CA UIM for SAP BASIS v5.21
User guide

Last Update: 11th of July 2016

AGENTIL S.A.
rue du Pré de la Fontaine, 19
1217 Meyrin
Switzerland

http://www.agentil.com/

©copyright 2014 AGENTIL – all rights reserved

Table of Contents

1. Presentation 8
1.1. Architecture 8
1.1.1. The probe engine 9
1.1.2. The monitoring library 9
1.1.3. Monitoring schemes 9
1.1.4. Monitoring levels 9
1.1.5. Communication 10
1.1.6. Persistence 10
2. Installation 10
2.1. Prerequisites 10
2.2. Overview 10
2.3. Install the probe on windows 11
2.3.1. Overview 11
2.3.2. Manually importing the probe in the UIM archive 11
2.3.3. Installing the Java JRE for probe user interface 11
2.3.4. Installing the VC 2005 redistributable package 11
2.3.5. Installing the probe package in UIM 12
2.3.6. Downloading and installing the JCO library 12
2.4. Install the probe on Linux 12
2.4.1. Overview 12
2.4.2. Installing the probe package in UIM 13
2.4.3. Install the 3.0.12 SAP RFC library 13
2.5. Install optional transport 13
2.6. Creating the SAP communication user 16
2.6.1. Authorization objects needed by the probe 16
2.7. Adding the message server ports to the “services” file 17
2.8. The license key 18
3. Using the probe 19
3.1. Starting the probe 19

©copyright 2014 AGENTIL – all rights reserved

3.2. Starting the GUI 19
3.3. GUI presentation and usage 20
3.3.1. My SAP Systems 20
3.3.2. The ABAP connector 23
3.3.3. JAVA connector 24
3.3.4. HANA connector 26
3.3.5. Web client connector 26
3.3.6. Create and use templates 29
3.3.7. Monitoring Library 38
3.3.8. Probe setup 43
4. Monitor jobs 47
4.1. Monitor job common definition 48
4.2. Alarms 48
4.3. QoS 49
4.4. Data 50
4.4.1. SAP values and parameters 50
4.4.2. Messages and expressions 50
4.5. Alarm tagging 51
5. SAP instances monitoring 52
6. SAP jobs monitoring 53
7. Process Chains BI 61
8. IDOC exchanges monitoring 65
9. Batch inputs 68
10. SAP updates 71
11. SAP transaction times 73
12. Short dumps monitoring 75
13. RFC destinations monitoring 77
14. Long blocking locks on DB objects 80
15. Dispatcher queues 82
16. Work processes monitoring 84
17. Update service monitoring 87
18. SAP transports 88

©copyright 2014 AGENTIL – all rights reserved

19. Sys log monitoring 89
20. SAPconnect (SOST/SCOT) 91
21. ABAP instance response time 92
22. SAP users 94
23. ABAP instance memory 95
24. SAP buffers 96
25. SAP spools 97
26. QRFC 99
27. TRFC 100
28. Database backups 102
29. Database size 103
30. SAP change settings 104
31. Custom CCMS monitoring 105
31.1. Purpose 105
31.2. Configuration 106
31.2.1. Execution definition 106
31.2.2. Monitoring definition 106
31.3. Execution and tests 117
32. Custom SAP Control monitoring 118
32.1. Purpose 118
32.2. Configuration 118
32.2.1. Execution definition 119
32.2.2. Monitoring definition 119
32.1. Execution and tests 122
33. PI/XI Java messages 123
34. PI/XI ABAP messages 124
35. PI/XI Channels 125
36. PI/XI Consumer caches status 127
37. ICM 128
38. Application logs 129
39. SAP reports 130
40. Hana services status 134

©copyright 2014 AGENTIL – all rights reserved

41. Hana database CPU utilization 136
42. Hana database memory utilization 137
43. Hana database disk utilization 139
44. Hana backups 141
45. Hana connections 144
46. Hana blocked transactions 145
47. Hana threads 147
48. Hana tables 148
49. Hana merge statistics 149
50. Hana alerts 151
51. Hana replication status 151
52. Hana replication shipping statistics 153
53. Hana replication LOG retention 154
54. Create new monitor jobs 155
54.1. Collect new metrics 156
54.2. Create new alarms and QOS 159
54.2.1. Creating a new monitor 160
54.2.2. Creating an Alarm or QOS job 161
55. Configuration 169
55.1. Configuring the general setup of the probe 169
55.1.1. Setting the log level 169
55.1.2. Setting the base Subsystem ID 169
51.1.3 UIM QOS ids 170
55.2. Create and tune Monitoring templates 171
55.3. Assign templates to the SAP systems 171
56. Managing probe updates 171
56.1. How to update the probe 171
56.2. Updates icons 171
56.3. The job update menu 173
56.4. The diff tool 174
56.5. Conflict 174
57. SNC RFC communication 175

©copyright 2014 AGENTIL – all rights reserved

57.1. SNC client folder 175
57.2. Installation of the SNC libraries 175
57.3. Copie of the « License ticket file » 175
57.4. Setting the new variables 176
57.5. Creating the PSE of the SNC client 176
57.6. Creating the SNC client certificate 177
57.7. Importing of the client certificate in the SAP SNC server 178
57.8. Exporting of the SAP SNC server certificate 178
57.9. Importing of the SAP SNC server certificate 179
57.10. Creating the credential file for the SNC client user account 181
57.11. Define the SNC client user in the USRACLEXT SAP table 182
57.12. Setting the SNC in the client JCO connection 182
58. UMP dashboards generation 182
58.1. QOS ids definition 183
58.2. Generate and import dashboards 183
58.3. System dashboard 184
58.4. Default dashboards customization 185
58.4.1. Principle: 185
59. Troubleshooting 186
59.1. Installation 186
59.1.1. 32 bits Java runtime environment installed on a 64 bits system 186
59.2. Instances availability 186
59.3. License problems 186
59.3.1. No license found in GUI 186
59.4. Probe to GUI connection failure 187
59.1. Alarm/QOS not received in UIM 188
59.2. Connection is not working 189
59.3. The probe doesn't seem to start 190
59.4. Monitoring – SAP configuration compliance 192
59.4.1. CCMS path not found 192
59.4.2. CCMS entry "DB KPIs …" not present 192
59.4.3. CCMS entry for Database not present 193

©copyright 2014 AGENTIL – all rights reserved

59.4.4. Instances availability 193
59.4.5. Irrelevant monitoring data 198
59.4.6. Old CCMS entries 199
59.4.1. RFC destination monitoring: 203
59.4.2. Cannot find « SAP updates » metrics in the CCMS 210
59.4.1. CCMS entry for Update Services Status not updated 210
59.4.2. Cannot find Transactional and Queued RFC metrics in the CCMS 210
59.4.3. /SDF/UPDATE_INFO not remote enabled 211
59.4.4. partner '127.0.0.1:3302' not reached 213

©copyright 2014 AGENTIL – all rights reserved

1. Presentation

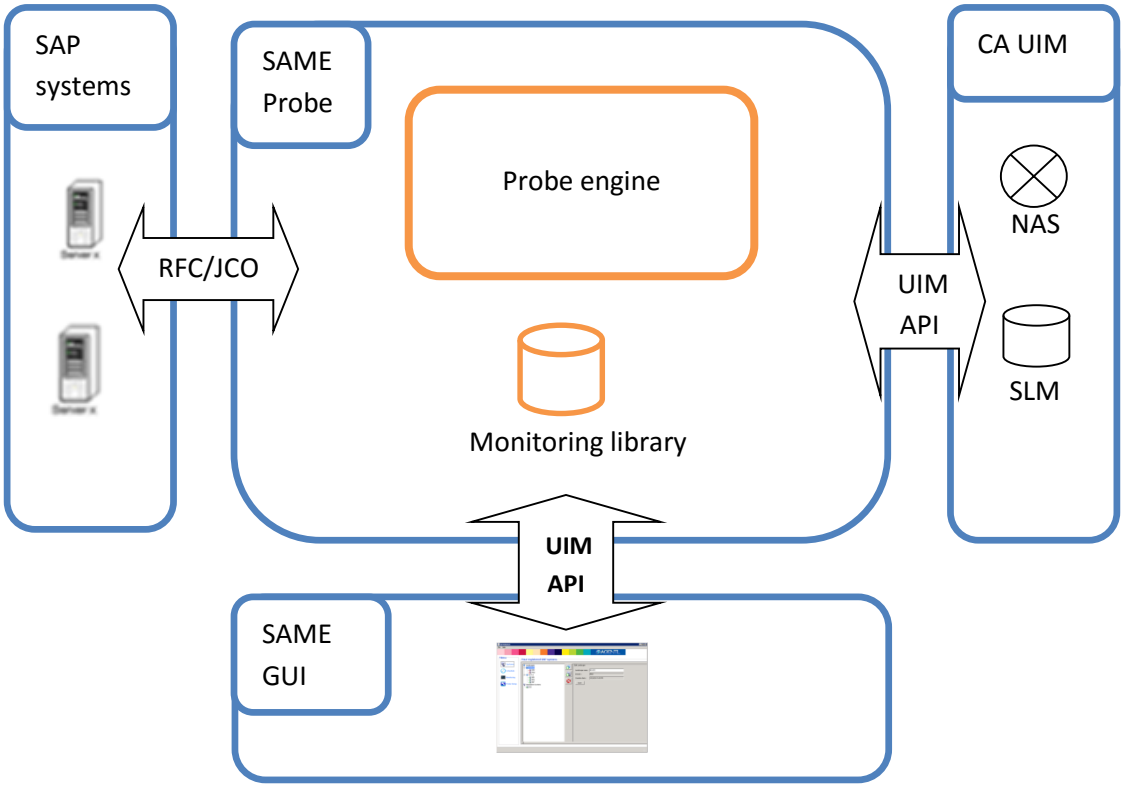
CA UIM for SAP BASIS is an application developed by AGENTIL for the monitoring of ABAP and Java SAP systems.

It has been designed to be easily integrated into CA UIM. Once installed, it will behave as any other regular probe that you can find in the portfolio.

It makes now possible to add SAP monitoring information and events to your unified IT monitoring front end.

The probe features a preconfigured monitoring library that allows deploying the monitoring of several SAP systems in a very short time.

1.1.Architecture



©copyright 2014 AGENTIL – all rights reserved

1.1.1. The probe engine

The engine is the heart of the probe. It executes monitoring jobs loaded from the SAP library. It also handles jobs customization, SAP systems profile setup, SAP data analyze and alarm triggers. It is meant to be integrated in CA UIM. It can be fully controlled and setup through a user interface.

1.1.2. The monitoring library

The monitoring library is loaded in the engine. It contains the definition of the jobs that will be executed in order to monitor your SAP servers.

These jobs, also called "**monitor jobs"**, are grouped by functional scope. These groups are named "**Monitors**".

Monitor jobs are meant to be executed regularly, at scheduled time.

1.1.3. Monitoring schemes

There are three kinds of monitor jobs:

- Alarm jobs will get a particular performance indicator from SAP and process it according to a predefined threshold or formula. It will then fire or clear an alarm in UIM console, depending on the result.
- QoS jobs are meant to build UIM QoS (used in dashboard and SLM). They will get a single performance value from SAP and send it to UIM Monitor, with an eventual pre-processing job.
- Report jobs: Generates an html document reporting the status and health of your systems. It will bring the most important events to your attention.

Each job in the library comes already predefined. You don't have to worry about how to monitor your SAP database or ABAP dispatcher. Just assign the relevant monitor to your system and the monitoring will begin.

The library can be customized via the probe GUI in order to be better adapted to your implementation. It will evolve and get more featured in time. It can be shipped separately from the engine.

1.1.4. Monitoring levels

Monitoring a SAP system will by essence have an impact on it. Resources will be temporarily used by the probe in order to gather information. The monitor jobs provided by the probe will collect different levels of information with different impacts on the systems:

- Basic monitoring: Use consolidated data from the CCMS: Non measurable impact but limited information.
- Advanced monitoring: Provides richer and more accurate monitoring, at the cost of consuming sometimes more resources on the system.

Important note: The probe engine is designed to be robust against glitches in the CCMS module. But if it is filled with incorrect data or stays unavailable for more than 5 minutes, this will have impact on the monitoring.

©copyright 2014 AGENTIL – all rights reserved

1.1.5. Communication

The library is based on the use of RFC calls to monitor ABAP instances, and on SAPControl web service for JAVA instances.

The HANA connector will use straight JDBC interface to connect to the database.

The probe communicates with the system through the Java API.

The GUI communicates directly with the probe using the API also.

1.1.6. Persistence

User settings will be stored in a JSON configuration file. It is loaded at probe engine startup. The probe doesn't use any database, because all collected metrics are already stored by CA UIM in its own database.

2. Installation

2.1. Prerequisites

- Supported OS: Windows server 2003/2008/2012 32/64 bits, Linux Suse, Cent OS, Fedora.
- CA UIM version 5.0 or more
- A Robot to install the probe. CA UIM robot 5.0 or more
- Administrator access to install the needed libraries on the robot (Java JRE, JCO library, C++ libraries).
- Communication open between the UIM robot and SAP: firewall ports opened between the probe and the SAP systems (message server and SAP gateway).
- The memory needs of the probe depend on the number of servers that are monitored. **But the VM must be able to allocate 1GB of memory**. The average footprint for a 10 systems installation is approximately 500MB.
- It is strongly recommended to use the probe on a dedicated server or VM.

2.2. Overview

The first installation steps differ between Windows and Linux, but after that, the procedure is common to both OS:

- OS specific installation
- Install optional transport (**Warning: To be done before creating user role**)
- Create a SAP user for the probe
- Configure windows services file.
- Configure the probe

Important: The probe engine is a java program and needs a Java JRE to be started. You have to deploy the UIM **java_jre (version 6 or above)** probe on the same robot than the SAP probe.

©copyright 2014 AGENTIL – all rights reserved

2.3. Install the probe on windows

2.3.1. Overview

Installing the probe on the selected UIM robot involves completing the following steps:

- Import (or download) the probe in the UIM archive
- Install the Oracle Java Runtime Environment
- Install the VC 2005 redistributable package if not present (only on 2003 and 2008)
- Drag and drop the probe from the UIM archive to the SAP monitoring selected system. This will install the package.
- Install the **3.0.12 SAP RFC library**. Mind the type of OS: 32/64 bits
- Install the probe license in the probe GUI

2.3.2. Manually importing the probe in the UIM archive

UIM for SAP BASIS is delivered as a single ZIP file. You should also be able to download the package automatically from the UIM Web archive. If needed, you can use the following procedure to add the probe package to your UIM server archive.

1. Start the UIM infrastructure manager.
2. Navigate to the archive screen.
3. Right click in the upper right frame and select import.
4. Select the basis_agentil_[version].zip file.
5. Click OK.

2.3.3. Installing the Java JRE for probe user interface

The sapbasis user interface is a Java software. You need to install the Java Runtime environment (JRE) version 1.6 or above on the servers you planned to open the user interface.

Download a copy on http://www.java.com/

If you have a 64 bits system, you have to follow the link "all Java downloads" (http://www.java.com/en/download/manual.jsp) to download a 64 bits version.

2.3.4. Installing the VC 2005 redistributable package

The following only applies on windows server 2003 and 2008:

To connect to a SAP ABAP system the sapbasis probe uses the SAP JCO library. This library depends on the Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. Install it on the host where the probe is installed with the following procedure:

1. Navigate to the following web page:
   http://www.microsoft.com/technet/security/bulletin/MS09-035.mspx

©copyright 2014 AGENTIL – all rights reserved

2. Click the link:
   Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package (KB973544)
3. Scroll to the "Files in This Download" section.
4. Download one of the following platform-specific files:
   64-bit system: vcredist_x64.exe
   32-bit system: vcredist_x86.exe

CAUTION: You must use the KB973544 version. Others versions packages might not be compatible with the SAP RFC library.

2.3.5. Installing the probe package in UIM

To install the probe, use the following procedure

1. In the infrastructure manager, navigate to the archive window.
2. Drag and drop the package sapbasis_agentil on the SAP monitoring system.
3. **Do not start the probe yet, you need first to install the JCO library**

2.3.6. Downloading and installing the JCO library

To communicate with the SAP ABAP systems, the probe uses the SAP Java Connector API: JCO. Install it with the following procedure:

1. Navigate to the following web page:
   https://service.sap.com/connectors (you must have a valid SAP OSS user ID)
2. Navigate to "SAP Java Connector"->"Tools & Services" in the left menu
3. Download the Zip file corresponding the to the latest JCO connector Version 3.0.12 for windows.
4. Unzip the archive.
5. Copy the sapjco3.jar file in the .\lib folder of the probe installation directory. (UIM_INSTALL_DIR \probes\application\sapbasis_agentil\lib)
6. Copy the sapjco3.dll file in the installation directory (UIM_INSTALL_DIR \probes\application\sapbasis_agentil\)

Warning: From probe version 2.5, you must use JCO 3.0.9 version or above

2.4. Install the probe on Linux

2.4.1. Overview

Installing the probe on the selected UIM robot involves completing the following steps:

- Import (or download) the probe in the UIM archive and install it (Same as windows section).
- Install the Oracle Java Runtime Environment (Not described here)
- Install the **3.0.12 SAP RFC library**. Mind the type of OS : 32/64 bits

©copyright 2014 AGENTIL – all rights reserved

2.4.2. Installing the probe package in UIM

To install the probe, use the following procedure

4. In the infrastructure manager, navigate to the archive window.
5. Right click on any package and choose import. Select the package file of the probe.
6. Wait that the probe package is successfully installed and appears in the repository.
7. Select, then Drag and drop the package sapbasis_agentil on the robot hosting the probe.
8. **Do not start the probe yet, you need first to install the JCO library**

2.4.3. Install the 3.0.12 SAP RFC library

1. Navigate to the following web page:
   https://service.sap.com/connectors (you must have a valid SAP OSS user ID)
2. Navigate to "SAP Java Connector"->"Tools & Services" in the left menu
3. Download the Zip file corresponding the to the latest JCO connector Version 3.0.12 for Linux. Mind the 32/64 bits version.
4. Unzip the archive.
5. On Linux 64 kernels, copy the libsapjco3.so file in the /lib64 folder
6. Copy the sapjco3.jar file in the lib folder of the probe installation's folder

2.5. Install optional transport

Because of SAP's client mechanisms for data isolation (000/200/800 etc…), in some cases the probe will only access to the data available in its client of connection.

By example, the user of the probe is connected in client 000, it will not see the jobs running in client 800, and therefore won't be able to monitor them.

The monitor jobs concerned by this restriction are the following:

- SAP jobs
- IDOC
- SAP Connect
- Transports
- Spools

A workaround is to create one connector for each client. The drawbacks are that you need to create several users per systems and it makes the configuration mechanism more difficult.

In order to overcome this problem, an optional transport can be installed. It will make possible for the probe to access data of other clients from its client of connection.

The transport will install a customized version of the function: "RFC_READ_TABLE"

©copyright 2014 AGENTIL – all rights reserved

It will install a new function called Z_AGL_RFC_READ_TABLE. It will have the capability to read cross client data, which is not possible with the standard function.

Note: This transport is optional, you will be able to use all features of the probe without it.

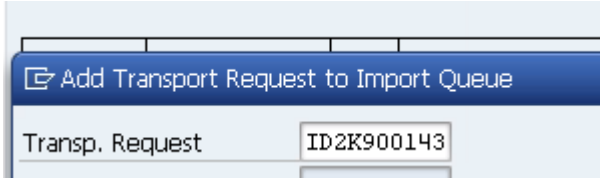
Warning: The transport needs to be installed before installing the user role. If you installed the role before, you will need to re-install it after applying the transport.

In order to install the Z_AGL_RFC_READ_TABLE function, you have to import the request ID2K900133 into the monitored SAP system.

You have to extract the 2 files from the zip file "SAME_ID2K900143.zip" **located in the SAP folder of the probe install root.**

Then copy "ID2K900143.ID2" in the "cofiles" sub-folder of the SAP transport directory and "R900143.ID2" in the "data" sub-folder.

You can now Log-on to the SAP system, run the STMS transaction and add the ID2K900143 request to the import queue of the SAP system:

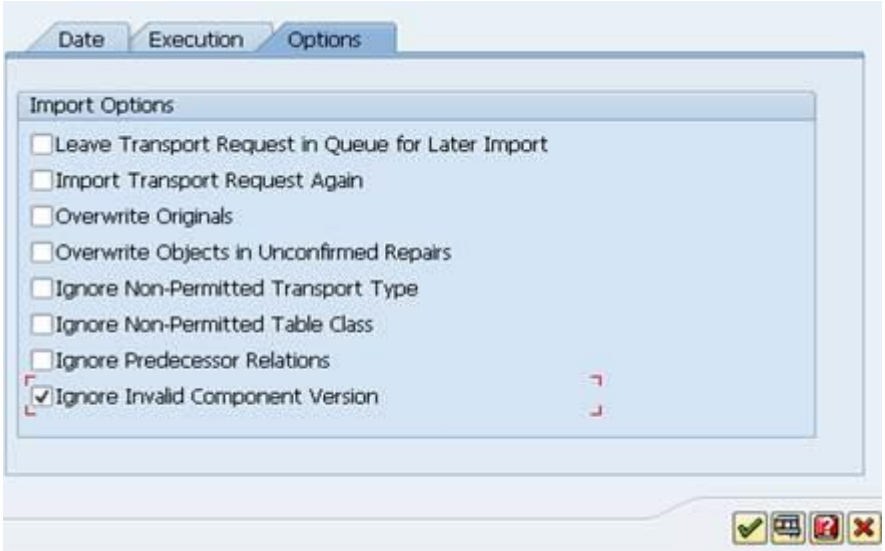


Then when importing the request, it is possible that you receive an error message about component mismatch:

In that case see the detail.

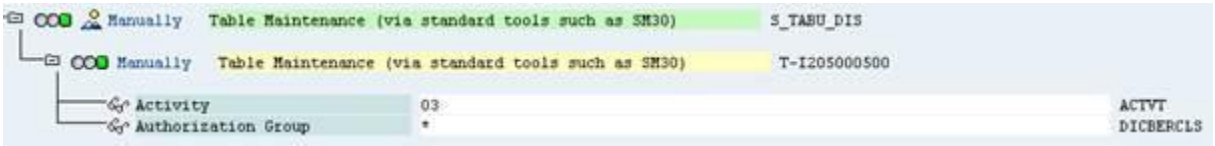
To force the import you will have to select the "Ignore Invalid Component Version" option:

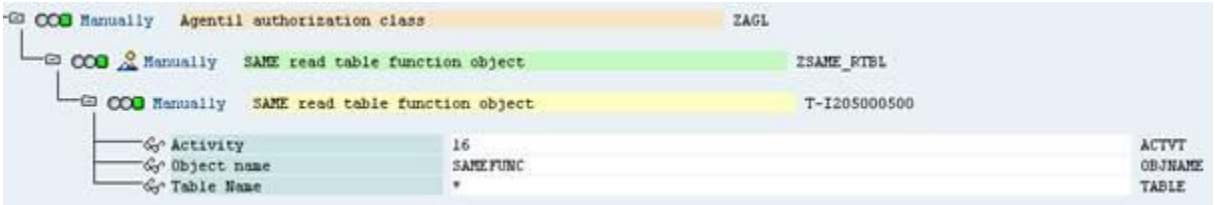
©copyright 2014 AGENTIL – all rights reserved



To run the function, the user profile must contain the authorization objects “S_TABU_DIS” and “ZSAME_RTBL”.

At least, you can design a role with:





Note: You can restrict the access to a list of tables by setting the “TABLE” field of the “ZSAME_RTBL” authorization object.

©copyright 2014 AGENTIL – all rights reserved

2.6. Creating the SAP communication user

A communication user with a restricted authorization profile is required in each monitored ABAP system. Use the following procedure to create it:

Use the supplied ZUIM_SAME_AGENTIL_SAP_PROBE_V5.20.SAP file. This file is located in the probe installation directory. (UIM_INSTALLATION\probes\application\sapbasis_agentil\SAP)

a) Start the PFCG transaction
b) In the menu select Role->upload
c) Select the role file
d) Edit the role
e) Edit authorization data
f) Generate the role

1) Create a system user in client 000 in the SAP environment using SU01 (name it "SAP_PROBE" for example)
2) "Assign the newly created role to the SAP user in the "Roles" tab of the SU01 transaction."

2.6.1. Authorization objects needed by the probe

The authorization profile contains the following objects:

OBJECT	FIELD	LOW	ACCESS REASON
S_ADMI_FCD	S_ADMI_FCD	ST0R	Read uptime with Function Module
S_BTCH_ADM	BTCADMIN	*	Get background job status
S_DATASET	ACTVT	33,A6	Read lock entries
S_DBCON	ACTVT	03	DBA Job & backup status
S_RFC	ACTVT	16	RFC connection
S_RFC	RFC_NAME	/BDL/BDL11	RFC destination check
S_RFC	RFC_NAME	/BDL/BDL3	RFC destination check
S_RFC	RFC_NAME	CTS_WB0_DIS	Read RZ20
S_RFC	RFC_NAME	EDI1	EDI: Processing of one IDoc
S_RFC	RFC_TYPE	FUGR	Read RZ20
S_RFC	RFC_NAME	GET_DB16_INFO	Get Oracle DB info (DBA jobs)
S_RFC	RFC_NAME	IRFC	TRFC_QINS_OVERVIEW
S_RFC	RFC_NAME	ORFC	TRFC_QOUT_OVERVIEW
S_RFC	RFC_NAME	RFC1	Read rz20
S_RFC	RFC_NAME	RSPC_API	Process chains BI
S_RFC	RFC_NAME	RSPC_BACKEND	Process chains BI
S_RFC	RFC_NAME	SADV	Get Oracle DB info (DBA jobs)
S_RFC	RFC_NAME	SALC	Read RZ20, cluster environment
S_RFC	RFC_NAME	SALX	Read RZ20
S_RFC	RFC_NAME	SCA5	DAY_ATTRIBUTES_GET (get working days)
S_RFC	RFC_NAME	SCSM_COLLECTOR	SWNC_COLLECTOR_GET_AGGREGATES DIA response time
S_RFC	RFC_NAME	SDB6DIAG	For DB2
S_RFC	RFC_NAME	SDBADIAG	For Oracle
S_RFC	RFC_NAME	SDDO	DD_DOMA_GET call to get RFC dest
S_RFC	RFC_NAME	SDIF	Read RZ20 (previous SAP version)
S_RFC	RFC_NAME	SDIFRUNTIME	Read RZ20
S_RFC	RFC_NAME	SENT	Reports generation
S_RFC	RFC_NAME	SFMSS_CONFIG	Backend: DB Configuration functions
S_RFC	RFC_NAME	SFMSS_DBUTIL	MSSQL DB size info
S_RFC	RFC_NAME	SFMSS_JOBS	MSS_GET_BACKUP_HIST
S_RFC	RFC_NAME	SLC4	Read RZ20
S_RFC	RFC_NAME	SLO2_ALV	Reports generation
S_RFC	RFC_NAME	SMSSDATA	Reports generation

©copyright 2014 AGENTIL – all rights reserved

```
S_RFC      RFC_NAME   SRFC              | Read rz20, secure RFC
S_RFC      RFC_NAME   STD1              | Reports generation on ECC 6
S_RFC      RFC_NAME   STD4              | Reports generation on ECC 6
S_RFC      RFC_NAME   STOR              | Break Down Objects: R3TR Objects
S_RFC      RFC_NAME   STUB              | Read uptime with Function Module
S_RFC      RFC_NAME   SXMB              | Read rz20
S_RFC      RFC_NAME   SXMI              | Read rz20
S_RFC      RFC_NAME   SYST              | Read rz20
S_RFC      RFC_NAME   SDTX              | For RFC_READ_TABLE
S_RFC      RFC_NAME   SPIAGENTALE       | Agents in ALE/IDoc
S_RFC      RFC_NAME   SXBP              | Job status
S_RFC      RFC_NAME   SYSU              | RFC resource administration
S_RFC      RFC_NAME   THFB              | Task handler functions
S_RFC      RFC_NAME   TMW_CLIENT_INTERFACES | Remote Interfaces for CM Server
S_RFC      RFC_NAME   TMW_CHANGEABILITY     | System Modifiability Control
S_RFC      RFC_NAME   ZAGLMON           | AGENTIL function call
S_RFC      RFC_NAME   /SDF/RI_ORACLE    | /SDF/GET_DB12_INFO
S_XMI_PROD EXTCOMPANY AGENTIL           | RFC connection
S_XMI_PROD EXTPRODUCT SAME              | RFC connection
S_XMI_PROD INTERFACE  XAL               | RFC connection
S_XMI_PROD INTERFACE  XMB               | RFC connection
S_RFC      RFC_NAME   SCSM_GLOB_SYSTEM  | SWNC_GET_WORKLOAD_SNAPSHOT function
ZSAME_RTBL ACTVT      16                | AGENTIL function
ZSAME_RTBL OBJNAME    SAMEFUNC          | AGENTIL function
ZSAME_RTBL TABLE      EDIDC TBTCO       | AGENTIL function
ZSAME_RTBL TABLE      TEDS3             | AGENTIL function
S_RFC      RFC_NAME   /SDF/IS_ABAP      | Update service
S_RFC      RFC_NAME   INSTALL           | Execute function INST_EXECUTE_REPORT
S_RFC      RFC_NAME   STUN              | Locks on DB objects
S_RFC      RFC_NAME   TMW_TRACKING      | Transports
S_RFC      RFC_NAME   STPA              | Transports
S_RFC      RFC_NAME   SUNI              | Execute function FUNCTION_EXISTS
S_PROGRAM  P_ACTION   SUBMIT            | Reports RSM13001, RSRFCPIN
S_RFC_ADM  ACTVT      Ext. maint.       | For RFC destinations
S_GUI      ACTVT      61(Export)        | Syslog
S_ADMI_FCD S_ADMI_FCD SM21              | Syslog
S_RFC      RFC_NAME   RSLG              | Syslog ALV style
S_RFC      RFC_NAME   SCSM_MTES_GET     | Load CCMSTreeElements (defined tables)
S_ADMI_FCD S_ADMI_FCD SP01              | Spool data (RSTS0014 ...)
ZSAME_RTBL TABLE      TSP01,TSP02       | Tables for spools
ZSAME_RTBL TABLE      NRIV              | Table for range numbers
S_CTS_ADMI CTS_ADMFCT TABL              | Transport monitor
S_CTS_SADM CTS_ADMFCT TABL              | Transport monitor
S_CTS_SADM DESTSYS    *                 | Transport monitor
S_CTS_SADM DOMAIN     *                 | Transport monitor
S_TOOLS_EX AUTH       S_TOOLS_EX_A      | SAP Transaction time monitor
S_ALV_LAYO ACTVT      23 (Maintain)     | Reports monitor
S_RFC      RFC_NAME   SFMSS_SIZE        | Execute function MSS_GET_DBSZHIST
S_RFC      RFC_NAME   SXMB_MONI         | Execute SXMB_GET_MESSAGE_LIST
S_XMB_AUTH ACTVT      03                | XI
S_XMB_MONI ACTVT      03                | XI Message
S_RFC      RFC_NAME   /SDF/CCMS_TOOLS   | Get system timezone
```

2.7.Adding the message server ports to the "services" file

It is advised to connect to the ABAP instances using the message server load balancing feature. For that, the probe needs to resolve the message server port of each system.

You have two possibilities: You can specify the connection port in the connector settings or use the services file: c:\%SystemRoot%\system32\drivers\etc\services

©copyright 2014 AGENTIL – all rights reserved

If you use the file, you need to add one line per monitored ABAP system.

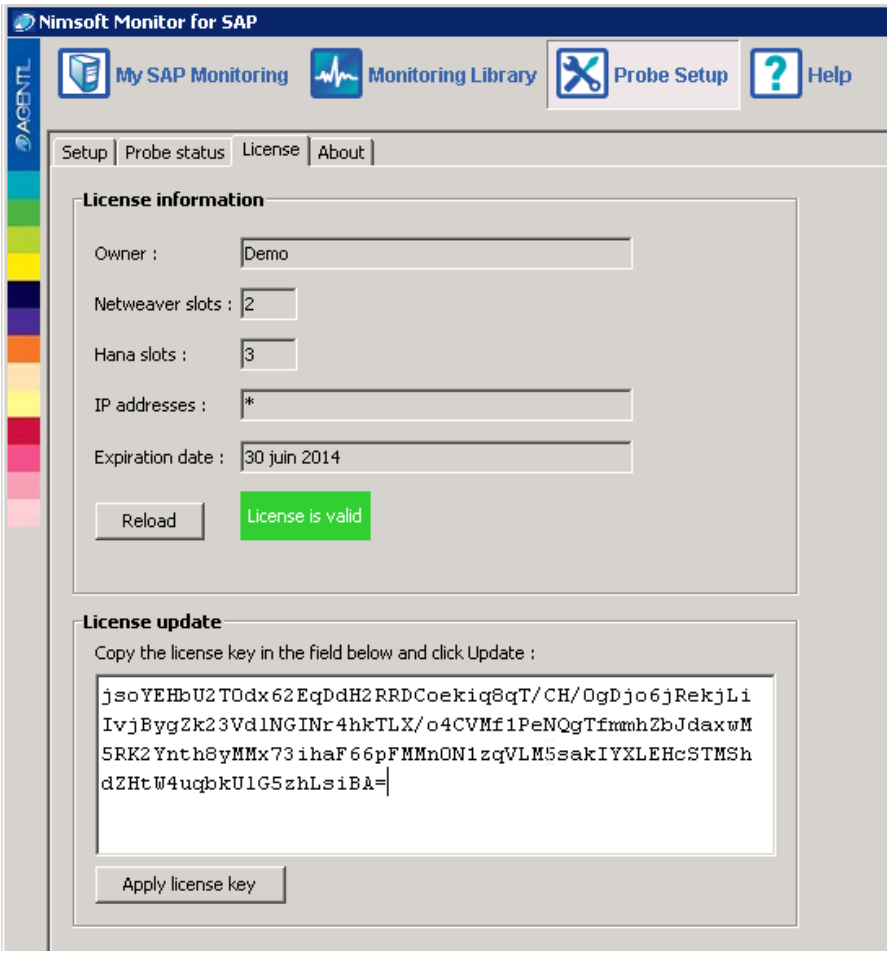
1. Log in the monitored SAP system and start transaction SMMS
2. Click on “goto -> parameters -> display”.
3. The parameters you are looking for are: “server service” and “server port”
4. Add these values to the “services” file. The format of the lines to add is:
   SERVICE PORT/tcp
   - SERVICE is the value of “server service”. (Entries are similar to “sapmsSID”)
   - PORT is the value of “server port”. (This value should be between 3600 and 3699)
5. Repeat for all ABAP servers
6. Save the file and wait for the system to update its internal tables. If it was already started, you may also need to restart the probe for the RFC library to clear its cache.

2.8. The license key

The license key of the product has to be installed in the via the probe’s user interface:

- Open the probe user interface
- In the probe setup tab, go in the license sub menu
- Copy the license key in the license update field and click on the “Apply license” button
- Your license is now installed in the probe. You can see license details in the “license information screen”

©copyright 2014 AGENTIL – all rights reserved



3. Using the probe

3.1. Starting the probe

Once you've installed the UIM package, you need to start the probe engine. From the infrastructure manager, right click on the sapbasis_agentil probe and select "Activate".

The probe icon should turn green. The probe engine will now be running.

NOTE: If you are re-installing a package over an existing one, the configuration file will be kept. User settings and customizations will be recovered from previous installation and applied to the new one.

3.2. Starting the GUI

To start the GUI, double click on the probe in the infrastructure manager. After few seconds, you should see the probe setup panel.

©copyright 2014 AGENTIL – all rights reserved

The GUI will try to connect to the probe engine at startup. If the engine is not running, you won't be able to see your configuration.

The reasons why the GUI might fail to connect to the probe engine can be several. See the trouble shooting section for more information.

3.3. GUI presentation and usage

It has four main sections:

- "My SAP Systems": where you define your SAP systems and your Monitoring templates
- "Monitoring Library": where the monitoring jobs are defined and where you can create new ones.
- "Probe setup": where you can tune probe internal configuration
- "Help": Opens documentation.

3.3.1. My SAP Systems

In this section, you will define the SAP environment and configure the monitoring. Are displayed the list of SAP systems being monitored and the available templates.

You will see two main panels:

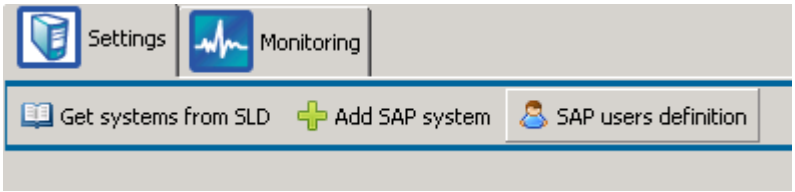
- On the left, a tree that will display systems, templates and jobs organization.
- On the right, the panel will display information about the object selected in the tree.

The right panel will usually have two sub-tabs: "Settings" and "Monitoring". In the first one you configure the definition of the object and in the second, how it is used for monitoring.

User definition

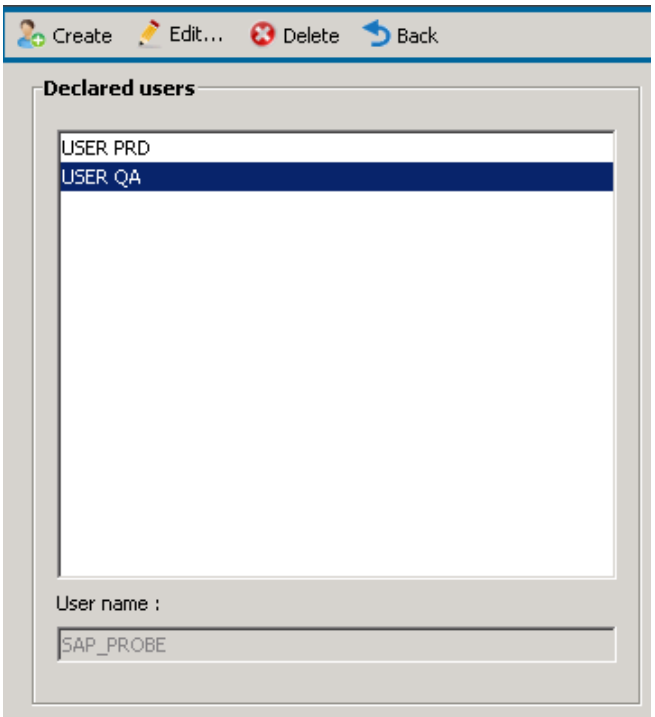
Before being able to connect to a SAP system or database, you need a user profile to be created on the system itself. Once this is done, you need to register this user in the probe. This step is mandatory before being able to create a SAP connector.

Select the SAP system root folder in the left panel and then click on "SAP user definition" button:



You will reach the user definition menu:

©copyright 2014 AGENTIL – all rights reserved



From there you can create new users or edit the ones displayed in the user list.

Warning: If you modify the user name or password of a user profile, it will be directly applied to SAP connectors using this profile.

Once you have defined your user profiles, you can then proceed to the SAP connectors creation.

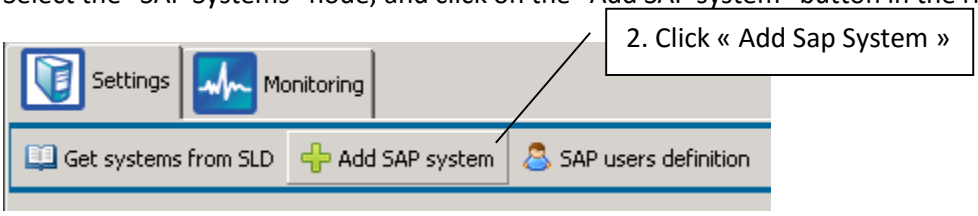
Create a SAP system

There are two ways to define the SAP systems:

- Manually, by setting the connection parameters yourself.
- Automatically, by reading the SAP landscape directory (SLA) and importing the parameters.

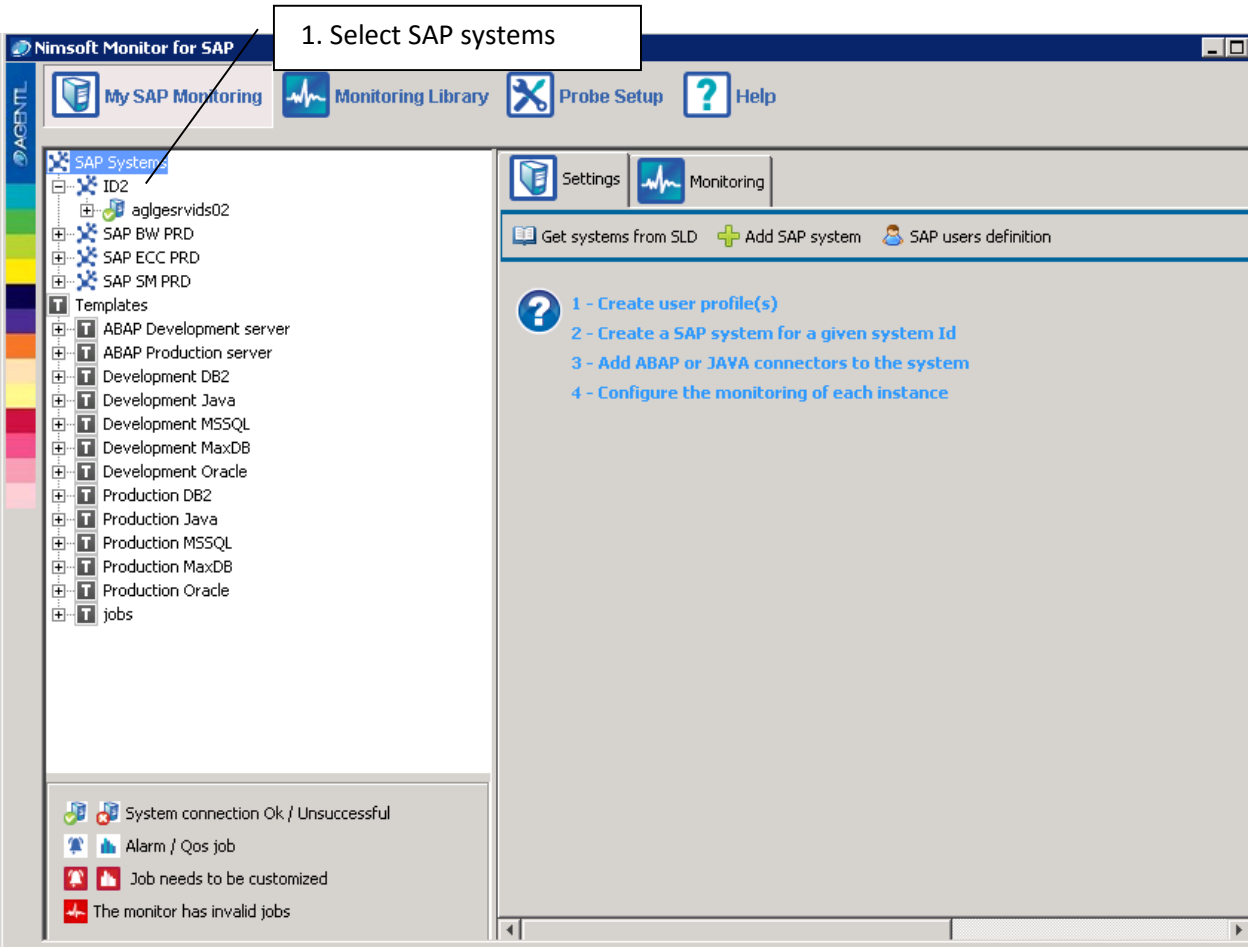
Manual creation

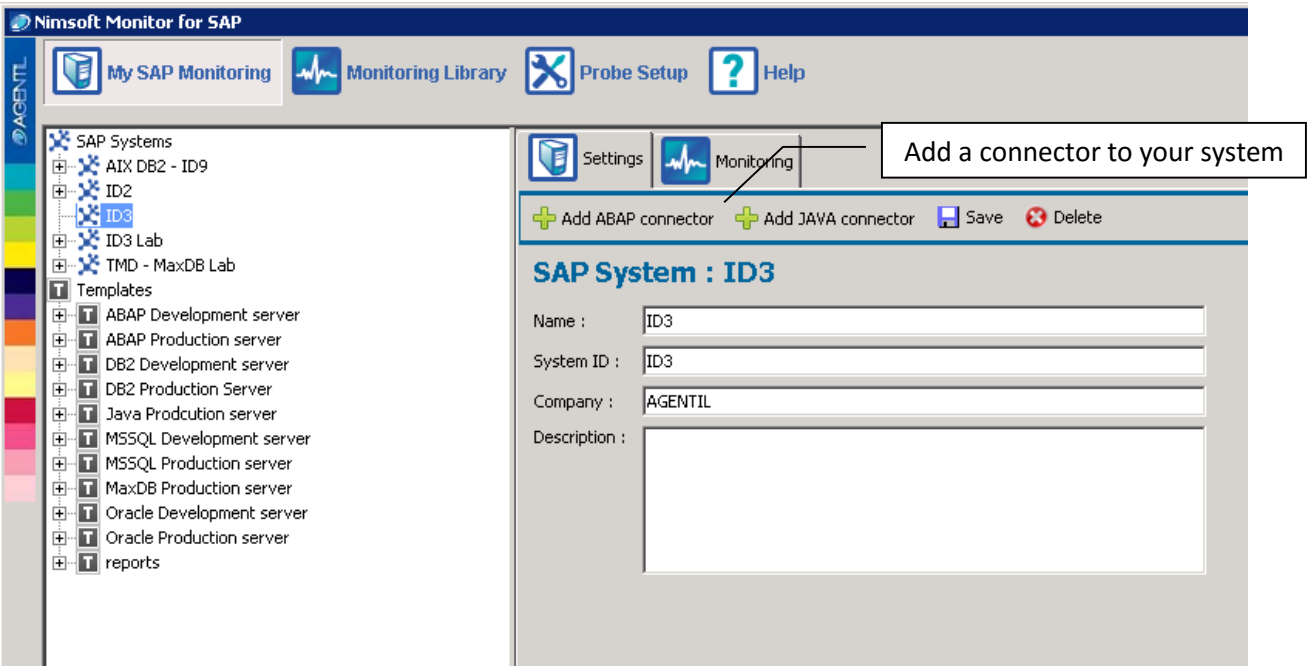
Select the "SAP Systems" node, and click on the "Add SAP system" button in the right panel form.



Then you can create the SAP system profile, which is in fact a place holder for connectors.

©copyright 2014 AGENTIL – all rights reserved





©copyright 2014 AGENTIL – all rights reserved

Once you filled the information, save the profile. The new system profile will appear in the left tree.

Create a SAP connector

The probe is using connectors to define how to connect to a SAP system. There are four kinds of connectors:

- ABAP connector, for ABAP stack instances
- Java connector, for JAVA stack instances
- SAP HANA connector, for the monitoring of HANA databases
- Web client connector for connecting to SAP web portal

Each connector gives access to different kind of information in the system. If you have double stack systems, you need to declare two connectors if you want to monitor both the JAVA and ABAP instances.

3.3.2. The ABAP connector

With this connector, you can define the connection parameters of the message server of your system.

Each connector is bound to a unique set of client-user-password definition. You can create several ABAP connectors if you want to access to the SAP system using multiple users or clients.

You can by example monitor the database with user A and the SAP jobs with user B.

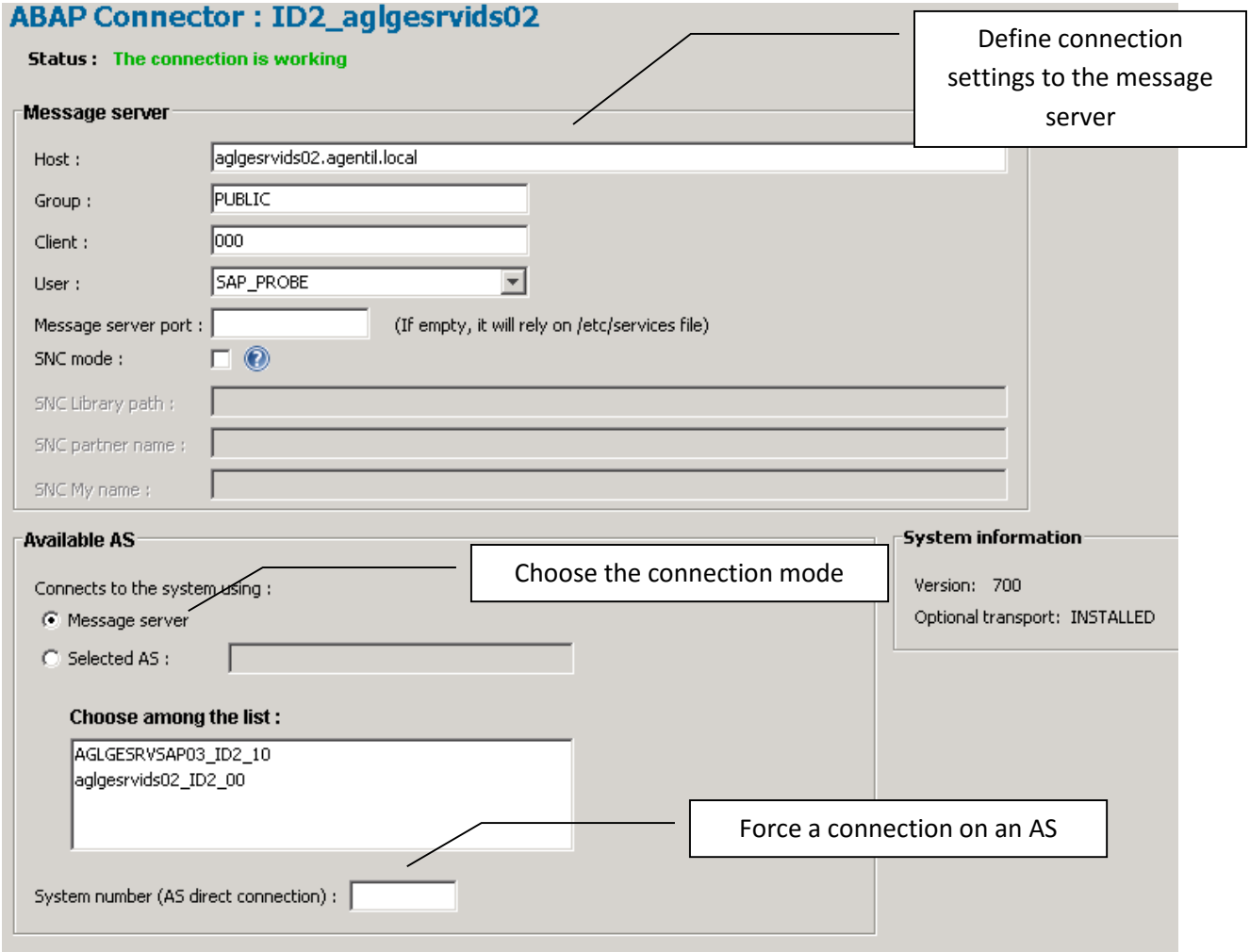
Once the message server is correctly set, you can press the “Save and Test” button. Your profile will be saved in the configuration file and the probe will get the available application servers in the system.

Warning: In order to connect to a SAP system via a message server, the appropriate service must be defined in the windows services file. (See prerequisites section)

Note: You have the possibility to force the connection to the system through one of the available application servers. However, it is recommended to use the message server.

When the definition of your SAP environment is over, you will see its representation in the left panel tree. The display will show the connection status of the connectors that you defined.

©copyright 2014 AGENTIL – all rights reserved



Direct application server connection:

If you want to bypass the message server, you can specify the system number of the application server you want to connect to. The probe will assume that the host of the AS is the same as the one defined in the message server profile.

SNC RFC communication

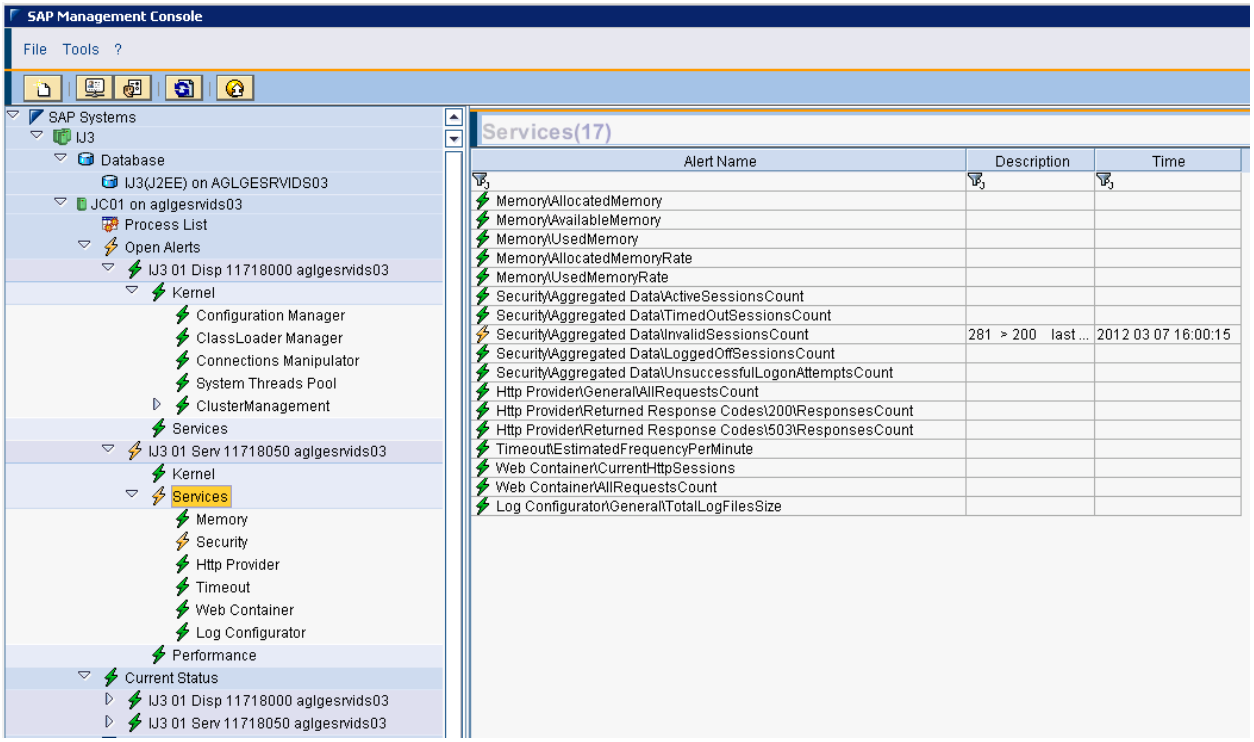
The ABAP connector can be configured to use the SNC mode for RFC communication. A chapter is dedicated to the configuration of such communication at the end of this documentation.

3.3.3. JAVA connector

The java connector allows defining a connection profile to the java SAP management console. With this profile, the probe will be able to extract information through the SapControl web service.

SAP management console *is not* SAP Enterprise Portal:

©copyright 2014 AGENTIL – all rights reserved

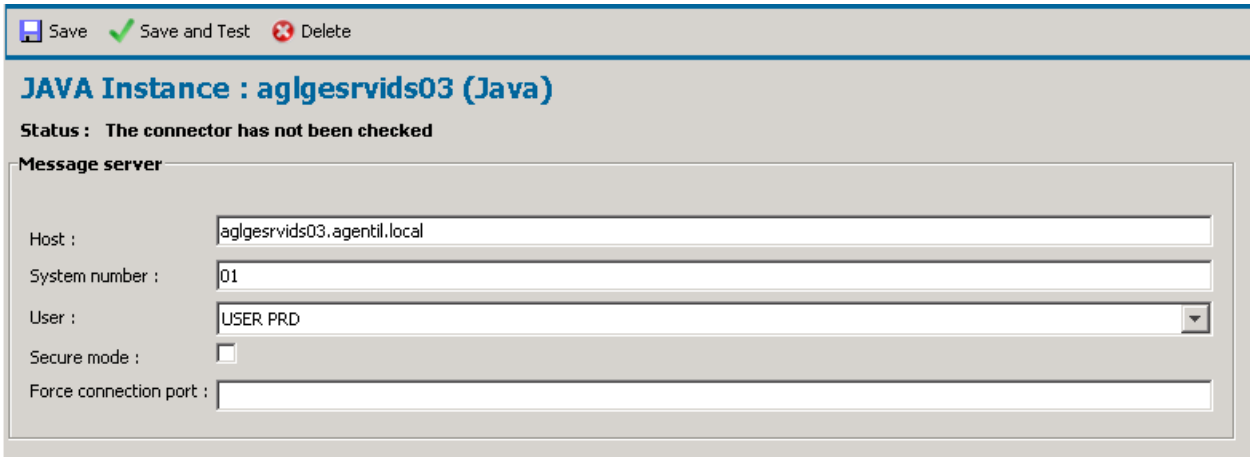


By default, this service is listening on the port *5[system number]13*. If the port has been changed, you can specify the new port number in the profile. Otherwise, it can be left empty.

User and password parameters are necessary only if they are requested to log in the management console.

The “secure mode” checkbox must be selected if SapControl is served through a secured channel (HTTPS).

Note: If your server uses **self-signed certificates**, you need to copy the certificates in the “certificates” folder where is installed the probe.



©copyright 2014 AGENTIL – all rights reserved

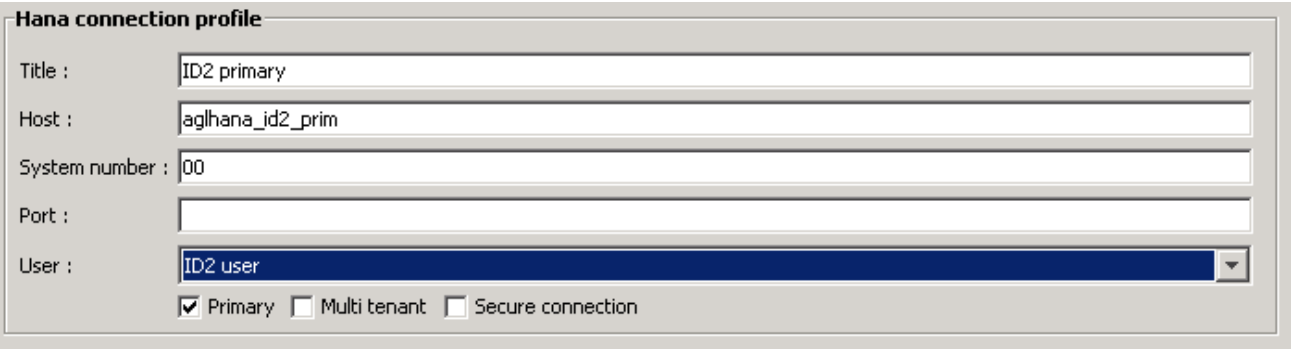
3.3.4. HANA connector

If your license allows SAP HANA connectors, you can create such connector within your SAP system.

But prior creating the connector, a dedicated user has to be added in the database. It will then be used by the connector. You need to register the user credentials in the probe's user menu.

The user must have read access on SYS and SYS_STATISTICS schemas.

Then, press the "Add Hana Connector" button and fill in the form.



Once defined, press the test and save button and check that the connection is working.

If a port number is specified, it will be used for the connection. If not, the connection port will be computed based on the system number (3XX15).

For multi-tenant systems, you can enable the check box. This will have an impact on the name of the source field of Alarms and QOS generated by the probe. If the source to be used by the probe (see probe settings) is the SID, for multi-tenant instances, it will prepend with the connector title: TENANT@SID.

Primary

If the system is replicated, use the primary checkbox to indicate if the system is primary or not.

Note: Only one primary connector is allowed per SAP system.

3.3.5. Web client connector

Web client connectors can be created if you have a license for SAP NetWeaver systems. A Web client connector will give a mean to the probe for getting information from SAP portal.

In order to create a web client connector, you first need to have created the SAP system container of the system you want to connect to. From the SAP system profile, press "Add web client connector" and fill the form:

©copyright 2014 AGENTIL – all rights reserved

The portal connection port will be build based on the System number field: 5XX00. If the portal uses a non-standard port number, you can set it in the port field.

The login URL set by default is the one of the NetWeaver admin panel, because it will request an authentication, allowing the probe to validate the user credentials.

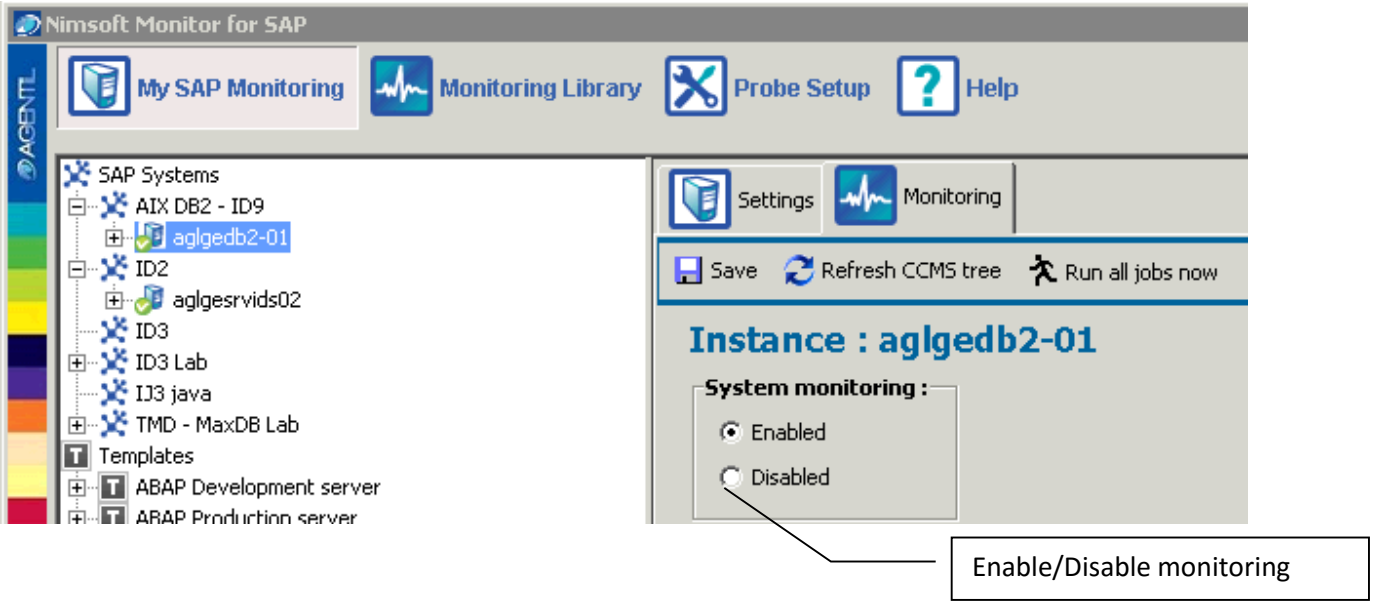
Enabling and disabling the monitoring

To enable or disable the monitoring of one server, select it in the tree panel and toggle the monitoring radio button in the right panel.

By default, newly created servers have their monitoring disabled.

When the connection to a server cannot be established, no monitoring jobs will run on that server. If monitoring is enabled, an alarm will be sent instead, warning about the connection problems.

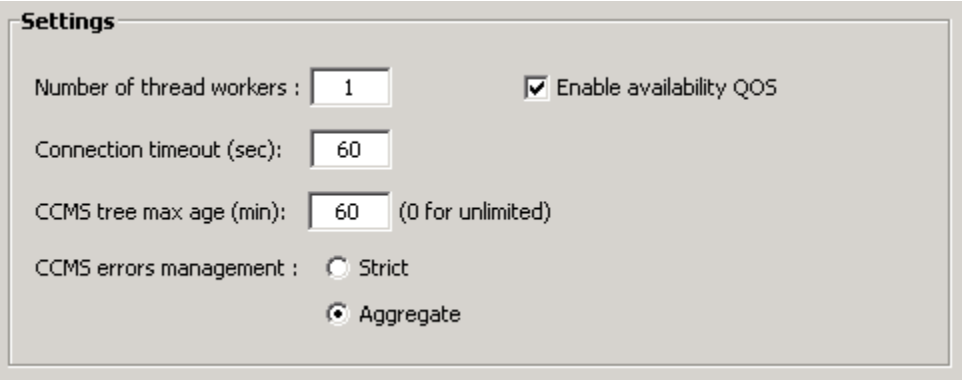
Note: Instance connection availability is checked every two minutes.



System monitoring options

From the monitoring section of a connector, you can tweak few monitoring parameters:

©copyright 2014 AGENTIL – all rights reserved



The number of thread workers: Defines how many probe tasks can read data on the system at the same time.

The connection timeout: Defines the timeout to detect a not responding SAP system

CCMS tree max age: The probe keeps in cache the structure of the CCMS tree. This field defines how often the probe will refresh its cache. Note that only the structure is concerned, not the data.

CCMS errors management: If not properly set, the CCMS can generate various issues, most of the time it concerns not available or not refreshed data. In **Strict** mode, the probe will generate an alarm message each time it meets a problem in the CCMS. In **Aggregate** mode (default), the probe will send a warning alarm only if new errors appeared. The user can then check in the CCMS errors panel to see the details.

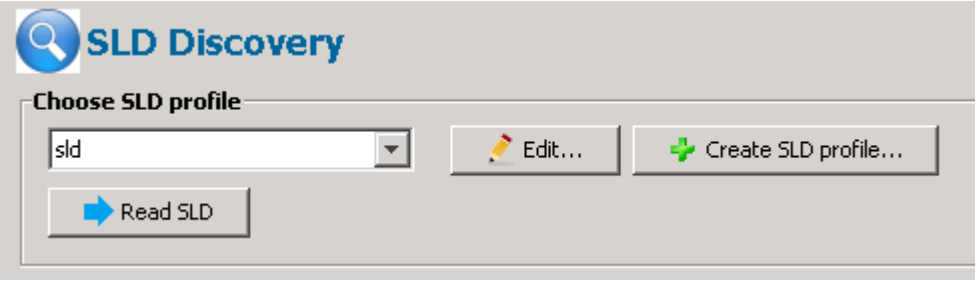
Availability QOS: If enabled, the probe will send a QOS with the value "true" each time a connection to the system works, or "false" if it fails.

Import system settings via SLD

Via the SAP landscape directory, the probe can discover the systems declared in the directory and get their connection parameters.

For that you first need to create a connection profile to the SLD: Select the root of the SAP systems tree and press the "get systems from SLD" button.

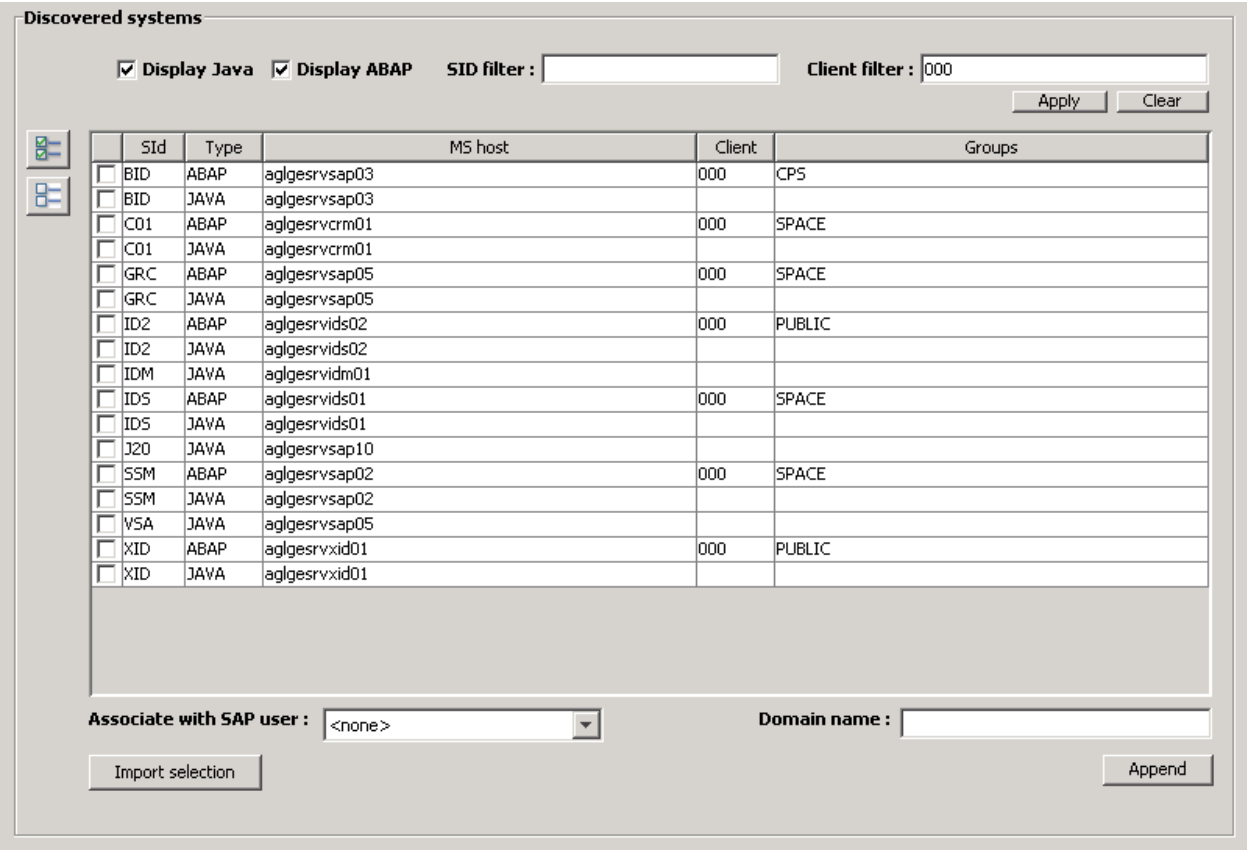
From this screen you can create or edit SLD profiles:



Once the profile is created, you can use it to read the SLD by pressing the "Read SLD" button.

