Configuration Guide
SAP IT Infrastructure Management

Target Audience

- Technical consultants
- Application consultants

CUSTOMER
Document version: 1.0 – 06/11/2012

Document History

 Caution

Before you start the implementation, make sure you have the latest version of this document. You can find the latest version at the following location: http://service.sap.com/instguides ▶ *SAP Components* → *SAP IT Infrastructure Management* ↵.

The following table provides an overview of the most important document changes.

Version	Date	Description
1.0	6/11/2012	New

Table of Contents

1 Settings

1.1 Settings: Applications

Set the options of the SAP Infrastructure Manager application in this dialog. Open the dialog by choosing *Config* → *Settings* → *Applications*.

Features

You can make the following settings:

- *Web Console*
  This option activates the switches for the support of the Web Console in the main window.
  Open the start page of the inventory serve and the web browser with the Web Console tab of the navigation bar, when the option is activated.
- *URL root*
  The start page is entered as the URL root.
- Log in with the user *superuser* and the password *public*
  The necessary services start automatically.
- *Report Server*
  Enter the host where the reporting server is installed. The reporting server analyses data in regular intervals that have been collected and makes them accessible in the form of PDFs or web pages.
- *ServiceCenter WebConsole*
  If the inventory data is captured by a separate instance of SAP IT Infrastructure Management, this option should be activated and the URL entered as URL root.
  The context menu of NodeManager automatically linksto the inventory data of the other instance.
- *Run application with high process priority*
  This increases the processing priority of the application. Use this function only if other applications are negatively influencing the handling of Infrastructure Manager.
- *Enable Netflow Collector*
  Enables the Netflow option of SAP IT Infrastructure Management. Network routers send regularly statistic data about load, protocol distribution and so on to the Netflow Collector that prepares and stores them in the system database for later evaluation via web interface.

1.2 Settings: Default Settings

The dialog *Default Settings* determines which filters and sort criteria are applied initially when opening the NodeManager. If a large number of objects are stored in the system database, the initial display of the data can take time depending on the sort criteria and therefore slow down user handling. In such case, the definition of suitable filters can improve the user handling.

Features

The following options can be set:

- *Use initial sort order in NodeManager lists*
  This option turns sorting on or off when opening a table in NodeManager. Turning off this option increases the speed. Results however will appear in no order and need to be sorted by selecting the column header.
- *NodeManager default filters*
  This defines type and site filters that are applied immediately after opening. The configuration corresponds to the filter settings in the NodeManager, for example, if a large amount of data is present due to large inventory scans, the initial deactivation of types Service and Software can significantly increase the display time. The filters can be changed in the normal filter settings to revert these entries visible again.
- *Ignore user assignment when filtering nodes in NodeManager*
  This activates the display of all nodes in the NodeManager irrespective of their assignment between nodes and user groups. If the limitation is not needed, this option can make the data management easier.
- *Show imported sites in map for all users*
  This is only relevant in MultiSite operation and allows imported maps from other sites to be visible for all users. Normally, these are only visible to superusers.
- *Event archive view*
  This option limits the number of event log entries that are shown in the event archive view (*View* → *Event* → *Archive View* in the main window). The default range determines the number of days that is shown when opening the event archive. Max. a displayed entry limits the top number of log entries shown. If there are more entries available, the event archive dialog shows an appropriate notification. The value should only be increased in the case that special analysis requires more data. This impacts the system performance.

1.3 Settings: Polling

For polling, several settings need to be done. Open this dialog with *Config* → *Settings* → *Polling*.

Features

In this dialog, you have the option to define basic poll settings.

- *Reset to defaults*
  This resets the fixed default settings.
- The availability threshold slider sets globally at which status level MOs were created to get into the availability statistics as *available* or *not available*. The settings take effect immediately on the Web Console.
- *Global availability maintenance schedule*
  Define maintenance intervals that should be excluded from the calcuation of the availability percentage. These settings only take effect on the calculation of the availability not the polling. This means status events are generated normally.

1.4 Settings: Preference

This dialog allows different settings to configure the appearance of the objects in the map.
Open this dialog with ▶ *Config* → *Settings* → *Preferences* ↵.

Features

The following options can be set:

- *Map font/background*
  Configure the font type that is used for descriptions in the map.
- *Set font*
  This opens the standard Microsoft Windows dialog for the font selection.
- *Set color*
  You can change the background color of the map.
- *Center map window when changing submap*
  Activate this to center the map when changing between the map view hierarchies.
- *Use double buffering*
  Deactivate this when complex maps are displayed and the refresh is unsteady. Furthermore, this option improves the graphical representation when using remote desktop connection.
- *Network objects*
  This controls the visualization of network objects in the map. Set a standard color for network lines and their connections to device icons in the map.
- *Show connection labels*
  This option toggles on or off the global display of description texts.
- *Severity display*
  You can define if the severity bar shows colored blocks or LED icons for severity levels.
- *Exclude assigned log entries from severity calculation*

Sets whether events that are already processed by a user are included in the calculation of the node severity or not (▶ *Edit* → *Set event status* → *Assign to user* ↵ in the log view). These entries are also excluded from the display of the severity levels in the main window.

> **Note**
> The changes take effect only after a restart of the entire system (including all services).

- *Animate alarm window border*
  Configure the blinking frame of the alarm windows. This option is also recommended when using remote viewing software.
- *Splash screen display*
  Configure the layout of the windows that are shown during the initialization phase. The standard bitmap start screen is set to default.
  - By selecting the option *Simple*, only a progress window is shown in the initialization phase.
  - *Hidden* suppresses all start information. Select one of the last two options when using remote viewing software with a limited band width to decrease data transfer load due to bitmaps.
- *Save window layouts when closing profile*
  This toggles the automatic saving of the window position and contents when closing the profile. This option can also be configured using ▶ *Config* → *Save layout on close* ↵.
- *Show confirm dialog when closing application*
  Allows the confirmation to be deactivated when closing. The message to save unsaved profile data however appears even if this checkbox is selected.
- *Allow users to keep profile active after logging out*
  This gives each individual user the possibility to keep the last opened profile active after closing. In this case, the option keep the current profile active after closing in the *Confirm Close* dialog is activated (shown when exiting the system with ▶ *Config* → *Confirm Close* ↵ in the main menu is activated). This ensures that the monitoring functions of the profile and the subsequent alarming stays active
- *Map arrange defaults*
  This option is used for the definition of preconfigured sets for the automatic object arrangement in the Map display.
- *Reset to defaults*
  You can revert the setting back to the standard values of the system.

1.5 Settings: Reporting

To make the general settings for reports, open the administrative area under ▶ *InfoCenter* → *Reports* → *Administration* ↵.

Features

In the *Reporting Settings* dialog, you can check and make the following settings:

- *Requested Microsoft Reporting Server*
  Enter the Microsoft Reporting server URL (Example: `http://ReportHost/ReportServer`).
- *Microsoft Reporting Services Version*
  Enter the version of your Microsoft Reporting Service.
- *Microsoft Reporting Services root path*
  Enter the root path of the report files in Microsoft Report Manager.
- *Webservice Credential User*
  You can enter a user account used for authenticating the Microsoft Reporting Service web service.
- *Webservice Credential Password*
  Enter the password for the user account.
- *Webservice Credential Domain*
  Enter the respective domain for the user account.
- *Save Rendered Reports in*
  Displays the physical web server path used by Reporting Services to save generated reports. You cannot change this path.
- *Default display format*
  Displays the formatting option for online-generated reports and indicates any Administrator report link that may be selected in the search list.
- *Rendering Online formats*
  The formatting options that are generated and stored in the background with online-generated reports in addition to the default format.
- *Scheduled report formats*
  The formatting options that are generated and stored in the background with time-triggered report runs.
- *Reply email address for report subscribers*
  The e-mail address to use for replies sent in response to a received e-mail (subscription).
- *Email subject*
  The subject line for the e-mail sent by Microsoft Reporting Services. You can use the placeholders as predefined in the legend.
- *Include weblink in email*
  Specify whether URLs are to be included in the subscription e-mail.
- *Default reporting date format*
  You can select the format of the date displayed in the report.
- *Pattern for Filename of Generated Report*
  Displays the naming pattern for the results file generated on the web server. The following parameters with obvious meanings are accordingly replaced in the file name:

- REP_NAME$
- REP_ID
- REP_UUID
- REP_START_DATE
- REP_END_DATE
- REP_GEN_DATE
- $REP_LAYOUTNR$
- $REP_SCHEDULED$
- REP_TITLE
- REP_GEN_USER

> Note
> The system replaces REP_GEN_USER with the user name of the user that is logged on.

