System Monitoring 7.2 - Setup and Configuration

- Initial Setup
- Content Update
- Setup Managed Systems
- Maintain Custom Templates
- Create Custom Metrics
- Create Custom Alerts
- Configuration Examples
  - Define file system variants for monitoring
  - Monitor OS Processes
  - Custom Introscope Metrics
  - Log Files
  - Custom OS Scripts
  - Custom CCMS Metrics

Initial Setup

Navigate to the Guided Procedure for configuration of System Monitoring in SAP Solution Manager configuration and execute the setup activities.

Entry Point: Starting from the SAP Fiori Launchpad of SAP Solution Manager, navigate to the tile group SAP Solution Manager Configuration and open the tile Configuration (All Scenarios). Alternatively, run the transaction SOLMAN_SETUP.

Navigate to Application Operation > System Monitoring

To set up System Monitoring, you have to follow the steps in the Guided Procedure.

General approach:

- If you configure System Monitoring the first time, start by performing the sub-steps under step 2. These steps only have to be performed in the beginning or whenever changes to the settings configured in this section are required.
- If you want to maintain monitoring templates (e.g. adding or removing new metrics/alerts, changing thresholds etc.), you can start directly with step 4. To activate any changes, continue with steps 5 and 6 afterwards.
- If you want to activate monitoring of a system (or several systems) using already existing templates, start directly with step 5.
Step 1: Overview

This step is the entry point and overview page of the system monitoring configuration. System Monitoring includes technical systems, DBMS and hosts.

The traffic light reflects the current configuration status of the monitoring infrastructure.

Step 2: Configure Infrastructure

In the sub-steps of step 2, you configure the monitoring infrastructure, including important global settings for alerting, housekeeping etc.

Under Steps, you see a list and a status overview of the sub-steps of the Configure Infrastructure step.

Step 2.1: Check Prerequisites

In this step, you use the automatic activities to check the prerequisites for the configuration of the System & Application Monitoring infrastructure.

Step 2.2: Configure Manually

In this step, you perform manual activities to configure the System and Application Monitoring infrastructure.

All activities in step 2.2 are optional. For more information, see the documentation (click on Display). For more information on the activity Extractor Framework see here. The activity Content Customization is used to change the content and appearance of notifications (email or SMS) and the Analysis Report (by default attached to email notifications).
Step 2.3: Default Settings

In this step you can enable or disable certain functions for the System & Application Monitoring on a global level (i.e. these settings affect all alerts from System Monitoring). It is possible to overwrite these settings on the level of templates as well as alerts.

- Incidents: Maintain settings for automatic incident creation in SAP Solution Manager ITSM.
- Notifications: Maintain settings for automatic creation of notifications (email or SMS).
- Third-Party components: Only relevant if the Alert Consumer BAdI interface is used.
- Automatic Alert Confirmation: Alert groups are automatically confirmed when they are ‘closed’ (i.e. when the status of the underlying event changes).

**Caution:** Please be aware that activation of these functionalities by default affects all alerts in System Monitoring. In most cases, it is better to activate them on the level of individual alerts.

Step 2.4: Reporting Settings

In this step, the BI content for BI-based reporting is activated. When entering the step, a health check is executed checking the readiness of the SAP Solution Manager internal BW. Afterwards, you can continue with the BI content activation.

Step 2.5: Housekeeping

In this step, you can specify the lifetimes of the metrics in the BI and the data in the Alert Store and Event Store.
BI retention times: Metrics are stored in BW InfoCubes for different aggregation levels. For each aggregation level, there is a pair of ‘twin cubes’. The time specified is the time interval after which the data loading will be switched from one to the other InfoCube of one pair (see here for a detailed explanation). The retention times are minimum times. Note that this is a global setting and cannot be changed for individual managed objects.

Alert Store housekeeping: You can specify after which time alert groups are confirmed automatically. This is defined as the number of days after the alert group was ‘closed’, i.e. after a status change of the underlying event (red or yellow to any other status). When confirmed, the alert group will disappear from the alert inbox, but can still be found via the Alert Search. Furthermore, you can specify when the alert group is finally deleted (after prior confirmation).

Step 2.6: Workmode Settings

In this step, you configure the standard behavior of System Monitoring, depending on the work mode. The settings affect all metrics and alerts within System Monitoring.