©copyright 2014 AGENTIL – all rights reserved

It will display the list of discovered systems:



SId	Type	MS host	Client	Groups
BID	ABAP	aglgesrvsap03	000	CPS
BID	JAVA	aglgesrvsap03		
C01	ABAP	aglgesrvcrm01	000	SPACE
C01	JAVA	aglgesrvcrm01		
GRC	ABAP	aglgesrvsap05	000	SPACE
GRC	JAVA	aglgesrvsap05		
ID2	ABAP	aglgesrvids02	000	PUBLIC
ID2	JAVA	aglgesrvids02		
IDM	JAVA	aglgesrvidm01		
IDS	ABAP	aglgesrvids01	000	SPACE
IDS	JAVA	aglgesrvids01		
J20	JAVA	aglgesrvsap10		
SSM	ABAP	aglgesrvsap02	000	SPACE
SSM	JAVA	aglgesrvsap02		
VSA	JAVA	aglgesrvsap05		
XID	ABAP	aglgesrvxid01	000	PUBLIC
XID	JAVA	aglgesrvxid01		

You can select the systems that you want to declare in the probe.

Note: You will still need to declare and assign the SAP user profile to use with each system. Before importing the selected systems, you can assign a user to them via the users combo box. Of course user profiles would have to be created on the systems prior to be able to connect.

If the systems that you import are going to use different username/password, you need to repeat the import operation several times.

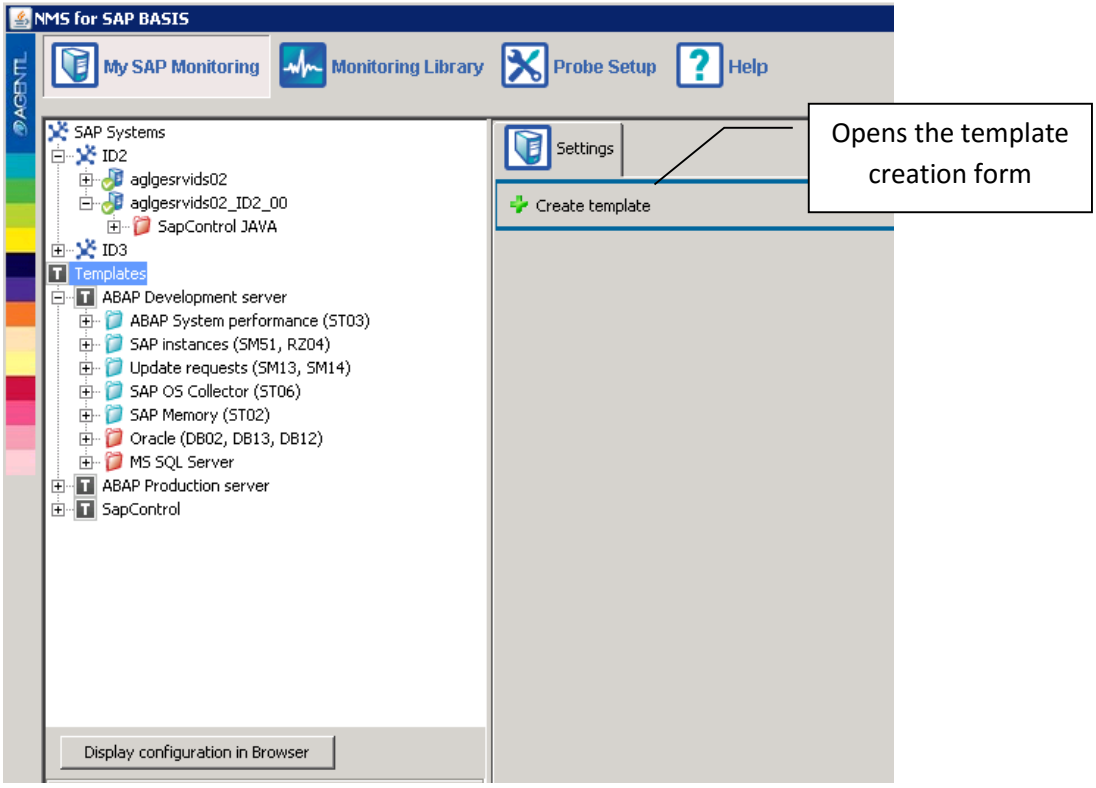
Before importing, you can also append a domain name to the system host names using the “Append” button. This can be useful as the probe won’t usually be in the same network domain than SAP systems.

3.3.6. Create and use templates

Templates are displayed under declared SAP systems in the left tree panel. They provide a mean to define one or several monitoring profiles that can be applied to your SAP systems.

To create a template, select the “Templates” root in the left tree panel, then click “Create template”.

©copyright 2014 AGENTIL – all rights reserved

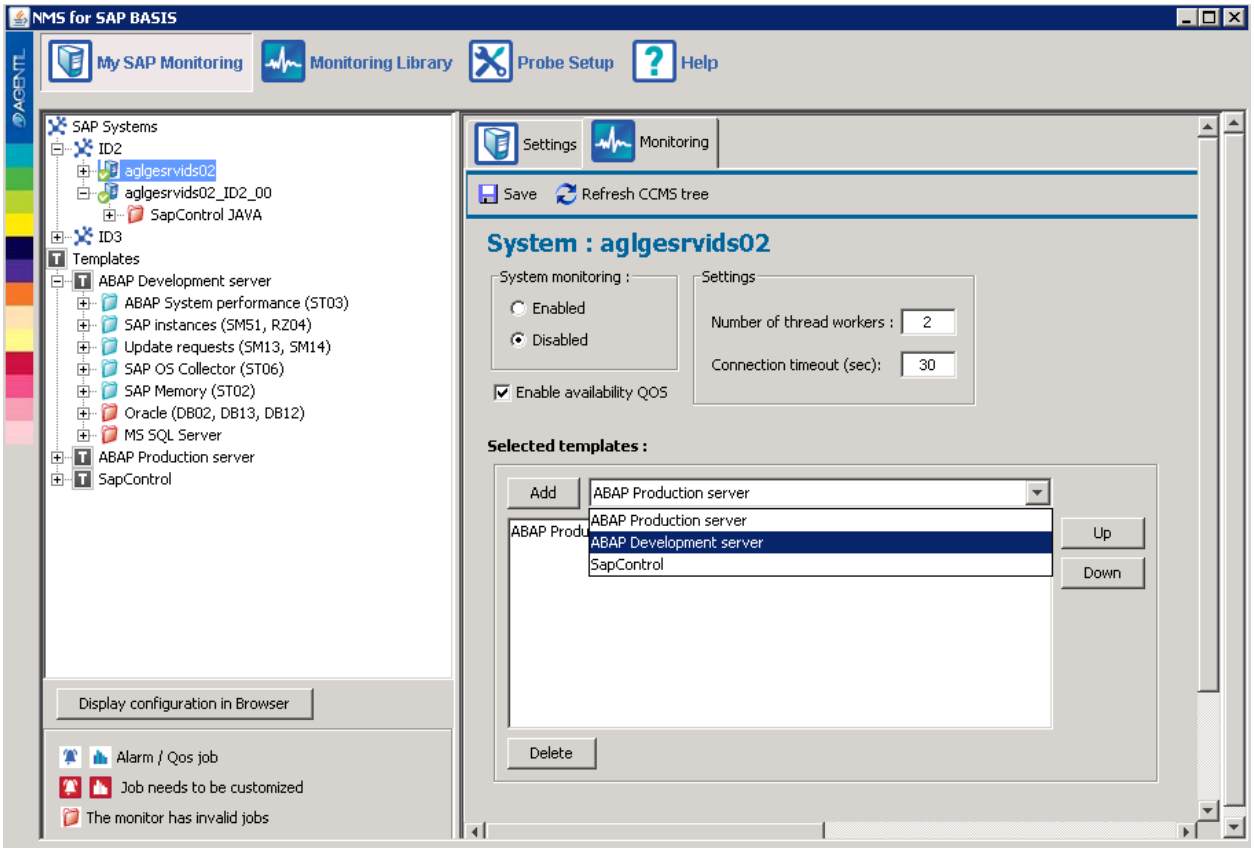


In a template, you define what functional module has to be monitored and how. To do that, you define which monitoring job is part of the template and optionally customize the ones that you need (change threshold, alarm severity, etc…).

Once a template is defined, you can assign it to a system. Then the jobs defined in the template will run on that system, using the customized parameters.

For that, select the system on which you want to apply the template, and click on the “Monitoring” tab. Add your template using the combo box and then click on Save.

©copyright 2014 AGENTIL – all rights reserved



Define once, apply to many

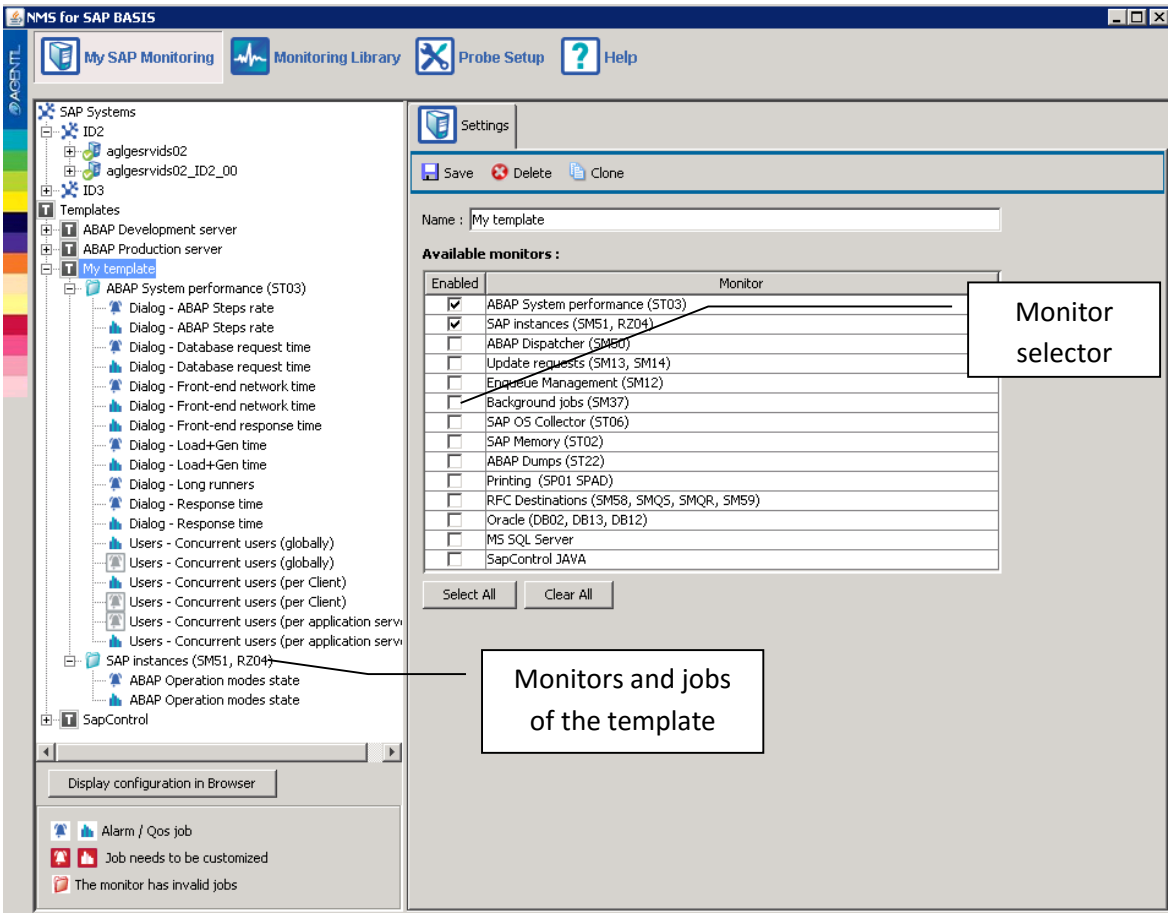
The first goal of templates is to ease the monitoring definition phase. If you have fifteen instances to monitor, you don't want to configure them one by one. They probably have only few different profiles (Production servers and Development servers by example). You can then only define a template per profile and assign it to you systems accordingly.

If a job or a parameter needs to be updated, you can directly update the template. Systems using it will be impacted by your change directly.

Template definition

In order to define a template, you first have to choose which monitors you want to add. From the "Create template" form, you can select monitors among the ones available and then save. The monitors you have picked will appear as children of the monitor in the left tree panel.

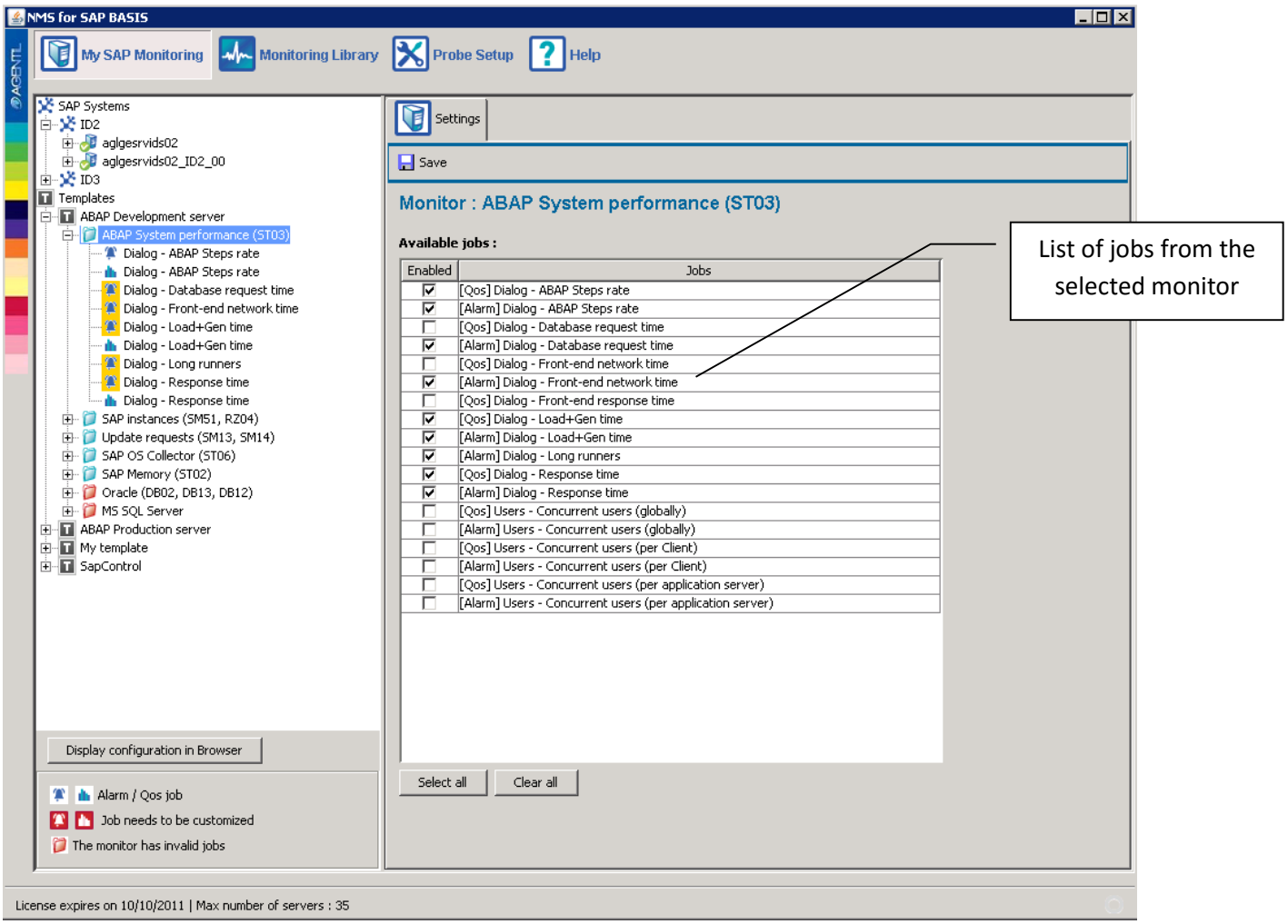
©copyright 2014 AGENTIL – all rights reserved



Once you have activated the desired monitors, you can customize the jobs contained in each. For that, select a monitor in the tree. You will see on the right panel all its jobs.

You can enable or disable jobs using the check boxes. When your selection is done, press the “Save” button. This will update the display in the tree panel.

©copyright 2014 AGENTIL – all rights reserved



Once you have selected the jobs, you can start to customize them.

Job customization can be done at 3 different levels:

- Library level: You want to change the default values.
- Template level: You want to adapt a job to a specific monitoring profile.
- System level: You want to adapt a job to a specific system.

Make sure to make the customization at the right place, it will ease your customization work and its maintenance.

Note that customization is applied in the following order of priority: System level, template level, library level.

The granularity of the customization starts at the job parameter level. The following table shows the out coming customization of job parameters customized at different levels:

©copyright 2014 AGENTIL – all rights reserved

	Job parameter P1	Job parameter P2	Job parameter P3
Library	A	B	Empty
Custo Template T1	(Not changed)	C	(Not changed)
Custo Template T2	E	D	(Not changed)
Custo System S1	(Not changed)	(Not changed)	G
Applied customization	E	D	G

By example:

A job J1 is taken from the monitoring library and added in template T1. You customize the severity of J1 in order to generate a WARNING message instead of a CRITICAL one.

Then in the library, you change the default settings of the job to in order to run every minute instead of every hour.

If you assign T1 to a system, it will run every minute and generate a WARNING message if the alarm condition is met.

Now, if you override the schedule time of J1 in T1 in order to run every five minutes, then it will run every five minutes on the system, still with WARNING message.

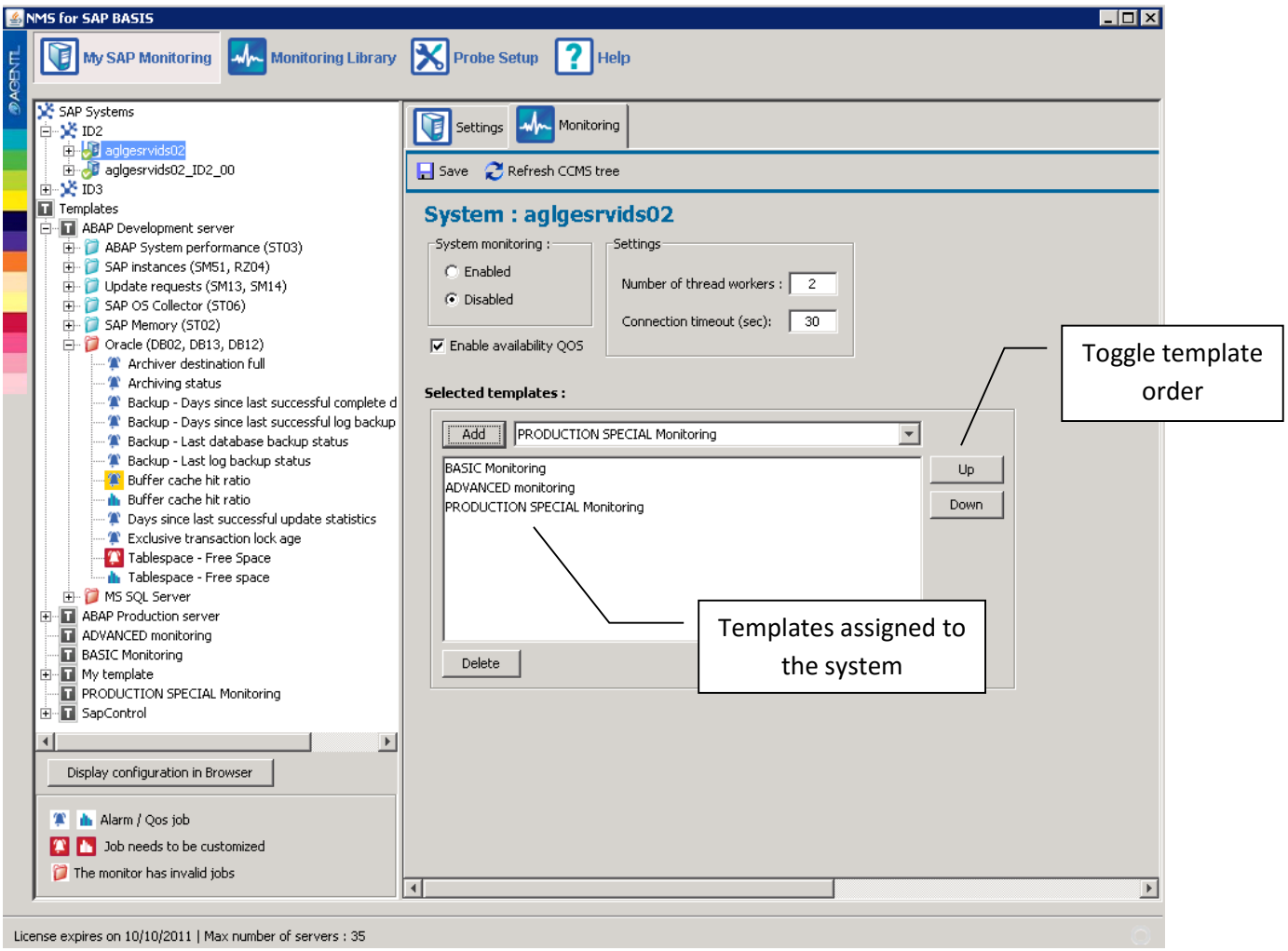
Cascade template

You can assign more than one template to a system, in a cascading manner. You can by example define a basic template that is suitable for a basic monitoring of all you systems. Then you can create an advanced template where you add more jobs, and where you customize more drastic thresholds, that you can apply only to your sensitive servers.

The order in which the templates are added to a system has a great importance. They are applied in their order of appearance in the list, meaning that the customization present in the last template will override the one in previous templates, if there are conflicts.

For instance, a basic monitoring template should be added first.

©copyright 2014 AGENTIL – all rights reserved



When assigning several templates to a system, each job contained in each template will be scheduled. The customization applied will depend on the order of the templates.

Note: A template can only add jobs. You can't create a template that would "remove" jobs defined in templates previously applied. To do that, you have to customize the jobs that you don't want to keep, by toggling the "Enable" parameter of each job.

Job customization granularity

The jobs added in a template can be customized. The granularity of the customization is done at the job parameter level. That means that if you only change one part of the job, it is only the parameters that you changed that will be recorded in the template. The remaining elements that compose the job will stay transparent to a customization done in the library or in another template. **This is crucial to understand.**

Consider the following example:

©copyright 2014 AGENTIL – all rights reserved

T1 = [JOB1 + JOB2]

T2 = [JOB1 + JOB2]

The templates are applied on a system in the following order: T1 then T2. Job customization appears between brackets.

T1	JOB1{state=disabled}	JOB2{Param1 = A}
T2	JOB1 {not customized}	JOB2{Param2 = B}
Result	JOB1{state=disabled}	JOB2{Param1 = A, Param2=B}

The result shows that JOB1 is disabled, even if it is not disabled in T2, which is applied last. It's because T2 did not customized JOB1, so all parameters of JOB1 stayed transparent in T2. Any customization applied at a level before will then be taken into account.

Customize the Jobs

When you activate a monitor in a template, some of its jobs will appear with a red colored icon in the tree panel. These jobs must be customized in order to be able to run.

In some cases, monitor jobs cannot have default values set in the library. This is often because it is too dependent on the customer organization specificities. By example, the threshold of the maximum connected users can't be set by default, as it varies from a company to another.

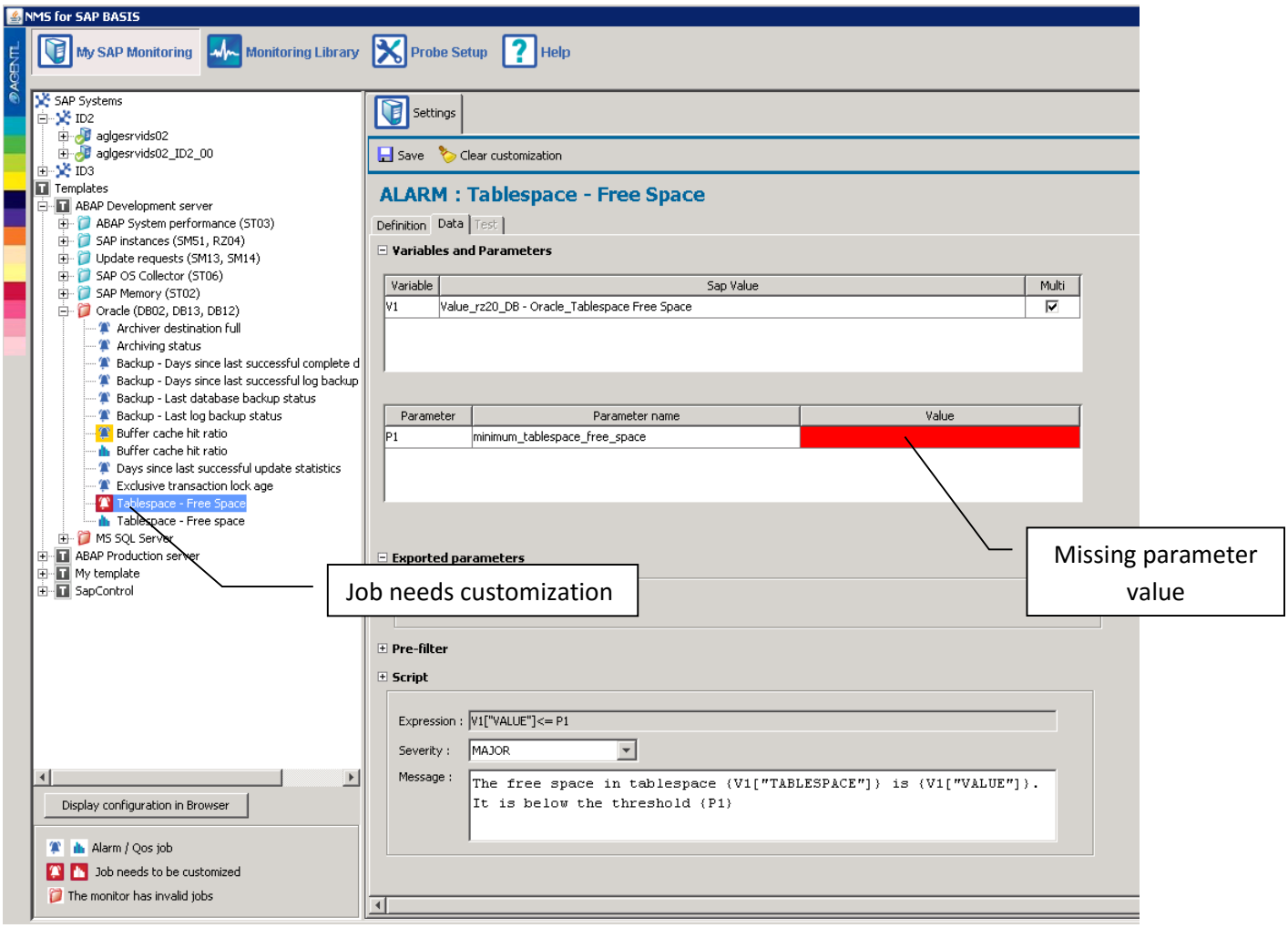
In this case, the action of customizing a job means to open the job definition and to set one or several of its parameters. Most of the time, it is a threshold that needs to be set (empty by default).

Select a job that needs customization in the tree panel. Its definition will be displayed on the right. Select the "data" tab. The panel shows the data section, consisting in defining the SAP data needed by the job, and how these data will be processed.

In the parameter table, you will see the parameters defined in the job, with their associated value. If a parameter has no value, you must set it. See [job customization] section for more information on this topic.

When each parameter has a value, press the "Save" button. You should see the job's icon becoming normal (white and blue) in the tree panel. This is the sign of a well configured job.

©copyright 2014 AGENTIL – all rights reserved



You have to repeat this operation until all jobs are properly set. Note that a red flagged job will not run, but won't prevent other jobs from being executed.

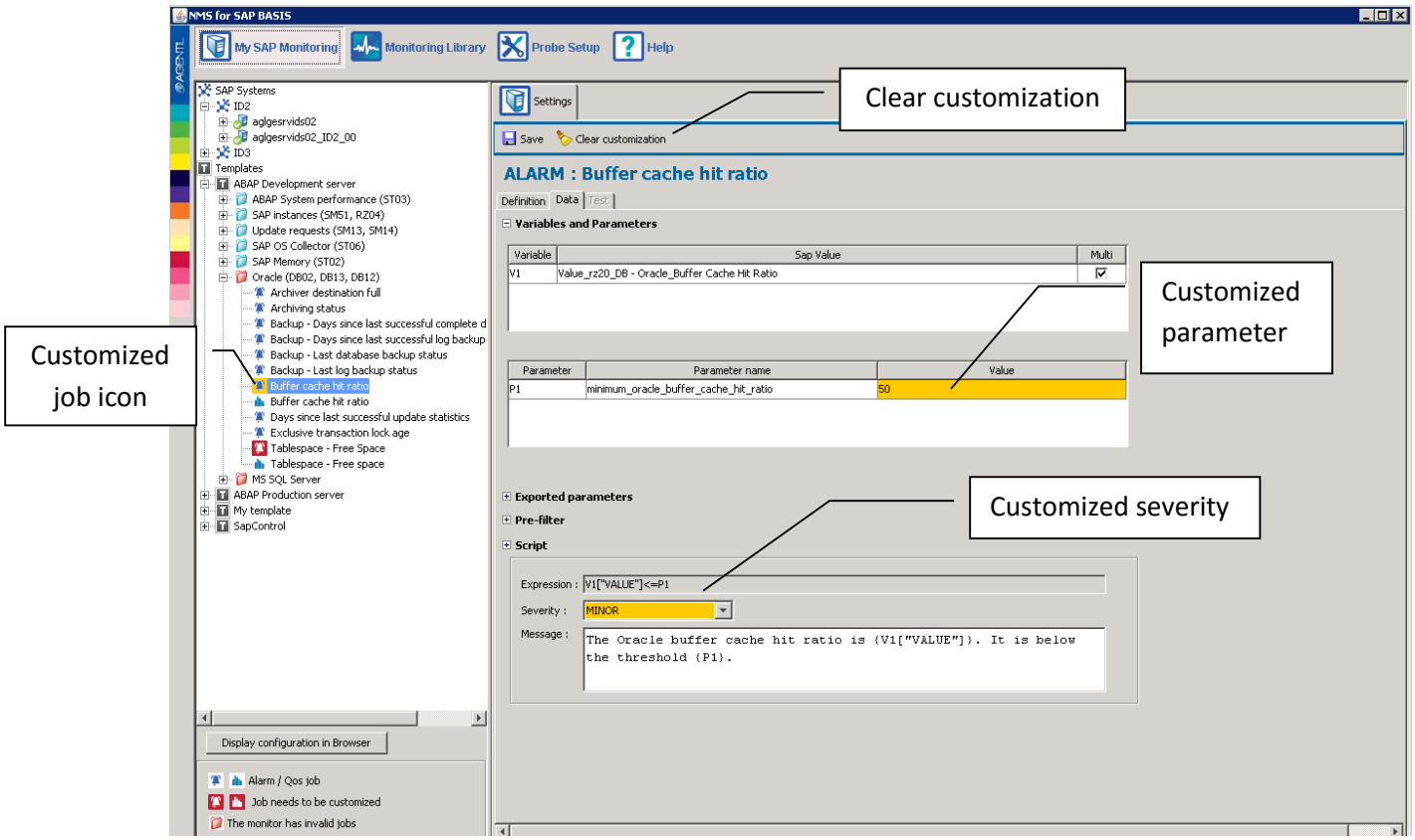
<u>Note</u>: Modifications of the monitoring (enabling/disabling monitors or jobs, customization) will be applied in the scheduler of the probe engine as soon as the save button is pressed**.**

Customization rendering

When you change a parameter of a job that is different than the default value, the background of the parameter and the job icon turns orange. This is to help you to know what has been customized and where.

You can always fall back to the default settings of the job by pressing the "clear customization" button.

©copyright 2014 AGENTIL – all rights reserved



3.3.7. Monitoring Library

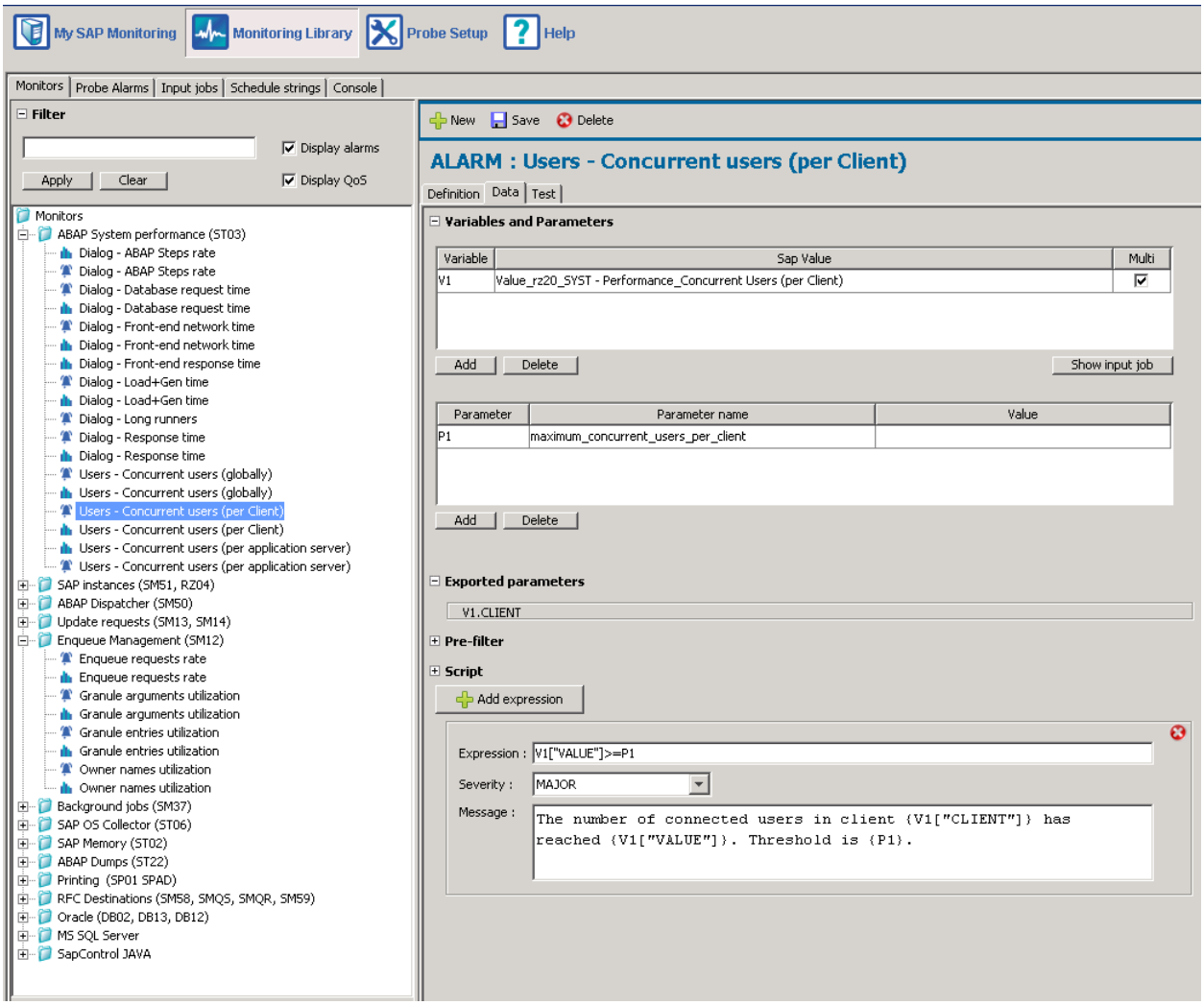
This section contains the definition of the monitoring library. It has five sub tabs: monitors, probe alarms, input jobs, schedules and console.

Monitors

This tab contains two main panels: A tree panel and a form panel.

The tree represents all available monitor jobs, grouped by monitors. The definition of the item that you select in the tree will be displayed in the form panel.

©copyright 2014 AGENTIL – all rights reserved



Probe alarms

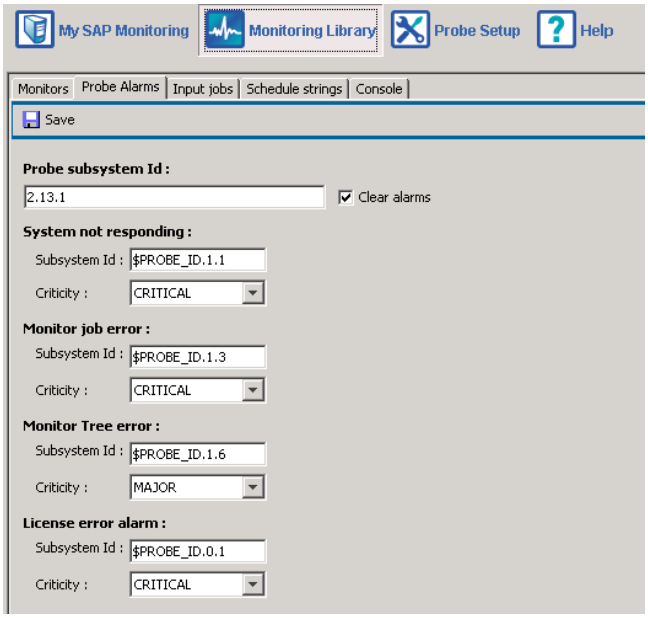
The probe alarms tab displays internal alarms customization.

These alarms will be raised in UIM when the following events occur:

- SAP system not responding
- Monitor job error : A job failed to be processed or failed to get SAP data
- Monitor tree error : The monitor tree of a system could not be loaded
- License error : Your license has expired or there are too many declared systems

For each alarm, you can customize the severity and the subsystem Id

©copyright 2014 AGENTIL – all rights reserved



Input jobs

Input jobs define how to fetch a specific data in a SAP server. They can fetch isolated data as well as bigger structures like tables.

This section is here in the purpose of showing what data is exactly going to be fetched and used by monitor jobs. It is a read only section unless you have the “development” license.

Data fetched by input jobs are used by monitor jobs.

By example:

- Alarm jobs will use data fetched by an input job to compare it to a threshold.
- QOS jobs will use these data (or extract a part of it) to send a QOS message.

An additional container, called “SAP value” can be created out of an input job: Some input jobs can return a large amount of data, SAP value’s role is to act like a pointer that designate a specific data in an input job result.

Monitor jobs defines which SAP data it needs through the use of SAP values. Different monitor jobs using SAP values from the same input job will only make the job to be executed once. This process saves time and resources.

There are four kinds of input jobs:

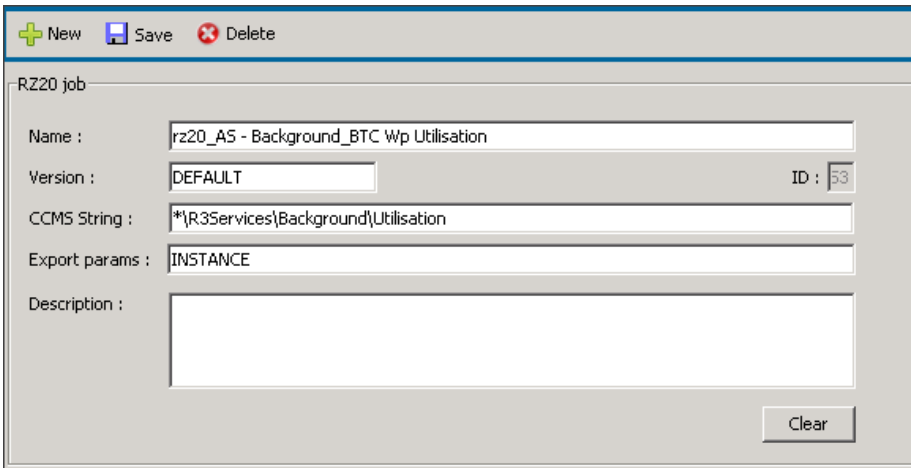
- RZ20 jobs
- RFC jobs
- SapControl jobs

©copyright 2014 AGENTIL – all rights reserved

- Web checks jobs

RZ20 jobs

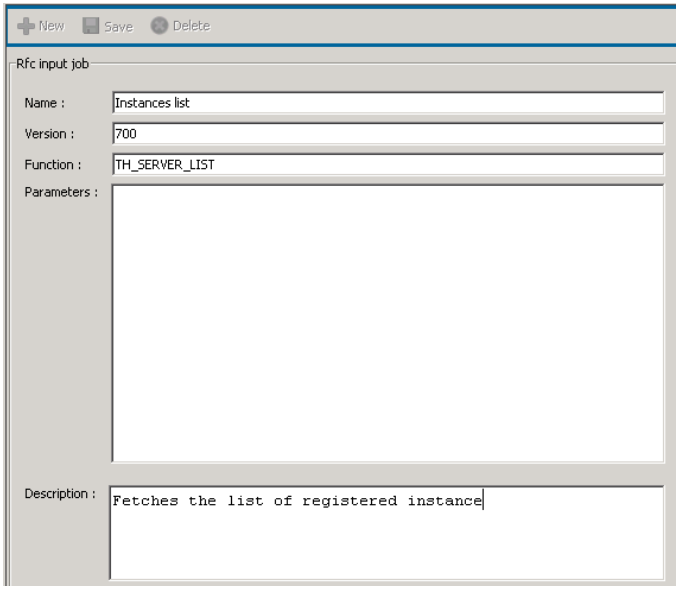
A RZ20 job fetches data from the CCMS tree that you get via the RZ20 transaction. It is mainly identified by its CCMS string, defining a precise node in the CCMS tree to get.



RFC jobs

A RFC job defines a RFC function to execute, with the associated parameters.

Note that this job is not open to be modified.



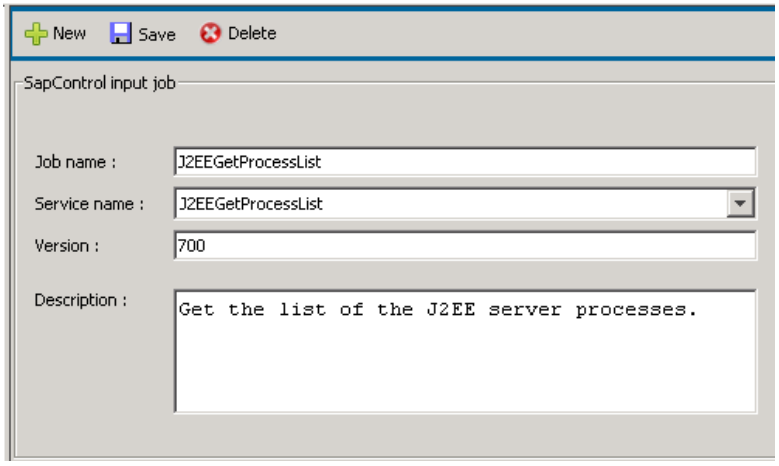
SapControl jobs

SapControl jobs are using the SapControl web service in order to fetch data from a SAP server. Of course, this web service must be available on the targeted SAP server.

The service will be reached at http://[INSTANCE_HOSTNAME]:5[INSTANCE_SYSTEM_ID]13

©copyright 2014 AGENTIL – all rights reserved

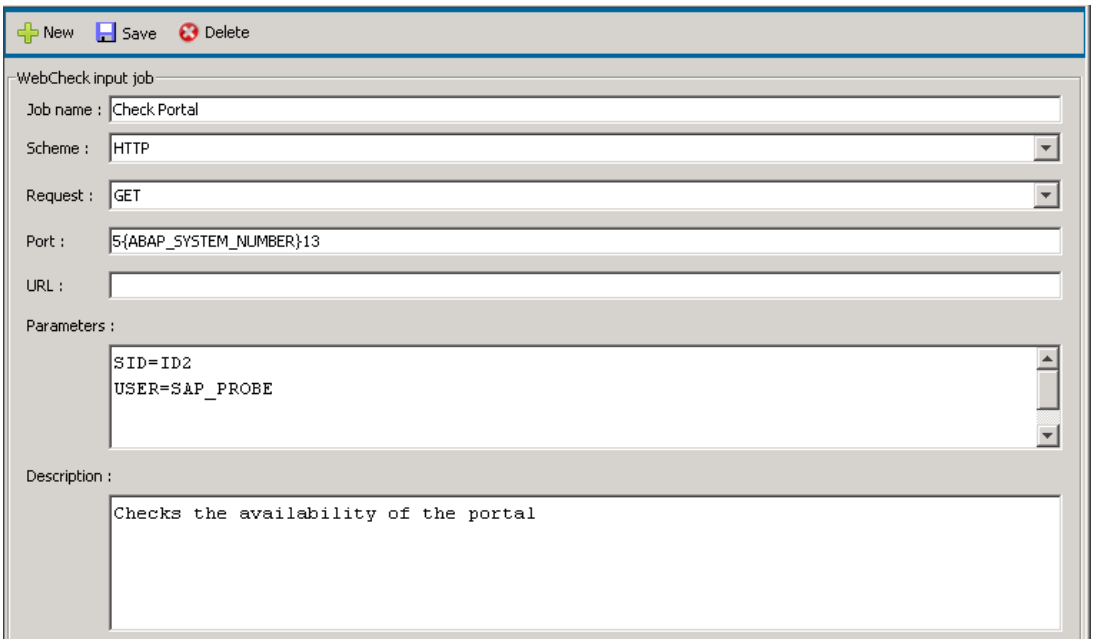
SapControl jobs are limited to the available services provided by SapControl. This can vary from an implementation to another.



Web Check jobs

These jobs are meant for checking the availability of a given URL.

You define the job by setting the scheme, the request type, a port number, an URI and optional parameters. The job will check the status code of the request, the response time and reports errors if any.



Schedule strings

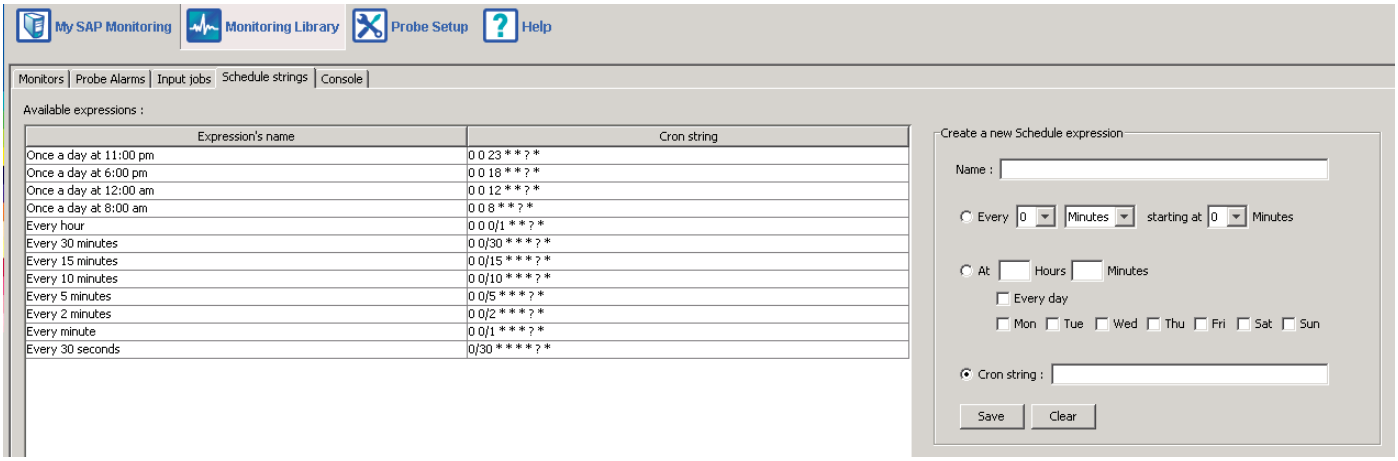
The schedule strings tab allows defining more scheduling possibilities.

©copyright 2014 AGENTIL – all rights reserved

Schedule strings use the well-known CRON format, a fast and powerful way of defining schedules for jobs.

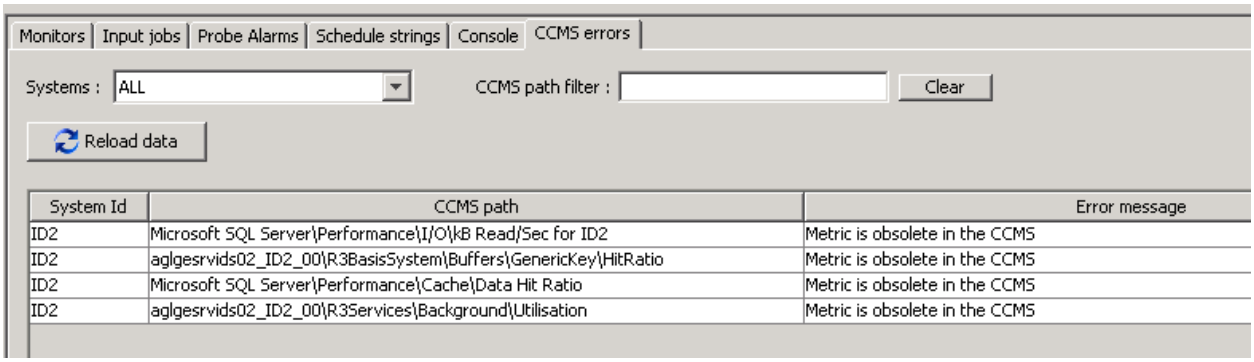
Check here for more information about how to define CRON jobs: http://www.quartz-scheduler.org/docs/tutorials/crontrigger.html

Once you have defined a schedule string in that table, you can use it for any monitor job.



CCMS errors console

This console displays the current CCMS errors detected on the systems. It is an help to quickly identify CCMS data availability problems.



3.3.8. Probe setup

The section has four sub tabs: Setup, Probe status, License and About.

Setup

The setup allows tuning internal probe parameters and configuration:

RFC connection retries: In case of intermittent connection problems, there is a retry mechanism that can take place. You can set the number of retries and the time to wait in-between.

Probe memory: In this section, you can adjust the maximum memory that the probe can use, and set warning and restart thresholds. If these thresholds are set to 0, they will have no effects.

©copyright 2014 AGENTIL – all rights reserved

Probe threads: This parameter defines how many paralleled tasks the probe will use to monitor your systems. The higher this number is, the more cpu and memory the probe will use and the more jobs per minute the probe will execute.

Log level: You can also tune the log verbosity. The debug mode produces large log files and should be used only in specific cases. You can specify the maximum age of log files to keep. The log file is rotated each time that the probe is started.

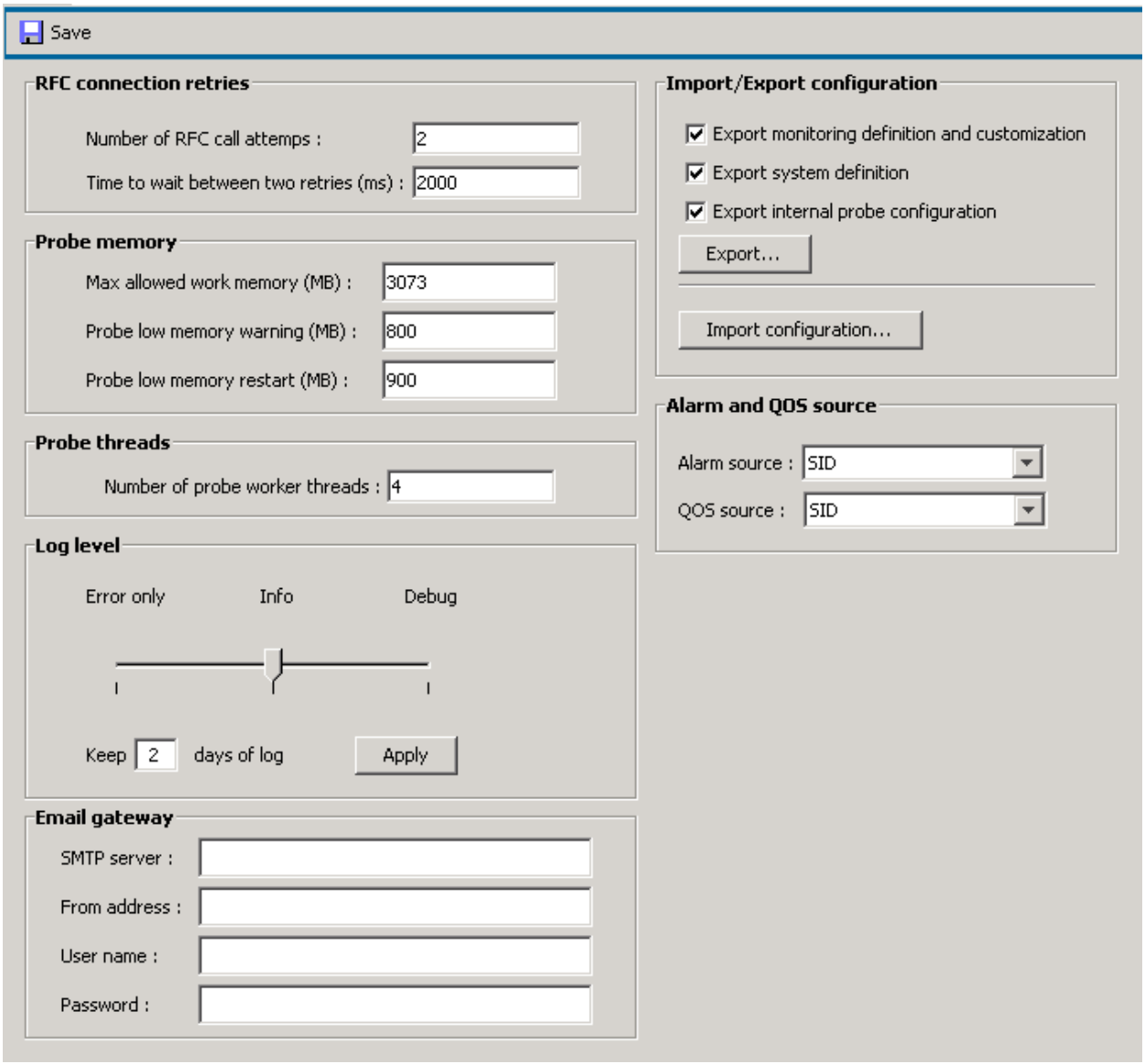
Email gateway: The reporting jobs of the probe can be set to send reports by email. If you want to use this feature, you need to define the SMTP server to use and the FROM address. User and password fields are optional.

Export configuration: It is possible to export partly or completely the configuration of the probe. You can use it for backup, test or to deploy another instance of the probe. These are the different cases :

- If all items are selected, it will export the entire configuration.
- If you select only “Export monitoring definition + customization”, you will export all the customization, the new templates and the default library.
- If you select only “Export system definition”, you will export the connection profiles of the defined SAP systems. The configuration of the monitoring of the systems won’t be exported, neither customization applied at system level.
- If you select both “Monitoring definition” and “System definition”, you will export in addition the configuration of the monitoring of the systems and all system customizations.
- The third box is independent from the others and will include if selected probe internal configuration: The items that you can set in the setup section, internal alarms settings, etc…

Import configuration: You can import in the probe configuration files previously exported. The data that you import will overwrite the existing configuration.

©copyright 2014 AGENTIL – all rights reserved



Memory Consumption

By default, the probe is set to start with a maximum of 1GB of work memory. If you monitor more than 80 servers, it is advised to increase this limit. The recommendation is to allocate 1GB per additional hundreds of systems.

Note: The memory used by the probe's process can be greater than the value set in "max allowed memory" field. It will only limit the size of the java heap memory.

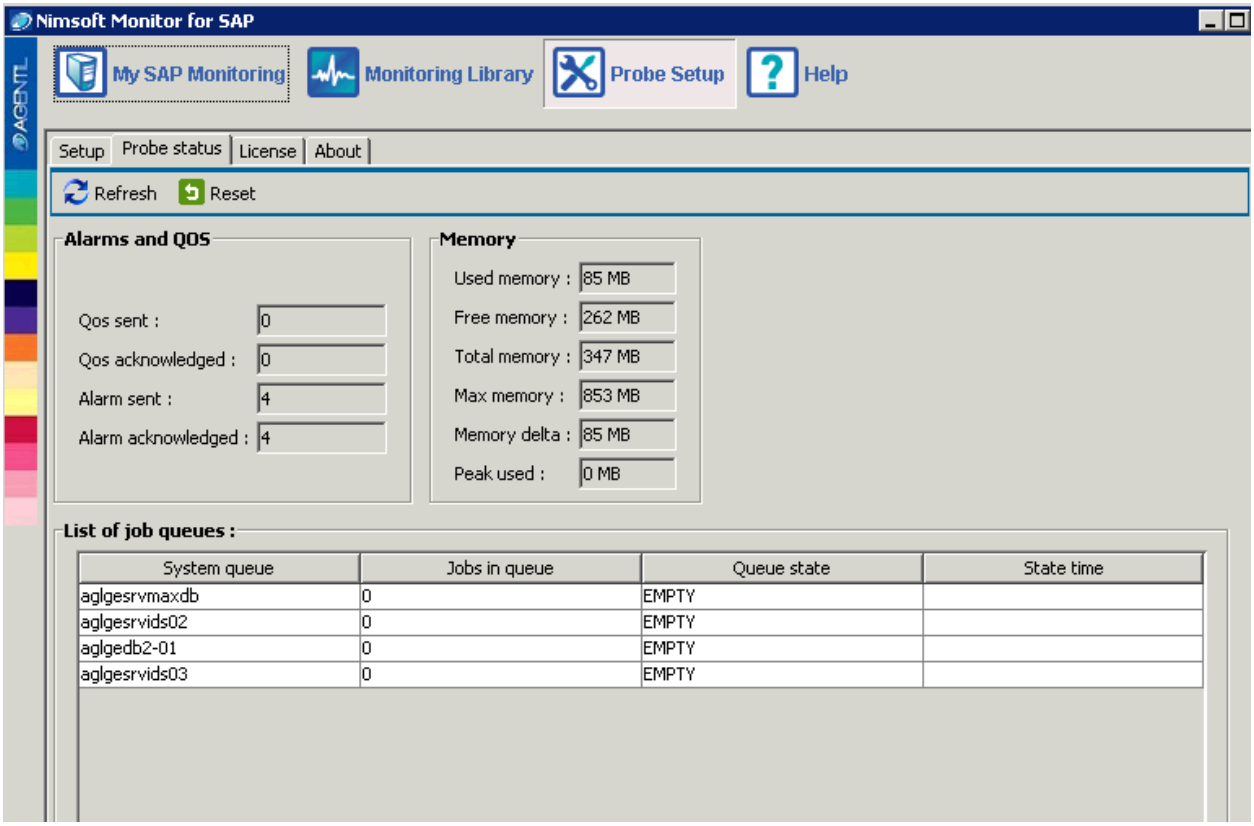
Warning: This field will only be usable for probes running on windows machines. For linux, the starter file sapbasis_agentil_starter.exe has to be manually updated in order to change the maximum allowed memory.

©copyright 2014 AGENTIL – all rights reserved

Probe status

This panel displays information about the general status of the probe. You can read the current memory consumption, as well as the job queues and the amount of Alarms and QOS sent.

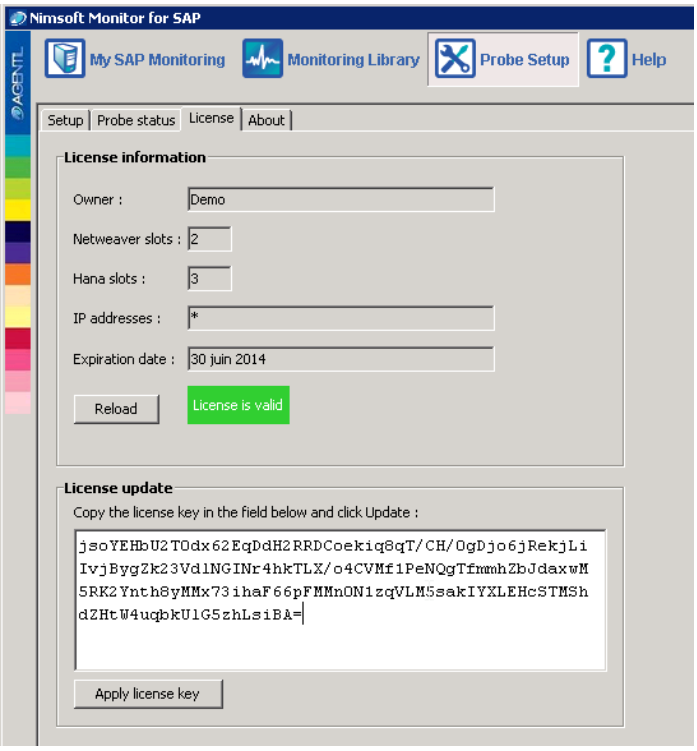
The data are being reset when the probe restarts of if you hit the “Reset” button.



License

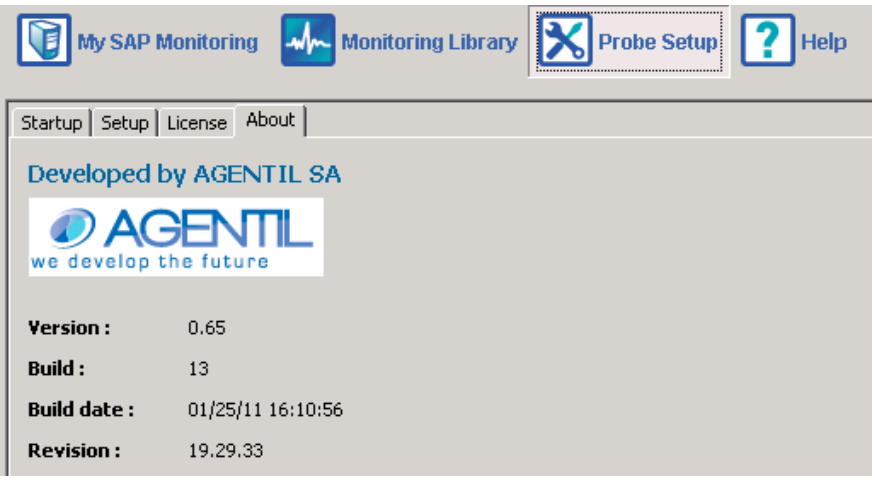
This tab displays the license information and allows setting the license key in the probe.

©copyright 2014 AGENTIL – all rights reserved



About

This tab provides useful information concerning the version of the probe that you are running. The "revision" field should be attached to any customer support requests.



4. Monitor jobs

Monitor jobs are the monitoring tasks executed by the probe. They follow the same principles: The task is set to collect specific information on a SAP system. The collected data is then analyzed and, based on the result, a signal is sent to the monitoring interface.

©copyright 2014 AGENTIL – all rights reserved

The probe can generate two kinds of signals: Alarms and QoS. These are the standard signals used by UIM Monitor probes to provide monitoring information to the central server.

4.1. Monitor job common definition

Some parameters are common in the definition of each monitor job type:

- **Job name**: An explicit name telling what is being done
- **Job state**: A checkbox indicating if the job is active or not. That gives the possibility to disable a job temporarily from the whole monitoring, without removing it from the scheduled monitors.
- **Job schedule**: Defines when the job will run. It is defined using schedule strings.
- **Job expression**: Basically, it defines what SAP data to fetch, what parameters to set and how they are processed. Will be more explained in a latter section.
- **Job description**: A short description of what is being monitored.

4.2. Alarms

Parameters specific to alarms are the following:

- **Severity**: Defines the severity level of the alarm: CRITICAL, MAJOR, MINOR, WARNING, INFORMATIONAL
- **Subsystem**: Mapped on the subsystem id of UIM. See UIM documentation for more information on this parameter. The strings “$monitor_id” and “$probe_id” will be replaced by their actual values when the alarm will be fired. By example, if you set the subsystem like this: “$probe_id.$monitor_id.5” and the subsystem of the probe is 1 and current monitor subsystem is 3, the resulting subsystem of the job will be : 1.3.5
- **Suppression key**: A key meant for jobs that can possibly generate several alarms. This key must be chosen in order to discriminate all alarms generated by a job. This gives the possibility to trigger and clear them independently.
- **Message**: The text message of the alarm that will be displayed in UIM. The string “V1” and “P1” will be replaced by their value according to the expression form. This allows having dynamic alarm messages.
- **Solution**: This field tells possible actions to take when this job fires an alarm. This should help administrator to pin point the problem faster.

©copyright 2014 AGENTIL – all rights reserved

ALARM : Dialog - Database request time

Definition | Data | Test

Alarm definition

Enabled : ☑

Name : Dialog - Database request time

Schedule : Every 5 minutes ID : 20

Subsystem : $MONITOR_ID

SuppKey : {V1["MTE"]}

Descriptions

Description : Average time for processing logical database requests (calls to the SAP database interface)

Solution : Check the database performance using transaction DB02

4.3. QoS

Parameters specific to QoS are the following:

- **QoS type**: synchronous or asynchronous. See UIM documentation.
- **Group**: The name of the group to which the QoS belongs to.
- **Target**: A String identifying what is being monitored.
- **The maximum value** of the sample.
- The **unit** of the value.
- A short string of the unit.

QOS : Dialog - ABAP Steps rate

Definition | Data | test

Qos definition

Enabled : ☑

Name : Dialog - ABAP Steps rate

Schedule : Every 5 minutes

Group : QOS_SAP

Sample Max : 0.0

Unit : steps per second

Unit short : Stp/s

Description : Average number of ABAP dialog steps per minute. A dialog step is the processing used to navigate from one application screen to another. It forms the basic unit of work in an ABAP program.

©copyright 2014 AGENTIL – all rights reserved

4.4. Data

The data section of a job defines what SAP data is needed for the job's purpose and how it will be processed. A system of variables and parameters is used to define SAP data and to give customization capabilities.

These variables and parameters are then used in an expression that will be evaluated at run time. The job will use the result of the evaluation to achieve its goal.

There are 2 main sections helping to define this:

- SAP values and parameters
- Messages and expressions

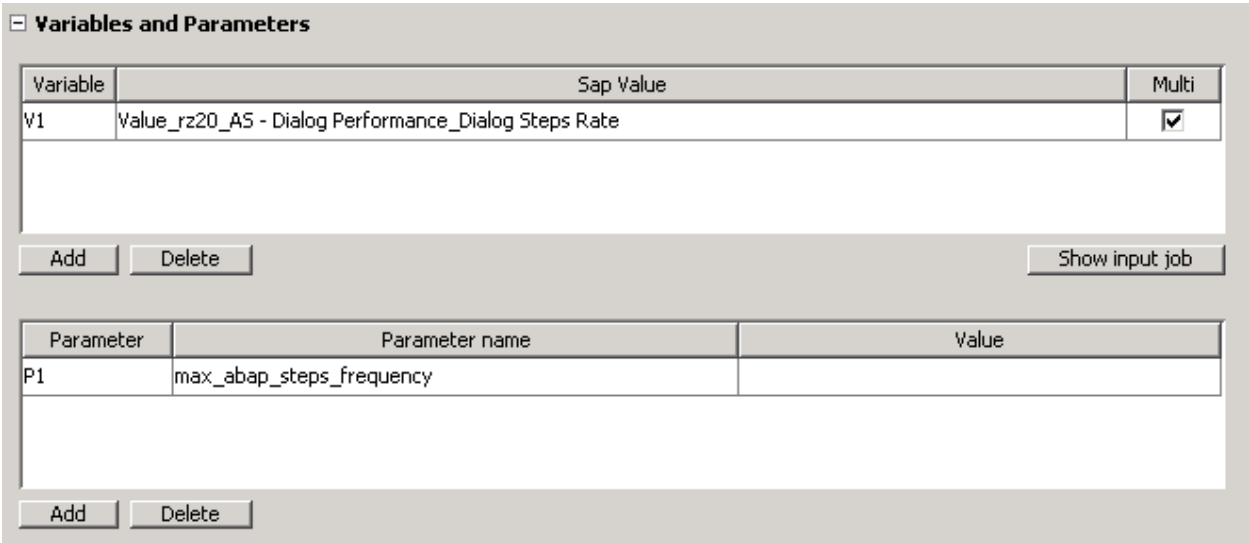
4.4.1. SAP values and parameters

The SAP values are defined in a table specifying the SAP data that are needed by the job. Each line represents a value: V(x). A job can fetch several different values from SAP.