The length of the file name is limited to 32 letters. The system automatically deletes all characters not contained within [a-zA-Z0-9_-] from the file name. Spaces are replaced by underscores. If the file name is not unique on the Web server, the system adds the sequential number of the report to the file name. Any existing files with the same name are replaced with this file.

- *Pattern for Directory Path appended to root*
  Displays the naming pattern for the file path appended to the root path (see above). Replacement operations are made exactly the same as with the file names except that you can use "/" and "\" in path names. All backward slashes are replaced by forward slashes.

> Note
> In the `http://localhost/ReportServer` default value for *Requested Microsoft Reporting Server*, you must replace *localhost* with the Report server computer name.

1.6 Creating Configuration Files

You can create a configuration file that can be used by support employees to check the system configuration.

Procedure

1. Open the database administrator by choosing *Start* → *Database Administrator*.
2. Open the *System Info* tab.
3. Choose *Save to file*.

The Microsoft Windows registry only contains the installation path and versions of the files installed. If you have a problem with a corrupted registry, start the setup again and all registry entries are restored. You do not need to change configuration in the Microsoft Windows registry manually.

This page is left blank for documents that are printed on both sides.

2 Automatic Data Acquisition (Discovery) on Discovery Server

The Discovery server enables automatic detection of network nodes and their organizing into classes. SAP IT Management Infrastructure uses the agentless monitoring that works with standard protocols that are, by default, delivered and supported by all objects in the IT infrastructure. This includes Simple Network Management Protocol (SNMP), Web-Base Enterprise Management (WBEM) or its Microsoft implementation, Windows Management Instrumentation (WMI) – even ping and http. There is in principle an agent for these protocols on the devices, albeit a standard agent provided by the manufacturer. It is not necessary to install and maintain a specific CMDB agent.
Automatically detecting network components requires tools such as the SNMP or WMI protocol.

2.1 Specifying Settings for Automatic Data Acquisition (Discovery) on Discovery Server

Prerequisites

- You have made the necessary settings on network components.
- You have enabled ports on network firewalls.

Procedure

1. Specify global settings for the discovery server.
2. Edit scan profiles (change and create).
3. Specify automated scheduled scans.
4. Enable authentication sets:
   a) Acquire inventory data via WMI.
   b) Acquire inventory data via SNMP.
   c) Acquire inventory data via SSH/Telnet/FTP.
   d) Test the authentication set.
5. Define triggers and alarms.

2.2 Settings for Data Acquisition (Discovery) on Network Components

To perform the discovery automatically, you must first make the necessary settings on the network components.

Prerequisites

All installed software requires a transparent TCP/IP connection between the computers on which they run.

Features

Make the following settings on the network components:

- Set a fixed IP address at the server (no Dynamic Host Configuration Protocol (DHCP)), configuring it in the network components as a trap address.
- Set a high-performance link to the Domain Name System (DNS), alternatively a local host file, for the automatic name resolution.
- Enable the SNMP protocol.
- Configure the SNMP community strings.

> Note
> To minimize complexity, particularly for AutoDiscovery, use the most uniform Get and Trap community strings possible.

- Configure a trap IP address (IP address of the SAP IT Infrastructure Management system).
- Make the security configurations for SNMP polling (IP address of the SAP IT Infrastructure Management system) for authorized computers.

If you use firewalls, enable the following services:

- Transmission Control Protocol/Internet Protocol (TCP/IP) between all servers.
- Specific ports
- ICMP (Ping) and SNMP between the SAP IT Infrastructure Management server and the monitored nodes.

You can apply the settings manually on each Windows-based system, or you can make all the settings with Windows Domain Controller and transmit then to all connected systems.

2.3 Specifying Settings on Network Components with Windows Domain Controller

You can use global group policies to make all the configurations and security settings in the Domain Controller.

Procedure

In Microsoft Management Console, you can find the global group policies. Perform the following steps:

1. Run the `MMC` command and add a snap-in.
2. Select *Group Policy Object Editor* from the dialog.
3. Select *Domain Policies* as your group policy object. All changes are sent to the domain members.
4. Set up global SNMP as follows:
   a) Select SNMP in the policy tree generated in the Microsoft Management Console (*Default Domain Policy* → *Computer Configuration* → *Administrative Templates* → *Network* → *SNMP*).
   b) Enable *Communities* and add a new one.

      Caution
      You cannot define global communities with change authorization.

   c) Enter the IP address of the SAP IT Infrastructure Management system under the *Authorized Manager* policy so that it alone is allowed to initiate SNMP requests.
   d) If required, you can configure the SNMP service for automatic start on each client PC (*Default Domain Policy* → *Computer Configuration* → *Windows Settings* → *Security Settings* → *System Services*). Adapt the SNMP services accordingly in the right-hand selection dialog.

      Note
      If the SNMP agent is not installed on the client computer, the domain settings have no effect on client systems.

   e) Regulate the global ICMP and SNMP enabling within the Windows firewall:
      A) Select Windows Firewall from the policy tree in the Microsoft Management Console: Allow ICMP Exceptions (*Default Domain Policy* → *Computer Configuration* → *Administrative Templates* → *Network* → *Network Connections* → *Windows Firewall* → *Domain Profile*).
      Enable *Allow inbound echo requests*.
      B) Select *Windows Firewall: Define port exceptions* from the same subtree and add the following objects:
      - 161:UDP.*.enabled:SNMP_161
      - 162:UDP.*.enabled:SNMP_162

   f) As of Windows Server 2003 SP1, users can no longer access Windows services and installed software via WMI without Administrator rights. Therefore, you need an auxiliary script:

A) Select the WMI Control properties from Computer Management (▶ *Computer Management (Local)* → *Services and Applications* → *WMI Controls* ↵. Choose *Properties* from the context menu).

B) Select the *Root* item on the *Security* tab and open the *Security* settings. Continue with the *Advanced* settings.

C) Configure a new user in the advanced settings (for example, `WMIUSER`) with the three permissions: *Execute Methods*, *Enable Account* and *Remote Enable*.

D) Selecting the advanced security settings is required so that the rights are passed on to all the other namespaces. After applying all the settings, exit WMI Control.

E) Export your security settings with the following command:

```
wmic /namespace:\\root\ /output:  C:\wmiexport.txt path __systemsecurity call getSD
```

The display includes a large number of numerical values separated by commas and spaces following the SD = { parameter.

F) Delete the spaces.

G) Enter the sequence of numbers as generated under array in the following script:

>>> MISSING TARGET TEXT FOR TEXT-ID: 'SourceCode' (language: en) <<<

```
strSD = array()set namespace =
createobject("wbemscripting.swbemlocator").connectserver(,"root")set
security = namespace.get("__systemsecurity=@")nStatus
= security.setsd(strSD)
```

H) Save the result as `WMIUSER_ADD.vbs`.

I) Run the generated script on all computers in the domain. This can be done when a user logs on or when starting the client PC.

a) Select scripts from the Microsoft Management Console (▶ *Default Domain Policy* → *Computer Configuration* → *Windows Settings* → *Scripts (Startup/Shutdown)* ↵).

b) Link the corresponding script to *Startup*.

