOTE

The remainder of this section describes the specific configuration requirements for the `r3monale` alert monitor. "Alert-Collector Monitor Query Conditions" on page 130 describes general configuration query rules which apply to all alert collector monitors. If you use OVO for UNIX tools 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 4-7. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 4-2 on page 132.

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 4-7 on page 151 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 4-7 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:	‘ ‘
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	‘ ‘

Table 4-7 IDOC_CURRENT_STATUS Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
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 4-7 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 Example 4-3, 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 4-2 on page 132.

Example 4-3 Example 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 R/3 or a range of statuses defined in a group. Table 4-8 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 Example 4-3 with the iDOC status number listed in Table 4-8 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 4-8 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		✓

Table 4-8 Possible iDOC Status (Continued)

iDOC Status	Description	Check Inbound	Check Outbound
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		
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		

Table 4-8 Possible iDOC Status (Continued)

iDOC Status	Description	Check Inbound	Check Outbound
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		

Table 4-8 Possible iDOC Status (Continued)

iDOC Status	Description	Check Inbound	Check Outbound
39	IDoc is in the receiving system (ALE service)		
40	Application document not created in receiving system		
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)	✓	

Table 4-8 Possible iDOC Status (Continued)

iDOC Status	Description	Check Inbound	Check Outbound
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		
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. The alert monitor `r3monchg` references the SAP R/3 transactions **`SE06`**.

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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

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 Table 4-9.

Table 4-9 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 130.

Environment Variables

The `r3monchg` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3monchg` monitor uses the command line parameters described in Table 4-5 on page 135. 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 4-5 on page 135.

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 135.

NOTE

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 130.

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 4-10.

Table 4-10 Comparing Include and Exclude Conditions for the Same Parameter

Select Options	Alert Type: CHANGE_OPT (SAP R/3 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 4-11 on page 162 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 4-2 on page 132.

Table 4-11 CHANGE_OPT Configuration Parameters (SAP R/3 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 [a]	PATCH
		= High:	
NSP_EDTFLAG	Flag indicating which specified name space(s) to set to ON.	= Sign: I	I
		= Opt: EQ, CP	CP
		= Low [b]	*
		= High:	
SWC_EDTFLAG	Flag indicating which specified software components to set to ON.	= Sign: I	I
		= Opt: EQ, CP	CP
		= Low: <specified software component> [b]	*
		= High:	

a. PATCH=set to patch system
b. See list of name space change options for SAP R/3 4.6. X in Table 4-13

In Example 4-4, 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).

Example 4-4 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  =
```

Example 4-5 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 Example 4-5, 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 4-12 and Table 4-13.

Table 4-12 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 4-13 Name System Change Options for SAP R/3 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
/SAPRRR/	Ready-to-Run R/3
/SAPSMOSS/	Interface: R/3 messages to the SAP Online Service Sy
/SAPTRAIN/	SAP training

r3moncts: The Correction & Transport System Monitor

The 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` references:

- transport requests and object lists created using SAP R/3 transaction **`SE01`**
- tasks created using SAP R/3 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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

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 Table 4-14.

Table 4-14 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 130.

Environment Variables

The `r3moncts` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3moncts` monitor uses the command line parameters described in Table 4-5 on page 135. 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 4-5 on page 135.

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 135.

NOTE 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 130.

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 4-15.

Table 4-15 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

Table 4-15 TRFUNCTION Request Functions (Continued)

Letter Code	Function Description
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

NOTE 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 4-15.

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. Table 4-16 on page 169 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 4-2 on page 132.

Table 4-16 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 R/3 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 Example 4-6, the monitor generates a message if a new request occurs within the last time frame.

Example 4-6 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 4-17 on page 170 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 4-2 on page 132.

Table 4-17 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. [a]	
		= 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	

Table 4-17 REQUEST_RELEASED Configuration Parameters (Continued)

Parameter Name	Description	Query Conditions	Default Value
USERNAME	The login name of the SAP R/3 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 [b]	
		= High	
WORKBENCH	Workbench Requests	= Sign I, E	
		= Opt: EQ	
		= Low [b]	
		= High	

a. You can only specify the listed functions (* means all).
b. Any entry other than 'X' will be treated as space.

In Example 4-7, an event generating an alert occurs if any *customizing* request was released in the last time frame.

Example 4-7 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 4-18 on page 172 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 4-2 on page 132.

Table 4-18 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 R/3 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 Example 4-8, `r3moncts` generates a message for any new task *created* within the last specified time frame.

Example 4-8 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 4-19 on page 173 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 4-2 on page 132.

Table 4-19 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 R/3 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 Example 4-9, `r3moncts` generates a message for any new task *released* in the last time frame.

Example 4-9 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 4-20 on page 174 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 4-2 on page 132.

Table 4-20 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	

Table 4-20 OBJECT_USED Configuration Parameters (Continued)

Parameter Name	Description	Query Conditions	Default Value
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 Example 4-10, an event generating an alert occurs if any object with Object Type "LIMU" is used by a task or a request.

Example 4-10 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 4-21 on page 176 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 4-2 on page 132.

Table 4-21 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 [a]	
		= High	

Table 4-21 OBJECT_RELEASED Configuration Parameters (Continued)

Parameter Name	Description	Query Conditions	Default Value
IN_TASK	Alert generated if object container is a task.	= Sign I, E	
		= Opt: EQ	
		= Low [a]	
		= High	

a. Any entry other than 'X' will be treated as space.

In Example 4-11, an event generating an alert occurs if any object is released by a task.

Example 4-11 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 R/3 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 R/3 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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

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 Table 4-22.

Table 4-22 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 130.

Environment Variables

The `r3mondmp` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3mondmp` monitor uses the command line parameters described in Table 4-5 on page 135. 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 4-5 on page 135.

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 135.

NOTE

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 130.

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. Example 4-12 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.

Example 4-12 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 you can use to generate an ABAP dump in order to verify that the `r3mondmp` monitor correctly reports dumps to OVO in the form of a message. If the test completes successfully, a message about the test dump appears in the OVO message browser. For more information about SPI for SAP transports, see the transports read-me file `/usr/sap/trans/readme` on the OVO managed node; for more information about importing and applying SPI for SAP transports, see the *HP OpenView Smart Plug-in for SAP Installation 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.

NOTE 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 R/3 transaction **`SM36`** or **`SM38`**
- Job details including ID number using SAP R/3 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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

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:

- 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 4-2 on page 132.

The runtime cost of a job selection grows in the order shown in Table 4-23.

Table 4-23 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 Table 4-24

Table 4-24 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 130.

Environment Variables

The `r3monjob` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3monjob` monitor uses the command-line parameters described in Table 4-5 on page 135. 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 4-5 on page 135.

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." 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 135.

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.

IMPORTANT

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 4-25.

Table 4-25 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 4-26 on page 186 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 4-26 on page 186 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 4-2 on page 132.

Table 4-26 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 [a]	
MAX_RUNTIME	Job run time in minutes which, if exceeded, generates an alert.	= Sign I, E	I
		= Opt: EQ, GE, GT, BT	GT
		= Low [b]	5
		= High [a]	

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_MAX_RUN_TIME alert type.

In Example 4-13, an event generating an alert occurs if any report named <*jobname*>* has a runtime exceeding five minutes.

Example 4-13 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 Example 4-14, an event generating an alert occurs if all reports named SAP*, except reports SAPZ*, have a runtime exceeding ten minutes

Example 4-14 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 OVO 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 OVO message browser. For more information about SPI for SAP transports, see the transports read-me file `/usr/sap/trans/readme` on the OVO managed node; for more information about importing and applying SPI for SAP transports, see the *HP OpenView Smart Plug-in for SAP Installation 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 4-27 on page 188 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 4-2 on page 132.

Table 4-27 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 Example 4-15, an event generating an alert occurs if any report named <*jobname*>* has a runtime of less than one minute.

Example 4-15 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 Example 4-16, an event generating an alert occurs if all reports named SAP*, except reports SAPZ*, have a runtime of less than two minutes

Example 4-16 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 OVO 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 OVO message browser. For more information about SPI for SAP transports, see the transports read-me file `/usr/sap/trans/readme` on the OVO managed node; for more information about importing and applying SPI for SAP transports, see the *HP OpenView Smart Plug-in for SAP Installation 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 4-28 on page 190 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 4-2 on page 132.

Table 4-28 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 Example 4-17, an event generating an alert occurs if any report named <*jobname*>* does not start more than one minute after the scheduled start time.

Example 4-17 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. Table 4-29 on page 191 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 4-2 on page 132.

Table 4-29 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 Example 4-18, an event generating an alert occurs if any report named <*jobname*>* aborts.

Example 4-18 The Default JOB_ABORTED Configuration

```
AlertMonFun   =ALL =ALL =ALL  =ALL  =JOBREPORT =1\
=WARNING   =Aborted      =R3_Jobs \
=JOB_ABORTED  =JOBNAME  =I  =CP= <jobname>*
```

In Example 4-19, an event generating an alert occurs if jobs named SAP_REORG_ABAPDUMPS or ITOTEST are aborted.

Example 4-19 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 OVO if a job aborts. For more information about SPI for SAP transports, see the transports read-me file `/usr/sap/trans/readme` on the OVO managed node; for more information about importing and applying SPI for SAP transports, see the *HP OpenView Smart Plug-in for SAP Installation 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 R/3 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 R/3 system - this is the most common cause of locked objects.
- An entire SAP instance fails.

The alert monitor `r3monlck` references the SAP R/3 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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

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 Table 4-30.

Table 4-30 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 130.

Environment Variables

The `r3monlck` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3monlck` monitor uses the command-line parameters described in Table 4-5 on page 135. 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 4-5 on page 135.

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 135.

NOTE 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 130.

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 4-31 on page 195 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 4-2 on page 132.

Table 4-31 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 Example 4-20, an event generating an alert occurs if any lock exceeds a time span of 24 hours.

Example 4-20 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 R/3 transaction **SM63**
- Configuration modes in SAP R/3 transaction **RZ04**

NOTE 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 R/3 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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

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 Table 4-32

Table 4-32 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 130.

Environment Variables

The `r3monoms` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3monoms` monitor uses the command-line parameters described in Table 4-5 on page 135. 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 4-5 on page 135.

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 135.

NOTE

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 130.

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 4-33 on page 199 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 4-33 on page 199 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 R/3 central instance whose application server(s) you want to specify with APSERVER, as illustrated in the Example 4-21.

Example 4-21 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 Example 4-21 on page 198 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 4-2 on page 132.

Table 4-33 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	
		= 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. This query condition is mandatory; if it is not present, the monitor does not perform any check.
b. Only for use when specifying a range.

In Example 4-22, an event generating an alert occurs if a scheduled operation mode switch is more than three minutes late.

Example 4-22 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 R/3 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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

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 Table 4-34.

Table 4-34 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 130.

Environment Variables

The `r3monrfc` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3monrfc` monitor uses the command-line parameters described in Table 4-5 on page 135. 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 4-5 on page 135.

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 135.

NOTE

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 130.

Limitations

It is not possible to configure `r3monrfc` to monitor the following RFC destinations, even though they are listed in SAP transaction SM59:

- HTTP Connection to External Server
- HTTP Connection to R/3 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 number of reconnect errors to the target system exceeds a defined threshold. Table 4-35 on page 202 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 4-2 on page 132.

Table 4-35 CHECK Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
CONNECTION_TYPE	Type of SAP RFC connection to monitor. Type 1= App. Server, Type 3= R/3 System, Type M= CMC, Type T =TCP/IP.	= 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 Example 4-23, an event generating an alert occurs whenever the RFC_DESTINATION test fails for any *one* of the type 3 SAP-RFC destinations.

Example 4-23 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 Example 4-24, an event generating an alert occurs whenever RFC_DESTINATION test fails for the single SAP-RFC destination named OV_C01_099.

Example 4-24 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.
- If a specified printer has received erroneous spool requests.

The alert monitor `r3monspl` references output tasks in SAP R/3 transaction **`SP01`** and report sources in SAP R/3 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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

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 Table 4-36.

Table 4-36 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 130.

Environment Variables

The `r3monspl` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3monspl` monitor uses the command line parameters described in Table 4-5 on page 135. 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 4-5 on page 135.

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 135.

NOTE

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 130.

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 4-37 on page 206 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 4-2 on page 132.

Table 4-37 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 Example 4-25, an event generating an alert occurs if there are more than 50 spooler entries.

Example 4-25 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 4-38 on page 207 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 4-2 on page 132.

Table 4-38 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 Example 4-26, an event generating an alert occurs if there are more than 50 erroneous spool requests.

Example 4-26 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 4-39 on page 208 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 4-2 on page 132.

Table 4-39 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 Example 4-27, `r3monspl` generates an alert if any printer has a spool entry-state error.

Example 4-27 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 and failed exports and imports for the monitored system
- confirmed and unconfirmed repairs in the monitored system.
- connections using a connection test (PING) to the configured systems
- TP-Tests of the configured systems.

The alert monitor `r3montra` references transport routes in SAP R/3 transactions **`STMS`** and **`SE01`**.

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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

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 Table 4-40.

Table 4-40 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 130.

Environment Variables

The `r3montra` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3montra` monitor uses the command-line parameters described in Table 4-5 on page 135. 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 4-5 on page 135.

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 135.

NOTE 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 130.

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 4-41 on page 212 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 4-2 on page 132.

Table 4-41 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	
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:	

Table 4-41 TRANS Configuration Parameters (Continued)

Parameter Name	Description	query conditions	Default Value
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 R/3 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 Example 4-28, 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.

Example 4-28 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 4-42 on page 214 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 4-2 on page 132.

Table 4-42 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	

Table 4-42 REPAIR Configuration Parameters (Continued)

Parameter Name	Description	Query Conditions	Default Value
R_UNCONFIR	Filtering option to include all unconfirmed repairs.	= Sign: I, E	I
		= Opt:	EQ
		= Low [a]	X
		= High	
USERNAME	The login name of the SAP R/3 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 Example 4-29, 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.

Example 4-29 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 4-43 on page 216 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 4-2 on page 132.

Table 4-43 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 Example 4-30, an event generating an alert occurs if the alert threshold of four RFC-connect errors is exceeded for the specified target system.

Example 4-30 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 4-44 on page 217 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 4-2 on page 132.

Table 4-44 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	

Table 4-44 TPTEST Configuration Parameters (Continued)

Parameter Name	Description	Query Conditions	Default Value
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 Example 4-31, an event generating an alert occurs if the alert threshold of four TPTEST errors is exceeded for the specified target system.

Example 4-31 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 R/3 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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

Alert Types

The update monitor has the following alert types.

- "UPDATE_ACTIVE"

  This is used to get information about the status of update processes and sends an alert if a process is not active.

- "UPDATE_ERRORS_EXIST"

  This is used to get information on update processes which have errors.

File Locations

The `r3monupd` monitor uses the files listed in Table 4-45.

Table 4-45 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 130.

Environment Variables

The `r3monupd` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3monupd` monitor uses the command-line parameters described in Table 4-5 on page 135. 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 4-5 on page 135.

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 135.

NOTE

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 130.

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 Example 4-32, an event generating an alert occurs if any update is stopped.

Example 4-32 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 Example 4-33, an event generating an alert occurs if any update error occurs.

Example 4-33 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 R/3 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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

Alert Types

The SAP-user monitor has only one alert type:

- "USER_LOGGEDIN_MAX"

  This is used to define the maximum number of logged in users.

File Locations

The `r3monusr` monitor uses the files listed in Table 4-46.

Table 4-46 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 130.

Environment Variables

The `r3monusr` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3monusr` monitor uses the command-line parameters described in Table 4-5 on page 135. 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 4-5 on page 135.

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 135.

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 4-47 on page 224 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 R/3 central instance whose application server(s) you want to specify with APSERVER, as illustrated in the Example 4-34.

Example 4-34 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 130. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 4-2 on page 132.

Table 4-47 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	
		= 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 Example 4-35, an event generating an alert occurs if the number of users logged in exceeds thirty.

Example 4-35 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 R/3 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 77.

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 143 and "Understanding Configuration-File Error Messages" on page 143.

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 128.

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 Table 4-48.

Table 4-48 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 130.

Environment Variables

The `r3monwpa` monitor uses the environment variables described in Table 4-4 on page 134. 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 4-4 on page 134.

Command-Line Parameters

The `r3monwpa` monitor uses the command-line parameters described in Table 4-5 on page 135. 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 4-5 on page 135

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 135.

NOTE

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 130.

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 4-49.

Table 4-49 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 4-50 on page 229 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 R/3 central instance whose application server(s) you want to specify with APSERVER, as illustrated in the Example 4-36.

Example 4-36 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 130. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 4-2 on page 132.

Table 4-50 WP_AVAILABLE Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
APSERVER	specifies an application server to monitor	= Sign: I, E	
		= Opt: CP	
		= Low	
		= 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:	

Table 4-50 WP_AVAILABLE Configuration Parameters (Continued)

Parameter Name	Description	Query Conditions	Default Value
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:	
UPD	Threshold for update work processes	= Sign: I, E	
		= Opt: GT, GE, LT, LE	
		= Low <number>	
		= High	

Table 4-50 WP_AVAILABLE Configuration Parameters (Continued)

Parameter Name	Description	Query Conditions	Default Value
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 Example 4-37, an event generating an alert occurs if the number of available Dialog work processes is less than fifty.

Example 4-37 The Default WP_AVAILABLE Configuration

```
AlertMonFun   =ALL   =ALL  =ALL  =ALL =WP  =1\
=WARNING   =Availability  =R3_WP\
=WP_AVAILABLE    =DIA   =I    =LT  =50   =
```

NOTE 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 Example 4-37 on page 231, 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 235.

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 4-51 on page 233 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 R/3 central instance whose application server(s) you want to specify with APSERVER, as illustrated in the Example 4-38.

Example 4-38 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 130. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 4-2 on page 132.

Table 4-51 WP_IDLE Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
APSERVER	specifies an application server to monitor	= Sign: I, E	
		= Opt: CP	
		= Low	
		= 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 4-51 WP_IDLE Configuration Parameters (Continued)

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 Example 4-39, an event generating an alert occurs if the number of idle Dialog work processes is less than ten.

Example 4-39 The Default WP_IDLE Configuration

```
AlertMonFun    =ALL =ALL =ALL   =ALL =WP =1\
=WARNING    =Idle   =R3_WP\
=WP_IDLE  =DIA =I  =LT =10  =
```

NOTE 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 Example 4-39 on page 234, 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 235.

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 4-52 on page 236 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 R/3 central instance whose application server(s) you want to specify with APSERVER, as illustrated in the Example 4-40.

Example 4-40 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 130. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 4-2 on page 132.

Table 4-52 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	
		= High	

In Example 4-41, `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.

Example 4-41 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 R/3 central instance whose application server(s) you want to specify with APSERVER, as illustrated in the Example 4-42.

Example 4-42 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 130. For more information about the meaning of the query conditions in the alert-collector monitor configuration files, see Table 4-2 on page 132.

Table 4-53 Configuration Parameters

Parameter Name	Description	Query Conditions	Default Value
APSERVER	Specifies an application server to monitor	= Sign: I, E	
		= Opt: CP	
		= Low	
		= 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 Example 4-43, an event generating an alert occurs if the status of a running workprocess is *critical*. Example 4-43 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.

Example 4-43 The Default WP_STATUS Configuration