The SAP parameters are defined in a table specifying parameters that will be used to evaluate the expression. Each line defines a parameter P(x).

Using parameters gives the user the possibility of tuning the result of the expression according to his needs. The obvious example is the definition of a threshold that is better being set at run time rather than being hard coded.

Parameters are not necessarily being given a value. If left empty, the job will have to be customized in the template using it. If a value is given, it will stand as the default value. It can be overridden later in a template.



4.4.2. Messages and expressions

©copyright 2014 AGENTIL – all rights reserved

Alarm job's purpose is to send an alarm signal containing an alarm message associated to a severity, if the SAP data are matching a given condition.

This part is meant to define the message, the severity and the expression to evaluate.

The expression string is a formula specifying how the SAP values and parameters are processed.

For alarms, the expression must be Boolean. A true result will fire the alarm.

For QoS, the expression result must be numeric or Boolean.

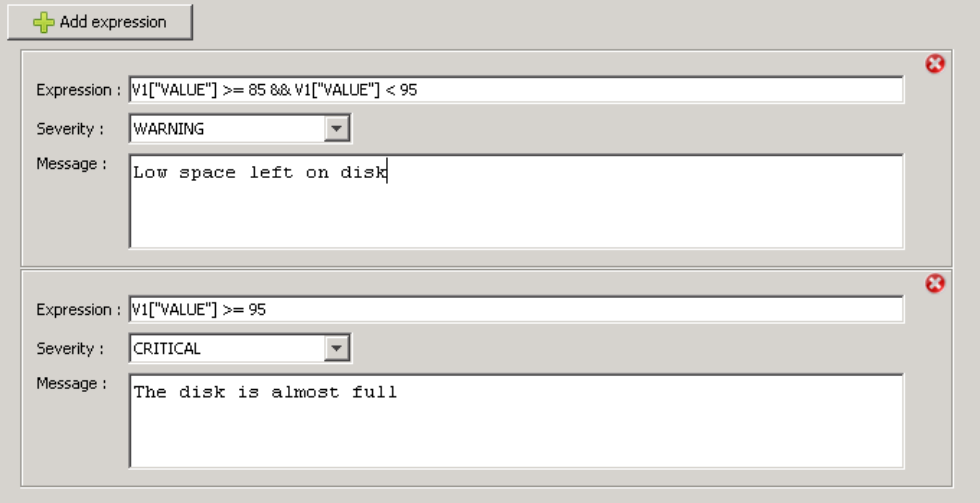
An alarm can have several set of expression, each one with its associated message and severity.

By example:

We need an alarm checking the used percentage of a disk. The alarm will send two signals:

- A WARNING if the capacity is over 85%, with the message : "low space left on disk"
- A CRITICAL if the capacity is over 95%, with the message : "The disk is almost full"

This implementation would look like this:



An alarm job can have as many expression sets as needed

Of course, QOS jobs don't have severity or message and are limited to one expression only. The QOS value will be the result of the expression.

4.5. Alarm tagging

Monitor jobs using a surveillance table to define the monitoring configuration will often propose the possibility to tag an alarm generated by a given line.

This is useful for example when used with an alarm filter, when we want to redirect a specific alarm to a specific person.

©copyright 2014 AGENTIL – all rights reserved

By default, when a text is set in the tag field, it will prefix the alarm message. Following variables will be replaced:

- %SID%: will be replaced by the SID of the current SAP system
- %COMPANY%: will be replaced by the company associated to the SAP system
- %MSG%: will replace the alarm message itself, so you can add a suffix

Example:

Alarm message = “30 short dumps in last 15 min”

Tag = (%SID%) %MSG% (warn Bob)

Result: (PRD) 30 short dumps in last 15 min (warn Bob)

5. SAP instances monitoring

The SAP instances monitoring is probably the most important surveillance job to configure. It will check for the availability of every application server of your SAP system.

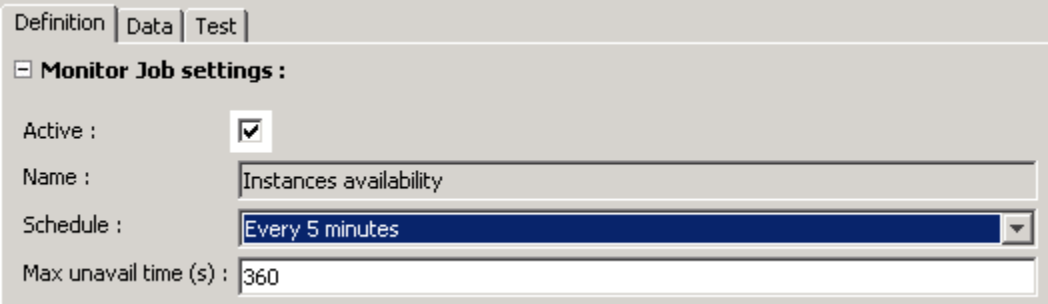
Monitoring capabilities

Based on a list of expected instances that you have to define, the job will regularly check for the availability of each application servers.

An alarm will be sent if one is missing or not responding. An alarm can also be sent if an unexpected instance is found.

Job schedule definition

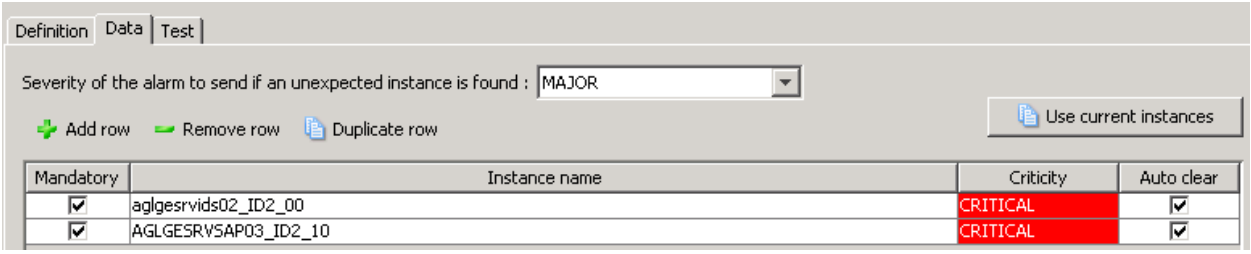
The check will be performed on a regular basis. By default, it is set to run every 5 minutes.



Surveillance table

In this table, you will be able to define the list of expected application servers. You set a new server by pressing the “Add row” button, but you can also use the current detected instances by pressing the “Use current instances” button.

©copyright 2014 AGENTIL – all rights reserved



Mandatory

If checked, the probe will send an alarm if the instance is not seen or not responding.

Auto clear

If checked, the probe will automatically clear alarms if the alarm condition is not met anymore.

QOS

The probe will automatically send an availability QOS named: SAPBASIS_INSTANCE_AVAILABILITY

Containing true if the instance is responding, false instead. QOS target will be set with instance name.

6. SAP jobs monitoring

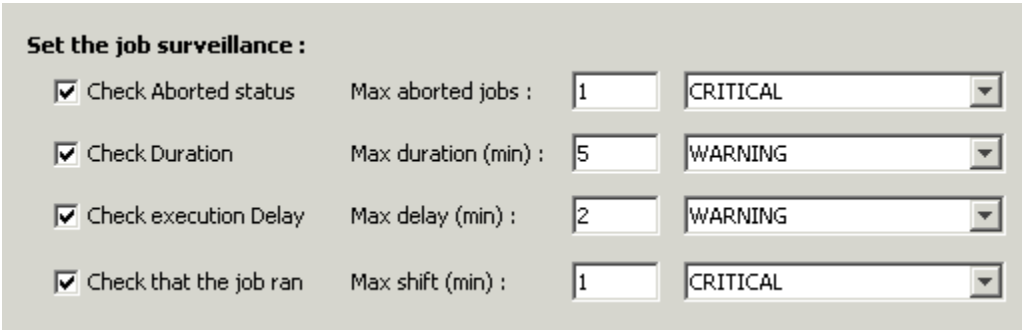
Since version 2.0, the probe has the capability to monitor SAP jobs. To enable this feature, there is a prerequisite: You need to install a specific transport in the SAP target systems (see prerequisites section). Otherwise, the probe will only see the jobs of the client where the probe user belongs to.

Monitoring capabilities

You can monitor four different aspects of a SAP job:

- Its execution status: Sends an alarm if the job got aborted at least X times.
- Its duration : Sends an alarm if the job ran for more than X minutes
- Its execution delay: Sends an alarm is the job took more than X minutes to be executed since its release date.
- Its occurrence: Sends an alarm if the job did not started/finished after X minutes.

For each aspect, you can set a threshold. If reached, an alarm will be sent. The severity of the alarm can be customized for each aspect.

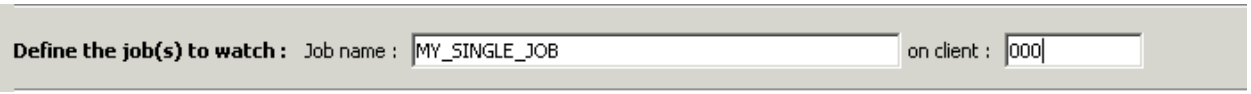


©copyright 2014 AGENTIL – all rights reserved

Job definition

You can define the job to monitor by setting its name and the client on which it will run. The monitoring can be applied to a group of job as well as to a single one:

Single job on a single client:



A group of jobs on two clients:

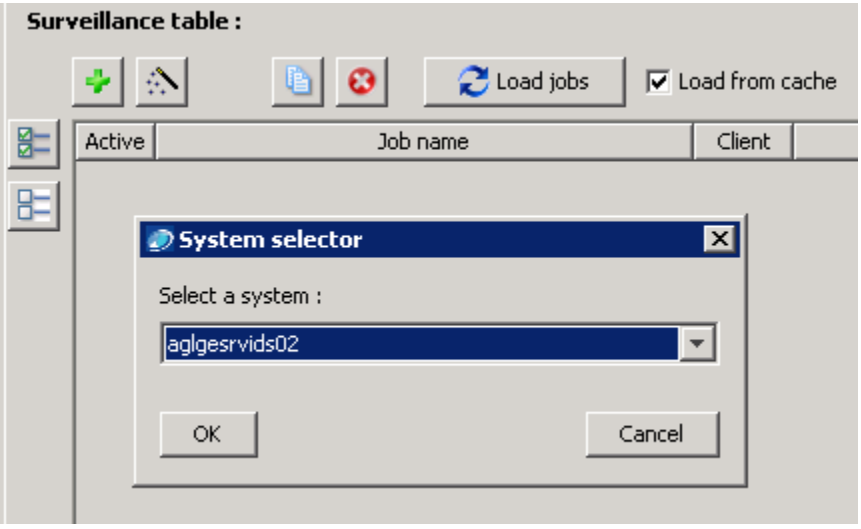
All jobs, all client:

For job name, the '*' character can be used as wild-card character. For client, you can use the standard regular expressions syntax.

Job Selector

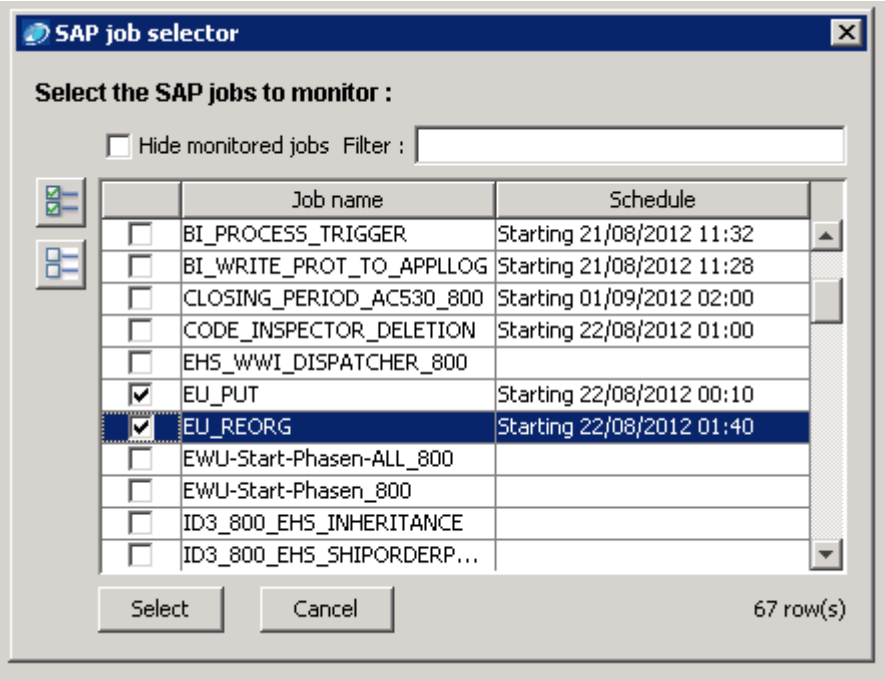
You can load the list of scheduled jobs from SAP and select the jobs that you want to monitor. Press the "Load jobs" button and select the system to read.

If the job list has already been loaded, it will be read from the cache of the probe. If you want to refresh the list from the system, uncheck the "Load from cache" option.

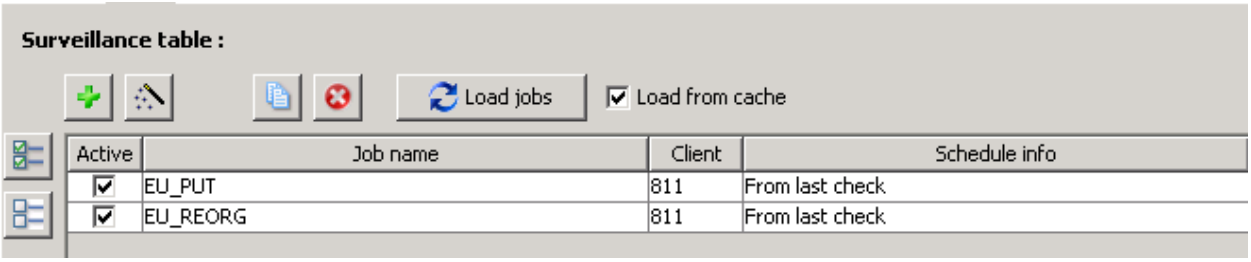


Once the list is loaded, you can select the jobs that you want to monitor:

©copyright 2014 AGENTIL – all rights reserved



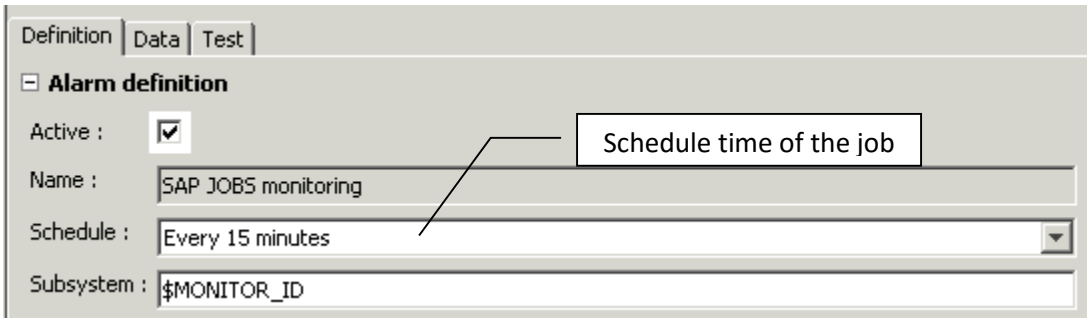
Once you selected the jobs, you can press on “Select”, they will be added in the surveillance table:



Then you can select a job and click on the wizard button for tuning the monitoring. By default it will activate job status monitoring and send a major alarm if the job fails at least once since the last check.

Time window definition

Like other types of monitors, SAP job monitoring is not real time surveillance. It is executed at scheduled time and will analyze jobs that were executed in a period of time. The time between two jobs analysis and the period definition can be customized.



©copyright 2014 AGENTIL – all rights reserved

By default, the monitor will be executed every 15 minutes, and will look for jobs that were executed since the last check.

You have 2 ways of setting the surveillance timing:

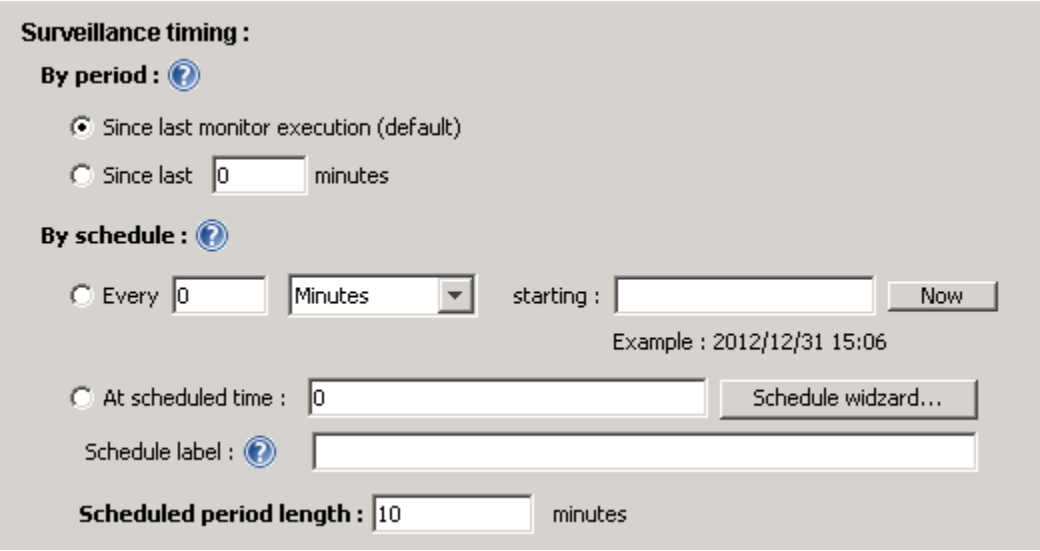
By period: A period is a slice of time in which the probe will look for jobs. It ends at the current time, and starts X minutes in the past:

- If "since last monitor execution" is set, X will be the number of elapsed minutes since the last check.
- Otherwise, it will be the number of minutes set in the "since last" field.
- **Note**: A too deep period is not recommended, because the probe will have to collect much more data for its surveillance. This will have impacts on resources consumed by the probe and on target systems.

By schedule: This mode is useful if you need to watch for a job at a very specific period. The common use case is the surveillance of the occurrence of a job, which must start and end in a given timeframe. A scheduled period is defined by its start, and its duration. The start can set by two ways:

- Using a periodic occurrence, which define a number of units of time between two periods: Example, Every 2 hours starting at 8:05am means that the period will start every 15 minutes from a time base: 8h20, 8h35, 8h50, etc…
- Using a "cron" like syntax schedule, with the help of the schedule wizard.

Once the occurrence of the period is set, you need to set its length in the "Schedule period length" field.



©copyright 2014 AGENTIL – all rights reserved

Calendar

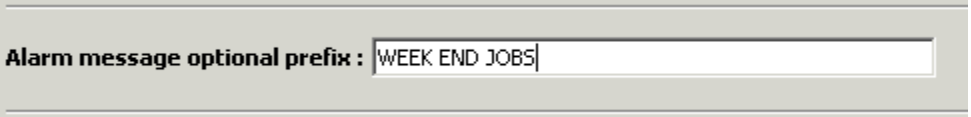
You can set a SAP calendar. This will prevent job monitoring during closed days.

Warning: Some jobs are set to run the next working day if their schedule happens to be during a closed day. This case is not handled by the probe !

Alarm tag

If you define the surveillance of a large number of jobs, it might be difficult to link an alarm received in the alarm console to its surveillance definition.

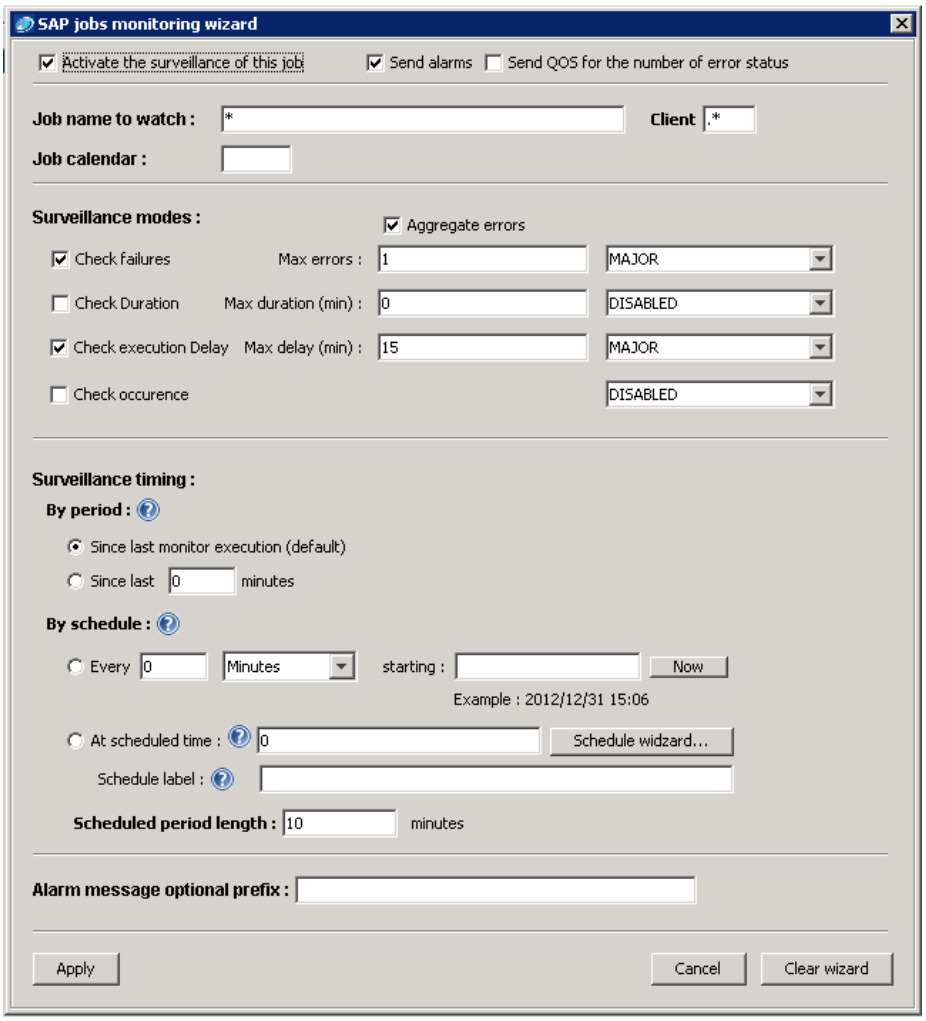
To help you sorting out job alarms, you can specify a prefix to use in the alarm message that a surveillance definition will generate:



The wizard

The configuration of SAP jobs monitoring being complex, a wizard will help you configure it properly:

©copyright 2014 AGENTIL – all rights reserved



By using the wizard, you should be able to define the job surveillance in 3 steps:

- Defining the job name
- Defining the type of surveillance
- Defining the time period

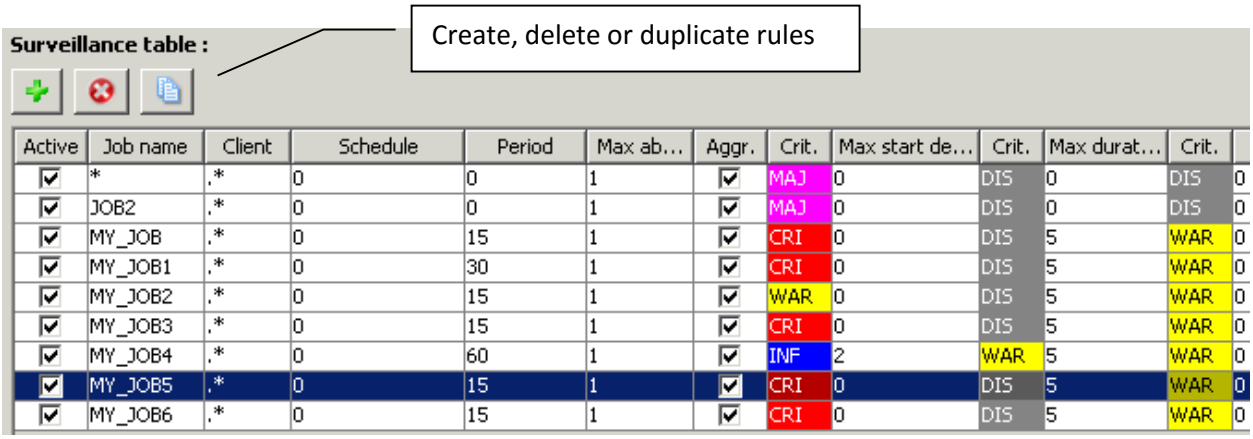
When you tuned the necessary parameters, you can save the surveillance definition by hitting the "Create" button. This will add it in the surveillance table.

Surveillance table

This table holds all surveillance definitions that have been created by the wizard. Each line of the table will reflect a surveillance definition: Job name, type of monitoring, period, etc…

The use of the wizard is optional. You can directly create surveillance rules in the table. The process is faster if you get familiar with it.

©copyright 2014 AGENTIL – all rights reserved



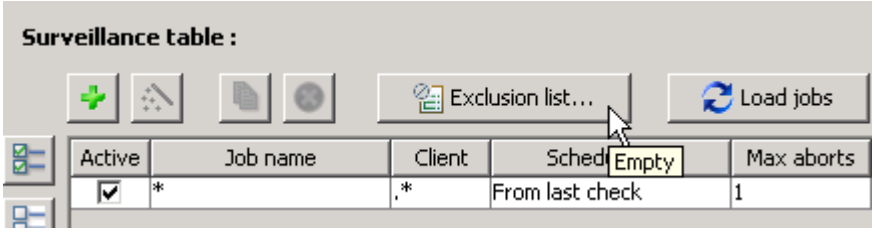
Active	Job name	Client	Schedule	Period	Max ab...	Aggr.	Crit.	Max start de...	Crit.	Max durat...	Crit.	
☑	*	.*	0	0	1	☑	MAJ	0	DIS	0	DIS	0
☑	JOB2	.*	0	0	1	☑	MAJ	0	DIS	0	DIS	0
☑	MY_JOB	.*	0	15	1	☑	CRI	0	DIS	5	WAR	0
☑	MY_JOB1	.*	0	30	1	☑	CRI	0	DIS	5	WAR	0
☑	MY_JOB2	.*	0	15	1	☑	WAR	0	DIS	5	WAR	0
☑	MY_JOB3	.*	0	15	1	☑	CRI	0	DIS	5	WAR	0
☑	MY_JOB4	.*	0	60	1	☑	INF	2	WAR	5	WAR	0
☑	MY_JOB5	.*	0	15	1	☑	CRI	0	DIS	5	WAR	0
☑	MY_JOB6	.*	0	15	1	☑	CRI	0	DIS	5	WAR	0

If you select a rule in the table, it will populate the wizard for a clearer definition overview.

Active:	Use this field to activate or deactivate a line of configuration.
Job name:	A filter to define the job that you want to monitor. Use * for all.
Client:	A filter to match only a subset of clients.
Schedule info:	Defines the schedule defined for the job. This field can only be modified via the wizard.
Max aborts:	The threshold for the maximum number of aborted jobs within a period.
Abort severity:	Defines the severity of the alarm to send if a job get aborted.
Aggregate:	If checked, an alarm will be sent if the total number of aborted jobs is over the threshold. If not check, then one alarm will be sent per job having a number of abort status equal or greater than the threshold.
Max duration:	The threshold for the maximum job duration
Duration severity:	The severity for the duration alarm.
Max start delay:	The threshold for the maximum execution delay.
Delay severity:	The severity for the delay alarm.
Occurrence severity:	The severity used for schedule alarm.
Calendar:	The execution calendar of the job. The check of the job won't be performed on calendar's closed days.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.

©copyright 2014 AGENTIL – all rights reserved

Exclusion list



The exclusion list can be used when you activated to SAP jobs collection in the daily report monitor job.

You can specify a list of jobs that you want to ignore, so they do not appear in the report.

Note: This has no effect on the real time surveillance!

QOS for SAP jobs

If you select the QOS checkbox, the probe will send a QOS containing the number of aborted status for the job defined in the surveillance rule, in the specified period.

It will also send a QOS containing the duration of the job. One QOS will be sent for each occurrence of the job.

QOS names will be:

- SAPBASIS_SAPJOBS_DURATION : Duration of each occurrence of a job
- SAPBASIS_SAPJOBS_STATUS : Status of each occurrence of a job (true if OK)
- SAPBASIS_SAPJOBS_NBABORTED : Number of aborted occurrences of a job.

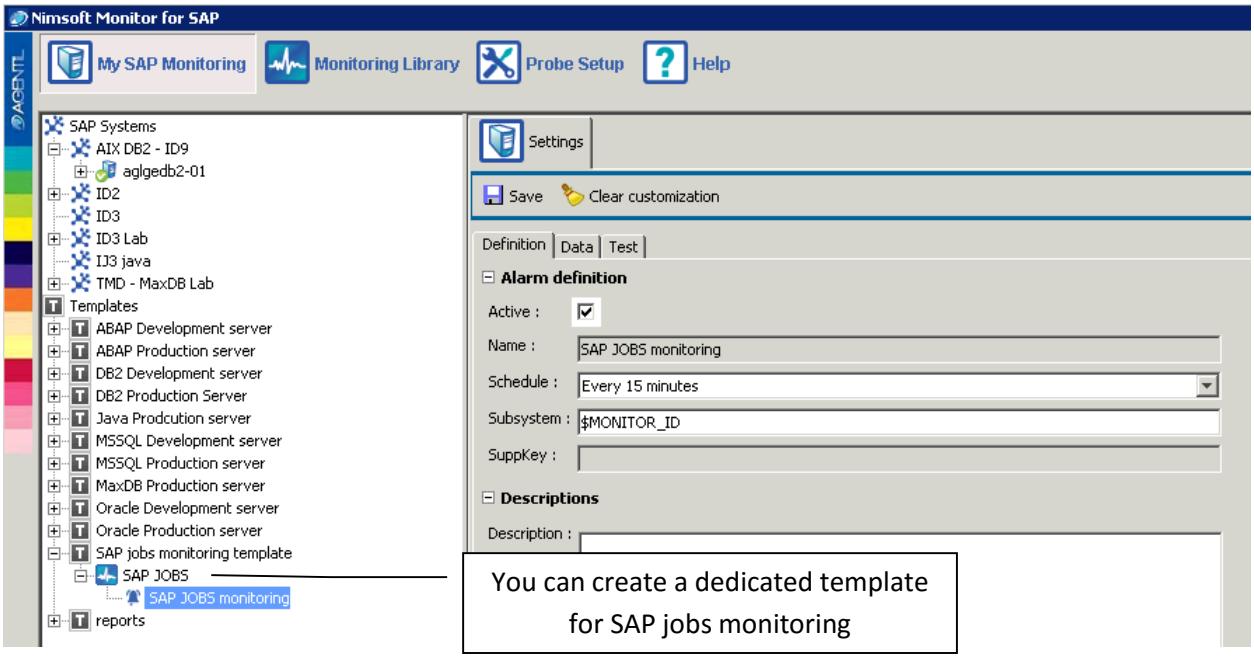
How to enable the SAP job monitoring on a system

This job is available in the monitoring library like all other regular jobs. It is located in the “SAP JOBS” monitor.

In order to assign it to a system, you must include it in an existing template or create a dedicated template for it.

Example:

©copyright 2014 AGENTIL – all rights reserved



Then you just need to assign the template to a system to have this monitor job activated on it.

You can customize the monitoring (surveillance rules creation) at different levels:

- In the monitoring library
- In the template
- In the system

It is **highly** recommended to create surveillance rules at template level, where you will get maximum flexibility.

Note: You cannot reduce the number of inherited surveillance rules (from library to template or from template to system)

7. Process Chains BI

In version 2.5 the probe introduced the monitoring of process chains. This is very similar than the monitoring of SAP jobs concerning the monitoring capabilities and the configuration.

This monitor allows defining a list of process chains that you want to watch, with different level monitoring for any of them.

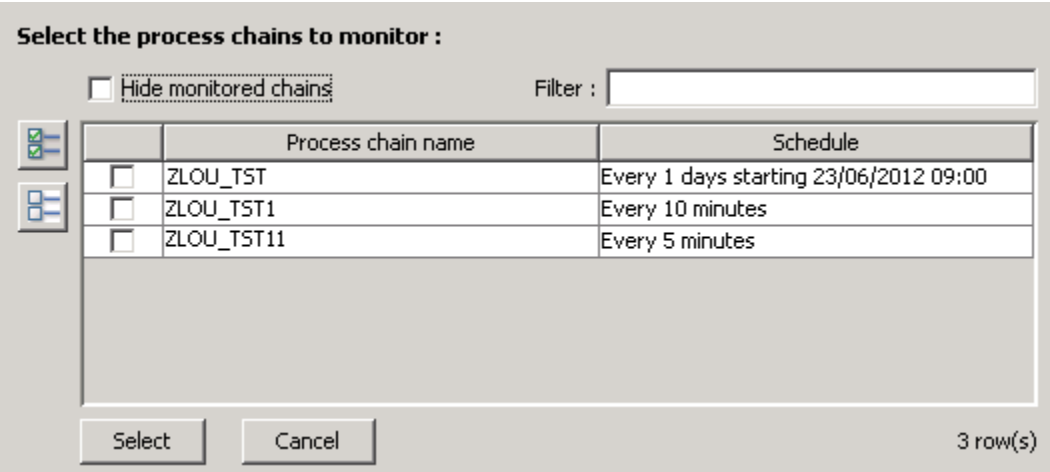
Process chain Selector

You can load the list of process chains from SAP and select the chains that you want to monitor. Press the “Load process chains” button and select the system to read.

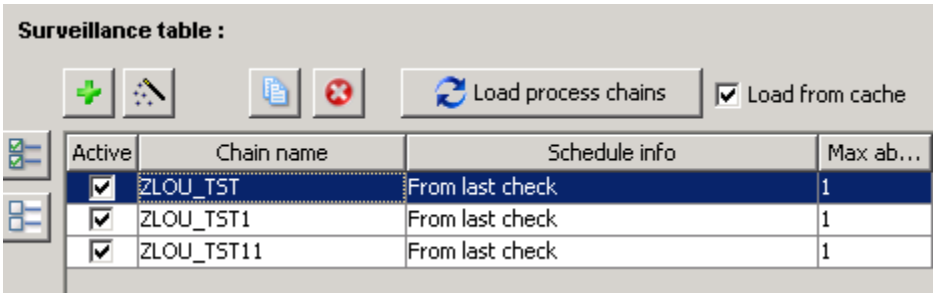
If the process list has already been loaded, it will be read from the cache of the probe. If you want to refresh the list from the system, uncheck the “Load from cache” option.

©copyright 2014 AGENTIL – all rights reserved

Choose the process chains that you want to monitor among the list:

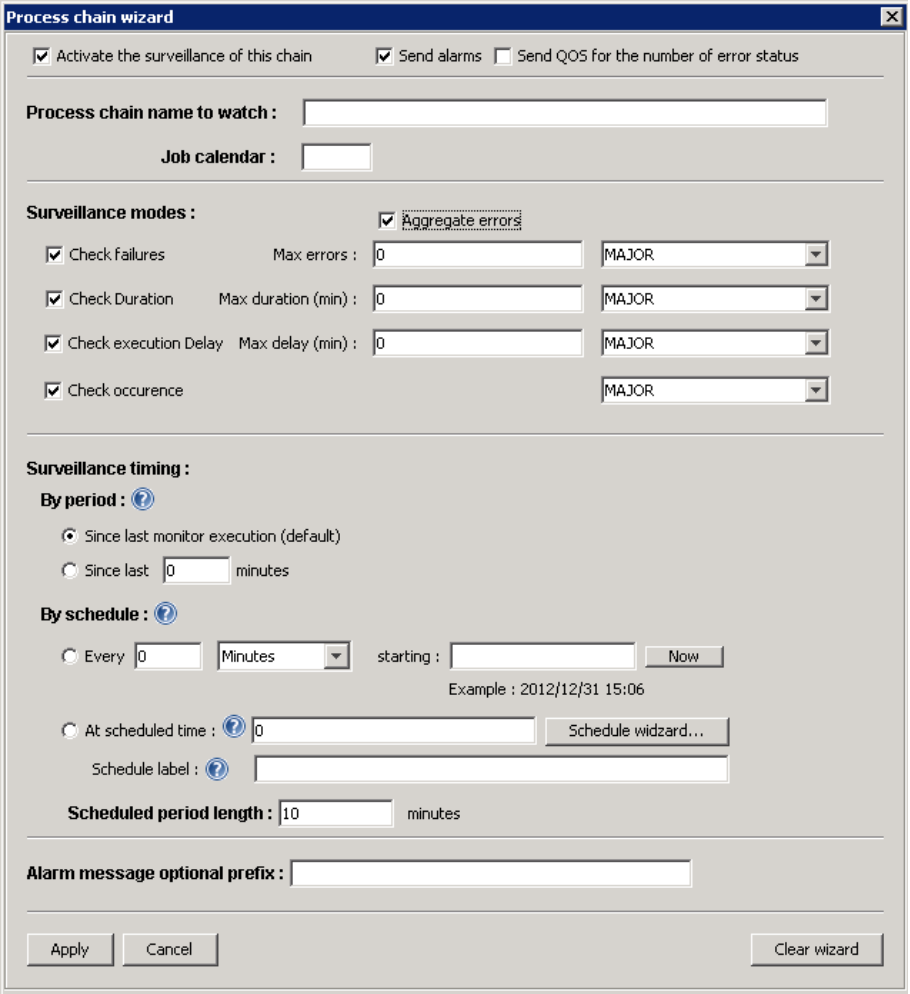


Once selected, press “Select” to add them in the surveillance table:



Now you can select any process chain and click the “wizard” button to open the configuration wizard.

©copyright 2014 AGENTIL – all rights reserved



Configure surveillance

You can set four types of surveillance:

- Failures check : Be warned if a process chains does not complete successfully
- Duration check : Be warned if it lasts too long
- Delay check : Be warned if the start delay is too long
- Occurrence check: Be warned if it did not run in the expected time window.

Select the appropriate surveillance, set the alarm threshold and severity.

Surveillance table

This table holds all surveillance definitions that have been created by the wizard. Each line of the table will reflect a surveillance definition: Job name, type of monitoring, period, etc…

The use of the wizard is optional. You can directly create surveillance rules in the table. The process is faster if you get familiar with it.

<u>Active:</u> Use this field to activate or deactivate a line of configuration.

©copyright 2014 AGENTIL – all rights reserved

Chain name:	A filter to define the process chain that you want to monitor. Use * for all.
Schedule info:	Defines the schedule defined for the process chain. This field can only be modified via the wizard.
Max aborts:	The threshold for the maximum number of aborted process chains within a period.
Abort severity:	Defines the severity of the alarm to send if a process chain is aborted.
Aggregate:	If checked, an alarm will be sent if the total number of aborted process chains is over the threshold. If not check, then one alarm will be sent per process chain having a number of abort status equal or greater than the threshold.
Max duration:	The threshold for the maximum duration
Duration severity:	The severity for the duration alarm.
Max start delay:	The threshold for the maximum execution delay.
Delay severity:	The severity for the delay alarm.
Occurrence severity:	The severity used for schedule alarm.
Calendar:	The execution calendar of the Process chain. The check won't be performed on calendar's closed days.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.

Configure the surveillance period

You can choose between four types of periods:

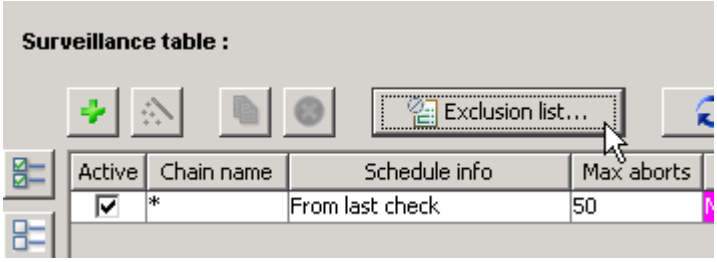
- Since last monitor execution (default): The probe will automatically set the period depth to match the last monitor execution: since the last time the process chain has been checked.
- Since last X minutes: You set an arbitrary period depth.
- At periodic time: Every 2 hours.
- At scheduled time: You specify an execution schedule of the chain and then the probe computes the relevant period depth. This mode is mostly useful to monitor the occurrence of a job execution. You can by example check if a job ran every 2 hours from 8:00am to 6:00pm

The default settings will set the period depth to the last checked time. If available, the real schedule of the chain will be available in the “Every” option of the period definition.

The probe will detect if the process chain is bound to a calendar. The check won’t happen during closed days.

©copyright 2014 AGENTIL – all rights reserved

Exclusion list



The exclusion list can be used when you activated to Process chains BI collection in the daily report monitor job.

You can specify a list of process chains that you want to ignore, so they do not appear in the report.

Note: This has no effect on the real time surveillance!

QOS

If the QOS option is enabled for a given line, following QOS will be sent:

QOS names will be:

- SAPBASIS_PROCESSCHAIN_DURATION : Duration of each occurrence of a process chain
- SAPBASIS_ PROCESSCHAIN_STATUS : Status of each occurrence of a process chain (true if OK)
- SAPBASIS_ PROCESSCHAIN_NBABORTED : Number of aborted occurrences of a process chain.

8. IDOC exchanges monitoring

Since version 2.0, the probe has the capability to monitor IDOC exchanges. To enable this feature, there is a prerequisite: You need to install a specific transport in the target SAP systems (see prerequisites section).

Monitoring capabilities

In this monitor, you can define the IDOC exchanges to watch based on the following characteristics:

- Client number
- Message type
- Partner
- Direction

The monitor will trigger an alarm if the number of IDOC messages matching the filter and having a wrong status is over a threshold.

You can base the trigger on the “ERROR” status or on the “WAITING” status.

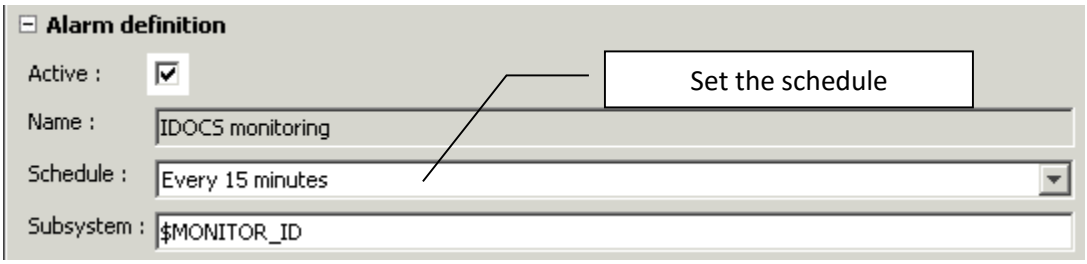
By example: You can define a rule to trigger an alarm if you have more than 10 IDOC messages in ERROR state, on client 100, of message type “TYPE_ABC”.

©copyright 2014 AGENTIL – all rights reserved

Job schedule definition

Like other type of monitors, IDOCS monitoring is not real time surveillance. It is executed at scheduled time and will analyze IDOC messages from a past period.

By default, the job will run every 15 minutes, but you can set a different schedule:



You have to specify the period depth to look for IDOC messages. The end of the period is set to match the schedule time of the monitor.

Surveillance table

This table holds the definition of surveillance rules of IDOC messages. The rules are set directly by filling the table manually.

The left part of the table holds the IDOC filter definition:

Set IDOC filter based on client, message type, partner and direction

Definition | Data | Test

Add row | Delete row | Duplicate

Active	Client	Message type	Partner	Direction
☑	000	TYPE1	PARTNER1	OUTBOUND
☑	.*	TYPE2	.*	INBOUND
☑	100	TYPE3	.*	ANY
☑	.*	TYPE4	.*	ANY
☑	.*	TYPE5	.*	ANY

You can use regular expressions in the IDOC filter in order to match different entries.

The right part holds the surveillance definition:

Define surveillance parameters : Status, period, threshold, severity

Status	Time Period (min)	Max errors	Criticity	Prefix	Alarm	QOS
ERROR	60	10	CRITICAL		☑	☑
ERROR	60	5	WARNING		☑	☑
ERROR	60	2	MINOR		☑	☐
WAITING	60	2	MAJOR		☑	☐
WAITING	30	1	INFORMATIONAL		☑	☐

<u>Active:</u> Use this field to activate or deactivate a line of configuration.

<u>Client:</u> A filter to match only IDOC messages for/from a given client

©copyright 2014 AGENTIL – all rights reserved

Message type:	A filter to match only IDOC message of a given type
Partner:	A filter to match only IDOC for/from a given partner
Direction:	Defines the direction of the IDOC messages to look for
Status:	Define the type of status to look for.
Time period:	Defines how far in the past the monitor will look for IDOC messages at each check.
Max errors:	The threshold for the maximum number of IDOC messages matching the filters and status settings.
Aggregate	If enabled, the monitor will count the number of IDOC matching the filter and send an alarm if it reaches the threshold. If not enable, it will send an alarm per IDOC.
Severity:	The severity of the alarm.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.

Alarm tag

To make IDOC alarms easier to sort in the alarm console, you can set a prefix to add in the alarm message. This can be useful if you have lots of surveillance rules.

QOS with IDOC

If you select the QOS checkbox, the monitor will send a QOS containing the number of IDOC messages matching the filter, having the specified status in the time period.

The QOS name will be:

- SAPBASIS_IDOC_NBERRORS for lines looking IDOC messages in error
- SAPBASIS_IDOC_NBWAITING for lines looking for waiting messages

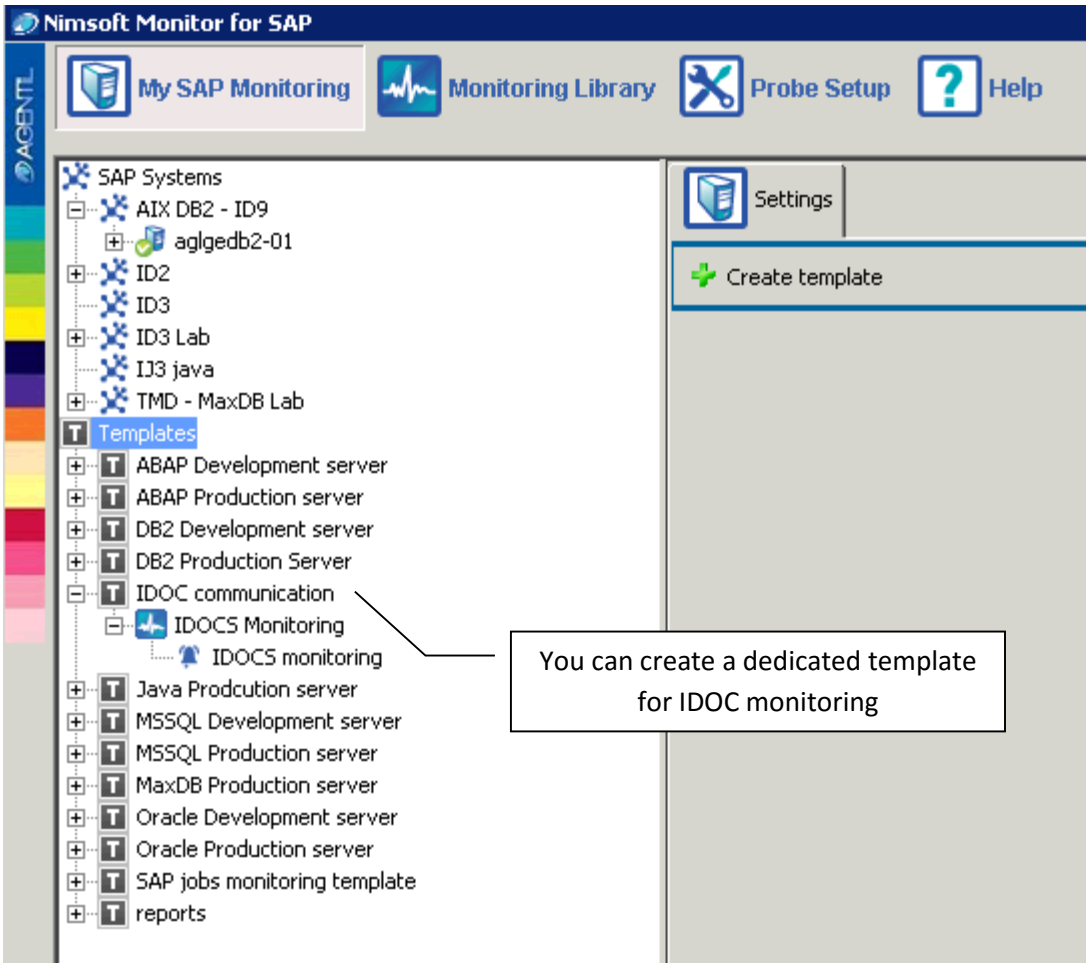
How to enable the IDOC monitoring on a system

This job is available in the monitoring library like all other regular jobs. It is located in the “IDOC monitoring” monitor.

In order to assign it to a system, you must include it in an existing template or create a dedicated template for it.

Example:

©copyright 2014 AGENTIL – all rights reserved



Then you just need to assign the template to a system to have this monitor job activated on it.

You can customize the monitoring (surveillance rules creation) at different levels:

- In the monitoring library
- In the template
- In the system

It is **highly** recommended to create surveillance rules at template level, where you will get maximum flexibility.

Note: You cannot reduce the number of inherited surveillance rules (from library to template or from template to system)

9. Batch inputs

Version 2.5 of the probe introduced Batch inputs monitoring. You can define a list of batch inputs to monitor and be notified in case of failure.

©copyright 2014 AGENTIL – all rights reserved

The principle is quite similar than other monitoring jobs: The check is performed at a periodic time that you can customize.

When the check is executed, the probe will fetch the status of the batch inputs declared in the surveillance table and generate alarms if thresholds are met.

The surveillance table

You can define the batch inputs by the following parameters:

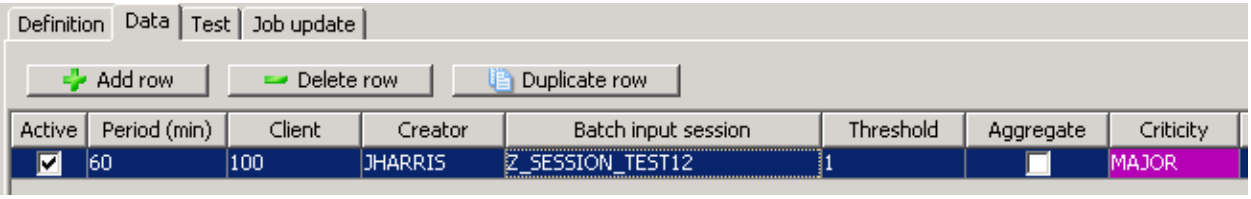
- The client where the batch input occurred
- The creator of the batch input
- The name of the batch input session

Then you can define the monitoring:

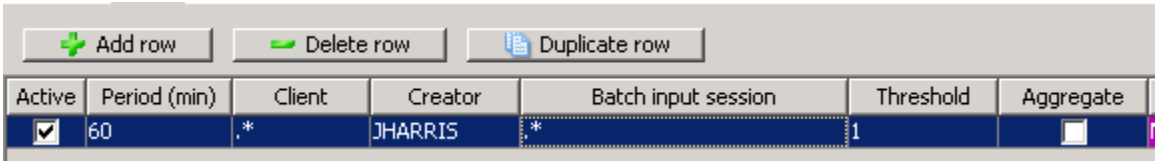
- The period parameter : The time window in which to look for the information
- The threshold : The number of failures that will trigger an alarm
- The severity of the alarm
- The aggregation mode
- The Alarm tag
- The activation of the QOS

By example: This line will check for a batch input that occurred in the last 60 minutes on client 100, being created by “JHARRIS” and with “Z_SESSION_TEST_12” as session name.

If the probe founds at least 1 failure, it will send a MAJOR alarm.

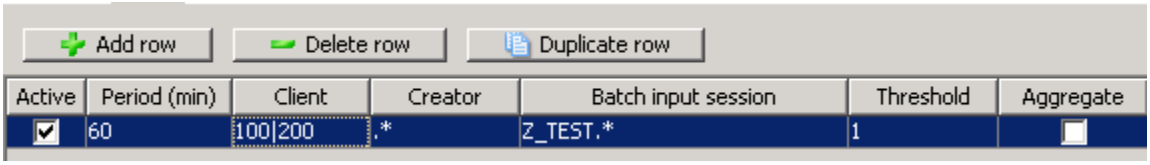


You can use wildcard (.*) character in any of the parameter defining a batch input. By example, in one line you can define to watch all batch inputs created on any client by the user “JHARRIS”:



Or to watch any batch input starting with “Z_TEST” on client 100 and 200:

©copyright 2014 AGENTIL – all rights reserved



Active:	Use this field to activate or deactivate a line of configuration.
Period:	Defines how far in the past the monitor will look for batch input sessions at each check
Client:	A filter to match only a subset of clients.
Creator:	A filter to match only a given creator or subset of creators.
Batch input session:	A filter to match only a given session name.
Max errors:	The maximum number of failed sessions matching the filters.
Aggregate:	If checked, the threshold will be compared to the total number of sessions matching the filter. If not checked, one alarm per failed session will be sent.
Severity:	The level of severity of the alarm generated by this line of surveillance.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

Aggregate mode

If the aggregate checkbox is selected, the probe will generate only one alarm per line. In the opposite, it will generate one alarm per batch input session matching the filter.

Alarm tag

If set, the Alarm tag will be prepended to the alarm message. This can be useful if you use an alarm filtering tool. It will help to sort out the messages and to apply the proper redirection according to line of the surveillance table that generated the alarm.

QOS

If the QOS checkbox is set, the probe will send a QOS corresponding to the number of failures that have been detected for a given line of surveillance.

QOS name will be: SAPBASIS_BATCHINPUTS_NBERRORS

©copyright 2014 AGENTIL – all rights reserved

10. SAP updates

Since version 2.5, the probe introduced SAP updates monitoring. You can define a list of updates and be notified if there are too much of it in “error” or in “not competed” state.

The principle is quite similar than other monitoring jobs: The check is performed at a periodic time that you can customize.

When the check is executed, the probe will fetch the status of the updates declared in the surveillance table and generate alarms if thresholds are met.

The surveillance table

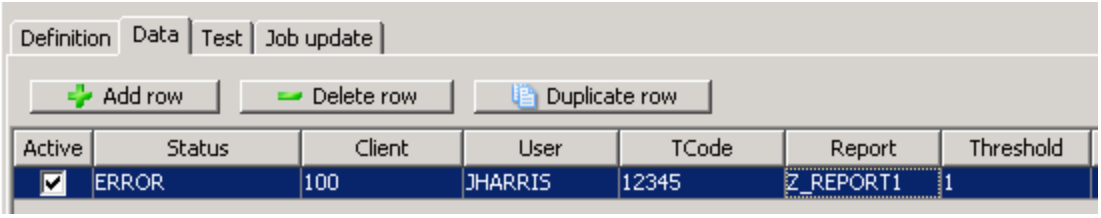
You can define the batch inputs by the following parameters:

- The client where the update occurred
- The status of the update : ERROR, INCONSISTENT or NOT COMPLETED
- The user who created the batch input
- The TCODE
- The report name

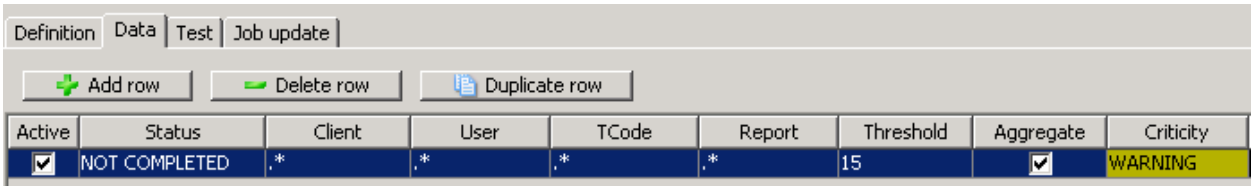
Then you can define the monitoring:

- The threshold : The number of updates matching the filter that will trigger the alarm
- The severity of the alarm
- The aggregation mode
- The Alarm tag
- The activation of the QOS

By example: This line will check for an update that occurred on client 100, created by JHARRIS, with 12345 as TCODE and Z_REPORT1 as report name. If there is at least in update in error matching this filter, the probe will send an alarm.



You can use wildcard (.*) character in any of the parameter defining an update. By example, this line will watch for any updates not completed and generate a WARNING alarm if there are more than 15:



©copyright 2014 AGENTIL – all rights reserved

Active: Use this field to activate or deactivate a line of configuration.

Status: The status of updates to look for.

Client: A filter to match only a given client or subset of clients

User: A filter to match only a user or a subset of users.

TCode: A filter to match only TCode of a subset of TCodes.

Report: If checked, this line of surveillance will used for showing threshold and severity in the daily report

Threshold: The maximum number of updates having the specified status and matching the defined filters.

Aggregate: If checked, the threshold will be compared to the total number of updates matching the filter. If not checked, the probe will group updates having the same Client/User/TCode/Report values and compare the cardinality of each group to the threshold. Several alarms can potentially be generated.

Severity: The level of severity of the alarm generated by this line of surveillance.

Auto clear: If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

Alarm tag: This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.

Alarm: If checked, this line of surveillance will be used for alarm generation.

QOS: If checked, this line of surveillance will be used for QOS generation.

Aggregate mode

If the aggregate checkbox is selected, the probe will generate only one alarm per line. In the opposite, it will generate one alarm per SAP update matching the filter.

Alarm tag

If set, the Alarm tag will be prepended to the alarm message. This can be useful if you use an alarm filtering tool. It will help to sort out the messages and to apply the proper redirection according to line of the surveillance table that generated the alarm.

QOS

If the QOS checkbox is set, the probe will send a QOS corresponding to the number of updates matching the filter of each surveillance lines.

QOS names will be:

- SAPBASIS_UPDATES_NBUNCOMPLETE: Holding number of incomplete updates
- SAPBASIS_UPDATES_NBERROR: Holding number of updates in error.

The QOS sent depends of the configuration of the surveillance rule.

©copyright 2014 AGENTIL – all rights reserved

11. SAP transaction times

Version 2.5 of the probe introduced SAP transaction times monitoring. You can define a list of transactions or types of transaction and receive an alarm if the average execution time per step is too high.

The check will be performed periodically within a customizable period. It will monitor transactions declared in the surveillance table and report alarms if any threshold is reached.

Surveillance table

You can define the transactions by the following parameters:

- Transaction name: SE16, ST22,…
- An optional list of transactions to exclude
- Transaction task type: DIALOG, BACKGROUND, SPOOL, UPDATE …

Then you can define the monitoring:

- The period parameter : The time window in which to look for the information
- The minimum count: The minimum number of steps required to calculate the average.
- The threshold : The maximum average time per step that will trigger an alarm
- The severity of the alarm
- The aggregation mode
- The Alarm tag
- The activation of the QOS

In this example, the probe will monitor SE16 transactions of the last 10 minutes and all UPDATE transactions of the last 600 minutes, except the one starting with "Z".

Active	Transaction	Excluded transactions	Task	Period (min)	Threshold (ms)	Min count	Aggregate	Criticity
☑	SE16		BACKGROUND	60	500	10	☑	MAJOR
☑	.*	Z.*	DIALOG	60	600	30	☑	MAJOR
☑			DIALOG				☐	MAJOR

BACKGROUND
DIALOG
HTTP
RFC
SPOOL
UPDATE
UPDATEV2

<u>Warning:</u> This monitor can become a big resource consumer on the target system if the period of analyze is greater than 30 min, that is why it has been locked to 30 min max. This can be overridden, but many care has to be taken here.

Table fields:

<u>Active:</u> Use this field to activate or deactivate a line of configuration.

©copyright 2014 AGENTIL – all rights reserved

Transaction:	Defines the transaction to watch for. You can use regexp to match a subset of transactions.
Excluded transactions:	A filter to exclude some transactions. Mostly useful if you defined a large subset (like '*') in the transaction field.
Task:	The type of task in which the transaction is running.
Period:	The period of time for which the average response time will be computed.
Max time/step:	The threshold for the maximum time per step in milliseconds.
Min step count:	The minimum number of steps expected in order to consider the response time to be relevant, and thus evaluate the alarm condition.
Aggregate:	Is selected, it will compute the global response time of all the transactions matching the 'transaction filter'. If not selected, the response time of each transaction will be compared to the threshold. Potentially several alarms per line can be generated.
Time Period:	Defines how far in the past the monitor will look for short dumps at each check. If set to 15 min, it will look for transactions occurred in the last 15 min.
Severity:	The level of severity of the alarm generated by this line of surveillance.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

The exclusion list

The format of the exclusion list must follow regular expressions pattern:

- You can give a list of transactions by using "|" (pipe) character as separator : SE16|SE37|SE38
- To match any character, you can use ".*" The following will match any transaction starting by Z: Z.*
- You can also combine rules. The following will match any transactions starting by Z or SE16 transaction: Z.*|SE16
- The complete regular expression constructs are described here : http://docs.oracle.com/javase/1.4.2/docs/api/java/util/regex/Pattern.html

Aggregate mode

If the aggregate checkbox is selected, the probe will generate only one alarm per line. In the opposite, it will generate one alarm per transaction matching the filter.

©copyright 2014 AGENTIL – all rights reserved

Alarm tag

If set, the Alarm tag will be prepended to the alarm message. This can be useful if you use an alarm filtering tool. It will help to sort out the messages and to apply the proper redirection according to line of the surveillance table that generated the alarm.

QOS

If the QOS checkbox is set, the probe will send a QOS signal containing the average time of the transactions matching the surveillance filter of the line.

QOS name will be: SAPBASIS_TRANSACTION_TIMES

QOS target will be set with the name of transaction.

12. Short dumps monitoring

Since version 2.0, the probe has the capability to monitor short dumps.

Monitoring capabilities

In this monitor, you can define the short dumps to watch based on the following characteristics:

- Instance name
- Client number
- Error Id
- Report

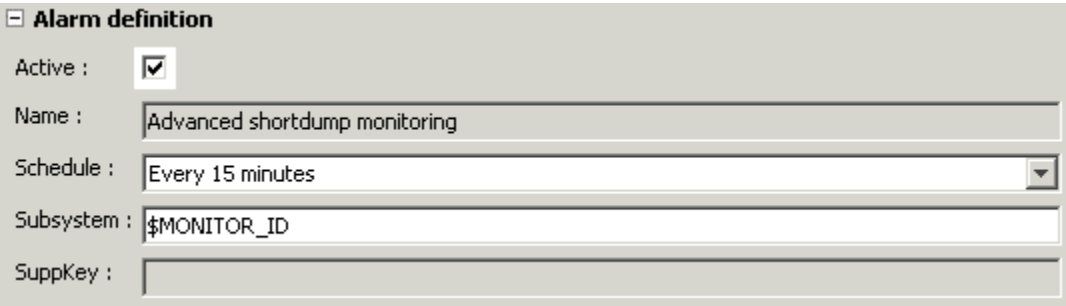
The job will get all short dumps matching the filter. If the number of jobs is over a threshold, it will trigger an alarm. The severity of the alarm can be customized.

You can create all the surveillance rules that you need.

Job schedule definition

Like other type of monitors, shortdumps monitoring is not real time surveillance. It is executed at scheduled time and will analyze shortdumps from a past period.

By default, the job will run every 15 minutes, but you can set a different schedule:



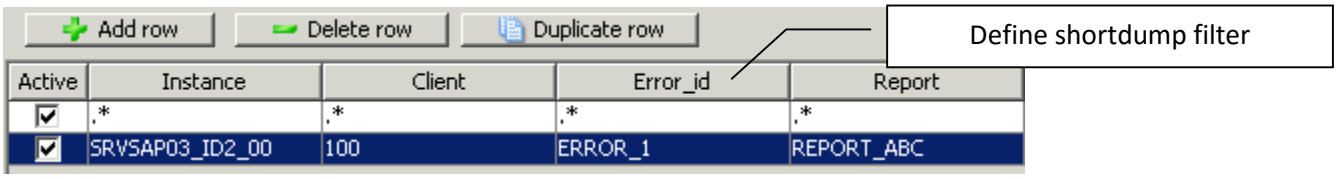
©copyright 2014 AGENTIL – all rights reserved

You have to specify the period depth to look for shortdumps. The end of the period is set to match the schedule time of the monitor.

Surveillance table

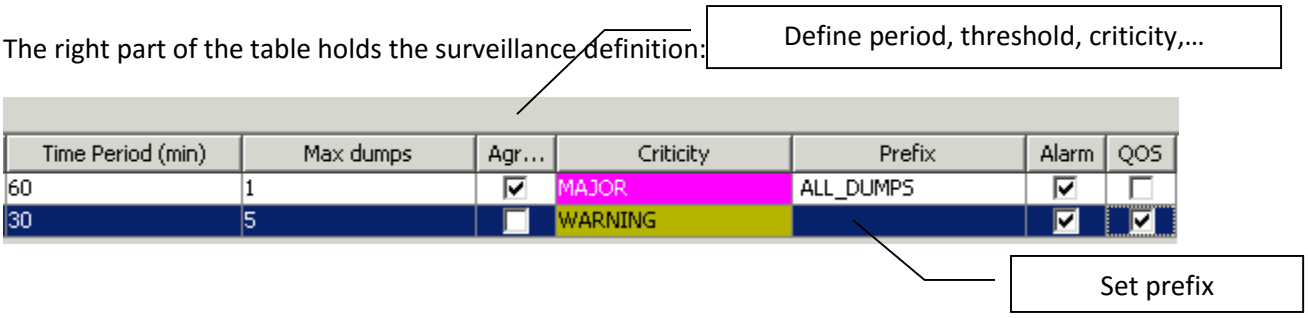
This table holds the definition of surveillance rules of shortdumps. The rules are set directly by filling the table manually.

The left part of the table holds the filter definitions:



You can use regular expressions in the short dump filter in order to match different entries.

The right part of the table holds the surveillance definition:



Active:	Use this field to activate or deactivate a line of configuration.
Instance:	A filter to match only a subset of instances.
Client:	A filter to match only a subset of clients.
Error_id:	A filter to match only short dumps with the given error_id.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report
Time Period:	Defines how far in the past the monitor will look for short dumps at each check. If set to 15 min, it will look for shortdumps occurred in the last 15 min.
Max dumps:	The threshold used to trigger an alarm. If the number of dumps matching the filter is greater or equal to this value, then an alarm with the appropriate severity will be sent.
Aggregate:	If checked, the threshold will be compared to the total number of dumps matching the filter. If not checked, the probe will group dumps having the same Error_id and Report values and compare the cardinality of each group to the threshold. Several alarms can potentially be generated.
Severity:	The level of severity of the alarm generated by this line of surveillance.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.

©copyright 2014 AGENTIL – all rights reserved

QOS: If checked, this line of surveillance will be used for QOS generation.

Alarm tag

To make shortdumps alarms easier to sort in the alarm console, you can set a prefix to use in the alarm message. This can be useful if you have lots of surveillance rules.

QOS with Shortdumps

If you select the QOS checkbox, the monitor will send a QOS containing the number of short dumps matching the filter, in the time period.

QOS name will be: SAPBASIS_SHORTDUMPS_NB

Aggregate dumps

If the aggregate checkbox is not selected, the monitor will use the threshold to trigger alarms for dumps having the same report and error Id. If selected, it will combine all dumps matching the filter

How to enable the short dumps monitoring on a system

This job is available in the monitoring library like all other regular jobs. It is located in the "ABAP dumps" monitor.