Caution

Make sure that the script is filed in the correct place. The best way to do this is to copy the `WMIUSER_ADD.vbs` file, open the respective folder with the *Display file…* option and then save the file.

g) Add the script to the policy.

d) If Microsoft Windows firewall is enabled, you can enable the respective ports via the domain policies.

e) Select *Windows Firewall: Allow remote administrator exceptions* from the policy tree in the Microsoft Management Console (▶ *Default Domain Policy* → *Computer Configuration* → *Administrative Templates* → *Network* → *Network Connections* → *Windows Firewall* → *Domain Profile* ↵).

2.4 Example Result for Script Export Security Settings

Example result of function call:

>>> MISSING TARGET TEXT FOR TEXT-ID: 'SourceCode' (language: en) <<<

```
wmic /namespace:\\root\ /output: C:\wmiexport.txt path __systemsecurity call
getSD(__systemsecurity)->getSD() executedMethod executed.Output parameters:instance
of __PARAMETERS{ ReturnValue = 0; SD = {1, 0, 4, 129, 148, 0, 0, 0, 164, 0, 0, 0,
0, 0, 0, 0, 20, 0, 0, 0, 2, 0, 128, 0, 5, 0, 0, 0, 0, 2, 24, 0, 63, 0, 6, 0, 1,
2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 2, 20, 0, 19, 0, 0, 0, 1, 1,
0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 2, 20, 0, 19, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 5,
19, 0, 0, 0, 0, 2, 20, 0, 19, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 5, 20, 0, 0, 0, 0, 2,
36, 0, 35, 0, 0, 0, 1, 5, 0, 0, 0, 0, 0, 5, 21, 0, 0, 0, 189, 125, 6, 42, 228,
50, 192, 71, 45, 218, 50, 167, 190, 4, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0,
32, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0};};
```

Adjusted result for the `WMIUSER_ADD.vbs` script:

>>> MISSING TARGET TEXT FOR TEXT-ID: 'SourceCode' (language: en) <<<

```
strSD
=array(1,0,4,129,148,0,0,0,164,0,0,0,0,0,0,0,20,0,0,0,2,0,128,0,5,0,0,0,0,2,24,0,63,0,6,0,1,2,0
namespace = createobject("wbemscripting.swbemlocator").connectserver(,"root")set
security = namespace.get("__systemsecurity=@")nStatus = security.setsd(strSD)
```

2.5 Settings for Enabling Ports with Network Firewalls

Port 135 is always needed to configure the Distributed Component Object Model (DCOM) connection. The exchange of data then occurs over randomly selected ports.
When a network firewall is in place, the required ports must be enabled. There is a script you can use to specify a fixed port range for the DCOM. For more information, see *Port Definition Script for DCOM Scans* [page 18].

Note
Microsoft recommends that you open ports 5000 and above, and define a minimum of 15 to 20 (for more information, see the Knowledge Base article 250367 at `http://support.microsoft.com`).

If there are network firewalls between the SAP IT Infrastructure Management Site systems and the SAP IT Infrastructure Management CMDB, enable ports `42380/tcp` to *42388/tcp* in both directions.

List of ports for internal communication in SAP IT Infrastructure Management

Server	Port
NMDBServer	Port: 42380/tcp (in + out)
NMProcMonServer	Port: 42381/tcp (in + out)
NMHistoryServer	Port: 42383/tcp (in + out)
NMEventServer	Port: 42384/tcp (in + out)
NMPollServer	Port: 42385/tcp (in + out)
NMDiscoveryServer	Port: 42388/tcp (in + out)

2.6 Port Definition Script for DCOM Scans

>>> MISSING TARGET TEXT FOR TEXT-ID: 'SourceCode' (language: en) <<<

```
Const HKEY_LOCAL_MACHINE = &H80000002strComputer = "."Set
oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\" &
_      strComputer & "\root\default:StdRegProv")strKeyPath =
"SOFTWARE\Microsoft\Rpc\Internet"oReg.DeleteKey HKEY_LOCAL_MACHINE,
strKeyPathstrKeyPath = "SOFTWARE\Microsoft\Rpc\Internet"oReg.CreateKey
HKEY_LOCAL_MACHINE,strKeyPathstrKeyPath =
"SOFTWARE\Microsoft\Rpc\Internet"strValueName =
"Ports"strValue = "5000-5020"oReg.SetStringValue
HKEY_LOCAL_MACHINE,strKeyPath,strValueName,strValuestrKeyPath =
"SOFTWARE\Microsoft\Rpc\Internet"strValueName = "PortsInternetAvailable"strValue =
"Y"oReg.SetStringValue HKEY_LOCAL_MACHINE,strKeyPath,strValueName,strValuestrKeyPath
= "SOFTWARE\Microsoft\Rpc\Internet"strValueName = "UseInternetPorts"strValue =
"Y"oReg.SetStringValue HKEY_LOCAL_MACHINE,strKeyPath,strValueName,strValue
```

2.7 Specifying Global Settings for Discovery Server

Before you run a general discovery, check or configure the following items:

1. Choose ▶ *Manage* → *Discovery Control* ↵ and then ▶ *Scan* → *Default Configuration* ↵.
2. Check the following general settings and make any necessary changes:
   a) *Request options*
   Not only is the Get community defined under *Request options*, but also the technical parameters for the polling mechanism. Changes in this dialog have fundamental effects on how long the polling of network segments take. Therefore, make changes only upon the advice of your technical consultant.
   All network nodes are polled with the communities as given here. If a network node has a community that is not entered here, the device is not recognized as an SNMP node, even if it is in fact SNMP-enabled.

Note

Only enter those Get communities here that are also entered at your device. It sometimes makes sense to manually configure individual devices rather than run a global configuration. Each inapplicable entry slows down the function.

b) *Actions*
This setting is used to define the options with which the discovery is to be started. We recommend that you activate all the options under *Basic Information*.

c) *Node naming*
To configure the name resolution.

Note

To prevent manual settings from being changed when nodes are named, select the *Change only new nodes* checkbox.

Note

Only use this function if you have a fast connection to your name server (DNS). A name review must be performed on each and every address detected.
In principle, the Discovery server can also run a DNS zone transfer, although the respective DNS authorization also needs to be granted. Check your corresponding log or DNS configuration.

d) *Log messages*
Here you define which events are sent to the log. By default, all events are sent to the log.

Note

If the entire option is disabled, no messages are sent to the log. While this of course results in fewer messages, automatic alerts cannot be configured.

e) *Extended*
If HTTP servers are subject to discovery and access is granted by a proxy (that is, indirectly), the access data needs to be specified in the configuration.

Note

Clear Data deletes data generated previously, although no nodes or self-created maps. Recalculating the topology may then take some time, but if not performed, Automaps can no longer display anything.

3. To limit the log entries for automatic discovery, choose *Manage* → *Discovery Control* and then *File* → *Base Configuration*.
   - Under *Maximum saved scans*, specify the maximum number of scan logs that can be saved.

- Under *Maximum saved topology trees*, specify the maximum number of topologies that can be saved.

2.8 Specifying Settings for Network Scans

Under the menu ▶ *Scan* → *New* ↵, in the *Discovery Scan* dialog, you can create new scan profiles. You can modify existing profiles by choosing *Change*.

1. Choose ▶ *Manage* → *Discovery Control* ↵ and then *Scan*.
2. Perform a *Normal discovery* or *topology scan*.
3. Choose *Next*.
4. Enter a description of the specific actions in the *Description* field. If you choose *Save this scan as profile*, the scan is saved and can be opened later.
   - *Add Network*
     Opens the dialog in which you can select a network for a full-network discovery.
   - *Add IP range*
     Opens the dialog for a network segment in which you can indicate the range to be scanned.

     > Recommendation
     > We recommend that you work with the *Add IP Range* function because it ensures that each possible IP address is also be checked by ICMP.