By removing the check mark for any work mode, the monitoring will completely be switched off during the active period of the work mode for any managed object for which the corresponding work mode has been scheduled, i.e. metrics/events will not be updated anymore on the level of the Event Calculation Engine. In particular, no alerts will be generated during that time.

It is recommended to remove the flag for one or several work modes (e.g. Planned Downtime, Maintenance) to be able to have a ‘switch’ available for deactivating monitoring temporarily by scheduling the corresponding work mode for the affected managed object(s).

However, this is a global setting only - if the flag is removed, this setting cannot be overwritten on template/alert level! (Individual metrics/alerts can be deactivated for specified work modes in the templates.)

Warning: Do not remove the flag for No workmode configured - it will deactivate the monitoring for all managed objects for which no work mode has been scheduled!

Content Update
Step 2.7: Update Content

A content version contains SAP monitoring content for all System and Application Monitoring scenarios. When a content version is applied, it updates the content for all scenarios, so this step need not be performed for each scenario separately.

The monitoring content contains monitoring templates (pre-defined lists of metrics/alerts for the different supported technologies) and corresponding data collector templates. When required, SAP publishes a new content. Changes in the new content version can include:

- new metrics/alerts
- changes to existing objects (typically corrections for incorrectly defined metrics/alerts).

New content versions are implemented using the Rapid Content Delivery. This requires - among other prerequisites - connections from your SAP Solution Manager to the SAP Service Marketplace. If your security policy does not allow this, it is also possible to download the content and apply it manually in your SAP Solution Manager.

There is no recommended strategy how frequently to check for a new content version and apply it. In general, content updates are not required as long as monitoring is working. A content update should be performed before starting to create custom templates for System Monitoring. Sometimes new metrics/alerts are shipped with a content update; in case you want to make use of the latest innovations, a content update needs to be performed. You may also be asked by SAP support in a customer incident to apply the latest content.

The new or changed monitoring settings are not automatically active. However, whenever you activate monitoring for one or several systems, the new content version will be used for the managed objects affected. Consequently, the monitoring could theoretically behave differently than before. This is also the case if you are using custom templates, because all objects (metrics/events/alerts) which have not been changed are just referencing to the SAP delivered templates! All changed objects, however, are not affected by the content update. You can also copy objects to the customer namespace by deliberately changing settings (see the section about template maintenance below) if you want to protect them against unwanted changes triggered by content updates. A possible side effect could be that you get new alerts.

See also KBA 2213849 - OSS Connection Issue when Updating Solution Manager Technical Monitoring Content.

Setup Managed Systems

Step 5: Define Scope

In this step you select the managed object you want to configure for system monitoring. Without selecting a managed object you cannot proceed to the next setup steps.

Please note that selecting a managed object and configuring monitoring (in step 6) creates a so-called entry point. If you select a technical system in step 5, a corresponding entry point will be created for this technical system, and System Monitoring will be activated for all associated managed objects (including technical instances, database and hosts). This allows you to remove monitoring for the whole entry point in one go, if required. If you would select an additional managed object for the same technical system, e.g. the database under the Databases tab, an additional entry point would be created, and removing the monitoring for the technical system would not remove the monitoring for the associated database (and the database host), because they are part of a different entry point. Hence, it is recommended to always select the technical system on the Technical Systems tab. In particular, databases and hosts should only be selected in step 5 in the case of stand-alone databases or stand-alone hosts.
**Step 6: Setup Monitoring**

In this step monitoring templates will be assigned to the managed systems in scope.

Each technical system is associated with several managed objects (e.g. technical instances, database(s), database instances, database replication group, hosts), which logically form a hierarchy below the technical system level. This hierarchy is pulled from the LMDB and displayed in step 6. Note that the assignment of managed objects to the technical system cannot be changed in step 6. If any wrong information is displayed here (e.g. outdated or missing technical instances etc.), the root cause is to be searched on LMDB/SLD level (e.g. data supplier not updating the information).

Based on the information about installed products as maintained in the LMDB, default templates are automatically assigned to the different managed objects. The current assignment can be seen in the column **Assigned Templates**. The assignments can be changed per managed object and per product via **Assign Templates**. Only templates matching the corresponding product (either the SAP delivered standard template or corresponding custom templates) can be assigned. Per product, only one template can be assigned at the same time.