You just need to assign a template containing the job to a system to have available on it.

You can customize the monitoring (surveillance rules creation) at different levels:

- In the monitoring library
- In the template
- In the system

It is **highly** recommended to create surveillance rules at template level, where you will get maximum flexibility.

Note: You cannot reduce the number of inherited surveillance rules (from library to template or from template to system)

13. RFC destinations monitoring

In version 3.0 is introduced a new way of monitoring of RFC destinations. It was previously done via the CCMS, which had a lot of disadvantages. This new monitor will be easier to configure and provides more accurate results.

Monitoring capabilities

This monitor will check the availability of RFC destinations from all available application servers. A ping, or authority check will be automatically performed, based on the type of destination.

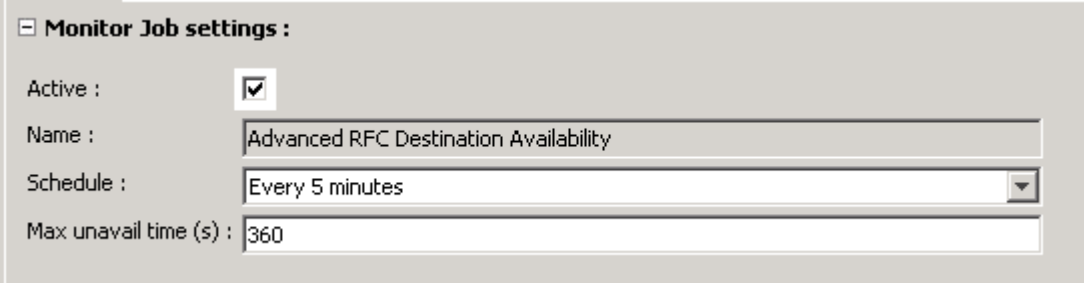
©copyright 2014 AGENTIL – all rights reserved

A list of destinations will have to be defined. For each destination, you will be able to define the level of severity to use if it comes to be unavailable. You can also define if the destination must be reachable from all application servers, or if at least one successful connection is enough.

Job schedule definition

RFC destinations check will be performed on a regular basis. This can be configured in the job definition.

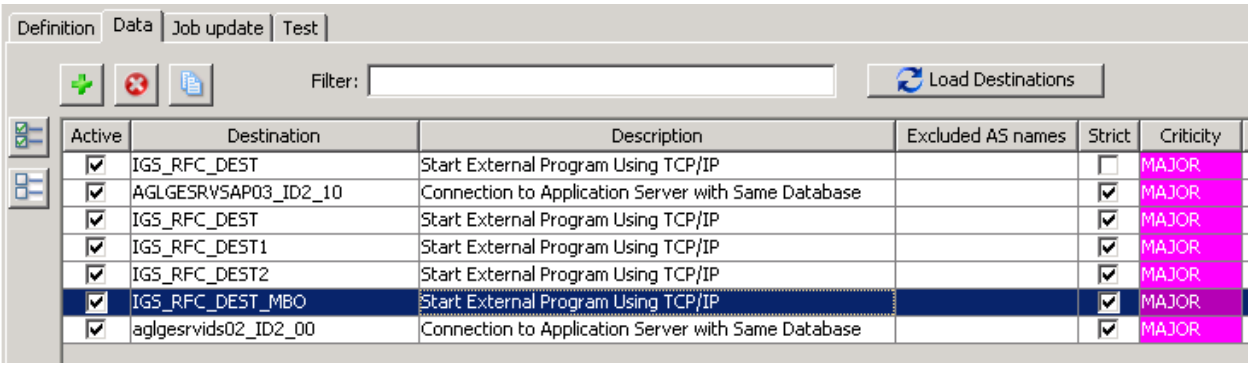
By default, the job will run every 5 minutes, but you can set a different schedule:



Surveillance table

This table holds the definition of destinations to watch. Adding new entries in the table can be done by two ways:

- Use the “Load destinations” button to get the list of defined destinations of a given SAP system.
- Use the “Plus” button to create a new row in the table, and type the destination name manually.



Active	Destination	Description	Excluded AS names	Strict	Criticity
☑	IGS_RFC_DEST	Start External Program Using TCP/IP		☐	MAJOR
☑	AGLGESRVSAP03_ID2_10	Connection to Application Server with Same Database		☑	MAJOR
☑	IGS_RFC_DEST	Start External Program Using TCP/IP		☑	MAJOR
☑	IGS_RFC_DEST1	Start External Program Using TCP/IP		☑	MAJOR
☑	IGS_RFC_DEST2	Start External Program Using TCP/IP		☑	MAJOR
☑	IGS_RFC_DEST_MBO	Start External Program Using TCP/IP		☑	MAJOR
☑	aglgesrvids02_ID2_00	Connection to Application Server with Same Database		☑	MAJOR

<u>Active:</u> Use this field to activate or deactivate a line of configuration.

<u>Destination:</u> Defines the destination to check.

<u>Excluded AS names:</u> A coma separated list of application servers: Use that field if there are AS from which you don't want to check the destination

<u>Check mode:</u> AUTO : the probe will detect if the destination needs authentication or if a simple PING is enough. NO_AUTHENTICATION : The check is done via a simple PING.

<u>Strict:</u> If selected, the connection to the destination must work from all application servers. Otherwise, a connection working from at least one AS is sufficient.

<u>Severity:</u> The level of severity of the alarm generated by this line of surveillance.

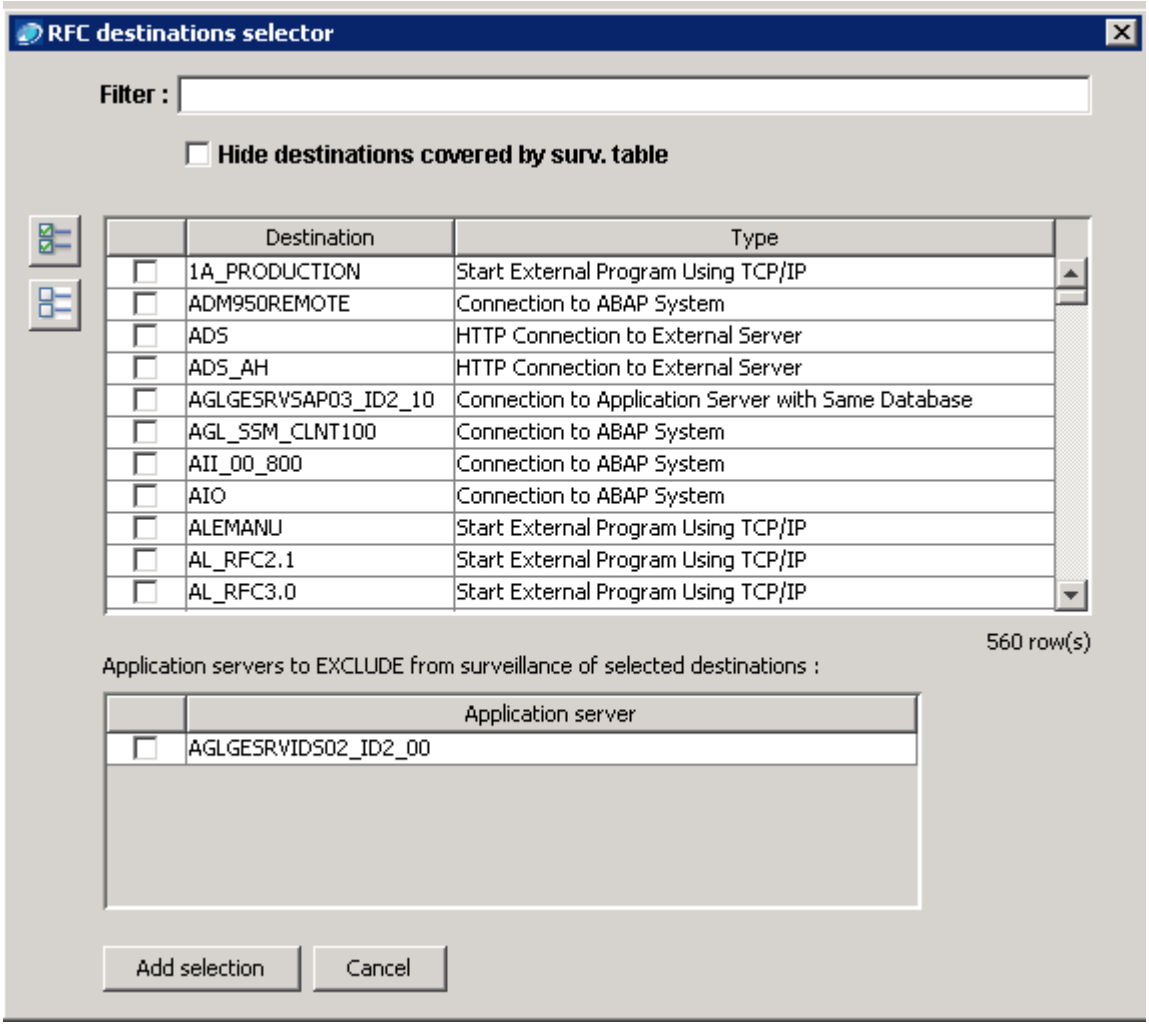
©copyright 2014 AGENTIL – all rights reserved

Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

Destinations selector

The selector will display all available destinations in a table. Select the ones you are interested to monitor.

In some cases, you might also want to exclude the check of a given set of destinations on some application servers. You can select the servers to exclude from the selector, they will be added in the “excluded AS” field.



©copyright 2014 AGENTIL – all rights reserved

Excluded AS names

For a given destination, you can exclude the application servers from which you don't want the destination to be checked. You must use the exact AS name as it appears in the list of available AS in the SAP connector of the probe. Use space as separator between AS names.

Strict mode

If the strict mode is activated for a destination, it means that an alarm will be sent if the destination fails from any application server. If not set, an alarm will be sent only if the destination fails from all instances.

Auto clear

If auto clear is active, the probe will automatically clear alarms that were sent for unavailable destinations that became online again.

Alarm tag

To make alarms easier to sort in the alarm console, you can set a prefix to use in the alarm message. This can be useful if you have lots of surveillance rules.

QOS

If you select the QOS checkbox, the monitor will send a QOS containing a true value if the destination is responding, false otherwise.

QOS names will be:

- SAPBASIS_RFC_DESTINATION_AVAILABILITY_PER_AS: Target contains AS name + destination
- SAPBASIS_RFC_DESTINATION_AVAILABILITY_PER_SYSTEM : Target contains destination

14. Long blocking locks on DB objects

Since version 3.0, it is now possible to monitor the time waited to acquire a lock on a database object.

Monitoring capabilities

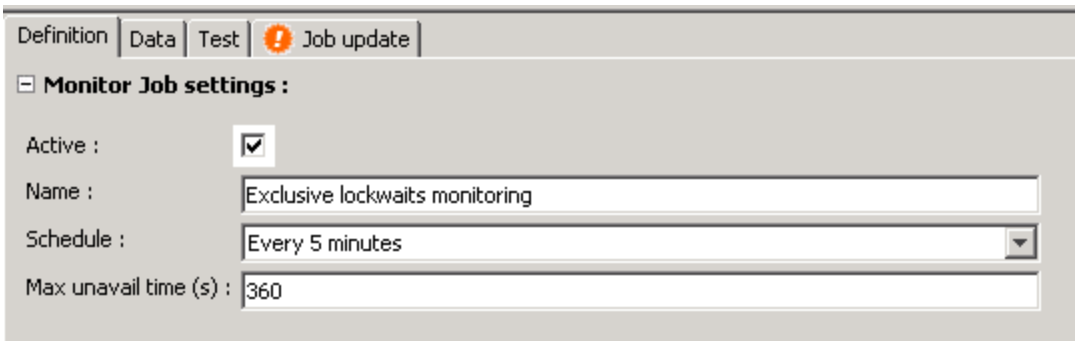
This monitor will check for the current exclusive lock requests on database objects. You can configure a maximum wait time per object and receive an alarm if the threshold is reached.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.

By default, the job will run every 5 minutes, but you can set a different schedule:

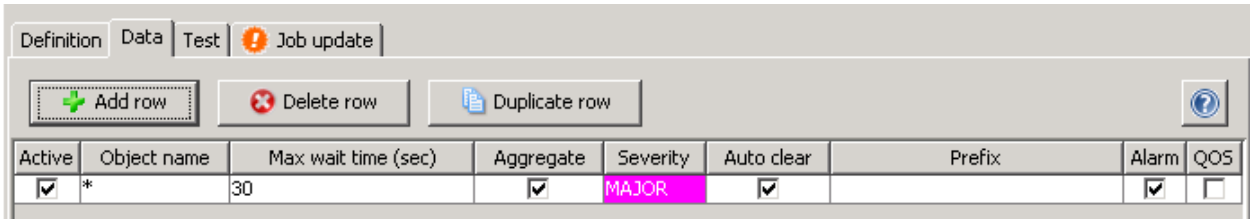
©copyright 2014 AGENTIL – all rights reserved



Surveillance table

This table holds the definition of the objects to watch, and the maximum allowed time to wait for it.

In order to create a new rule in the surveillance table, use the « Add row » button, then set object name, threshold and severity.



When adding a new rule, the default setting will be a surveillance of all objects, and a maximum time of 30 seconds.

You can define large scope rules by using regular expressions as object name. A star (*) will cover all objects. But you can also create custom rules on specific objects.

Active:	Use this field to activate or deactivate a line of configuration.
Object name:	The name of the database object to look for. You can use regular expressions, or * to match any object.
Max wait time:	The threshold for the maximum time an exclusive lock can be held, in seconds.
Aggregate:	If checked, the alarm will indicate how many matching objects are held by an exclusive lock since too long time. If not checked, the probe will send an alarm per matching object being subject of a too long exclusive lock.
Severity:	The level of severity of the alarm generated by this line of surveillance.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

©copyright 2014 AGENTIL – all rights reserved

Aggregate

If the aggregate option is enabled, the probe will aggregate all objects matching the rule in one single alarm. If not enabled, one alarm per object matching the rule will be sent.

Example:

Let's assume that we have 3 objects matching a rule, having requests waiting for more than threshold.

If aggregate is enabled, you will receive one alarm with message: "3 objects have requests waiting for more than threshold."

If not enabled, you will receive 3 alarms with message: "Object XXX has requests waiting for YYY sec."

Auto clear

If auto clear is active, the probe will automatically clear alarms that were sent for objects that no longer have request waiting for too long.

Alarm tag

To make alarms easier to sort in the alarm console, you can set a prefix to use in the alarm message. This can be useful if you have lots of surveillance rules.

QOS

If you select the QOS checkbox, the monitor will send a QOS containing the current waiting time on the object.

QOS name will be: SAPBASIS_LOCKWAITS_NBLOCKS

The target of the QOS will contain the object name.

15. Dispatcher queues

Since version 3.0, it is now possible to monitor the fill rate of the dispatcher queues.

Monitoring capabilities

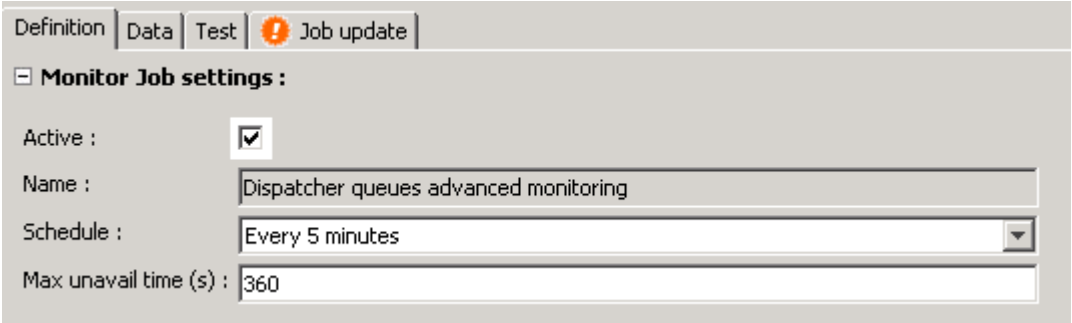
For each queue, you can generate metrics and set alarms based on the number of queued requests, and the number of requests written during a given period.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.

By default, the job will run every 5 minutes, but you can set a different schedule:

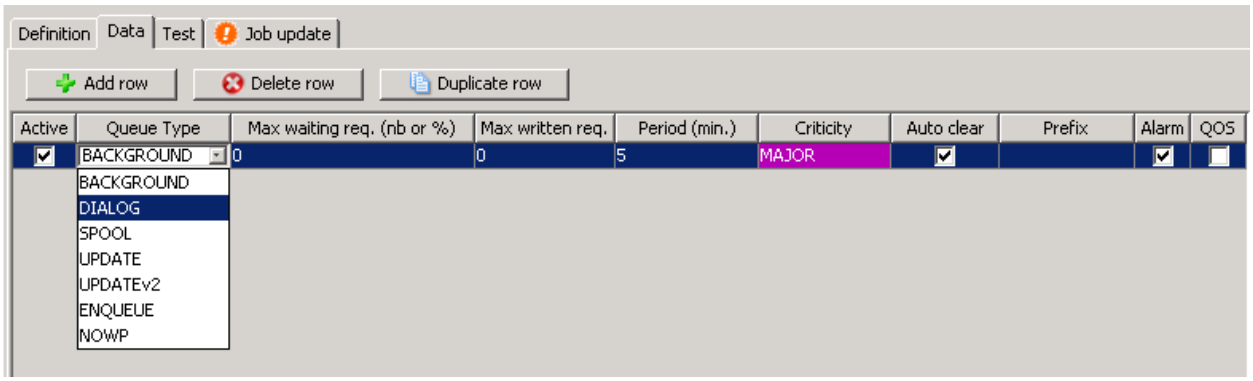
©copyright 2014 AGENTIL – all rights reserved



Surveillance table

This table holds the definition of the monitoring of each queue.

In order to create a new rule in the surveillance table, use the « Add row » button, then select the appropriate queue, set thresholds and severity.



Active:	Use this field to activate or deactivate a line of configuration.
Queue type:	Choose the type of queue to watch
Current waiting requests:	The threshold for number of waiting requests, in absolute or in percentage of the total capacity of the queue.
Max written requests:	The threshold for the number of requests written in the queue with the configured period.
Period:	The period of time used by the Max written request threshold.
Severity:	The level of severity of the alarm generated by this line of surveillance.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.

©copyright 2014 AGENTIL – all rights reserved

Max waiting requests:

In this field, you can set an absolute number, or a percentage. If a value greater than 0 is set, an alarm will be sent if the number of queued requests is greater or equal to the threshold. If a percentage is set, an alarm will be sent if the usage of the queue is greater or equal to the threshold.

Max written requests and Period:

If a value greater than 0 is set, an alarm will be sent if the number of written request during the period, is greater or equal to the threshold.

The minimum period depth must be at least 5 minutes

Auto clear

If auto clear is active, the probe will automatically clear alarms that were sent for queues that no longer match the defined thresholds.

Alarm tag

To make alarms easier to sort in the alarm console, you can set a prefix to use in the alarm message. This can be useful if you have lots of surveillance rules.

QOS

If you select the QOS checkbox, the monitor will send three different QOS per queue:

- SAPBASIS_DISPATCHER_QUEUES_NB_WAITING: containing the current number of queued requests.
- SAPBASIS_DISPATCHER_QUEUES_PERCENTAGE_USED: Containing the current fill rate.
- SAPBASIS_DISPATCHER_QUEUES_WRITTEN_REQUESTS_IN_PERIOD: Containing the number of requests written in the last period.

The target of the QOS will contain the queue name and instance name.

16. Work processes monitoring

Since version 3.0, you can monitor the work processes at different levels, based on the task type. This new monitor is more accurate than the previous one based on CCMS.

Monitoring capabilities

For each different type of work processes, you can collect metrics and set alarms based on the following indicators:

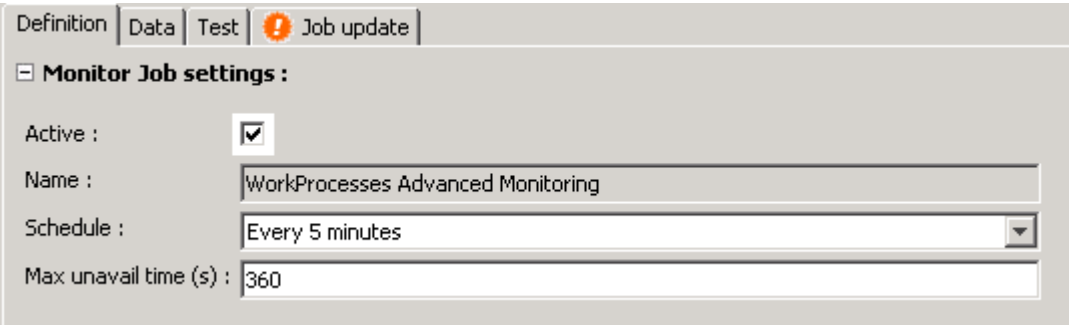
- The running time of current task
- The number of processes having a specific status and used by a given user (Busy, private, stopped, etc…)

©copyright 2014 AGENTIL – all rights reserved

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.

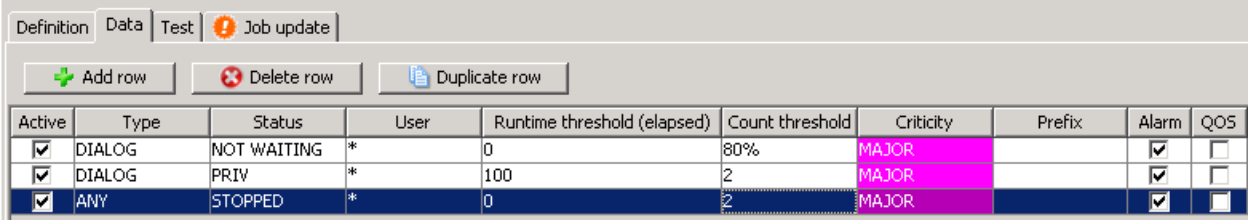
By default, the job will run every 5 minutes, but you can set a different schedule:



Surveillance table

This table holds the definition of the monitoring of work processes.

In order to create a new rule in the surveillance table, use the « Add row » button, then select the appropriate type of work process.



Fields description:

Active:	Use this field to activate or deactivate a line of configuration.
Type:	The type of workprocess to watch, or ANY to watch all.
Status:	Watch for the processes of the given status
User:	A filter to match only the process used by the given user. Regular expressions may be used.
Runtime threshold:	The threshold for the maximum runtime (seconds) of a given process. Does not depend on the configured status.
Count threshold:	The threshold for the number of processes being in the defined status. Use an absolute value or a percentage of the total number of processes available for the given task (specify % unit).
Severity:	The level of severity of the alarm generated by this line of surveillance.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

©copyright 2014 AGENTIL – all rights reserved

Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

Following parameters have to be set:

- The type of work process: choose the appropriate type, or ANY if you want to match any type.
- Status: The work processes having the given status to look for.
- User: The work processes used by the given user to look for.
- Runtime threshold: The maximum allowed runtime, in seconds.
- Count threshold: The maximum number of processes matching the type, status and user of the surveillance rule. Can be set in percent or absolute number. If percentage is used, it will be based on the total number of processes of the given type (or all if ANY is set).

Example:

Considering the screen shot above, the monitoring will result in the following:

- Line 1: Send an alarm if more than 80% of the Dialog processes are busy
- Line 2: Send an alarm if a Dialog process in private mode runs for more than 100 seconds, or if there is more than 1 Dialog process in private mode.
- Line 3: Send an alarm if there is more than one process stopped.

Note: Runtime and count thresholds are “OR’ed”. Meaning that an alarm will be sent if at least one of the threshold is reached. You won’t be able to set a rule to check if there are more than 10 processes running for more than 300 seconds.

Alarm tag

To make alarms easier to sort in the alarm console, you can set a prefix to use in the alarm message. This can be useful if you have lots of surveillance rules.

QOS

If you select the QOS checkbox, the probe will send two QOS per line, containing the number of processes matching the rules, in absolute and percentage.

The name of the QOS will be computed according to the surveillance settings:

- Status = NOT_WAITING : Qos names will be SAPBASIS_WORKPROCESS_PERCENTAGE_USED and SAPBASIS_WORKPROCESS_USED

©copyright 2014 AGENTIL – all rights reserved

- Status = ON_HOLD : Qos names will be SAPBASIS_WORKPROCESS_ON_HOLD_PERCENTAGE_USED and SAPBASIS_WORKPROCESS_ON_HOLD_USED

The target of the QOS will be set with the process type (DIALOG/BACKGROUND/etc…)

17. Update service monitoring

Since version 3.0, the availability of the update service can be monitored otherwise than through CCMS. This has the advantage to get rid of the regular availability problems encountered with CCMS.

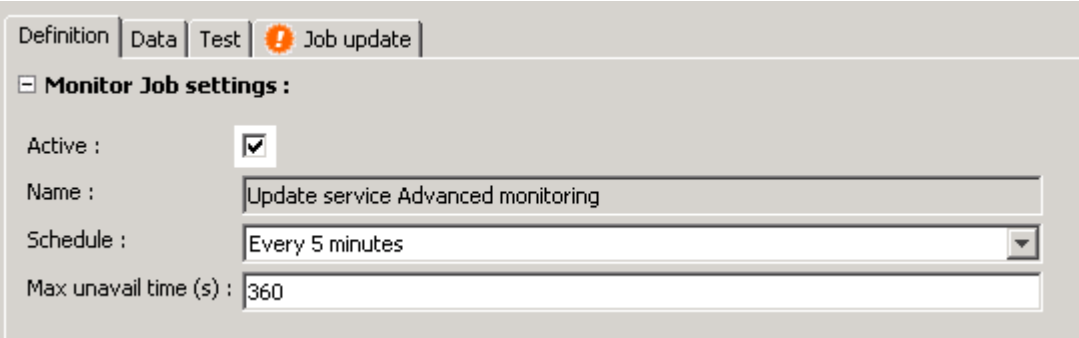
Monitoring capabilities

In this monitor, you will be able to define the severity of the alarm generated if the update service is no longer available.

Job schedule definition

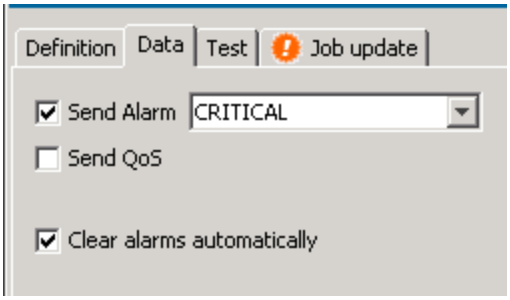
The check will be performed on a regular basis. This can be configured in the job definition.

By default, the job will run every 5 minutes, but you can set a different schedule:



Configuration

The settings of update service monitoring are done via the configuration panel:



For the service status, you can set the following:

- Activation of the check.
- If alarm has to be sent, and for which severity.
- If a QOS has to be sent.

©copyright 2014 AGENTIL – all rights reserved

Automatic alarm clear

If enabled, alarms generated by this monitor will be cleared if the alarm condition is not met anymore.

QOS

If enabled, update service QOS name will be: SAPBASIS_UPDATE_SERVICE_AVAILABILITY (true if OK)

18. SAP transports

Since version 3.0, it is possible to monitor SAP transports status.

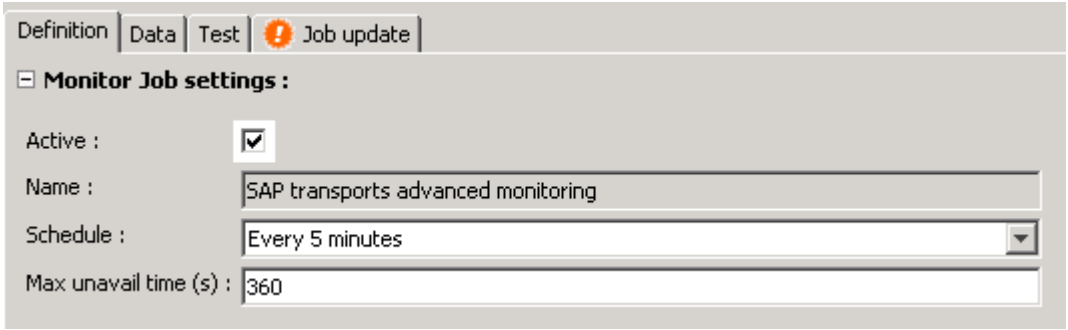
Monitoring capabilities

Monitors the status of SAP transports. It will look for failed transport and trigger an alarm if a transport matches the monitoring rules.

Job schedule definition

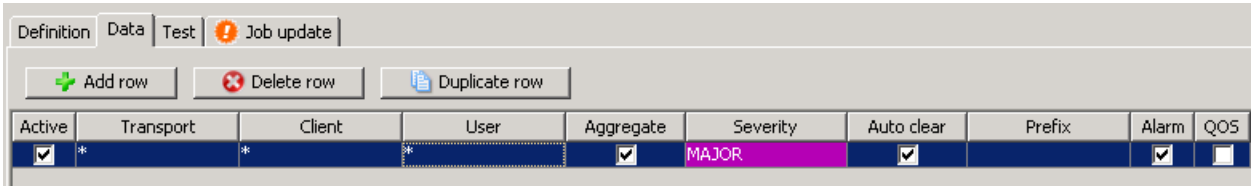
The check will be performed on a regular basis. This can be configured in the job definition.

By default, the job will run every 5 minutes, but you can set a different schedule:



Surveillance table

The definition of the surveillance is done by creating rules in the surveillance table. Press the "Add row" button to create a new rule:



Fields description:

Active:	Use this field to activate or deactivate a line of configuration.
Transport:	A filter to match only a given transport name. The use of regular expression can be made here.
Client:	A filter to match only a subset of clients.
User:	A filter to match only a subset of users.

©copyright 2014 AGENTIL – all rights reserved

Aggregate: If checked, the probe will send one alarm indicating the number of failed transports matching the filter. If not checked, the probe will send an alarm for each failed transport matching the filter. Several alarms can potentially be generated.

Severity: The level of severity of the alarm generated by this line of surveillance.

Auto clear: If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

Alarm tag: This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.

Alarm: If checked, this line of surveillance will be used for alarm generation.

QOS: If checked, this line of surveillance will be used for QOS generation.

By default, a new created rule will be set to check for all transports, from any client and any user.

The following parameters have to be set:

- Transport: The name of the transport to check, * if any.
- Client: The client on which the transport occurs, * if any.
- User: The user who created the transport, * if any.
- Severity: The severity of the alarm that will be sent if a transport in error and matching the filter is found.

Aggregate

If set, only one alarm per line of surveillance will be sent. The message will look like: “There are X transport in error”

If unset, one alarm per transport in error will be sent: “Transport XXX on client 100 from user YYY has failed”

Auto clear

If set, the probe will clear the alarms if the alarm condition is not met anymore.

Alarm tag

To make alarms easier to sort in the alarm console, you can set a prefix to use in the alarm message. This can be useful if you have lots of surveillance rules.

QOS

If enabled, a QOS containing the number of failed transports will be sent:
SAPBASIS_TRANSPORT_NBFAILED

19. Sys log monitoring

Since version 3.0, it now possible to monitor system logs of each instance.

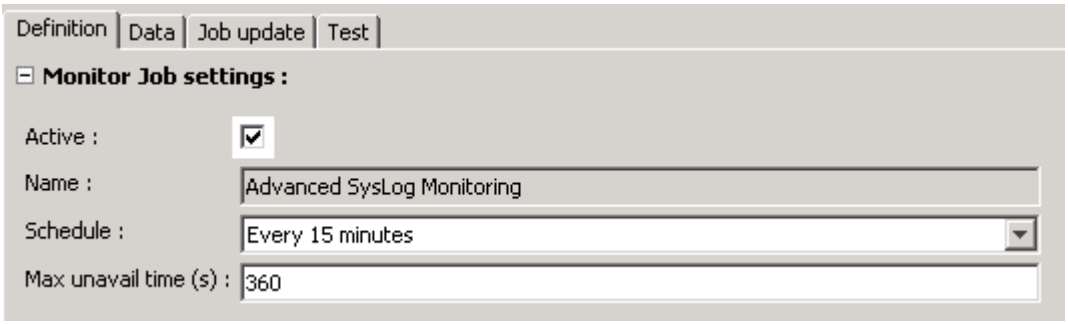
©copyright 2014 AGENTIL – all rights reserved

Monitoring capabilities

With this monitor, you can define patterns to match in the system logs of a given instance. These lines can be forwarded in an alarm, or counted and used as a trigger.

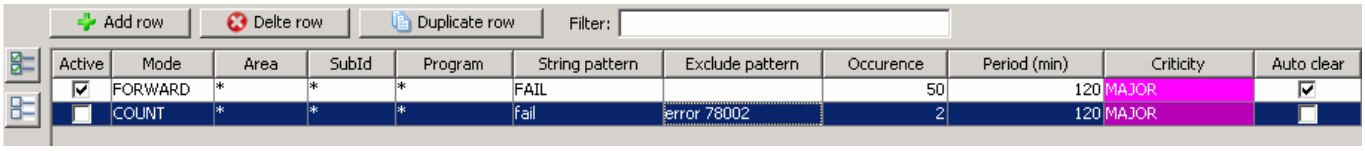
Job schedule definition

This check is performed on regular basis. By default it is set to run every 15 minutes:



Surveillance table

The definition of sys log monitoring is done by setting a list of rules in the surveillance table:



Following parameters can be set:

Active:	Use this field to activate or deactivate a line of configuration.
Mode:	Choose the surveillance mode
Id:	A filter for the line Id of the log
SubId:	A filter for the SubId of the line.
Program:	A filter for the program associated with the line.
String pattern:	This field can be used to define the text pattern to look for in the log. Regular expressions can be used, or a coma separated list of strings.
Exclude pattern:	Use this field to exclude lines following a given pattern. Regular expressions can be used, or a coma separated list of strings.
Occurence:	In COUNT mode: The threshold for the maximum number of lines matching the filters. In FORWARD mode, the minimum number of (identical) matching lines necessary to forward the line in an alarm.
Period:	Defines how far in the past the probe will look for log lines. If set to 60, it will look for log lines written in the last 60 minutes.
Severity:	The level of severity of the alarm generated by this line of surveillance.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

©copyright 2014 AGENTIL – all rights reserved

Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

Warning: In forward mode, if the period wider than the occurrence time of the monitor, you might receive duplicated alerts.

Alarm tag

To make alarms easier to sort in the alarm console, you can set a prefix to use in the alarm message. This can be useful if you have lots of surveillance rules.

QOS

If QOS is enabled on a given line, it will send a QOS named SAPBASIS_SYSLOG_OCCURENCE, containing the number of log lines matching the filter.

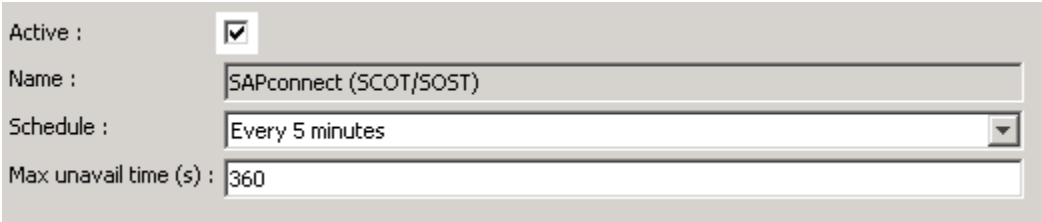
20. SAPconnect (SOST/SCOT)

Monitoring capabilities

Monitors email, Fax and pager messages sent by a netweaver instance. The probe will check for messages in ERROR or WAITING states that were sent during a past period. Filters can be applied on the client, the node, the receiver and the subject of the message. If the number of messages matching the filter is greater than a threshold, an alarm will be sent.

Job schedule definition

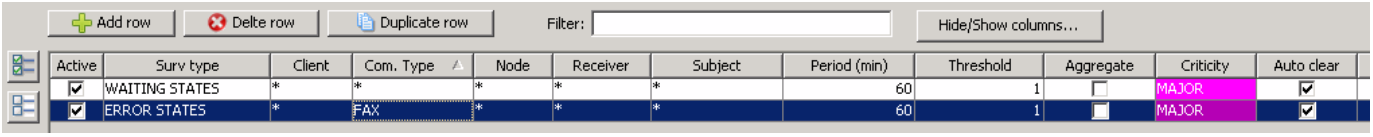
The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 5 minutes, but you can set a different schedule:



Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring. You can apply filters based on the client, the node, the receiver, the subject and the type of message. The threshold field will define when to trigger an alarm.

©copyright 2014 AGENTIL – all rights reserved



Active	Surv type	Client	Com. Type	Node	Receiver	Subject	Period (min)	Threshold	Aggregate	Criticity	Auto clear
☑	WAITING STATES	*	*	*	*	*	60	1	☐	MAJOR	☑
☑	ERROR STATES	*	FAX	*	*	*	60	1	☐	MAJOR	☑

Active: If checked, the rule is enabled and will be processed

Client: Filter the surveillance for a given client. A star ('*') will match any client.

Com. Type: Defines which type of message to look for. Select * for any.

Node: Filter the surveillance for a given node. A star ('*') will match any node.

Receiver: Filter the surveillance for a given receiver. A star ('*') will match any receiver.

Subject: Filter the surveillance for a given subject. A star ('*') will match any subject.

Period: The period of time in the past (computed from now) to look for messages.

Threshold: The alarm threshold. If the number of messages matching the monitoring rule is greater or equal to the threshold, the alarm will be triggered.

Aggregate: If enabled, one alarm will be triggered if the number of messages matching the rule is greater than threshold. If not enabled, one alarm per message matching the rule will be sent.

Severity: Defines the level of severity of the alarm that will be generated if one of the thresholds is reached.

Autoclear: If set, the generated alarms will be automatically cleared from the console if the alarm condition is not fulfilled anymore.

Alarm tag: You can define some text to use as a prefix of the alarm message generated by the current rule.

Alarm/QOS: Defines if an alarm/metric has to be generated for the given rule.

QOS

- These are the metrics that will be generated if the QOS option is enabled:
- SAPCONNECT_TRANSFER_WAITING: The number of waiting messages
- SAPCONNECT_TRANSFER_ERROR: The number of messages in error

21. ABAP instance response time

Monitoring capabilities

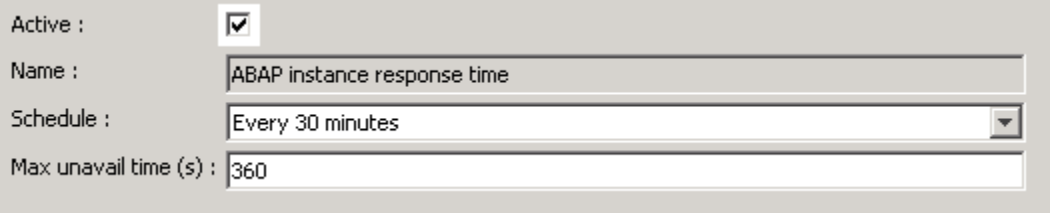
This monitor is dedicated to the monitoring of the ABAP instances response time, for DIALOG, SPOOL and UPDATE tasks.
Three metrics can be watched: Total response time, Database response time and the number of steps per minute. The metrics are computed over a configurable period of time.

©copyright 2014 AGENTIL – all rights reserved

Use the surveillance table to adjust the monitoring settings: Thresholds, severity, filters, etc...
Thresholds are independent from each other, and can be set to 0 if no check is requested

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 30 minutes, but you can set a different schedule:



Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring:

Active	Task	Max response time (ms)	Max DB resp. time (ms/%)	Max steps rate (steps/min)	Min step count	Period (Min)	Severity	Auto clear
☑	DIALOG	800	40%	0	100	30 minutes	MAJOR	☑
☑	SPOOL	1	0	0	1	5 minutes	MAJOR	☑
☑	UPDATE	1	0	0	1	5 minutes	MAJOR	☑

Active:	Use this field to activate or deactivate a line of configuration.
Task:	Defines the task to watch
Max response time:	The threshold for the average time per step (Milliseconds) for a given task, within the configured period
Max DB response time:	The threshold for the average DB response time. Can be absolute value (Milliseconds) or a percentage of total response time (in that case, specify the % unit).
Max steps rate:	The threshold for the average number of steps per minute over the configured period.
Min step count:	The minimum number of steps encountered within the period. If below the limit, response times won't be computed and no alarms will be sent.
Period:	The period of time used to compute response time. If set to 10 minutes, it will look for the steps that occurred 10 minutes before the start of the check.
Severity:	The level of severity of the alarm generated by this line of surveillance.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

©copyright 2014 AGENTIL – all rights reserved

22. SAP users

Monitoring capabilities

This monitor is dedicated to the surveillance of SAP user connections on the system. It will look for interactive, RFC and plugin users and triggers alarm if the number of connected users reaches a threshold.

Use the surveillance table to define the configuration of the monitoring: Instances, thresholds, severity, etc...

Four thresholds can be defined, one for the total number of connections, and three others for Interactive, RFC and plugin users.

Leave a threshold to 0 if unused

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 15 minutes, but you can set a different schedule:

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring. You can apply filters based on the instance name:

Active	Instance	Max active users	Max interactive users	Max RFC users	Max pluggin users	Severity
☑	*	0	0	0	0	MAJOR

Active:	Use this field to activate or deactivate a line of configuration.
Instance:	A filter to match only a subset of instances.
Max active users:	Sets the threshold for the total number of connection (sums interactive, RFC and plugin)
Max interactive users:	The threshold for interactive users.
Max RFC users:	The threshold for RFC users.
Max pluggin users:	The threshold for plugin users.
Severity:	The level of severity of the alarm generated by this line of surveillance.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

©copyright 2014 AGENTIL – all rights reserved

Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.

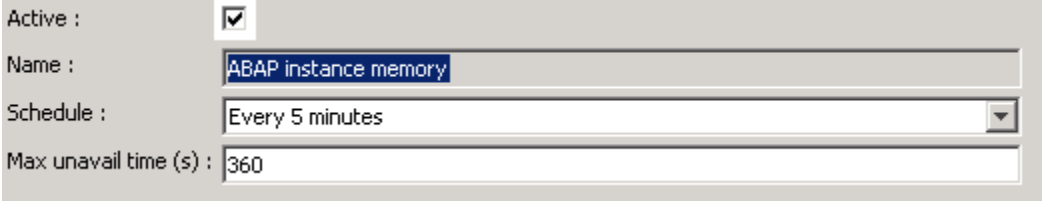
23. ABAP instance memory

Monitoring capabilities

This monitor is dedicated to the monitoring of ABAP instances memory. The focus will be put on extended and heap memory usage, paging and rolling memory.
Use the surveillance table to adjust the monitoring settings: Instance, thresholds, severity, etc...
Thresholds are independent and can be set to 0 if not used.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 5 minutes, but you can set a different schedule:



Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring. You can apply filters based on the instance name:

Active	Instance	Max Extended Mem (%/MB)	Heap usage (%/MB)	Peak heap usage (%/MB)	Max paging (%)	Max rolling (%)	Severity	Auto clear
☑	*	95%	50%	50%	90%	1%	WARNING	☑

Active:	Use this field to activate or deactivate a line of configuration.
Instance:	A filter to match only a subset of instances.
Max extended memory:	The threshold for the extended memory usage. Use absolute value (Megabytes) or percentage of total available (specify % unit).
Heap usage:	The threshold for heap memory usage. Use absolute value (Megabytes) or *percentage of the total extended memory* (specify % unit)
Peak heap usage:	The threshold for the maximum heap usage since instance startup. Use absolute value (Megabytes) or *percentage of the total extended memory* (specify % unit)
Max paging:	The threshold for the max paging memory in percent.
Max rolling:	The threshold for the max rolling memory in percent.
Severity:	The level of severity of the alarm generated by this line of surveillance.

©copyright 2014 AGENTIL – all rights reserved

Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

24. SAP buffers

Monitoring capabilities

This monitor is dedicated for the detection of SAP buffers. It will look for buffer used space, hit ratio, directory used, swap rate and quality.
Hit ratio, swap rate and buffer quality metrics can be computed since the startup of the instance, or within a period of time.
Use the surveillance table to define the buffers monitoring settings: Buffer name, thresholds, severity, filters, etc...
Note: Once you defined a surveillance line for a specific buffer name, other lines using "*" as buffer name filter will not match the specified buffer name.
Multiple severity syntax: All thresholds can be defined by using the multiple severity syntax

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 30 minutes, but you can set a different schedule:

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring. You can apply filters based on the instance and buffer name:

Active	Instance	Buffer name	Max used space ...	Min hit ratio (%)	Max dir. used (%)	Max swap (%)	Min quality (%)	Period (min)	Min Requests	Severity
☑	*	*	95	80	95	50	80	30	200	MAJOR
☑	*	Program	0	80	95	50	80	30	200	MAJOR

Active:	Use this field to activate or deactivate a line of configuration.
Instance:	A filter to match only a subset of instances.
Buffer name:	The name of the buffer to look for, or * for any buffer.

©copyright 2014 AGENTIL – all rights reserved

Max used space:	The threshold for the current used space of a given buffer (percent).
Minimum hit ratio:	The threshold for the minimum hit ratio for a given buffer. Computed from instance startup or within a period.
Max directory used:	The threshold for the maximum directory usage of a given buffer. Computed from instance startup or within a period.
Max swap:	The threshold for the maximum swap rate of a given buffer. Computed from instance startup or within a period.
Minimum quality:	The threshold for the minimum quality rate of a given buffer. Computed from instance startup or within a period.
Period:	If a value greater than 0 is set, it will define the period for the computation of hit ratio, swap and quality rate metrics. Computed since startup otherwise.
Min Requests:	Define a minimum of requests to consider the computed metrics as relevant. Below this value, no alarms will be sent.
Severity:	The default level of severity of the alarm generated by this line of surveillance. Applies when multiple severity syntax is not used
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

25. SAP spools

Monitoring capabilities

This monitor is dedicated for the monitoring of spools and spool requests: Used number and size for the spools, status and waiting time for the spool requests.
The configuration can be set via the two surveillance tables. The first one has a fixed size and allows to define spool size and used number thresholds.
The second is dedicated to the requests and allows to create any number of surveillance rules.
Use the surveillance tables to adjust the monitoring settings: Thresholds, severity, filters, etc...
Unused thresholds have to be set to 0. Thresholds are independent one on the other.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 30 minutes, but you can set a different schedule:

©copyright 2014 AGENTIL – all rights reserved

Active :	☑
Name :	Spools
Schedule :	Every 30 minutes
Max unavail time (s) :	360

Surveillance table for Spools

Surveillance rules have to be added in the table in order to define the monitoring:

Active	Metric	Threshold	Severity	Aggregate	Auto clear
☑	Max spool number utilization (%)	50	MAJOR	☑	☑
☑	Max spool size (MB)	50 MB	WARNING	☑	☑

Active: Use this field to activate or deactivate a line of configuration.

Metric: Read only field, defines the metric being configured (used number or size)

Threshold: The threshold of the corresponding metric, expected percent for used number and Megabytes for size for size.

Severity: The level of severity of the alarm generated by this line of surveillance.

Aggregate: If checked, the generated alarms will indicated the number of spools breaking the threshold. Otherwise, an alarm will be sent for each spool over the limit, indicating spool details.

Auto clear: If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

Alarm tag: This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.

Alarm: If checked, this line of surveillance will be used for alarm generation.

QOS: If checked, this line of surveillance will be used for QOS generation.

Report: If checked, this line of surveillance will used for showing threshold and severity in the daily report

Surveillance table for Spool requests

Surveillance rules have to be added in the table in order to define the monitoring. You can apply filters based on the output device and on the printer.

Active	Output Device	User	Max completed ...	Comp. w. error sev	Max Errors	Error severity	Max wait time (min)	Max wait severity	Aggregate	Auto clear
☑	*	*	0	WARNING	1	MAJOR	480	WARNING	☑	☑

Active: Use this field to activate or deactivate a line of configuration.

Output device: A filter to match a subset of printers. Use * to match all.

User: A filter to match only a subset of users. Use * to match all

Max completed with error: The threshold for the maximum number of requests with "Completed with error" status.

©copyright 2014 AGENTIL – all rights reserved

Max completed with error severity:	The severity for the "max completed with error" alarm.
Max errors:	The threshold for the maximum number of requests with "error" status.
Error severity:	The severity for the "error" alarm.
Max wait time:	The threshold for the time a requests can stay in "Waiting" status. Set in minutes.
Max wait severity:	The severity for the "waiting requests" alarm.
Aggregate:	If checked, generated alarm will report the number of requests breaching a threshold. If not checked, one alarm per request will be sent.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

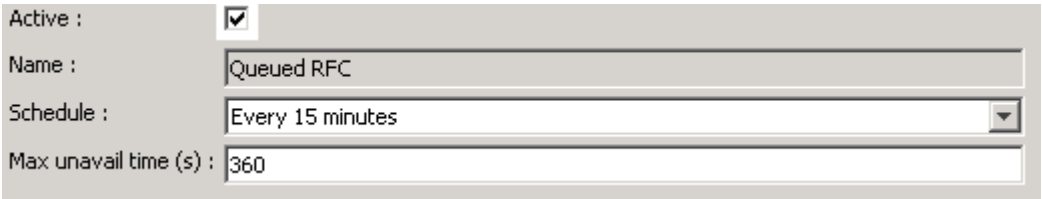
26. QRFC

Monitoring capabilities

This monitor is dedicated to the monitoring of QRFC queues. It can watch for queue error status, the number of current entries and too old entries.
The surveillance can be customized to match a specific queue, client, destination or direction. Use the table to configure the monitoring settings: Thresholds, severity, filters, etc...
Unused thresholds can be set to 0. Thresholds are independent.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 15 minutes, but you can set a different schedule:



©copyright 2014 AGENTIL – all rights reserved

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring. You can define filters based on the client, the queue, the destination and the direction:

Active	Client	Queue	Destination	Direction	Error Sev.	Max entries	Max Sev.	Oldest entry age (min)	Queue status	Wait Sev.
☑	*	*	*	INBOUND	MAJ	50	WAR	30	ANY	WAR
☑	*	*	*	OUTBOUND	DIS	100	WAR	0	ANY	DIS
☑	*	*	*	OUTBOUND	MAJ	0	DIS	1440	ANY	WAR

Active: Use this field to activate or deactivate a line of configuration.

Client: A filter to match only a subset of clients.

Queue: A filter to match only a given queue or subset of queues.

Destination: A filter to match a given destination.

Direction: Defines if the rule is to be applied for INBOUND or OUTBOUND queues.

Error severity: The severity of the alarm in case of queue error status.

Max entries: A threshold to define the maximum number of entries per queue.

Max severity: The severity of the alarm sent in case of too many entries.

Oldest entry age: The threshold for the age of the oldest entry in a queue, in minutes.

Queue status: Defines the status of the queue for which the "old entry check" will be performed. If NOSEND is set, it will only watch for old entries of queues having NOSEND status.

Wait severity: Defines the severity of the alarm sent for old entries.

Aggregate: If checked, for each breached threshold, only one alarm will be sent, indicating how many queues are over the limit. If not checked, one alarm per queue will be sent.

Auto clear: If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

Alarm tag: This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.

Alarm: If checked, this line of surveillance will be used for alarm generation.

QOS: If checked, this line of surveillance will be used for QOS generation.

Report: If checked, this line of surveillance will used for showing threshold and severity in the daily report

27. TRFC

Monitoring capabilities

This monitor is dedicated to the monitoring of TRFC. It will watch for the number of TRFC having a given status and for age of the TRFC entries. You can customize the monitoring for a specific direction, destination, function/program or user. Use the surveillance table to adjust the monitoring settings: Thresholds, severity, filters, etc... Unused threshold has to be set to 0.

©copyright 2014 AGENTIL – all rights reserved

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 30 minutes, but you can set a different schedule:

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring. You can define filters based on the direction, the destination, the function/program or the user:

Active	Direction	Destination	Function/Prog	User	Status	Max entries	Max Sev.	Max entry age (hours)	Age Sev.
☑	OUTBOUND	*	*	*	ANY	0	DISABLED	1	WARNING
☑	OUTBOUND	*	*	*	IN_ERROR	1	MAJOR	0	DISABLED
☑	INBOUND	*	*	*	ANY	0	DISABLED	1	WARNING
☑	INBOUND	*	*	*	IN_ERROR	1	MAJOR	0	DISABLED

Active: Use this field to activate or deactivate a line of configuration.

Direction: The direction of the TRFC entries to check.

Function/Program: A filter to match only a given function or program

User: A filter to match only a given user or subset of users.

Status: Defines the status of the TRFC entries to check. If set to SYSFAIL, it will only look for entries with SYSFAIL status.

Max entries: Defines the maximum number of entries matching the filters and status.

Max severity: Defines the severity of the alarm sent if maximum number of entries is reached.

Max entry age: Defines the maximum age of a TRFC entry matching the filters. Specified in hours.

Age severity: The severity of the too old entries alarm.

Auto clear: If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

Alarm tag: This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.

Alarm: If checked, this line of surveillance will be used for alarm generation.

QOS: If checked, this line of surveillance will be used for QOS generation.

Report: If checked, this line of surveillance will used for showing threshold and severity in the daily report

©copyright 2014 AGENTIL – all rights reserved

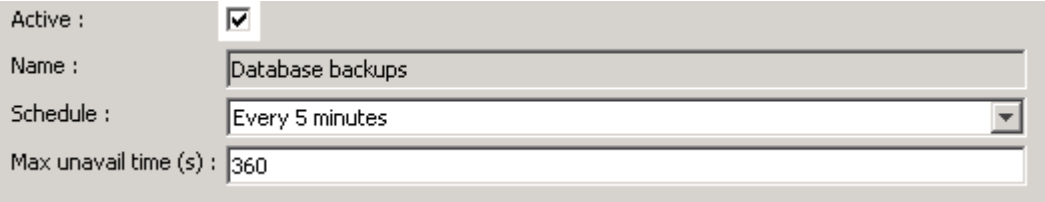
28. Database backups

Monitoring capabilities

This monitor is dedicated to the monitoring of database backups. It will work independently from the type of database and is compatible with Oracle, MSSQL and DB2. For each type of backup, you can define a customized monitoring. The probe will monitor the backup status, duration, size (MSSQL only) and occurrence. Use the surveillance table to adjust the monitoring settings: Thresholds, severity, filters, etc...

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 5 minutes, but you can set a different schedule:



Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring:

Active	Backup type	Error sev.	Unknown sev.	Min. error level	Max duration (min)	Max size (Mb)	Max Age (min)	Default Criticity
☑	ANY	MAJOR	WARNING	1	0	0	0	MAJOR

Active:	Use this field to activate or deactivate a line of configuration.
Backup type:	Defines which type of backup you want to monitor. Be careful to choose a type appropriate for your database. If ANY is selected, all backup entries will be checked.
Error severity:	Defines the severity of the alarm sent in case of backup error. Set to DISABLED if not used.
Unknown severity:	Defines the severity of the alarm sent in case of backup with an UNKNOWN status. Set to DISABLED if not used.
Minimum error level:	For MSSQL database, there are some error status that you might want to ignore. Use this field to set the level that you want to consider as an error.
Max duration:	Defines the maximum duration for a backup.
Max size:	Defines the maximum size of a backup (works for MSSQL only).
Max age:	Defines the maximum time elapsed since the last backup.
Default Severity:	The default level of severity applied for a generated alarm if the multiple severity syntax is not used for a threshold.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

©copyright 2014 AGENTIL – all rights reserved

Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

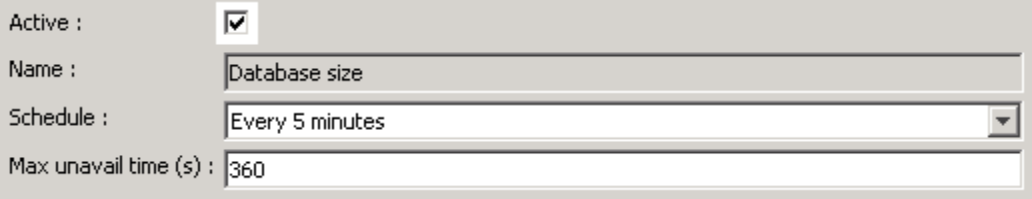
29. Database size

Monitoring capabilities

This monitor is dedicated to the monitoring of SAP database size. The probe will watch for data and log used space as well as current log mode. For Oracle and DB2 databases, it will also monitor the tablespaces used space. A first surveillance table will be dedicated to the configuration of global database used space monitoring. A second one will be for the tablespaces Use the surveillances table to adjust the monitoring settings: Thresholds, severity, filters, etc... Unused thresholds have to be set to 0.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 5 minutes, but you can set a different schedule:



Surveillance table for global DB size

Surveillance rules have to be added in the table in order to define the monitoring:

Active	Max TOTAL used space (%) - DB2 ONLY	Max DATA used space (%)	Max LOG used space (%)	Expected LOG mode	Severity
☑	80	80	80	FULL (MSSQL)	MAJOR

Active:	Use this field to activate or deactivate a line of configuration.
Max TOTAL used space:	The threshold for the used space of the total maximum available. Only available for DB2, it will have no effect on other DB.
Max DATA used space:	The threshold for the used space of the total available space for DATA.
Max LOG used space:	The threshold for the used space of the total available space for LOG
Expected LOG mode:	Define the LOG mode that is expected.
Severity:	The level of severity of the alarm generated by this line of surveillance.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

©copyright 2014 AGENTIL – all rights reserved

Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

Surveillance table for tablespaces

Surveillance rules have to be added in the table in order to define the monitoring:

Active	Tablespace	Max used space (%)	Severity
☑	*	80	MAJOR

Active:	Use this field to activate or deactivate a line of configuration.
Tablespace:	The tablespace name to look for. You can use * to match any tablespace or regular expressions.
Max used space:	The threshold for the tablespace used space.
Severity:	The level of severity of the alarm generated by this line of surveillance.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report.

30. SAP change settings

Monitoring capabilities

The probe will check that system and clients change modes are matching the monitoring configuration. You can define the expected global change mode of the SAP system and make sure to be notified as soon as the mode changes. This can be used primarily to make sure that your production system cannot be modified. For each client or for each type of client role, you can define the expected customization options. You can also check that each client has the correct logical name. Use the surveillance table to adjust the monitoring settings: Thresholds, severity, filters, etc...

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run once a day at 8:00, but you can set a different schedule:

©copyright 2014 AGENTIL – all rights reserved

Active :	☑
Name :	SAP change settings
Schedule :	Once a day at 8:00 am
Max unavail time (s) :	360

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring:

Active	Client	Logical name	Role	Client change	Cross client custo change	Cross client repository change	Severity
☑	*	*	Production	☐	☐	☐	MAJOR

Active:	Use this field to activate or deactivate a line of configuration.
Client:	Define the client for which to set the rule, or * for a role based surveillance.
Logical name:	The expected logical name for a given client (Client has to be specified in client field)
Role:	If Client field contains *, this rule will define the customization settings for all clients associated to the given role. If a specific client is set in client field, it will also check that the client is associated to the given role.
Client change:	Defines if the client configuration can be changed or not.
Cross client customization change:	Defines if cross client customization is enabled or not.
Cross client repository change:	Defines if cross client repository change is enabled or not
Severity:	The level of severity of the alarm generated by this line of surveillance.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

31. Custom CCMS monitoring

31.1. Purpose

This monitor is dedicated to SAP implementations where the CCMS is used as main monitoring interface. In such case, the CCMS is often widely customized, and the time spent on this configuration cannot be invested again in another monitoring interface.

©copyright 2014 AGENTIL – all rights reserved

By using this monitor, you can decide to simply forward CCMS alarms and metrics into UIM Monitor. This lets the monitoring configuration stay in SAP. No additional configuration is needed in the probe.

But this monitor has also the capability to import the CCMS alarm definitions (thresholds, severity, messages, etc…) into the probe, and to migrate the monitoring configuration away from SAP. This gives the advantage of being able to use the efficient and time saving template mechanism. Instead of having a spread CCMS configuration over all your systems, this will be regrouped in one single template.

The visibility of the configuration becomes much better, and the deployment of configuration updates becomes a single click action.

31.2. Configuration

This monitor is similar than any other monitors in the probe, in the way you will enable it on a system. You first need to add this monitor in a template (existing or new). Then, you can open its definition panel by selecting the monitor node in the template's tree.

31.2.1. Execution definition

The common execution parameters of the monitor can be set from the definition panel. The schedule and activation state are defined here and can be modified according to your needs.

The monitor will be executed periodically, based to the chosen schedule. For each execution, it will collect CCMS metrics according to the monitoring configuration.

The collection time defined in the CCMS is not followed. The monitor will always fetch the latest available values at the rate of its executions. For example, if the schedule is set to run every 5 minutes, all metrics will be collected at this rate, even if the collection rate set in the CCMS is 30 seconds, or 1 hour.

31.2.2. Monitoring definition

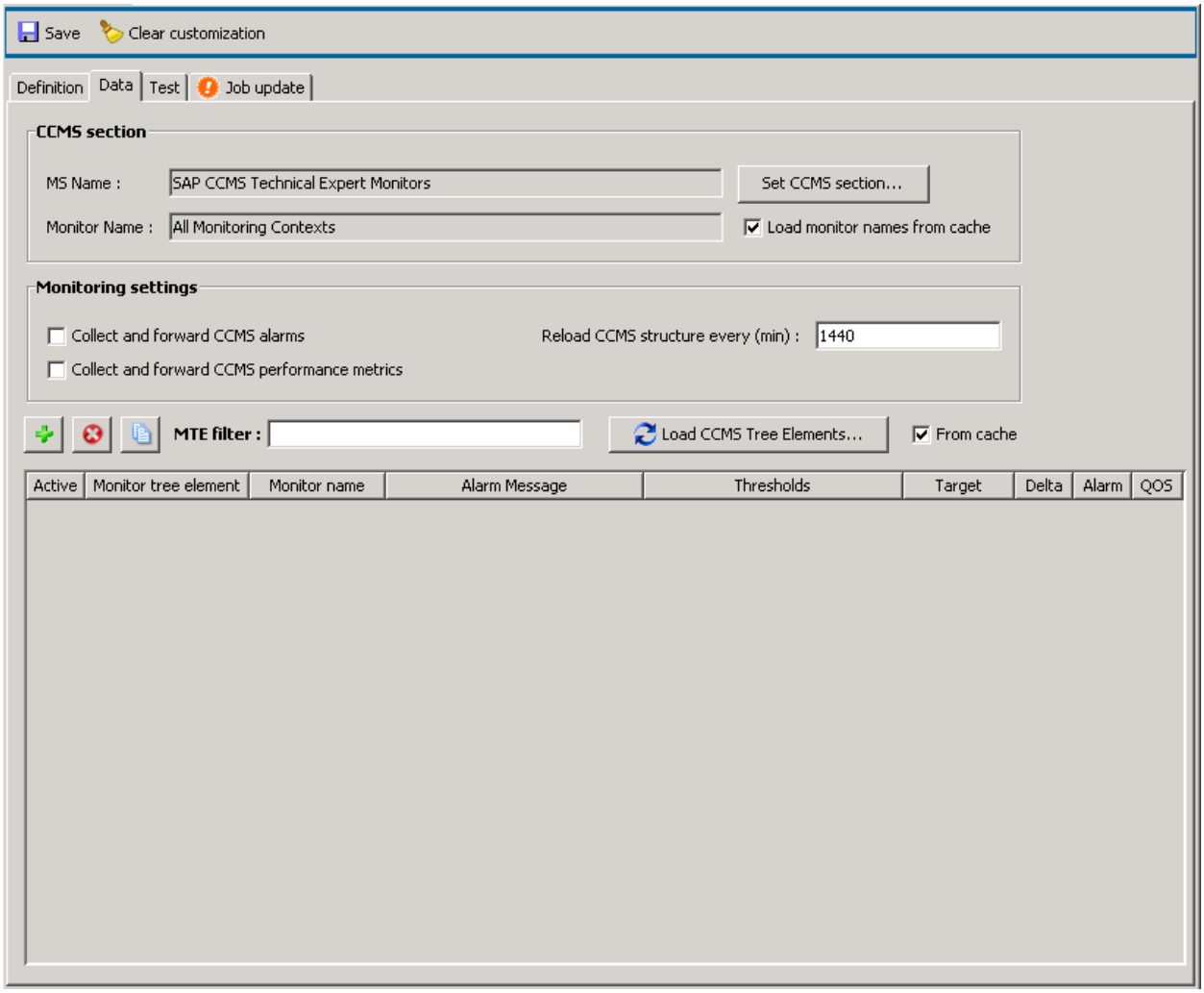
The Data tab is where the CCMS monitoring can be configured and customized. For this monitor, there are three different ways of implementation.

The first one is simply to *"forward"* all CCMS alarms and performance metrics into UIM Monitor, as it is. Any modification of the monitoring has to be done in the CCMS for each system.

The second one is the opposite. Instead of passively forwarding what comes from the CCMS, you can define exactly which metrics you want to collect and how you want to monitor them. All the settings will then be located in the probe. The CCMS will only be used to get metric values.

The third one is a combination of the two first: You can collect and forward all CCMS metrics and/or alarms by default, but set in the probe a specific configuration for a subset of metrics.

©copyright 2014 AGENTIL – all rights reserved



CCMS section definition

The configuration of this monitor starts by defining which CCMS section will be collected. By default, it will collect elements from *"SAP CCMS Technical Expert Monitors, All monitoring contexts"* section, which covers all available metrics. However, you can choose to collect metrics from any other available sections. Use the "Set CCMS section" button to get a list of available sections, and select the one you want to monitor.

Note: Custom CCMS monitor can collect only one context section of the CCMS tree.

Monitoring settings : Forward CCMS metrics

Once you have defined the CCMS section, you can set how the monitoring information will be forwarded to UIM Monitor.

If you want to forward **all** performance metrics, you simply need to check the "Collect and forward performance metrics" checkbox. The probe will convert CCMS metrics into UIM QoS. It will then be visible in the SLM and UMP widget.

©copyright 2014 AGENTIL – all rights reserved

Warning: CCMS can contain a lot of metrics, and using this option may generate lots of QOS data, including a potentially large number of irrelevant ones. To use only if you are sure that you want ALL CCMS numeric values to be forwarded as QOS.

If you want to forward **all** CCMS alarms, you need to check the "Collect and forward CCMS alarms" checkbox. The probe will get current CCMS alarms and convert them into UIM alarms signals. The alarms will then appear in UIM's alarm manager. CCMS red flag alarms are mapped to Critical severity. Yellow flag is mapped to warning.

Actions applied on alarms from UIM monitor (Accept, acknowledge, etc...) won't have any effect on alarms status in the CCMS. But if an alarm is cleared in the CCMS, it will also be cleared in UIM monitor.

Note: It is not mandatory to select one of these checkboxes in order to get any alarm or metric. If you are only interested in a subset of metrics, you simply need to declare the CCMS path of these metrics in the surveillance table, without selecting any checkbox. You can also decide to forward all alarms, but only a subset of metrics, etc…

Monitoring settings : CCMS structure refresh

A startup, the probe will collect the CCMS tree structure and data. When the monitor runs, it will only refresh metric values, but not the structure of the tree itself. That means that if a new node is added in the tree, it will not be detected right away.

Loading tree structure is very consuming in time (5 to 40 seconds) and memory and cannot be executed for each run. However, you can set a timer after which the probe will refresh the CCMS tree structure. To refresh the structure every 4 hours is usually a good tradeoff, the CCMS structure is not meant to change so often.

This timer can be set in the "Reload CCMS tree structure" field.

Conversion of CCMS metrics into UIM's Alarms and QoS

Before going further, you need to be aware of few constraints that exist in UIM Alarms and QoS objects. To understand these aspects will help you to generate accurate and useful Alarms and QoS.

Concerning QoS, you must distinguish QoS definition from QoS data. Qos definition identifies a type of metric, with a unique, meaningful name. In this definition will also be set units, metric boundaries, sample rate etc… This definition is declared once.

When a metric is later collected from SAP, a QoS container will be used to transport the metric value itself, and also the source of the data (the SAP system), and the target (the instance name, disk name, client name, etc…).

This container will be associated to its definition by the name.

Example: Let's consider the following type of metrics: *Free disk space in percent.*

The QoS definition will be like:

©copyright 2014 AGENTIL – all rights reserved

- Name : Free disk space
- Unit : percent
- Max value : 100
- Etc…

Then, given that we are monitoring 2 systems with 2 disks each, generated QoS for each run will look like this :

- Name=Free disk space, Source=QAL, Target=C:, Value=20%
- Name=Free disk space, Source=QAL, Target=D: , Value=25%
- Name=Free disk space, Source=PRD, Target=C: , Value=37%
- Name=Free disk space, Source=PRD, Target=D: , Value=28%

This example shows that QoS definition will be a common reference for metrics coming from different systems. In a data analyses perspective, it is important to be able to identify similar metrics from different systems, and to organize them in a way that they can be displayed and analyzed as being the same type of object.