```
AlertMonFun     =ALL =ALL =ALL  =ALL =WP   =1\
                =CRITICAL   =WP_Status  =R3_WP\
                =WP_STATUS     =STATUS =I  =CP  =*   =
# New feature in SPI for SAP Version 8.0
```

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 128.

Report Description

The TemSe report references the SAP R/3 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 R/3 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 R/3
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 OVO functionality and CCMS to control the flow of messages between SAP R/3 and OVO.

In this Section

The information in this section describes how to control message flow between SAP R/3 and OVO and includes the following topics:

- "OVO Message Customization" on page 243

  Customize OVO message template conditions.

- "Customizing CCMS Message Flow in SAP R/3" on page 247

  Use SAP R/3 features to control how CCMS alert monitors generate specific messages.

- "SAP Solution-Manager Integration" on page 253

  Use the `r3ovo2ccms` command to write OVO 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 OVO.

NOTE

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 R/3.

For details on the procedures outlined in these sections, refer to your SAP R/3 documentation and to the manuals supplied with OVO.

OVO Message Customization

With the aid of standard OVO 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 the view message browser 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 Views” on page 243.

- **Changing severity levels**

  change the severity level of messages. For more information, see “Changing the Message Severity” on page 245.

- **Suppressing messages**

  suppress specific messages by setting a suppress condition in the `opcmsg` template. For more information, see *HP OpenView Smart Plug-in for SAP Installation Guide*.

Setting Up the Message Views

The `View Message Browser` window is your own customized presentation of a selection of the messages displayed in your message browser. The message browser displays every message belonging to the managed nodes and message groups assigned to you: the `View Message Browser` window displays only the messages you actually want to see.

In this way, you can configure the view so that only the most important messages are displayed and, as a consequence, concentrate on messages needing immediate attention.

Use the `Browser View` window to specify which messages are displayed in the view message browser. You can set up simple or complex views, select specific messages to be displayed, or define a filter to display only a subset of the incoming messages. For example, if you want to display messages with a severity level of critical, you can specify that messages of all other severity levels are not displayed.

To view all messages belonging to a node and a particular group, first use the view message browser to view all of the messages on the specified node. Then use the view message browser again to narrow the view down to only the messages from the specified group.

To define your customized message-browser view:

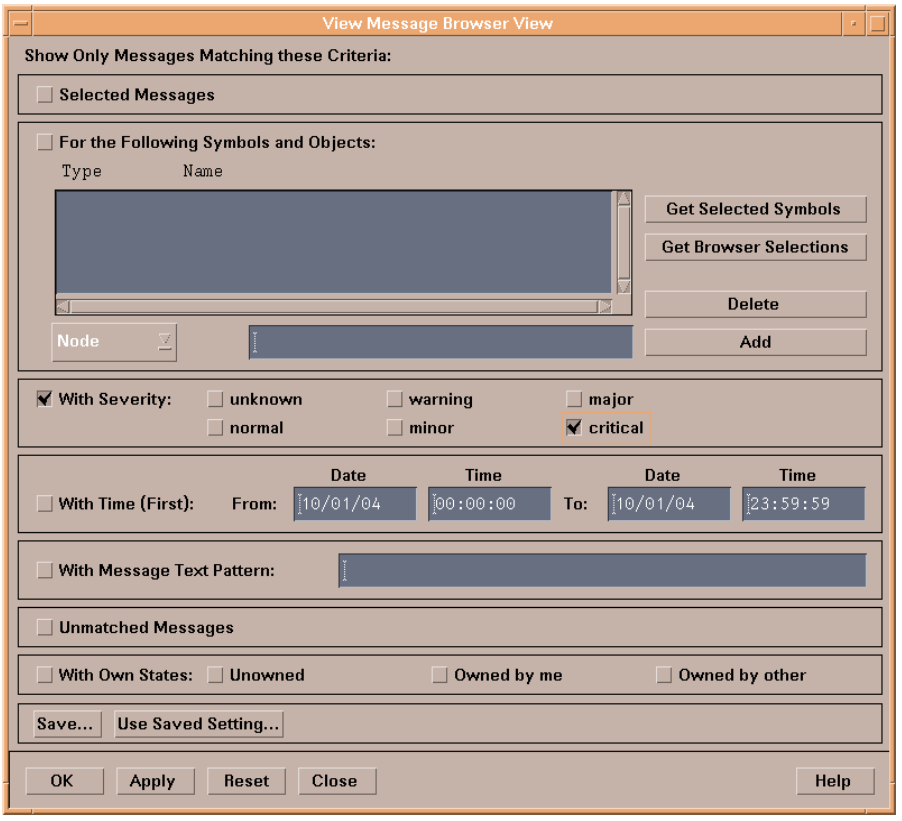
1. On the menu bar at the top of the `Message Browser` window, click `View` to display the `View` pull-down menu.
2. From the `View` pull-down menu, select `Some` to display the `Browser View` window illustrated in Figure 5-1 on page 245.
3. Define the filtering patterns to be used.

   For example, if you click the `Critical` button, all messages other than those marked `Critical` are not displayed in the `Message Browser` window.
4. Click `[OK]` to implement your filtering pattern(s).

NOTE

If a critical event occurs on one of your managed nodes after you have defined a new message-browser view, the `Message Groups` window is immediately moved into the foreground.

Figure 5-1 **Browser View Window**



Changing the Message Severity

To change the severity of specific SAP R/3-generated messages in the message browser:

1. Log on to OVO as user `opc_adm`.
2. Select the following menu items from the menu bar of the `Node Bank` window:

   `Actions > Configure Messages > Logfiles, Console, Trap...`

3. OVO displays a list of message-source templates. From this list, select `SAP R/3 opcmsg`.
4. Display the message conditions window to change the severity level of a specific message. See your OVO documentation for details.

5. Distribute the changed message configuration to the applicable SAP nodes. See your OVO documentation for details.

Customizing CCMS Message Flow in SAP R/3

SAP R/3 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 R/3:

1. Select the following items from the SAP R/3 menu bar:

   ```
   Tools > Administration > Computing Center >
   Management System > Control > Control Panel
   ```

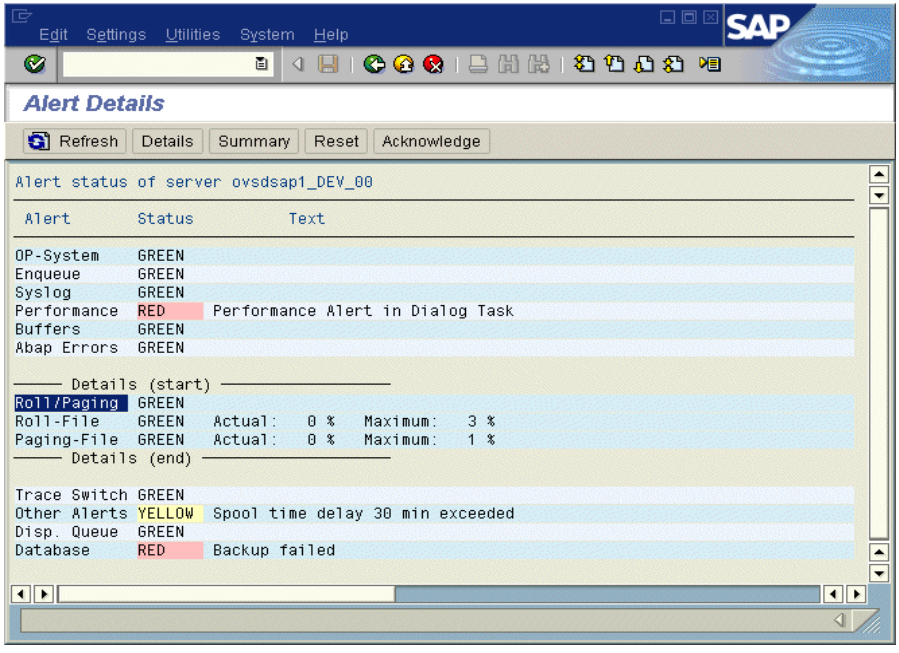
NOTE Alternatively, you can enter the following transaction code into the SAP R/3 command field: `RZ03`

2. Select your SAP R/3 instance.
3. Select the following menu items from the SAP R/3 menu bar:

   ```
   Monitoring > Alert-Details
   ```

4. Click `Roll/Paging` in the `Type` column.

Figure 5-2 Alert State window



5. Proceed as follows to disable, for example, Roll/Paging alerts:
   a. Click `Roll/Paging`
   b. From the R/3 menu bar, select the following menu items:

      `Settings > Disable`

      The selected item and the suppressed message type are now marked as “disabled” in the SAP GUI.
6. Return to the `CCMS Control Station` window and save your settings.
7. Check the OVO message browser. You should not receive any more Roll/Paging messages.

NOTE 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 R/3 CCMS Alert Monitor Messages

To set thresholds for SAP R/3 CCMS alert monitor messages:

1. Select the following items from the SAP R/3 menu bar:

   `Tools > Administration > Computing Center > Management System > Control > Control Panel`

2. Select the SAP R/3 instance (under `Server name`) for which you want to define a performance limit value.
3. Click `Alert details`
4. From the SAP R/3 menu bar, select the following menu items:

   `Settings > Threshold values`

   The Alert Thresholds window appears.

5. Click `Performance` to display the Performance Alerts Thresholds window
6. Edit the time threshold values as appropriate
7. To save your new thresholds, select the following items from the SAP R/3 menu bar:

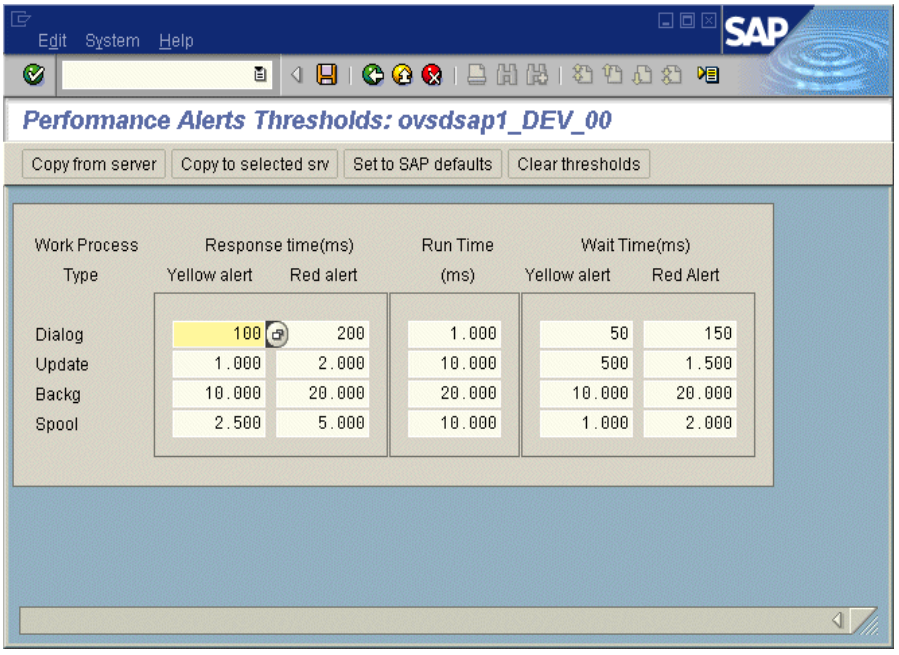
   `Edit > Save`

   When the limit you just defined is reached, you will receive a warning or a critical `Dialog performance` message (similar to Figure 5-3).

NOTE This example assumes that you want to set a specific performance limit that will trigger a related dialog-performance message.

To initialize your SAP R/3 CCMS before you have empirical data for thresholds, it may be a good idea to apply the SAP defaults by clicking `Set to SAP defaults` in the `Alert Thresholds` window.

Figure 5-3 **Performance Alert Thresholds**



Setting Up Messages for Inclusion in the SAP R/3 System Log File

Any messages recorded in the SAP R/3 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 OVO message browser with instructions for any appropriate actions, which are required.

To set up messages for inclusion in the SAP R/3 system log file, perform each of the following procedures in sequence:

- “Obtaining a Message ID from the SAP R/3 Syslog File” on page 251
- “Configuring the System Log Filter for Alert Generation” on page 251

Obtaining a Message ID from the SAP R/3 Syslog File

To obtain the message ID of a critical message:

1. Select the following menu items from the SAP R/3 menu bar to read the system log file:

   `Tools > Administration > Monitoring > System Log`

NOTE

Alternatively, you can enter the following transaction code into the SAP R/3 command field: `SM21`

SAP R/3 displays the Local Analysis window.

It may be a good idea to select appropriate time restrictions to limit the contents of the `syslog` file to the currently relevant entries.

2. Click `Refresh SysLog` to display the system log file of your SAP R/3 system.
3. Double-click the message that you want to use to trigger an alert. The system displays a `Message Details` window.
4. Look for and make note of the message ID.

   To display the ID numbers of all SAP R/3 syslog messages, enter the transaction code `SE92` into the SAP R/3 command field and click `List all numbers`.

Configuring the System Log Filter for Alert Generation

1. Select the following menu items from the SAP R/3 menu bar:

   `Tools > Administration > Computing Center > Management System > Control > Control panel`

   The system displays the CCMS control station panel.

2. Select your SAP R/3 instance.
3. Click `Alert details`.
4. Select the following menu items from the SAP R/3 menu bar:

   `Settings > Threshold values`

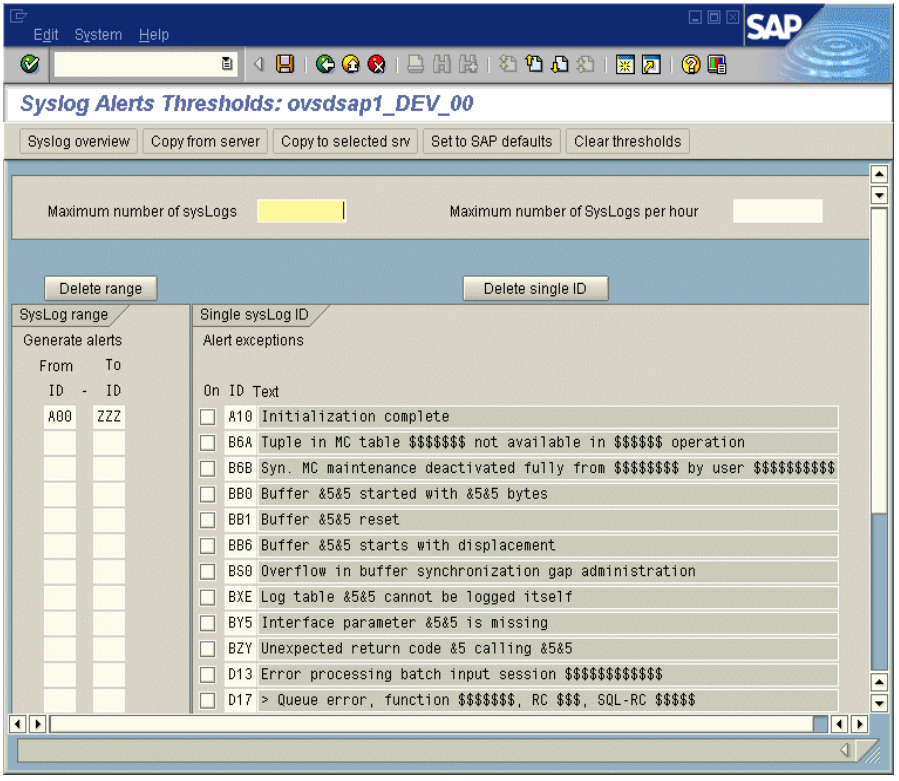
5. Click `Syslog`. The SAP system displays the `Syslog Alert Thresholds` window.

   In the `Syslog Alerts` window shown, you can see that all messages—ranging from A00 through ZZZ—are *enabled*. This implies that these messages are able to generate an alert if they occur in the Syslog. All `Single Syslog ID` messages (shown on the right) are *disabled*. If you want to enable any of these currently disabled messages, click `[ON]` to the left of the message ID field (for instance, BB1).

6. To save your new settings, select the following items from the SAP R/3 menu bar:

   `Edit > Save`

Figure 5-4 Syslog Alert Thresholds



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 OVO. With the SPI for SAP's Solution-Manager integration, you can configure the SPI for SAP to inform OVO 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 OpenView managed objects, for example; by means of an automatic or operator-initiated action attached to a message condition in a template. 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:

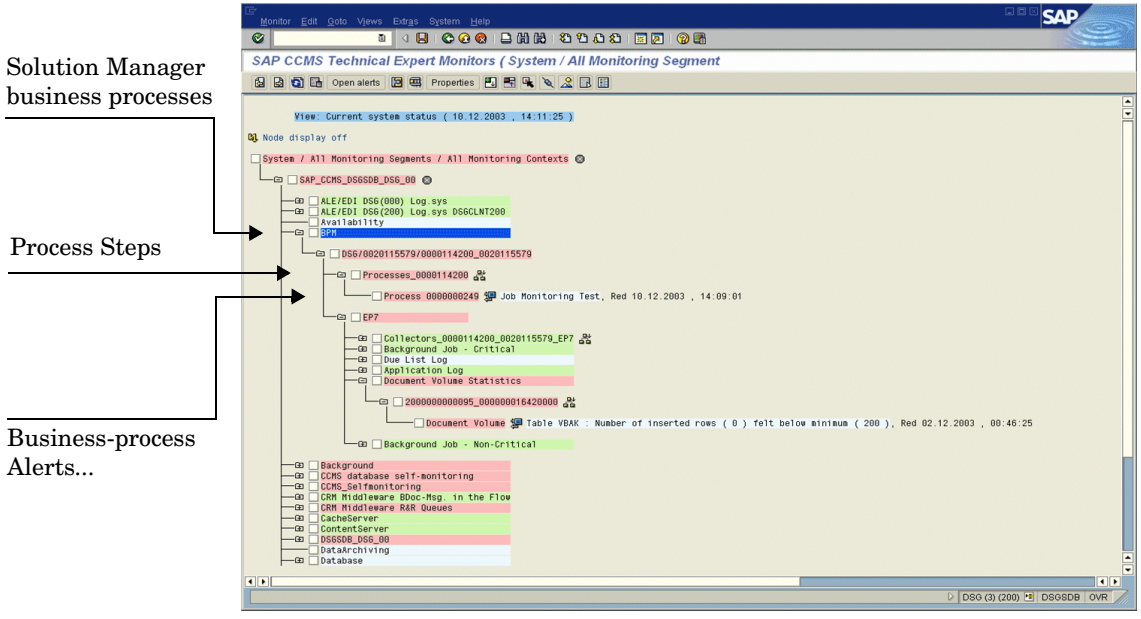
Support package 29 is required for full support of the BC-XMW interface. According to SAP, earlier SP levels will work, but the XMW interface designation will not be recognized.

- 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 OVO. Using the CCMS interfaces, the SPI for SAP ensures that the power of both SAP and OVO can be used to enhance and improve the information available to system administrators in both areas.

Figure 5-5 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 OVO and relate to problems not normally of particular interest to SAP, such as hardware and network performance. Conversely, Figure 5-5 on page 254 shows how you can use the Solution-manager integration to monitor specific CCMS alerts and, by linking the

generated OVO messages to a defined service ID, monitor the status of specific services. In this way, you cannot only ensure that OVO 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 OpenView Navigator.

To summarize how the SPI for SAP's Solution-manager integration enhances communication in both directions between SAP and OVO:

- **SAP -> OVO**

  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 OVO" on page 255.

- **OVO -> SAP**

  You can attach an action to an OVO message condition, which calls the `r3ovo2ccms` command and uses it to populate the CCMS tree with messages and objects monitored by OVO. For more information about using the `r3ovo2ccms` command, see "The r3ovo2ccms Command" on page 260.

Sending Messages from SAP to OVO

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 OVOmessage the condition generates with a known Service ID and, in this way, link the message directly to a service in the OVO service tree. For more information about setting up `r3monal`, the CCMS alert monitor, see "r3monal: the CCMS 4.x Alert Monitor" on page 62.

To set up communication between the SAP Solution Manager and OVO

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.

NOTE 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 OVO.
4. If you want to link the OVO messages to services in OVO, 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)distribute the SPI for SAP `opcmsg` template with the new (or modified) conditions.

Sending Messages from OVO to SAP

The first and most important thing you need to do is to inform OVO which of the incoming OVO 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 template condition, 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 260.

To set up an automatic action in an OVO template, follow the instructions below. Note that the names and titles of the windows can sometimes vary according to the type of template you select. The example described here uses a performance-threshold policy.

1. Open the `Message-source Templates` window, using the following menu option:

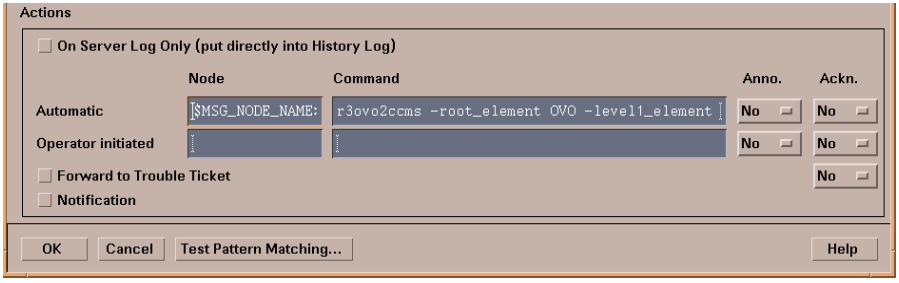
   `Window > Message Source Templates`

2. Locate and double-click the template which generates the OVO message you want to forward to SAP and write into the CCMS tree. For example, you might choose a message from a performance monitor, which is configured to monitor CPU load on the SAP server.
3. In the `Message and Suppress Conditions` window, locate and double-click the condition, which generates the message you want to forward to SAP. Note that not all messages need to be forwarded. For example, the rules which generate a critical message are probably of more interest than the rules which generate messages with severity level “warning” or “normal”.
4. In the `Actions` field of the `Condition No.` 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, it is created for you when the message is forwarded to SAP. Note that the default name of the root element for OpenView in the CCMS monitor tree is ZSAPSPI.

   Note too that, providing you have not modified the default settings, you do not need to supply an absolute path with the command. On MS Windows nodes, you do not need the `.exe` file extension, either. For more information about the `r3ovo2ccms` command, see “The r3ovo2ccms Command” on page 260.

   The `Node` field defines the name of the node where the template you are modifying is assigned and the `r3ovo2ccms` command runs. If you use the $MSG_NODE_NAME variable in conjunction with the -host option in the Command field, the SPI for SAP assumes the name of the node associated with the original message. Assuming the remote-monitoring feature is enabled, this is true even for nodes, which the SPI for SAP is monitoring remotely.

Figure 5-6 Configuring an Automatic Action



5. 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, browse to the following transaction:

      `Change Mode: Setup Business Process Monitoring`

   b. Select the process step to which you want to assign the CCMS alert for OpenView

   c. Manually enter the name of the OpenView CCMS monitor element, which you want to assign to the business-process step.

NOTE

The name of the monitor that you enter must match the entry created by the `r3ovo2ccms` command as it appears in the CCMS 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, for example; OpenView.

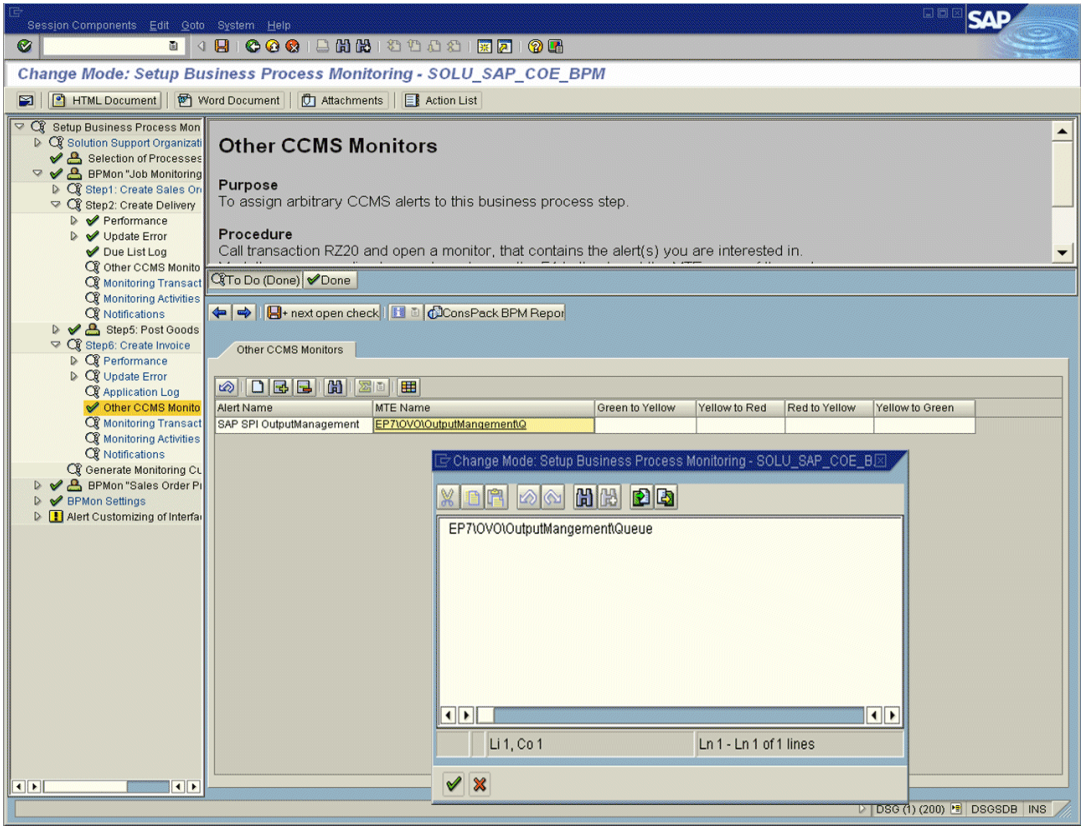
6. Next, you need to create a CCMS monitor set, for example; OpenView, and generate a CCMS monitor, for example; SAPSPI, to host the OpenView alerts sent by the `r3ovo2ccms` command. Remember to use only ASCII characters when defining the name of a CCMS monitor set; the SPI for SAP cannot currently interpret non-ASCII characters in monitor-set names.

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) in order to make them visible to the Solution Manager. Scroll down the list of contexts displayed and select “ZSAPSPI”.

NOTE

The context ZSAPSPI is only visible for selection in the list of contexts displayed *after* the first OVO message sent by the `r3ovo2ccms` command appears in the CCMS tree. “The r3ovo2ccms Command” on page 260 explains how to use the `r3ovo2ccms` command to send a dummy message to CCMS, which creates the ZSAPSPI context.

Figure 5-7 Assigning CCMS MTEs to Business Process Steps



The r3ovo2ccms Command

The mechanism which the SPI for SAP uses to forward OVO messages to SAP and write them directly into the CCMS tree is the `r3ovo2ccms` command, which the SPI for SAP installs in the default OVO actions directory on the OVO 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 template that generates an OVO message, which you want to forward to CCMS. The SPI for SAP uses the configured action to forward the OVO 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 OVO.

Parameter Options The following options can be used with the `r3ovo2ccms` command parameters:

`-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 OVO.

`-number <SAP_instance_number>`

The instance number of the SAP System, where the original event/problem was detected by OVO.

`-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 OVO message relating to a problem with CPU load on the SAP server “mezcal” and write it directly into a defined location in the CCMS tree. You can configure the OVO template 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.

Example 5-1 Writing OVO Messages into the CCMS Tree

