Automating ITIL v3 Event Management with IT Process Automation: Improving Quality while Reducing Expense

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for NetIQ

November 2008

Automating ITIL v3 Event Management with IT Process Automation: Improving Quality while Reducing Expense

Table of Contents

Automating ITIL v3 Event Management with IT Process Automation: Improving Quality while Reducing Expense

Abstract

IT organizations around the world are improving their IT operations capabilities by implementing the Incident and Problem Management processes from the IT Infrastructure Library (ITIL). Yet while the majority of those organizations are focused on ITIL v2 process adoption, the ITIL Event Management process is not introduced until ITIL v3.

Event Management can – and should – be used along with Incident and Problem management, regardless of ITIL version

Fortunately, Event Management can – and should – be used along with Incident and Problem management, regardless of ITIL version. The foundation it provides for improving other ITIL processes, as well as its potential for cost savings, positions Event Management as a critical process for organizations at any stage of ITIL adoption.

This paper introduces ITIL v3 Event Management principles, related activities, and typical challenges. It then discusses how to resolve those challenges using best practices as well as IT Process Automation (ITPA). Automating the process of Event Management with ITPA lowers IT costs by reducing manual labor. This approach also improves quality by ensuring rapid and consistent incident resolution.

A complete Event Management solution from NetIQ®, including automation, is also explored. NetIQ® AppManager® and NetIQ® Aegis™ provide broad event monitoring as well as automation through both event correlation and ITPA. A real-world scenario for automating Event Management using these products from NetIQ is introduced.

Introduction

ITIL provides a framework of best practice guidance for the management of IT. However, rather than the traditional focus of IT on technology management, ITIL recognizes the IT organization as a provider of services. An IT service, such as email or Internet access, provides the means of delivering value to users without the need to be aware of, understand, or worry about the underlying technology or management processes.

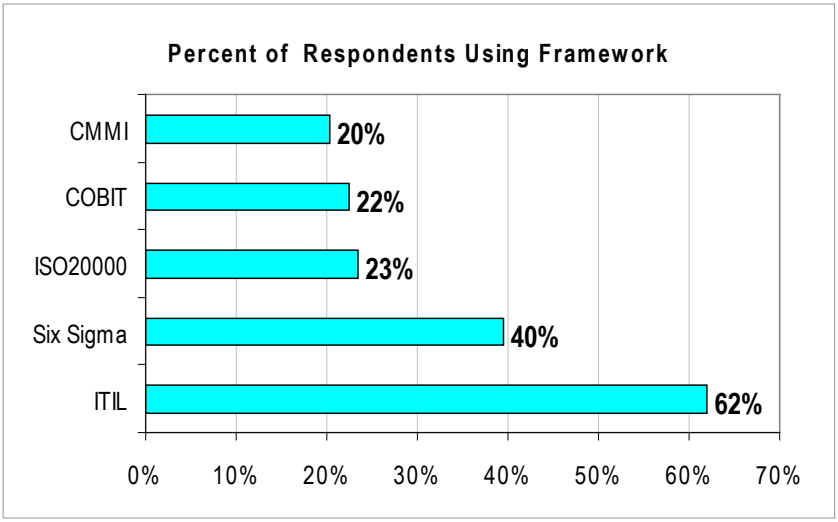

Figure 1 - Best Practice Framework Adoption

Now in its third version, ITIL has become the most widely adopted best practice framework for IT management throughout the world. Based on EMA research, Figure 1 illustrates the rate of adoption of ITIL versus other frameworks.

Each version of ITIL has improved over its predecessor and a key improvement in ITIL v3 is the addition of a Service Lifecycle that includes five stages: Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement.

It is the Service Operation book that describes the best practice processes used to manage the applications and infrastructure that support the delivery of services. It is during this stage of the lifecycle that services actually deliver their value.

The IT operations staff must ensure the value of those services is delivered to the funding organization and its users by managing their health from end to end. Of course, this does not happen without challenges. There are many tradeoffs – whether tactical, strategic or economic – within any IT organization. Decisions must be made carefully around reactive versus proactive management, quality versus cost, and levels of staffing versus automation, especially during times of tightly constrained budgets.

The ITIL v3 Event Management process serves as a case in point for the challenges involved with IT operations

The ITIL v3 Event Management process serves as a case in point for the challenges involved with IT operations. It is vital for ensuring the operational health of services, and there are a number of critical decisions to make so it can be done cost-effectively and with high quality. Strangely, there was no specific Event Management process in ITIL v2. Now, with ITIL v3, the Event Management process is clearly articulated in the Service Operation book and is instrumental in delivering agreed levels of service. Many of the other twenty-six ITIL v3 processes also benefit from integration with the Event Management process.