You can now understand that the probe must have a way to know how to group metrics into a common QoS definition. It also needs a way to identify which information to put in the target field.

This is the mechanism that the probe is currently using to achieve this:

CCMS metrics are considered from the same type if they belong to the same attribute group. (Defined in *PROPERTIES.ATTRGROUP* of the *BAPI_SYSTEM_MTE_GETPERFPROP* result)

In order to identify the target part of a metric, we do the following: All metrics belonging to the same group are compared together. Nodes of the paths that are not constant are then considered as target parts.

<u>Example:</u>

Let's consider metrics coming from following CCMS paths:

- *AGLGESRVSAP03_PRD_10\OperatingSystem\Filesystems\C:\Percentage_Used*
- *AGLGESRVSAP03_PRD_10\OperatingSystem\Filesystems\D:\Percentage_Used*
- *AGLGESRVSAP02_QAL_00\OperatingSystem\Filesystems\C:\Percentage_Used*
- *AGLGESRVSAP02_QAL_00\OperatingSystem\Filesystems\D:\Percentage_Used*

These metrics are considered as belonging to the same type, because they all belongs to the same CCMS group: *CG_FilesystemPercentageUsed*

If we compute the target field based on the changing nodes of the path, we find the following:

- Target 1 : *AGLGESRVSAP03_PRD_10 – C:*
- Target 2 : *AGLGESRVSAP03_PRD_10 – D:*

©copyright 2014 AGENTIL – all rights reserved

- Target 3 : *AGLGESRVSAP02_QAL_00 – C:*
- Target 4 : *AGLGESRVSAP02_QAL_00 – D:*

The result will be that 4 QoS objects will be sent to UIM Monitor, they will all belong to the *CG_FilesystemPercentageUsed* QoS definition, but will have a different target, source and value field.

The same constraints exist for Alarms. As it is sometime difficult to recall the context of an alarm based on the alarm message, the probe will prefix each message by the attribute group name, and the context attribute of the path:

Example:

Alarm message:*" [CRM Middleware R&R Queues - Queues on Hold (100)] SUBCHECK on Hold"*

Warning: If the CCMS metrics are not properly organized and split across meaningful attribute groups, the QoS and Alarms signals that the probe will send might be difficult to use and understand in UIM monitor's side.

The meaningfulness of QoS and Alarm names directly depends on the ones of the CCMS attribute group names. In some cases, you might want to customize these group names to a more user friendly name, or to force metrics from different groups to belong to the same QoS definition. You can do this in the surveillance table described below.

Each fired alarm has a field called **the suppression key.** This is an identifier that is used to link a given CCMS metric with an alarm signal. If an alarm condition is cleared in the CCMS, this field is used to be able to clear the alarm in UIM monitor as well. The probe uses the CCMS path as suppression key, as it identifies exactly a given metric.

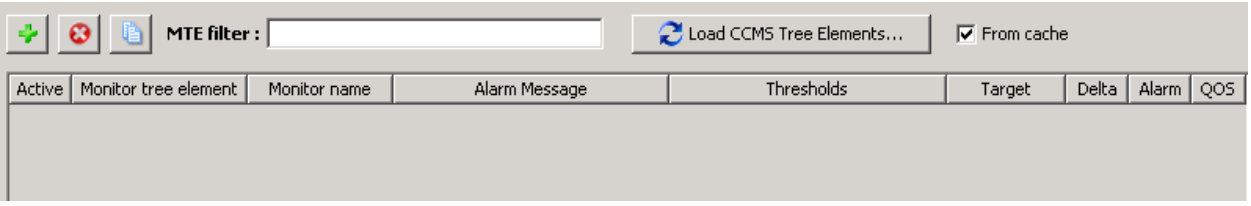
Customize CCMS metrics monitoring

The monitor has a surveillance table where you can explicitly define a CCMS path to collect and monitor. Once a path is set in the table, the way it will be monitored is no longer inherited from the CCMS, but it will follow the definition set in the table.

Each row of the table will define the monitoring to apply on a given CCMS path or group of paths. These are the available settings:

- **Active :** If unset, the definition won't be taken into account.
- **Monitor tree element :** The CCMS path itself.
- **Monitor name :** The place to set a meaningful name to the metric.
- **Alarm message :** The message template used to generate alarm messages.
- **Thresholds :** The definition of thresholds and alarm severities.
- **Target :** The definition of the QoS target pattern.
- **Delta :** Currently unused. Allows working on metric's evolution (delta) instead of raw value.
- **Alarm :** If checked, evaluates and sends alarm.
- **QoS :** If checked, sends QoS.

©copyright 2014 AGENTIL – all rights reserved

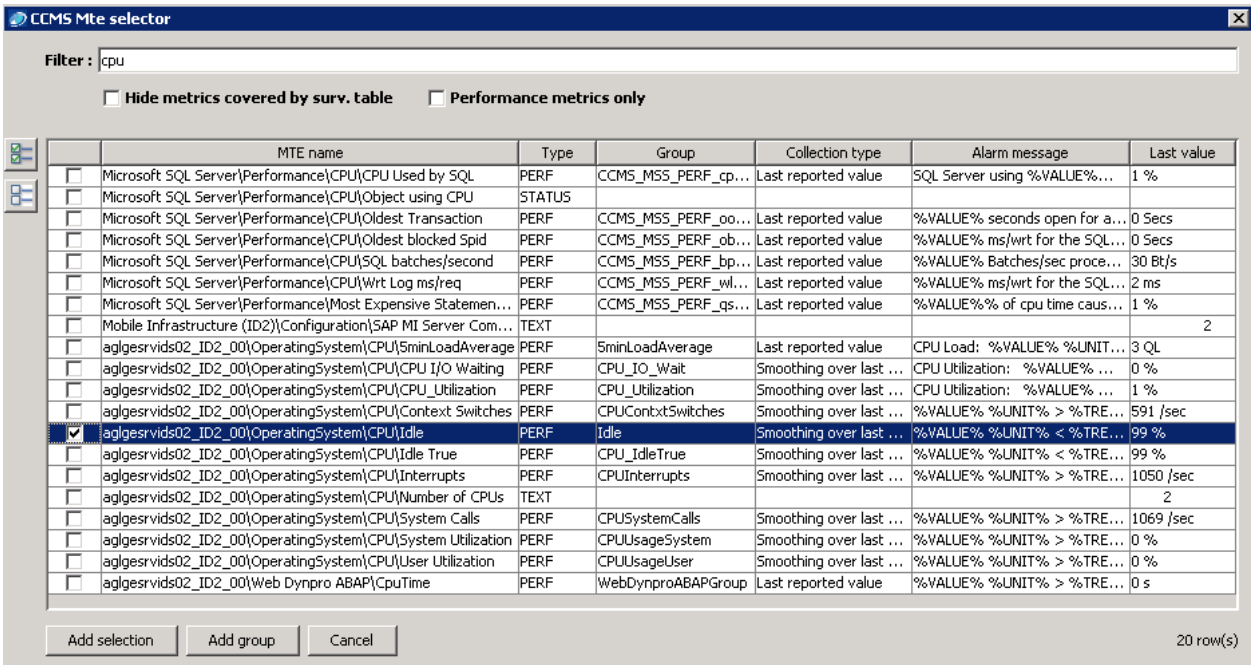


Instead of filling the table manually, you can load the available CCMS paths from one system and import the metrics you are interested in:

- Press on the "Load CCMS tree elements" button. This will load actual CCMS paths and display them in a table, along with group name, collection type, latest value and unit.
- Select the paths to import in the surveillance table

To import the paths, you have two possibilities:

- Selection import: Will simply import all the selected paths in the surveillance table. Use *"Add selection"* button.
- Group import: If you select one path, you can decide to import all the paths belonging to the same attribute group. Use the *"Add group"* button.



	MTE name	Type	Group	Collection type	Alarm message	Last value
☐	Microsoft SQL Server\Performance\CPU\CPU Used by SQL	PERF	CCMS_MSS_PERF_cp...	Last reported value	SQL Server using %VALUE%...	1 %
☐	Microsoft SQL Server\Performance\CPU\Object using CPU	STATUS				
☐	Microsoft SQL Server\Performance\CPU\Oldest Transaction	PERF	CCMS_MSS_PERF_oo...	Last reported value	%VALUE% seconds open for a...	0 Secs
☐	Microsoft SQL Server\Performance\CPU\Oldest blocked Spid	PERF	CCMS_MSS_PERF_ob...	Last reported value	%VALUE% ms/wrt for the SQL...	0 Secs
☐	Microsoft SQL Server\Performance\CPU\SQL batches/second	PERF	CCMS_MSS_PERF_bp...	Last reported value	%VALUE% Batches/sec proce...	30 Bt/s
☐	Microsoft SQL Server\Performance\CPU\Wrt Log ms/req	PERF	CCMS_MSS_PERF_wl...	Last reported value	%VALUE% ms/wrt for the SQL...	2 ms
☐	Microsoft SQL Server\Performance\Most Expensive Statemen...	PERF	CCMS_MSS_PERF_qs...	Last reported value	%VALUE%% of cpu time caus...	1 %
☐	Mobile Infrastructure (ID2)\Configuration\SAP MI Server Com...	TEXT				2
☐	aglgesrvids02_ID2_00\OperatingSystem\CPU\5minLoadAverage	PERF	5minLoadAverage	Last reported value	CPU Load: %VALUE% %UNIT...	3 QL
☐	aglgesrvids02_ID2_00\OperatingSystem\CPU\CPU I/O Waiting	PERF	CPU_IO_Wait	Smoothing over last ...	CPU Utilization: %VALUE% ...	0 %
☐	aglgesrvids02_ID2_00\OperatingSystem\CPU\CPU_Utilization	PERF	CPU_Utilization	Smoothing over last ...	CPU Utilization: %VALUE% ...	1 %
☐	aglgesrvids02_ID2_00\OperatingSystem\CPU\Context Switches	PERF	CPUContxtSwitches	Smoothing over last ...	%VALUE% %UNIT% > %TRE...	591 /sec
☑	aglgesrvids02_ID2_00\OperatingSystem\CPU\Idle	PERF	Idle	Smoothing over last ...	%VALUE% %UNIT% < %TRE...	99 %
☐	aglgesrvids02_ID2_00\OperatingSystem\CPU\Idle True	PERF	CPU_IdleTrue	Smoothing over last ...	%VALUE% %UNIT% < %TRE...	99 %
☐	aglgesrvids02_ID2_00\OperatingSystem\CPU\Interrupts	PERF	CPUInterrupts	Smoothing over last ...	%VALUE% %UNIT% > %TRE...	1050 /sec
☐	aglgesrvids02_ID2_00\OperatingSystem\CPU\Number of CPUs	TEXT				2
☐	aglgesrvids02_ID2_00\OperatingSystem\CPU\System Calls	PERF	CPUSystemCalls	Smoothing over last ...	%VALUE% %UNIT% > %TRE...	1069 /sec
☐	aglgesrvids02_ID2_00\OperatingSystem\CPU\System Utilization	PERF	CPUUsageSystem	Smoothing over last ...	%VALUE% %UNIT% > %TRE...	0 %
☐	aglgesrvids02_ID2_00\OperatingSystem\CPU\User Utilization	PERF	CPUUsageUser	Smoothing over last ...	%VALUE% %UNIT% > %TRE...	0 %
☐	aglgesrvids02_ID2_00\Web Dynpro ABAP\CpuTime	PERF	WebDynproABAPGroup	Last reported value	%VALUE% %UNIT% > %TRE...	0 s

Group imports

In order to reduce the amount of configuration work, it is very useful to be able to cover several paths with one row of the surveillance table.

©copyright 2014 AGENTIL – all rights reserved

This is done by using this simple syntax in CCMS path definition: Non constant nodes from a list of paths of the same group are replaced by the string *%VARx%*, where *x* is the depth of the node in the path.

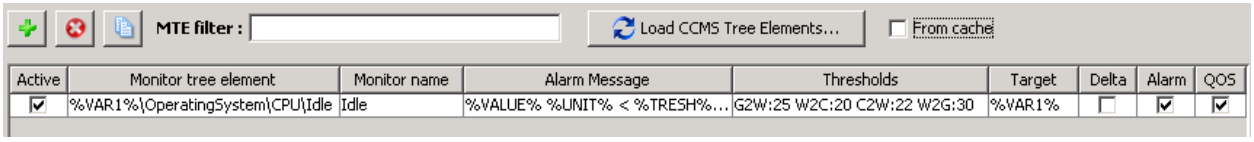
Example:

Consider the following paths:

- *AGLGESRVSAP03_PRD_10\OperatingSystem\Filesystems\C:\Percentage_Used*
- *AGLGESRVSAP03_PRD_10\OperatingSystem\Filesystems\D:\Percentage_Used*
- *AGLGESRVSAP02_QAL_00\OperatingSystem\Filesystems\C:\Percentage_Used*
- *AGLGESRVSAP02_QAL_00\OperatingSystem\Filesystems\D:\Percentage_Used*

To make a group import on these paths will generate the following surveillance pattern:

- ***%VAR1%**\OperatingSystem\Filesystems**%VAR4%**\Percentage_Used*



Active	Monitor tree element	Monitor name	Alarm Message	Thresholds	Target	Delta	Alarm	QOS
☑	%VAR1%\OperatingSystem\CPU\Idle	Idle	%VALUE% %UNIT% < %TRESH%...	G2W:25 W2C:20 C2W:22 W2G:30	%VAR1%	☐	☑	☑

Then, when parsing CCMS tree structure, all paths matching this surveillance pattern will be monitored according to the definition set in the row.

The advantages are several:

- Thresholds and severities settings defined in a unique row. Any update applies automatically to all paths from all systems using this surveillance table.
- Any new CCMS path matching this pattern will be automatically covered by the surveillance rule. No configuration needed if a new disk is added for example.
- You can combine paths belonging to different attribute groups in the same logical object. Useful if you have discrepancies in group naming across your systems.

Alarm message definition

When paths are imported in the surveillance table, the default alarm pattern set in the CCMS will be imported as well. From there you are free to refactor messages as you wish. We use a simple syntax that will help to easily build alarm message patterns. You can compose an alarm message and use variables that will be replaced at evaluation time:

- %VALUE% : The current value of the metric.
- %UNIT% : the unit associated with the metrics in the CCMS.
- %THRESH% : The threshold for which the alarm has been fired.
- %VARx% : The node name at the x'th depth in the path.

Example:

Consider the following alarm message pattern:

©copyright 2014 AGENTIL – all rights reserved

- "Free disk space on disk **%VAR4%** for instance **%VAR1%** is **%VALUE% %UNIT%**. Threshold is **%THRESH% %UNIT%**"

If the alarm is generated for this path:
AGLGESRVSAP03_PRD_10\OperatingSystem\Filesystems\C:\Percentage_Used

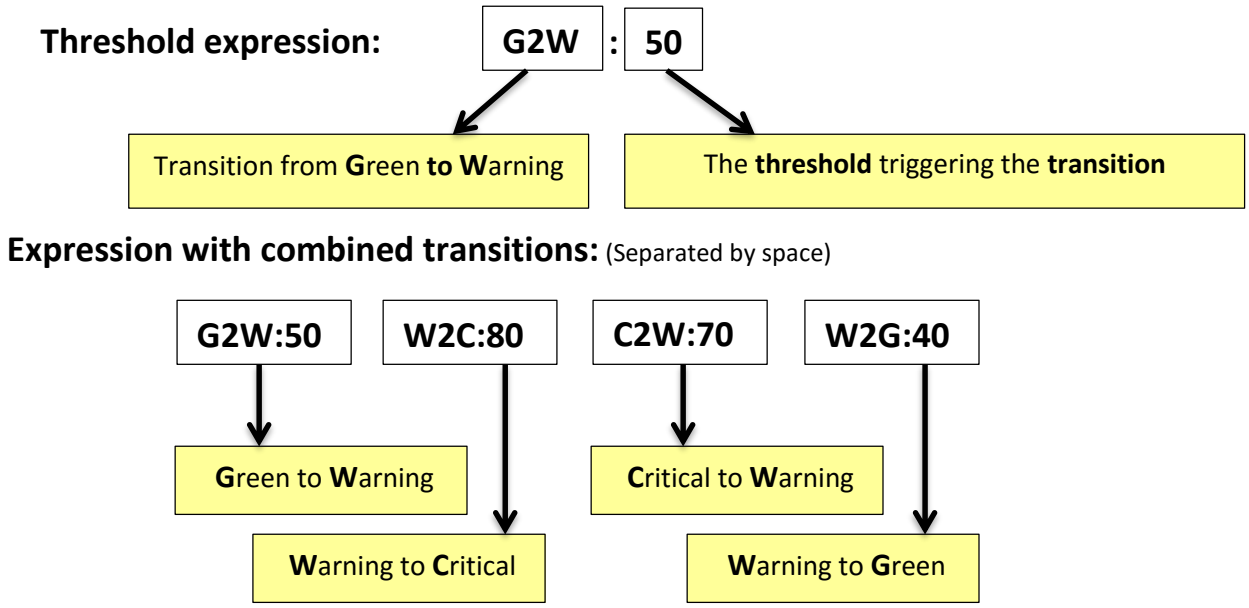
The alarm message would look like:

"Free disk space on disk **C:** for instance ***AGLGESRVSAP03_PRD_10*** is **50 Mb**. Threshold is **55 Mb"**

Thresholds and severities definition

When you import performance metric paths in the surveillance table, the CCMS default threshold, alarm message and severity will be imported as well. We use a simple syntax to easily customize thresholds and severity levels. The syntax is quite similar than in the CCMS, we use similar string patterns to define the transitions from one severity to another.

A threshold expression is defined with the following syntax:



©copyright 2014 AGENTIL – all rights reserved

Transition letters:

G	→	Green (no alarm)
I	→	Informational
W	→	Warning
m	→	minor
M	→	Major
C	→	Critical

Example:

G2W:70 W2C:90

Value t1 = 50	→	**G**reen (No alarm)
Value t2 = 80	→	**W**arning alarm
Value t3 = 90	→	**C**ritical alarm
Value t4 = 60	→	**G**reen (Alarm cleared)

G2W:70 W2C:90 C2W:80 W2G:60

Value t1 = 70	→	**W**arning alarm
Value t2 = 95	→	**C**ritical alarm
Value t3 = 85	→	**C**ritical alarm
Value t4 = 70	→	**W**arning alarm
Value t5 = 50	→	**G**reen (Alarm cleared)

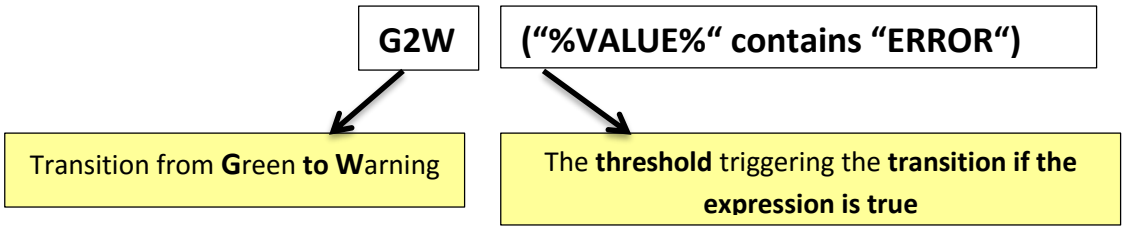
©copyright 2014 AGENTIL – all rights reserved

Available keywords:

== / !=	Checks if the following string is exactly equal to the reported value: → **”%VALUE%” == ”Update service is inactive”**
contains	Checks if the following string is present in the reported value: → **”%VALUE%” contains ”ABORTED”** **Ex: VALUE = “Job XYZ is aborted” → TRUE**
containsAND	Checks if all members of the following list of strings are present in the reported value: → **”%VALUE%” containsAND [”ABORTED”,”XYZ”,”job”]** **Ex: VALUE = “Job XYZ is aborted” → TRUE** **Ex: VALUE = “Job ABC is aborted” → FALSE**
containsOR	Checks if at least one member of the following list of strings is present in the reported value: → **”%VALUE%” containsOR [”ABORTED”,”XYZ”,”ABC”]** **Ex: VALUE = “Job XYZ is aborted” → TRUE** **Ex: VALUE = “Job ABC is aborted” → TRUE**
memberOf	Checks if the reported value equals at least to one of the member of the following list: → **”%VALUE%” memberOf [”ABORTED”,”ERROR”,”FAILED”]** **Ex: VALUE = “Aborted” → TRUE** **Ex: VALUE = “FAILED” → TRUE**

©copyright 2014 AGENTIL – all rights reserved

Syntax for alphanum values:



Example:

G2W:("%VALUE%" contains "WARNING")

Value t1 = "Backup finished with warnings"

→ Send **W**arning alarm

Value t2 = "Backup finished successfully"

→ No alarm sent

G2W:("%VALUE%" contains "WARNING") W2C:("%VALUE%" contains "ERROR")

Value t1 = "Backup finished with warnings"

→ Send **W**arning alarm

Value t2 = "Backup finished with errors"

→ Send **C**ritical alarm

G2C:("%VALUE%" contains "JOB_XYZ"
and "%VALUE%" containsOR ["ERROR","FAILED"])

Value t1 = "Job_XYZ failed to run"

→ Send **C**ritical alarm

Value t2 = "Job_XYZ finished with errors"

→ Send **C**ritical alarm

©copyright 2014 AGENTIL – all rights reserved

Note: You don't need to define the complete transition path: *"G2W:50 W2C:90"* is sufficient if you want to keep the same threshold value for lowering down the severity.

Note: The lower is better/higher is better aspects are handled automatically.

QoS target definition

When you import a path in the surveillance table, the target field will be computed according to the other available paths belonging to the same group. However, you are free to modify the target string pattern that you want to see in QoS.

The syntax is quite similar than alarm message definition. You can use variables that will be evaluated at execution time:

- %VARx% : The node name at the x'th depth in the path.
- %SID% : The system Id of the SAP system

Example:

Consider the following path:
AGLGESRVSAP03_PRD_10\OperatingSystem\Filesystems\C:\Percentage_Used

And the following target definition: *%VAR1% - Disk %VAR4%*

The resulting target value of the QoS will be: *"AGLGESRVSAP03_PRD_10 – Disk C:"*

Cache

The path definitions and available CCMS sections are fetched from probe's cache by default. If you need a fresh update, you can uncheck the "from cache" checkbox in order to reload the data from the SAP server.

Note: The cache is commonly used by the GUI and by the monitor. If you reload the tree structure from the user interface, it will update the cache used by running monitors.

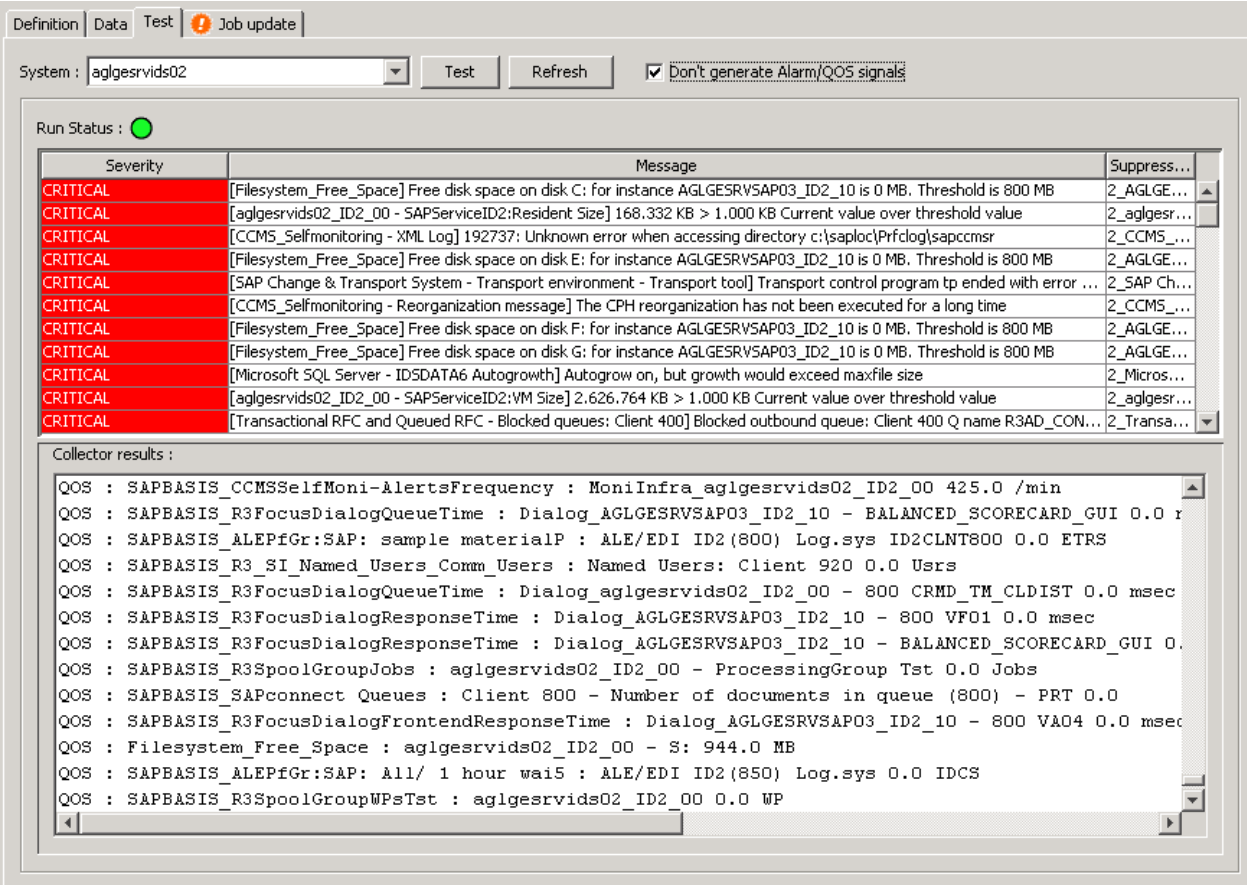
31.3. Execution and tests

Once you have configured the custom CCMS monitor job, you can test its results from the "Test" panel.

The alarm window will show all generated alarms (fired and cleared), and the log area will display generated QoS.

Note: By default, if you run a monitor in test mode, no Alarm or QoS events will be sent to UIM Monitor. To enable this, you need to uncheck the "Don't generate Alarm/QoS" signals.

©copyright 2014 AGENTIL – all rights reserved



Warning: When this monitor is active on several SAP systems with the "forward all" option, the number of QoS that will be generated can be very large. As an example, 40 systems with 500 metrics each will generate 120'000 QoS **per hour**. Make sure the servers and database are sized accordingly.

32. Custom SAP Control monitoring

32.1. Purpose

This monitor will give the possibility to extend the surveillance of Java systems to additional metrics. It is very similar than custom CCMS monitoring in its principle, except that it will get metrics from the java SAP management console, through SAP Control protocol.

Combined with the use of configuration templates, the visibility of the monitoring is greatly improved, and the deployment of configuration updates becomes a single click action.

32.2. Configuration

This monitor is similar than any other monitors in the probe, in the way you will enable it on a system. You first need to add this monitor in a template (existing or new). Then, you can open its definition panel by selecting the monitor node in the template's tree.

©copyright 2014 AGENTIL – all rights reserved

32.2.1. Execution definition

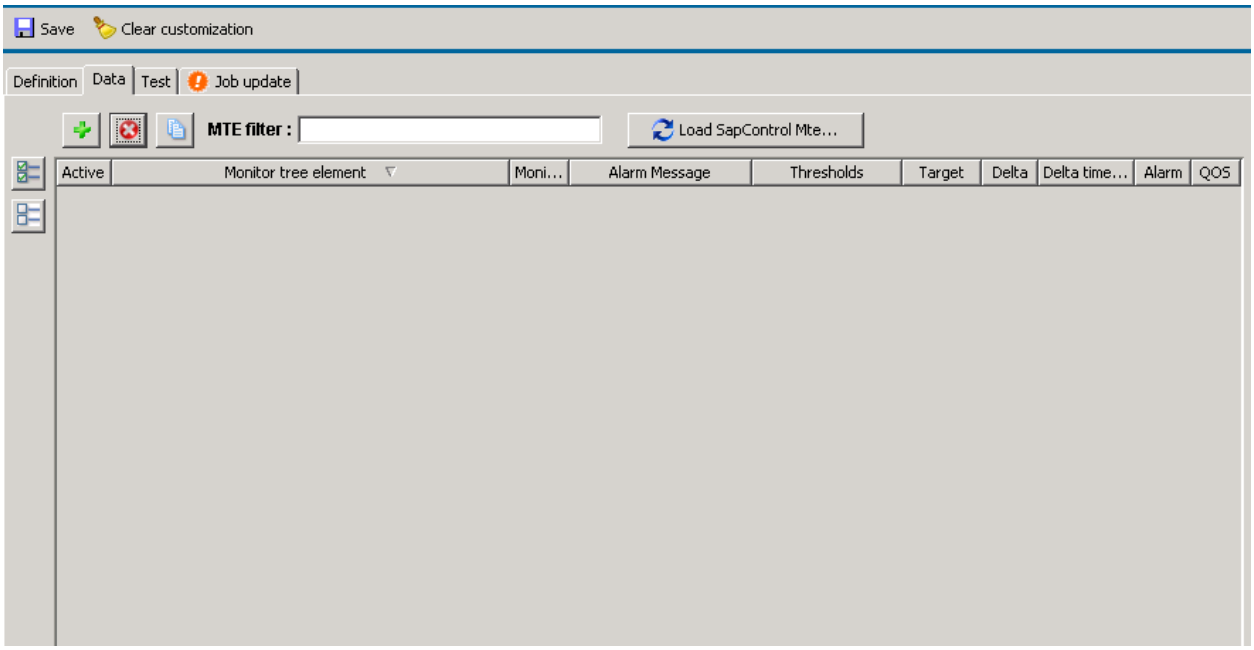
The common execution parameters of the monitor can be set from the definition panel. The schedule and activation state are defined here and can be modified according to your needs.

The monitor will be executed periodically, based to the chosen schedule. For each execution, it will collect metrics from java SAP management console, according to the monitoring configuration.

The collection time set in the SAP console is not relevant. The monitor will always fetch the latest available values at the rate of its executions. For example, if the schedule is set to run every 5 minutes, all metrics will be collected at this rate, even if the collection rate set in the console is 30 seconds, or 1 hour.

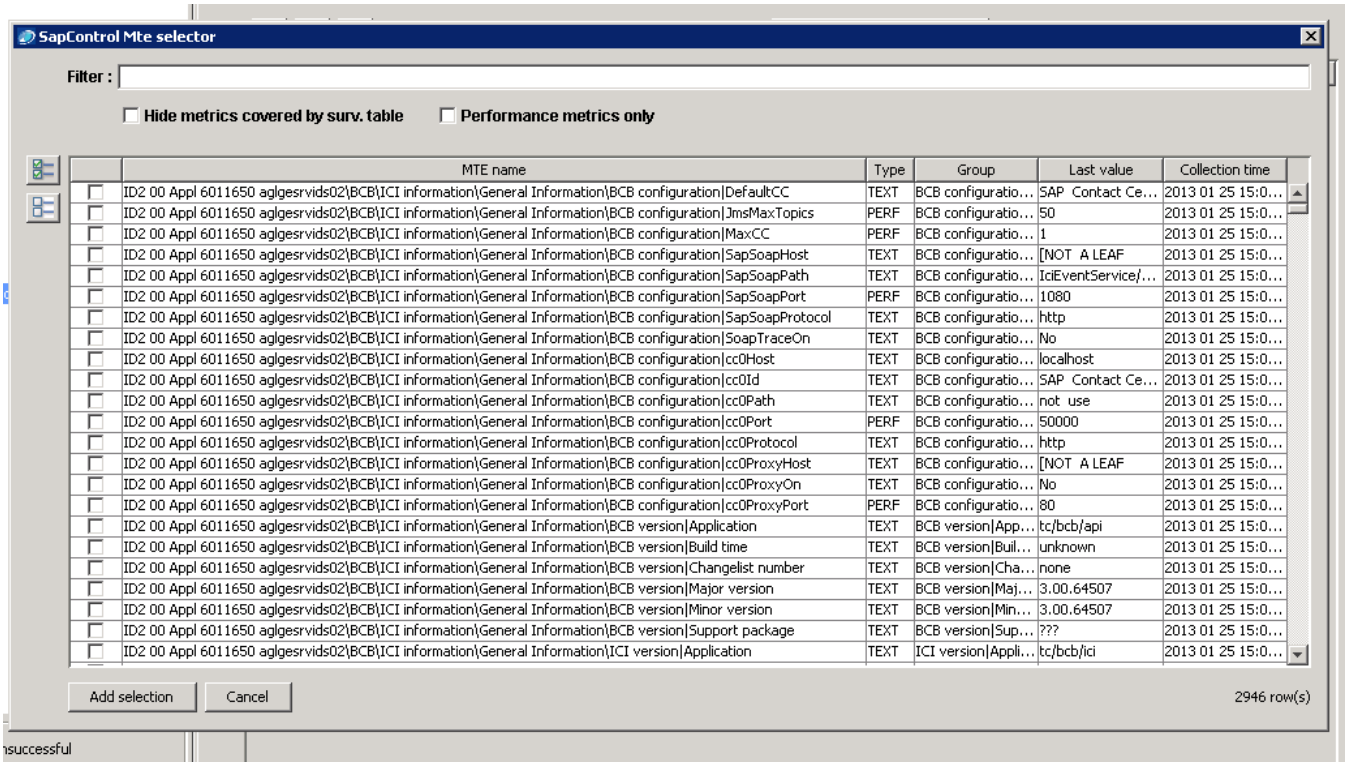
32.2.2. Monitoring definition

The Data tab is where the monitoring can be configured and customized.



From there, you can get the list of available metrics by pressing “Load SapControl MTEs…”. The probe will connect to the system and display a list.

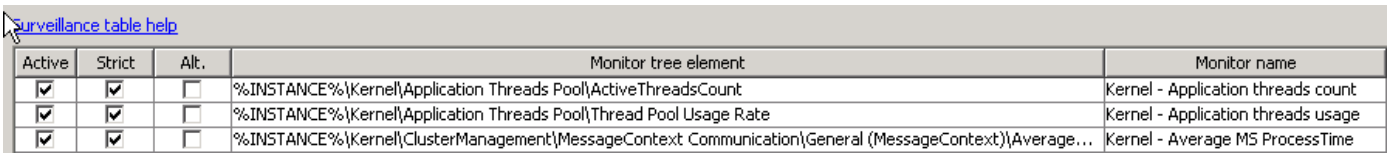
©copyright 2014 AGENTIL – all rights reserved



MTE name	Type	Group	Last value	Collection time
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\DefaultCC	TEXT	BCB configuratio...	SAP Contact Ce...	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\JmsMaxTopics	PERF	BCB configuratio...	50	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\MaxCC	PERF	BCB configuratio...	1	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\SapSoapHost	TEXT	BCB configuratio...	[NOT A LEAF	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\SapSoapPath	TEXT	BCB configuratio...	IciEventService/...	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\SapSoapPort	PERF	BCB configuratio...	1080	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\SapSoapProtocol	TEXT	BCB configuratio...	http	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\SoapTraceOn	TEXT	BCB configuratio...	No	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\cc0Host	TEXT	BCB configuratio...	localhost	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\cc0Id	TEXT	BCB configuratio...	SAP Contact Ce...	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\cc0Path	TEXT	BCB configuratio...	not use	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\cc0Port	PERF	BCB configuratio...	50000	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\cc0Protocol	TEXT	BCB configuratio...	http	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\cc0ProxyHost	TEXT	BCB configuratio...	[NOT A LEAF	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\cc0ProxyOn	TEXT	BCB configuratio...	No	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB configuration\cc0ProxyPort	PERF	BCB configuratio...	80	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB version\Application	TEXT	BCB version\App...	tc/bcb/api	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB version\Build time	TEXT	BCB version\Buil...	unknown	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB version\Changelist number	TEXT	BCB version\Cha...	none	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB version\Major version	TEXT	BCB version\Maj...	3.00.64507	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB version\Minor version	TEXT	BCB version\Min...	3.00.64507	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\BCB version\Support package	TEXT	BCB version\Sup...	???	2013 01 25 15:0...
ID2 00 Appl 6011650 aglgesrvids02\BCB\ICI information\General Information\ICI version\Application	TEXT	ICI version\Appli...	tc/bcb/ici	2013 01 25 15:0...

From this list, you can select the metrics you are interested in. The type, last value and collection time are displayed. You can use the filter to reduce the list.

Once you made a selection, click on the import button. This will create a set of surveillance rules for each selected metric in the table. The Monitoring Tree Element column will contain the path to the metric in the current status table of the SAP java MMC.



Surveillance table help

Active	Strict	Alt.	Monitor tree element	Monitor name
☑	☑	☐	%INSTANCE%\Kernel\Application Threads Pool\ActiveThreadsCount	Kernel - Application threads count
☑	☑	☐	%INSTANCE%\Kernel\Application Threads Pool\Thread Pool Usage Rate	Kernel - Application threads usage
☑	☑	☐	%INSTANCE%\Kernel\ClusterManagement\MessageContext Communication\General (MessageContext)\Average...	Kernel - Average MS ProcessTime

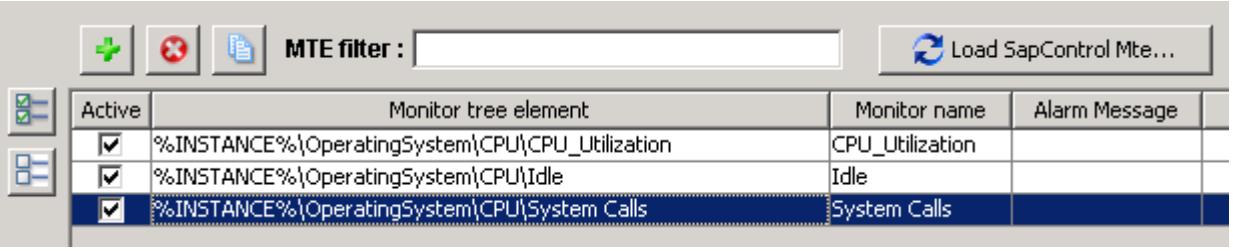
Grouping metrics

Metric paths in the java current status console are often composed by a dynamic part, like the name of the instance or a disk name. In order to reduce the amount of configuration work, you can use a specific syntax in the path definition in order to cover a set of paths with only one row.

You can do this by replacing the part that is “instance dependent” by a variable.

By example, the above surveillance table will allow to monitor few CPU metrics from the instance “AGLGESRVPID01” only. In order to be able to get the similar metrics from any instance, you could configure it like this:

©copyright 2014 AGENTIL – all rights reserved



This way, any instance name will match the surveillance rule. The name of the variable is free, only the position in the definition path is important.

Metric names

In order to have friendly metric names, you can define it in the "monitor name" field. By default, the last part of the metric path is chosen.

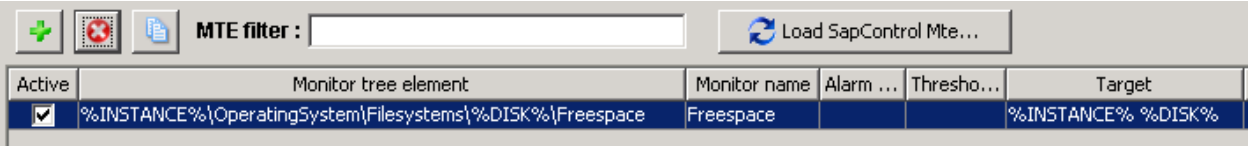
QOS configuration

In the surveillance table, the QOS checkbox has to be selected.

For each metric, you will need to set the target definition that will be used in the QOS. The string can include variables defined in the metric path, like %INSTANCE%, or %VARx% (The node name at the x'th depth in the path).

<u>Example:</u>

For the metric path: *%INSTANCE%\OperatingSystem\Filesystems\C:\Freespace,* the variable %VAR4% will contain "C:"



The above configuration can be used to get the filesystem free space of any disk from any instance. The QOS target definition will be composed by the instance name followed by disk name.

It is advised to avoid creating different QOS definitions for identical metric types. By applying the above configuration mechanism, only one QOS definition will be created for filesystem free space, the disk and instance possibilities will be discriminated in the target field.

Alarm configuration

The Alarm checkbox of the metric has to be selected to activate the alarm mechanism. Then you must set the Alarm message and the Alarm threshold field. The configuration is similar than for Custom CCMS monitoring, you can refer to the <u>Alarm message definition</u> and <u>Thresholds and severities definition</u> chapter of Custom CCMS monitor.

Strict mode

This option is useful to define if a metric is mandatory or not.

©copyright 2014 AGENTIL – all rights reserved

When strict mode is enabled, the probe will notify if the collection of any metric matching the MTE path fails. If not enabled, the probe will ignore problems encountered with the MTE path.

Alternate

Sometimes the names of the metric's path change from a SAP version to another. With this option you can define several MTE path for a unique metric. The probe will use the first one matching.

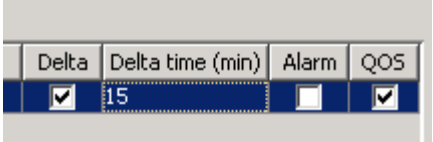
When this option is active, it means that the specified MTE path is an alternative for the one defined above.

Note: This option must be disabled for the first definition of each metric paths.

Delta

This monitor gives the possibility to calculate and use the difference between current and previously read data (the delta) in the QOS and Alarm mechanisms. It can be useful more metrics that are only increasing.

To enable the delta calculation, simply check the delta checkbox and specify the delta time.



The configuration above will use the delta between the current value, and the value read 15 minutes before. The delta will be used in QOS values and compared to Alarm thresholds.

Note that the delta time must be coherent with the job execution schedule. If you set a delta time to 5 min and the job is only executed every 15 minutes, the delta calculation will not work, as the metric will only be collected every 15 min. In the opposite, if you set a delta time to 15 min and if the job runs every 5 minutes, then the calculation will work correctly.

32.1. Execution and tests

Once you have configured the custom SAP Control monitor job, you can test its results from the "Test" panel.

The alarm window will show all generated alarms (fired and cleared), and the log area will display generated QoS.

Note: By default, if you run a monitor in test mode, no Alarm or QoS events will be sent to UIM Monitor. To enable this, you need to uncheck the "Don't generate Alarm/QoS" signals.

©copyright 2014 AGENTIL – all rights reserved

33. PI/XI Java messages

Monitoring capabilities

This monitor is dedicated to the monitoring of PI/XI messages status of Java stack instances. It has to be assigned to a Web portal connector to the target SAP system, with user credentials having access to the PI/XI messages view. With this monitor, you will have the possibility to be notified when a given number of messages from an XI component are in a given state, within a period of time.

You can filter in or out certain types of messages by using Sender, Receiver and Interface fields. You can adjust the level of alarm severity depending on the type of status or on message characteristic.
A disabled severity will filter out the messages matching the filters, for all subsequent lines.

Prerequisites

In case of the user management engine (UME) referred to a data source served by an ABAP client stack, the user account to access PI/XI information in the web portal must meet the following prerequisites:

- The web client connection user must be created in the client of the UME associated ABAP system (normally it is the "production" client, ask to the users administrator).
- Following roles must be granted to the user: SAP_XI_DISPLAY_USER_J2EE, SAP_XI_RWB_SERV_USER (exclusively, DO NOT USE A COPY)vv

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 15 minutes, but you can set a different schedule:

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring. The multiple severity syntax can be used in the "Max messages" field.

Active	Status	Period	Component	Sender	Receiver	Interface	Max messages	Aggr.	Severity
☑	SYSTEM ERROR	CURRENT_HOUR	mssql.xi.id2	*	*	*	20	☑	MAJ

<u>Active:</u> Use this field to activate or deactivate a line of configuration.

<u>Status:</u> Define the type message status to look for.

<u>Period:</u> Defines the period of time in which the probe will look for messages.

<u>Component:</u> Defines the xi component associated with the messages. The exact component name must be specified here.

<u>Sender:</u> A filter for the sender of the messages.

<u>Receiver:</u> A filter for the receiver of the messages.

<u>Interface:</u> A filter for the message interface.

<u>Max messages:</u> The threshold of the alarm generated if an equal or greater number of messages pass the alarm filter.

©copyright 2014 AGENTIL – all rights reserved

Aggregate:	If not set, threshold will be compared to the number of messages grouped by Sender, Receiver and Interface. If set, the threshold will be compared to the cumulated number of messages.
Severity:	The default severity to apply when the simple threshold syntax is used.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

34. PI/XI ABAP messages

Monitoring capabilities

This monitor is dedicated to the monitoring of PI/XI messages status of ABAP stack instances. It requires to be associated with an ABAP connector to the target SAP system. With this monitor, you will have the possibility to detect and to be notified when a message or a group of messages has a particular status.

Use the surveillance table to define the monitoring settings. You can filter in or out certain types of messages by using Client, Sender, Receiver and Emit/Rec Interface fields. You can adjust the level of alarm severity depending on the type of status or on message properties.
A disabled severity will filter out the messages matching the filters, for all subsequent lines.

This monitor will analyze the messages received since the last check time, with a maximum analyze depth of 60 minutes.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 15 minutes, but you can set a different schedule:

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring. The multiple severity syntax can be used in the “Max messages” field.

Active	Status	Client	Sender	Receiver	Emit.Interface	Rec.Interface	PID	Max messages	Aggr.	Severity
☑	ANY_ERROR	000	*	*	*	*	*	1	☑	MAJ

Active:	Use this field to activate or deactivate a line of configuration.
Status:	Define the type message status to look for.
Client:	The client in which the messages will be collected
Sender:	A filter on the sender of the messages.

©copyright 2014 AGENTIL – all rights reserved

Receiver:	A filter on the receiver of the messages.
Emitter Interface:	A filter on the message emitter interface.
Receiver interface:	A filter on the message receiver interface.
PID:	A filter on the message PID.
Max messages:	The threshold for the number of messages going through the filter.
Aggregate:	If not set, one alarm per message matching the filters will be sent. If set, an alarm will be sent only if the cumulated number of messages matching the filter is not below the threshold.
Severity:	The default severity to apply when the simple threshold syntax is used.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

35. PI/XI Channels

Monitoring capabilities

This monitor is dedicated to the monitoring of PI/XI channel status. It has to be assigned to a Web portal connector to the target SAP system, with user credentials having access to the PI/XI channels view. With this monitor, you will have the possibility to detect and to be notified when a Channel has not an appropriate status.

With the surveillance table, you can customize how the channels will be monitored and how you will be notified. Channels can be monitored based on their service, channel name and party or a particular log text.

You can actually monitor two states: activation state and channel state.
A disabled severity will filter out the channels matching the filters, for all subsequent lines.

Prerequisites

See PI/XI Java messages.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 15 minutes, but you can set a different schedule:

©copyright 2014 AGENTIL – all rights reserved

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring. The multiple severity syntax can be used in the “Max messages” field.

Active	Service	Channel	Party	Activation state	Channel state	Log	Threshold	Aggr.	Severity
☑	*	*	*	ANY	ERROR	*	1	☐	MAJ

Active:	Use this field to activate or deactivate a line of configuration.
Service:	A filter on the channel service
Channel:	A filter on the channel name.
Party:	A filter on the channel party.
Activation state:	The activation state to monitor.
Channel state:	The channel state to monitor.
Log:	A filter on the channel log.
Threshold:	In aggregate mode, the threshold for the maximum number of channels matching the filter.
Aggregate:	If not set, one alarm per channel matching the filters will be sent. If set, an alarm will be sent only if the cumulated number of channels matching the filter is not below the threshold.
Severity:	The default severity to apply when the simple threshold syntax is used.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

©copyright 2014 AGENTIL – all rights reserved

36. PI/XI Consumer caches status

Monitoring capabilities

This monitor is dedicated to the monitoring of PI/XI consumer caches. It has to be assigned to a Web portal connector to the target SAP system, with user credentials having access to the PI/XI channels view. With this monitor, you will have the possibility to detect and to be notified when a consumer cache status is not ok.

With the surveillance table, you can define custom monitoring for a specific cache name or define a global policy applied to all. You can adjust the alarm severity according to your needs.

Prerequisites

See PI/XI Java messages.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 15 minutes, but you can set a different schedule:

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring.

Active	Cache name	Severity
☑	*	MAJ

Active:	Use this field to activate or deactivate a line of configuration.
Cache name:	A filter on the cache name.
Severity:	The alarm severity to use when a cache is not in the right state.
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.
Report:	If checked, this line of surveillance will used for showing threshold and severity in the daily report

©copyright 2014 AGENTIL – all rights reserved

37. ICM

Monitoring capabilities

The Internet Communication Manager (ICM) ensures that communication between the SAP System (SAP Web Application Server) and the outside world via HTTP, HTTPS and SMTP protocols works properly. The purpose of this monitor is to check the global status of the ICM as well as communication indicators concerning the thread usage, number of connections and queued requests.

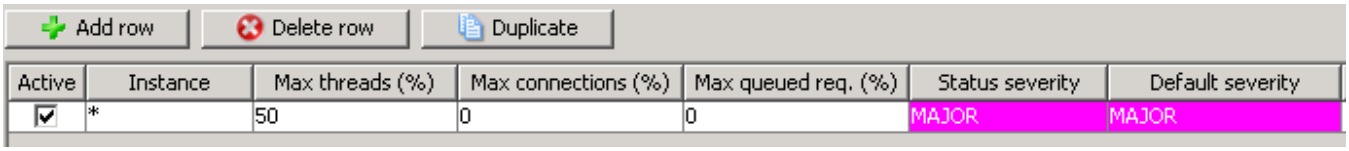
Thresholds are independent and can be set to 0 if not used. Advanced threshold syntax can be used for every fields.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 15 minutes, but you can set a different schedule:

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring.



Active:	Use this field to activate or deactivate a line of configuration.
Instance:	A filter on the instance name.
Max threads	The threshold for the maximum number of threads used in the thread pool
Max connections	The threshold for the maximum number of connections used in the connection pool
Max queued requests	The threshold for the maximum number of queued requests
Status severity	The severity of the alarm to send if status is not valid
Default severity	The severity used for alarms if advanced threshold syntax is not used in threshold fields
Auto clear:	If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.
Alarm tag:	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.
Alarm:	If checked, this line of surveillance will be used for alarm generation.
QOS:	If checked, this line of surveillance will be used for QOS generation.

©copyright 2014 AGENTIL – all rights reserved

38. Application logs

Monitoring capabilities

Application logging records the progress of the execution of an application so that you can reconstruct it later if necessary. Errors or problems occurring in the application can be detected by checking the application logs. The purpose of this monitor is to be able to detect specific problems in your applications. For that, it will check specific combinations of log object and sub-object discovered from your system. For each combination, it is possible to define filters on the mode, the minimum class, the type, the user, the transaction and the report.

You can monitor logs globally, or messages contained in each log. The probe will generate an alert if a log or messages are matching the configured filters. The probe will look for logs written since the last check.

Thresholds are independent and can be set to 0 if not used. Advanced threshold syntax can be used for every fields.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition. By default, the job will run every 15 minutes, but you can set a different schedule:

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring.

Add object | Delete row | Duplicate | ☑ load objects from ca

Active	Check type	ObjectTxt	Sub-objectTxt
☑	CHECK_MESSAGES	Standard Message Object (IUMS)	Program Error (ERROR_PROG)
☑	CHECK_MESSAGES	Standard Message Object (IUMS)	UPDATE Error (ERROR_UPD)
☑	CHECK_LOGS	Standard Message Object (IUMS)	Normal Error (ERROR)
☑	CHECK_MESSAGES	Standard Message Object (IUMS)	Other Serious Error (ERROR_BIG)

Client	User	Transaction	Report	Mode	Minimum Log class	Type	Threshold
*	*	*	*	Batch processing	VERY IMPORTANT	ABORTED	3
*	*	*	*	Dialog processing	IMPORTANT	ERROR	2
*	*	*	*	Batch input pro...	LESS IMPORTANT	WARNING	1
*	*	*	*	ANY	INFORMATION	ANY	0

Active	Use this field to activate or deactivate a line of configuration.
Check type	With CHECK_LOGS, threshold will be compared to the number of logs matching then filter. With CHECK_MESSAGES, it will be compared to the sum of messages from logs matching the filter.
ObjectTxt	The description of the object to monitor
Sub-ObjectTxt	The description of the sub object to monitor

©copyright 2014 AGENTIL – all rights reserved

Client	A filter on the client
User	A filter on the user
Transaction	A filter on the transaction
Report	A filter on the report
Mode	A filter on the mode of the log
Minimum log class	A filter on the log class. It will take into account only logs with class of the same importance or higher
Type	A filter on the type of the log
Threshold	The threshold used by the alarm, compared to the number of logs or messages matching the filter. Behavior depends on the check type
Aggregate	This is only effective in CHECK_MESSAGES mode. If checked, it will count the number of messages from every logs matching the filter. If not, the threshold will be compared only to the number of messages contained in each log, potentially generating several alarms
Severity	The severity used for alarms if advanced threshold syntax is not used in threshold field
Alarm tag	This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix
Alarm	If checked, this line of surveillance will be used for alarm generation
Metric	If checked, this line of surveillance will be used for Metric generation

39. SAP reports

You can generate reports in HTML format showing information about various components of your SAP systems. Reports can be sent by email and stored in an archive.

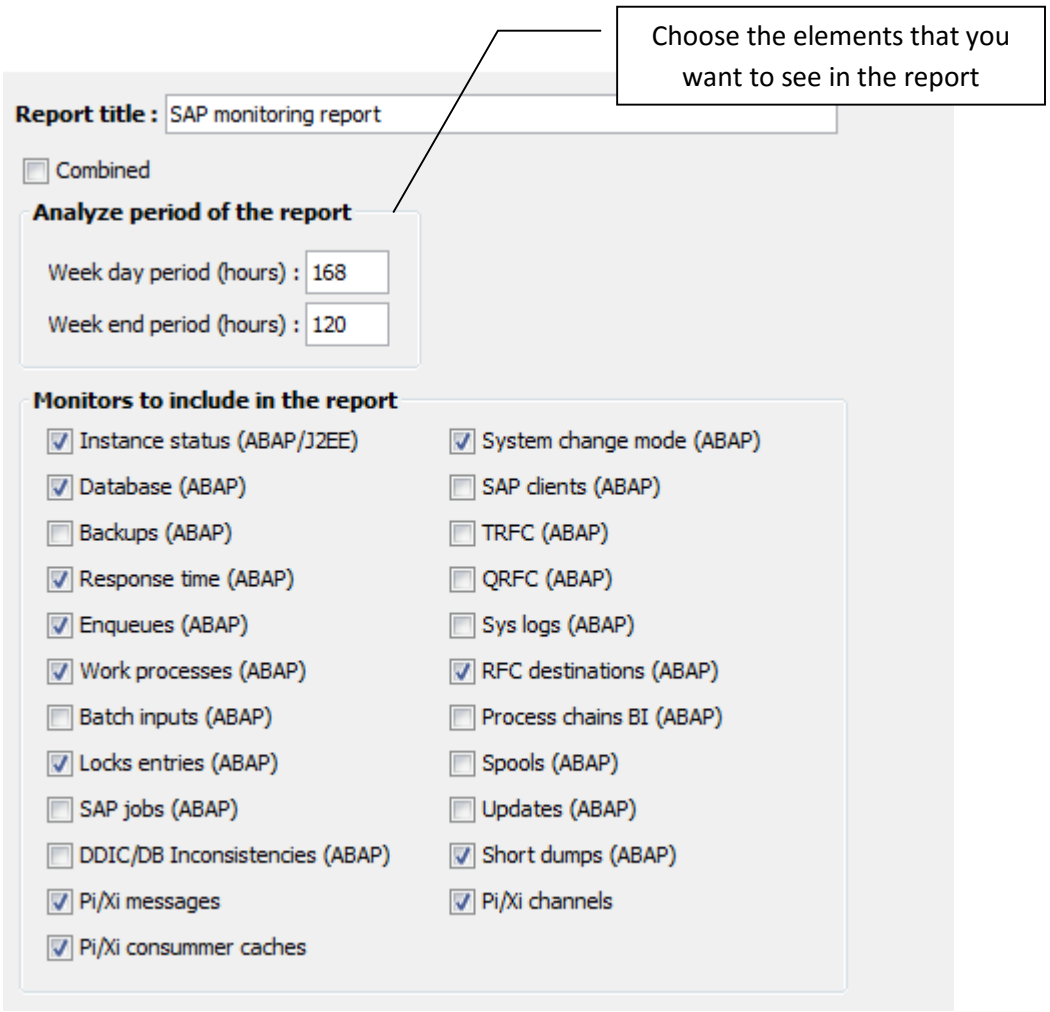
The report job works like all other monitor jobs, its execution is scheduled at a given time. This job will look back in the past until a customizable depth and collect information. After analysis, this information will be used to build an HTML report.

You can choose the information that you want to see in the report among a list of items:

- System/instance status
- Database (size/backup/DBA jobs/inconsistencies)
- Number of short dumps and error details
- Dialog response time
- Enqueues maximum fill levels
- Lock entries
- Number range ratio
- Number of QRFC in/out, outbound TRFC status
- Updates in error or not yet completed.
- Work processes

©copyright 2014 AGENTIL – all rights reserved

- RFC destinations availability
- TRFC, QRFC
- Sys logs : Displays sys logs and highlights errors
- Batch inputs status (from a session list to provide)
- Aborted SAP job number and details
- Process chains
- Spools and spool requests



Important: For most monitors, you can use the real time monitoring configuration to associate the configured thresholds and filters with the report.

By example: if you configured the threshold for ABAP short dumps to 10 with a WARNING severity, the number of short dumps will be highlighted in yellow color in the report if it goes above 10.

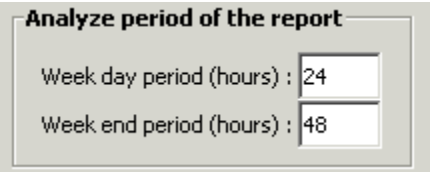
In order to link the configuration of a monitor job to the report, the “report” check box must be enabled for each line of surveillance that you want to associate.

Of course, the corresponding monitor job must be active for the given SAP system.

©copyright 2014 AGENTIL – all rights reserved

Time window

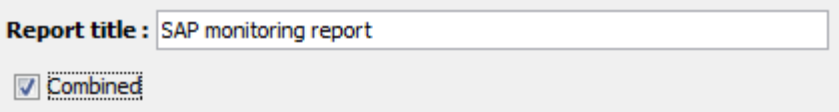
You can set the depth of the analyze period of the report:



By example, if you set a period of 24 hours and if your report is set to be executed on Monday at 8am, it will analyze the data available since the last 24 hours, starting from the execution time : From Sunday at 8am.

You can choose a longer period for week end report. Week end period will be used if the report is executed on Monday. Otherwise, it is the week day period that will be used.

Combined



The combined option gives the possibility to merge the reports generated for each connector of a SAP system into one document. By example, you get the report of all Java instances merged with the ABAP stack. This simplify the reporting for a single SAP system and reduces the number of generated documents.

For the moment, you can merge the reports together from:

- One ABAP instance connector
- One SAP web client connector
- Multiple Java instances connectors

You cannot merge reports from multiple ABAP or web client connectors within a SAP system.

Note: For the combined option to work, the report job of each connector that you want to merge must have the combined option "checked" **AND** have the <u>same</u> schedule time.

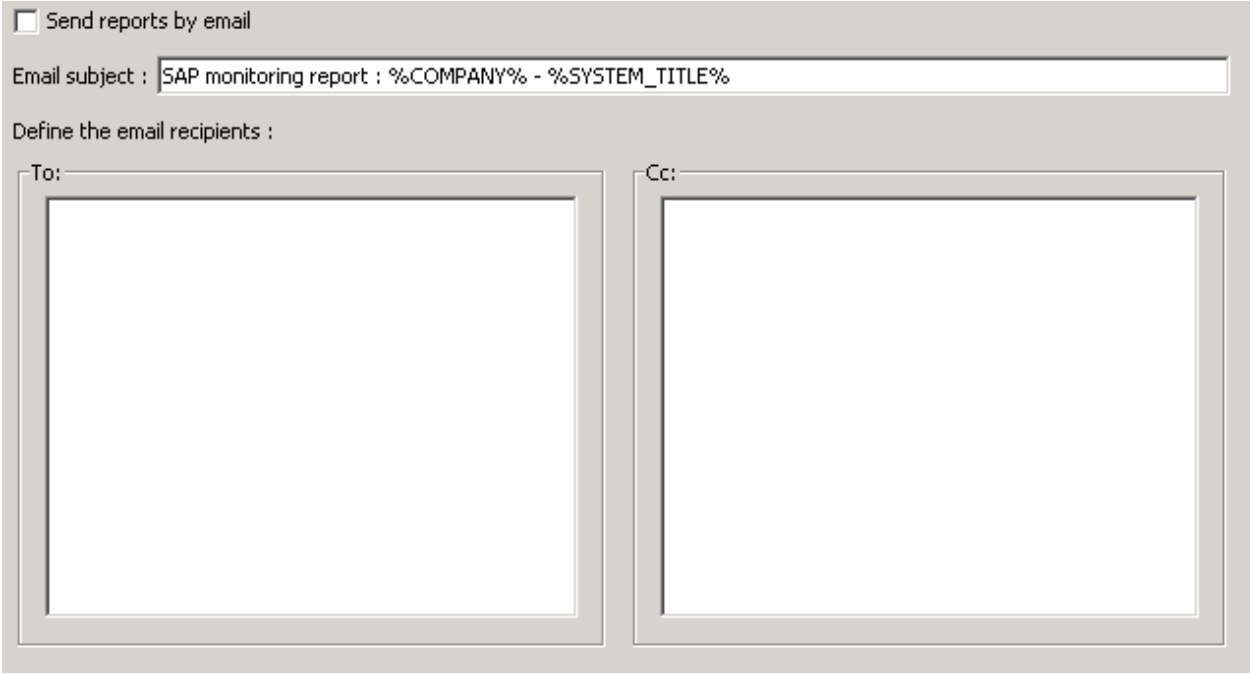
<u>Additionally</u>, report file name, title and receiver list must be the same for consistency.

Email settings

You can setup the report job to send the generated reports by email, to a list of recipients. You can also define the email subject by using variables that will be replaced by actual values:

- %SID%: The system Id of the SAP system for which the report is generated
- %SYSTEM_TITLE%: The title defined for the SAP system in the connector.
- %COMPANY%: The company associated with the report

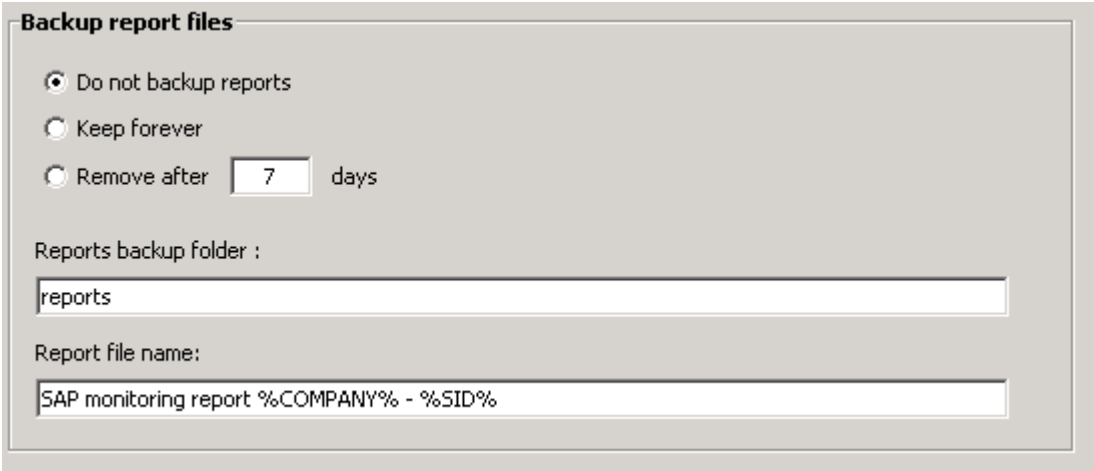
©copyright 2014 AGENTIL – all rights reserved



Warning: If you activate the email report, you need to set SMTP parameters in the probe setup.

Backup reports

If you activate backup, the generated reports will be copied in the *reports* folder in the probe engine installation folder. You can change the report folder and customize the report file name by using variables that will be replaced by actual values (see email chapter for available variables)



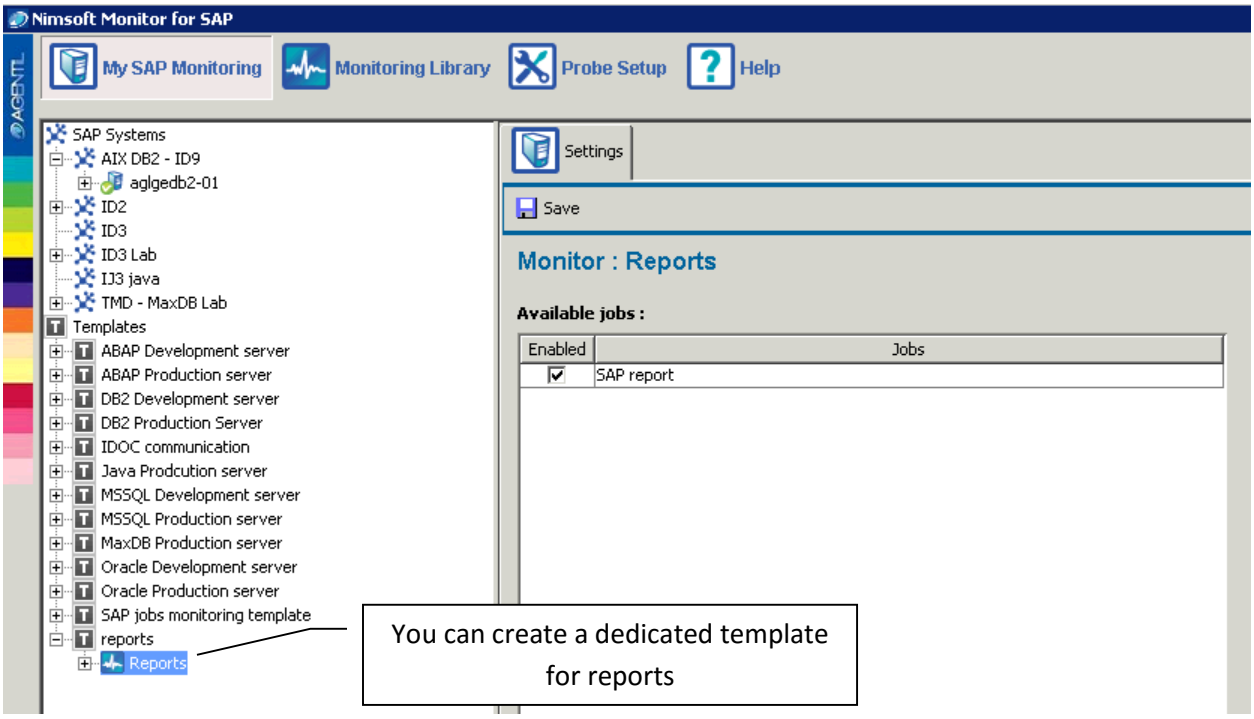
How to enable the report job on a system

This job is available in the monitoring library like all other regular jobs. It is located in the “Reports” monitor.

In order to assign it to a system, you must include it in an existing template or create a dedicated template for it.

©copyright 2014 AGENTIL – all rights reserved

Example:



Then you just need to assign the template to a system to have this monitor job activated on it.

40. Hana services status

Monitoring capabilities

This monitor will watch for the availability of following SAP Hana services:

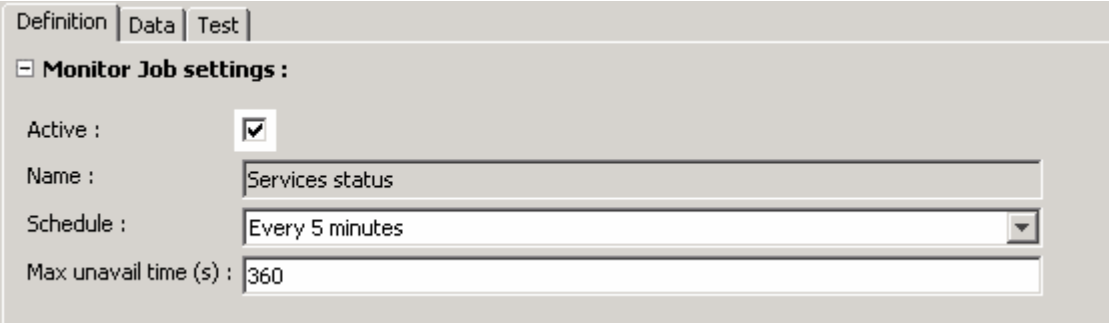
- Nameserver
- Indexserver
- Statistics server
- Xsengine
- Preprocessor
- Daemon

It will send an alarm if one of the services is not running, and can send metrics containing service status.

