Implementation Methodology

System Monitoring
Design Operations

Dietmar-Hopp-Allee 16
D-69190 Walldorf

CS	STATUS
customer	published
DATE	VERSION
April 2009	3.0

Table of Contents

1 Management Summary

1.1 Overview of Current Methodology

System monitoring describes a concept to monitor key figures for performing a qualitative and quantitative assessment of system operation. The main focus is set on a proactive monitoring, that is a preventative solution monitoring to prevent incidents. This contrasts with the reactive monitoring and analyses using monitoring methods, which is triggered when an incident occurs. The objective is to ensure system availability, stable operation and performance stability. Proactive monitoring is based on reporting of historical developments and trends. This can be automated to a certain degree.

The aim of the design phase is to verify existing process to be monitored, define KPI's and threshold for the monitoring itself. Apart of this clear roles, responsibilities and auto reaction tasks needs to be defined.

This implementation methodology should be regarded in conjunction with the implementation methodology for the other phases *Setup and Operations* and *Optimization* phase.

1.2 Run SAP Implementation Methodologies

As IT landscapes grow and solutions become increasingly mission-critical, the cost of successfully operating an IT landscape becomes a key business issue. To optimize operations and to reduce cost SAP has harnessed its experience with thousands of customers and created:

- *SAP Standards for End-to-End Solution Operations* that span customers' mission-critical operations landscapes and aim at reducing the risk of failure and increasing the skill base
- Run SAP, a robust operational methodology that underpins these standards and complements SAP's implementation methodology AcceleratedSAP (ASAP)
- *SAP Enterprise Support*, a support offering that enables *SAP Standards for End-to-End Solution Operations* at lower total cost and across mission-critical support systems

2 Design Operations

2.1 Goal of the Design Operations Phase

In this phase the operations processes are designed. Based on the results of scoping you should analyze the existing operations processes, the current toolset and also the possible interdependencies of the new processes.

A blueprint should be produced for the processes and the usage of the tools. Adjust the *SAP Standards for End-to-End Solution Operations* to the needs of the organization. Determine the tools to be used in the future.

You should plan the testing of new operational processes at this early stage of your project.

The goal is to set up a technical monitoring concept that is central, proactive, and automated:

- Central: A centralized monitoring approach simplifies both setup and day-to-day operations. Logons to the faulty component can be prevented if the problem can be rectified using the information stored in the central system.
- Proactive: Preventative solution monitoring detects problems right from the outset. In this way, severe disruptions to system operations can be counteracted in advance.
- Automated: Automated monitoring can respond quickly and reliably. It also reduces operating costs.

Dependencies on all other topics, especially the following will be put in place

- Incident management: occurrence of incidents prevented by automatic surveillance of the respective systems and interfaces
- Interface monitoring: monitoring of threshold values is essential for business process-oriented monitoring
- Root cause analysis: makes extensive use of System Monitoring information
- System administration: Administration-related decisions based on monitored data
- Business process and interface monitoring: which comprise the *Alert Management* (ALM) An alert is a notification informing its recipients that a critical or very important situation has arisen.

2.2 Requirements and General Conditions for the Design Operations Phase

You should not start the *Design Operations* phase without having created the following deliverables during the *Assessment & Scoping* phase:

- Collection of business and technical requirements
- Scope that is confirmed with all stakeholders
- Analysis of possible influences of the operational infrastructure
- Evaluation whether organizational changes are needed

2.3 Essential Resources for the Design Operations Phase

Before you start the *Design Operations* phase, make sure you have all resources with the required skills in place. In case of deficits, use trainings, help portal resources and books referred under accelerators. To ensure a successful design multiple teams with different roles like strategist, component expert and generalist need to run their activities in accordance with the corporate strategy, corporate policies, and the goals of their organizations. Efficient collaboration between these teams is required to optimize and ensure the efficiency of system monitoring.

You will need in-depth knowledge of existing relevant processes and toolset as well as skills in process modeling and conception.

2.4 Key Deliverables of the Design Operations Phase

After successful completion of the *Design Operations* phase you should have a confirmed concept for all *E2E Solution Operations* processes. The concept should comprise detailed process descriptions including process steps as well as the technical design.