After verifying the correct assignment of templates, click **Apply and Activate** to write the monitoring configuration to the directory tables and activate monitoring. This is required after each change within an assigned template or in case the template assignment was changed. Depending on the number of selected systems, the activation may take few seconds until several minutes.

The **Assignment Status** column shows if the settings according to the assigned templates are active (green) or if a further activation via **Apply and Activate** is required (yellow).

Via **Maintain MO-Specific Settings**, you can overwrite template settings (e.g. threshold values) for individual managed objects. However, it is not possible to change template assignments for the managed object without discarding the managed object specific settings. The **Directory Browser** allows to access the configuration in the Alerting Directory to check details of the currently active configuration.

**Step 7: Complete**
The System Monitoring setup is completed for the managed systems in scope. In this step the status of all previous steps of the configuration is displayed.

Maintain Custom Templates

When configuring System Monitoring following the procedure described above, it is important to consider whether the assigned monitoring template is sufficient to reflect your monitoring requirement. SAP has provided various monitoring templates over the past years to cover a wide range of products adopted by the most customers. These SAP provided monitoring templates is delivered within the component ST-CONT (details see the section Content Update) and contain the definitions of the metrics, events, and alerts as well as the details of settings such as the assigned threshold value, which can be found under Step 4 - Template Maintenance of the System Monitoring Guided Procedure.

The following example shows the view under Step 4 - Template Maintenance. There are multiple monitoring templates listed under the corresponding managed objects (e.g. technical instances, database(s), database instances, database replication group, hosts) under the Templates menu at the left hand side of the screen. For instance, under the managed object Database, the monitoring templates for HANA, Oracle and Sybase databases etc. are available. When double-clicking any of these templates, the detailed view is displayed at the right hand side. All the metrics, alerts and their setting details can be checked here.

Nevertheless, it is easy to identify that the already activated metrics or alerts cannot be deactivated or the assigned threshold value cannot be modified anymore (all settings are greyed out), which is made by design. These predefined SAP delivered monitoring templates are called as the standard templates. Of course, standard templates alone could not fulfill the customer's monitoring requirement, considering the fact that each customer has own preferred set of metrics and also it can vary depending on the system role (e.g. production or development system). Therefore, we SAP come up with the concept custom (monitoring) template and each customer can flexibly define own preferred set of metrics in it.

The custom template can be created conveniently by copying the standard template. The user needs to first mark the corresponding standard template and press the button Create Custom Template.
Once the button is pressed, the newly created custom template will be listed under the standard template with the icon in front and its details will be shown in the template details view at the right hand side. The default name of the custom template is always “Derived from <Name of the Standard Template>” and it can be changed according to the own preference under the tab Template Settings in the template details view. It is important to think about a meaningful name for the custom template, for instance, a suffix “PROD” or “DEV” etc. can be attached to differentiate the monitoring template assigned to production or development system later on. In this example, we named the custom template “Test_SAP HANA DB_DEV”.

It is recommended to press Save button to persist the changes before going further. When saving the template, a pop-up will show up to ask for package assignment, which prepares for the possible transportation in the future, since the monitoring templates can be transported. Please press the OK button after specifying the preferred package.

Similar to the default settings as written in the above section Step 2.3, it is possible to configure incidents, notification and third-party settings respectively under the tab Incidents, Notification and Third-Party Components in the template details view. For example, a distribution list (DL) can be maintained under the notification settings so that the members of the DL could receive email notification when there is any alert involved in this template is triggered.

In the next step, the user can define the monitoring metrics and alerts according to own requirement. So far the custom template still persists the group of metrics and alerts as well as their settings copied from the standard template and they can be viewed under the tab Metrics. All the
Metrics included in this template are displayed in a scrollable table under the tab Metrics. The user can scroll up and down to check the metrics. What is important to mention is that it is highly recommended to apply Expert Mode to work with the metrics and alerts. The Expert Mode can be entered via pressing the button Expert Mode at the top right corner.

After applying the Expert Mode, more information can be accessed such as metrics, events and alerts hierarchy as well as data collection and usage details of each metric. Depending on own requirement, the user can activate or deactivate the metrics flexibly via checking or unchecking the checkbox under the column Active. Moreover, the metric settings such as the threshold type and value of the metric can be adjusted in the metric details view underneath the metrics table.