Job schedule definition

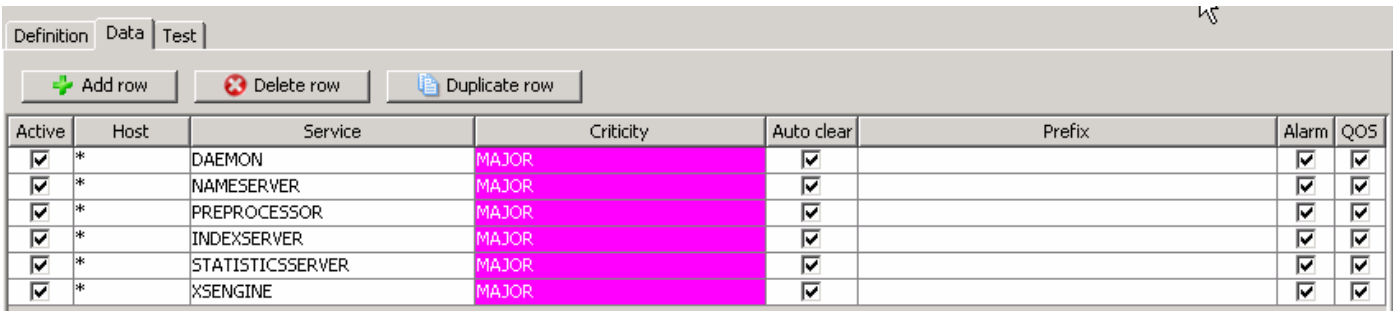
The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 5 minutes, but you can set a different schedule:

©copyright 2014 AGENTIL – all rights reserved



Surveillance table

The services to monitor have to be defined in the surveillance table. Use the "Add row" button to create a new rule.



Active	Host	Service	Criticity	Auto clear	Prefix	Alarm	QOS
☑	*	DAEMON	MAJOR	☑		☑	☑
☑	*	NAMESERVER	MAJOR	☑		☑	☑
☑	*	PREPROCESSOR	MAJOR	☑		☑	☑
☑	*	INDEXSERVER	MAJOR	☑		☑	☑
☑	*	STATISTICSSERVER	MAJOR	☑		☑	☑
☑	*	XSENGINE	MAJOR	☑		☑	☑

The following fields of the table can be set to adjust the monitoring:

Active: If checked, the rule is enabled and will be processed

Host: Can be used to restrict the monitoring to a given host (multi instance case). A star ('*') will match any host.

Service: Defines which service is monitored.

Criticity: Defines the level of severity of the alarm that will be generated if the service becomes offline.

Auto clear: If set, the alarm generated when the service goes down will be cleared when the service comes back again

Prefix: You can define some text to use as a prefix of the alarm message generated by the current rule

Alarm/QOS: If enabled, it will respectively send alarm/metric. You can use this option to only generate alarm, or only send metric for a given service.

QOS

If enable, the metric sent will be named SAPHANA_SERVICE_STATUS, containing true if the service is online. Service name will be set in metric's target.

©copyright 2014 AGENTIL – all rights reserved

41. Hana database CPU utilization

Monitoring capabilities

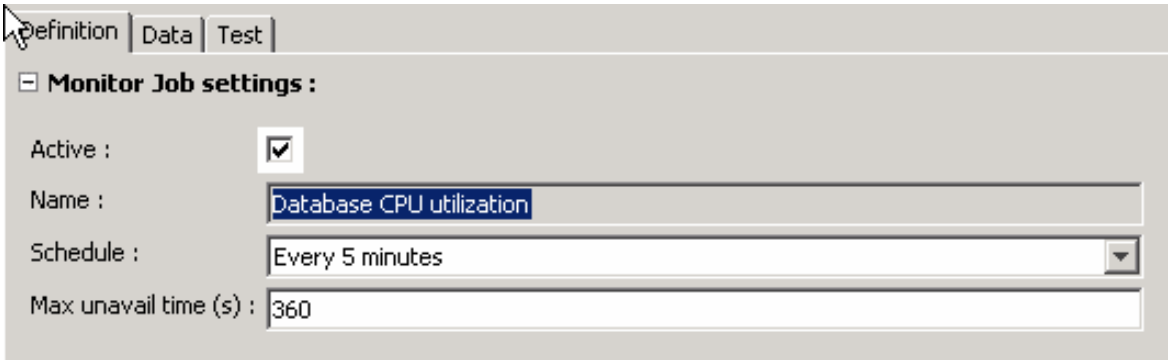
Monitors the CPU usage of HANA instances at different levels:

- Instance level : all services combined
- Service level : CPU usage of one service

It monitors instant CPU usage as well as usage over a period of time (smoothed).

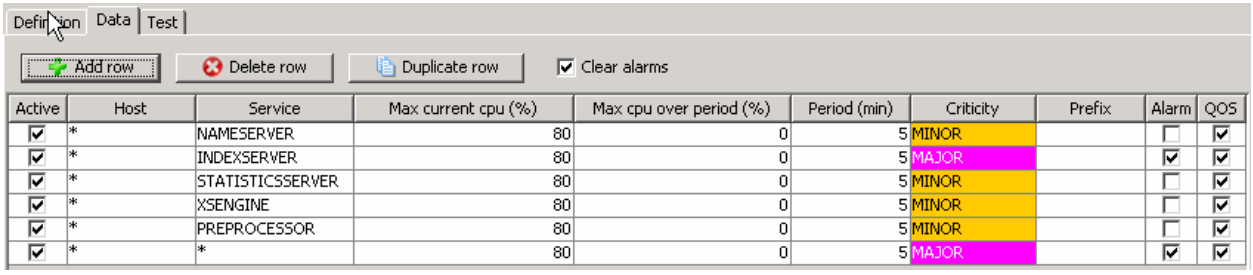
Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 5 minutes, but you can set a different schedule:



Surveillance table

The CPU monitoring will be defined in a surveillance table. From there, you can select the services to watch and set the appropriate thresholds:



Active	Host	Service	Max current cpu (%)	Max cpu over period (%)	Period (min)	Criticity	Prefix	Alarm	QOS
☑	*	NAMESERVER	80	0	5	MINOR		☐	☑
☑	*	INDEXSERVER	80	0	5	MAJOR		☑	☑
☑	*	STATISTICSSERVER	80	0	5	MINOR		☐	☑
☑	*	XSENGINE	80	0	5	MINOR		☐	☑
☑	*	PREPROCESSOR	80	0	5	MINOR		☐	☑
☑	*	*	80	0	5	MAJOR		☑	☑

Active: If checked, the rule is enabled and will be processed

Host: Can be used to restrict the monitoring to a given host (multi instance case). A star ('*') will match any host.

Service: Defines which service is monitored. **A star ('*') will match any service, and therefore, it will calculate the combined usage of all services. Otherwise, it is the usage of the specified service that will be calculated.**

Max current cpu (%): The alarm threshold for the current CPU usage.

©copyright 2014 AGENTIL – all rights reserved

Max cpu over period (%): The alarm threshold of the CPU usage over the period set in the “Period” field.

Period: The period of time used to calculate the CPU usage.

Criticity: Defines the level of severity of the alarm that will be generated if one of the thresholds is reached.

Auto clear: If set, the generated alarms will be automatically cleared from the console if the alarm condition is not fulfilled anymore.

Prefix: You can define some text to use as a prefix of the alarm message generated by the current rule.

Alarm/QOS: Defines if an alarm/metric has to be generated for the given rule.

Default thresholds

A threshold set to 0 will disable the check and prevent any alarm to be sent for this particular check. By default, thresholds are set to 0 when you create a rule.

By example, if you want to monitor the delta usage and not the current one, you can simply set current usage threshold to 0.

QOS

These are the metrics that will be generated if the QOS option is selected:

- SAPHANA_DB_CPU_UTILIZATION : The instant CPU utilization per host
- SAPHANA_DB_CPU_UTILIZATION_PER_SERVICE : The instant CPU utilization per service
- SAPHANA_DB_CPU_UTILIZATION_SMOOTHED_PER_SERVICE : The smoothed CPU utilization per service. (smoothed over 1 minute)

42. Hana database memory utilization

Monitoring capabilities

Monitors the memory usage of the HANA database at different levels:

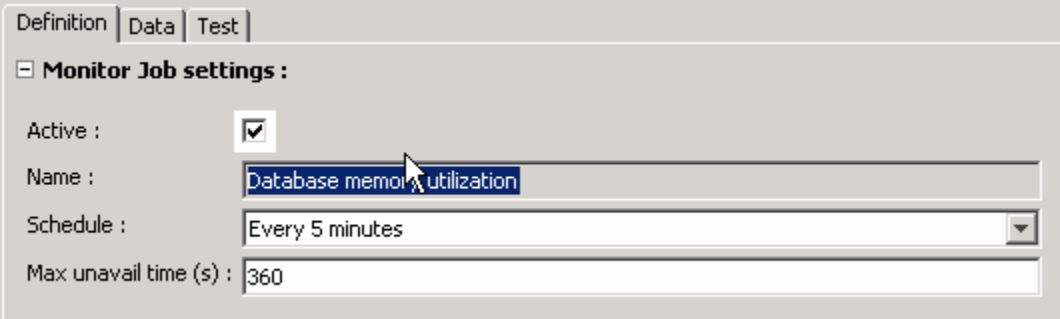
- Instance level: The combined usage of all services
- Service level: The usage of each individual service.

It gives the possibility to monitor the current memory consumption as well as an increase of the consumption over a given period of time.

Job schedule definition

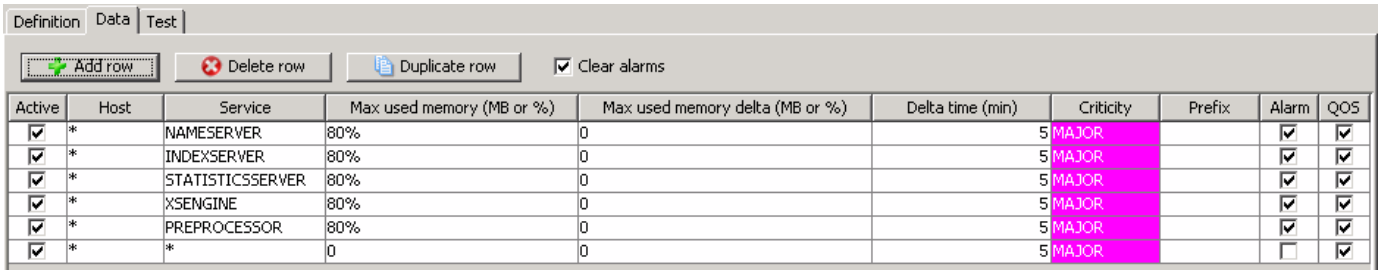
The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 5 minutes, but you can set a different schedule:

©copyright 2014 AGENTIL – all rights reserved



Surveillance table

The memory monitoring will be defined in a surveillance table. From there, you can select the services to watch and set the appropriate thresholds:



Active	Host	Service	Max used memory (MB or %)	Max used memory delta (MB or %)	Delta time (min)	Criticity	Prefix	Alarm	QOS
☑	*	NAMESERVER	80%	0	5	MAJOR		☑	☑
☑	*	INDEXSERVER	80%	0	5	MAJOR		☑	☑
☑	*	STATISTICSSERVER	80%	0	5	MAJOR		☑	☑
☑	*	XSENGINE	80%	0	5	MAJOR		☑	☑
☑	*	PREPROCESSOR	80%	0	5	MAJOR		☑	☑
☑	*	*	0	0	5	MAJOR		☐	☑

Active: If checked, the rule is enabled and will be processed

Host: Can be used to restrict the monitoring to a given host (multi instance case). A star ('*') will match any host.

Service: Defines which service is monitored. **A star ('*') will match any service, and therefore, it will calculate the combined usage of all services. Otherwise, it is the usage of the specified service that will be calculated.**

Max used memory (MB or %): The alarm threshold for the current memory usage. You can specify percentage or absolute value in Mega Bytes.

Max used memory delta (MB or %): The alarm threshold of the memory consumption increase over the period set in the "Delta time" field. Example: Send an alarm if the memory usage increases by 20% in the last 5 min.

Delta time: The period of time used to make a delta comparison of the memory usage.

Criticity: Defines the level of severity of the alarm that will be generated if one of the thresholds is reached.

Prefix: You can define some text to use as a prefix of the alarm message generated by the current rule.

Alarm/QOS: Defines if an alarm/metric has to be generated for the given rule.

©copyright 2014 AGENTIL – all rights reserved

Default thresholds

A threshold set to 0 will disable the check and prevent any alarm to be sent for this particular check. By default, thresholds are set to 0 when you create a rule.

By example, if you want to monitor the delta usage and not the current one, you can simply set current usage threshold to 0.

Delta times

If you want to use the delta memory monitoring, you must take into account the fact that the probe will need to take two snapshot of the memory usage before being able to compute the delta, and eventually to generate an alarm. So, if you set a delta time of 10 minutes, then you will have to wait at least 10 minutes to get a result.

Clear alarms option

If set, the generated alarms will be automatically cleared from the console if the alarm condition is not fulfilled anymore.

QOS

These are the metrics that will be generated if the QOS option is selected:

- SAPHANA_DB_MEMORY_USED_PER_SERVICE: The current memory usage per service (MB)
- SAPHANA_DB_MEMORY_PERCENTAGEUSED_PER_SERVICE: The current memory usage per service (%)
- SAPHANA_DB_MEMORY_USED: The current memory usage per instance (MB)
- SAPHANA_DB_MEMORY_PERCENTAGEUSED: The current memory usage per instance (%)
- SAPHANA_DB_MEMORY_ALLOC_SIZE: The current memory allocation size per instance (MB)
- SAPHANA_DB_MEMORY_EFFECTIVE_ALLOC_SIZE : The current effective allocation size per service (MB)

43. Hana database disk utilization

Monitoring capabilities

Monitors the disk used space of the HANA database at different levels:

- Instance level: The combined usage of all services
- Service level: The usage of each individual service.

Disk utilizations are split into several categories: DATA, LOG, TRACE, DATA_BACKUP and LOG_BACKUP. For each category, you can monitor the current disk usage as well as the delta usage over a period of time.

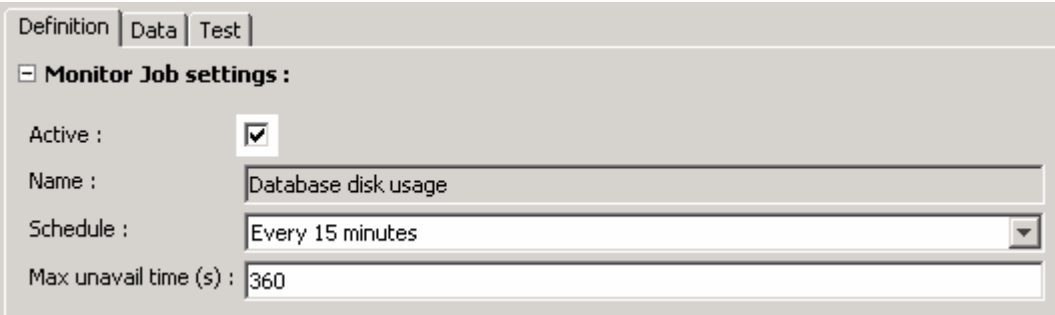
You can define custom monitoring rules based on the host, the service and the type of usage.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.

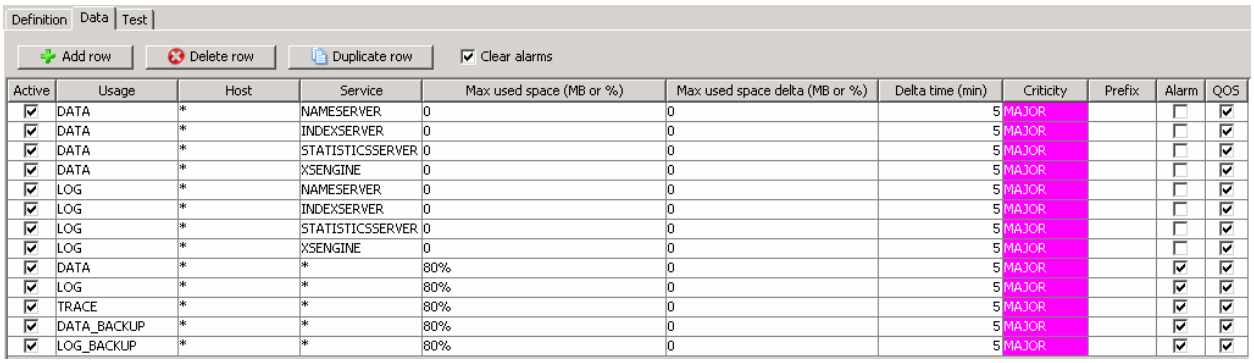
©copyright 2014 AGENTIL – all rights reserved

By default, the job will run every 15 minutes, but you can set a different schedule:



Surveillance table

Disk usage monitoring will be defined in a surveillance table. From there, you can define the hosts, the services and the type of usage to watch based on the current and delta disk used space.



Active	Usage	Host	Service	Max used space (MB or %)	Max used space delta (MB or %)	Delta time (min)	Criticity	Prefix	Alarm	QOS
☑	DATA	*	NAMESERVER	0	0	5	MAJOR		☐	☑
☑	DATA	*	INDEXSERVER	0	0	5	MAJOR		☐	☑
☑	DATA	*	STATISTICSSERVER	0	0	5	MAJOR		☐	☑
☑	DATA	*	XSENGINE	0	0	5	MAJOR		☐	☑
☑	LOG	*	NAMESERVER	0	0	5	MAJOR		☐	☑
☑	LOG	*	INDEXSERVER	0	0	5	MAJOR		☐	☑
☑	LOG	*	STATISTICSSERVER	0	0	5	MAJOR		☐	☑
☑	LOG	*	XSENGINE	0	0	5	MAJOR		☐	☑
☑	DATA	*	*	80%	0	5	MAJOR		☑	☑
☑	LOG	*	*	80%	0	5	MAJOR		☑	☑
☑	TRACE	*	*	80%	0	5	MAJOR		☑	☑
☑	DATA_BACKUP	*	*	80%	0	5	MAJOR		☑	☑
☑	LOG_BACKUP	*	*	80%	0	5	MAJOR		☑	☑

Active: If checked, the rule is enabled and will be processed

Usage: The type of usage of the disk

Host: Can be used to restrict the monitoring to a given host (multi instance case). A star ('*') will match any host.

Service: Defines which service is monitored. **A star ('*') will match any service, and therefore, it will calculate the combined usage of all services. Otherwise, it is the usage of the specified service that will be calculated.**

Max used space (MB or %): The alarm threshold for the current disk usage. You can specify percentage or absolute value in Mega Bytes.

Max used space delta (MB or %): The alarm threshold on the delta disk usage increase over the period set in the "Delta time" field. Example: Send an alarm if the disk usage increases by 20% in the last 5 min.

Delta time: The period of time used to make a delta comparison of the disk usage.

Criticity: Defines the level of severity of the alarm that will be generated if one of the thresholds is reached.

©copyright 2014 AGENTIL – all rights reserved

Prefix: You can define some text to use as a prefix of the alarm message generated by the current rule.

Alarm/QOS: Defines if an alarm/metric has to be generated for the given rule.

Default thresholds

A threshold set to 0 will disable the check and prevent any alarm to be sent for this particular check. By default, thresholds are set to 0 when you create a rule.

By example, if you want to monitor the delta usage and not the current one, you can simply set current usage threshold to 0.

Delta times

If you want to use the delta disk usage monitoring, you must take into account the fact that the probe will need to take two snapshot of the usage before being able to compute the delta, and eventually to generate an alarm. So, if you set a delta time of 10 minutes, then you will have to wait at least 10 minutes to get a result.

Clear alarms option

If set, the generated alarms will be automatically cleared from the console if the alarm condition is not fulfilled anymore.

QOS

These are the metrics that will be generated if the QOS option is enabled:

- SAPHANA_OVERALL_DATA_DISK_PERCENTAGE_USED: Disk used space by DATA type (%)

- SAPHANA_OVERALL_LOG_DISK_PERCENTAGE_USED: Disk used space by LOG type (%)

- SAPHANA_OVERALL_TRACE_DISK_PERCENTAGE_USED: Disk used space by TRACE type (%)

- SAPHANA_OVERALL_DATA_BACKUP_DISK_PERCENTAGE_USED: Disk used space by DATA_BACKUP type (%)

- SAPHANA_OVERALL_LOG_BACKUP_PERCENTAGE_USED: Disk used space by LOG_BACKUP type (%)

- SAPHANA_OVERALL_DATA_DISK_USED_SPACE: Disk used space by DATA type (MB)

- SAPHANA_OVERALL_LOG_DISK_ USED_SPACE: Disk used space by LOG type (MB)

- SAPHANA_OVERALL_TRACE_DISK_ USED_SPACE: Disk used space by TRACE type (MB)

- SAPHANA_OVERALL_DATA_BACKUP_DISK_ USED_SPACE: Disk used space by DATA_BACKUP type (MB)

- SAPHANA_OVERALL_LOG_BACKUP_ DISK_USED_SPACE: Disk used space by LOG_BACKUP type (MB)

44. Hana backups

Monitoring capabilities

This monitor will check that the backups are executed correctly and on time. It will also monitor the backup duration and the size of generated files.

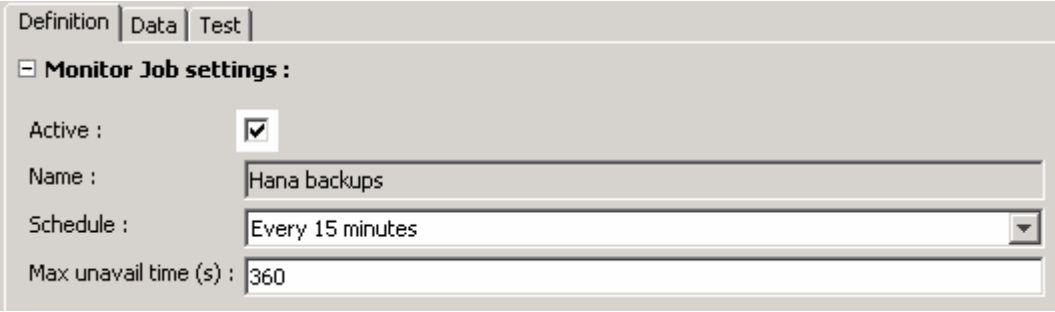
©copyright 2014 AGENTIL – all rights reserved

LOG and DATA backups will be processed separately.

Note: Only the backup events that have occurred since the last check will be taken into account. This monitor has to stay continuously enabled if you don't want to miss any backup.

Job schedule definition

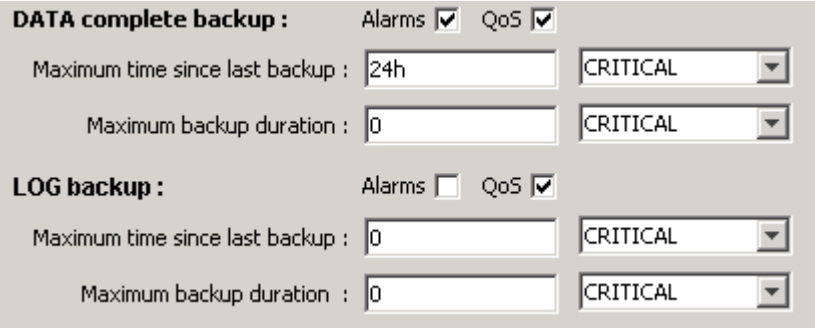
The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 15 minutes, but you can set a different schedule:



Backup occurrence and duration

The first items of the configuration panel will define the DATA and LOG backup monitoring configuration:

You will be able to define the maximum time between two successful backups, and a maximum backup duration:



For each type of backup and check, you can customize the level of severity to use for the alarm that would be generated if a threshold is reached.

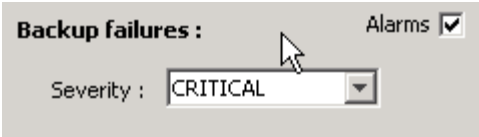
You can also define whether to send Alarm/Qos or not.

A threshold set to 0 will disable the check and prevent any alarm to be sent.

Backup status

This monitor will generate an alarm if a failed backup event is detected. For that, the alarm check box must be activated:

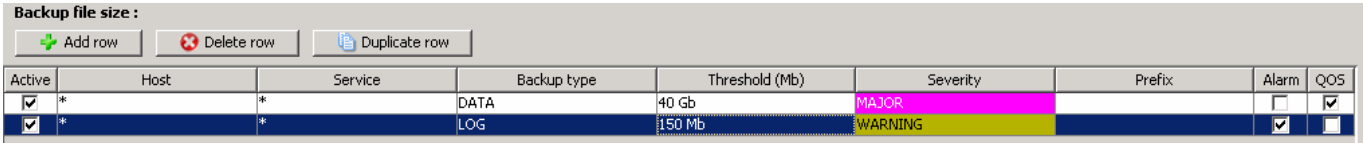
©copyright 2014 AGENTIL – all rights reserved



The severity of the alarm can be customized as well.

Backup file size

The file size monitoring configuration is done via a surveillance table:



Active	Host	Service	Backup type	Threshold (Mb)	Severity	Prefix	Alarm	QOS
☑	*	*	DATA	40 Gb	MAJOR		☐	☑
☑	*	*	LOG	150 Mb	WARNING		☑	☐

Active: If checked, the rule is enabled and will be processed

Host: Can be used to restrict the monitoring to a given host (multi instance case). A star ('*') will match any host.

Service: Defines from which service the backup files will be checked. **A star ('*') will match any service.**

Backup Type: The type of backup

Threshold: The maximum file size. Unit can be specified: TB, GB, MB or KB. If no unit specified, the value will be assumed as bytes. **If set to 0, the size won't be monitored**.

Severity: Defines the level of severity of the alarm that will be generated if one of the thresholds is reached.

Prefix: You can define some text to use as a prefix of the alarm message generated by the current rule.

Alarm/QOS: Defines if an alarm/metric has to be generated for the given rule.

QOS

These are the metrics that will be generated if the QOS option is enabled:

- SAPHANA_DATA_BACKUP_DURATION: The duration of the last DATA backup in minutes.
- SAPHANA_LOG_BACKUP_DURATION: The duration of the last LOG backup in minutes.
- SAPHANA_TIME_SINCE_LAST_DATA_BACKUP: The number of elapsed hours since last DATA backup.
- SAPHANA_TIME_SINCE_LAST_LOG_BACKUP: The number of elapsed minutes since last LOG backup.
- SAPHANA_DATA_BACKUP_FILE_SIZE: The size of the DATA backup file.
- SAPHANA_LOG_BACKUP_FILE_SIZE: The size of the LOG backup file.

©copyright 2014 AGENTIL – all rights reserved

45. Hana connections

Monitoring capabilities

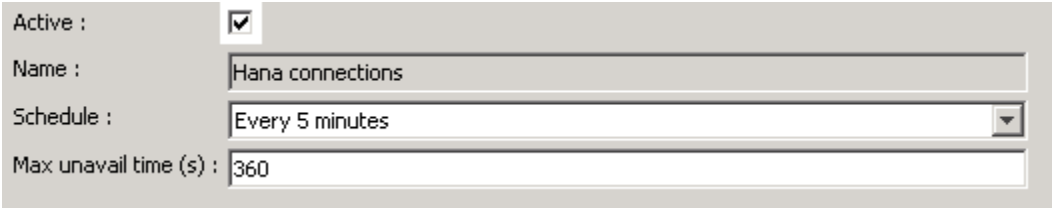
This monitor will check the number of current connections to the database. You can configure it to send an alarm when too many connections are open on a given instance.

It differentiates RUNNING connections from IDLE connections.

You can also monitor the connections of a given user or group of users.

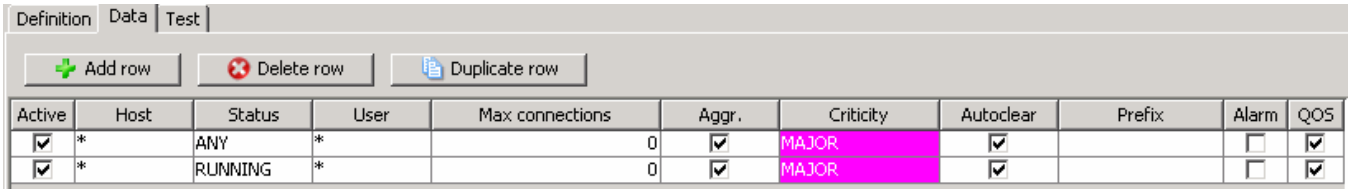
Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 5 minutes, but you can set a different schedule:



Monitoring table

The definition of the monitoring is done via the monitoring table. From there you can define the host, the state of the connection, the user and the connection alarm threshold.



Active	Host	Status	User	Max connections	Aggr.	Criticity	Autoclear	Prefix	Alarm	QOS
☑	*	ANY	*	0	☑	MAJOR	☑		☐	☑
☑	*	RUNNING	*	0	☑	MAJOR	☑		☐	☑

Active: If checked, the rule is enabled and will be processed

Host: Can be used to restrict the monitoring to a given host (multi instance case). A star ('*') will match any host.

Status: Specifies the status of the connections to check : IDLE, RUNNING or ANY**.**

User: If different than star ('*'), only the connections of the given user will be taken into account.

Max connections: The threshold of the connection alarm. **If set to 0, the size won't be monitored**.

Aggregate: Defines how the connections are aggregated before comparing them to the threshold (see aggregate mode).

Severity: Defines the level of severity of the alarm that will be generated if one of the thresholds is reached.

©copyright 2014 AGENTIL – all rights reserved

Autoclear: If set, the generated alarms will be automatically cleared from the console if the alarm condition is not fulfilled anymore.

Prefix: You can define some text to use as a prefix of the alarm message generated by the current rule.

Alarm/QOS: Defines if an alarm/metric has to be generated for the given rule.

Aggregate mode

If the aggregate mode is on, then only one alarm can be generated by the line of surveillance. The probe will sum all the connections matching the filter (host, status, user) and compare the number to the threshold.

If the mode is off, then connections will be put in different groups. Each group will contain connections on the same host. Then the probe will compare the number of connections from each group to the threshold. In that mode, several alarms can be sent (one per group)

QOS

These are the metrics that will be generated if the QOS option is enabled:

- SAPHANA_CONNECTION_COUNT: The number of current connections per instance.
- SAPHANA_CONNECTION_COUNT_PER_USER: The number of current connections per user.
- SAPHANA_CONNECTION_RUNNING_COUNT: The number of current running connections per instance

46. Hana blocked transactions

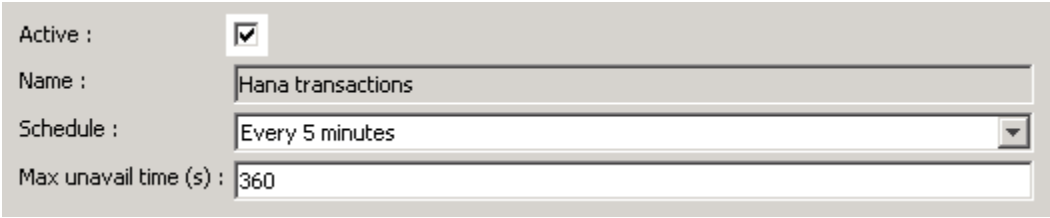
Monitoring capabilities

This monitor will look for blocked transactions and notifies when too many transactions are blocked since too long time.

You can customize the monitoring based on the host and the user running the transaction. You can also filter by schema and table name.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 5 minutes, but you can set a different schedule:



©copyright 2014 AGENTIL – all rights reserved

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring. You can apply filters based on the host, the user, the schema and the table. The max blocked time and max blocked transactions thresholds will define when to trigger an alarm for the transactions matching the filter.

Definition | Data | Test

Add row | Delete row | Duplicate row

Active	Host	Schema	Table	User	Max blocked time (s)	Max blocked trans.	Aggr.	Criticity	Autoclear	Prefix	Alarm	QOS
☑	*	*	*	*	30	10	☑	MAJOR	☑		☑	☑

Active: If checked, the rule is enabled and will be processed

Host: Can be used to restrict the monitoring to a given host (multi instance case). A star ('*') will match any host.

Schema: Can be used to restrict the monitoring on the transactions happening within a given schema. A star ('*') will match any schema.

Table: Can be used to restrict the monitoring on the transactions done on a given table. A star ('*') will match any table.

User: If different than star ('*'), only the connections of the given user will be taken into account.

Max blocked time: Only the transactions blocked since more than this threshold will be taken into account.

Max blocked transactions: The alarm threshold of the maximum blocked transactions.

Aggregate: If checked, an alarm will be sent if the total number of transactions blocked since more than the time threshold is over the max blocked threshold. If not checked, one alarm per transaction blocked since more than threshold will be sent.

Severity: Defines the level of severity of the alarm that will be generated if one of the thresholds is reached.

Autoclear: If set, the generated alarms will be automatically cleared from the console if the alarm condition is not fulfilled anymore.

Prefix: You can define some text to use as a prefix of the alarm message generated by the current rule.

Alarm/QOS: Defines if an alarm/metric has to be generated for the given rule.

QOS

These are the metrics that will be generated if the QOS option is enabled:

- SAPHANA_TRANSACTIONS_BLOCKED_COUNT: The current number of blocked transactions per instance.

©copyright 2014 AGENTIL – all rights reserved

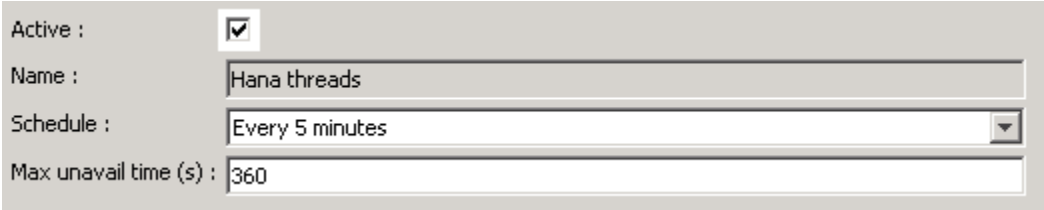
47. Hana threads

Monitoring capabilities

This monitor will check for long running threads. You can define a max runtime threshold in order to be notified if a thread is running for too long. You can specify different thresholds per service.

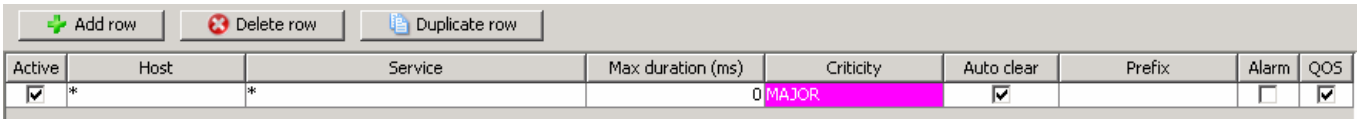
Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 5 minutes, but you can set a different schedule:



Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring. You can apply filters based on the host and the service. The max duration threshold will define when to trigger an alarm.



Active: If checked, the rule is enabled and will be processed

Host: Can be used to restrict the monitoring to a given host (multi instance case). A star ('*') will match any host.

Service: Filters threads from a given service. A star ('*') will match any service.

Max duration (ms): The threshold for the long running threads alarm.

Severity: Defines the level of severity of the alarm that will be generated if one of the thresholds is reached.

Autoclear: If set, the generated alarms will be automatically cleared from the console if the alarm condition is not fulfilled anymore.

Prefix: You can define some text to use as a prefix of the alarm message generated by the current rule.

Alarm/QOS: Defines if an alarm/metric has to be generated for the given rule.

QOS

These are the metrics that will be generated if the QOS option is enabled:

- SAPHANA_THREADS_COUNT: The current number of running threads.

©copyright 2014 AGENTIL – all rights reserved

48. Hana tables

Monitoring capabilities

This will monitor the following aspects of the database column store tables:

- The number of records.
- The number of delta records (not persistently written).
- The amount of delta memory (space used by delta records).
- The disk space used by the table.

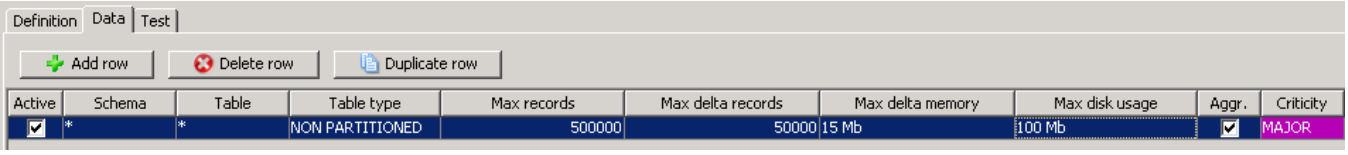
The monitoring can be customized based on filter set on the schema, the table and the type of table (partitioned or not).

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 15 minutes, but you can set a different schedule:

Surveillance table

Surveillance rules have to be added in the table in order to define the monitoring. You can apply filters based on the schema, the table or the table type.



Active: If checked, the rule is enabled and will be processed.

Schema: Can be used to restrict the monitoring on the tables within a given schema. A star ('*') will match any schema.

Table: Can be used to restrict the monitoring on a given table. A star ('*') will match any table.

Table type: Select the type of table to monitor between partitioned or non-partitioned.

Max Records: The threshold of the alarm on the maximum number of records.

Max delta records: The threshold of the alarm on the maximum number of delta records.

Max delta memory: The threshold of the alarm on the maximum delta memory (use KB/MB/GB units).

Max disk usage: The threshold of the alarm on the maximum disk used space (use KB/MB/GB units).

©copyright 2014 AGENTIL – all rights reserved

Aggregate: If checked, one alarm will be sent indicating the number of tables reaching each threshold. Potentially, there could be one alarm per breached threshold. If not checked, one alarm per table breaching a threshold will be sent. Potentially, there could be one alarm per table and per threshold.

Severity: Defines the level of severity of the alarm that will be generated if one of the thresholds is reached.

Autoclear: If set, the generated alarms will be automatically cleared from the console if the alarm condition is not fulfilled anymore.

Prefix: You can define some text to use as a prefix of the alarm message generated by the current rule.

Alarm/QOS: Defines if an alarm/metric has to be generated for the given rule.

Default thresholds

A threshold set to 0 will disable the check and prevent any alarm to be sent for this particular check. By default, thresholds are set to 0 when you create a rule.

By example, if you want to monitor the delta usage and not the current one, you can simply set current usage threshold to 0.

QOS

These are the metrics that will be generated if the QOS option is enabled:

- SAPHANA_TABLE_RECORD_COUNT: The number of records per table.
- SAPHANA_TABLE_DELTA_RECORD_COUNT: The number of delta records per table.
- SAPHANA_TABLE_DELTA_MEMORY: The amount of delta memory per table
- SAPHANA_TABLE_DISK_USAGE: The used space per table

Caution:

If you activate the QOS collection with the aggregate option set to OFF and without filtering the table name, it will certainly generate lots of metric data per check.

49. Hana merge statistics

Monitoring capabilities

This monitor will check for the time taken by the merge operation applied on each table. You can customize the monitoring by setting filters on the host, the schema and the table.

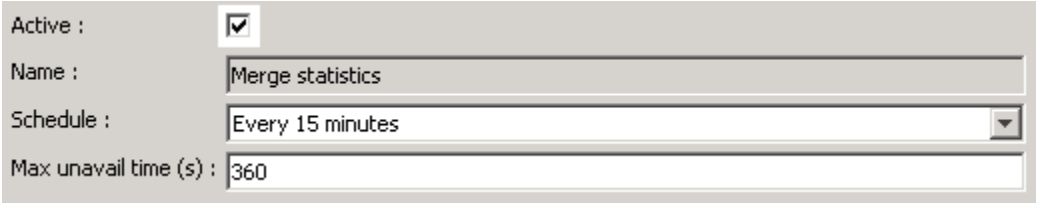
The probe will look for merge operations that happened since a time configurable in the “period” field.

©copyright 2014 AGENTIL – all rights reserved

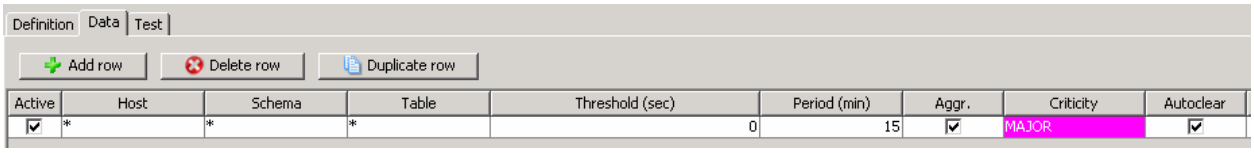
Any merge operation longer than threshold will trigger an alarm if the host, schema and table match the filter.

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 15 minutes, but you can set a different schedule:



Surveillance table



Active: If checked, the rule is enabled and will be processed.

Host: Can be used to restrict the monitoring to a given host (multi instance case). A star ('*') will match any host.

Schema: Can be used to restrict the monitoring on the tables within a given schema. A star ('*') will match any schema.

Table: Can be used to restrict the monitoring on a given table. A star ('*') will match any table.

Threshold: The maximum delta merges time before sending an alarm.

Period: The period of time in the past (computed from now) to look for merge operations.

Aggregate: If checked, one alarm will be sent indicating the number of merge operations reaching the threshold. If not checked, one alarm per merge operation will be sent.

Severity: Defines the level of severity of the alarm that will be generated if one of the thresholds is reached.

Autoclear: If set, the generated alarms will be automatically cleared from the console if the alarm condition is not fulfilled anymore.

Prefix: You can define some text to use as a prefix of the alarm message generated by the current rule.

Alarm/QOS: Defines if an alarm/metric has to be generated for the given rule.

©copyright 2014 AGENTIL – all rights reserved

QOS

These are the metrics that will be generated if the QOS option is enabled:

- SAPHANA_DB_MERGE_STATISTICS_TIME: The time of the last delta merge per table.
- SAPHANA_DB_MERGE_STATISTICS_COUNT: The number of records merged in the last operation, per table.

Caution:

If you activate the QOS collection with the aggregate option set to OFF and without filtering the table name, it will certainly generate lots of metric data per check.

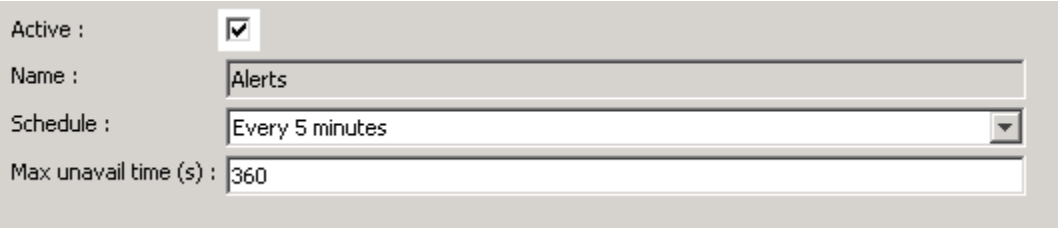
50. Hana alerts

Monitoring capabilities

This monitor will collect the current alerts from HANA statistics engine and forward them through probe alarm interface.

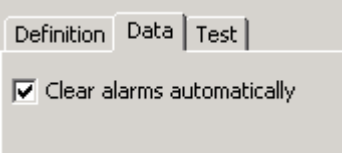
Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 5 minutes, but you can set a different schedule:



Alarm auto clear

The only configuration option of this monitor is to set if you want the alarms to be cleared if the alert is not present anymore in the statistics engine:



51. Hana replication status

Monitoring capabilities

This monitor will check several HANA replication indicators to see if replication is running fine:

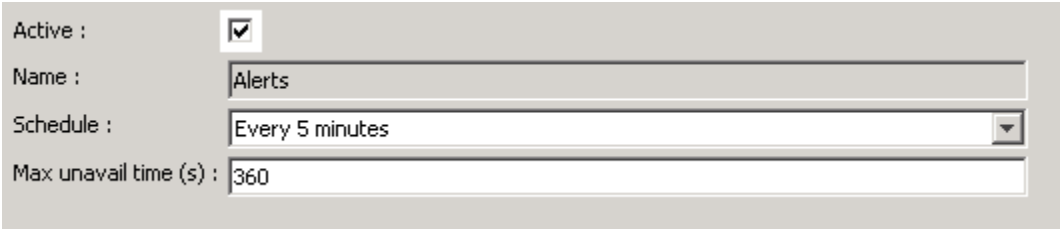
- Check expected replication mode
- Check replication status on primary and secondary

©copyright 2014 AGENTIL – all rights reserved

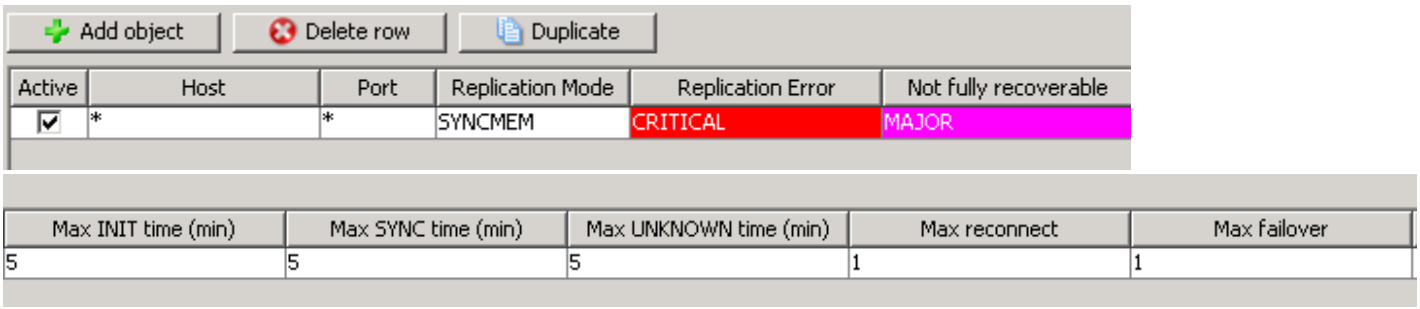
- Check secondary fully recoverable
- Check long lasting intermediate states
- Check reconnect and failover occurrences

Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 5 minutes, but you can set a different schedule:



Surveillance table



Active: Use this field to activate or deactivate a line of configuration.

Host: A filter on the host name.

Port: A filter on the port

Replication Mode: Defines the expected replication mode. Send an alarm if different.

Replication Error: Defines the error severity to send when replication status is in error state.

Not fully recoverable: Defines the error severity to send when the secondary is not fully recoverable.

Max INIT time: The maximum time allowed for the replication status to be in INITIALIZING state.

Max SYNC time: The maximum time allowed for the replication status to be in SYNCING state.

Max UNKNOWN time: The maximum time allowed for the replication status to be in UNKNOWN state.

Max reconnect: The maximum number of reconnects allowed between 2 checks.

Max failover: The maximum number of failovers allowed between 2 checks.

©copyright 2014 AGENTIL – all rights reserved

Auto clear: If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

Alarm tag: This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.

Alarm: If checked, this line of surveillance will be used for alarm generation.

Metric: If checked, this line of surveillance will be used for Metric generation.

52. Hana replication shipping statistics

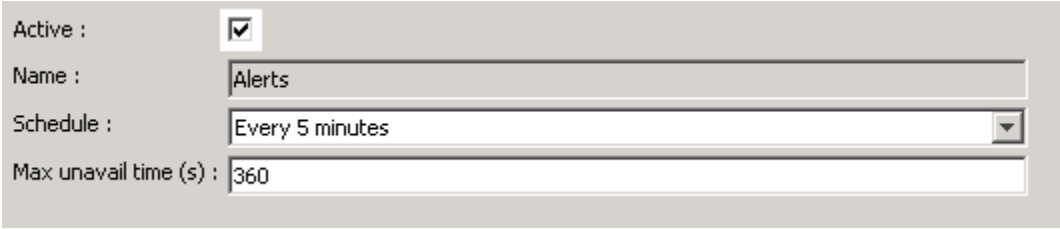
Monitoring capabilities

To monitor the replication shipping statistics of HANA database. It will monitor the flow of log and data segments between primary and secondary, looking for delay or size issues:

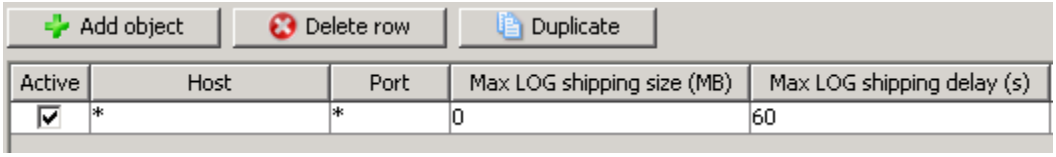
- Log data shipping delay
- Log data size to ship
- Last delta data size to ship
- Last delta data size shipping duration

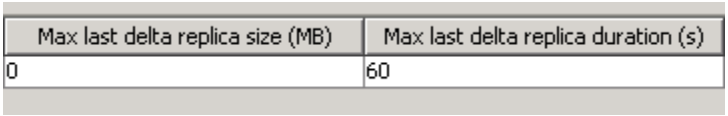
Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 5 minutes, but you can set a different schedule:



Surveillance table





Active: Use this field to activate or deactivate a line of configuration.

©copyright 2014 AGENTIL – all rights reserved

Host: A filter on the host name.

Port: A filter on the port

Max LOG shipping size: The maximum size of log segments waiting to be shipped to secondary.

Max LOG shipping delay: The maximum time between replicated Log position on secondary and current position in primary

Max last delta replica size: The maximum size of delta data segments waiting to be shipped to secondary.

Max last delta replica duration: The maximum transfer duration of delta data segments.

Default severity: The alarm severity to use for any threshold breach, if the advanced threshold syntax is not used.

Auto clear: If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

Alarm tag: This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.

Alarm: If checked, this line of surveillance will be used for alarm generation.

Metric: If checked, this line of surveillance will be used for Metric generation.

53. Hana replication LOG retention

Monitoring capabilities

If maximum LOG retention is reached, log buffers will be reused and replication will not be possible anymore.

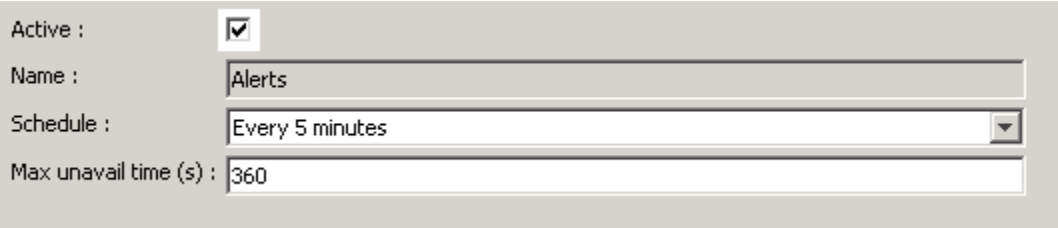
This monitor will check the log backup retention and warn if it is approaching the limits. It will compare the average daily log backup throughput with the defined retention limit parameter, and the physical remaining disk space.

It is also possible to monitor the average size of daily log backups, computed over a configurable period of time.

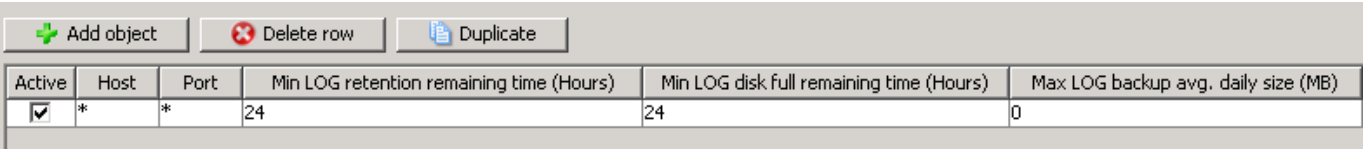
Job schedule definition

The check will be performed on a regular basis. This can be configured in the job definition.
By default, the job will run every 5 minutes, but you can set a different schedule:

©copyright 2014 AGENTIL – all rights reserved



Surveillance table



Active: Use this field to activate or deactivate a line of configuration.

Host: A filter on the host name.

Port: A filter on the port

Min LOG retention remaining time: The minimum time expected before reaching the retention limit parameter settings.

Min LOG disk full remaining time: The minimum time expected before a disk full situation.

Max LOG backup avg. daily size: The maximum average size of generated log backup on a daily basis, computed over a configurable period.

Default severity: The alarm severity to use for any threshold breach, if the advanced threshold syntax is not used.

Auto clear: If checked, the alarm will be cleared as soon as the alarm condition is not met anymore.

Alarm tag: This field allows to add custom text within the alarm message. %MSG% variable will contain the actual generated message and can be used such as: "my_prefix %MSG% my_suffix". By default, tag will be used as prefix.

Alarm: If checked, this line of surveillance will be used for alarm generation.

Metric: If checked, this line of surveillance will be used for Metric generation.

54. Create new monitor jobs

If you purchase the development license, you have the capability to extend the library by creating your own monitor jobs.

©copyright 2014 AGENTIL – all rights reserved

54.1. Collect new metrics

The main use case in extending the monitoring library is to monitor metrics that are missing in the library. All metrics are collected by **input jobs**.

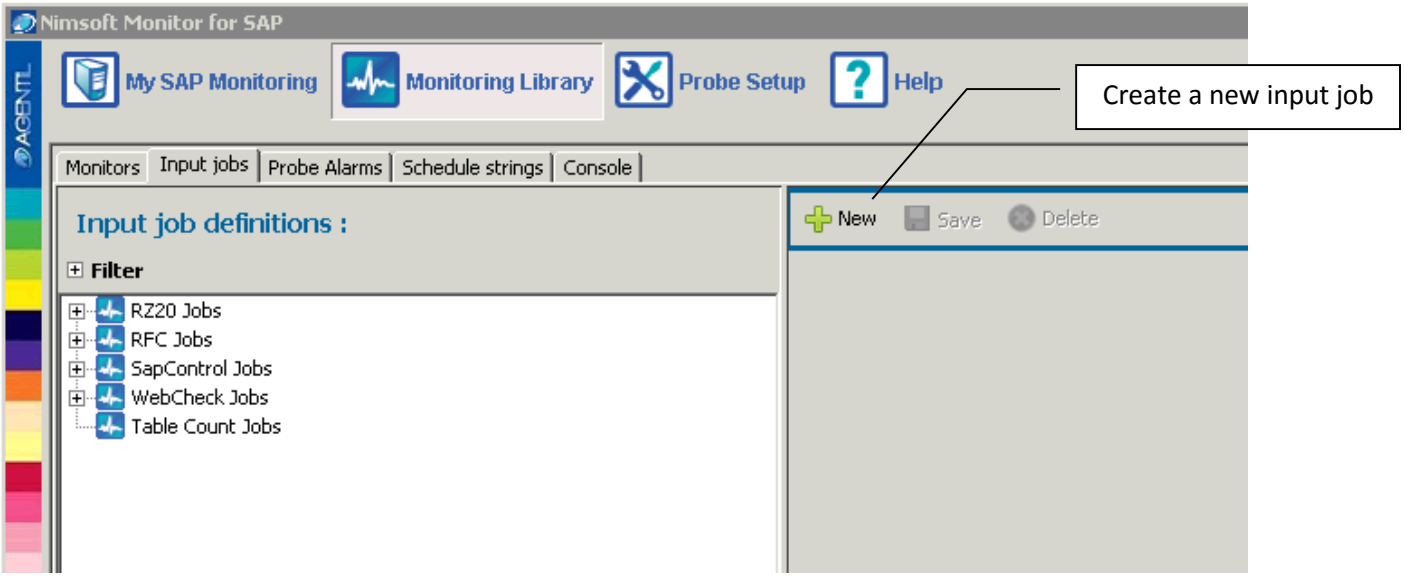
The result of an input job usually contains multiple metrics that can be used separately. That's why you have to define a structure called a **monitored value** that will extract a part of the result of an input job.

This monitored value can then be used in an Alarm or QOS job.

Monitored values can contain simple data (a number) as well as more complex data (table). Once you have defined an input job, you can execute it against a system, and create a monitored value directly from the displayed results.

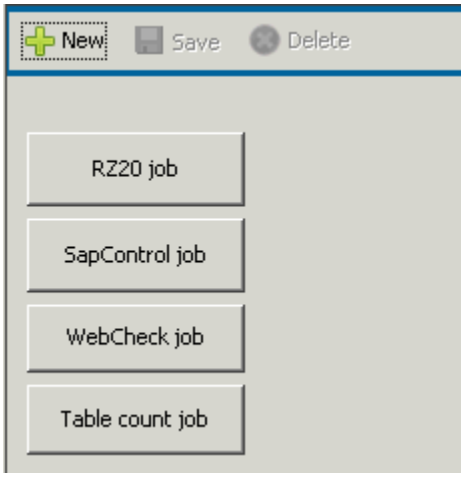
Create an input job

Go in the "Monitoring library" section, select "input job" section. Then hit the "New button"



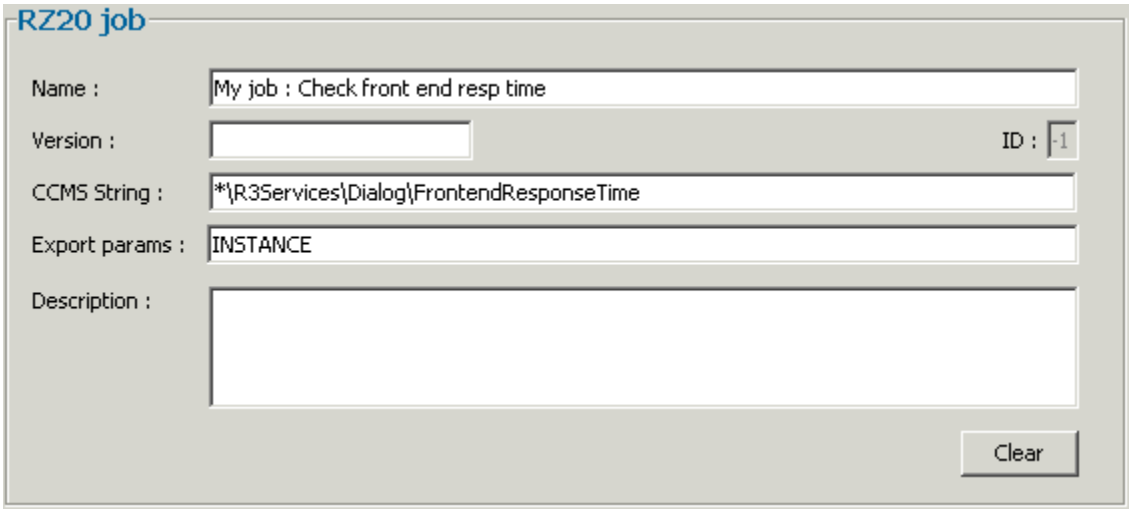
Then select the type of job that you want to create:

©copyright 2014 AGENTIL – all rights reserved



It will open the corresponding job editor:

By example, RZ20 input job:



Set the corresponding job parameters and **save**. The new job will appear in the input job tree in the left panel.

RZ20 jobs have 2 specific fields:

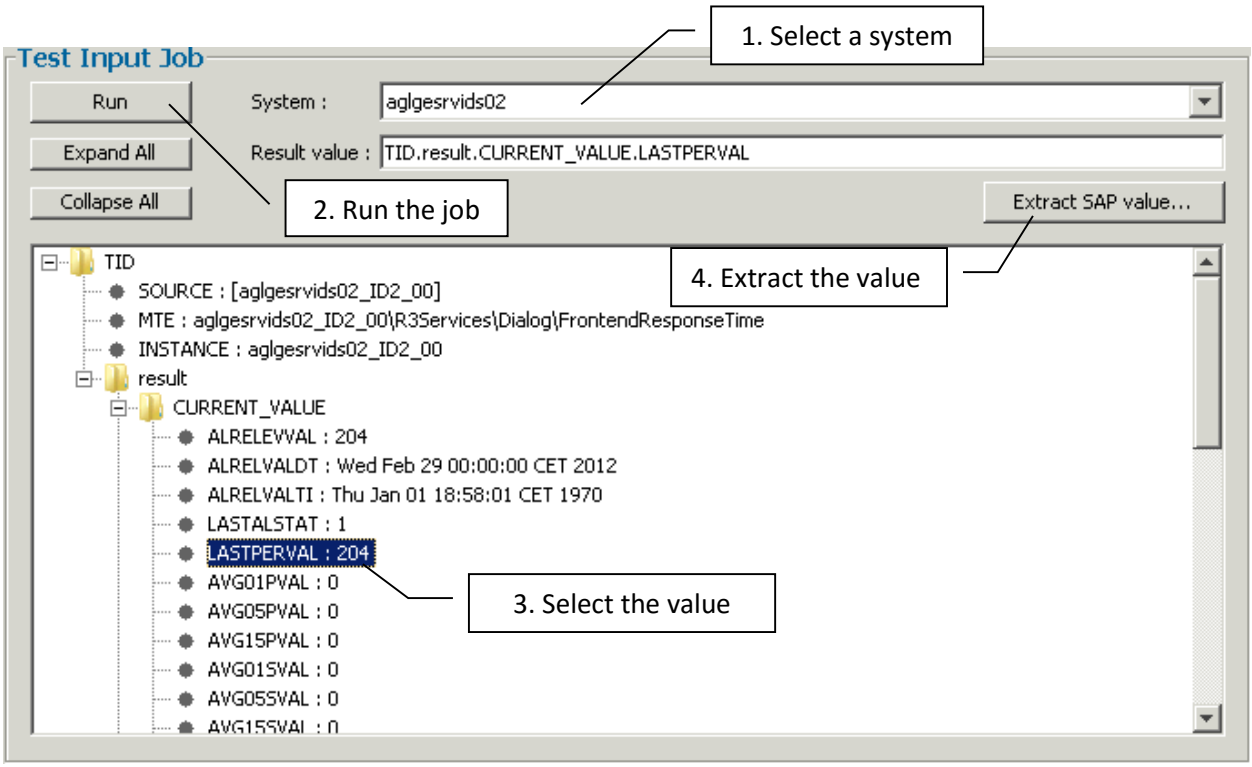
- CCMS string: The path in the CCMS tree to the targeted metric. You can hit several similar metrics by replacing variable parts in the path by '*', like instance name or disk name for example. Job results will be held in a table, each row corresponding to a matched path.
- Export params gives the possibility to name each path part replaced by '*'. The replaced part will appear in the result table, in the column having the specified name.

Now that you have created your job you, want to test it against a system. For that you can use the "Test input job" panel.

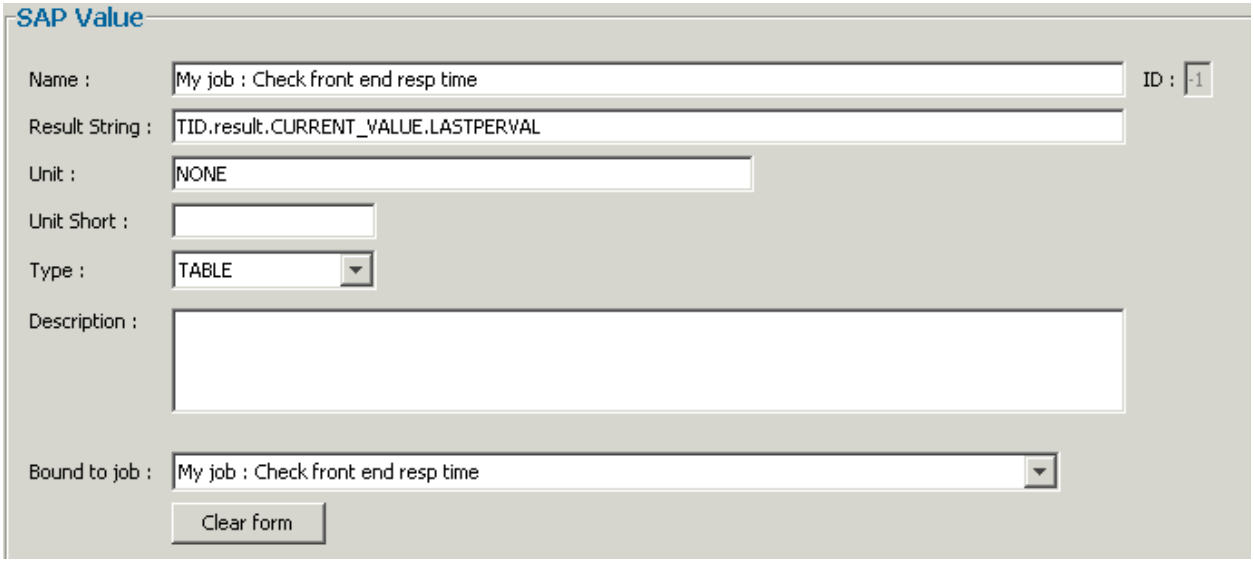
Select the system with which you want to test the job and then hit the "Run" button.

©copyright 2014 AGENTIL – all rights reserved

The result of the job execution will be displayed in the panel. Select the metric that you want to use and click on “Extract SAP value” button.



This will open the monitored value editor, pre-filled with the metric path in the input job result:



The result string and type parameter are automatically filled. You can specify the Unit and Unit short parameters, set an optional description and change the name of the input job.

©copyright 2014 AGENTIL – all rights reserved

Once you are done with the settings, you can save the monitored value. It will appear as a child node of its input job in the left tree panel.

Note: An input job can be associated with several monitored values. But a monitored value is only associated to one input job.

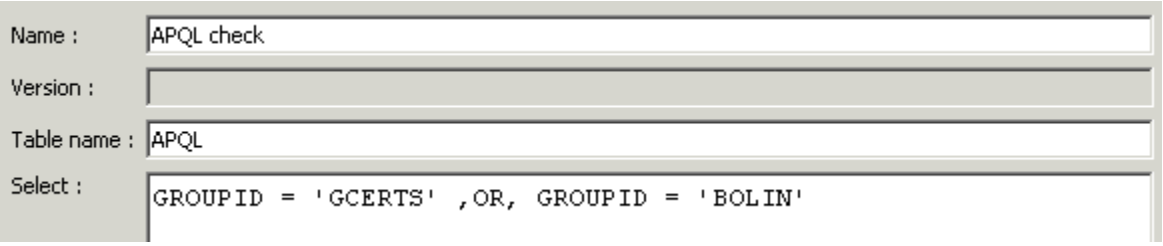
At this stage, you have configured the way to fetch a new metric in SAP. You are now ready to use it in an Alarm or QOS.

Table count input job

The purpose of this job is to get the number of lines of an SQL SELECT result.

You need to specify a table name and an optional SQL request, by following the syntax that you would use in the SE16 transaction.

If no SELECT is defined, it will simply return the table size.



Note: It is advised to put OR and AND statements between colon, like shown in the above example.

The number of lines will be held in the “NBLINE” parameter of the result of the job. You can then extract a monitored value from it and use it in an alarm like all other regular values.

54.2. Create new alarms and QOS

Alarms and QOS jobs included in the default library can be customized, but the metrics they use and few intrinsic parameters cannot be modified. That’s why you can create new monitor jobs that you can configure exactly like you want.

You might want to create a new monitor job in order to monitor a new SAP metric that you created, or to change the monitoring of existing metrics.