ITIL v3 Event Management

ITIL v3 defines an event as a change of state that has significance for the management of a configuration item or IT service. This definition is intentionally quite broad since it is used to describe a practically unlimited number of scenarios. Some events simply indicate normal activity where no additional action is required. Other events may signal the need for routine action such as archiving to a log file. Still other events may indicate the abnormal operation of a service or configuration item and require an incident to be created. The various types of events may be classified as follows:

- **Informational** – These events indicate normal operational activity. However, they are still useful for trending, statistics and reporting. They may also be used for researching past activity. These events usually don't require further action. By way of example, an informational event may be created when a user logs on to a system.
- **Warning** – These events indicate some unusual activity, status or operation. They may need further review or processing to determine if additional action should be taken. For example, when a system is approaching a threshold of memory utilization a warning event may be generated to indicate that system performance may begin to degrade soon.

- **Exception** – These events typically indicate something bad has happened. They need immediate review and may require action to resume normal operation or service levels. An example of an exception event is a network outage or system failure.

While the Incident Management process is invoked when some events occur, it is important to note that Event Management is not the same as Incident Management. In fact, ITIL v3 has positioned Event Management, Incident Management and Problem Management as peer processes within Service Operations.

Positioning Event Management within Service Operations

The Service Operations stage of the ITIL v3 Service Lifecycle includes several related processes, functions and activities that are often confused with Event Management. To get the most from the Event Management process it is important to understand how these other elements of Service Operations differ from as well as support the Event Management process.

The Service Operations stage of the ITIL v3 Service Lifecycle includes several related processes, functions and activities that are often confused with Event Management.

Incident Management

ITIL v3 defines an incident as an unplanned interruption to an IT service, or a reduction in the quality of an IT service. Incidents also include the failure of a configuration item – even if it has not yet impacted a service. Some events may result in the creation of a corresponding incident. Users may also detect incidents and report them directly to the Service Desk. When an incident occurs, the Incident Management process is responsible for restoring normal service operation and reducing the impact on users and business operations.

Problem Management

ITIL v3 defines a problem as the cause of one or more incidents. The idea behind Problem Management is to prevent incidents from occurring or recurring. This implies a proactive approach for preventing incidents. It also implies that the root cause of incidents must be found and fixed through a Change Management process to eliminate recurring incidents. A good Problem Management process will also retain information about problems, workarounds, recovery processes and solutions to assist with the Incident Management process.

Service Desk

Rather than a process, the Service Desk is an ITIL function. As mentioned, users may report incidents directly to the Service Desk. Whether incidents are derived from the Event Management process or from individual users, the Service Desk is responsible for tracking and managing them. The Service Desk function manages the incident lifecycle including categorization and prioritization, initial investigation, involvement of specialists, providing status to users, and closing incidents when the user is satisfied.

Monitoring

There are a number of common Service Operation activities that are not defined as ITIL processes. The monitoring activity is used to detect the status of services to ensure they maintain committed service levels and ultimately deliver their expected value to the business. Monitoring tools are designed to capture events sent by configuration items. Monitoring tools may also independently check the status of services or configuration items and create events when, for instance, status information is found to be outside normal ranges.

To summarize, when a warning or exception event has been detected by the Event Management process or Monitoring Activities, it may also result in an incident, problem or change. Or, in the case of an informational event, it may simply be logged for possible future use. The Service Desk function manages the lifecycle of all incidents, whether they were reported by individual users, the Event Management process or Monitoring Activities. Event Management in ITIL v3 is a distinct process of its own. It also relates to several other ITL processes, functions and activities within Service Operations as well as other stages of the Service Lifecycle.

Event Management Challenges

The tools, processes and configuration items in an IT environment should be configured to generate the right set of events. If required events are not produced, or if monitoring tools do not detect required events, the risk for a negative service impact rises dramatically. When events with predictive value are lost, ignored or simply not generated, processes like Incident and Problem Management will fail to take needed action.

*Most event consuming processes suffer from too **many** rather than too **few** events.*

However, most event consuming processes suffer from too *many* rather than too *few* events. Consider the load on the Service Desk function if every event were to create a corresponding incident. Simply recording and tracking these events would be overwhelming. The Service Desk staff should spend its time only on events that matter to the supported business. Yet only a portion of all events are important from a service-impact perspective.