To name an example, the metric “Memory Usage of Main Storage of Column-Store Tables” is about checking the main store memory usage of the column tables, as described under the Overview tab in the metric details view. Additionally, when selecting the Threshold tab, all the threshold related settings of the metric can be checked. The threshold type of the metric “Memory Usage of Main Storage of Column-Store Tables” is set to be Numeric Threshold (Green/Yellow/Red). The threshold value is set as such that when the memory usage of the column-store tables equals or exceeds 25% of the main store memory, a yellow alert will be triggered and when it equals or exceeds 30%, a red alert will be triggered.

Once the metric is modified, the column Modified will be checked, which means that the original metric settings copied from the standard template is overwritten. Correspondingly, a new metric ID distinct from the original ID will be generated for the modified metric, which can be checked under the tab Others in the metric details view.

Apart from the individual metrics, the user can also define the preferred set of alerts and the following activities such as creating email/SMS notification and raising incident under either the tab Alerts or the tab Metrics, Events, Alerts Hierarchy. The alerts can be activated or deactivated in a similar manner by checking or unchecking the checkbox in the column Active. In addition, the incident and notification settings can be configured for each alert under the tab Incidents and Notifications respectively in the alert details view. The idea behind is that an incident or a email/SMS notification can be generated on the occurrence of the specified alert. Third-Party component settings is also possible, which enables the alert forwarding to the third party component. The incidents, notification and third-party component settings in this alert level overwrite the settings in the template as well as global level as stated in the above section Step 2.3.

What’s more, compared to the tab Alerts, the logical relationship among metrics, events and alerts can be viewed under the tab Metrics, Events, Alerts Hierarchy, for instance, the metric “Memory Usage of Main Storage of Column-Store Tables” composes the event with the same name and
this event corresponds to the alert "Memory Usage of Main Storage of Column-Store Tables". An event can consist of multiple metrics (1:n), however, and only relates to an alert (1:1). This relationship introduced along with the Monitoring and Alerting Infrastructure (MAI) enriches the semantic meaning of the alerts and the user can either activate all the metrics belonging to one alert or just activate a few in the scrollable table under the tab Metrics, Events, Alerts Hierarchy. After specifying the required metrics and alerts as well as configuring the necessary incident, notifications and third-party component settings, the custom template should be ready.

So far we discussed about creating custom monitoring template via copying the standard template. It is also possible to create custom template via copying already existing custom template. The procedure is similar and the difference is to mark the to be copied custom template and press the button Copy Custom Template instead of the button Create Custom Template. It fully depends on the user’s requirement to decide how to create own custom template and the two methods will not influence the way to work with the metrics and alerts etc.

Create Custom Metrics

Custom metric is supported in case the SAP delivered standard metrics could not satisfy the user needs. This section explains how you can create a custom metric in a custom template.

- Navigate to a custom template
- Change to Expert Mode
- Press the button Create and select Metric from the drop-down list. Afterwards, the Custom Metric Creation Wizard shows up at the right hand side. The Custom Metric Creation Wizard consists of two major steps, namely Specify Metric Attributes and Assignments. In the first step Specify Metric Attributes, the user should enter the details of metrics such as metric name and type and, more importantly, determine how the data can be collected (data provider, parameter, collection interval etc.). Then in the step Assignments, the user needs to specify the alert, to which this custom metric is assigned. The custom metric can be either assigned to a already existing standard alert or also to a custom alert.

- Fill in the name, category, class, data type and technical name for the custom metric under the Overview tab. The user can give a meaningful name to the custom metric and select a category out of the pre-defined categories Availability, Performance, Exceptions, Configuration and Self-Monitoring. The first four categories are self-explained and the Self-Monitoring category deals with the monitoring of SAP Solution Manager itself such as Monitoring and Alerting Infrastructure (MAI) and Extractor Framework. Next, the user can specify the class as either Metric or Metric Group, depending on whether the data provider returns more than one value. The data type is used as usual and can be selected among String, Floating Point and Integer. It is also required to enter a technical name, with which the metric can be checked easily, for instance, in the Alerting Directory. Lastly, do not forget to check the checkbox Active so that the metric can be used in the next step.
Select the required data collector from the list of provided data collectors and enter the parameter value. In this example, it is intended to search any warning messages in the dev_icm log file. More details about the usage of data collector File Text Pattern Search can be found in SAP Note 2257249.