   You can configure multiple network ranges for each profile.
5. Choose *Next*.
6. In the dialog box, specify the actions to be executed for the specified networks or network areas. The dialog box displays all the settings you made under *Actions*. See *Global Settings* for more information.
7. You can adapt the settings to the specific scan.
8. Choose *Next*.
9. You can enable automatic group assignments.
   You can set automatic group assignments as needed (for example, the network segment to be scanned is only located in Bldg. A at one specific campus, therefore all detected components are automatically assigned to the "Location – Bldg. A" group). This group assignment is independent from the automatic *Function Group* assignment and is therefore optional.
10. Choose *Next*.
    The data entered is displayed once more in full for control purposes.
11. If necessary, you can go back to previous dialogs to make changes by choosing *Prev*.
12. Choose *Save profile*.
13. Choose ▶ *Scan* → *Reload/Start scan* ↵ to enable your generated profile.

2.9 Automatic Scheduled Scans

The SAP IT Infrastructure Management Task Scheduler is responsible for executing regularly recurring tasks and manages a list of tasks and schedules according to which the tasks are performed. You can assign any task to any schedule to prompt its execution.

Procedure

You create or modify a task from the context of the application in which an action is to be executed.

1. To create a new task that is to be linked to a discovery profile, choose ▶ *Manage* → *Discovery Control* ◀ and then ▶ *Scan* → *Schedule* ◀:
   - *Name*
     Links the task to a name, which should indicate the action that it stands for. Note that the name must be unique to identify the task. A default name is automatically generated from the context of the application.
   - *Description*
     Gives the task a user-defined description or comment.
   - *Enabled*
     This checkbox allows you to temporarily disable a task. While the action is then no longer executed, all its parameters (schedule, configuration) remain.
   - *Owner*
     Links a task to a user.
   - *Use Schedules*
     Lists all the schedules defined for all tasks. The *Use* field in the first column of the list directly links the current task to any existing schedule. This also allows you to link an action to multiple schedules. Note that any change to a schedule then automatically applies to all the tasks linked to it.
2. If you want to create a new schedule, choose *Add new* from the context menu.
   The dialog allows you to define your schedule (under *Schedule*) and the next time it is to be executed (under *Next execution*). The following fields are available:
   - *Name*
     Assigns a name to the created schedule. The name is also displayed in the list of defined schedules.
   - *Enabled*
     This checkbox allows you to temporarily disable a task. This function corresponds to the *Enable/Disable* function in the *Edit Task* dialog.
   - *Other tasks using this schedule*
     Displays a list of all defined actions. The actions that are checked are linked to the schedule currently being edited. You can select or deselect any link as needed.
   - *Change*
     Changes the parameters and the interval and/or times at which the schedule runs.

2.10 Authentication Sets Implementation

You use authentication sets to centrally create access information (login, secure communication) for network components to allow access to the SAP Infrastructure Management system through system functions without any user interaction.
It is for example necessary to specify authentication information on the secure SNMPv3 protocol access for polling the respective components. The login information for automatic Telnet and SSH polling via Device Configuration Management (through the Provisioning module) is also stored here.

Features

You can make these settings in the Authentication Sets dialog by choosing *Config* → *Authentication Sets* from the main SAP IT Infrastructure Management window.

- In the upper section, the *Authentication Sets* dialog field displays a list of all the defined authentication sets in the system. The buttons arranged underneath allow you to define new sets or modify or delete existing ones.
- The lower section displays and qualifies the user and user group assignments and the node and node group assignments for the authentication sets selected above (select the SNMPv3 or CIM protocol here).
- Use the buttons on the *Users* or *User Groups*dialog to authorize individual users and/or user groups for a selected authentication set. If an authentication set is not assigned to any user or user group, it can only be used by the system itself, for status polling or polling of configuration information, for example.
- The *Nodes* and *Node Groups* dialogs display the devices / device groups for which the selected authentication set is applicable.
- *Add..* allows you to add nodes or node groups.
- *Delete* deletes existing assignments.
- For SNMPv3 authentication, the access method and the Management Information Base (MIB) subset for which the setting is applicable is defined under *Access Types*.

If multiple authentication sets are to be conceivable for a specific scan, the preferential order is defined as follows:

1. An individual user has priority over a user group.
2. An individual node has priority over a node group.
3. Longer MIB paths have priority over shorter MIB paths (with SNMPv3).

Activities

Create Authentication Set

To create a connection to a network component via SNMPv3, Telnet or SSH protocol, you need to store the authentication parameters as configured on the device as an authentication set in SAP IT Infrastructure Management.

The *Authentication Set* (*Config* → *Authentication Sets* → *Add*) dialog allows you to enter all the respective necessary information. Depending on your selected authentication type, different input options are available:

- SNMPv3
- Telnet/ SSH/ FTP
- WMI

The following values must be configured:

- *Name*
  An arbitrary name that identifies the authentication set in the overview list.
- *Authentication type*
  Allows you to select an authentication type (SNMPv3, Telnet or SSH).
- *Context*
  The context name under which you run the SNMPv3 polling. This context name must have first been defined on the corresponding network component. It describes a collection of management information that can be accessed under this identifier by a management application.
- *User-Based Security Model*
  Selects the user-oriented security model for SNMPv3.
- *Security Type*
  Select the security level at which login and data communication are to take place:
  - No encryption upon login or data transmission (*None*)
  - Secured user login (*Authentication*)
  - Secured login and data transmission (*Privacy*)
- *User Name*
  If *Authentication* is selected in the *Security Type* field, the name of the user who is logging in needs to be entered here.
- *Authentication*
  Select the type of encryption to be used for user authentication:
  - *NoneMD5* or *SHA*

  Enter the associated password under *Password* and *Confirm*.
- *Privacy*
  If you selected the *Privacy* option in the *Security Type* field, you need to select the type of encryption for the data transmission:
  - *None*
  - *DES* or *AES*

  The encryption password is also entered here.
- *Telnet / SSH / FTP User*
  Specifies the login information needed for access by *Telnet*, *SSH* or *FTP*. Depending on the parameters required for the respective network component, a user name and/or a password can be indicated.

- *Telnet / SSH Extended User*
  For advanced configuration tasks via *Telnet* or *SSH* (setting configuration parameters, for example), some network components may require another user to have a higher access privilege level. The corresponding user data can be entered in this group.
- *WMI User*
  Polling WMI data from Microsoft Windows PCs requires a Windows user account to have the correct authorization to access the information. Enter the corresponding information (domain, user name, and password).

Test Authentication Set

To test the correct allocation of authentication sets, a test function has been integrated into NodeManager. You can open it in the main/context menu item of NodeManager's by choosing *Manage* → *Authentication Sets*. You can make the following settings:

- *Node*
  When the dialog opens, the node for which the authentication set assignment is to be tested is already pre-selected from the node you selected earlier in NodeManager. You can change your selection using the Browse button (…).
- The list in the lower section of the dialog shows all the authentication sets applicable to the selected setting, sorted in descending order according to priority.
  Since the system has to decide among several authentication set options, the uppermost entry is always used during operation. The listing of all suitable authentication sets, however, offers you the possibility of detecting unwanted overlaps and correcting them as needed.
- *User*
  Making a change in the user selection field restricts the authentication sets to just those that are available to the respective user based on a direct or user group assignment. The default entry displays those authentication sets used by the system itself (for polling tasks, for example).
- *Access Type*
  This field specifies the desired type of access to the device information:
  - Read only (*Get/Read*)
  - Read and write (*Set/Write*)
  - Device notification messages (*Trap/Notify*)
- *Authentication Type*
  Select the desired access protocol (for example, *SNMPV3* or *Telnet*).
- *Object ID*

For SNMP polls, a specific variable can additionally be indicated since this information likewise impacts the selection of a suitable authentication set.