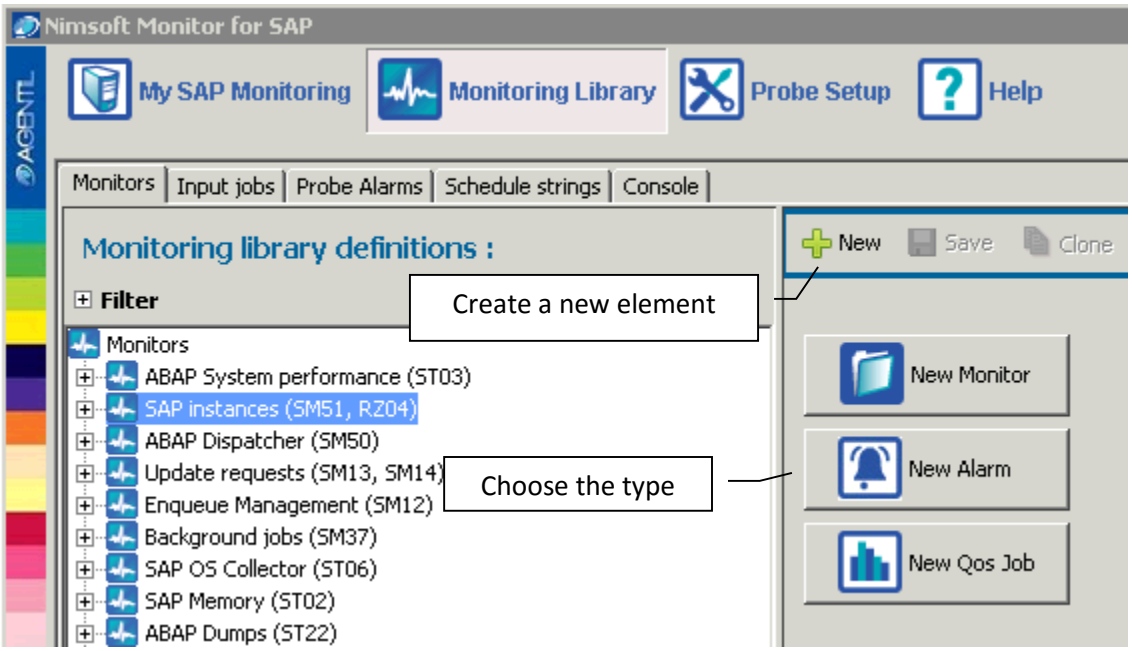
To create a new monitor job, go in the “Monitoring library” section, select the “Monitors” tab and hit the “New” button.

You will then be able to choose between 3 elements:

- Create a new Monitor (job container)
- Create a new Alarm
- Create a new QOS

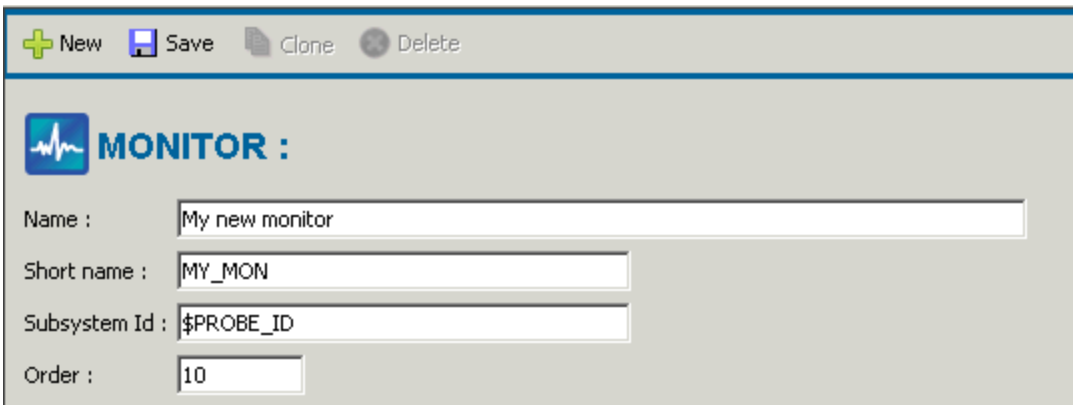
©copyright 2014 AGENTIL – all rights reserved

Click on the element that you want to create.



54.2.1. Creating a new monitor

Monitors are job containers. It's mainly useful for grouping jobs per monitoring scope.



A monitor has following parameters:

- A Name : best if meaningful
- A short name : used in Alarm and QOS data structure in UIM
- A subsystem Id : Used to sort and filter alarms in UIM
- An order : Its position in the display list in the monitoring library

When you save the monitor, it will appear in the monitors tree. You will then be able to include it in a template and to assign it to SAP systems.

©copyright 2014 AGENTIL – all rights reserved

54.2.2. Creating an Alarm or QOS job

Select the monitor in which you want to add the job, then click on the "New" button and select the appropriate job. It will open the job editor.

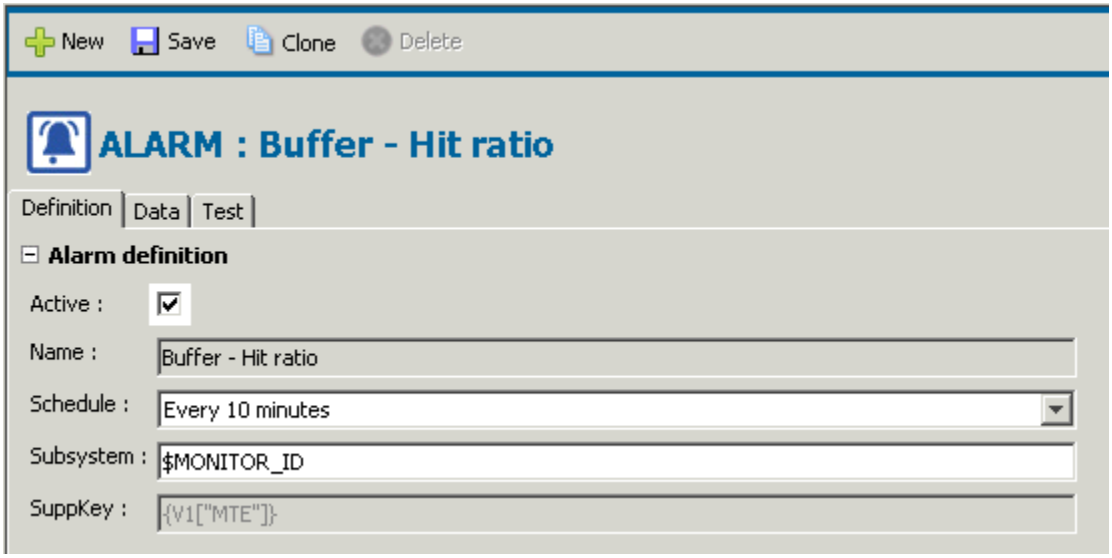
Alarm and QOS jobs configuration are quite similar, both have 2 parts:

- A definition part: Name, schedule, description, etc…
- A data part: The SAP metrics to use and the way to process them

Alarm definition

The definition part of an alarm has the following parameters:

- Its state: Active or not. It won't be executed if inactive.
- Its name: Prefer meaningful names.
- Its schedule: Choose how often the job will run
- Its subsystem Id: Associated will all the alarms that this job will generate. Used to sort and filter the alarms in UIM
- Its suppression key: Must be unique for each different type of alarms that the job will generate



<u>Suppression key mechanism</u>:

The suppression key is a parameter that you should consider with care. It is the only link that that ties the Alarm from the probe to UIM.

If the condition that triggered an alarm is not true anymore, the probe will send a "clear" signal to UIM in order remove it from the alarm console. The suppression key will be used to match the clear to the appropriate alarm in the UIM database.

It is important that two alarms referring to two different problems are not using the same suppression key, otherwise if one of the problems disappears, both alarms will be cleared.

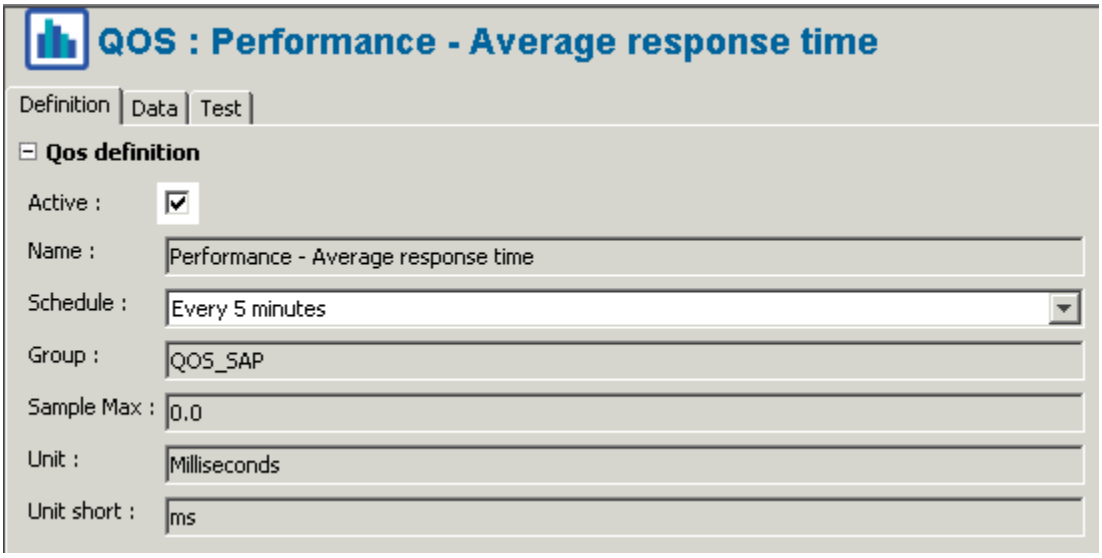
©copyright 2014 AGENTIL – all rights reserved

The probe prepends the job Id and system Id to the suppression key, insuring the isolation of the alarms for each different job. But if one job generates alarms aiming different scopes, by example disk sizes, the subsystem field must be set in order to differentiate alarms set for one disk, and alarms sent for another. You can then use the disk name as suppression.

QOS definition

The definition part of a QOS job has the following parameters:

- Its state: Active or not
- A name
- Its schedule
- Its QOS group: Used in UIM to order QOS
- A sample max value (optional): Used to improve graph scales in UMP dashboards
- A unit name and short name



Monitor job data configuration

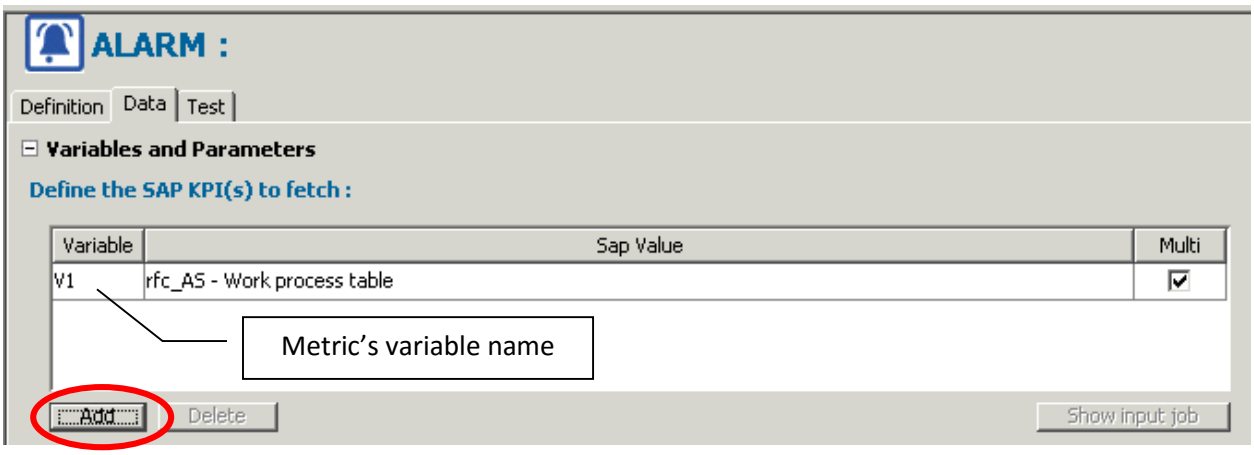
In the data part of an alarm, you can configure the following parameters:

- SAP metrics to use
- Alarm expressions
- Alarm parameters
- A pre-filter: used to improve the processing of big tables
- A script definition: used to process complex data
- Alarm expression: compare SAP metrics to parameters
- Alarm message
- Alarm severity

©copyright 2014 AGENTIL – all rights reserved

SAP metrics

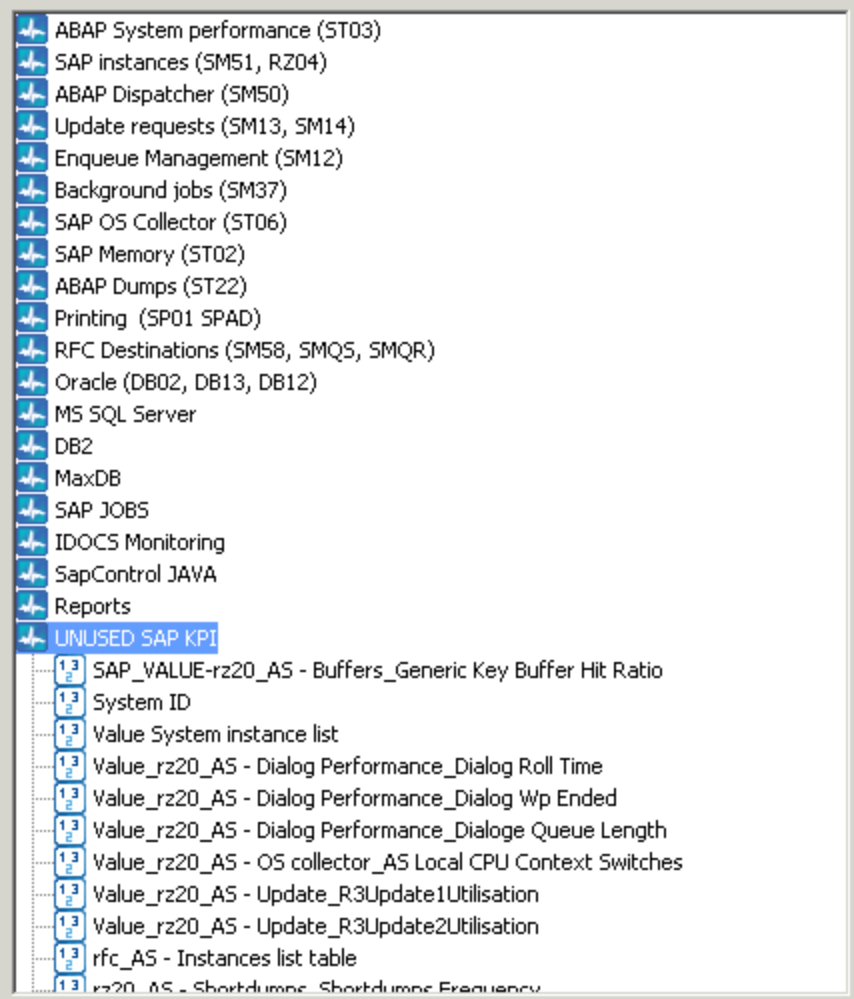
The first table of the panel displays the metrics used by the alarm. Each metric get an arbitrary variable name starting by “V”. This metric can then be referred by using this variable name.



To add a metric, simply click on the “add” button. It opens panel showing all available monitored values. They are ordered by monitors.

Unused monitored values are grouped in a monitor at the bottom of the list. Select the one you are looking for and validate. The monitored value will be added into the table, and can be used in the alarm expression with its variable name: V1, V2, etc…

©copyright 2014 AGENTIL – all rights reserved



Types of metrics

Monitored values can contain 3 types of data:

- Scalar values (a number, a string): You get the value contained in the variable directly by using the variable name in the expression. By example: V1 > 100
- Maps (like a table, but with one row only): You get values in the variable by using their field name. By example: V1["DISK_SIZE"] > 100
- Tables. Each row contains a map, where you can get the values using the column name. Tables need to by parsed using a script. By example: *for(item:V1){ item["name"] }*

Warning: Monitored values extracted from RZ20 input jobs will always be a table type. The value itself will be contained in the column named "VALUE", and the path to the value in the CCMS tree will be set in the column named "MTE".

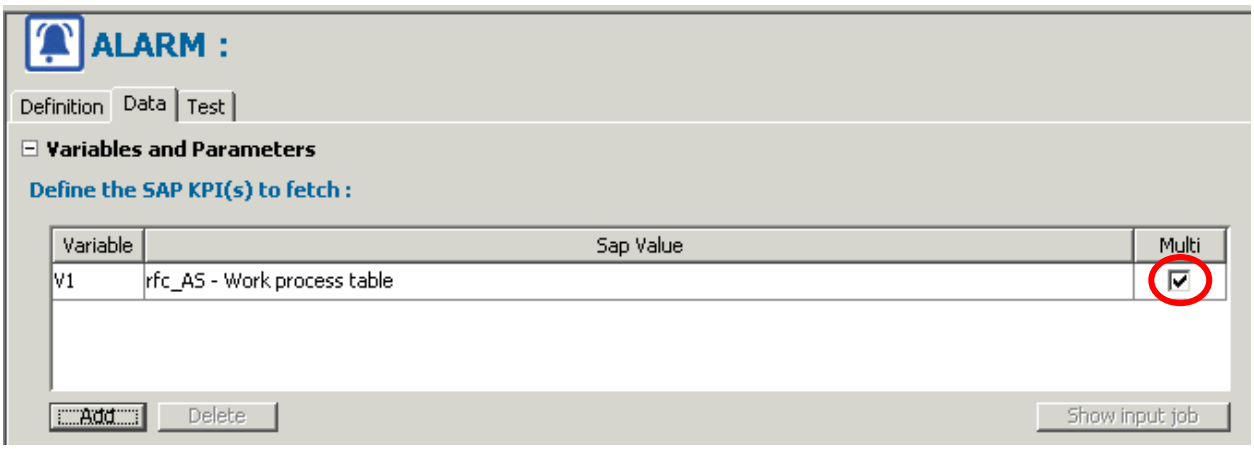
Parsing table

There are 2 ways of parsing a table:

Using the "multi" option:

©copyright 2014 AGENTIL – all rights reserved

Selecting the “multi” option in the monitored values table will have the following effect: Instead of passing the entire table to the alarm, the probe will only pass one row at a time, and execute the alarm for each row.



By example, considering a monitored value containing RZ20 results about disk space of 3 different disks:

If multi is not selected, the variable V1 will contain a table of 3 rows:

Instance	Name	value
SAP01_PRD_00	C:	1220
SAP01_PRD_00	D:	3000
SAP01_PRD_00	E:	5000

The mechanism of sending a different alarm for each row will be difficult to achieve if the alarm get the entire table at once. But if you select the multi checkbox, the alarm will be called 3 times, and V1 will contain consecutively the each row of the table. The alarm expression can be as simple as that: V1[“VALUE”] > P1

In summary, the “multi” option will help to process results aggregated in a table, where the content of each row needs to be processed independently than the others.

<u>Using the alarm script</u>:

The use of the script to process tables is recommended when the metric to analyze is the combination of data contained in several rows.

Let’s consider the following example of an alarm, getting the number of errors for a set of jobs. An alarm signal will be sent if the total number of error is greater than a threshold:

©copyright 2014 AGENTIL – all rights reserved

JOB_NAME	CLIENT	ERRORS
JOB_1	000	12
JOB_2	000	3
JOB_3	000	50

You can consider using the following script to parse the table:

Script

```
TOTAL_ERRORS = 0;
for(V1:item){
   TOTAL_ERRORS = item["ERRORS"] + TOTAL_ERRORS
}
```

The variable "TOTAL_ERRORS" created in the script can be used in the alarm expression and in the alarm text message: TOTAL_ERRORS > P1

Script

When you need to pre-process monitoring information contained in monitored values, the scripting capabilities of monitor jobs can be useful.

The script uses the apache JEXL engine. It is quite simple to use. See online documentation (http://commons.apache.org/jexl/reference/syntax.html). Scripts are mostly used for parsing tables or consolidating information from heterogeneous data. See usage examples in the monitoring library.

Variables that you create in the script can be used in alarm's expression and message.

By example:

©copyright 2014 AGENTIL – all rights reserved

Script

```
HAS_ERROR = false;
ERROR_MSG = "";

for(item:V1){
 if(item["name"].contains("SDM")
    && item["statetext"].equals("Running")==false){
  HAS_ERROR = true;
  ERROR_MSG = "SDM is not running.";
 }
}
```

Expression : HAS_ERROR

Severity : MAJOR

Message : {ERROR_MSG}

Alarm expression

To create an expression, click on the “Add expression” button

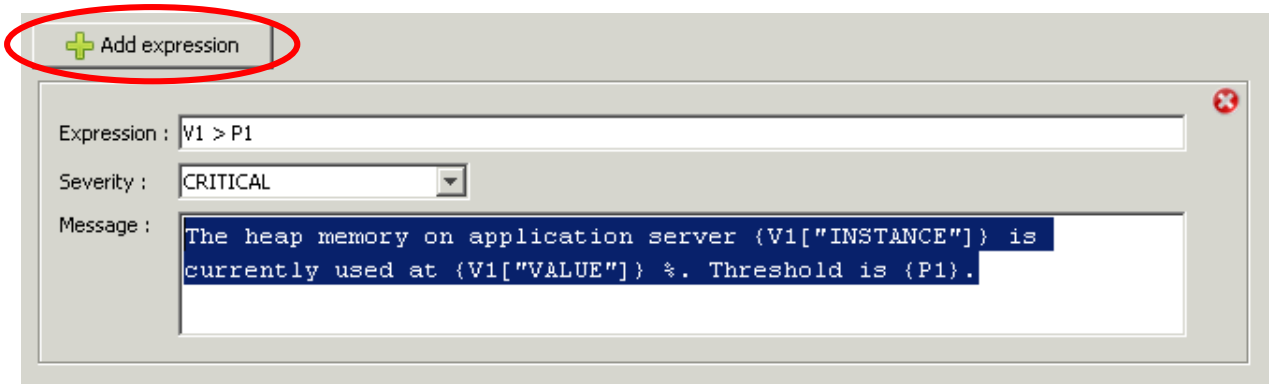
The alarm expression defines if an alarm signal must be triggered, based on the value of the metric. It is composed by:

- An expression that is evaluated
- The severity
- The text message of the alarm

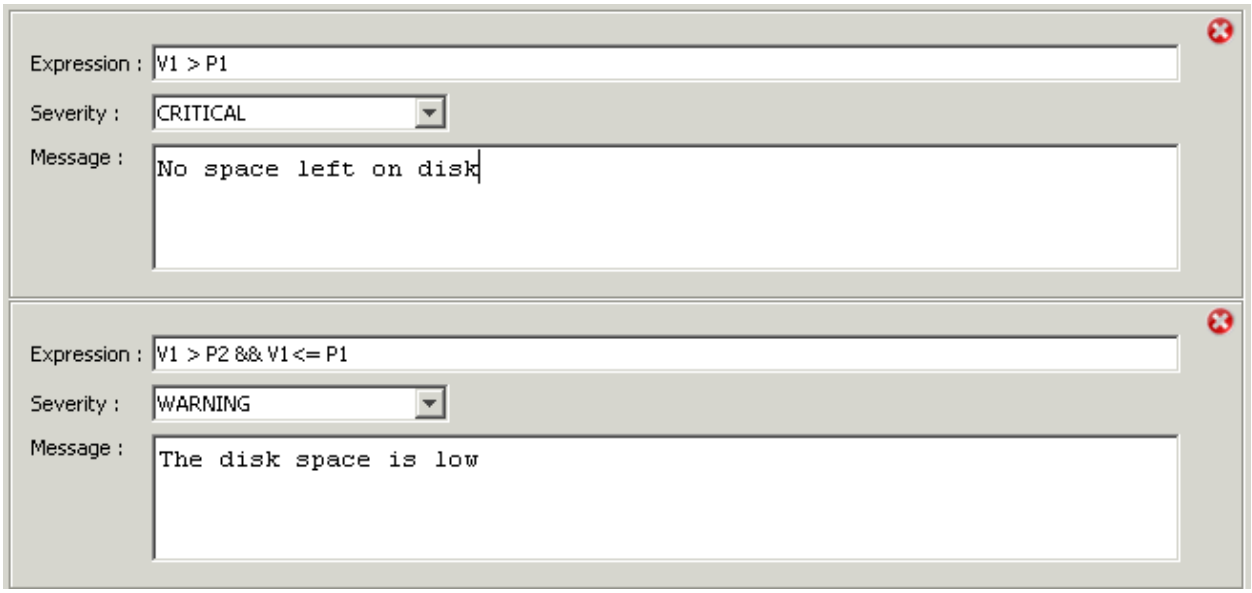
If the expression is evaluated to true, then an alarm signal will be sent with the specified text and severity.

Metric values can be used in the alarm message by simply putting the variable name between “{}”.

©copyright 2014 AGENTIL – all rights reserved



You can add multiple alarm expression in order to send several alarm levels:



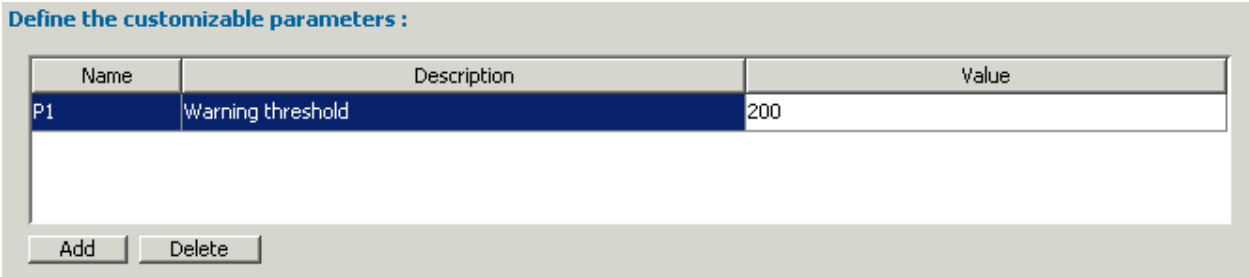
Job parameters

Parameters give more flexibility to your job. You can use them to define alarm expressions that can be customized, simply by changing a parameter value.

The value of a parameter can be customized from a system to another. By example, you don't want to use always the same threshold for disk space monitoring.

You can create parameters in the parameters table by clicking the "add" button. Then give it a meaningful description and a value. Each parameter that you create gets an arbitrary name starting with "P". You can use any parameter in the alarm expression by referring to its name.

©copyright 2014 AGENTIL – all rights reserved



You can decide to put a default value in the parameter, or to left the value empty. If it is empty, the user will have to customize the value in the template or in the system.

Pre-filters

This field can be used to improve the processing of monitoring values containing a long table.

It can contain an expression similar to what you can use in alarm expressions. If the expression is true, the job will process the data.

This field is mostly useful if you are using “Multi” monitored values.

55. Configuration

The configuration of the probe involves completing the following steps:

1) Configure the common options of the probe
2) Define the SAP systems that you want to monitor
3) Define and tune your monitoring templates
4) Assign the templates to your systems

55.1. Configuring the general setup of the probe

55.1.1. Setting the log level

In the probe setup window, you can define the log level of the probe.

55.1.2. Setting the base Subsystem ID

In the windows, you can define the global subsystem id prefix of the probe. Then, in each subsystem ID, you can redefine the subsystem ID. To do this you can either enter an arbitrary ID or use the keyword $SYSTEM_ID which will be replaced the probe level subsystem id.

You can configure the subsystem id of the UIM alarms at 3 different levels.

- Probe level configuration: The ID defined at this level will be globally available through the variable $PROBE_ID.

©copyright 2014 AGENTIL – all rights reserved

- Monitor level configuration: Each monitor can have its own subsystem ID available through the variable $MONITOR_ID in the contained alarms. By default all the monitors have unique subsystem ID generated with the $PROBE_ID variable as prefix.
- Alarm level configuration: In all the alarms you can configure a subsystem ID using a combination of the probe and monitor subsystem ID prefix. By default all the alarms have subsystem ID defined as equal to the subsystem ID of the containing monitor.

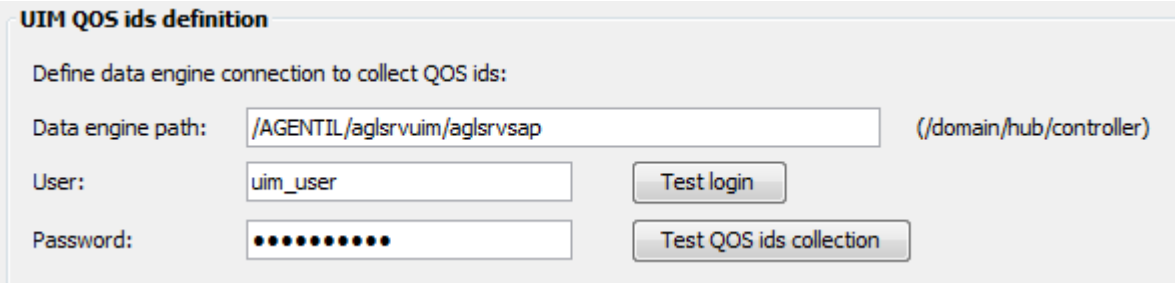
For example, by default, if the general subsystem ID is defined as: "2.13.1", the subsystem ID defined in the monitor "ST03" is $PROBE_ID.1 (which is expended into 2.13.1.2.1) and the subsystem ID defined in the monitor "ST06" is $PROBE_ID.2 (which is expended into 2.13.1.2.2).

All the alarms in monitors ST03 and ST06 are defined as $MONITOR_ID. So, all alarms in ST03 and ST06 will be sent with the subsystem 2.1.1 and 2.1.2 respectively.

51.1.3 UIM QOS ids

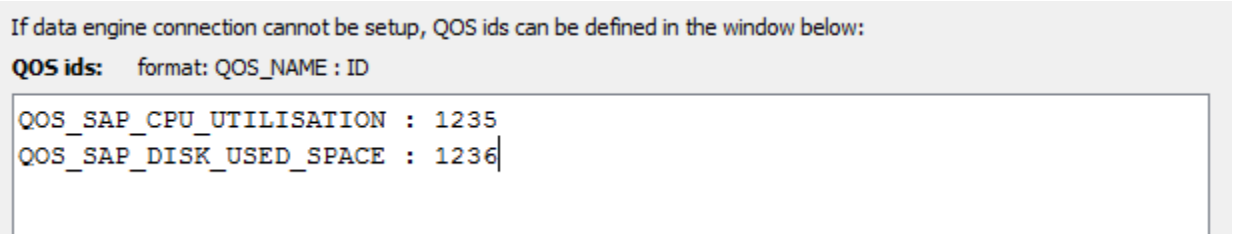
In order to generate dashboards, the probe needs to get the QOS ids of the metric used in the dashboard definition.

For that, you can register the Data engine path and user credential so the probe can call data engine methods to collect QOS ids.



Once the parameters are registered, you can test the connection with the test button, and test the QOS ids collection with the Test QOS ids collection button.

If connection to data engine cannot be established, you can register the QOS ids manually in the dedicated text area:



Press apply to save the QOS ids.

Note: The QOS ids registered manually won't be reloaded in the text area next time you run the GUI.

©copyright 2014 AGENTIL – all rights reserved

55.2. Create and tune Monitoring templates

The monitoring library already defines few templates that you can use. It is recommended to clone them and to update the copy.

You can also create your own templates. Some jobs must be customized in order to be runnable. They appear with a red icon.

55.3. Assign templates to the SAP systems

When you have defined all the templates that you need, you can assign them one by one to your systems. If not already done, you can then enable the monitoring of each system.

If a system has its monitoring enabled, each change done in its configuration or in a template that it uses will be applied right away.

56. Managing probe updates

New versions of the probe usually contain updates of the monitoring library. They can be of different kinds:

- New monitor jobs added
- Existing jobs updated
- Jobs removed or replaced

In such cases, it is important to be able to manage the impacts of the upgrade on the existing configuration.

In that matter, the probe gives the possibility to check the change and the impacts for any upgraded job.

56.1. How to update the probe

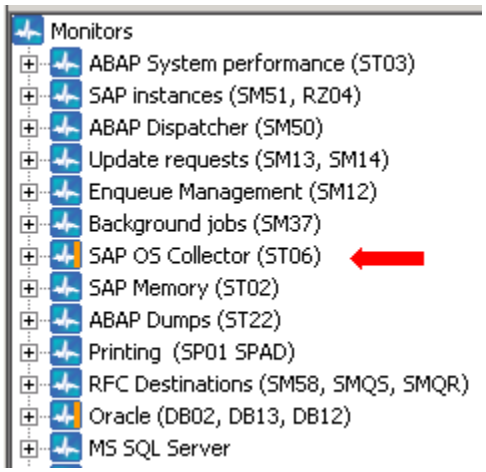
The update mechanism has been designed to simplify the work of the user.

When a new version of the probe is released, you can simply apply the package over the current one. This procedure is safe and won't affect your existing configuration. The interface will later give you the choice to apply the changes or not.

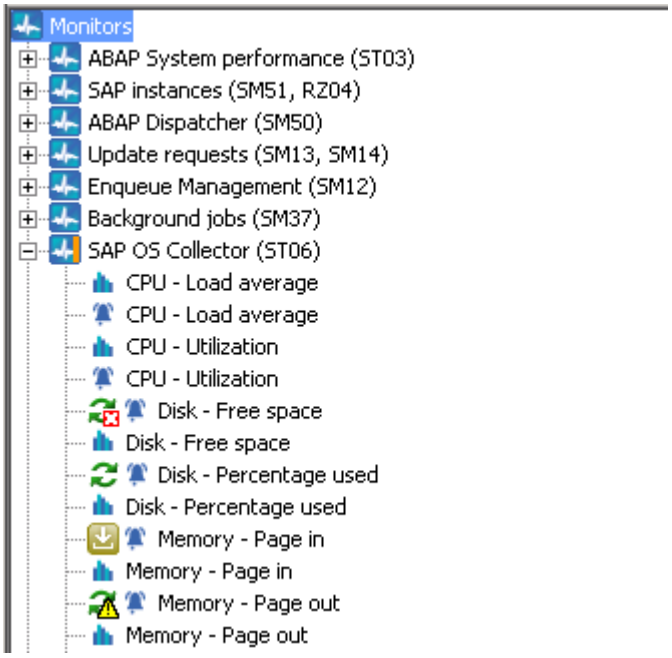
56.2. Updates icons

When the new version has been installed, launch the user interface and open the monitoring library section. The monitors that contain updated jobs will be shown with a specific icon:

©copyright 2014 AGENTIL – all rights reserved



Open one of the flagged monitors, you will see that updated jobs will be shown along with specific icon:



The update icons have the following meanings:

An update of the job is available.

An update of the job is available and is **potentially** in conflict with one of its customized versions

The job is obsolete, it can be removed. Might be replaced by a new one

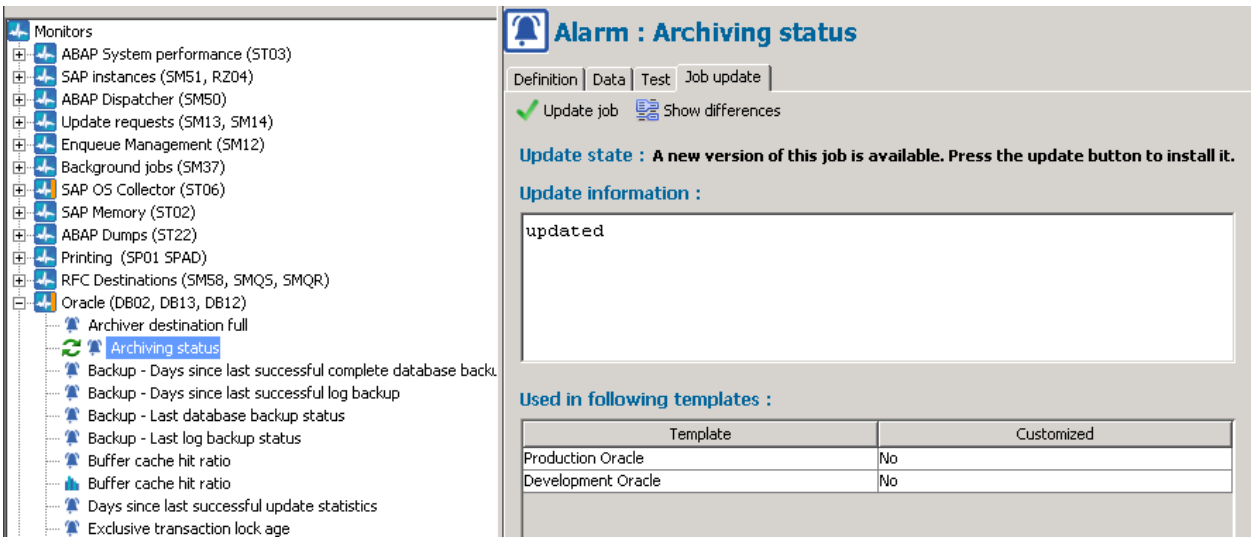
©copyright 2014 AGENTIL – all rights reserved

This is a new job. It has been installed, but won't be active by default in the templates using its monitor.

The job has been updated automatically: Happens by example if the update won't have impact on the current configuration. (Example: cosmetic changes)

56.3. The job update menu

Each updated job will have an additional tab available in its definition screen. Select a job in the library and click on the "Job update" tab



From this menu, you can see the following:

- The update state of the job: New, updated, obsolete.
- The update description: Some information about what has been updated and why.
- A table displaying the templates using the job, and if it has been customized

Then you can perform the following actions:

- Update the job: It will overwrite the default parameters of the previous version.
- Show the differences between the new and the previous version.
- Clear the update flag: The job will no longer be displayed as an updated job.
- Delete the job: In case of obsolete job, you can take the decision to delete it.

Note: A job will be flagged to be in conflict with current configuration if one of its instances has been customized in a template or in a system.

When you decide to accept the update, you can press on the "Update Job" button. It will replace the default definition of the previous job.

©copyright 2014 AGENTIL – all rights reserved

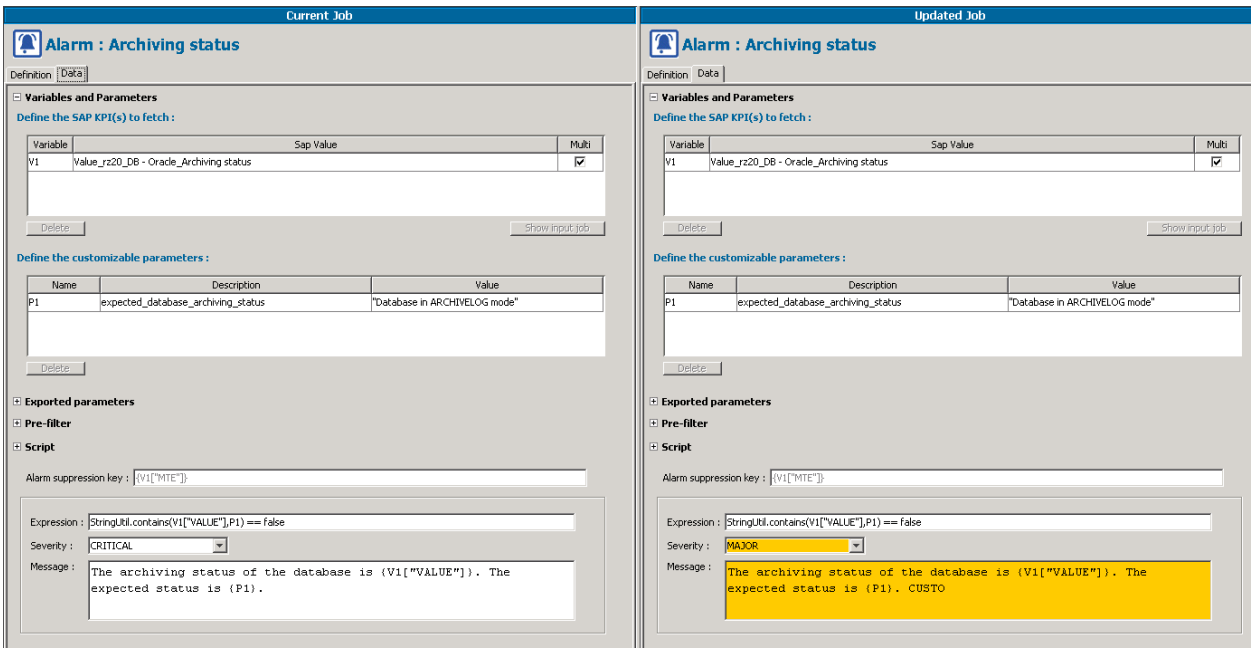
Note: Existing customizations of the job in templates or systems will remain valid and won't be lost. The update will only change the default values. A customized value that has been updated will stay customized.

56.4. The diff tool

When an existing job has been updated, you have the possibility to display the new and the previous version of the job side by side. Use the "Show differences" button to display the tool.

The new version will be displayed in the right window, with the updated parameters highlighted. The left panel will show the current version with highlighted customized parameters.

If you use the diff tool from the definition of the job in the monitoring library, it will show the difference with the default parameters. If you use it from the template or system definition, it will show the difference with customized parameters, if any.



56.5. Conflict

When a job is flagged to be in conflict, that means that it is only a potential conflict. The probe detected that the job has been customized in a template or in a system, and to apply the update might affect the logic of the job combined with the customized part.

In case of conflict, the user must use the diff tool for each conflicting job instance and check that the update won't affect its configuration.

If the conflict actually exists, the user can choose not to apply the upgrade, or to merge its customization in the newer version.

©copyright 2014 AGENTIL – all rights reserved

57. SNC RFC communication

This chapter describes how to set the SAP Secured Network Communication (SNC) protocol operational with the probe. In the following sections, the SAP server will be called « SNC server » and the probe will be called « SNC client ».

57.1. SNC client folder

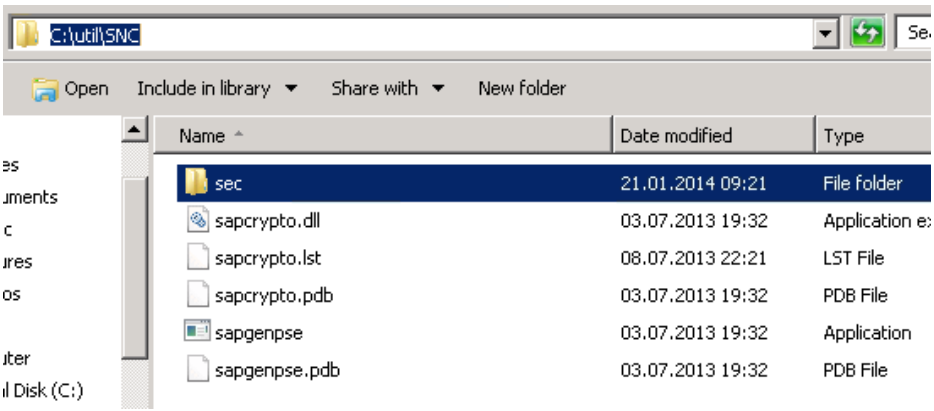
The SNC client folder will be used to store the cryptographic libraries and certificates.
By example: C:\util\SNC\sec
We will use this folder as example in the installation procedure.

57.2. Installation of the SNC libraries

In SAPNET, the archive file of the cryptographic libraries for « X64-NT-x86_64 » was downloaded from

Here the last archive was

Extract the files to the folder C:\util\SNC\

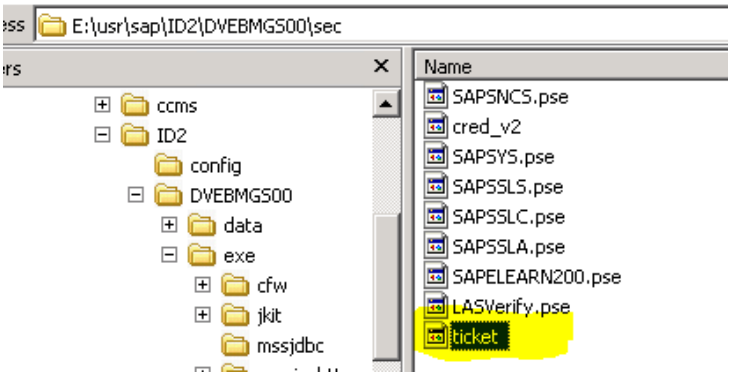


57.3. Copie of the « License ticket file »

©copyright 2014 AGENTIL – all rights reserved

If the license ticket file is not available within the crypto archive file, then you can get it from the “sec” folder of an ABAP instance running in SNC.

Example: E:\usr\sap\ID2\DVEBMGS00\sec



Then copy it to the SNC client folder « C:\util\SNC\sec ».

57.4. Setting the new variables

Two environment variables must be set for the SNC client application:

- SECUDIR=C:\util\SNC\sec
- PATH=%PATH%; C:\util\SNC

57.5. Creating the PSE of the SNC client

We use the SNC configuration scenario called « *Using Individual PSEs for Components* »,

Here we decided to use this Distinguish Name for the SNC client:

CN=SAME01, OU=AGL, O=AGL, C=CH

Start a Windows command on the host of the SNC client then execute:

>set SECUDIR=C:\util\SNC\sec
>set PATH=%PATH%; C:\util\SNC
>cd C:\util\SNC\sec
>..\sapgenpse gen_pse -v -p SAME01 -s 1024

Got absolute PSE path "C:\util\SNC\sec\SAME01.pse".
Please enter PIN: (**here enter a PIN password**)
Please reenter PIN:

©copyright 2014 AGENTIL – all rights reserved

get_pse: Distinguished name of PSE owner: **CN=SAME01, OU=AGL, O=AGL, C=CH**
Supplied distinguished name: "CN=SAME01, OU=AGL, O=AGL, C=CH"
Creating PSE with format v2 (default)
Generating key (RSA, 1024-bits) ... succeeded.
certificate creation... ok
PSE update... ok
PKRoot... ok
Generating certificate request... ok.
PKCS#10 certificate request for "C:\util\SNC\sec\SAME01.pse":

-----BEGIN CERTIFICATE REQUEST-----
MIIBeTCB4wIBADA6MQswCQYDVQQGEwJDSDEMMAoGA1UEChMDQUdMMQwwCgYDVQQL
EwNBR0wxDzANBgNVBAMTBlNBTUUwMTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEA/gdMIrzE4lEDVNaH8/kuodA5/8s/sIFAsqrEL1+BzT0I6xwMr9q1qTYmvplt
U0bqghQkwfWBTgVNL8Aep0rCBmMhfzXTsDn+Gxpk/Bwi9//fj4KgG1eshKZW42uN
+FB6vADyb2pO3s7StnIow8pR9z+XdXSO7Ts9d6Ah2fjXGhsCAwEAAaAAMA0GCSqG
SIb3DQEBBQUAA4GBAI7JNaOi+uynmLoH58BoExIhLKwi2Ks8SjfM9vj6oAOSiusO
5Cur8aobN9tEvXLT6d4P/B3qU68u29JOz5YXN2HHcolkOoeePrlxKfgotvoJG40b
RQ8Xqz2aEIrJJZfZ8YLeX6sSFQJhCQR3iyvuahTe6j9tXiHVWfWLErtgO+6C
-----END CERTIFICATE REQUEST-----

57.6. Creating the SNC client certificate

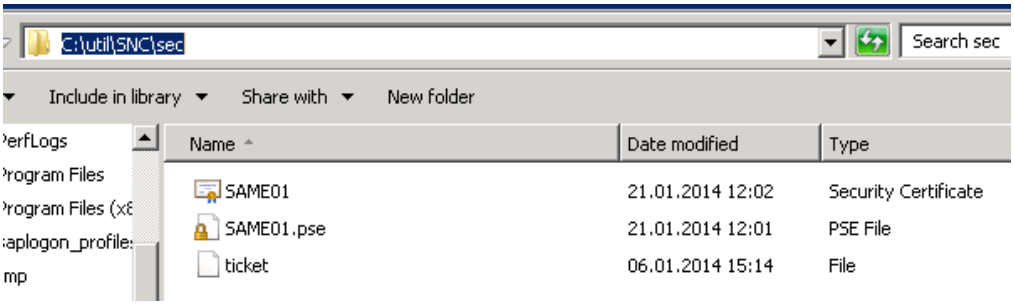
Start a Windows command on the host of the SNC client then execute:

>set SECUDIR=C:\util\SNC\sec
>set PATH=%PATH%; C:\util\SNC
>cd C:\util\SNC\sec
>..\sapgenpse export_own_cert -v -p SAME01.pse -o SAME01.crt

Opening PSE "C:\util\SNC\sec\SAME01.pse"...
No SSO credentials found for this PSE.
Please enter PIN: (**here enter the PIN password previously assigned**)
PSE (v2) open ok.
Retrieving my certificate... ok.
Writing to file (PEM-framed base64-encoded)... ok.

The file certificate “SAME01.crt” is created in the “sec” folder:

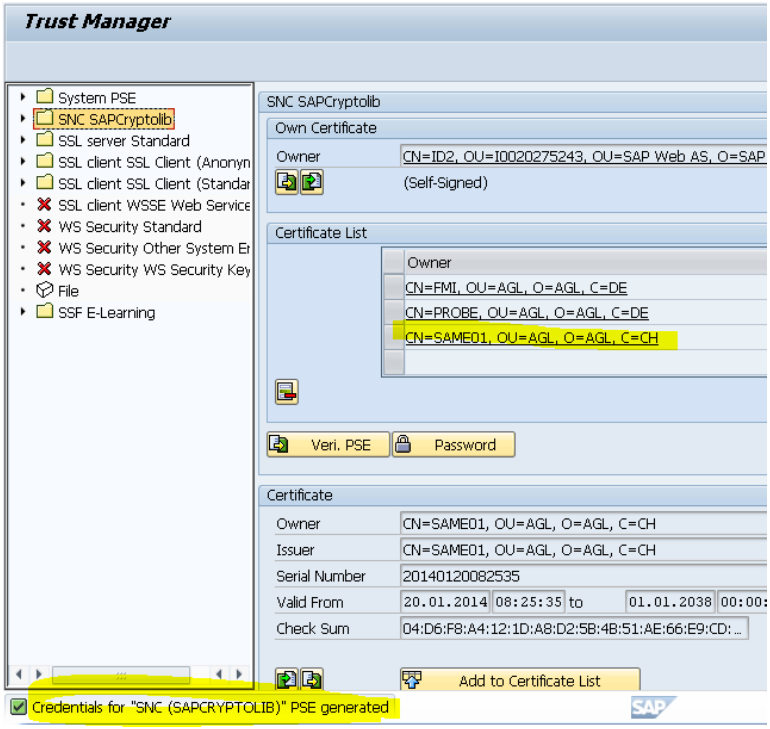
©copyright 2014 AGENTIL – all rights reserved



57.7. Importing of the client certificate in the SAP SNC server

In the SAP server, start the STRUST command to import the client certificate in the “SNC SAPCryptolib” PSE:

Example in a SAP instance with the previously created “SAME01.crt” certificate

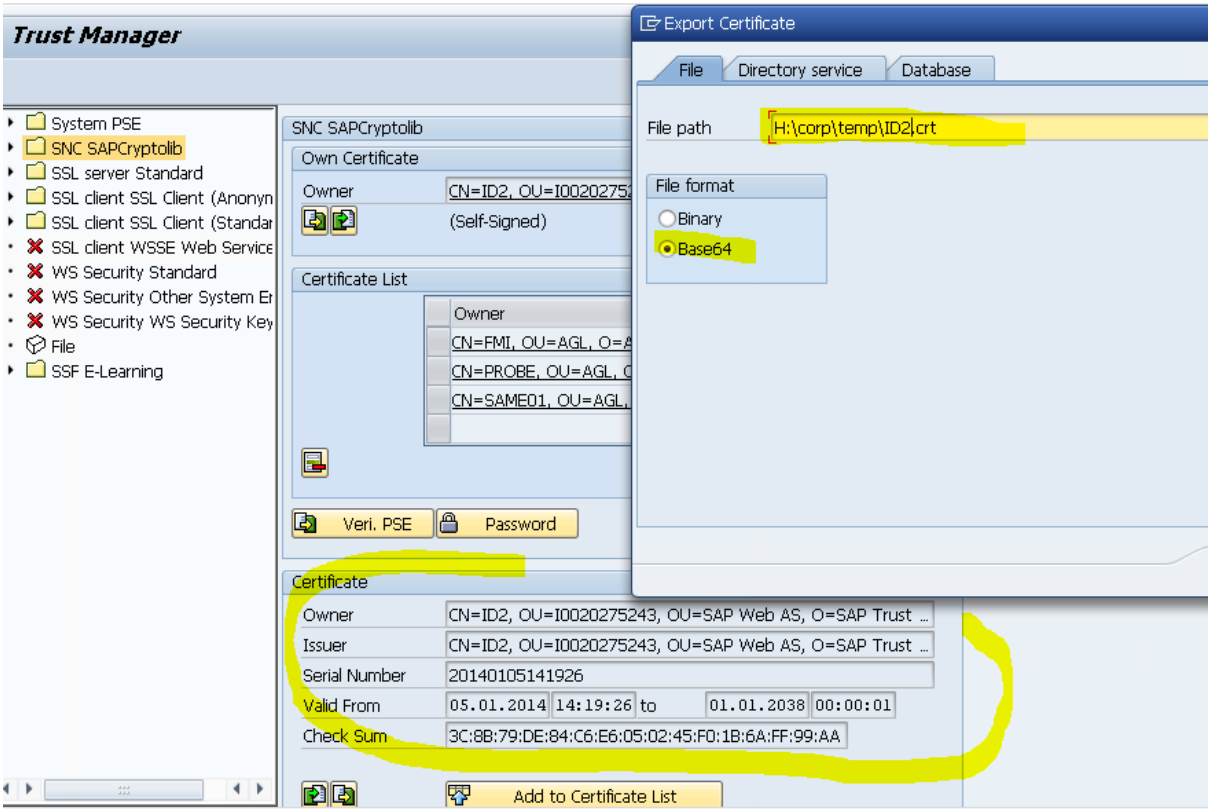


57.8. Exporting of the SAP SNC server certificate

In the SAP server, start the STRUST command to export the SAP server certificate from the “SNC SAPCryptolib” PSE:

Example on a SAP instance : export in “ID2.crt” file

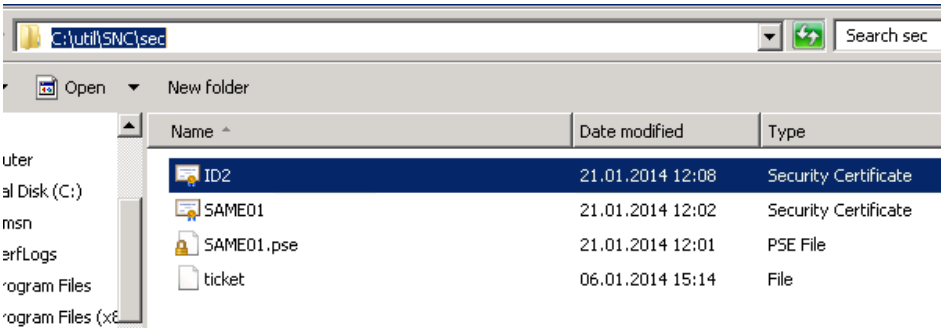
©copyright 2014 AGENTIL – all rights reserved



57.9. Importing of the SAP SNC server certificate

Copy the SAP certificate to the “sec” folder of the SNC client.

Here the example of “ID2.crt” file



Start a Windows command on the host of the SNC client then execute:

>set SECUDIR=C:\util\SNC\sec
>set PATH=%PATH%; C:\util\SNC

©copyright 2014 AGENTIL – all rights reserved

```
>cd C:\util\SNC\sec
>..\sapgenpse maintain_pk -v -a ID2.crt -p SAME01.pse
Opening PSE "C:\util\SNC\sec\SAME01.pse"...
No SSO credentials found for this PSE.
Please enter PIN:                    (enter the PIN password you created previously)
PSE (v2) open ok.
retrieving PKList
Adding new certificate from file "ID2.crt"
----------
Subject : CN=ID2, OU=I0020275243, OU=SAP Web AS, O=SAP Trust Community, C=DE
Issuer  : CN=ID2, OU=I0020275243, OU=SAP Web AS, O=SAP Trust Community, C=DE
Serialno: 20:14:01:05:14:19:26
KeyInfo : RSA, 1024-bit
Validity  -  NotBefore:   Sun Jan 05 15:19:26 2014 (140105141926Z)

          NotAfter:   Fri Jan 01 01:00:01 2038 (380101000001Z)
------------------------------------------------------------------------------

 PKList updated (1 entries total, 1 newly added)
```

©copyright 2014 AGENTIL – all rights reserved

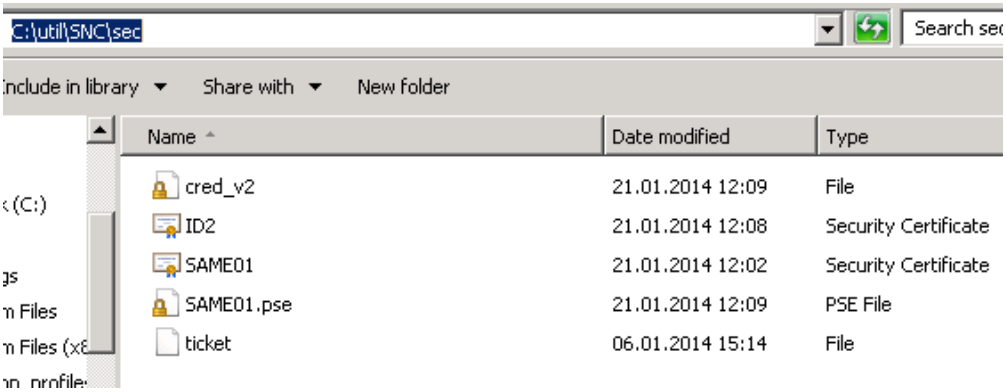
57.10. Creating the credential file for the SNC client user account

You have to allow the OS account of the SNC client application to access the PSE, by creating the credential file “cred_v2”.

Here the example for the user accound “SYSTEM” on the SAME01 PSE

set SECUDIR=C:\util\SNC\sec
set PATH=%PATH%; C:\util\SNC
cd C:\util\SNC\sec
..\sapgenpse seclogin -p SAME01.pse -O SYSTEM
running seclogin with USER="fls"
creating credentials for well-known group "NT AUTHORITY\SYSTEM" ...
Please enter PIN: (**enter the PIN password you created previously**)
Adjusting credentials and PSE ACLs to include "NT AUTHORITY\SYSTEM"...
C:\util\SNC\sec\cred_v2 ... ok.
C:\util\SNC\sec\SAME01.pse ... ok.
Added SSO-credentials (#0) for PSE "C:\util\SNC\sec\SAME01.pse"
"CN=SAME01, OU=AGL, O=AGL, C=CH"

The file “cred_v2” is created in the “sec” folder

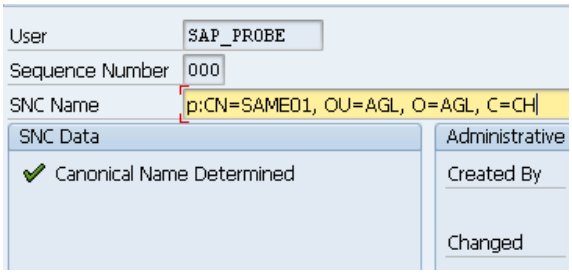


©copyright 2014 AGENTIL – all rights reserved

57.11. Define the SNC client user in the USRACLEXT SAP table

In the SAP SNC server, run the SM30 transaction to add the SNC client user and its Distinguished Name. Be carefull, the table is client dependant.

Here the example for the user “SAP_PROBE” in client 000 with “p:CN=SAME01, OU=AGL, O=AGL, C=CH”.



57.12. Setting the SNC in the client JCO connection

The JCO connection must be defined with 3 SNC parameters:

jco.client.snc_mode=1

jco.client.snc_partnername= <DN of the SAP SNC server>

jco.client.snc_myname= <DN of the SNC client>

jco.client.snc_lib= <full path of the sapcryptolib library file>

Here for example with ID2 SAP system and SAME01:

jco.client.snc_mode=1
jco.client.snc_partnername= p:CN=ID2, OU=I0020275243, OU=SAP Web AS, O=SAP Trust Community, C=DE
jco.client.snc_myname=p:CN=SAME01, OU=AGL, O=AGL, C=CH
jco.client.snc_lib= C:\util\SNC\sapcrypto.dll

58. UMP dashboards generation

The probe gives the possibility to generate preconfigured SAP dashboard files that you can import in the Unified Monitoring Portal.

©copyright 2014 AGENTIL – all rights reserved

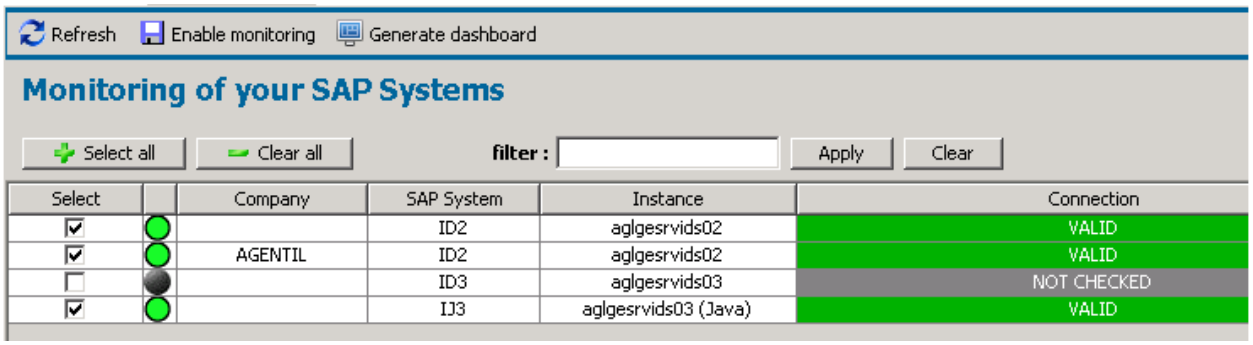
58.1. QOS ids definition

Before generating any dashboard, you need to configure the probe so it can discover the QOS ids of the metrics going to be used in the dashboards. You can either define a connection to the data engine and the discovery will be automatic, or you can register each QOS ids manually.

See QOS ids paragraph in the setup section of this document.

58.2. Generate and import dashboards

From the “My SAP monitoring” tag, select the “SAP systems” root in the left panel tree. Click on the Monitoring tab: It will show the list of available systems.



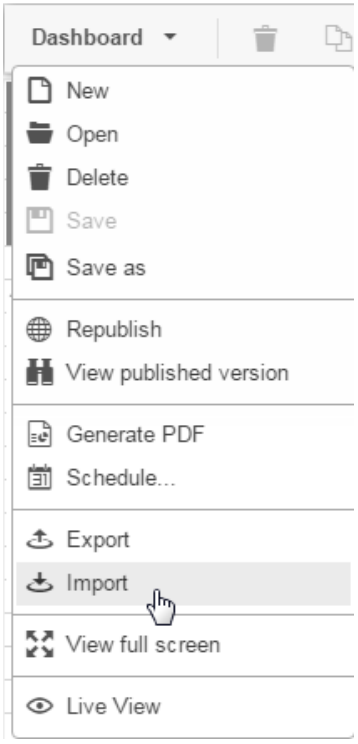
You can select the systems for which you want to create dashboards and then click on the “Generate Dashboard” button.

The probe will ask you to select the folder where you want the files to be created.

Now you are ready to import the dashboard files in the UMP. Log in the UMP web portal and open a dashboard editor (HTML5 version).

From the menu, press on the import button:

©copyright 2014 AGENTIL – all rights reserved



Then press on import dashboard file and select the file to import. The dashboard will now be available for edition in the Dashboard designer. You can modify it or add new items.

Once you have finished with dashboard edition, don't forget to publish it vie the "publish button", then your dashboard will be available through the CustomDashboard interface (see UMP documentation).

58.3. System dashboard

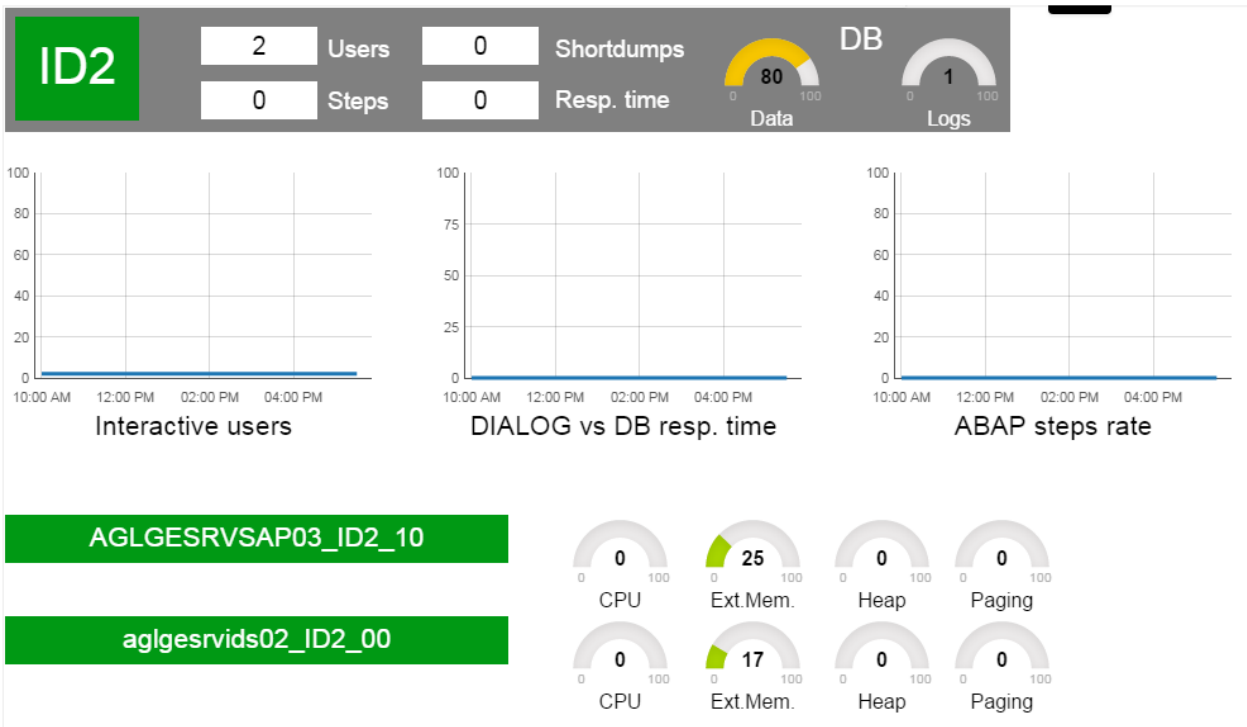
The system dashboard is composed by several screens allowing to drill down. The main screen will display a summary of monitored SAP systems.

Details for each system will be displayed in a row: Instances and Update state, Number of users, steps rate, short dumps, response times and database:

	Instances	Updates	Users	ABAP steps rate	Shortdumps	Response times (ms) DIALOG	UPDATES	SPOOL	DB usage DATA	LOG
ID2			2	0	0	0	0	5	80	1
ID3			NaN	0	NaN	NaN	NaN	NaN	0	0
SSM			0	1	0	3	0	0	100	59

If you click on the system SID, it will drill down the system dashboard:

©copyright 2014 AGENTIL – all rights reserved



It displays a system specific dashboard.

You can use the all the dashboards as they are, or customize them with your own elements.

58.4. Default dashboards customization

If you want to generate dashboards customized according to your taste, this is possible. However, you will need to understand some of the definition principles and format.

The definition is contained in a set of json files located in the *UMP/html5* folder of the probe engine:

- **landscapeDashboard.json**: Defines the dashboards showing SAP landscape overview.

- **systemDashboard.json**: Defines the system dashboard overview.

- **widgets** folder: Contains the definition of the widgets used by dashboard definition files

- **canvas**: Contains the definition of default dashboard canvas

- **datasources**: Contains the definition of the dashboard data sources

58.4.1. Principle:

If you want to replace a metric by another, you simply need to change the QOS name in the DATASOURCE section of the widget used to display the metric (And the label widget associated)

If you want to add a new metric, use the same definition pattern than existing metric's widget. Will then only need to set new widget coordinates and DATASOURCE.

©copyright 2014 AGENTIL – all rights reserved

You can even create your own custom widgets (to put in widgets folder) and use it in the dashboard definition files.

We acknowledge that it is not a trivial mechanism and requests some experience on using json format. Don't hesitate to contact Agentil for getting help, or to share your creation.

59. Troubleshooting

59.1. Installation

59.1.1. 32 bits Java runtime environment installed on a 64 bits system

When starting the probe, the following message is displayed:
java.lang.UnsatisfiedLinkError: D:\path\application\sapbasis_agentil\sapjco3.dll: Can't load AMD 64-bit .dll on a IA 32

Prerequisite:

- Your probe is installed on a windows 64 bits system and your Java JRE is a 32 bits version (it is installed in the C:\program Files

Solution:

- Download and install a 64 bits Java JRE version.

59.2. Instances availability

If you get those alarms below, this is because you should configure at least one operation mode in the RZ04 transaction:

[*SID*][ALARM][ABAP Instances availability] Error : Fail to get SAP data : No TIDS matching CCMS path "System Configuration\Instance Status*\Status"
[*SID*][QOS][ABAP Instances availability] Error : Fail to get SAP data : No TIDS matching CCMS path "System Configuration\Instance Status*\Status"

Wait until the CCMS update the tree and wait also that the probe update this own data tree.