Determining and defining which events should be generated depends in part on the processes that will consume them. Event logging processes require a large number of events – even simple informational events – to be captured and saved for potential future use. Yet it turns out that many events are simply duplicates or provide the same information value as other events. So capturing every single possible event is not really the objective. It is far better to perform some intelligent processing of events to eliminate duplicates, retain those with specific value, and organize them so they become most useful to the processes that consume them.

Yet even if events can be reduced to a subset where each remaining event has specific value, someone or something still needs to make sense of them. These meaningful events need to be categorized, prioritized and routed to the appropriate person or process so that necessary action – even if it is to simply log the event – can be determined and taken. For instance, the Service Level Management process must track the occurrence and trends of events related to service levels agreements (SLA).

Large, complex, and/or heterogeneous environments often include cumbersome, human-intensive activities in the Event Management process. In order to scale, events need to be assigned to the right owners who often have expert knowledge on a limited set of applications. However, operations teams continue to be organized around technology domains resulting in silos of data and expertise. The challenge of scaling event processing is compounded by the fact that many events that turn into incidents or problems require involvement of multiple experts that are working on separate teams.

A robust Event Management process built on well-designed tools can dramatically reduce costs by reducing manual labor requirements

Overall, many IT organizations have yet to gain control of their Service Operation processes. This leads to high costs as well as low quality services. Fortunately, with the introduction of ITIL v3, more organizations are realizing that improvements in the Event Management process have a large and positive downstream impact on other ITIL processes. A robust Event Management process built on well-designed tools can dramatically reduce costs by reducing manual labor requirements. It can transform IT from reactive to proactive so that service quality and consistency can be significantly improved.

Automating Event Management

Different ITSM vendors have each taken different paths toward addressing the challenges of Event Management. Some have realized that any substantial solution must incorporate automation. The classic, and still highly valuable, approach to automating the Event Management process is event correlation. Another approach to automation, though currently less well known, takes Event Management to an entirely new level by utilizing IT Process Automation (ITPA) to replace manual recovery actions.

Event Correlation

Event correlation directly attacks the challenges related to having too many events. It helps pinpoint the relatively few events and corresponding information that are really important. It can be described by four related steps.

- **Event Filtering** eliminates irrelevant events. Since the event correlation process may be distributed across a number of tools which often specialize in particular types of events, event relevancy may be determined in the context of individual tools.
- **Event Aggregation or De-duplication** involves eliminating multiple copies of the same event. Some event sources continue to generate events – with the same information – until the issue causing the events is resolved. Many events can be eliminated by simply keeping one of the events, perhaps along with a count of the number of occurrences within a relevant time period.
- **Event Masking** makes use of the idea that some events are already implied by other events and can be eliminated. If a segment of an organization's network fails, it is readily apparent that systems, storage and application components which are only connected through that segment will not be accessible.

- **Root Cause Analysis** is essentially a more complex and powerful version of event masking since it also determines which events can be explained by others. However, it uses more intelligence, like dependency maps, to eliminate extraneous events generated by the root cause event.

IT Process Automation

The other notable approach to automation, pioneered by NetIQ, is based on integrating ITPA with Event Management. When used in sequence, after event correlation, ITPA has the power to make IT Operations far more efficient and effective at managing the operational health of services. Focusing only on the events that matter, ITPA cuts down on manual processing and reduces IT costs.

The other notable approach to automation, pioneered by NetIQ, is based on integrating ITPA with Event Management.

ITPA solutions have been found useful for automating a wide variety of repetitive operations tasks including those found in run books. Network and systems operations staff as well as systems administrators follow procedures in run books for everything from re-starting a server to provisioning a new service. These procedures cover all steps required to complete various activities, and, for more complex processes, include decision trees so that variations in environmental variables can be addressed.

As noted in ITIL v3, responses to events may be driven manually or through automation. ITPA is perfectly matched to many of the automation opportunities around Event Management. However, with such a focus on provisioning applications of ITPA like Change Management, most vendors have yet to apply ITPA to Event Management.

Improving Quality and Reducing Expenses with NetIQ Solutions

Through two solutions, NetIQ provides a comprehensive approach to automated Event Management. NetIQ AppManager provides monitoring across a wide range of technologies while NetIQ Aegis goes beyond event monitoring to automate the Event Management process.