2.11 Specifying Settings for Inventory Data Scans via WMI

To gather inventory data via WMI, two scans of different types are necessary. The first scan records the corresponding systems in the SAP Infrastructure Management database, to use the second scan to fill these systems with inventory data.
For both discovery scans, you create a new profile. You assign a new authentication set to these scans. This authentication set contains the user and the user's password.

Prerequisites

You have made the settings for the network components and the firewall.

Procedure

1. To create an Authentication Set for WMI scans, in the main window of the SAP Infrastructure Management system, choose *Config* → *Authentication Set* and then *Add*.
   When you create the set, specify the following settings:
   a) Select *WMI* as *Authentication Type* and enter the corresponding user with the defined password. You only need to define a domain if the corresponding user is also a domain user. For local users, enter ".\" as the domain.
   b) Specify the users or user groups that can use the authentication set for the Discovery scan.
2. For a Discovery scan, create a new profile that records the corresponding systems in the SAP Infrastructure Management database.
   When you create the profile, specify the following settings:
   a) Select the scan type *Normal discovery* or *topology scan*.
   b) Enable the IP area *Configs*.
   c) On the *Protocols* tab, select the defined Authentication Set for WMI scans.
   d) Specify the remaining settings.
   e) Save the profile.
3. For a Discovery scan, create an additional profile that reads the inventory data from the systems and transmits the data to the database.
   When you create the profile, specify the following settings:
   a) Select the scan type *Inventory Scan*.
   b) Enable the IP area *Configs*.
   c) On the *Protocols* tab, select the defined Authentication Set for WMI scans.
   d) Define the *Inventory Actions*.
   Note that the properties can only be read if the Managed Objects (MOs), which are subordinate units of a node, are already detected. For new nodes, always enable the *Detect managed objects* option.
   e) Using *Extended Properties*, read all the properties configured for the nodes. These extended properties are defined separately in Class Manager for each node class.
   f) Save the profile.

4. Start both newly created Discovery scans in the following order:
   a) *Normal discovery* or *topology scan*
   b) *Inventory scan*

2.12 Specifying Settings for Inventory Data Scans via SNMP

To gather inventory data via SNMP, two scans of different types are necessary. The first scan records the corresponding systems in the SAP Infrastructure Management database, to use the second scan to fill these systems with inventory data.
For both discovery scans, you create a new profile and, to these scans, you assign a new authentication set, which contains the user and the password.

Prerequisites

You have made the settings for the network components and the firewall.
You have made the global settings for the Discovery server.

Procedure

1. To create an authentication set for SNMP scans, in the main window of the SAP Infrastructure Management system, choose *Config* → *Authentication Set* and then *Add*.
   When you create the set, specify the following settings:
   a) Select *SNMP* as *Authentication Type* and enter the corresponding user with the defined password. You must only define a domain if the corresponding user is also a domain user. For local users, enter `".\"` as the domain.
   b) Specify the users or user groups that can use the authentication set for the Discovery scan.
2. For a Discovery scan, create a new profile that records the corresponding systems in the SAP Infrastructure Management database.
   When you create the profile, specify the following settings:
   a) Select the scan type *Normal discovery* or *topology scan*.
   b) Enable the IP area *Configs*.
   c) On the *Protocols* tab, select the defined Authentication Set for SNMP scans.
   d) Specify the remaining settings.
   e) Save the profile.
3. For a Discovery scan, create an additional profile that reads the inventory data from the systems and transmits the data to the database.
   When you create the profile, specify the following settings:
   a) Select the scan type *Inventory Scan*.
   b) Enable the IP area *Configs*.
   c) On the *Protocols* tab, select the defined authentication set for SNMP scans.

d) Define the *Inventory Actions*.
Note that the properties can only be read if the Managed Objects (MOs), which are subordinate units of a node, are already detected. For new nodes, always select the *Detect managed objects* option.
e) Using *Extended Properties*, read all the properties configured for the nodes. These extended properties are defined separately in Class Manager for each node class.
f) Save the profile.

4. Start both newly created Discovery scans in the following order:
a) *Normal discovery* or *topology scan*
b) *Inventory scan*

2.13 Configuration Data Scan

SAP IT Infrastructure Management enables configuration data to be scanned and set by command line interface (CLI) or File Transfer Protocol (FTP). Secure Shell (SSH), Telecommunication Network (Telnet), and FTP are provided as communication protocols.
In NodeManager, you can assign a special protocol, such as CLI, to each node.

Features

- Store the statement sequence necessary to scan and set a configuration in the system database in the form of class-specific macros. SAP IT Infrastructure Management provides a number of predefined macros covering the most frequently required configuration tasks for widely distributed network components. In addition, you can define your own macros to execute specific tasks.
- You can then run these class-specific macros manually or automatically at any time with a discovery scan.
- To be able to run this function, you need the necessary login information for Telnet, SSH, or FTP access. Store this information for the respective components with the Authentication Set function. When you scan configuration data, the outputted configuration information is compared to a reference configuration that may have previously been saved and identified (by default, the last configuration is always used as the reference) and saved to the database as a new dataset (only if there is a difference).
- Additionally to saving a configuration, you can also generate provisioning scripts, which are managed similar to the configurations. They are not linked directly to the node from which they resulted but only indirectly with a provisioning node. This allows the script to be disassociated from the node that generated it and reassigned to another node. Therefore scripts serve more the administrative planning of configuration information while the result of running a macro (that is, configuration) has more of a documenting character.

When executed, the lines of a script are sent without change to the network component. The result of its execution (that is, the response returned by a network component based on the commands sent) is not saved with the script.

Activities

Add protocols in Node Manager

To add a protocol to a node in Node Manager, choose ▶ *View* → *Node Manager* ↵ and then ▶ *File* → *Properties* ↵. You can make the CLI settings under ▶ *System* → *CLI* ↵.

Scan configuration data with Discovery scan

To enable the automatic scan of configuration data during a Discovery scan:

1. Create a new scan profile by choosing *Discovery Control*: ▶ *New* → *Provisioning Scan* → *Next* → *Next* ↵.
2. On the *Macros* dialog page, select the macros you want to use.

3 Triggers and Alarms

SAP IT Infrastructure Management offers you the option of processing occurring events and differenciates between internal and external messages. Internal messages can represent threshold monitoring (SAP IT Infrastructure Management terms these “triggers”) or system messages, for example. External messages are standardized message formats such as SNMP traps or syslogs. SAP IT Infrastructure Management processes all messages centrally.

3.1 Definition of Triggers and Alarms

SAP IT Infrastructure Management provides several features related to the definition of triggers and alarms.

Features

- SAP IT Infrastructure Management provides a filter mechanism for occurring events. This allows you to define the events that are to lead to log entries or to automatic alarm reactions, for example.
- In SAP IT Infrastructure Management, multiple event filters are already preset. However, they are only just a start and must be further managed by the administrator. You can also define new filters to specify which events lead to log entries or automatic alarm reactions, for example.
- To access the filter settings, choose the *Event Filter* icon or choose *Config* → *Event Correlation*.
- The window that opens displays all the predefined event filters. Each filter is assigned to a series of actions to be executed when activated.

  Note

  Filters *4000* to *4400* are used to ensure that no event will ever be omitted. Except for the special *Goto action*, you should never define any normal-operation filter above these numbers. You can find further information about the *Goto action* function (activating, disabling, or restarting polls on a node or group) under *Goto Filter Action*. Filters *1000* and *1100* are furthermore responsible for ensuring polled nodes are given *red* or *green* status.

- A filter consists of a unique filter number, a short description of what the filter is designated for, the node to which it applies, the message to be filtered for, and to what type of event it pertains.
- When an event occurs, the filters are processed in numerical order. As soon as a filter is found for the event, the associated actions are executed.