```
r3ovo2ccms -root_element OVO -level1_element Performance
-level2_element CPU -text "CPU load: bottleneck situation
90%" -host mezcal
```

In the example above, the OVO message will appear in the `OVO > 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, “mezcal”.

6 The SPI for SAP Performance Monitors

This section describes in detail how to install, set up, and use the SPI for SAP performance monitor and its features.

In this Section

The information in this section describes how to install and configure 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 OpenView Performance Agent. The section includes the following topics:

Performance Monitors Overview

The SPI for SAP performance subagent (SAP/Performance subagent) uses a selection of performance monitors to collect SAP R/3 performance data and store them either in the OVO Embedded Performance Component (CODA) or the Performance Agent (Unix/MS 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 informatFion about the following topics:

- Performance monitoring with the SPI for SAP
- How to use OVO to install the SAP/Performance subagent
- The performance monitors and how to configure them

Implemented ABAP-function modules inside SAP R/3 are accessed by means of an RFC-call. The performanceF 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 R/3 Performance alert monitor (`ST03`), which is part of the SAP R/3 CCMS subsystem.

You can configure the SAP/Performance subagent to specify which monitors should be run on specified SAP R/3 instances and how frequently. For more information, see "Configuring the SAP/Performance Subagent" on page 279.

The Performance Agent runs in MS Windows operating systems as a service and in UNIX operating systems as a daemon (background) process that runs independently of the OVO agent processes. To start or stop the SAP/Performance subagent processes, use the appropriate OVO application in the `OVO Application Bank` window. For more information, see "Managing the SAP/Performance Subagent" on page 295.

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 you can continue to use all existing data and data sources. If you are using an older version such as A.08.50 or A.08.71, 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 very old version of the SAP/Performance subagent such as A.08.10 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 323.

2. **Remove existing SAP/Performance subagent data and data sources**

   - SPI for SAP A.09.x

     If you are upgrading from version A.09.x 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 A.08.50 or A.08.71

     If you are upgrading from versions A.08.50 or A.08.71 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 A.08.10 or earlier

  If you are upgrading from version A.08.10 or earlier of the SPI for SAP, see "Migrating the SAP/Performance subagent with the OpenView Performance Agent" on page 267 or "Upgrading the SAP/Performance subagent with CODA" on page 270 for more information about cleaning up old data sources.

3. **Upgrade the SPI for SAP**

   For more information, refer to the *HP OpenView Smart Plug-in for SAP Installation 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 273.

5. **Configure the new SAP/Performance subagent**

   For more information about installing the SAP/Performance subagent, see "Configuring the SAP/Performance Subagent" on page 279.

6. **Upgrade the SPI for SAP/OV Reporter Integration**

   For more information about upgrading the SPI for SAP Reporter integration, see "Upgrading the SPI for SAP Reports" on page 375.

Migrating the SAP/Performance subagent with the OpenView Performance Agent

If you are using the OpenView Performance Agent as your performance data source and want to upgrade the SAP/Performance subagent from the previous to the most recent version, it is extremely important that you 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, as follows:

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

- MS 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 323.

3. **Clean up data sources**

   If you are upgrading from versions A.08.71or 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 and locates and updates the old data to the new format for you. For more information, see "To Configure the SAP/Performance Subagent" on page 281.

   If you are upgrading from version A.08.10 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 OVO 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:

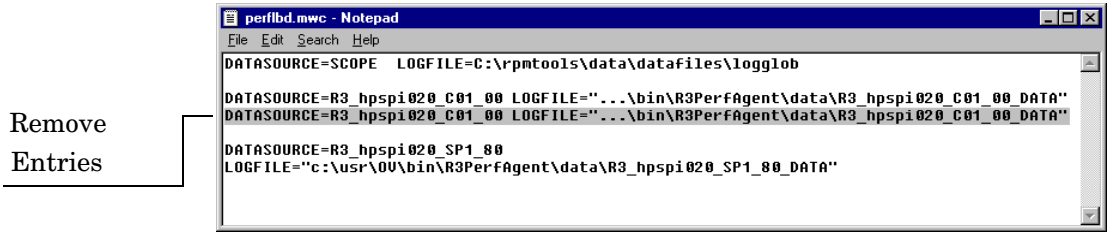
        `/var/opt/perf/data/perflbd.rc`

      - MS 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 6-1 on page 269. Entries in the `perflbd` file relating to the SAP/Performance subagent start with: `DATASOURCE=R3_*`.

Figure 6-1 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`

- MS 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 OpenView Smart Plug-in for SAP Installation Guide*.

5. **Install the new version of the SPI for SAP**

   Install the new version of the SPI for SAP on the OVO management server. For more information, see “Installing the SPI for SAP” in the *HP OpenView Smart Plug-in for SAP Installation 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 273.

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 279.

   Note that after finishing the migration described here, you do not need to execute steps 1 and 2 specified in "To Configure the SAP/Performance Subagent" on page 281. 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 OVO Embedded Performance Component (CODA) as your performance data source and want to upgrade the SAP/Performance subagent from the previous to the most recent version, it is extremely important that you 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, as follows:

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 323.

2. **Clean up SAP/Performance subagent data sources**

   If you are upgrading from version A.08.71 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 and locates and updates the old data to the new format for you. For more information, see "To Configure the SAP/Performance Subagent" on page 281.

   If you are upgrading from version A.08.10 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`

- MS 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 6-2 on page 272. 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:

```
# ddfutil \
%OvDataDir%\bin\r3perfagent\data\R3_MARTI_WA4_00_DATA \
-rm all
```

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 “Deinstalling the SPI for SAP” in the *HP OpenView Smart Plug-in for SAP Installation Guide*.

4. **Install the new version of the SPI for SAP**

   Install the new version of the SPI for SAP on the OVO management server. From more information, see “Installing the SPI for SAP” in the *HP OpenView Smart Plug-in for SAP Installation Guide*.

5. **Install the new SPI for SAP SAP/Performance subagent**

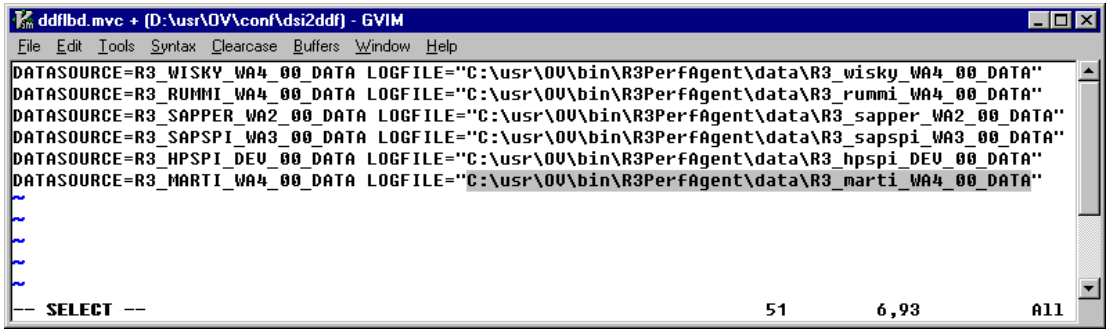
   Install the new version of the SAP/Performance subagent as described in “Installing the SAP/Performance Subagent” on page 273.

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 279.

Note that after finishing the migration described here, you do not need to execute steps 1 and 2 specified in “To Configure the SAP/Performance Subagent” on page 281. You can proceed directly to step 3 and adapt the configuration file before starting the SAP/Performance subagent in steps 4 and 5.

Figure 6-2 The ddflbd.mwc File



Installing the SAP/Performance Subagent

This section describes how to use the OVO GUI to install the SPI for SAP functionality for the performance-agent on the SAP servers you want to manage with OVO and the SPI for SAP. Note that the instructions in this section assume the following is true:

- the OVO Agent is already installed and running on the selected SAP servers
- the `dsi2ddf` wrapper is present on the OVO management server and, in addition, you have selected the source you want the performance monitor subagent to use for performance data.

  For more information about installation pre-requisites and selecting the performance-data source, see the *HP OpenView Smart Plug-in for SAP Installation Guide*.
- Either the OpenView Performance Agent or the OVO 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 10.20, refer to the *HP OpenView Smart Plug-in for SAP Software Release Notes*.

To install the SAP/Performance Agent package:

1. **Stop the Performance Agent**

   On the node where you want to install the SAP/Performance Agent, stop the Performance Agent by entering the following command in a shell:

   - AIX operating systems:

     `/usr/lpp/perf/bin/mwa stop`
   - HP-UX/Solaris operating systems:

     `/opt/perf/bin/mwa stop`
   - MS Windows operating systems:

     `mwacmd stop`
2. **Select the Managed Nodes for subagent installation**

Start OVO and, in the `Node Bank` window, select the managed node(s) where you want to install the SAP/Performance Agent.

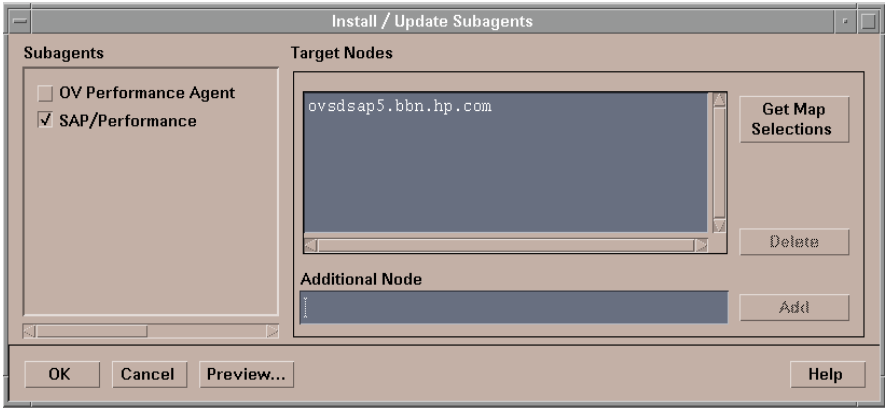
3. **Open the subagent-installation window**

   From the `Actions...` menu, select:

   `Subagents` > `Install/Update...`

   The `Install / Update Subagent` selection window is displayed.

Figure 6-3 Subagent Selection Window



4. **Select the subagent package to install**

   Select the `SAP/Performance` subagent and ensure the target nodes for installation are correct.

5. **Install the SAP/Performance subagent package**

   Click `[OK]` to start the installation of the subagent package. The OVO subagent installation writes general information and errors to `stdout`. Further information can be found in the following log files on the OVO management server:

   - `/var/opt/OV/log/OpC/mgmt_sv/product_inst.log`
   - `/var/opt/OV/log/OpC/mgmt_sv/product_inst_err.log`
   - `/var/opt/OV/log/OpC/mgmt_sv/product_inst_sum.log`

Locating the SAP/Performance Subagent Files

This section lists 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: MS Windows"

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/OV/bin/R3PerfAgent/bin`
  - `r3perfconfig`

    SPI for SAP performance-monitor configuration tool
  - `r3perfagent`

    SPI for SAP performance-monitor agent
- Configuration files:

  DCE: `/var/lpp/OV/conf/sapspi/`

  HTTPS: `/var/opt/OV/conf/sapspi/`
  - `r3perfagent.cfg`

    Configuration file for the performance monitors if you use the `Distribute Local Config` application in the `SAP R/3 Admin Local` Application group.

    If you use the `Actions: Agents > Install/Update S/W & Config...` the location is:

    `/var/opt/OV/conf/sapspi`
- `Dsilog` files: `/var/lpp/OV/bin/R3PerfAgent/data`
  - `R3_<HOSTNAME>_<SID>_...`

Immediately after installation, this directory is empty; the SPI for SAP uses the directory to store the dsi log files, which `r3perfconfig` and `compdsifile.sh` compile.

- Templates: `/var/lpp/OV/bin/R3PerfAgent/template`
  - `R3statistics.<PERF-MONITOR>`

    Files the SPI for SAP uses to compile the dsi log 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 performance monitors if you use the `Distribute Local Config` application in the `SAP R/3 Admin Local` Application group.

    If you use the `Actions: Agents > Install/Update S/W & Config...`

    `/var/opt/OV/conf/sapspi`
- `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 dsi log files, which `r3perfconfig` compiles.

- Templates: `/var/opt/OV/bin/R3PerfAgent/template`
  - `R3statistics.<PERF-MONITOR>`

    Files the SPI for SAP uses to compile the dsi log files
  - `parm.UX`

    Template for the performance-agent parameter file.

SAP/Performance Subagent Files: MS Windows

This section lists the files which the SPI for SAP installs as part of the SAP/Performance subagent package for MS 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 MS Windows
- Configuration files: `%OVDATADIR%\conf\sapspi\`
  - `r3perfagent.cfg`

    Configuration file for the various performance monitors.
- Dsi log 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 dsi log files, which `r3perfconfig.bat` and `compdsifile.bat` compile.
- Templates: `%OVDATADIR%\bin\r3perfagent\template`
  - `R3statistics.<PERF-MONITOR>`

    Files the SPI for SAP uses to compile the dsi log 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, and covers the following topics:

Selecting the Performance-data Source

The OVO Embedded Performance Component is, as the name suggests, embedded in the OVO software and available, by default, in any OVO for UNIX installation. However, you can use the OVO GUI to deploy the OpenView Performance Agent (previously MeasureWare) to the managed nodes, too. Note that OVO Smart Plug-ins use the OpenView Performance Agent as the default source for the performance data required for graphing in HP OpenView Performance Manager and OpenView Reporter. If both performance agents are installed on a managed node, then you have to tell the SPI for SAP which performance agent it should use for the collection of performance data so that it knows where and in what format to write the performance data it collects with its own performance monitors. Note that previously installed OpenView products that use the OpenView Performance Agent will continue to use Performance Agent as the data source.

The information in this section explains what to do if you are using the OVO Embedded Performance Component as the data source on the managed node and wish to switch to the Performance Agent. You can override the use of the OVO Embedded Performance Component by setting up a small text file, `nocoda.opt`, which changes the data source from CODA to the Performance Agent.

After you configure the `nocoda.opt` file, you must store it in a specific location on each managed node, whose performance-data source you want to change. The location of the `nocoda.opt` file on the managed node

varies according to the operating system running on the OVO management server and managed node. Table 6-1 shows the location of the `nocoda.opt` file on nodes managed by an OVO management server.

Table 6-1 OVO 7.0 for UNIX Management Servers

Managed-Node Operating System	Location of the nocoda.opt File
AIX	`/var/lpp/OV/conf/dsi2ddf/nocoda.opt`
HP-UX / Solaris	`/var/opt/OV/conf/dsi2ddf/nocoda.opt`
Windows	`%OVDATADIR%\conf\dsi2ddf\nocoda.opt`

To change the default setting for the data source, open the `nocoda.opt` file in a text editor and manually enter the appropriate information using the format and syntax illustrated in Example 6-1.

To change the performance-data source:

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 Example 6-1.

2. **Specify a generic data source**

   To designate the Performance Agent as the agent for all data sources, enter the key word ALL at the top of the file.

3. **Specify individual data sources**

   To designate Performance Agent as the agent for a data source tied to a specific SAP R/3 (or SAP R/3 ITS) instance, include a reference to each instance on a separate line of the `nocoda.opt` file, as shown in Example 6-1 and using the following format:

   `R3_<`*`Virtual_SAPITS_Instance_Name`*`>_<`*`SAPITS_Hostname`*`>_DATA`

4. **Save the changes to the nocoda.opt file**

   Save the changes to the `nocoda.opt` file

5. **Restart the OVO agent**

   Restart the OVO agent on the managed node where the `nocoda.opt` file has been modified.

Example 6-1 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
```