Deliverables

- Defined and verified processes (alert handling, escalation)
- Defined key performance indicators (KPIs) with reaction methods
- Defined threshold for the KPI's
- Clear tasks, roles, responsibilities and contact persons within the process e.g. alert handling
- Defined dependencies on and interfaces to other processes
- Defined service level definitions which might result in a service level agreements (SLAs)

2.5 Process Description

2.5.1 Process goal

The system monitoring standard covers monitoring and reporting of the status of IT solutions. The business unit expects that performance problems and errors are detected proactively and resolved before they affect business continuity. To provide transparency to the business units, customer IT has to report service levels, capacity trends and solution quality on a regular basis. In order to fulfill the demand of customer business given a limited IT budget, the customer IT must industrialize and automate monitoring and reporting for the solution. In the design phase process the needed information has to be collected to ensure a smooth setup-phase. This information comprises the KPI's, threshold values, auto-reaction methods.

2.5.2 Process steps

2.5.2.1 System monitoring

The process steps are split into alert monitoring and IT reporting steps because there are using different constraints.

Alert monitoring

1. Define and verify parts of solution landscape, which needs to be monitored
2. Define KPIs that are relevant for alerts and ad-hoc monitoring. In order to do this the Run SAP methodology provides a monitoring template.
3. Check SAP default threshold values for these KPI's and analyze customer specific need to change the default values.
4. Review the documentation for these KPIs. instructions must be compiled as to how to handle exceeding thresholds.
5. Review the assigned analysis methods for these KPIs.
6. Author actions can be defined and assigned. Automatic notifications and execution of operating system commands are particularly significant here.

7. Define alert handling and escalation paths
8. The roles and work centers must be assigned and the central alert inbox should be build up.
9. Reporting

The reporting part of system monitoring covers several steps of report creation. The individual processes are described below:

IT performance reporting

Parts of IT performance monitoring process are:

- Analyze the performance history
- Verifying whether target performance levels were met in past periods
- Check historic metrics that you are able to fine-tune monitoring threshold values for meaningful alerting
- Analyze trends and anticipate bottlenecks (for example, the growth of a database), so you can take preventive measures
- Use it as a basis for a capacity planning and resources optimization
- Use it as a basis for performance tuning

EarlyWatch alerts

The *EarlyWatch* process contains 5 steps (figure 1):

(1) Data collection

EWA contains defined data which will be collected and send to *SAP Solution Manager* on customer side.

(2) Implement own recommendations

Customer side checks the EWA Report and implements recommendations if needed.

(3) Data forwarding

The data is forwarded from the SAP customer system to SAP at regular intervals via the remote connection.

(4) Data analysis, customer contact

SAP analyses this data and provides a clear overview of the results in a report which can be downloaded from *SAP Solution Manager*.

(5) Implement SAP recommendations

SAP recommendations can be implemented on customer side.