- Define the threshold for alerting
Assign the custom metric to an alert. Since in this example, we want to assign this custom metric to a custom alert later on, the assignment here is left empty.

Lastly, click Finish button to complete creating the custom metric.

Do not forget to press Save button to persist the changes made in the custom template before going further. Consequently, the newly created custom metric can be found in the table of metrics under the tab Metrics. It is easy to find out that the checkbox under the column Custom-Created is checked, which indicates that this metric is not SAP delivered standard metric but a custom-made one.

In the next section, we will exemplify how to create a custom alert.

Create Custom Alerts

- Navigate to the custom template
- Change to Expert Mode
- Press the button Create and select Alert from the drop-down list. Then the Custom Alert Creation Wizard shows up at the right hand side. Like creating a custom metric, the Custom Alert Creation Wizard also consists of two major steps, namely Specify Alert Attributes and Assignments. In the first step Specify Alert Attributes, it is required to enter the alert name and category etc. and also configure the following activities when the alert is triggered, e.g. creating an email notification or raising an incident. Subsequently, in the step Assignments, the alert needs to be linked to a custom metric.
• Define the alert name, category and severity etc. under the **Overview** tab. The name should be given in relation to the name of to be assigned custom metric. Likewise, the category should be exactly the same as the category of the to be assigned custom metric. Severity determines the priority of the alert and it varies from 0 (very low) to 9 (most critical), which can be selected according to the organizational requirement. Do not forget to check the checkbox **Active** so that the alert can be monitored when applying the template.

• The incidents, notification and third-party components related settings can be configured under the respective tabs as described in the section **Maintain Custom Template**, if necessary.

• Specify the event rule, which will be applied for the custom alert and metric. The event rule serves for the calculation of the ratings for the event so as to decide whether or not to trigger an alert. For instance, an event is constituted of three metrics and two of them have green ratings but one has red rating. In this case, if the Worstcase Rule is applied, the event will get a red rating and thus trigger an alert. Otherwise, the event will get a green rating and no alert will be triggered.
Assign the previously created custom metric to the custom alert and click Finish button to complete wizard.

Do not forget to press Save button to persist the changes made in the custom template. Afterwards, the newly created custom alert and metric can be found under the tab Metrics, Events and Alerts Hierarchy. Like the case in the custom metric, the checkbox under the column Custom-Created is checked both for the custom event and alert.

Once the custom template including the custom metric and alert is assigned to the monitoring object, the corresponding monitoring data can be received and displayed in the System Monitoring.

**Configuration Examples**

**Define file system variants for monitoring**

A common requirement is to monitor either the free or the used space per file system, where only certain file systems have to be monitored or - the other way around - certain file systems need to be excluded from monitoring. Furthermore, different threshold values may apply to different file systems. In general, there are two ways to achieve this:

1. If you have many different thresholds for the different file systems, especially also if the thresholds depend on the managed object (host) or you have different file systems with different requirements and the template approach is hence not practicable, it may be better to use Advanced Monitoring.
2. In case you have basically the same requirements on several managed objects, it is possible to maintain this in the corresponding host templates (Linux, Windows, ...). This is described in the following.

The idea is to use a metric group instead of a metric. This has two advantages: (a) You can maintain several variants, reflecting different requirements (e.g. thresholds), and (b) you can use regular expressions to define file systems to be covered by each variant; all file systems which match the regular expression will be returned dynamically by the data provider, and for each one a separate metric will be created.

The metric groups required are already contained in the SAP standard templates (host templates), e.g. File System Used (%), and usually they have a standard variant ‘.*’, i.e. all file systems are covered (with the same threshold). In your custom templates, you can add your own variants within these metric groups. **Attention:** If a file system name matches the regular expression in more than one variant, several metrics will be created for the same file system (potentially with different thresholds)! In particular, don’t forget to deactivate the standard variant ‘.*’ if you have created your own variant(s) - this is often forgotten and leads to a common ‘issue’ of duplicate metrics.