To Configure the SAP/Performance Subagent

You need to complete the following steps to configure the SAP/Performance subagent:

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:

   - MS 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 R/3 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 performance agent

- no

  leaves the existing data source unchanged: the old data source *cannot* be used with the new version of the SPI for SAP performance agent

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 B.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.

When you are finished, the data sources are created and added to the following file, which differs according to whether you are using OpenView Performance Agent or the OVO Embedded Performance Component:

- MS 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**

IMPORTANT

This step does not apply to the OVO 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`

- MS Windows operating systems:

  `type parm.NT >> parm.mwc`

  The `parm.mwc` file is located in the following directory: `<drive_letter>\rpmtools\data\parm.mwc`

NOTE

You can represent several SAP R/3 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:** `/var/opt/OV/bin/OpC/monitor/`

     Global SAP/performance subagent settings for *all* SAP R/3 managed nodes

   - **Local:** `/var/opt/OV/share/conf/sapspi/local/<hostname>`

     Local SAP/performance subagent settings for *individual* SAP R/3 managed nodes, where <*hostname*> is the name of the SAP R/3 server, to which the local configuration pertains.

To open the `r3perfagent.cfg` file double-click the `PerfAgt` icon in the `SAP R/3 Admin` application group.

NOTE

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 Performance Agents to upload the latest configurations.

4. **Start the performance agent**

   Start the performance agent on the managed node by entering the following command in a shell:

   - UNIX operating systems: **`mwa start`**
   - MS Windows operating systems: **`mwacmd start`**

5. **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]`

   - MS Windows operating systems:

     `r3perfagent_service [-e | -s]`

   Or, alternatively, in the OVO GUI, use the following SPI for SAP application

- UNIX operating systems:

  ```
  SAP R/3 UN*X > PerfAgt Start
  ```

- MS Windows operating systems:

  ```
  SAP R/3 NT > PerfAgt Start
  ```

Figure 6-4 r3perfagent.cfg File Example

Configure Performance Agent Monitoring (r3perfagent.cfg)

```
#RemoteMonitoring  =sapwolf2     =ovsdsap1

#-------------------------------------------------------------
# PerfMon    SAP        SAP     SAP       SAP      RFC FUNCTION     Enable =1/       Polling Interval   Hold Connection
#          hostname   System   Number    Client                    Disable=0          (minutes)       Enable =1/Disable =0

#

# SAP SID ------------------------------------------------
# These Performance Monitors collect SID related Metrics and should therefore
# run only once per SID (either on the Central Instance, or on ONE AppServer)

PerfMon     =ALL       =ALL    =ALL       =ALL    =DBINFO_PERF          =1              =15             =0
PerfMon     =ALL       =ALL    =ALL       =ALL    =JOBREP_PERF          =1              =60             =0
PerfMon     =ALL       =ALL    =ALL       =ALL    =UPDATE_PERF          =1              =1              =0
PerfMon     =ALL       =ALL    =ALL       =ALL    =SPOOL_PERF           =1              =20             =0
PerfMon     =ALL       =ALL    =ALL       =ALL    =DOCSTAT_PERF         =1              =60             =0

# SAP AppServer ------------------------------------------
# These Performance Monitors collect AppServer related Metrics and should
# therefore run on each AppServer of interest.

PerfMon     =ALL       =ALL    =ALL       =ALL    =WP_PERF              =1              =15             =0
PerfMon     =ALL       =ALL    =ALL       =ALL    =STATRECS_PERF        =1              =1              =0
PerfMon     =ALL       =ALL    =ALL       =ALL    =WLSUM_PERF           =1              =60             =0
PerfMon     =ALL       =ALL    =ALL       =ALL    =USER_PERF            =1              =5              =0
PerfMon     =ALL       =ALL    =ALL       =ALL    =SAPBUFFER_PERF       =1              =15             =0
PerfMon     =ALL       =ALL    =ALL       =ALL    =SAPMEMORY_PERF       =1              =15             =0
PerfMon     =ALL       =ALL    =ALL       =ALL    =ICMSTAT_PERF         =1              =15             =0
```

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 OVO managed node.

NOTE

Although the remote host is not an OVO managed node, it must nonetheless be present in the OVO Node Bank. If you do not add the remote host to the OVO Node Bank, OVO 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 message browser.

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 RemoteHost. For more information about the `r3itosap.cfg` file, refer to the *HP OpenView Smart Plug-in for SAP Installation Guide*.

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 manually add (with `r3perfconfig`) an additional data source for the system you plan to monitor remotely and then enable the new RemoteMonitoring keyword (by removing the leading hash symbol "#") in the `r3perfagent.cfg` file.

On the same line in the `r3perfagent.cfg` file, tell the SPI for SAP performance agent the name of the local server which you want to perform the monitoring and, in addition, the name of the remote server, which you want to monitor. As illustrated in Example 6-2 on page 287, a new line is required for each *additional* server that you want to monitor remotely.

Note that 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 290.

Example 6-2 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

The performance agent uses an internal scheduler to ensure 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 agent 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 agent continues to run until it has completed its task. However, the scheduler tracks the progress of the performance agent 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-agent scheduler falls ten minutes behind schedule, it sends a message to the OVO management server with the warning that the scheduler is out of synchronization. If the performance-agent 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-agent scheduler and the messages it generates, see “The r3perfagent.cfg Configuration File” on page 290.

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 Example 6-2 on page 287. 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 286.

The r3perfagent.cfg Configuration File

The SPI for SAP provides a default configuration for the `r3perfagent` monitor, which 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:

  ```
  Tracefile =<HostName> =<TraceLevel>
  ```

  — **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 a trace level. Use a new line for each individual host.

  — **Trace level**:

=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 applications 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" on page 275.

- **AgentHostname**

  The AgentHostname keyword is not currently used

- **SyncBack**

  The SyncBack keyword accepts the following parameters:

  `SyncBack =<Enable|Disable> =<SyncBack Threshold>`

  — **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.

  — **Enable/Disable**

=0	Disable the scheduler synchronization
=1	Enable the scheduler synchronization. This is the default setting.

- **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 OVO object to associate with the behind-schedule message. This is the default value.

  — **OpC MsgGroup**

=R3_General	The OVO 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 OVO 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 “Remotely Monitored Node”.

— **RemoteHost**

This is the name of the *remote* SAP server you want to monitor from the SAP server defined in “Server Node”. Although the remote host does not have the SPI for SAP software installed and is *not usually* an OVO managed node, it must appear in the OVO Node Bank.

For more information, see “Remote Performance Monitoring” on page 286.

- **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 298.

— **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

The SPI for SAP SAP/Performance subagent can be controlled using command-line options, which differ according to the platform and operating system. The SPI for SAP SAP/Performance subagent can be managed either by using command-line options or the tools that are installed by the SPI for SAP. For more information, see:

- "SAP/Performance agent Command Line Syntax" on page 295
- "SAP Logins for the SAP/Performance agent" on page 296
- "SAP/Performance agent Applications" on page 297

SAP/Performance agent Command Line Syntax

The following options can be used 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`**

The following syntax can be used with the `r3perfagent` command on MS 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

The services can also be controlled from the `Services` option in the MS Windows Control Panel.

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 OVO indicating that it was unable to start as a result of authorization problems.

NOTE

Note that SAP has a security mechanism which blocks further logins from a user who has tried (and failed) 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 which 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 OVO 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 which 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 redistribute to the managed nodes.

4. **Restart the SAP/Performance agent**

   Restart the SPI for SAP SAP/Performance agent on each of the OVO managed nodes where the SAP/Performance agent is running. On each managed node, enter:

   ```
   r3perfagent start
   ```

NOTE The SPI for SAP cannot collect performance metrics during the period when the SAP/Performance agent is not running.

SAP/Performance agent Applications

Table 6-2 shows which applications are available for the SAP/Performance Agent in the appropriate SPI for SAP application group—`SAP R/3 NT` or `SAP R/3 UN*X`.

Table 6-2 Performance Agent Applications

Application 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. This means that snapshot monitors must be scheduled to run on a regular basis to create a comprehensive picture of the performance of the SAP R/3 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

- "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 its different states

- "STATRECS_PERF"

  returns the response/net times of defined transactions

- "SYSUP_PERF"

  monitors the status of the SAP R/3 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

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.

NOTE 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 monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set.

Frequency It is recommended to run the monitor once every 15 minutes.

Datasource The SAP R/3 transaction `ST04` (DB Performance Overview)

Metrics Table 6-3 shows the values in the performance table returned by the monitor.

Table 6-3 DBINFO_PERF Performance Monitor Metrics

Order	Metric Name	Description	% Value	Cumulation
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

Table 6-3 DBINFO_PERF Performance Monitor Metrics (Continued)

Order	Metric Name	Description	% Value	Cumulation
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 R/3 System that you want to monitor.

Type

The DOCSTAT_PERF monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set.

Frequency

It is recommended to run the monitor hourly.

Data Source

The SAP R/3 transaction `ST07` (quantity structure) is used as the data source for this monitor.

Metrics

Table 6-4 shows the values in the performance table returned by the DOCSTAT_PERF monitor.

Table 6-4 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

ICMSTAT_PERF

The performance monitor, ICMSTAT_PERF, monitors the status and performance of the SAP Internet Communication Manager (ICM).

Type

The ICMSTAT_PERF monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set.

Frequency

It is recommended to run the monitor approximately once every fifteen minutes or so.

Datasource

The SAP R/3 transaction `SMICM` (ICM Monitor) is used as the data source for this monitor.

Metrics

Table 6-5 shows the values in the performance table returned by the ICMSTAT_PERF monitor.

Table 6-5 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

Table 6-5 ICMSTAT_PERF Performance Monitor Metrics (Continued)

Order	Metric Name	Description
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.

Frequency

It is recommended to run the monitor between once an hour and once a day.

Datasource

The SAP R/3 transaction `SM37` (Background Job Overview) is used as the data source for this monitor.

Metrics

Table 6-6 shows the values in the performance table returned by the JOBREF_PERF monitor.

Table 6-6 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

Table 6-6 JOBREF_PERF Performance Monitor Metrics (Continued)

Order	Metric Name	Description
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 R/3 repository, programs, and database tables.

NOTE 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 *timeframe*.

Frequency It is recommended to run the monitor every fifteen minutes.

Data Source The SAPBUFFER_PERF monitor reads information from the SAP buffers transaction `ST02`.

Metrics Table 6-7 shows the values in the performance table returned by the SAPBUFFER_PERF monitor.

Table 6-7 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

Table 6-7 SAPBUFFER_PERF Performance Monitor Metrics (Continued)

Order	Metric Name	Description
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
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.

NOTE 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.

Frequency It is recommended to run the monitor every fifteen minutes.

Data source The SAPMEMORY_PERF monitor reads information from the SAP buffers transaction `ST02`.

Metrics Table 6-8 shows the values in the performance table returned by the SAPMEMORY_PERF monitor.

Table 6-8 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

Table 6-8 SAPMEMORY_PERF Performance Monitor Metrics (Continued)

Order	Metric Name	Description
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 their different states.

Type

The SPOOL_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.

Frequency

It is recommended to run the monitor once every 10 to 30 minutes.

Data Source

The SAP R/3 transaction `SP01` (Output Controller) is used to get the data part of this monitor.

Metrics

Table 6-9 shows the values in the performance table returned by the monitor.

Table 6-9 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 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.

Frequency

It is recommended you set this monitor to run once a minute.

Data Source

SAP R/3 transaction STAT (Local transaction statistics).

Metrics

Table 6-10 shows the values in the performance table returned by the monitor.

Table 6-10 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 OpenView Performance Manager.
2	SAP_RESPONSE_TIME	Time SAP takes to respond
3	SAP_NET_TIME	Net Time

Table 6-10 STATRECS_PERF Performance Monitor Metrics (Continued)

Order	Metric Name	Description
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 R/3. There are two possible configurations:

- Global from `SAP R/3 Admin`
- Local from `SAP R/3 Admin Local`

To set and upload the STATRECS_PERF configurations:

1. **Open and edit the r3perfstat.cfg configuration file**

   Open the `r3perfstat.cfg` file by double-clicking the `Statistical Records` icon from the `Application Bank`. If you select the global configuration file, the settings will be used for all nodes except for those with local configurations.

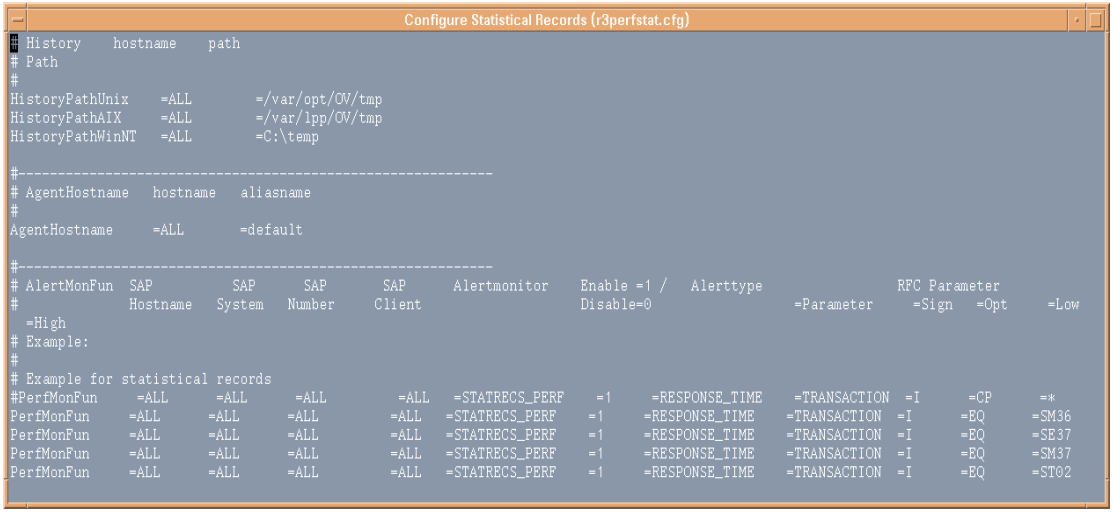
2. **Modify and save the r3perfstat.cfg configuration file**

   Change any values as required and save the file. This file is stored on the OVO management server. It must be uploaded into SAP R/3.

3. **Upload the new configuration to SAP R/3**

   To upload the configurations into SAP R/3, double-click the `.write STAT Rec Config` application, which you can find in the `SAP R/3 Admin` application group in the `Application Bank`.

Figure 6-5 Configuring Statistical Records



SYSUP_PERF

The SYSUP_PERF performance monitor is used to determine whether the SAP R/3 system is available or not.

Type

The SYSBUF_PERF monitor is of type *snapshot* and does not make use of alert types or parameters. One monitor run gathers only one value set.

Frequency

This monitor runs once a minute. The run frequency cannot be modified.

Data Source

Internal SAP RFC calls.

Metrics

Table 6-11 shows the values in the performance table returned by the monitor.

Table 6-11 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 R/3 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.

Frequency

It is recommended you set this monitor to run once a minute.

Data Source

The UPDATE_PERF monitor uses the SAP R/3 transaction `SM13` (Update Records) as its data source.

Metrics

Table 6-12 shows the values in the performance table returned by the monitor.

Table 6-12 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.

Frequency

It is recommended to run the monitor every five minutes.

Data source

The USER_PERF monitor reads information from the SAP transaction `SM04` (Overview of Users).

Metrics

Table 6-13 shows the values in the performance table returned by the USER_PERF monitor.

Table 6-13 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 monitor is mandatory; you must configure it for every application server that you want to monitor.

NOTE You can use the WLSUM_PERF performance monitor to collect data previously collected by the MIB_PERF Monitor.

Type The WLSUM_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.