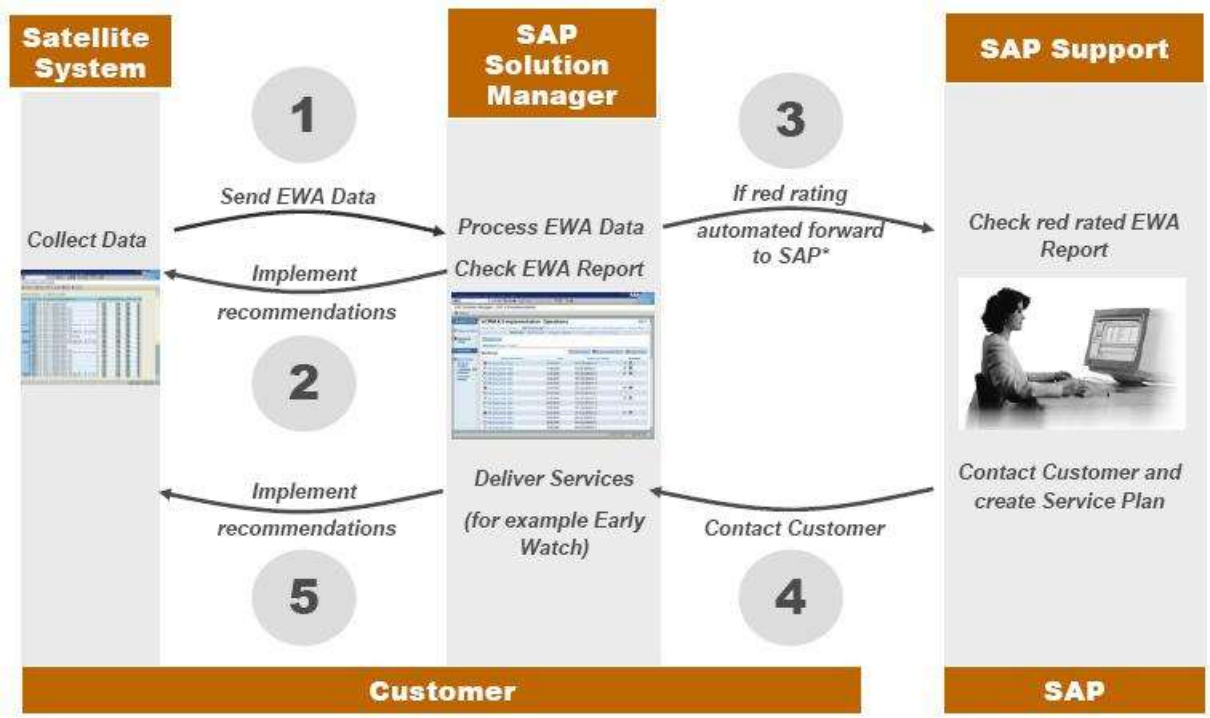

Figure 1: EarlyWatch alert process

Service level reporting

The SLR process contains 5 steps:

(1) A *Service Level Agreement* is defined between you and an IT organization. It covers:
- Your IT service quality requirements, for example performance and security
- Unambiguous and measurable service targets
- Communication structures

(2) Report types. Service level report types are templates for service level reports. The service level report types specify the contents and scope of the service level report.

(3) You specify the scope of the service level reporting, e.g.:
- Which business processes and which systems in your solution are analyzed
- Which checks and alert thresholds you require
- How the information is presented in the reports
- Report types

(4) The system creates the relevant service level report sessions, which you can process, to change details or add further information.

(5) You send the service level report to the responsible persons.

2.5.3 Process Requirements

Availability of all stakeholders from the IT department, the business units, and all potential corporate units affected by the processes.

2.5.4 General conditions

Reporting:

Before you can start with the *Setup* phase you have to define the following:

- Relevant content (KPIs) of the Service Level Reporting (business need)
- Frequency of the SLR
- Relevant people for the setup and operations steps
- Definition of the interfaces (organizational and technical)
- Relevant systems and solutions (that will be analyzed in SLR, EWA)
- In case of SLR: system availability (ST03 based or the recommended CCMS-ping based)
- General content of the service level reports (tables, graphics)
- Report customization (appearance)

System Monitoring:

- Basis setup of all the systems is needed.
- All monitored systems should be assigned to the central monitoring system

2.5.5 Organization (roles)

The IT processes run across the organization hierarchy. This works only if tasks and responsibilities are described clearly, therefore it is useful to develop a role concept. In smaller IT organizations the roles can also be combined.

2.5.5.1 Strategist

- Modifies, implements, and integrates specific support tools
- Plans and coordinates the exchange of technical components
- Covers the corporate strategy and corporate policy also PMO standards should be taken into consideration

2.5.5.2 Component expert

- Has technical, detailed knowledge of individual components
- Evaluates KPIs for specific components and customer-specific developments

2.5.5.3 Generalist

- Acts as an intermediary between solution and technology
- Integrates the monitoring process into the whole solution
- Localizes the root cause of an incident in the solution landscape
- Is able to make qualitative statements about the solution landscape

2.5.5.4 System administrator and customer development

System monitoring covers typically several systems from various areas (e.g. CRM, R/3, XI, BW) and from different vendors. For each involved component detailed technical knowledge is required.

2.5.6 KPI definition

To assess the quality of the process, clearly defined indicators and measurable objectives are required. The performance indicators should be collected and evaluated in regular reports. The historical data that is created in this way, can be used to identify mid- or long-term trends and derive the necessary measures.

Setup a procedure to check the KPI's frequently and check whether they need to be changed or adjusted.