.

59.3. License problems

59.3.1. No license found in GUI

Symptom:

You have installed the license in UIM, but when you start the GUI, you see the message "No license found" in the license section, and you can't see any configuration data.

Problem:

©copyright 2014 AGENTIL – all rights reserved

There is a communication issue between the probe and the GUI. The message concerning the license is misleading and irrelevant (old version).

Solution: Check the troubleshooting for probe to GUI connection issues

59.4. Probe to GUI connection failure

Symptom:

When starting the GUI, it does not seem to connect to the engine and does not load configuration data.

Problem:

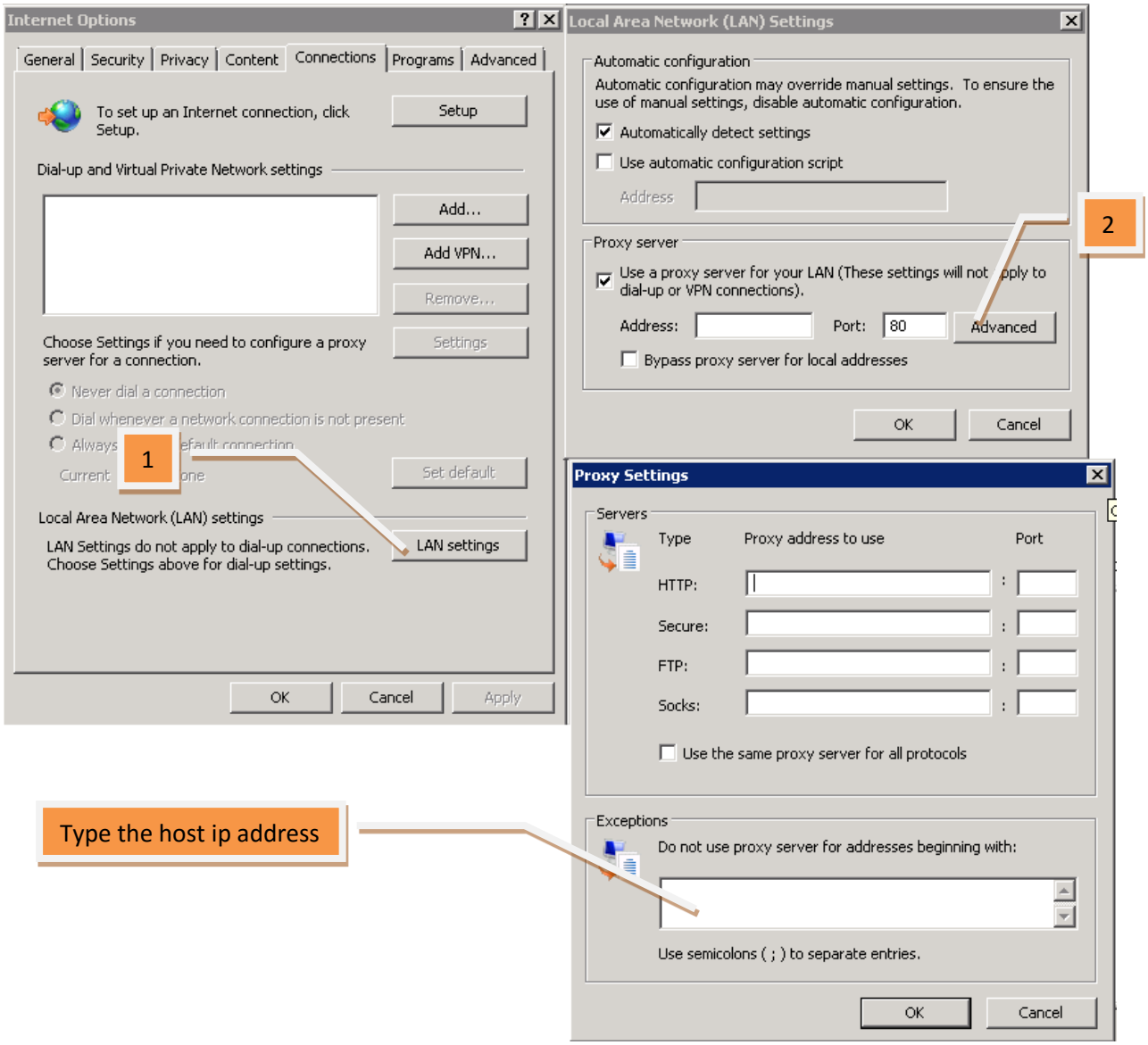
If you are using a proxy server, the GUI might have troubles to connect to the probe engine.

Solution1:

This situation can be solved by declaring the host running the GUI in the exceptions list of the proxy configuration.

This is located in you internet explorer, in Tools->Internet Options->Connections->Lan settings->Advanced

©copyright 2014 AGENTIL – all rights reserved



Solution2:

Former versions of the probe had a bug making impossible for the GUI to connect to the engine from a distant robot: Start the GUI from the same robot where is running the probe, or upgrade the probe version to the latest one (**fixed in V2.0 in February 2012**)

59.1. Alarm/QOS not received in UIM

Symptom:

You are in a condition where you expect Alarms and QOS to be received in UIM, but it seems that some are missing.

©copyright 2014 AGENTIL – all rights reserved

In the log file, you can see the following socket error: "**Address already in use**"

Problem:

The number of parallel connections that the probe can open is limited by the OS.

Solution:

Increase the number of parallel connections in windows, following this procedure:

Ephemeral Ports

The maximum value of an ephemeral TCP or UDP port number that is assigned by Windows Sockets in Microsoft Windows XP or Windows Server 2003 to an application is controlled by the MaxUserPort registry setting, which has a default value of 5000. Ephemeral ports begin with port number 1025. Therefore, by default, Windows XP or Windows Server 2003 assigns an application that performs a wildcard bind a number from 1025 to 5000.

To change the maximum value for ephemeral ports on a computer running Windows XP or Windows Server 2003, do the following:

1. Click **Start**, click **Run**, type **regedit.exe**, and then click **OK**.
2. Locate and then click the following registry subkey:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
3. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
4. Type **MaxUserPort** and then press ENTER.
5. Double-click the **MaxUserPort** value, and then type the maximum value in decimal or hexadecimal.

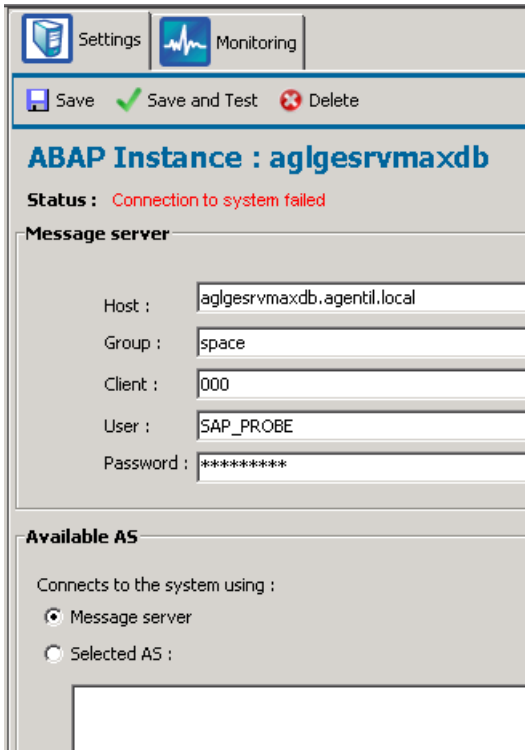
   You must type a number in the range of 500065534 (decimal). Setting this parameter to a value outside of the valid range causes the nearest valid value to be used (5000 or 65534).
6. Click **OK**.
7. Quit Registry Editor.

59.2. Connection is not working

Symptom:

The message server connection to a SAP system does not work.

©copyright 2014 AGENTIL – all rights reserved

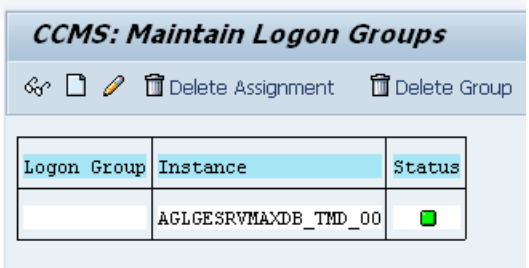


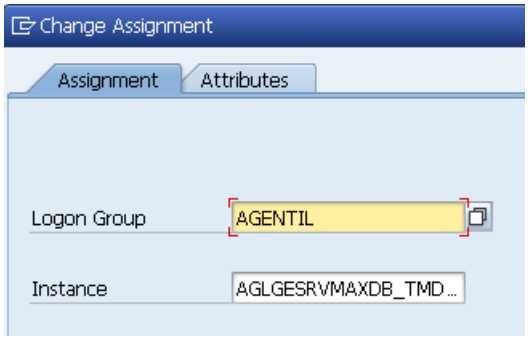
Problem:

The logon group configured in the probe does not exist in SAP

Solution:

Create the missing logon group with the transaction MSLG





59.3. The probe doesn't seem to start

Symptom:

The probe status is red in the infrastructure manager.

No java process containing "SAME.jar" in the command line is running.

©copyright 2014 AGENTIL – all rights reserved

Problem:

The probe might have a library or compatibility issue with the current OS settings.

Solution:

Open a cmd.exe and go the probe root folder, then launch the probe manually by running sapbasis_agentil_starter.exe.

You will see the execution stack of the probe. If you see the following exception:

©copyright 2014 AGENTIL – all rights reserved

The problem is an incompatibility between the Microsoft VC++ redistributable package needed by the probe and the ones installed.

You need to uninstall all packages and leave the one recommended in the prerequisites section.

59.4. Monitoring – SAP configuration compliance

59.4.1. CCMS path not found

Symptom:

Alarms starting by "**CCMS path not found**" are received in UIM, or in the CCMS error console.

Problem 1:

In this case, the probe tries to fetch an entry in the CCMS, but the entry does not exist.

Solution 1:

The SAP administrator must investigate why the entry is not present in the CCMS. This is a case by case investigation. As an example, a common issue is described in the "Instances availability" section

Problem 2:

The entry in the CCMS has just been created and the probe had no time to detect it. The probe refreshes its CCMS structure image once per hour.

Solution 2:

Force the refresh of the CCMS from the GUI, or increase the refresh rate (only if very necessary, because consumes memory and CPU)

59.4.2. CCMS entry "DB KPIs …" not present

Symptom:

If you get one of those alarms below:

```
Error :  Fail to get SAP data  : No TIDS matching CCMS path  "DB KPIs Microsoft SQL Server\*\Daily Growth"
Error :  Fail to get SAP data  : No TIDS matching CCMS path  "DB KPIs Oracle\*\Daily Growth"
Error :  Fail to get SAP data  : No TIDS matching CCMS path  "DB KPIs DB2 for Linux, UNIX, Windows\*\Daily Growth"
```

Problem:

The below CCMS entries are not present :

- DB KPIs Microsoft SQL Server
- DB KPIs Oracle
- DB KPIs DB2 for Linux, UNIX, Windows

©copyright 2014 AGENTIL – all rights reserved

Solution:

The existence of those values depend of the SAP version and the SAP Basis customizing. If applicable, run the SAP report RSDBKPIMON with SA38.

Warning: in case running the report RSDBKPIMON doesn't create the DB Kpis tree, please look at the SAP note 1298207

59.4.3. CCMS entry for Database not present

Symptom:

If you get one of those alarms below:

Error : Fail to get SAP data : No TIDS matching CCMS path "Microsoft SQL Server\ "
Error : Fail to get SAP data : No TIDS matching CCMS path "Oracle\..."
Error : Fail to get SAP data : No TIDS matching CCMS path "DB2 Universal Database for NT/UNIX\..."

Problem:
The below CCMS entries are not present :

- Microsoft SQL Server\...
- Oracle\...
- DB2 for Linux, UNIX, Windows\...

Solution:

The existence of those values depend of the SAP version and the SAP Basis customizing. If applicable, run the SAP report RSDBMON0 with SA38.

59.4.4. Instances availability

Symptom:

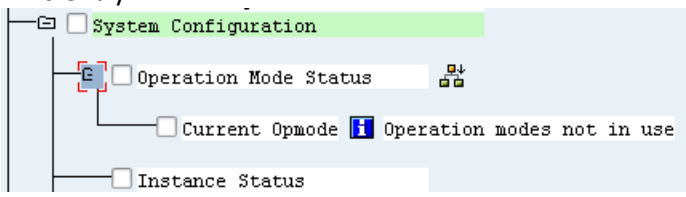
If you get those alarms below:

[*SID*][ALARM][ABAP Instances availability] Error : Fail to get SAP data : No TIDS matching CCMS path "System Configuration\Instance Status*\Status"
[*SID*][QOS][ABAP Instances availability] Error : Fail to get SAP data : No TIDS matching CCMS path "System Configuration\Instance Status*\Status"

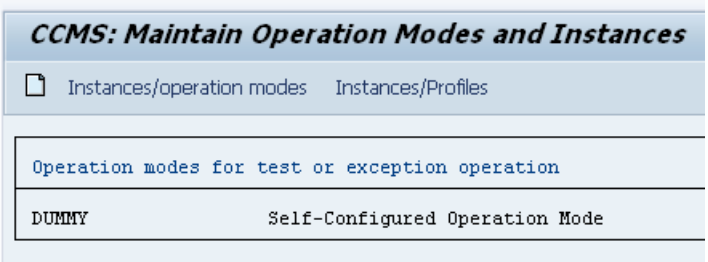
Problem:

©copyright 2014 AGENTIL – all rights reserved

No operation modes have been configured in the RZ04 transaction
RZ20 entry :

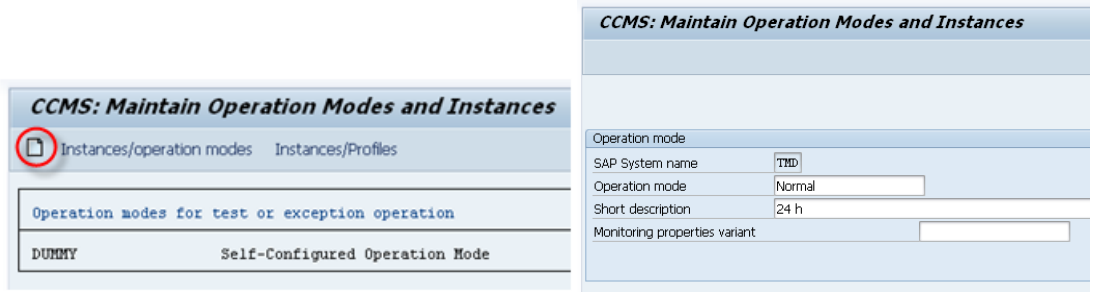


RZ04 :

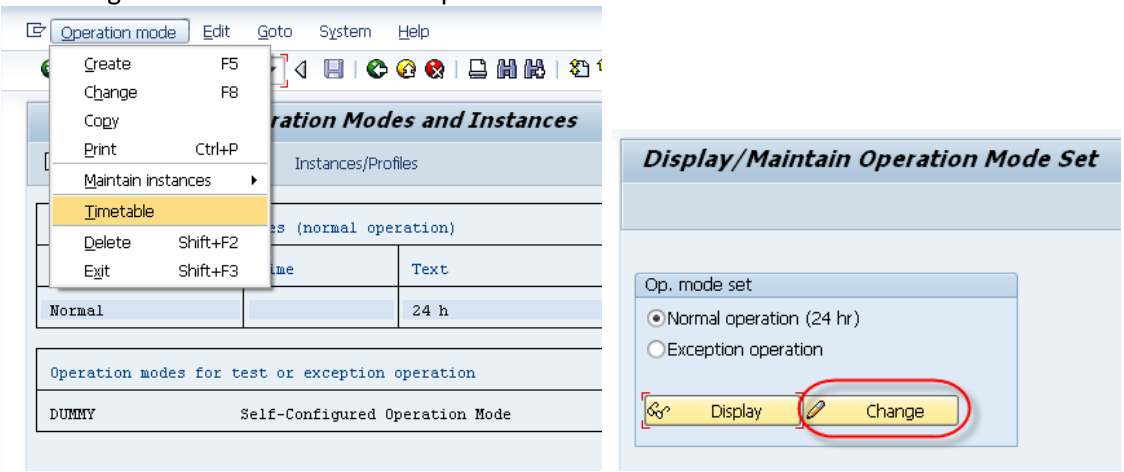


<u>Solution:</u>

Configure at least one operation mode in the RZ04 transaction.

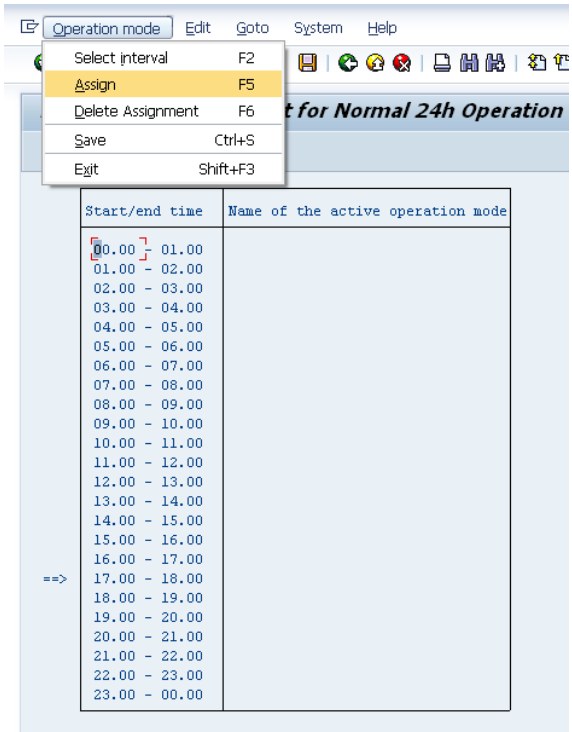


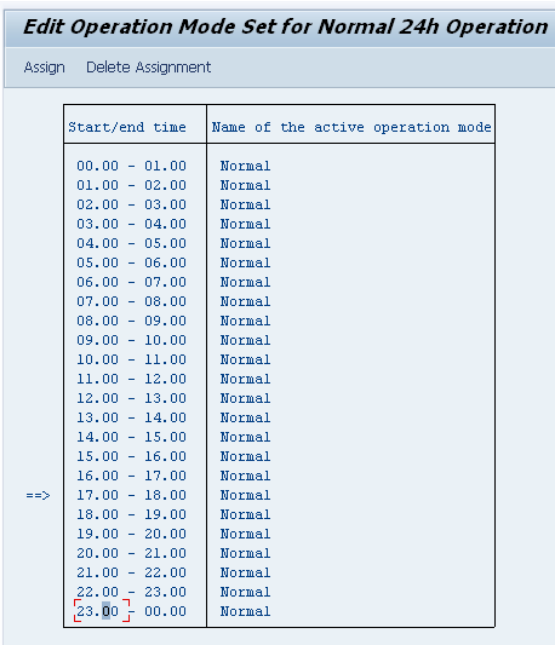
Then assign a timetable to this new operation mode “Normal”:



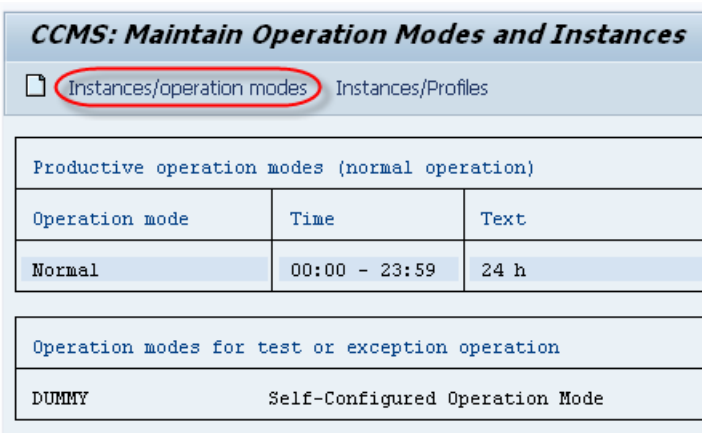
Select the first line, press F2. Select the last line, press F2. Assign with F5:

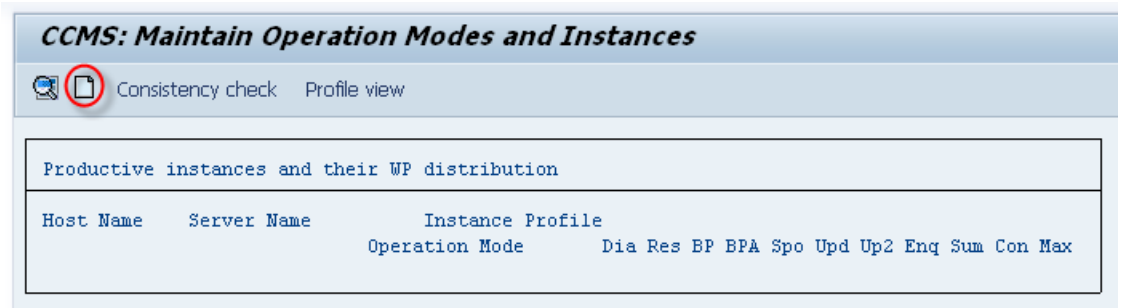
©copyright 2014 AGENTIL – all rights reserved





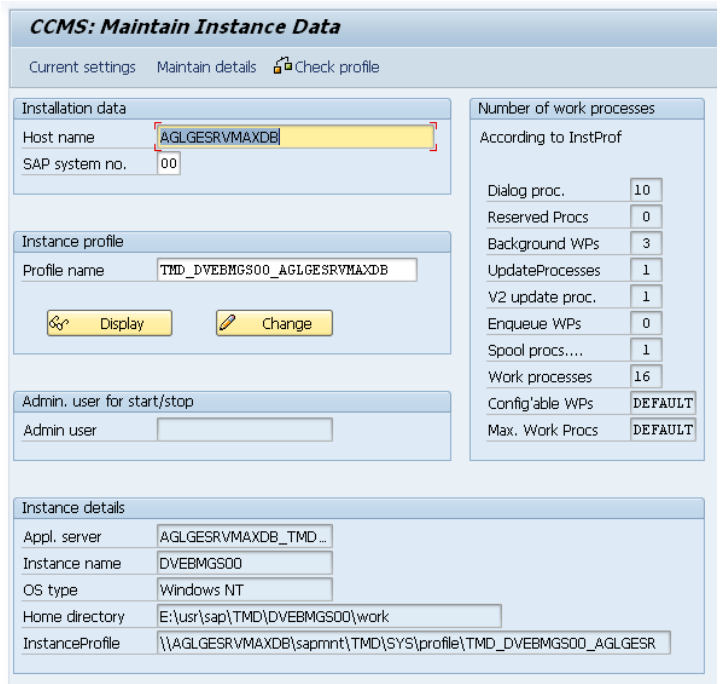
Assign this new operation mode to an instance:



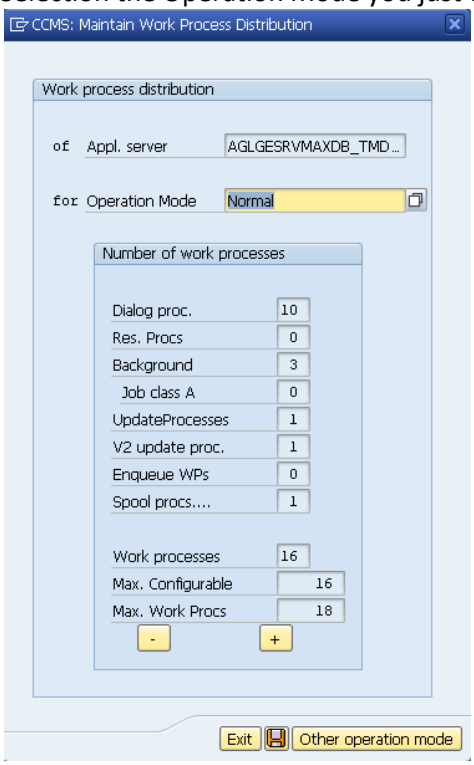


Set the host name and select the profile, then save:

©copyright 2014 AGENTIL – all rights reserved



Selection the Operation Mode you just created:



Your get this. Save.

©copyright 2014 AGENTIL – all rights reserved

CCMS: Maintain Operation Modes and Instances

Consistency check Profile view

Productive instances and their WP distribution

Host Name	Server Name	Instance Profile Operation Mode	Dia	Res	BP	BPA	Spo	Upd	Up2	Enq	Sum	Con	Max
AGLGESRVMAXD	AGLGESRVMAXDB_TMD_00	TMD_DVEBMGS00_AGLGESRVMAXDB Normal	10	-	3	-	1	1	1	-	16	16	18

Check in “Instances/Profiles” :

CCMS: Maintain Operation Modes and Instances

Instances/operation modes Instances/Profiles

Productive operation modes (normal operation)

Operation mode	Time	Text
Normal	00:00 - 23:59	24 h

Operation modes for test or exception operation

DUMMY	Self-Configured Operation Mode

You get this :

CCMS: Maintain Operation Modes and Instances

Change profile Display profile Consistency check Operation mode view

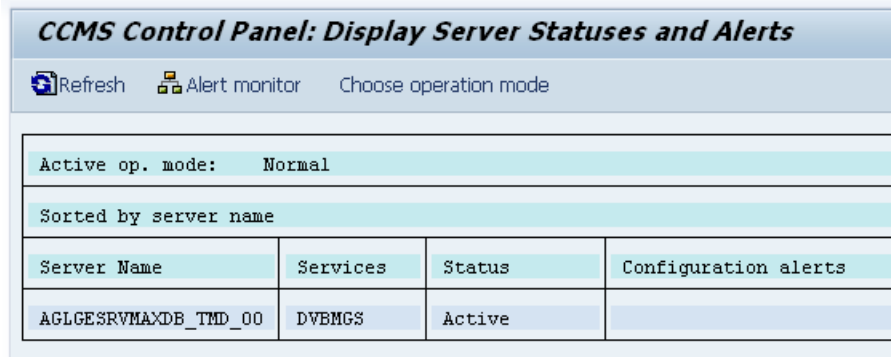
Productive instances with profiles from syst. TMD

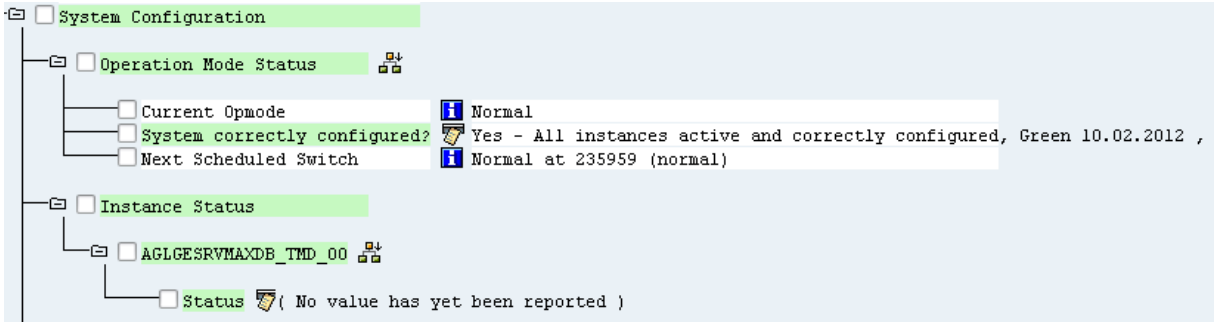
Default prof.
DEFAULT Activated: \\AGLGESRVMAXDB\sapmnt\TMD\SYS\profile\DEFAULT

Server name	Instance prof.
AGLGESRVMAXDB_TMD_00	TMD_DVEBMGS00_AGLGESRVMAXDB

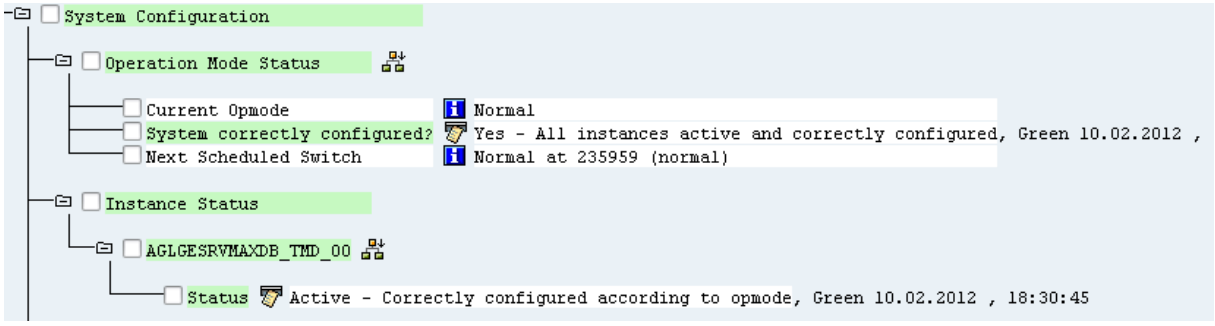
In RZ03 all is fine :

©copyright 2014 AGENTIL – all rights reserved





Wait until the CCMS updates the tree (default is 240 seconds). The Operation Mode Status & the Instance Status are correct:



Wait also that the probe update this own data tree or force it.

59.4.5. Irrelevant monitoring data

Symptom:

The data collected from the probe does not seem to match with reality.

Problem:

The probe highly relies on the CCMS. If it contains irrelevant values, it will be collected by the probe and potentially generate false alarms and wrong QOS

Solution:

©copyright 2014 AGENTIL – all rights reserved

Make sure that the data in the CCMS relevant and correctly updated.

In the RZ20 transaction, the following method can force the refresh of a part of the tree:

59.4.6. Old CCMS entries

Symptom:

This alarm are generated :

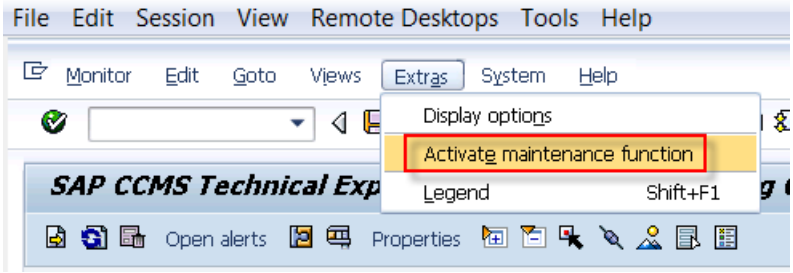
"Application server xxxxxxx_SID_NN is not active or the status not consistant with the operation modes configuration."

Problem:
After a system copy, the CCMS source entries are still present.

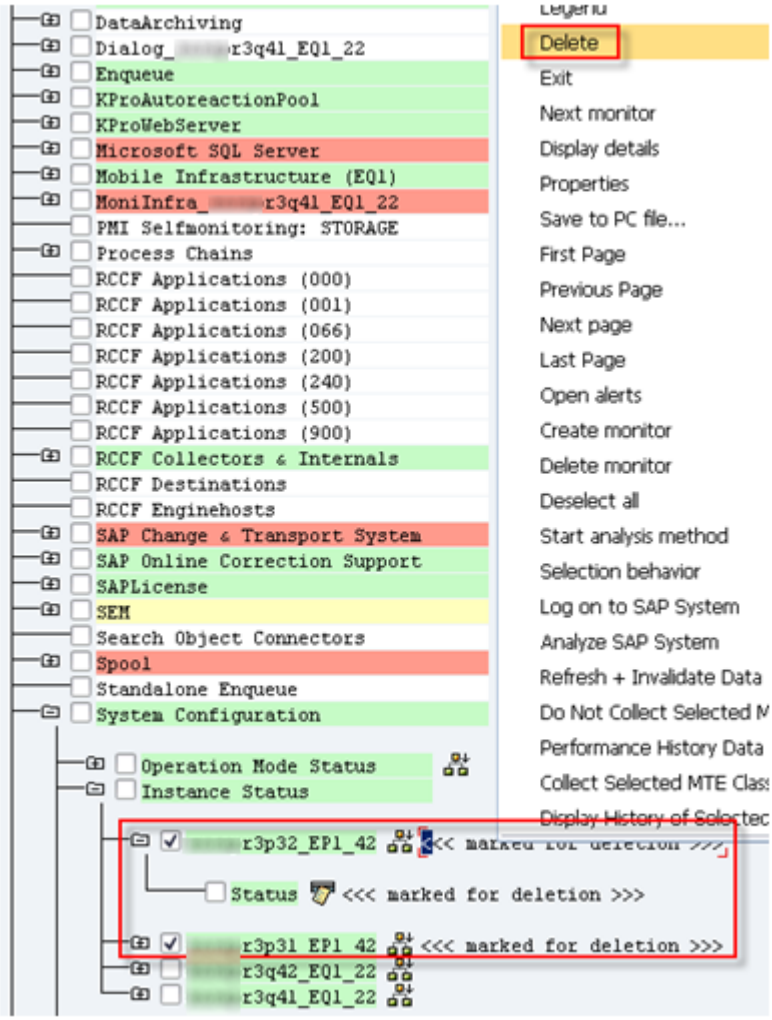
Solution:

You can delete old entries in RZ20 with this procedure:

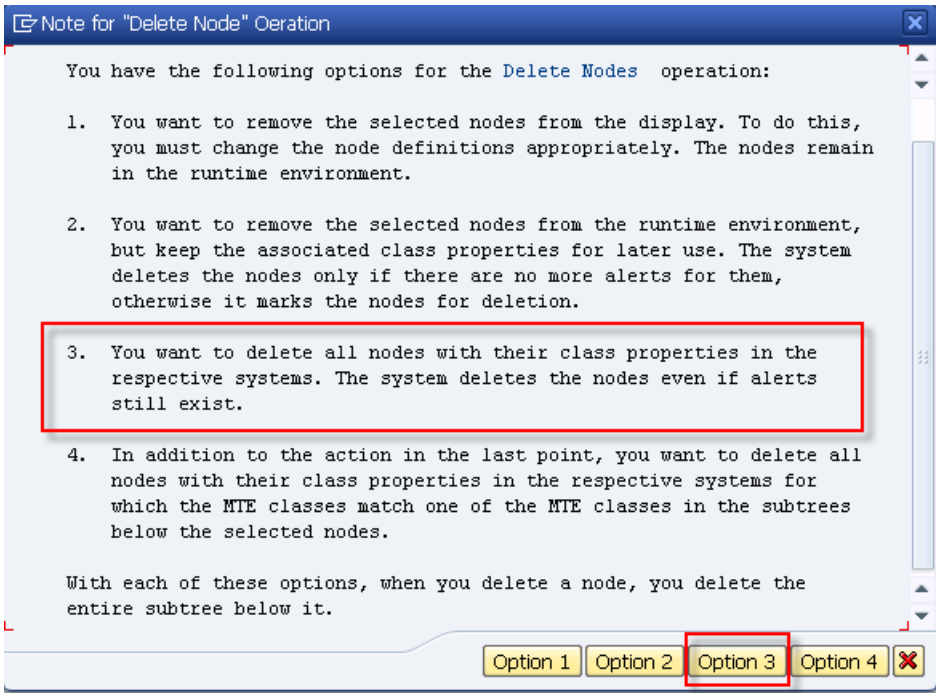
©copyright 2014 AGENTIL – all rights reserved



©copyright 2014 AGENTIL – all rights reserved

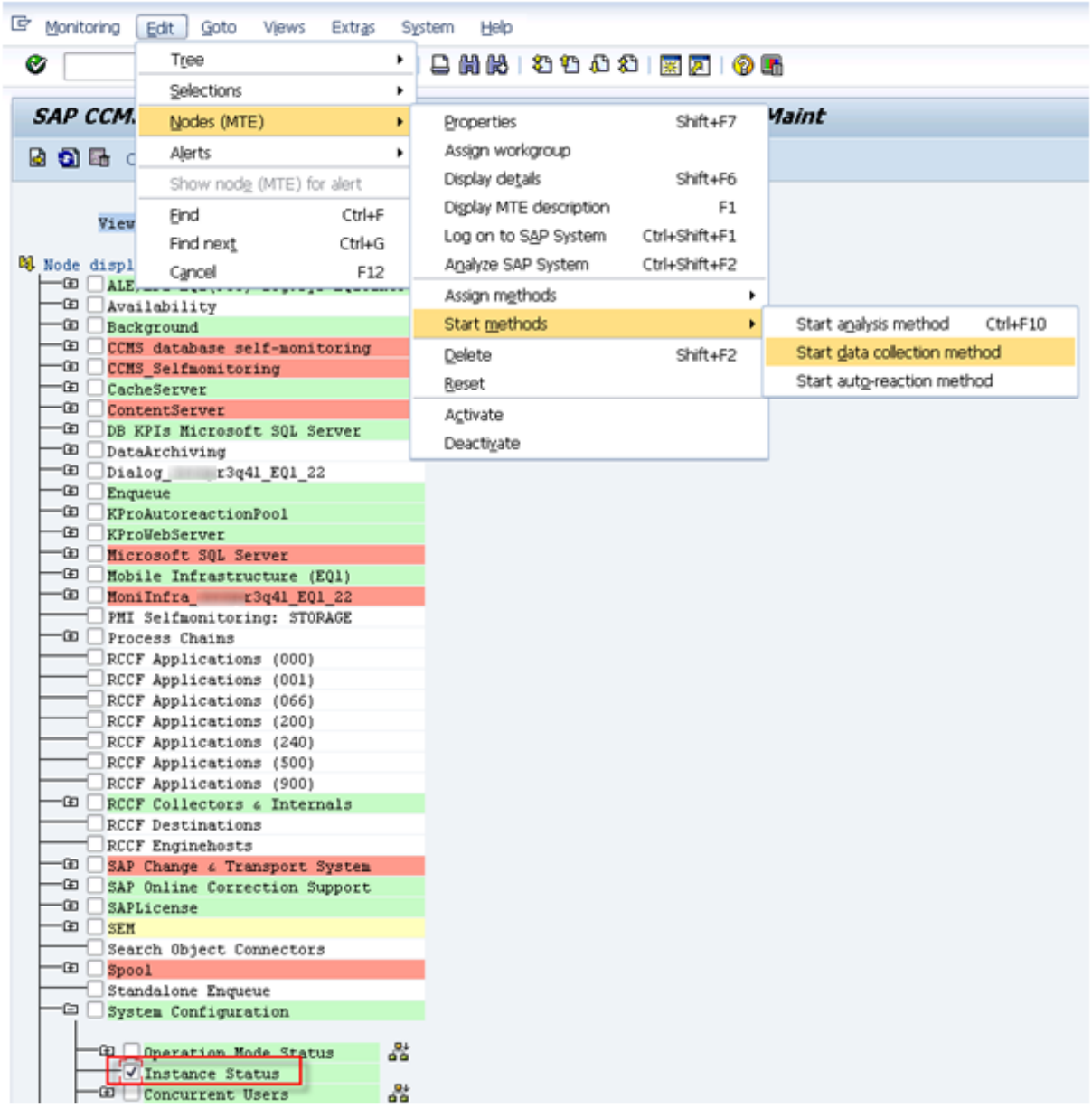


©copyright 2014 AGENTIL – all rights reserved



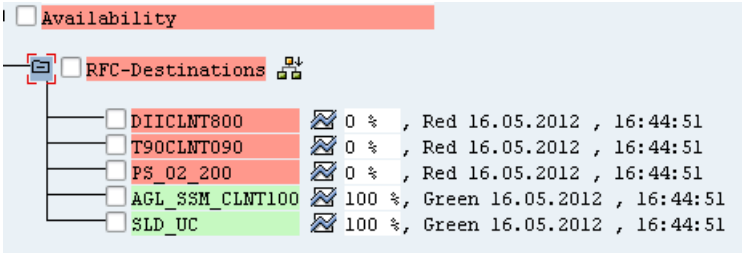
©copyright 2014 AGENTIL – all rights reserved

After that all entries in « Instance Status » is empty. You can recreate the good entries doing this :



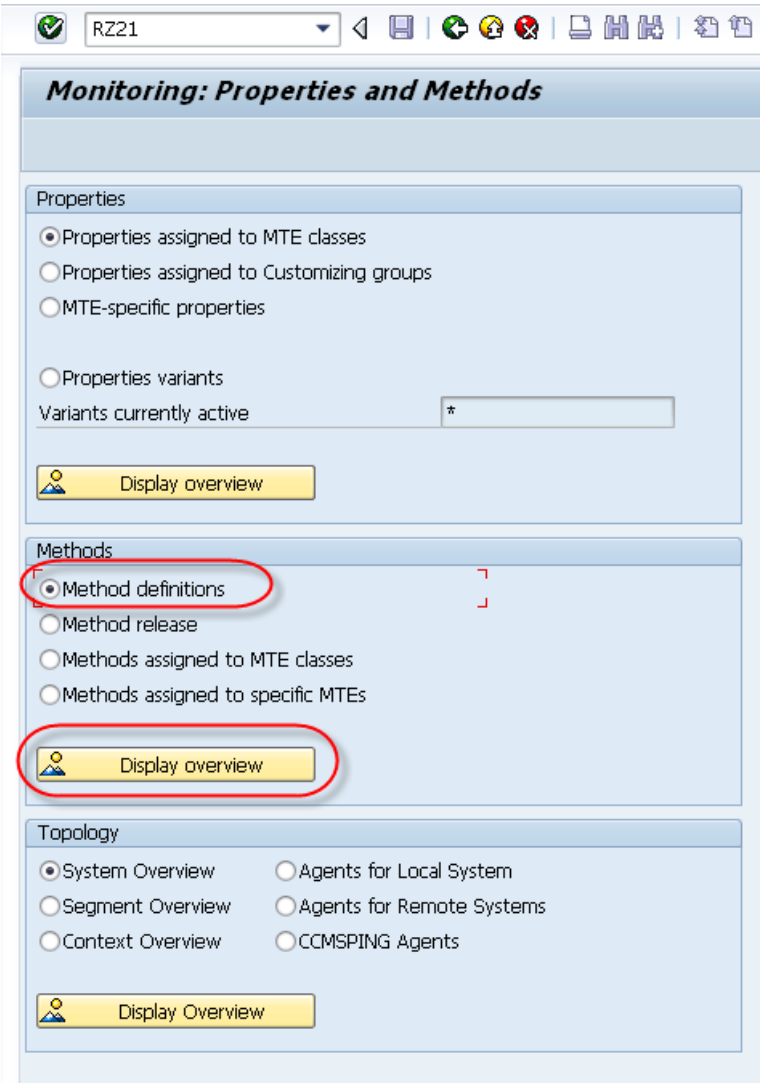
59.4.1. RFC destination monitoring:

Here is the procedure to create CCMS entries needed to monitor RFC Destinations Availability like below :

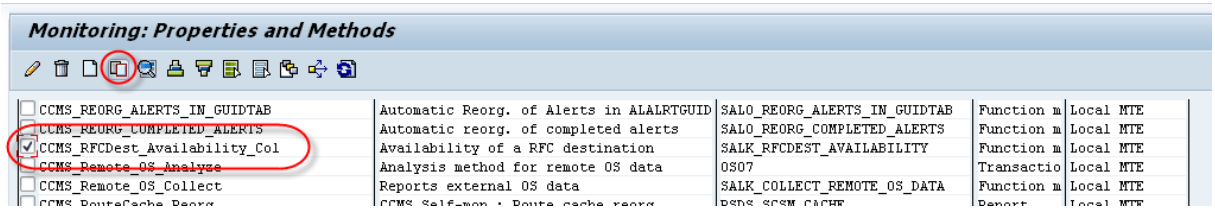


©copyright 2014 AGENTIL – all rights reserved

Run RZ21 transaction :

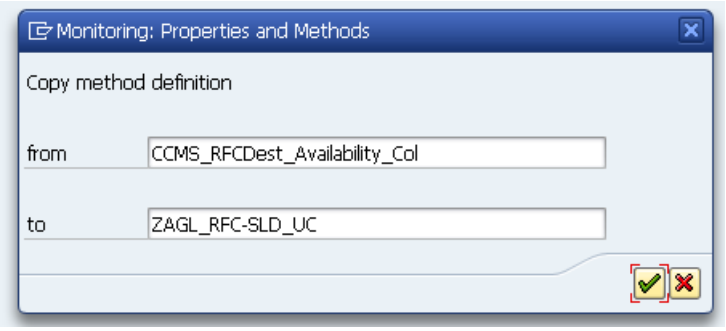


Copy the method CCMS_RFCDest_Availability_Col :



Put a Z* name with the RFC name at the end (or any naming convention you want) :

©copyright 2014 AGENTIL – all rights reserved



Set all those options :

©copyright 2014 AGENTIL – all rights reserved

Monitoring: Methods

Method definition

Name: ZAGL_RFC-SLD_UC

Description: Availability of RFC SLD_UC (Langua

Execution | Control | Parameters | Release | Addnl info

To be executed

Type of call

- ○ Report
- ○ URL
- ◉ Function module
- ○ Logical command
- ○ Transaction

Call: SALK_RFCDEST_AVAILABILITY

Execute method on

- ○ Any server
- ◉ The local server of the MTE to be processed
- ○ Specified RFC destination

Execute method for

- ◉ Individual MTE
- ○ Table of several MTEs

Method definition

Name: ZAGL_RFC-SLD_UC

Description: Availability of a RFC destination

Execution | Control | Parameters | Release | Addnl i

Execute method

- ◉ Periodically in dialog process (short-running program)
- ○ Periodically in background process (as job)
- ○ Only in central system, triggered by CCMS agents
- ○ Manually executable only

Startup method

- ☑ Execute method immediately after monitoring segment start

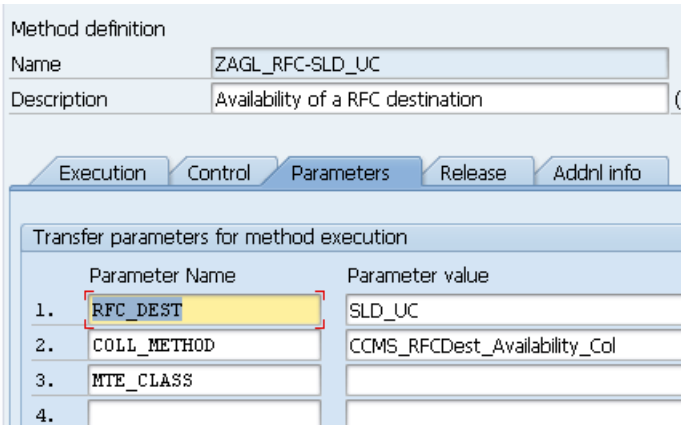
Execution location of startup method

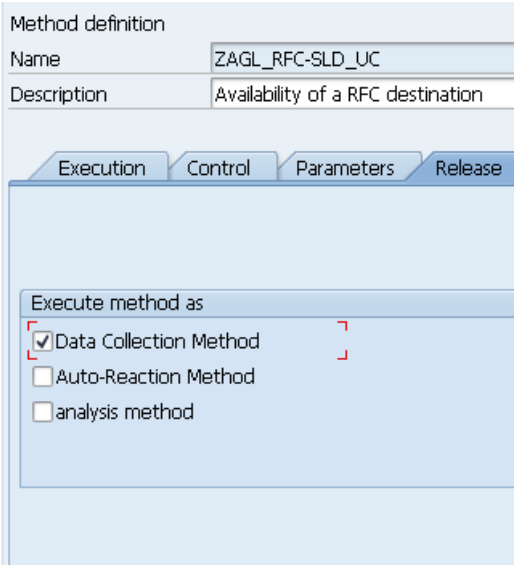
(Can only be selected for dialog execution)

- ○ On all application servers
- ◉ Only Once per System

©copyright 2014 AGENTIL – all rights reserved

Put the RFC name here :

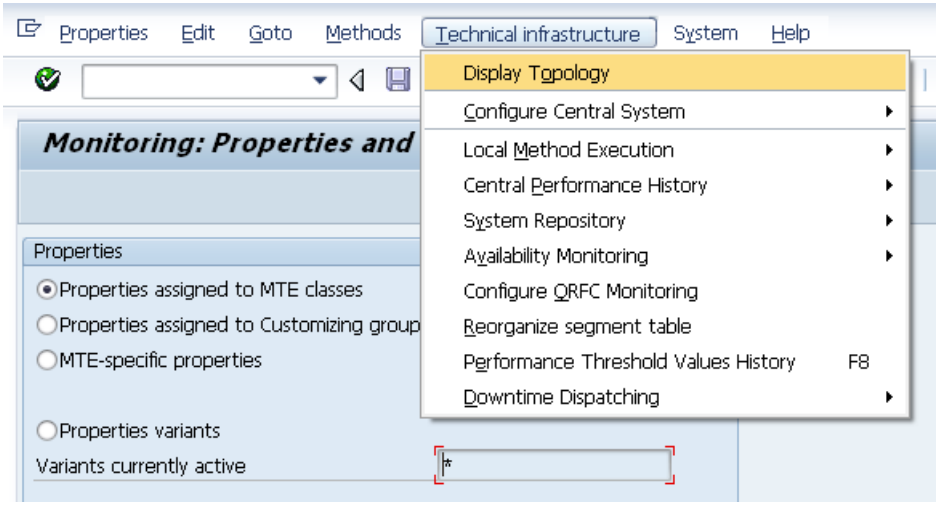




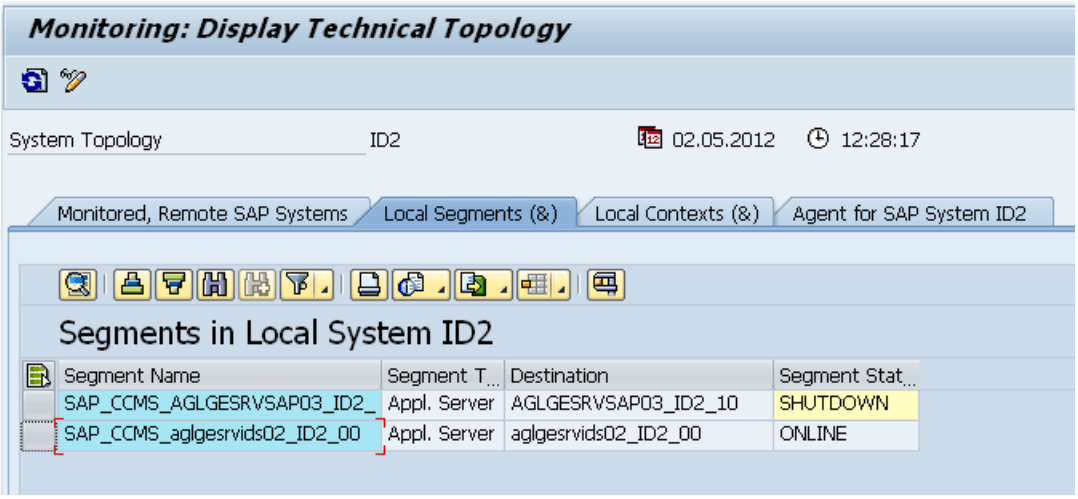
Go back to the previous list and refresh it. Here are 3 examples of new methods :

Z_RFC_ACE	Availability of a RFC ACE	SALK_RFCDEST_AVAILABILITY	Function m	Local MTE
Z_RFC_EHS_EXPERT	Availability of a RFC EHS_EXPERT	SALK_RFCDEST_AVAILABILITY	Function m	Local MTE
Z_RFC_SEEBURGER	Availability of a RFC SEEBURGER	SALK_RFCDEST_AVAILABILITY	Function m	Local MTE
Z_RFC_WWISERVER_EP1_200	Availability of a RFC WWISERVER_EP1_200	SALK_RFCDEST_AVAILABILITY	Function m	Local MTE

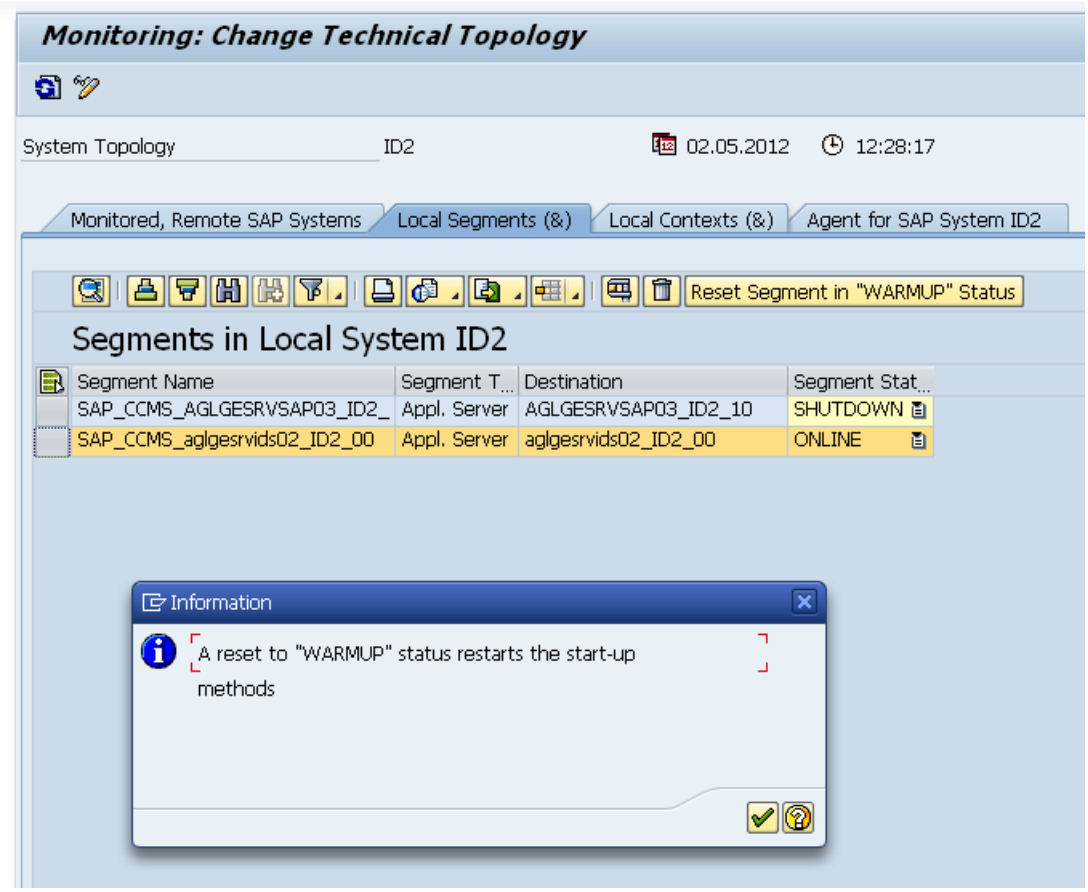
Go back to the previous menu and restart the local segment in order the activate the monitoring :



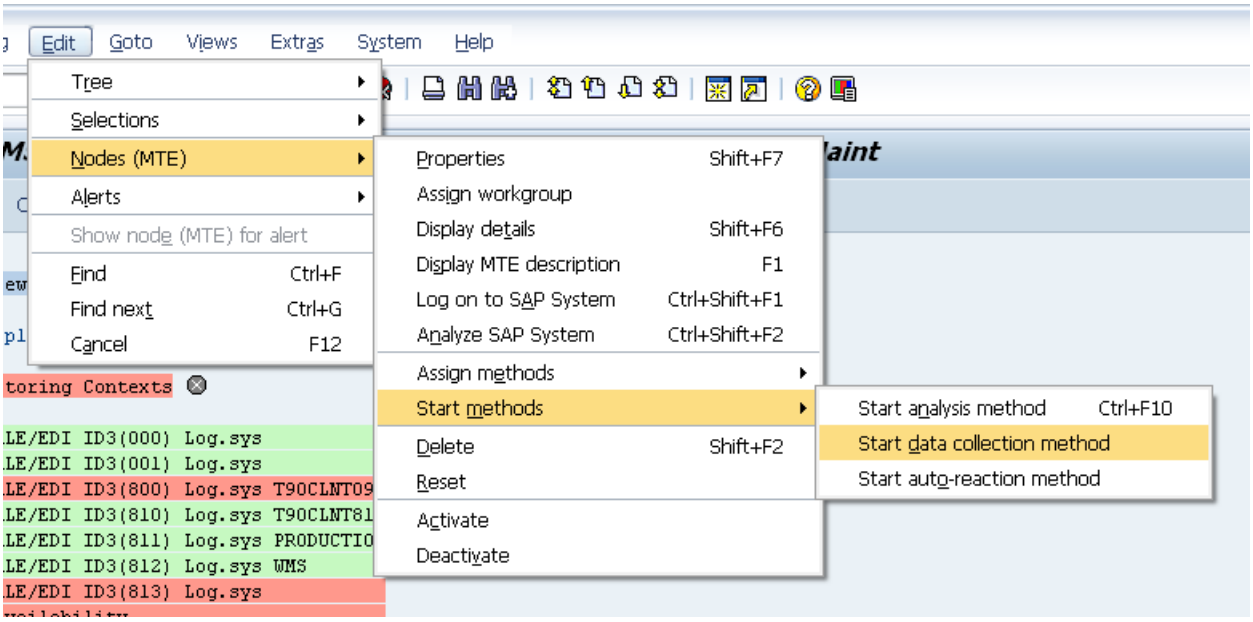
©copyright 2014 AGENTIL – all rights reserved



©copyright 2014 AGENTIL – all rights reserved



Start the collection in the RZ20 transaction :



©copyright 2014 AGENTIL – all rights reserved

59.4.2. Cannot find « SAP updates » metrics in the CCMS

Symptom:

Following metrics are missing in the CCMS :

"Update\UpdateServices\Old Update Records"

"Update\UpdateServices\Update Status

Problem**:**

The SAP update data collection is not enabled.

Solution:

Run the report: **RS_UPDATE_STATUS**

59.4.1. CCMS entry for Update Services Status not updated

Symptom:

If you get one of those alarms below:

The status of the update is not as expected. The status is “”.

Problem:
The CCMS entries “<SID>\Update\UpdateServices\Update Status” is not updated, is obsolete.

Solution:

To update the value depend of the SAP version and the SAP Basis customizing. If applicable, run the SAP report RS_UPDATE_STARTUP with SA38.

59.4.2. Cannot find Transactional and Queued RFC metrics in the CCMS

Symptom:

Following metrics are missing in the CCMS:

"Transactional RFC and Queued RFC\....”

Problem**:**

The data collection for this segment is not enabled.

©copyright 2014 AGENTIL – all rights reserved

Solution :

Run the function : **SALK_TRFC_DATENKOLLEKTOR**

59.4.3. /SDF/UPDATE_INFO not remote enabled

Symptom:

You receive following error message: “The function module "/SDF/UPDATE_INFO" cannot be used for 'remote' calls”

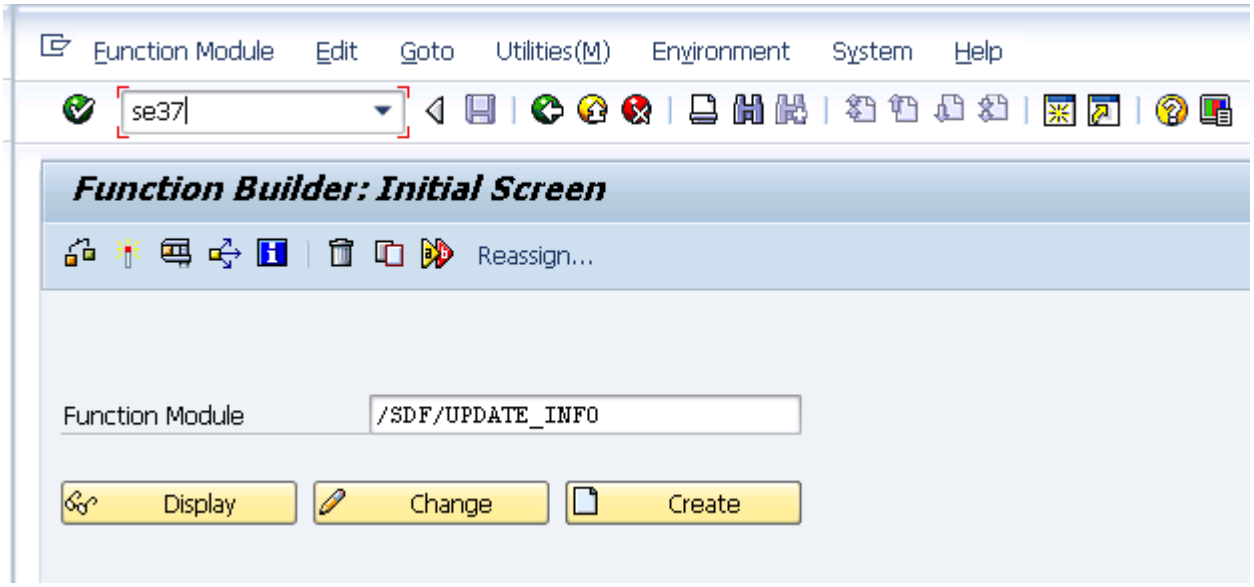
Problem:

A recent SAP patch changed the default configuration of this function module and turned off the ‘remote enabled’ feature.

Solution:

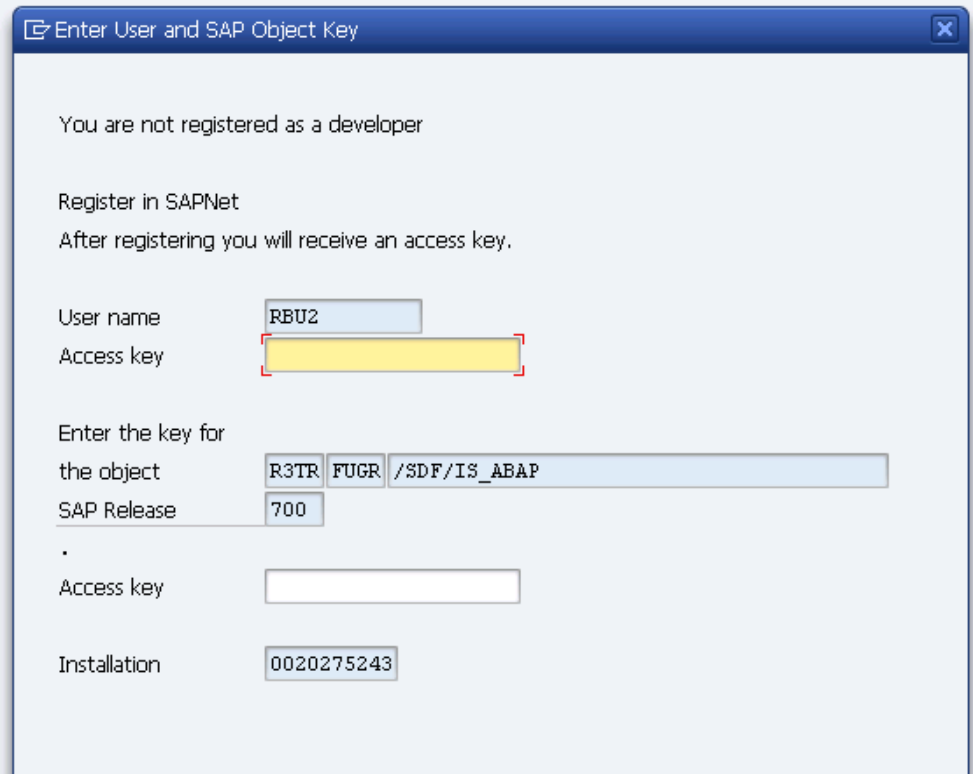
Re-enable the ‘remote enable’ mode. For that you will have to change the default configuration of the module. If your internal policy forbids such operation, you won’t be able to use the monitors related to this function module.

From SAP Gui, run the SE37 transaction, type /SDF/UPDATE_INFO in Function module field and press “Change”.



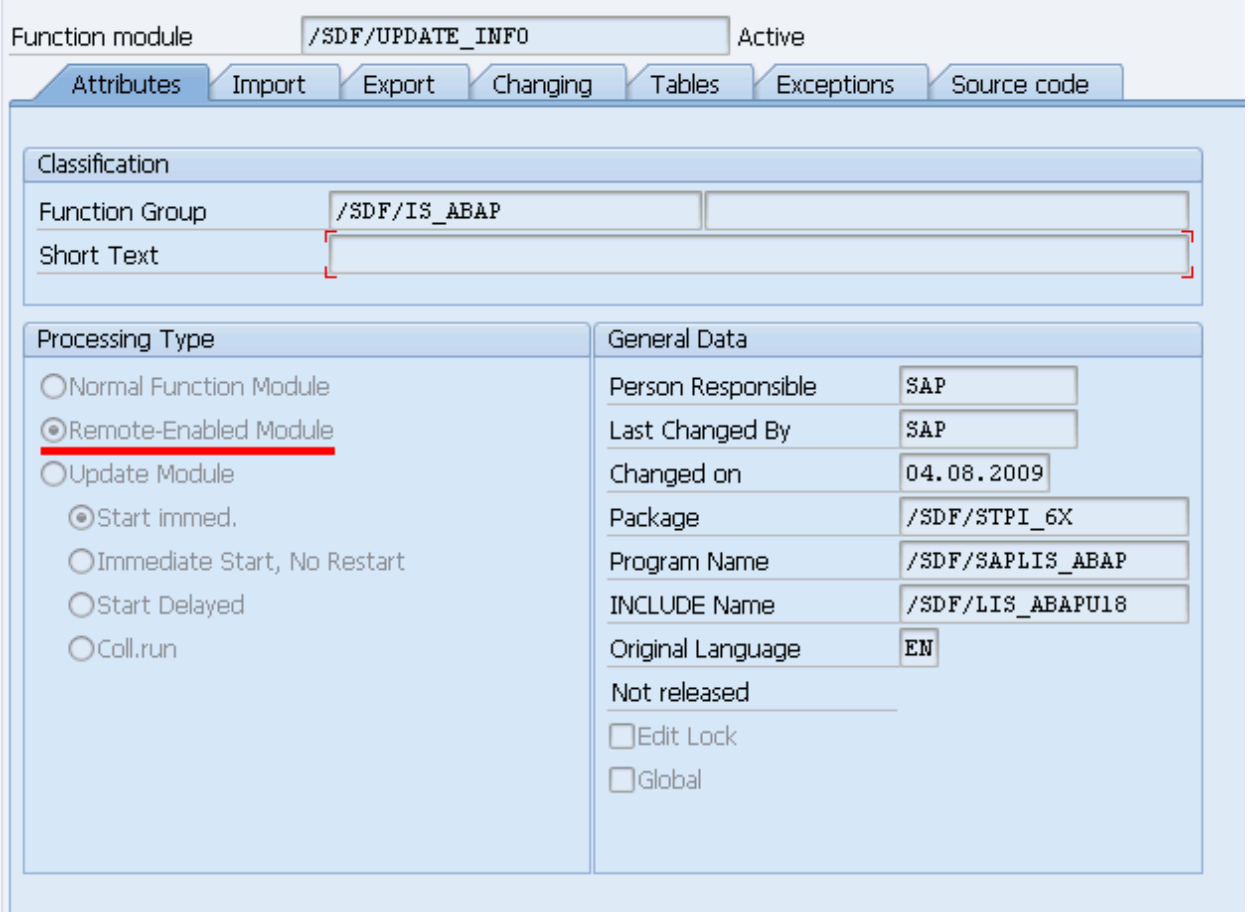
©copyright 2014 AGENTIL – all rights reserved

Fill in the User and SAP object key.



Open the 'Attributes' tab and activate the 'Remote-Enabled Module' :

©copyright 2014 AGENTIL – all rights reserved



59.4.4. partner '127.0.0.1:3302' not reached

Symptom:

Error message received when connecting to an ABAP message server : *"partner '127.0.0.1:3302' not reached"*

Problem:

One of the application servers is not correctly configured. If you test/run the instance availability check job, you get the following results in the job log window:

©copyright 2014 AGENTIL – all rights reserved

Collector results :

```
|----------------|----------|----------|--------|
|NAME            |HOST      |SERV      |TYPELIST|
|----------------|----------|----------|--------|
|BROSAPCP1_CP1_02|localhost |intraintra|DEUBSU2_|
|----------------|----------|----------|--------|
|BROSAPAP2_CP1_02|10.91.0.11|intraintra|DEBSU2__|
|----------------|----------|----------|--------|
|BROSAPAP1_CP1_02|10.91.0.10|intraintra|DEBSU2__|
```

In this example, you can see that the host of the first instance is set to localhost, instead of actual IP address. This is the cause of the problem

Solution :

Check that the localhost IP address of the application server is correctly set in its /etc/hosts file. Use RZ10 transaction to configure the proper IP.

©copyright 2014 AGENTIL – all rights reserved