Frequency Due to the way in which the performance monitor, WLSUM_PERF, measures and records time, it is *mandatory* to run the monitor hourly.

Data source The SAP R/3 transaction `ST03` (workload analysis) is used as the data source for this monitor.

Metrics Table 6-4 shows the values in the performance table returned by the WLSUM_PERF monitor.

Table 6-14 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 R/3 task (RFC, dialog)
5	CNT	The number of dialog steps
6	DBACTIVCNT	Counter for database-active dialog steps

Table 6-14 WLSUM_PERF Performance Monitor Metrics (Continued)

Order	Metric Name	Description
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
23	CHNGCNT	Number of modified database accesses
24	CHNGTI	Time for modified database accesses

Table 6-14 WLSUM_PERF Performance Monitor Metrics (Continued)

Order	Metric Name	Description
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 when, for example:

- processes need to wait for semaphores
- 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.

Frequency

It is recommended you set this monitor to run once every 15 minutes.

Data Source

The SAP R/3 transaction `SM50` (Work Process Overview) is used as the data source for this monitor.

Metrics

Table 6-15 shows the values in the performance table returned by the monitor.

Table 6-15 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

Table 6-15 WP_PERF Performance Monitor Metrics (Continued)

Order	Metric Name	Description
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 performance agent from the managed node, make sure that you *stop* the SPI for SAP performance agent, for example;
   - Use the SPI for SAP application, `PerfAgt Stop`, which resides in the `SAP R/3 UN*X` or `SAP R/3 NT` application group.
   - Use the following command as user root on the command line:

     `r3perfagent stop`
2. In the `Node Bank` window, select the managed node(s) from which the SAP/Performance agent is to be de-installed.
3. From the `Actions...` menu, select:

   `Subagents` > `Deinstall...`

   The `Deinstall Subagent` window is displayed.
4. Select the `SAP/Performance` subagent and the target nodes for de-installation.
5. Click `[OK]` to start the de-installation of the subagent package.

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:

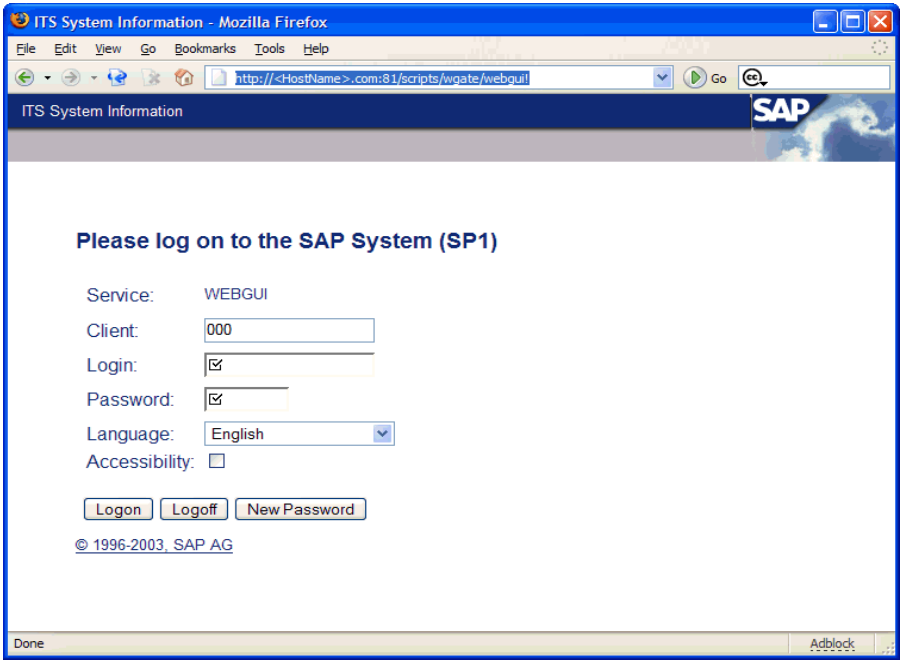
What is ITS?

The SAP **Internet Transaction Server** (ITS) provides the SAP R/3 user with an SAP R/3 transaction interface in a web browser. With this transaction interface, the SAP R/3 user can perform the following tasks:

- Use a web browser to log on to the SAP R/3 System
- Make requests for information by entering transactions directly in the SAP R/3 system
- Immediately see the results of the transaction request in a web browser by means of the transaction interface provided by ITS

NOTE The SAP ITS is only available for Linux and Microsoft Windows operating systems.

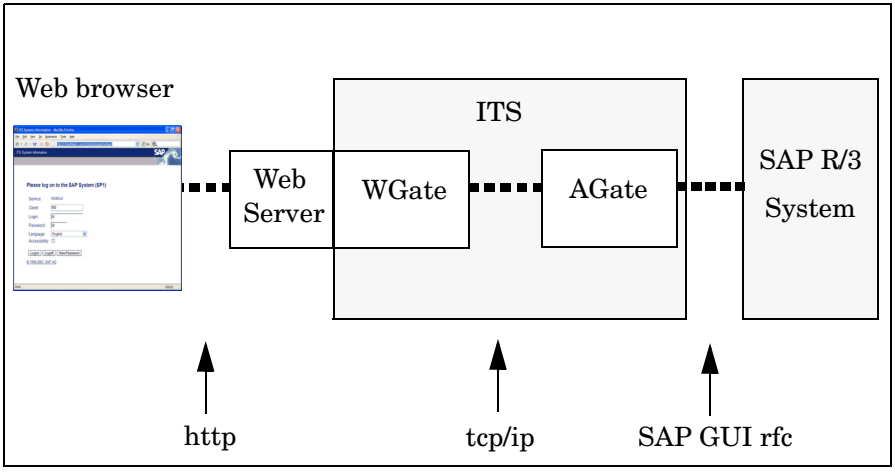
Figure 7-1 Logging in to SAP R/3 with ITS



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 7-2 **ITS Architecture**



Application Gateway

The application gateway links the ITS server to the SAP R/3 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 R/3 application server by means of either the DIAG or the RFC protocol.

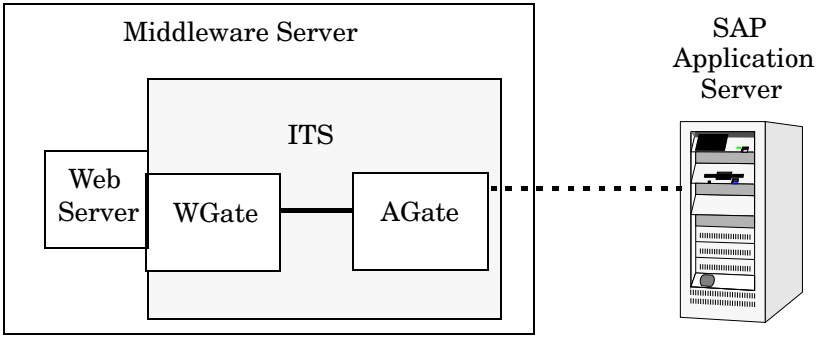
Web Gateway

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 7-3 is

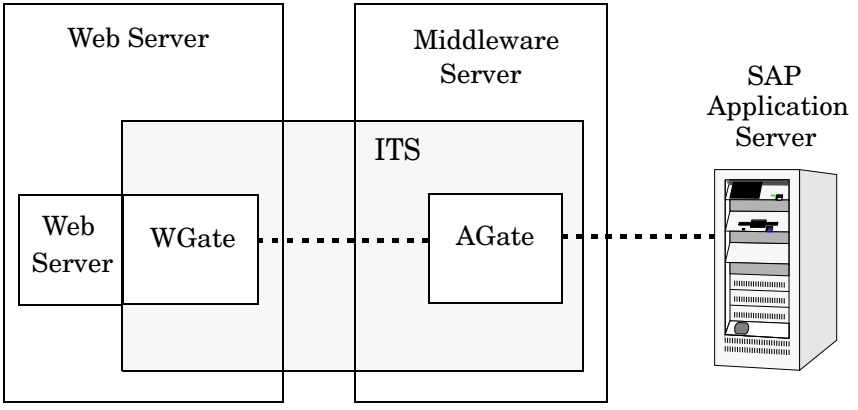
appropriate for test or development purposes, where small loads are present: the dual-host configuration shown in Figure 7-4 tends to work better in a production environment, where higher loads are tend to occur.

Figure 7-3 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 7-4 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 OpenView Performance Agent or the OVO Embedded Performance Component (CODA). OpenView performance tools such as the OpenView 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 OpenView Internet Services (OVIS), 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.

Installing the ITS 6.20 Monitor

The instructions in this section assume that either the OVO Embedded Performance Component (CODA) or the OpenView Performance Agent is already running on all OVO managed nodes, which you want to monitor with the ITS 6.20 monitor. To install the ITS 6.20 monitor on an OVO 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 332
- "Assigning the ITS 6.20 Monitor Template" on page 333
- "Distributing the ITS 6.20 Monitor Template" on page 334

NOTE You cannot remove the ITS 6.20 monitor components from the OVO 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:
  - MS Windows 2000, MS Windows 2003
  - SuSE Linux Enterprise Server (SLES) 8 or 9
  - Red Hat Enterprise Linux (RHEL) 3 or 4
- The installed OVO agent must be running.
- Either the OpenView Performance Agent or the OVO 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* - OpenView 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 OpenView 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 OpenView Smart Plug-in for SAP Installation Guide*.

- The `dsi2ddf` wrapper utilities must be available on the OVO management server and deployed to the ITS 6.20 server; for more information about required product versions, refer to the *HP OpenView Smart Plug-in for SAP Installation Guide*.

NOTE 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 ITS 6.20 monitor, you need to specify the source you want the ITS 6.20 to use for status metrics. For more information about installation pre-requisites and selecting the performance-data source, refer to the *HP OpenView Smart Plug-in for SAP Installation Guide*.

Assigning the ITS 6.20 Monitor Template

To assign the ITS 6.20 monitor templates to the appropriate ITS 6.20 server:

1. In the `Node Bank` window, select the SAP ITS 6.20 AGate servers to which you want to assign templates. Nodes selected together must have the same usage—application server or central instance.
2. From the menu bar, select the following menu option:

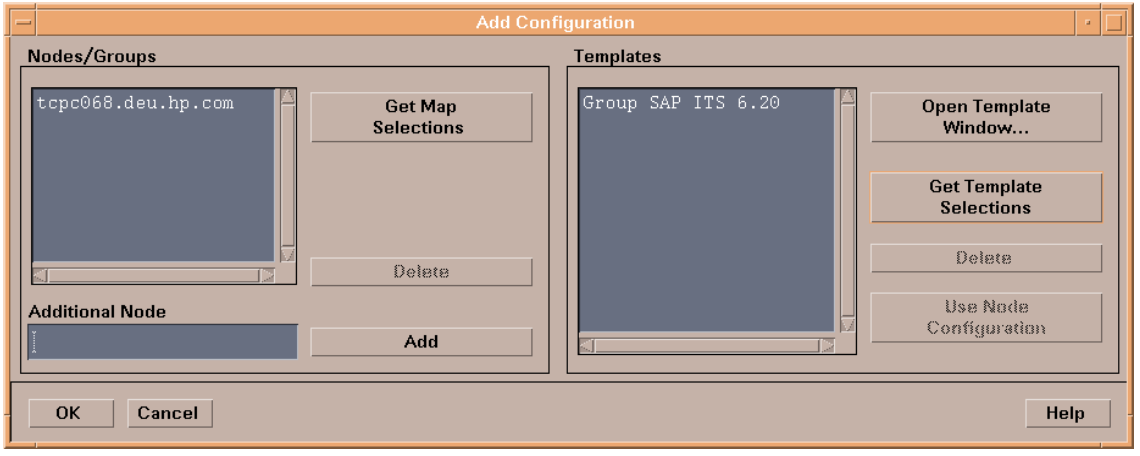
`Actions:Agents -> Assign Templates...`.

The `Define Configuration` window opens.

3. Click `[Add...]`. The `Add Configuration` window opens.
4. Click `[Open Template Window]`. The `Message Source Templates` window appears.
5. In the left pane, expand the `SAP R/3 SPI` template group and select the template group or groups you want to assign to the ITS 6.20 server.
6. Return to the `Add Configuration` window illustrated in Figure 7-5 on page 334 and click `[Get Template Selections]`.

   The newly assigned template is displayed in the `Templates` list.
7. Click `[OK]` to finish assigning the templates

Figure 7-5 Add Configuration Window



Distributing the ITS 6.20 Monitor Template

To distribute the ITS 6.20 monitor templates, carry out the steps in the following list:

1. Select the managed nodes (the ITS 6.20 servers) to which you want to distribute ITS 6.20 monitor components.
2. From the menu bar of the `Node Group` window, select the following menu option:

`Actions:Agents -> Install/Update SW & Config`

The `Install/Update ITO Software and Configuration` window appears.

3. Select the components you want to distribute.
4. Select `Force Update`.
5. Click `[OK]` to finish the distribution.

Verifying the ITS 6.20 Monitor Installation

This section describes how to verify that the installation of the ITS 6.20 monitor completed successfully:

1. As a first step, you can generate a report which lists template assignments for a given managed node, as follows:

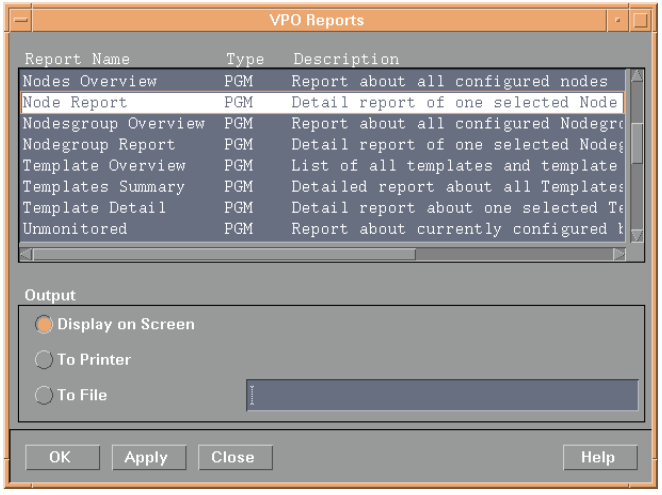
   a. In the `Node Bank` window, select the managed node(s) on which you have installed the ITS 6.20 monitor.

   b. Click the following menu option:

      `Actions -> Utilities > Reports`

   c. Select `Node Report` as illustrated in Figure 7-6.

Figure 7-6 Generating an OVO Node Report



In this case, the following ITS 6.20-specific templates should be present in the list of templates which the node report generates:

- `r3monits`

  Monitors the state of the ITS 6.20 components

2. Next you can log in to the managed node and check that the installation of the ITS 6.20 monitor has copied the appropriate components to the correct locations. For more information about what information is copied where during the installation of the ITS 6.20 monitor, see “ITS 6.20 Monitor: File Locations” on page 342.

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 have installed the ITS 6.20 monitor and, in addition, verified that the installation completed successfully as described in:

- “Installing the ITS 6.20 Monitor” on page 332
- “Verifying the ITS 6.20 Monitor Installation” on page 336

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 338
- “ITS 6.20 Monitor: Configuration Tasks” on page 338
- “ITS 6.20 Monitor: Default Configuration” on page 340
- “ITS 6.20 Monitor: File Locations” on page 342
- “ITS 6.20 Monitor: Configuration-File Key Words” on page 343

ITS 6.20 Monitor: Selecting the Performance-Data Source

OVO Smart Plug-ins can use either the OpenView Performance Agent or the OVO Embedded Performance Component (CODA) as the default source for the performance data required for graphing in OpenView Performance Manager and OpenView Reporter. For more information about selecting performance-data sources, see “Selecting the Performance-data Source” on page 279.

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 OVO agent. On MS 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`

   - MS 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 7-7 Configuring its_ping with the ITS 6.20 Administrator GUI

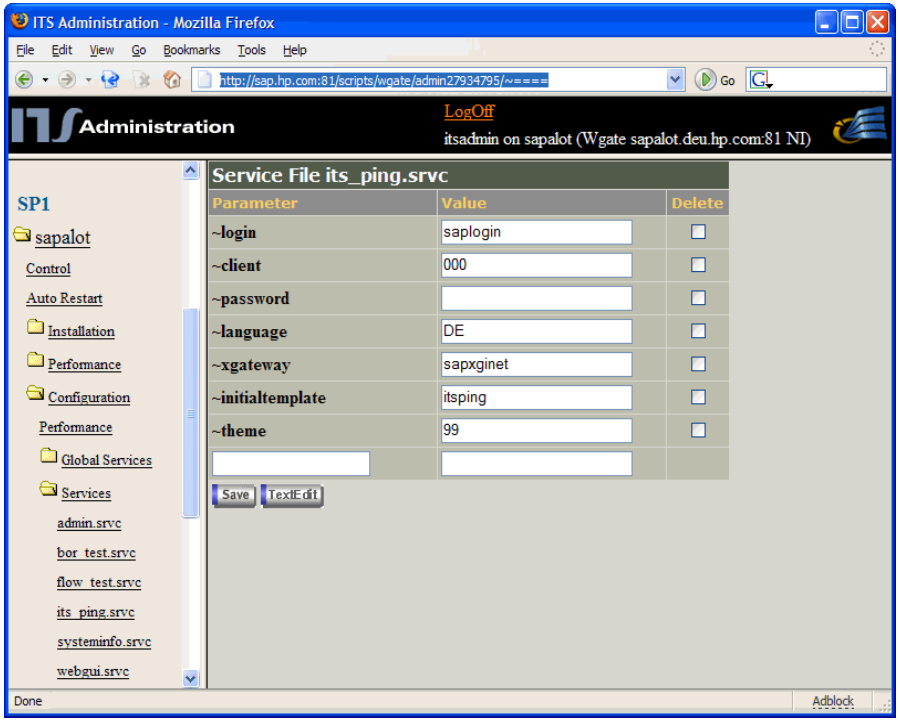


Figure 7-7 shows you how to set up the `its_ping` service using the ITS 6.20 administrator GUI.

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 Example 7-1. 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 342.

Example 7-1 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 OVO managed node (ITS 6.20 server):

- Linux Operating Systems:
  - Binaries:
    - DCE: `<OvDataDir>/bin/OpC/monitor/`
    - HTTPS: `<OvDataDir>/bin/instrumentation/`
  - Configuration files: `<OvDataDir>/conf/sapspi/[global|local]`
  - Trace files: `<OvDataDir>/log/`
- MS Windows Operating Systems:
  - Binaries:
    - DCE: `%OvDataDir%\bin\OpC\monitor`
    - HTTPS: `%OvDataDir%\bin\instrumentation`
  - Configuration files: `%OvDataDir%\conf\sapspi\[global|local]`
  - Trace files: `%OvDataDir%\log`

Table 7-1 lists the files the r3monits monitor uses.