The individual event types and their meanings are as follows:

Type	Description	Color
P1 / S1 = Fatal	Very critical information, for example, no response from node	red
P2 / S2 = Critical	Critical information, for example, system messages	yellow
P3 / S3 = Minor	Important incoming message, for example, traps being received	magenta
P4 / S4 = Warning	A threshold (trigger) has been exceeded or undershot	blue
P5 / S5 = Harmless	Information on an event has been logged	cyan
P6 / S6 = Normal	Expected information, for example, node response to SNMP, OK value when monitoring a logical port	green
P7 / S7 = Informative	Entries that are only written to the *History log*	gray

Activities

With event filters, you can perform the following actions:

- Start filters
- Stop filters
- Temporarily stop filters
  After restarting SAP IT Infrastructure Management, these are reactivated or started.

Selecting the *Perform initial actions* checkbox also enables active alerting when SAP IT Infrastructure Management is started.
The slider bar allows setting a limit on the severity level for an initial action.

- When the slider bar is set to the far left, initial actions run for all severities. When it is set to the far right, no initial actions are executed.
  In all other cases, only the log action or a database action is executed when initial events are generated.

3.2 Event Filter Creation

You can create event filters.

Features

Add adds a new filter to the event filters, sorting it by its number. You can make the following settings in the filter dialog:

Note

You can use placeholder characters in most fields:

- *: Placeholder for a sequence comprising none or any number of characters
- ?: Placeholder for exactly one arbitrary character

- *Active*
  This selection field allows you to indicate whether a filter should be turned on or off.
- *Filter#*
  A unique filter number must be given to each filter. Note that the default value is always 1.
- *Description*
  Enter a short description of the filter in this field.
- *Node name*
  A filter may be valid for one single node or for multiple nodes. Using the * symbol allows this filter to be valid for all nodes, or for all nodes of a group respectively.
- *Subobject name*
  Indicate the triggering MO as a further criterion.
- *RC object name*
  The name of the Root Cause Object that triggered the event in a correlation.
- *Node address*
  You can enter an IP address in addition.
- *Message*
  This setting determines the messages that merit a response. You can use the following special characters within your text: **$1** – **$9** placeholder for a sequence comprising none or any number of arbitrary characters.
  The omitted characters are buffered and reinserted for the placeholders in the respective actions associated with the output message.
- *Status Level*
  The event is usually generated as a function of status analysis. To classify it better, you can also reference the relevant status level in the filter.
- *Node Group/ MO Group*
  A filter can serve for all groups or for just one particular group. This field also supports the use of the * and ? placeholders.
- *Class*
  Allows you to indicate the type of device concerned.
- *Subobject type*
  A further attribute to better classify events to be analyzed.
- *Event type*
  Indicate here the type of SNMP event concerned from the following selection:
  - Info
  - Trigger

- Warning
- Syslog
- Error
- Trap

> Note
> Each event is assigned only one event type. If more than one option is selected, this means that different types of events apply, but not that one event must fulfill several conditions.

- *Traps*
  The MIB database is searched for set traps, which are then displayed.
- *Schedule*
  Opens the *Scheduler* dialog where you can enter an active time frame for a filter. The marked tracts in the dialog indicate an active filter. Selecting a day in the first column will either completely select or deselect the day.

> Note
> All inputs are inclusive; that is, a filter does not match until it meets all criteria. If configuration is too precise, it can occur that no filter matches.

After making the settings, you can disable filters to prevent editing.
The state is displayed by the corresponding icons. If a filter is temporarily disabled (Pause), this state is set to active after restarting or changing profiles.

3.3 Actions

After you have created a filter, you need to define the actions that are executed upon the occurrence of the event.

3.3.1 Creation of Single Actions

SAP IT Infrastructure Management allows you to create single actions that are executed when an event occurs.

Features

You can create single actions by choosing *Add* → *Single action*. You can deleted actions can with *Delete* and subsequently modify them with *Edit*.
Assigned actions always have the following attributes in common:

- *Active*
  Reactivates or disables the action.
- *Action*
  Numbering of the action under a filter.
- *Description*
  Descriptive text.
- *Comment*
  Comment field.

You can create the following actions:

- Log Action
- Execute Action
- Trap Forward Action
- Event Forward Action
- Filter Control Action
- Poll Control Action
- Goto Filter Action
- Authenticate Action
- ADO (Database) Action
- Pager Action (SMS Action)
- E-Mail Action

After making the settings, you can disable actions to prevent editing.
The state is displayed by the corresponding icons. If a filter is temporarily disabled (Pause), this state is set to active after restarting or changing profiles.

3.3.2 Log Action: Saving and Evaluating Messages

Log Action allows you to make the settings for how the message is saved and evaluated. Past events are easily identifiable by the severity level status display.

Features

After a new filter has been defined in the *Event Correlation* dialog and generated by choosing *OK*, a log action is automatically created. You can make the following settings in the *Log* dialog that opens:

- *Clear filter(s) #*
  The filter number to be reset by this event; you can indicate multiple filters.
- *Log message*
  The message to be logged. The following placeholders may be inserted to replace text.

Note

Note that the colon is an integral component of the placeholder and must be included:

- `$filter:` or `$f`
  Transfers the description from the filter settings.
- `$name:` or `$n`
  The name of the object generating the message.
- `$message:` or `$m`
  The original message text.
- `$type:` or `$p`
  Type of occurred event (Info, Error, Trigger, Trap).
- `$group:` or `$g`
  The group name of the object that generated the message.
- `$time:` or `$t`
  Point in time the event occurred.
- `$date:` or `$d`
  Date on which the event occurred.
- `$address` or `$a`
  Polling address of the object generating the message.
- `$hwadress` or `$h`
  MAC address of the object generating the message.
- `$1` – `$9`
  To be replaced by the text buffered for these placeholders in the message filter.

- *Severity*
  Establishes at which severity level the event is logged.

Note

The P (from source status level) and S (from source status level) severities establish the specific characteristic that the severity always corresponds to the status level passed to it. Therefore, the *Clear filter(s) #* setting may no longer be necessary.

- *Clear duplicates*
  Indicates whether identical events are overwritten in or added to the current log.

3.3.3 Definition of Alarm Actions

Certain events are able to generate a visual or acoustic alarm.

Features

You can make the following settings in the *Alarm* dialog (*Single Action* → *New alarm action*):

- *Message*
  The message that is to be sent.
  The special characters as indicated under Log Action / Log Message may also be used.
- *Alarm actions*
  Establish whether only the visual alarm or only the acoustic alarm or both options should be enabled.
- *Audio settings*
  Indicate whether global settings are to apply for an acoustic alarm or whether an individual setting is to be made for each filter.

Global Alarm Settings

Visual alarms can also be supplemented by an audible alarm (provided the sound function is installed). To do so, make the corresponding assignment in the main application. A given file can be activated and tested with the *Select Audio* option under ▶ *Config* → *Alarm settings...* ↵ from the main SAP IT Infrastructure Management window.

Select Media – Select Audio

Select a file from the *Select Media* dialog to play upon the occurrence of an alarm action, thus providing an additional audible warning of a critical network state. Desired WAV files should be saved in the ...`\Media` directory of the SAP IT Infrastructure Management system. Use the *Browse* button (...) to find and select the specific sound file desired.

 Note

In the underlying Terminal Server function of Microsoft, audible or modem/ISDN actions always relate to the server; that is, these functions are executed where the server is located and mean that the modem/ISDN adapter is also responding.

3.3.4 Execute Action

This setting enables you to specify a program or macro to start upon an event occurring.

Features

You can make the following settings under ▶ *Single action* → *New Execute action* ↵:

- *.exe/.mac file*
  The name of the program or macro that is to run.
  Use the *Browse* button (...) to select your desired file.
- *Parameters*
  The parameters to be transferred to the program.
  You can use the special characters as indicated under *Log Action / Log Message*.