NetIQ AppManager

To support complex, heterogeneous environments and provide service visibility across multiple, diverse systems, NetIQ AppManager performs monitoring and handles events related to networks, operating systems, security, databases, traditional applications, Web applications, storage devices, virtual hardware, VoIP and telephony components, Microsoft infrastructure, third party ITSM solutions, and others. It organizes the resulting data visually in self-maintaining service maps that provide a *single pane of glass* from which to visualize the impact of events on services delivered to end users. NetIQ AppManager also includes Rule Based Management Groups that dynamically update service maps according to user-specified rules.

NetIQ Aegis

The NetIQ Aegis solution is the only ITPA offering on the market that includes an embedded correlation engine. This allows processing of high event volumes without bogging down the workflow automation engine. NetIQ Aegis integrates with NetIQ AppManager and other leading third-party monitoring products to automate event processing. It provides the ability to automatically resolve events, dramatically reducing manual workload and associated costs. NetIQ Aegis offloads routine tasks so operators and administrators become more productive. For example, NetIQ Aegis tracks its actions to provide documented compliance with IT policies, enabling faster time to resolution of incidents and reduced business impact.

Automating Response to Common Events - A Real World Scenario

IT administrators spend excessive time performing repetitive and mundane Event Management activities such as freeing up disk space on servers when a threshold is breached. While it is important to proactively address these problems to maintain server availability, manual administration slows the progress of accomplishing larger goals like deploying business-enhancing services. Fortunately, a solution is available to help automate this process:

- NetIQ AppManager detects available disk space has fallen below a threshold, caused by growth in temp or log files.
- The event triggers a process in NetIQ Aegis which requests NetIQ AppManager to perform analysis of disk usage on the server.
- NetIQ Aegis takes the collected information and sends it via email to the designated server administrator with options for archival or deletion of designated files.
- The server administrator replies to the email with an approval code that confirms the clean up steps.
- NetIQ Aegis commands NetIQ AppManager to perform the designated clean up actions as approved.
- NetIQ Aegis sends an email to the server administrator confirming that the cleanup was or was not successful.

Automating this process, and literally any event response, ensures that the knowledge of recovering from known errors is captured and the recovery process is executed consistently when events indicate the error has occurred. But the primary benefit is lower cost through reduced labor as IT management shifts from responding to events to approving their resolution and allowing the tools to do the work.

The primary benefit is lower cost through reduced labor as IT management shifts from responding to events to approving their resolution and allowing the tools to do the work.

EMA Perspective

Event Management is a critical foundation for ITIL v3 and general ITSM best practices, including many of the individual ITIL processes, including Incident, Problem and Change Management. The ITIL Service Desk function and Monitoring Activities must also be well aligned with a robust Event Management process in order to operate smoothly and efficiently. However, without best practice processes and the right supporting tools, IT organizations can be overwhelmed by a flood of events. The key to success is automation, and best practice approaches to automating event processing should include both event correlation and IT process automation.

NetIQ has developed a unique and comprehensive solution for Event Management through its integrated NetIQ AppManager and NetIQ Aegis products.

These two methods for automating the Event Management process are far better when used together. Event correlation shows its strengths in eliminating extraneous events and reducing the event stream to only those events that matter. ITPA then reduces or eliminates the manual processing required for those remaining events. But simply applying ITPA to a raw event stream would exacerbate the challenges by overloading the automation engine with unimportant events.

NetIQ has developed a unique and comprehensive solution for Event Management through its integrated NetIQ AppManager and NetIQ Aegis products. Events are monitored, detected, and their processing is automated through both event correlation and ITPA. This solution ultimately improves overall service quality through reduced recovery times, improving availability, and it lowers IT costs by reducing the manual labor associated with Event Management.

About NetIQ

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. For more information on NetIQ's portfolio of award-winning products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications, please visit www.netiq.com or contact sales@netiq.com.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst and consulting firm dedicated to the IT management market. The firm provides IT vendors and enterprise IT professionals with objective insight into the real-world business value of long-established and emerging technologies, ranging from security, storage and IT Service Management (ITSM) to the Configuration Management Database (CMDB), virtualization and service-oriented architecture (SOA). Even with its rapid growth, EMA has never lost sight of the client, and continues to offer personalized support and convenient access to its analysts. For more information on the firm's extensive library of IT management research, free online IT Management Solutions Center and IT consulting offerings, visit www.enterprisemanagement.com.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

1770.112008