Table 7-1 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 Example 7-1.
`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

The TraceLevel keyword accepts the following parameters:

```
TraceFile =<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.

- **Trace level**:

=0	Disable. This is the default setting.
=1	Log only error messages
=2	Log all messages
=3	Log everything, including debug messages

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 342.

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 MS Windows operating systems respectively.

DatafilesLocation

The default location of the files containing the data, which the Performance Manager and OpenView 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`

  MS Windows Operating Systems:

  `%OvDataDir%\datafiles`

The OpenView 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 CODA, 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> =<ITSSystemID>
=<ITSSystemNr> =<MinAgates> =<ITSWgateHost> =<ITSWGatePort>
=<SAPSystem> =<SAPAppServer> =<SAPNumber>
```

- **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 System ID**:

  The System ID *<SID>* of the ITS 6.20 system you want to monitor on the remote host, for example: "IT1"

- **ITS System Nr**:

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:

```
WebServer =<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 OVO 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 OVO message that is sent when the threshold rule is violated.

- **OpC Message Group**

  =<*object*> — The message group assigned to the OVO 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 OVO 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 OpenView Reporter to examine the data collected by the ITS 6.20 monitor. For a complete list of the ITS reports available with the SPI for SAP, see Table 9-3 on page 386. 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 OpenView Reporter to generate and view reports relating to information collected by the ITS 6.20 monitor:

- HP OpenView Reporter
- SPI for SAP ITS 6.20 monitor Reports Snap-In

ITS 6.20 Service Reports: Configuring the OpenView Reporter

The installation of the SPI for SAP service reports described in "Installing the SPI for SAP Reports" on page 376 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 OV 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 OpenView Reporter. The OV Reporter automatically attempts to discover all the new systems you add to it. If it cannot find a node, OV 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 OV Reporter window
- Browse to the following file/directory on the OV Reporter machine, *host.name.com*:

  `\\<`*host.name.com*`>\rpmtools\Data\Webpages\reports.htm`

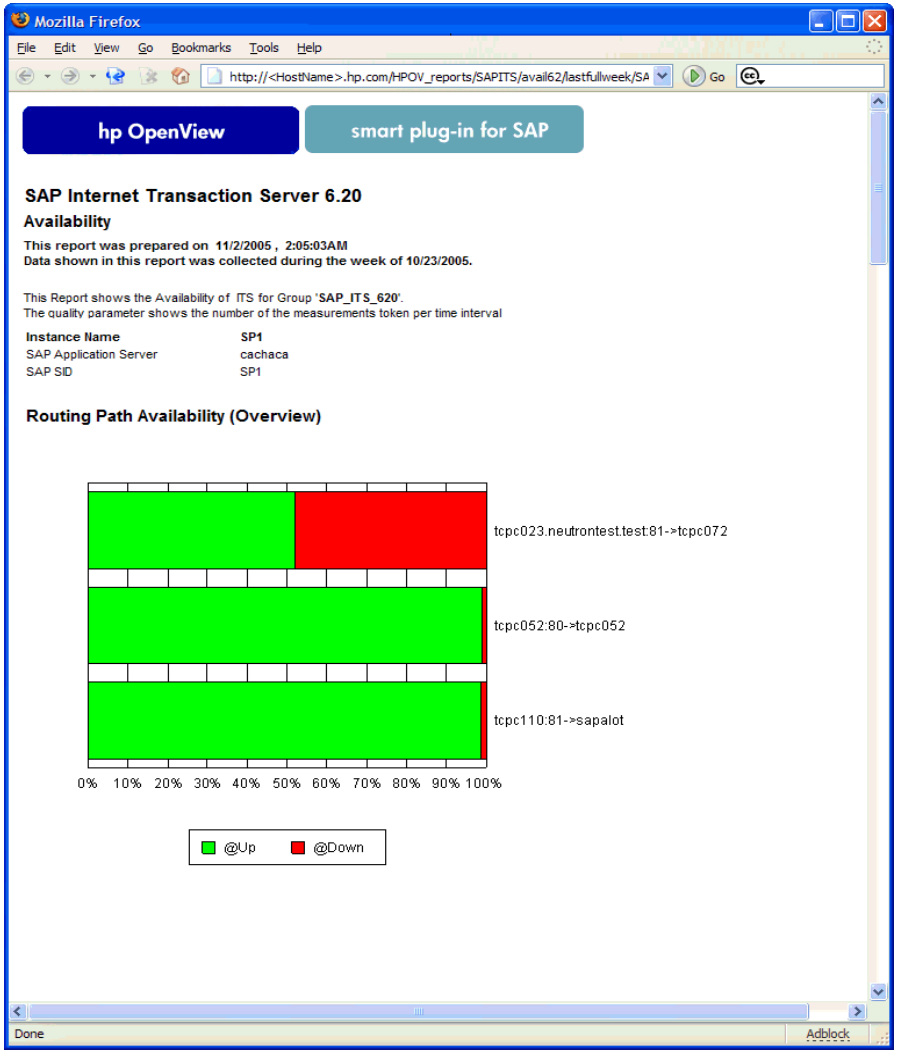
- open a (remote) Web-browser window and enter the following URL:

  `http://<`*host.name.com*`>/HPOV_reports/reports.htm`

  Note that this assumes that a Web server is running on the OV 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 7-8 shows an overview of the availability of the routing path in a SAP ITS 6.20 instance over the last full week.

Figure 7-8 ITS 6.20 Reports



8 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 OVO to provide you with information that is specifically designed to help you manage your SAP R/3 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. You can view the Service Views using the OVO 5.0 (or later) Java-based operator GUI.

NOTE You cannot use Service Views with versions of OVO earlier than 5.0.

Use the capabilities of OVO and Navigator to:

- 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

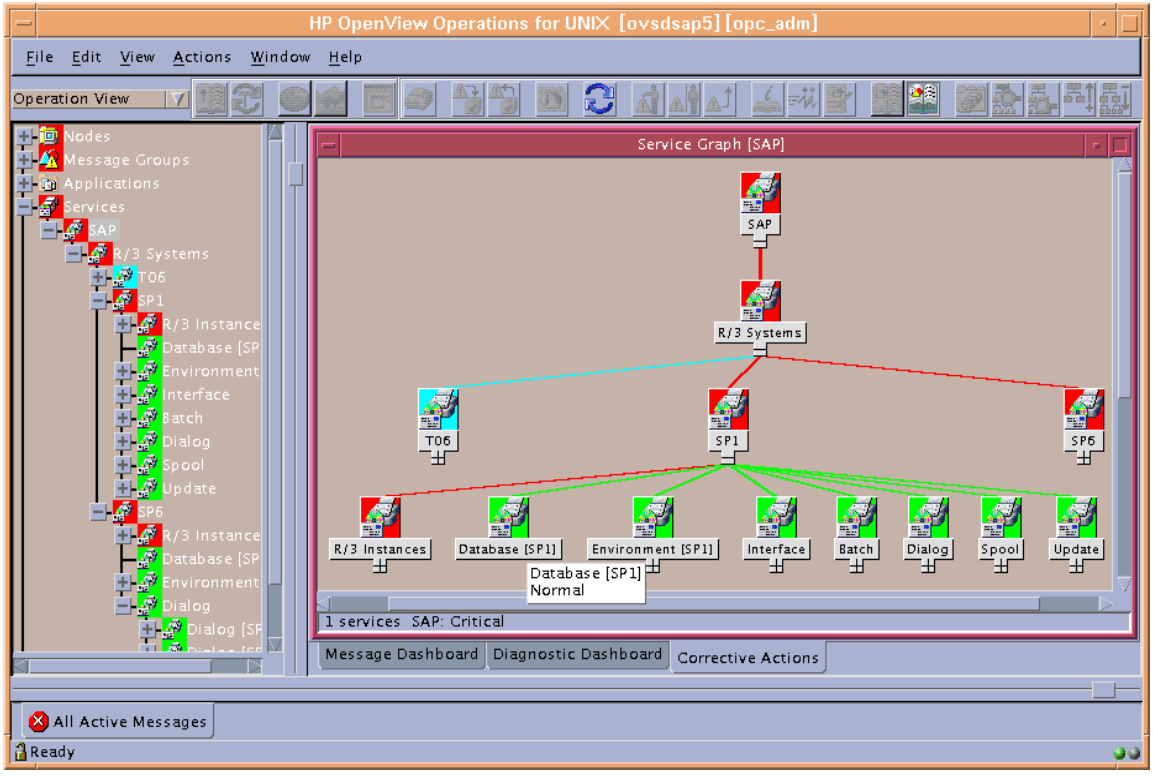
Define message-to-object mapping in the OVO message-source template by specifying a service ID. The environment model, message calculation and propagation rules, and available actions for each object are defined in the service-configuration file.

The scoping pane of the main window in the Java GUI shows discovered services in addition to the usual OVO managed nodes, message groups, and applications. Click a service to expand the service's navigation tree in the scoping pane. In the tree, you can select any service or sub-service and display a service graph.

In both the navigation tree and 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 your message browser, 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.

Figure 8-1 The Navigator GUI



For a detailed explanation of the concepts and implementation of Navigator, see the *HP OpenView Navigator Concepts and Configuration Guide*.

Service Views in the SPI for SAP

The SPI for SAP provides a `Service Discovery` application, which you can execute on each managed node to analyze the SAP R/3 environment and generate a service-configuration file. The service-configuration file represents all existing ownership and dependency relationships between objects on the nodes, message-propagation rules, and any actions that are available for objects. This file must be uploaded to the Navigator.

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.

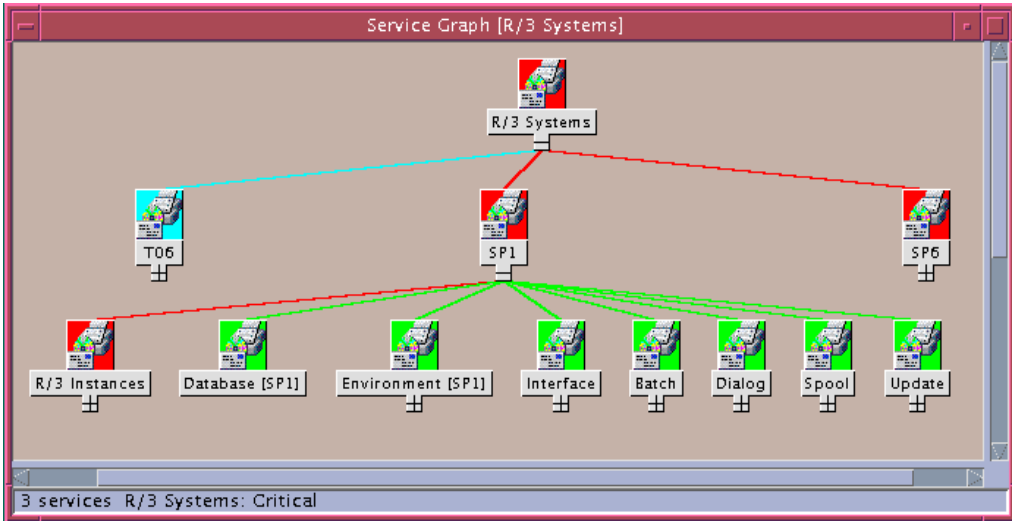
The first level is an accumulation object including all SAP R/3 systems. When you expand a first-level object, you see an object for each SAP R/3 system in your environment. The SAP R/3 Systems object changes status in response to a change of status in any of the objects that make up the instances that it contains.

The second level includes logical objects within each SAP R/3 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 R/3 system. Expand an SAP R/3 system object to display the following logical objects:

- R/3 Instances
- Database (<*SID*>)
- Environment (<*SID*>)
- Interface
- Batch
- Dialog
- Spool
- Update

Figure 0-2 shows an example SAP R/3 service view expanded to the logical object level.

Figure 8-2 Service View of R/3 Systems

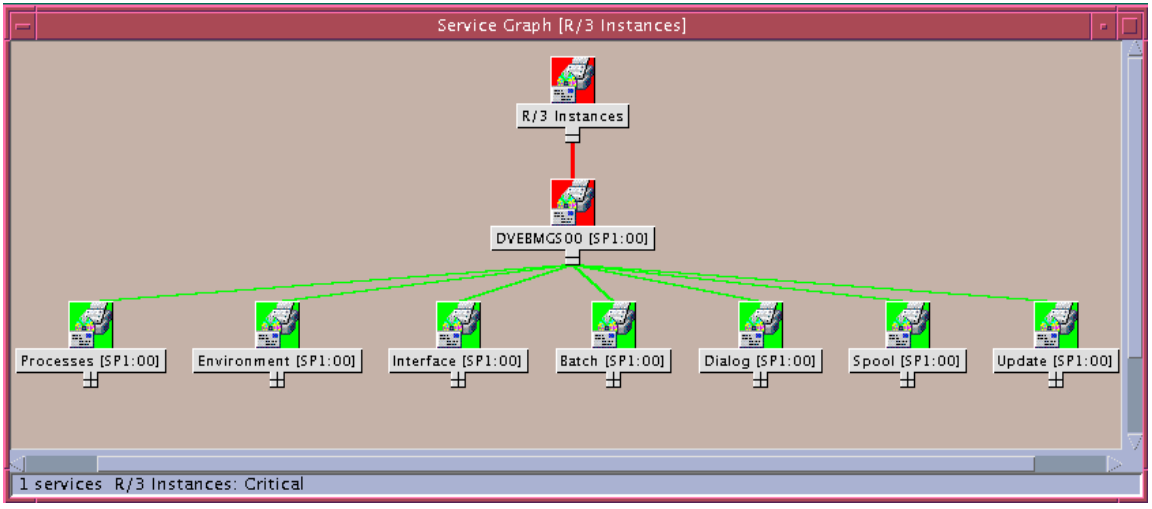


When you expand the SAP R/3 Instance object, each R/3 instance appears as an object in the tree. When you expand the environment object, you will see displayed three further objects:

- 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 8-3 Service View of an R/3 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

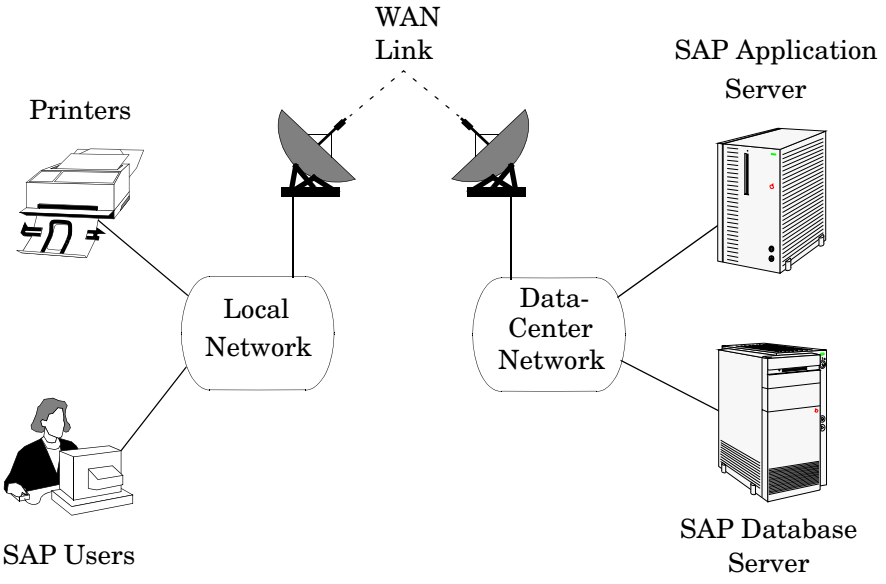
Line of Business Views

The SAP R/3 service view and the other service views available with OVO provide graphical representations of the individual areas you are monitoring, for example SAP R/3, 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 R/3 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 R/3 dispatch, dialog, and spooling processes for the specific SAP R/3 instance.

Figure 8-4 Service Areas Affecting Order Entry



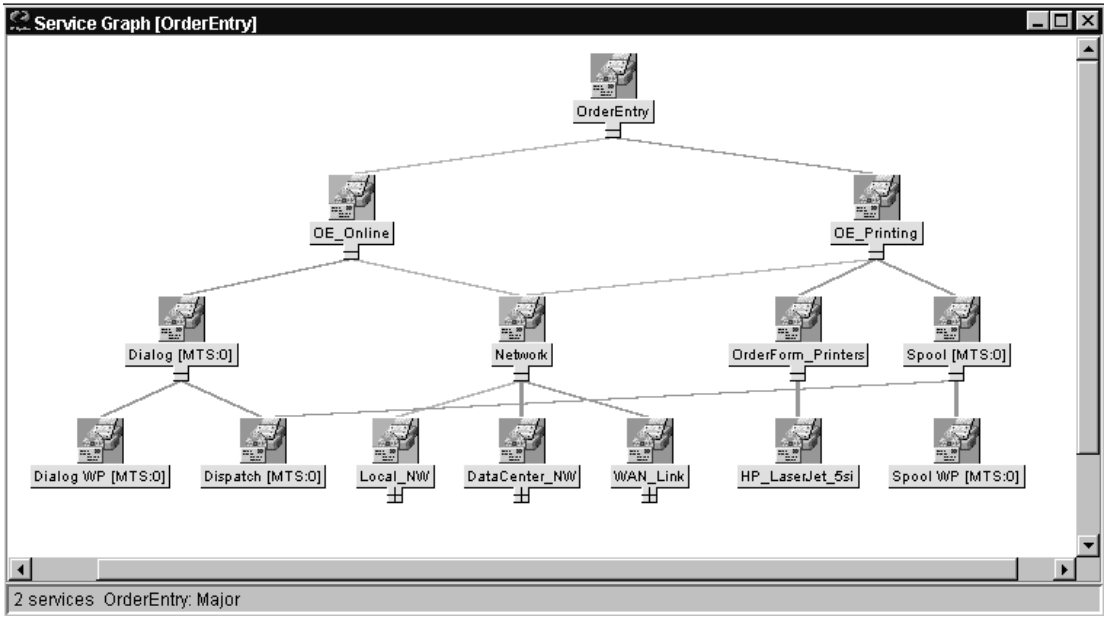
To create a line-of-business service view, you must first define the structure you want to see by generating a custom service-configuration file, in which you must define one or more logical objects (for example, Order Entry) to which messages will be propagated by the objects you include in the view.

Using the service-configuration files for the service areas you are interested in (for example, the SAP R/3 file), obtain the service names of the objects you want to include and add use references to them to your

Service Configuration file. See the *HP OpenView Service Navigator Concepts and Configuration Guide* for information on creating Service Configuration files.

Be aware that the services should only be built on top of logical (not physical) service objects. For example, use the SAP R/3 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.

Figure 8-5 Line of Business View for Order Entry



Configuring Service Views for SAP R/3

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 OVO database, as follows:

1. **Discover the SAP services**

   Discover which SAP services to monitor with the SPI for SAP on each of the SAP R/3 servers.

NOTE

Make sure that Perl 5.8 or later is installed in the default location on the managed node, for example in UNIX environments: `/usr/bin/perl`. If Perl is not installed in the default location, make sure it is accessible by means of the PATH environment variable. In a Microsoft Windows environment, the Perl interpreter is accessible through the PATH variable. Note that the Perl installation sometimes has an option to automatically add Perl to the PATH.

2. **Create a service-configuration file**

   Use the information about the discovered services to create a service-configuration file. The service-configuration file contains definitions for the services present on each SAP R/3 instance on each of the SAP R/3 servers that you want to monitor with OVO and the SPI for SAP.

   For more information, see “To create the Service Configuration file” on page 365.

3. **Upload the service-configuration file to OVO**.

   After OVO discovers the SAP services, you can use the OpenView Navigator tool (or, from OVO 5.0 onwards, the Java GUI) to display a graphical overview of the services.

   For more information, see “To Upload the Service Configuration File to OVO” on page 366.

4. **Assign SAP R/3 services to SPI for SAP operators**

   Assign the SAP R/3 services to the SPI for SAP operators who are responsible for them. In this way, the operators receive messages concerning only those services for which they are responsible.

   For more information, see "Assign the SAP Services to an OVO Operator" on page 366.

5. **Troubleshoot Service-discovery Problems** (optional)

   There are a number of ways in which you can attempt to troubleshoot problems that arise during the Service-discovery process.

   For more information, see "Troubleshooting Service Discovery" on page 368.

To create the Service Configuration file

1. Log in to OVO as `opc_adm`
2. Open the `Managed Nodes` window and the `SAP R/3 Admin` application group window
3. Select the node, nodes, or node group for which you want to generate a service configuration and drag it (or them) over the `SAP R/3 Admin` application group window and drop it (or them) onto the R/3 `Service Discovery` icon.
4. The `R/3 Service Discovery` application writes entries in the file `/var/opt/OV/tmp/SapSpiServices` for each SAP R/3 instance it discovers on each of the managed nodes selected in the previous step.

   Note that tracing is enabled by default and writes information and error messages relating to the SPI for SAP service-discovery process to the following file: `/var/opt/OV/tmp/r3sm.trace`

5. You can watch the progress of the `R/3 Service Discovery` application as it writes progress to `stdout`. After the `R/3 Service Discovery` application completes its tasks, you can examine the contents of the `/var/opt/OV/tmp/SapSpiServiceDiscovery` file to verify that the managed nodes have all been successfully discovered. If this is not the case, and managed nodes are missing from the list of discovered nodes, see "Common SPI for SAP Problems" on page 407.

To Upload the Service Configuration File to OVO

This section describes how to upload the service-configuration file to OVO:

NOTE You do *not* need to stop the OV services to complete this task.

1. Upload the service-configuration file to OVO. On the command line, enter:

   #/usr/bin/opcservice -replace /var/opt/OV/tmp/SapSpiServices

   ```
   Converting service file to XML ...
   Successfully added service file:/tmp/SapSpiServices
   ```

   Note that `/usr/bin/opcservice` takes care of the conversion to XML where appropriate.

NOTE If a Navigator GUI is open, it will not immediately reflect the changes made by the `.R/3 Service Discovery` application. You must refresh the Navigator GUI to load the new configuration. To refresh the Navigator GUI, open the `View` menu and select `Reload Configuration`.

Assign the SAP Services to an OVO Operator

This section describes how to assign the configured and uploaded SAP services to the SPI for SAP operators:

NOTE You do *not* need to stop the OV services to complete this task.

1. Assign the service to an operator. Enter:

   #/usr/bin/opcservice -assign <*Operator*> SAP_SPI:SAP

   ```
   Successfully assigned services to operator <Operator>
   ```

NOTE If a Navigator GUI is open, it will not immediately reflect the changes made by the `.R/3 Service Discovery` application. You must refresh the Navigator GUI to load the new configuration. To refresh the Navigator GUI, open the `View` menu and select `Reload Configuration`.

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 will fail.

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 will attempt to discover.

In the event that the service discovery fails, you can use the environment variables in Table 8-1 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 the SAP profiles in the following locations:

- **UNIX** (SAP application servers)

  `/sapmnt/<SID>/profile/`

- **Microsoft Windows**

  `\\<central_instance_host>\sapmnt\<SID>\SYS\profile\`

  The `<central_instance_host>` is the name of the host on which the SAP central instance is running. You can use the long or short hostname, the IP address of the hostname, or the UNC notation.

Table 8-1 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

Table 8-1 Service-discovery Environment Variables (Continued)

Environment Variable	Description
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