- *Use this login when running an executable*
  When this option is enabled, you can enter login information such as *User Name*, *Domain*, and *Password*, if the same information is needed for executing the action.
- *Always use this node when executing the file/macro*
  Enable this option if the selected macro is not to be executed for the node which triggered the event but rather always for the node as indicated. All Set/Tryset instructions contained in the macro then relate to this node.
- *No duplicate calls for … seconds*
  Indicates the number of seconds during which the program is not called up again.
  This value is applied to the following two checkboxes:
  - Block calls with same node name
    The program does not run within the time period given above in the event of identical node names.
  - Block calls with same parameters
    The program does not run within the time period given above in the event of identical parameters.
- *Hide program window on execution*
  If `exe` or `cmd` files are executed multiple times, a new window is displayed each time. This parameter prevents such repeated displays.

3.3.5 Trap Forward Action

The *Trap forward* action allows you to send an event to another computer able to evaluate traps in the form of an SNMP trap.

Features

You can make the following settings under *Single action* → *New trap forward action*:

- *Host*
  IP address of the computer to which the SNMP trap should be sent.
- *Community*
  Another community as configured in Microsoft Windows can be set for the trap.
- *Message*
  The message to be sent.
  You can also use the special characters as indicated under *Log Action* / *Log Message*.

> Note
> The message is augmented by specific trap details since certain textual additions are necessary to depict traps.

3.3.6 Filter Control Action

This action serves to temporarily deactivate an event filter. Filters which have been disabled by means of such an action are identified in the overview with a “paused symbol” preceding their filter number. Temporarily-disabled filters can be manually enabled again from the *Filter Properties* dialog. A new start of SAP IT Infrastructure Management will re-instate any temporarily disabled filters.

Features

You can make the following settings under *Single action* → *New filter control action*:

- *Filter#*
  The number of the filter to be enabled or disabled with the next button.
- *Filter control*
  Enable or *Disable* the particular filter. In the basic configuration, disabled filters will be indicated in the overview preceded by “.

> Note
> In order to use this action, you should differentiate the polling times for the specific groups in the SAP IT Infrastructure Management.

> Example
> Should a switch to which all the servers are connected fail, alarms will be generated for both groups (switch and server) even though only one component actually failed. This action will prevent this in that the filter which was conceived for the switch will *disable* the filter for the server. So that there will be enough time to do so, the polling for the *Server* group needs to be set to e.g. 300 seconds.

3.3.7 Event Forward Action

The *Event forwarding* action allows you to send an event as a TCP event from one SAP IT Infrastructure Management system to another. As opposed to the *Trap* forward action, which uses a UDP connection (connectionless), this action establishes a TCP connection (connection-oriented).

Features

You can make the following settings under *Single action* → *New event forward action*:

- Host
  IP address of the SAP IT Infrastructure Management system designated for this event.
- Message
  The message to be sent.

The special characters as indicated under *Log Action* / *Log Message* may also be used.

- Name
  Node name that this event should be assigned to on the receiving SAP IT Infrastructure Management system.
- *Event Type* (Info, Warning, Error, Trigger, Trap, Syslog)
  You can assign each event a further type so as to enable its reevaluation on the other SAP IT Infrastructure Management system.

3.3.8 Poll Control Action

This action allows you to enable, disable, or restart polling of a single node or a group of nodes.

Features

You can make the following settings under ▶ *Single action* → *New poll control action* ↵:

- *Poll control*
  Activate, deactivate, or reactivate polling for the node or group specified below.
- *Node*
  The name of the node to which the action is to apply. You can select the node by choosing *Select*....
- *Group*
  Specify a group for this action.

> Note
> The *enable* and *disable* functions also have an impact on availability. As with the *Enable/Disable Filter* action, combinations can also be set up to obtain the availability statistics of individual groups. The *Reset* function can likewise be used in combination with the *Enable/Disable Filter* action.

3.3.9 Goto Filter Action

This action serves when the same actions are always to be executed for a filter. This action should therefore always come at the end of the action list; always position the filter at issue after filter *4300*.

Features

You can make the following settings under ▶ *Single action* → *New goto filter action* ↵:

- *Goto Filter#*
  The filter to be executed.
- *Message*
  The message to pass with its own text or parameters.

Note

As a functional enhancement, event processing does not end after jumping to the respective filter, but rather not until a further match.

3.3.10 Authentication Action

You can use this action to check an event message, such as Trap or Syslog, for the presence of a character string representing a reference to a registered, and therefore authenticated, component. You can check event segments by entering the *Address*, *Name* or *Alias* field values as compared to the database fields and then have a new event of either *Authentication succeeded* or *Authentication failed* returned.

Features

You can make the following settings under *Single action* → *New authentication action*:

- *Authentication type*
  Indicate against what in the database the value is to be checked.
- *Value*
  Set a variable from the event.
- *Message*
  To specify the return event, you can indicate further values to pass.
- *Group*
  For defining a group affiliation.

3.3.11 ADO Database Action

This function allows you to save occurring events into a database. For entering datasets, this action uses the ActiveX Data Objects (ADO) interface of Microsoft Windows and must be configured accordingly.

Features

- Connect string
  The ADO connect character string that contains all the parameters necessary to set up a connection to a database via an ADO service provider. The connection string can be generated either by clicking on *Build...* or it can be saved in a UDL file and called up by means of *UDL file...* To create a UDL file, open a blank text file and name it using the `.udl` file extension. Open the file from Microsoft Windows Explorer to open an input dialog in which you can define the necessary parameters and save them to the file.

You can find more information on UDL files and ADO connection strings by opening a UDL file or clicking *Build...* and selecting the Help option in the *Data Link Properties* dialog box.

- *Table Name*
  Name of the database table in which to write the data.
  Add lets you define what is to be written into which field of the table.
- *Field name*
  Identifies the name of the field in the table.
- *Integer*
  Indicates the field is of *integer* type.
- *String*
  Indicates the field is of *string* type.
- *Length*
  For a string field, indicates the length of the string.
- *Index*
  The identifier in *Field Name* pertains to the table index.
- *Set*
  The text to be written into the column.
  The special characters as defined under *Placeholders* may also be used.
- *Increment*
  Increases the existing value by one.
- *Decrement*
  Decreases the existing value by one.

3.3.12 Pager Action

Important events can be forwarded directly to a pager.

Features

You can make the following settings under *Single action* → *New pager action* :

- *Service*
  Type of pager.
- *Number*
  Pager call number.
- *Message*
  The message to be sent.
  You can also use the special characters defined under Log Action / Log Message.
- *Config*

This opens the configuration menu in which basic items can be set such as modem settings and provider call numbers. Contact your SAP IT Infrastructure Management technical contact person for further configuration options.

3.3.13 E-mail Action

Allows you to forward messages to an e-mail address.

Features

You can make the following settings under *Single action* → *New Email action*:

Note
This action is divided into three different windows: *Message*, *Sender*, *SMTP Server*.

- *Destination email address*
  E-mail address of the message recipient.
- *Subject*
  E-mail subject line displayed to the recipient.
  The special characters as defined under *Log Action* / *Log Message* may also be used.
- *Message text*
  The message to be sent.
  The special characters as defined under *Log Action* / *Log Message* may also be used.
- *Priority*
  The priority level of the e-mail to be sent.
- *Character set*
  Selection menu for the character set to be used in the e-mail to ward off problems when it displays. This setting has an effect for the message recipient if the e-mail contains special characters (for example, umlauts). They are interpreted according to the character set as defined here.
- *Sender name*
  Name of the sender as displayed for the recipient (many SMTP servers require a name or an address).
- *Sender email address*
  The sender's e-mail address (many SMTP servers require a name or an address).

3.4 Creating Filters from Existing Messages

You can create filters that react to *Node responding* * and *No response* * messages for different groups and filters that process diverse types of messages. Since all messages are stored in the logs, they become the starting point when messages are to be analyzed.