These measured values could include (see table 1):

- Availability
- Performance
- Utilization capacity
- Except situations
- Security

Category	Specification	Proposed Threshold Value
Availability	Heartbeat of a technical component	A missing heartbeat signals a failure of the technical component
Performance	Average general response time	Empirical value based on the standard response time. Above-average deviations should be signaled
	Response times of particularly important subcomponents or actions	The KPI values that endanger core business processes should be used as threshold values
Utilization capacity	Hardware: CPU, I/O, memory, operating system	
	Application: Memory, processes	
	Processing queue: Overflows	
Exception situations	Terminations of processing steps, such as short dumps or exceptions	
Security	Unauthorized access or frequently failed access	
	Users with security-relevant authorizations	
	Super user access	

Table 1: KPI categories

2.5.7 Alert handling

Alerts are a key element of automatic monitoring. They quickly and reliably report errors – such as values exceeding or falling below a particular threshold value or that an IT component has been inactive for a defined period of time. These alerts are displayed both in the alert inbox of the system monitoring work center and in the native CCMS alert browser. If an alert is triggered in *Alert Management* (ALM) responsible or interested parties are identified and are informed about the situation by the immediate sending of alerts. Important is to define who needs what kind of alerts by which medium (mail, fax, phone call).

ALM is a business alert delivery infrastructure, which offers personalized alert settings, rule-based determination of recipients, and fast alert delivery. Note, that the use of ALM in the context of technical CCMS alerts is optional and need to be configured independently of the CCMS. In comparison to the ALM the CCMS provides a standard auto reaction method to trigger an alert handling. More information are provided in the accelerator under *Selected Alert Monitor Methods*.

Based on alerts it is important to define escalation paths to address critical situations to the right people.

2.5.8 Tools to support the process

IT performance reporting

IT performance reporting displays the development of the most important monitoring data in the managed systems, to identify potential problems as early as possible, and give an overview of the load and performance of the systems. The reports contain various periods, from the current day to the previous year, so you can see both the current, and the long-term development of the performance values. The values for each period are displayed in the appropriate level of detail.

Note, that *Central Performance History* (CPH) is no longer needed for this functionality. The new Extraction Framework is used for pushing the data in the BI. No more process chains are required. See the accelerator “Development News SAP Solution Manager 7.0 EHP 1” for detailed information.

EarlyWatch Alert

The *SAP EarlyWatch Alert* is a diagnosis which monitors SAP systems in the *SAP Solution Manager*. The *SAP Solution Manager* processes the data, which is downloaded from the monitored systems. You can display the report as HTML document or create a *Microsoft Word* document. You can use the documents as status reports and analyze them to avoid potential problems with these reports.

Service Level Reporting

The service level reporting exploits the EWA, BPM, local and remote CCMS, as well as local and remote BI as data sources for producing solution-bound service level reports. Systems, business processes, content and time horizon of each service level report can be customized by the user in the setup service level report workbench of the *SAP Solution Manager*.

Service level reporting enables the possibility to optimize and simplify mid- and long-term reporting as well as to fulfill internal and external *Service Level Agreements*.

CCMS monitoring

SAP's CCMS monitoring infrastructure, part of any *SAP NetWeaver* installation, gives you the possibility to centrally monitor any SAP environment – from individual systems, through networked SAP solutions, up to complex IT landscapes incorporating several hundred systems. It can be used immediately after installation. You can easily extend the infrastructure to include SAP and non-SAP components. For more information please see the accelerator for the topic central monitoring with CCMS.

Manual monitoring tools

Category	Work Center	Tool
Availability	System monitoring → Overview	
Performance	System monitoring → Proactive monitoring	*Transaction ST03 E2E Trace* *E2E Workload Analysis*
Utilization capacity	System monitoring	*Transactions OS06, ST04, DB50* *E2E Workload Analysis*
Exception situations	System monitoring → Alert inbox	*Alert Inbox Transaction ST22,* *E2E Exception Analysis,* *Log Viewer*
Security	System administration → User administration	*Security Audit Log SM20, System Log SM21* *Application Log* *Further Logs and Traces*

Table 2: Manual monitoring tools

2.5.9 Process output

The result is a comprehensive monitoring concept that proactively checks the components of the landscape covering all the managed infrastructures such as ABAP, Java and .Net as well as unmanaged infrastructures as native components. When problems occur, the persons responsible are notified automatically and alarms are displayed centrally. From here, further analysis can be carried out with direct access to root cause analysis or the service desk if necessary.

Reporting usage will enable a continuous improvement and a better planning based on statistics provided by IT performance monitoring. Furthermore, analyzing reports allows the company to check if a certain service level was met or not.

Index of Figures

Index of Tables