9 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 OVO to provide you with information that is specifically designed to help you manage your SAP R/3 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 OpenView Reporter (OV Reporter) using Crystal Reports templates and viewed using a web browsers. OV Reporter allows you to request both scheduled and on-demand versions of reports.

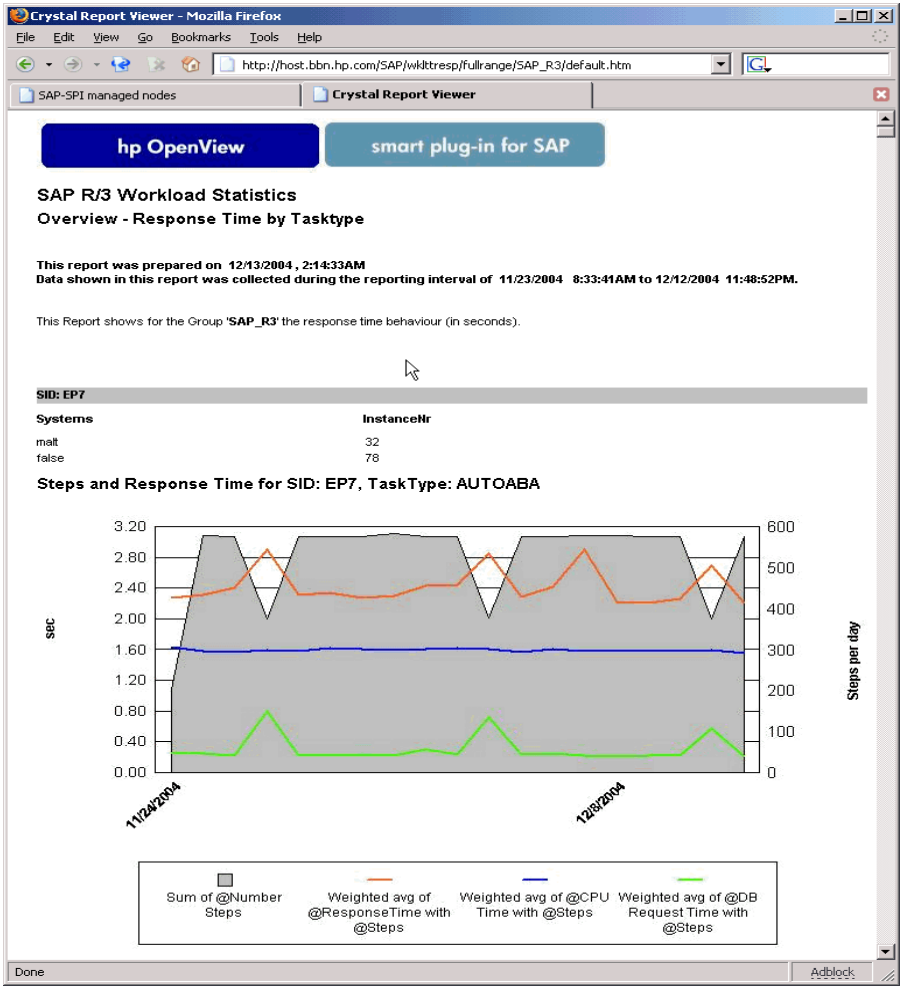
Figure 9-1 Service Reports Viewed in a Web Browser

SPI for SAP service reports correlate the data extracted from either the OVO Embedded Performance Component or the OpenView 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.

Figure 9-2 SAP Workload Statistics



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 OpenView Reporter software. For more information about supported software versions, refer to *HP OpenView Smart Plug-in for SAP Installation 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 266. For more information about upgrading the SPI for SAP itself, see "Upgrading the SPI for SAP" in the *HP OpenView Smart Plug-in for SAP Installation 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, for example; from A.09.02 to 10.20, you will 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 MS 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 376.

3. Schedule and generate the new service reports as described in "Generating SPI for SAP Reports" on page 387.

Installing the SPI for SAP Reports

This section explains how to install the SAP R/3 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 R/3 Service Reports, you must ensure that the following tasks have been completed:

1. **Performance Agent**

   Either the OVO Embedded Performance Component or the OpenView Performance Agent agent must be available on all SAP R/3 managed nodes for which you want to produce service reports.

   The OpenView Performance Agent agent must also have been configured according to the instructions given in "The SPI for SAP Performance Monitors" on page 263.

2. **Service Reports**

   OV Reporter must be available on an MS Windows 2000/2003 host.

   Note that if you want to edit existing (or create new) Service Reports for the SPI for SAP, make sure that Seagate's Crystal Reports is running on the machine hosting the OpenView Reporter. For more information about required or supported software versions, see the *HP OpenView Smart Plug-in for SAP Installation Guide*.

To Install SAP R/3 Service Reports

The service reports for SAP R/3 are installed into the OV Reporter product as a snap-in using InstallShield on the OpenView Reporter system. During set-up you will be asked to select the common application path of OV Reporter. This is the folder where you installed OV Reporter.

The set-up routine will attempt to discover this path automatically and indicate to you what it finds. In most circumstances you should avoid changing it and accept the default settings.

The set-up copies components to the directories as summarized in Table 9-1. All directory paths are relative to the OV Reporter common application path.

Table 9-1 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 CD and browse to the following directory:

   `\WINDOWS\OV_REPORTER\SAP_SPI_10.20`

   Double-click the `sapspi_reporter.msi` file, and select the `Complete Installation` 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 OpenView Reporter. Accept the default to ensure that all automatic configuration steps are correctly executed without the need for manual re-configuration.

NOTE 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 390. The installation should look similar to the example illustrated in Figure 9-3.
5. If you choose to add your SAP R/3 or SAP ITS systems to OpenView 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 OpenView Reporter.

   - Network: **`SAP`**
   - Domain: either **`SAP`** or **`ITS`**, as appropriate

   Check that your SAP R/3 and SAP ITS 6.20 hosts have been added to the appropriate OpenView 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 R/3 or SAP ITS 6.20) discovered on the monitored host.

   Click `[OK]` to display the newly added systems in the OV Reporter's Details Pane.
6. Use the OV Reporter GUI to schedule the generation of the SPI for SAP reports or generate them now using the following option:

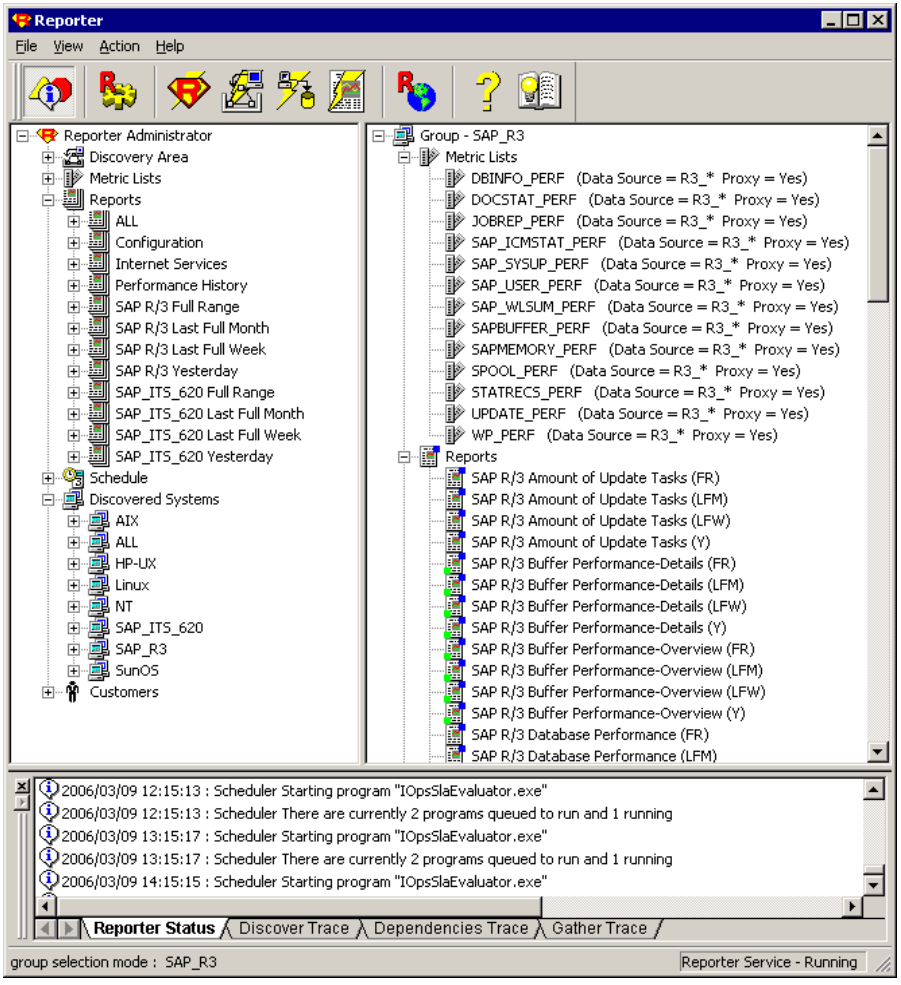
   `Actions > Run > Generate Reports`

NOTE

Make sure you allow enough time for OpenView Reporter to gather the report data and store it in the Reporter database before you start generating reports. For more information, see "Generating SPI for SAP Reports" on page 387.

7. 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 388.

Figure 9-3 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 OVO Embedded Performance Component (CODA) and OpenView Performance Agent to generate reports, which display vital information about the health and availability of the Systems in your SAP R/3 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 R/3 Reports" on page 381

  A complete list of all the SAP R/3-related reports provided with the SPI for SAP including the metrics used

- "SAP ITS 6.20 Service Reports" on page 386

  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 R/3 Service Reports" on page 387

  Hints to help you target more accurately the information you want to display in a report

- "Generating SPI for SAP Reports" on page 387

  Instructions for starting the generation of the SPI for SAP reports

- "Viewing SPI for SAP Reports" on page 388

  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* OVO managed nodes and do *not* have the SPI for SAP software installed, are monitored remotely from an OVO 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 26, and "Remote Performance Monitoring" on page 286.

SAP R/3 Reports

Table 9-2 lists the SAP R/3 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 298.

Table 9-2 SAP R/3 Performance Reports

Report	Purpose	Metrics
Database Performance	shows the important database performance metrics correlated together	• 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	show 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
E2E Time	shows the E2E Transaction Time of the configured transactions, divided into Response and Network Time	• Response Time • Network Time

Table 9-2 SAP R/3 Performance Reports (Continued)

Report	Purpose	Metrics
ICM Statistics - Overview	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 R/3 instances in the different, specified states (running, ready, released)	Number of Jobs in the status: • Running • Ready • Scheduled • Released • Aborted • Finished

Table 9-2 SAP R/3 Performance Reports (Continued)

Report	Purpose	Metrics
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
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 R/3 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.

Table 9-2 SAP R/3 Performance Reports (Continued)

Report	Purpose	Metrics
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 R/3 System (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 R/3 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)	
Workload Overview DB Overview	shows the work-load metrics based on database activity for a defined SAP R/3 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 R/3 system	

Table 9-2 SAP R/3 Performance Reports (Continued)

Report	Purpose	Metrics
SAP R/3 Memory	SAP R/3 Memory use for the defined System	• Extended Memory • Paging Area • Roll Area
SAP R/3 Users - Overview	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 R/3 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 R/3 module for users and user sessions (per SAP client/application server)	• Average Sessions • Average Users • SAP R/3 Module (FA, MM, SD)

Table 9-2 SAP R/3 Performance Reports (Continued)

Report	Purpose	Metrics
SAP R/3 Buffer Performance - Overview SAP R/3 Buffer Performance - Detailed Analysis	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 ITS 6.20 Service Reports

Table 9-3 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 9-3 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 R/3 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 OV 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:

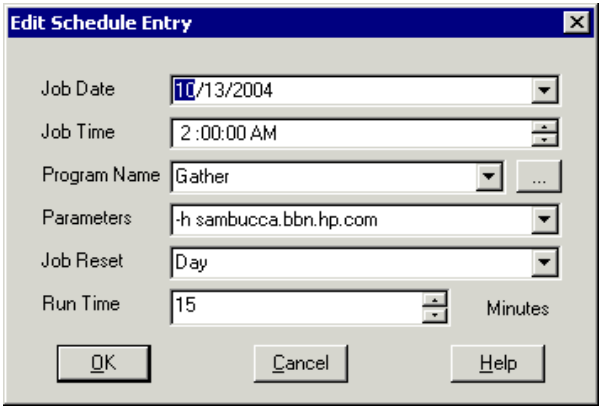
1. Make sure you complete the installation and configuration steps described in "To Install SAP R/3 Service Reports" on page 376 before you start generating reports.
2. Use the OV Reporter GUI to schedule data collection for the SPI for SAP reports using the following menu option:

   `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.

NOTE Due to differences between the way SAP and the SPI for SAP's performance-data sources (OVO Embedded Performance Component and OV Performance) 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 9-4 on page 388.

Figure 9-4 Setting up Data Collection for Reports



3. Use the OV Reporter GUI to start the generation of the SPI for SAP reports using the following option:

   `Actions > Run > Generate Reports`

NOTE 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 R/3 Service Reports" on page 376.

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 298. For more information about the SPI for SAP reports, see "Service Reports in the SPI for SAP" on page 380.

In this section, you can find information about the following topics:

SAP R/3 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.

- "DBINFO_PERF"

  This metric monitors database-performance analysis values

- "DOCSTAT_PERF"

  This metric collects the quantity-structure statistics (the document volume) for the last full hour

- "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 memory *buffers* for an SAP instance

- "SAPMEMORY_PERF"

  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"

  The status of the SAP R/3 instances

- "UPDATE_PERF"

  The number of update processes

- "USER_PERF"

  Monitors the number of users and user sessions per SAP client for a given SAP application server

- "WLSUM_PERF"

  Collects the performance-workload statistics hourly

- "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:

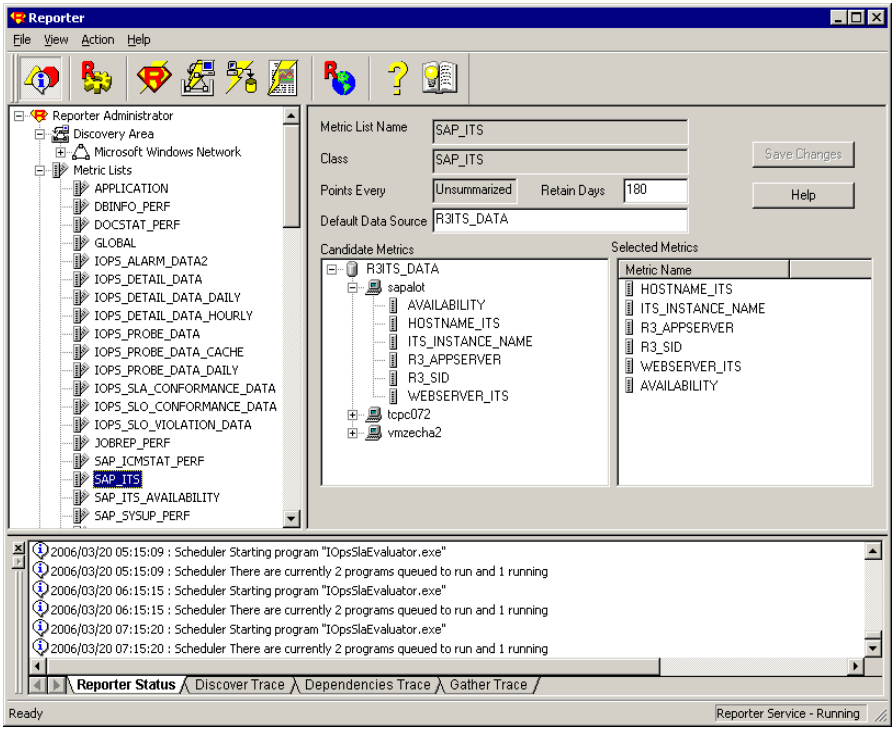
- `SAP_ITS`

  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 9-5 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 OpenView Reporter, you need to perform the following steps described in this section in the order specified. This section covers the following topics:

To Remove OpenView Reporter Snap-in Packages

Use the following instructions to help you remove the SPI for SAP snap-in package for the OpenView Reporter quickly and easily from the OpenView Reporter system:

1. In OV 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 OV Reporter System

To remove the SPI for SAP binaries from the OpenView Reporter system, you need to carry out the following steps on the OpenView Reporter system as the system administrator:

1. In the MS-Windows Start menu, browse to the following item:

   `Start:Settings > Control Panel > Add/Remove Programs`

2. Select: `HP OpenView Operations Performance for Windows`
3. Highlight: `Reports for hp OpenView smart plug-in for SAP`
4. Select: `Remove`

   Follow the on-screen instructions to complete the removal process.

10 Troubleshooting the SPI for SAP

This section provides information that is designed to help troubleshoot the problems you encounter when working with the SPI for SAP.

In this Section

The information in this section helps you through the process of troubleshooting the problems you encounter in the every-day use of the SPI for SAP. You will find information about the following topics:

Characterizing Problems

When you encounter a problem, make a note of all associated information. This information may be useful when you proceed to the next stage of problem analysis or if external support is required and you are requested to explain the problem to service personnel:

- **Context**

  What has changed? Determine if anything has changed on your network or with the product configuration:

  — Hardware?

  — Software (including OS, OVO, and SAP R/3 patches)?

  — Files?

  — Security (file permissions)?

  — Name services?

  — Utilization?

  — In what situation does (or did) the problem occur?

- **Duration**

  How long and how often? Is the problem consistent (fails every time) or inconsistent (fails only sometimes)?

Problem Identification Procedures

This section includes descriptions of procedures that you can use to identify the root of the problem that is causing the symptoms you have noted. You will not need all these procedures for every problem you encounter, as some problems can be easily localized to a particular component of the system. However, for most problems, you will need to check one or more of the following:

- The OVO agent and OVO management-server installation (including patches).
- SPI for SAP installation.
- The message-source templates that are distributed to managed nodes.
- The operation of the SPI for SAP monitors on managed nodes.
- SPI for SAP access to the SAP R/3 front end.

Checking the OVO Agent Installation

You must check the following:

- the OVO agent is installed on both the managed node and the management server.
- which version of the OVO agent is installed

To check whether the OVO agent is installed on a managed node or the OVO management server, go to the command line and enter the following command:

```
swlist
```

This provides information about the installed version of the OVO agent on the managed node or the OVO management server where you executed the command.

You can obtain more information by stopping the OVO agent, enabling tracing, and starting the OVO agent again, as follows:

1. Enable tracing of the OVO agent.

   To enable tracing of the OVO agent, open the following file and add the entry: **OPC_TRACE TRUE**:

   ```
   /opt/OV/bin/OpC/install/opcinfo
   ```

2. Stop the OVO agent.

   To stop the OVO agent, enter the following command:

   ```
   opcagt -stop
   ```

3. Restart the OVO agent.

   To restart the OVO agent, enter the following command:

   ```
   opcagt -start
   ```

4. Verify the information in the OVO trace file.

   To monitor the contents of the OVO trace file, enter the following command:

   ```
   tail -f /var/opt/OV/tmp/OpC/trace
   ```

Checking the OVO Server Installation

To check whether the server component is installed on the OVO management server, go to the command line and enter the following command:

```
swlist
```

This provides information about the installed version of theOVO server component that is installed on the management server.

You can obtain more information by stopping and starting the OVO agent with trace enable, as follows:

1. Enable tracing of the OVO management server.

   Open the following file `/opt/OV/bin/OpC/install/opcinfo` and add the entry: **`OPC_TRACE TRUE`**

2. Stop the OVO management server.

   Enter the following command:

   ```
   opcsv -stop
   ```

3. Restart the OVO management server.

   Enter the following command:

   ```
   opcsv -start
   ```

4. Verify the information in the OVO trace file.

   Enter the following command:

   ```
   tail -f /var/opt/OV/tmp/OpC/mgmt_sv/trace
   ```

Checking Installed Patches

To check whether you have the latest OVO patches installed, go to the command line and execute the following command:

```
swlist
```

The information displayed includes the patch number. To ensure that the patch has been distributed to managed nodes, you should check:

- to see which version of OVO the patch relates to, as well as
- note which version of OVO executable is on the managed node.

To check the version of an executable on a managed node where a UNIX operating system is installed, execute the `what` command, for example:

```
what opcgt
```

The output includes the version number.

To check the version of an executable on an MS Windows node, select and right-click the executable file in Windows Explorer, choose `Properties` from the context menu, then click the `Version` tab.

Testing the SPI for SAP Installation

You can check which version of the SPI for SAP is installed on the OVO management server or on a UNIX managed node by checking the versions of the `r3itogui` and the SPI for SAP monitors. To find out which versions of the `r3itogui` and the SPI for SAP monitors are installed on a particular system, enter the following commands:

```
what /opt/OV/lbin/sapspi/r3itogui
```

```
what /var/opt/OV/bin/OpC/monitor/r3mon*
```

The information displayed when you execute either of these commands includes the SPI for SAP version. For example:

```
/opt/OV/lbin/sapspi/r3itogui:
abcglob %u.%u
HP Open View SMART Plug-In for SAP Mon Oct 312:30:21 METDST 2004
HP Open View SMART Plug-In for SAP Rev. #.# Serie 700/800 HP-UX 11.X
alxxsnmp.c 20.7 SAP 04/07/08
```

Checking the Distributed Templates

You can check which message source templates are distributed to a managed node as well as any parameters (such as polling rate) that have been set for them. To obtain this information, enter the command:

```
/opt/OV/bin/OpC/utils/opcdcode /var/opt/OV/conf/OpC/monitor
```

The following is an example of the information that is displayed for each template that is found on the node:

```
Monitor "r3monjob"
DESCRIPTION "Monitoring of SAP R/3 batch jobs
INTERVAL "15m"
MONPROG "r3monpro
MAXTHRESHOLD
GEN_BELOW_RESET
THRESHOLD 0750000
RESET 0.250000
```

Checking the Execution of Monitors on HP-UX Nodes

To check that a monitor is running correctly, you can enable tracing, start the monitor from the command line, and then view the resulting trace file.

To start a monitor with tracing enabled, enter the following command:

/var/opt/OV/bin/OpC/monitor/<*monitor*> -trace 1

where <*monitor*> is the monitor name, for example, `r3moncol`.

When the monitor has started, you can view the trace file by entering the following command:

more /var/opt/OV/log/<*monitor*>.log

Additional trace information can be obtained for monitors that use Remote Function Calls (RFCs), by entering the following command:

more dev_rfc

This command displays the `rfc_dev` file, where you can see trace information regarding the establishment of the RFC connection, RFC-get and RFC-send data, and any RFC exceptions.

The monitors that use RFCs are:

- The batch job monitor, `r3monjob`

For the following monitors, there is an additional facility that allows you to validate the monitoring conditions that have been defined in the monitor configuration files:

- The process monitor, `r3monpro`

- The batch job monitor, `r3monjob`

For these monitors, you can add the switch, `-parser`, to the start monitor command, as follows:

`/var/opt/OV/bin/OpC/monitor/<monitor> -trace 1 -parser`

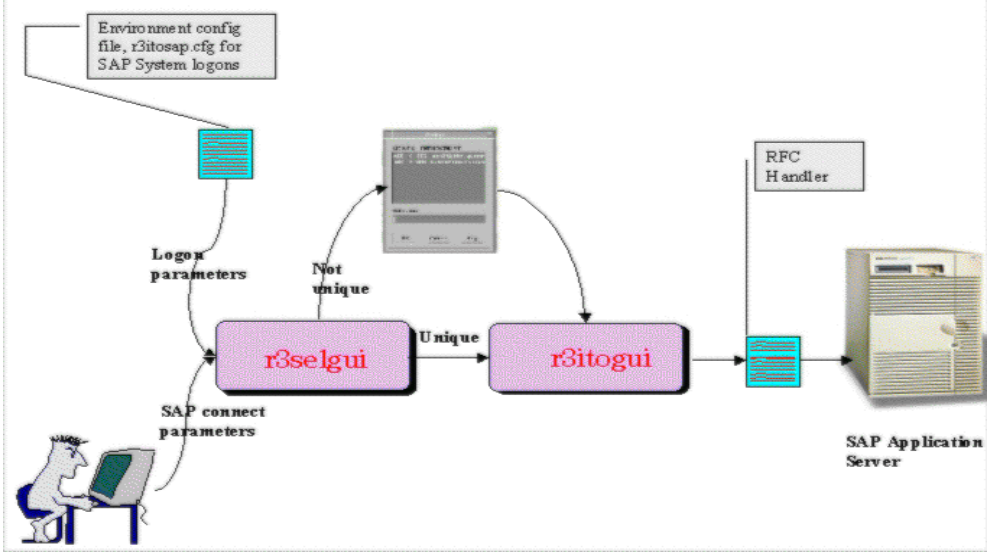
If the configuration is found to be invalid, a critical message is sent to the message browser. Otherwise, there is no message.

For information about configuration of SPI for SAP monitors, see "Customizing the SPI for SAP Monitors" on page 17.

Checking SPI for SAP Access to the SAP R/3 Front End

The SPI for SAP includes a number of applications and operator-initiated actions that open a SAP R/3 online session. Figure 10-1 illustrates how the connection to the SAP front end is made from the OVO desktop.

Figure 10-1 SPI for SAP Connection to the SAP R/3 Front End



You can test the connection to the SAP R/3 front end for a particular instance by starting the sapgui and the `r3selgui` utilities, each with trace enabled. To do this, go to the command line on the management server and enter:

```
export DISPLAY =<hostname>:0.0
/opt/OV/lbin/sapspi/sapgui/sapgui -host<hostname> -nr \
<SAP_instance_number>
/opt/OV/lbin/sapspi/r3selgui -exefile
/opt/OV/lbin/sapspi/r3itogui -host <hostname> -trace 1
```

To view the result of the trace, enter:

```
more dev_rfc
```

This command displays the `rfc_dev` file, where you can see trace information regarding the establishment of the RFC connection, RFC get and send data, and any RFC exceptions.

Figure 10-2 illustrates the different stages in the process of communication between OVO and SAP R/3

Figure 10-2 Message Flow between OVO and SAP R/3

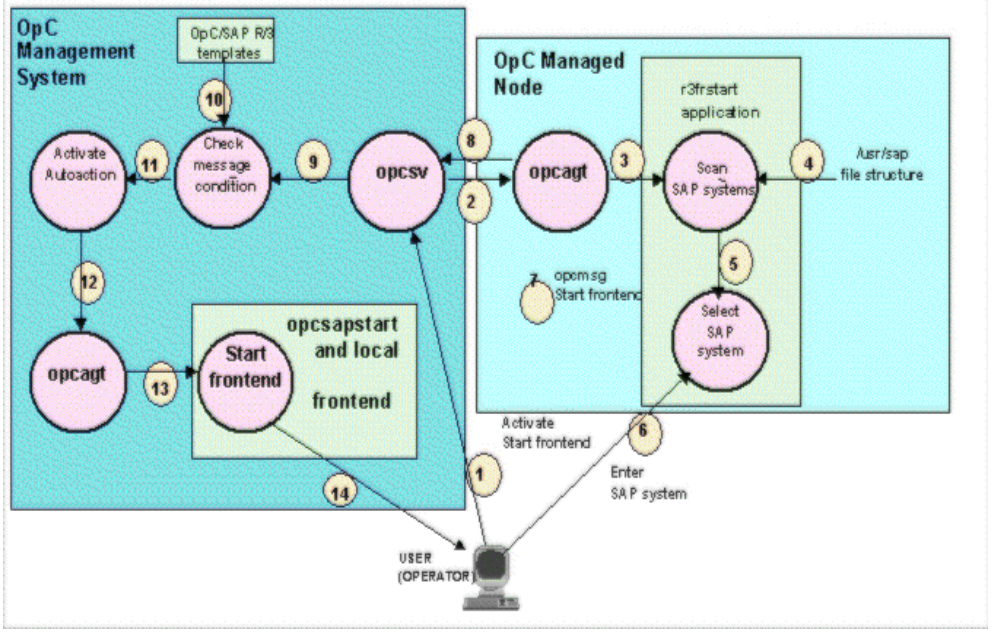


Table 10-1 summarizes the problems that can occur at different stages in this communication process, and the checks that you can make to discover the cause.

Table 10-1 Checking Communication Problems

Stages	Problem	Check
1, 2, 3	Permission problems on the managed node The action agent `opcacta` is not running on the managed node.	`rlogin` to the managed node as user `opc_op`, and try to start the `SAP R/3 Front End` application manually. Execute the command: **`opcagt -status`**
4, 5, 6	No read permissions in directory structure: `/usr/sap`	Log on to managed node: **`su opc_op`** execute: **`find /usr/sap -print`** If it is a problem with read permissions, the message "`Cannot Open`" will appear.
7, 8, 9	OVO agent or server is not running Problems with communication	On the management server and managed node, execute: **`opcagt -status`** On the management server, execute: **`opcsv -status`** Enable OVO trace mode on the managed node and the management server.
10, 11, 12	The message sent via `opcmsg` does not match the `r3frstart` message condition.	Check for the existence and order of the r3frstart condition in the `opcmsg` template. Check whether the message appears in the message browser after confirmation of the selected SAP system. In the message details, check the status of the automatic action.

Table 10-1 Checking Communication Problems (Continued)

Stages	Problem	Check
13, 14	OVO agent is not running on the management server. The shell script `opcsapstart` cannot be started.	On the management server, execute: **`opcagt -status`** On the management server, execute: **`/opt/OV/lbin/sapspi/sapgui/\`** **`opcsapstart <hostname>\`** **`<instance_number> <SID>`**

Common SPI for SAP Problems

SPI for SAP related problems could fall into one of the following areas:

SPI Product Cannot be Installed

- Check which management server components or managed node components cannot be installed.
- Check whether installation prerequisites have been met (both for the management server and managed nodes). Refer to the *HP OpenView Smart Plug-in for SAP Installation Guide*.
- Verify if the installation steps have been correctly executed. Refer to the *HP OpenView Smart Plug-in for SAP Installation Guide*.
- Verify that the product has already been installed (either on console or managed node).

Distributing SPI for SAP Software to an MS Windows Node Aborts

This is caused by a sharing violation in the following directory:

```
\usr\OV\bin\OpC\intel\monitor\cmds
```

You must ensure that no other process is using this directory on the node. To do this, close the MS Windows Explorer and the command shell on the managed node to which you want to distribute the SPI for SAP software.

Configuration Files Cannot be Edited

If you get an error message when you try to edit a configuration file using one of the applications in the `SAP R/3 Admin` or `SAP R/3 Admin Local` groups, this is probably because you have not distributed the SPI for SAP software components to the management server and nodes. Refer to the *HP OpenView Smart Plug-in for SAP Installation Guide*.

R/3 Service Discovery Fails on some Managed Nodes

If the `R/3 Service Discovery` application fails to collect the information it needs for a given host, the host will not appear in the SPI for SAP service tree. However, you add the missing information by hand and create the `SapSpiServices` file as follows:

1. For each managed SAP node whose service-discovery information is missing from the `SapSpiServiceDiscovery` file, log into the managed node and execute the following command. Enter:

   `/var/opt/OV/bin/OpC/cmds/r3sd`

   The `r3sd` command writes the information you need to `stdout`. The result should be similar to the example shown in Example 10-1.

Example 10-1 Example Output of the r3sd Command

```
{
[R3Instance]
Hostname=sapper
HostnameGUID=
SystemName=AST
InstanceName=DVEBMGS00
Number=0
Release=40B
DBName=AST
DBHostname=sapper
Process=Dialog
Process=Update
Process=Enqueue
Process=Batch
```

```
Process=Message
Process=Gateway
Process=Spool
}
```

2. For *each* managed node not *automatically* discovered by the `R3 Service Discovery` command, copy the output of the `r3sd` command (including opening and closing curly brackets {}) into the following file on the OVO management server:

   `var/opt/OV/tmp/SapSpiServiceDiscovery`

3. On the OVO management server, execute the following command. Enter:

   `/opt/OV/lbin/sapspi/r3sm -file \`
   `/var/opt/OV/tmp/SapSpiServiceDiscovery`

   If the program completes successfully, `r3sm` creates the following file, containing the SPI for SAP service tree, which you then upload to OVO, as described in "To Upload the Service Configuration File to OVO" on page 366:

   `/var/opt/OV/tmp/SapSpiServices`

SAP System Up/Down Not Reported Correctly

The symptom of this problem is that a message, reporting that the `r3monup.his` file cannot be accessed, appears in the message browser after each run of the `r3monsap` monitor. It is normal for this message to appear on the first run of the monitor, as the file is created by the `r3moncol` alert-collector monitor on its first run.

If the message continues to appear, this is probably because the monitor is failing to log on to the SAP R/3 system. You should check the environment configuration file (`r3itosap.cfg`) and ensure that the log-on information has been correctly set up.

Note that the SPI for SAP now uses the `r3status` monitor to check the status of SAP R/3. The `r3status` monitor is able to distinguish between the following states:

- a host that is *un*reachable
- a host that is reachable but whose SAP Systems are not available

- a host that is reachable and the SAP Systems are available, but where the specified SAP user could not log in

NOTE

The status monitor, `r3status`, considers an SAP instance as "not available" if the SAP instance being monitored does not respond within 60 seconds. However, this lack of response could be due to a number of different reasons, for example: all available dialog work processes are allocated, or all available SAP gateway connections are busy.

Another problem the SPI for SAP has when trying to determine the status of an SAP instance on a Unix system is that the RFC call can occasionally hang and, as a result, fail to return any information. One explanation for this is a bug in an SAP library. If the SAP GUI cannot connect to the SAP System whose status the `r3status` monitor is attempting to check, then it could be that the RFC call is simply hanging.

The `r3status` monitor can also occasionally report the status of an SAP instance incorrectly, namely; an SAP instance is reported as *down* when it is actually up and available. This is often due to a problem with the `ping` command. To find out if the `ping` command is causing the problem, you should enable tracing for the `r3status` monitor with level 3 and check the trace output in the `r3status.log` file for unusual `ping` entries, for example; the number or packets the ping commands sends and receives is *not* the same.

Duplicate OVO Messages in the Message Browser

You have not suppressed SAP-related messages in the standard OVO `opcmsg` template. The SPI for SAP has its own `opcmsg` template which is installed on managed nodes in parallel with the standard opcmsg template. If SAP-related messages are not suppressed in the standard template, some conditions will be reported by both templates. Refer to the *HP OpenView Smart Plug-in for SAP Installation Guide*.

Performance Monitor out of Synchronization

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. For more information, see "The Performance-Monitor Scheduler" on page 288.

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 whether or not this is the reason the `r3perfagent` Performance Monitor is having. You can do this for one individual remote host, or all (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 286.

Performance Monitor does not Work

If you change the SAP user name/password which the SPI for SAP uses to log in to SAP, you need to make sure that the changes are reflected in the `r3itosap.cfg` and, in addition, that the SPI for SAP components which use the information in the `r3itosap.cfg` are restarted in order to make them aware of the changes.

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. In addition, SAP itself has a security mechanism which prevents further logins from a user who has already tried and failed to login a given number of times. For more information, see "Managing the SAP/Performance Subagent" on page 295.

Work-Process monitor (r3monwpa) ends with an rfc exception

The alert type WP_CHECK_CONFIGURED instructs the work-process monitor, `r3monwpa`, to compare the number of actual running work processes with the number of work processes configured in the current operation mode. If there is no operation mode configured, the work-process monitor ends with an `rfc` exception.

If this `rfc` exception occurs, check that the operation mode is working correctly on each application server in the SAP environment where you have configured `r3monwpa` with the alert type "WP_CHECK_CONFIGURED".

To check the operation-mode configuration:

1. Connect to the affected SAP System
2. Start transaction "rz03"
3. Enter "F7" and check if there are any inconsistencies in the configured operation mode.
4. If you have inconsistency in the operation mode for your application server, disable the alert type WP_CHECK_CONFIGURED for this application server.

Index

D

E

J

K

P

Index