Procedure

1. Copy the message from the log and add it into a new filter as the message to receive. Make sure that the type of event is correctly defined since the message is also checked with this criterion.

   Note
   You can also create filters in the context menu of the log by choosing *Make new Event Filter*.

2. Confirm with *OK*. This brings up a dialog in which you can assign the received message a new priority.

   Note
   Such defined filters respond only to the exact message wording. To obtain general filters, reduce the content of the messages to the content that is necessary. You can do so by using placeholder characters.
   However, do not reduce the content of the messages to the extent that each and every message is processed; retain necessary information.

3.5 Testing the Filter Configuration

You can test all actions irrespective of the event occurring.

Procedure

1. Highlight the corresponding action entry.
2. Choose *Test action/filter* from the context menu.

3.6 Prefilter

The main features of this function are as follows:

- Integrates a syslog function.
- Reduces messages (SNMP traps and syslog events).

Features

Call up the prefilter function from the *Event Correlation* dialog.
You can use the following methods to reduce incoming messages when they are not generally disabled:

- Method 1:
  Identical messages from a node are totaled over the set interval and then forwarded to the filter system as one message indicating the sum.
- Method 2:
  Identical messages are only forwarded upon reaching the predefined number within the set interval.

If the prefilter function is enabled in the respective area, you can set an incoming message to *excluded* (forwarding prevented) or *included* (forwarding enabled) with filters.

Note

Both methods apply to all incoming events in the respective range; that is, if you set Method 1 in the SNMP trap range, all traps are received at the end of the interval.

The respective filter rules are established with *Add*.

Note

Always enter the IP address in the case of SNMP traps and syslog events.

3.7 Filter Export and Import

You can export filters individually or in multiples. If there are dependencies that were not factored in when making the selection, a prompt appears before exporting.

Features

- Export
  To start the export function, go to the context menu in the *Event Correlation* window (*Export*). Select a directory for the XML file. The filter configuration is exported using an XML file for a separate profile.
- Import
  Enter this XML file for the import (context menu: *Import*). If a filter number is already allocated, the number of the filter to be imported is, as with copy and paste, increased by 1.

This page is left blank for documents that are printed on both sides.

A Reference

A.1 The Main SAP Documentation Types

The following is an overview of the **most important** documentation types that you need in the various phases in the life cycle of SAP software.

Cross-Phase Documentation

SAPterm is SAP's terminology database. It contains SAP-specific vocabulary in over 30 languages, as well as many glossary entries in English and German.

- Target group:
  - Relevant for all target groups
- Current version:
  - On SAP Help Portal at http://help.sap.com → *Glossary*
  - In the SAP system in transaction STERM

SAP Library is a collection of documentation for SAP software covering functions and processes.

- Target group:
  - Consultants
  - System administrators
  - Project teams for implementations or upgrades
- Current version:
  - On SAP Help Portal at http://help.sap.com (also available as documentation DVD)

The **security guide** describes the settings for a medium security level and offers suggestions for raising security levels. A collective security guide is available for SAP NetWeaver. This document contains general guidelines and suggestions. SAP applications have a security guide of their own.

- Target group:
  - System administrators
  - Technology consultants
  - Solution consultants
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/securityguide

Implementation

The **master guide** is the starting point for implementing an SAP solution. It lists the required installable units for each business or IT scenario. It provides scenario-specific descriptions of

preparation, execution, and follow-up of an implementation. It also provides references to other documents, such as installation guides, the technical infrastructure guide and SAP Notes.

- Target group:
  - Technology consultants
  - Project teams for implementations
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/instguides

The **installation guide** describes the technical implementation of an installable unit, taking into account the combinations of operating systems and databases. It does not describe any business-related configuration.

- Target group:
  - Technology consultants
  - Project teams for implementations
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/instguides

Configuration Documentation in SAP Solution Manager – SAP Solution Manager is a life-cycle platform. One of its main functions is the configuration of business scenarios, business processes, and implementable steps. It contains Customizing activities, transactions, and so on, as well as documentation.

- Target group:
  - Technology consultants
  - Solution consultants
  - Project teams for implementations
- Current version:
  - In SAP Solution Manager

The **Implementation Guide (IMG)** is a tool for configuring (Customizing) a single SAP system. The Customizing activities and their documentation are structured from a functional perspective. (In order to configure a whole system landscape from a process-oriented perspective, SAP Solution Manager, which refers to the relevant Customizing activities in the individual SAP systems, is used.)

- Target group:
  - Solution consultants
  - Project teams for implementations or upgrades
- Current version:
  - In the SAP menu of the SAP system under ▶ *Tools* → *Customizing* → *IMG* ↵

Production Operation

The **technical operations manual** is the starting point for operating a system that runs on SAP NetWeaver, and precedes the application operations guides of SAP Business Suite. The manual refers

users to the tools and documentation that are needed to carry out various tasks, such as monitoring, backup/restore, master data maintenance, transports, and tests.

- Target group:
  - System administrators
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/instguides

The **application operations guide** is used for operating an SAP application once all tasks in the technical operations manual have been completed. It refers users to the tools and documentation that are needed to carry out the various operations-related tasks.

- Target group:
  - System administrators
  - Technology consultants
  - Solution consultants
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/instguides

Upgrade

The **upgrade master guide** is the starting point for upgrading the business scenarios and processes of an SAP solution. It provides scenario-specific descriptions of preparation, execution, and follow-up of an upgrade. It also refers to other documents, such as upgrade guides and SAP Notes.

- Target group:
  - Technology consultants
  - Project teams for upgrades
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/instguides

The **upgrade guide** describes the technical upgrade of an installable unit, taking into account the combinations of operating systems and databases. It does not describe any business-related configuration.

- Target group:
  - Technology consultants
  - Project teams for upgrades
- Current version:
  - On SAP Service Marketplace at http://service.sap.com/instguides

Release notes are documents that contain short descriptions of new features in a particular release or changes to existing features since the previous release. Release notes about ABAP developments are the technical prerequisite for generating delta and upgrade Customizing in the Implementation Guide (IMG).

- Target group:

- Consultants
- Project teams for upgrades

- Current version:
  - On SAP Service Marketplace at http://service.sap.com/releasenotes
  - In the SAP menu of the SAP system under *Help* → *Release Notes* (only ABAP developments)

Typographic Conventions

Example	Description
<Example>	Angle brackets indicate that you replace these words or characters with appropriate entries to make entries in the system, for example, “Enter your **<User Name>**”.
Example → *Example*	Arrows separating the parts of a navigation path, for example, menu options
Example	Emphasized words or expressions
Example	Words or characters that you enter in the system exactly as they appear in the documentation
http://www.sap.com	Textual cross-references to an internet address
/example	Quicklinks added to the internet address of a homepage to enable quick access to specific content on the Web
123456	Hyperlink to an SAP Note, for example, SAP Note 123456
Example	■ Words or characters quoted from the screen. These include field labels, screen titles, pushbutton labels, menu names, and menu options. ■ Cross-references to other documentation or published works
Example	■ Output on the screen following a user action, for example, messages ■ Source code or syntax quoted directly from a program ■ File and directory names and their paths, names of variables and parameters, and names of installation, upgrade, and database tools
EXAMPLE	Technical names of system objects. These include report names, program names, transaction codes, database table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE
EXAMPLE	Keys on the keyboard

SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany
T +49/18 05/34 34 34
F +49/18 05/34 34 20
www.sap.com

This document was created using stylesheet 2007-12-10 (V7.2) / XSL-FO: V5.1 Gamma and XSLT processor SAXON 6.5.2 from Michael Kay (http://saxon.sf.net/), XSLT version 1.

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressly prohibited, as is any decompilation of these components.
Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.

Documentation in the SAP Service Marketplace

You can find this document at the following address: http://service.sap.com/instguides

SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany
T +49/18 05/34 34 34
F +49/18 05/34 34 20
www.sap.com