**Example:**

Go to your custom template and select the metric group for the file system monitoring you want to change. Switch to Expert mode and create a new metric variant by clicking the button Add Variant.
Enter the regular expression to identify the file system(s) in the Filesystem column. In the example we use `^(!/*media).*$` to exclude file systems that start with `/media` (i.e. the variant will return all other file systems).

Save your template. Verify that only the custom variant is active.

When you select the line corresponding to a variant, you can change the threshold of this variant. Otherwise, the threshold of the metric group is
The main difficulty is finding the regular expression. Here are some examples:

- One particular file system (Linux/Unix): /oracle(.*)(* (monitor file system /oracle)
- A range of file systems (Windows): [C-F].* (monitor file systems C to F)
- Exclude a file system (Windows): [^D].* (monitor all file systems except D)
- Exclude all file systems that contain sda or sdb or sdc: .*(?sda|sdb|sdc).*
- Exclude two file systems /media and /scratch: ^!(?!MEDIA.*)(?!/scratch.*)*$

See also SAP Solution Manager 7.1 document: Template Maintenance - File System Variants.pdf

Monitor OS Processes

The preferred way of monitoring OS processes is using the data collector **SapHostAgent GetProcessInfo**. When creating a custom metric, you have to select the Data Collector Type **Diagnostic Agent (push)** and the Data Collector Name **SapHostAgent GetProcessInfo**. Of the available data collector parameters you have to maintain NAME and KEY_FIG. NAME is the process name pattern as a regular expression, KEY_FIG provides a drop-down selection of the available key figures including Number of processes, Total CPU Time (%), Total Memory (KB), Total Memory (MB), Total Priv Pages (KB), and Total Priv Pages (MB).

More details can be found here.

An alternative way for older SAP Solution Manager releases using the CA Introscope EM can be found here: OS Process Monitoring

Custom Introscope Metrics

Even though the content of the SAP delivered templates in the Monitoring and Alerting Infrastructure (MAI) is based on the proven best practices for technical monitoring, from time to time customers miss metrics they consider necessary for their customer-specific monitoring. Also the integration of 3rd party monitoring can be based on the metrics for the 3rd party system monitored in CA Introscope. Thus, it is possible to create custom metrics and alerts out of the metrics available in CA Introscope Enterprise Manager (EM) but not in the SAP delivered templates.

Please refer to the following Wiki Page for the detailed description: SAP Solution Manager 7.2 - non-SAP Monitoring Custom Introscope Metrics

See also Solution Manager 7.1 Document: How to create custom Introscope metrics

Log Files

There are several data providers available for monitoring log files. They are described here: Log File Monitoring Data Provider

Example:

A very flexible data provider is **File Text Pattern Search**. Please note that for FOLDER you have to specify the absolute path to the file without any wildcards. However, you are allowed to use variables. Hint: Collector parameter variables in the context of a managed object are listed in the Alerting Director Browser (can be accessed via transaction MAI_TOOLS). For the parameters FILEPATTERN and SEARCHPATTERN regular expressions are allowed.

The data provider returns the number of matches of SEARCHPATTERN found in all files matching FILEPATTERN - either as delta since last data collection, or the total, to be controlled via the parameter DELTA_READ.
Custom OS Scripts

The Remote Operating System Script Collector (ROSSC) allows you to integrate custom monitoring scripts (OS commands) in the SAP Solution Manager Monitoring and Alerting Infrastructure (MAI). This is useful if you have, for example, created scripts to monitor the availability of databases or network connections.

The OS script is executed by the Diagnostics Agent. A data provider Remote OS Script is available for creating custom metrics. You have to specify the script name, the command option string (optional) and the return type (default is String). The prerequisite is that the script has been stored in a dedicated folder on the managed object host and that the activation steps in the Agent Administration have been performed.

Custom CCMS Metrics

See also Solution Manager 7.1 Document: How to create custom CCMS metrics

See the SAP Help section for a detailed description of how to include CCMS MTEs into MAI based monitoring: https://help.sap.com/viewer/c413647187a54db59d18cb074ce3dafd/7.2.05/en-US/c53dae540a53a427e10000000a441470.html

Some examples can be found here: https://help.sap.com/viewer/c413647187a54db59d18cb074ce3dafd/7.2.05/en-US/89e4b854fda16874e10000000a44538d.html