ITIL – A guide to event management

Event management process information

Why have event management?

An event can be defined as any detectable or discernable occurrence that has significance for the management of the IT Infrastructure of the delivery of IT service and evaluation of the impact a deviation might cause to the services. Events are typically notifications created by an IT service, configuration item or monitoring tool. Effective service operation is dependent on knowing the status of the infrastructure and detecting any deviation from normal or expected operation. This is provided by good monitoring and control systems, which are based on two types of tools:

- Active monitoring tools that poll key configuration items to determine their status and availability. Any expectations will generate an alert that needs to be communicated to the appropriate tool or team for action.
- Passive monitoring tools that detect and correlate operational alerts or communications generated by configuration items.

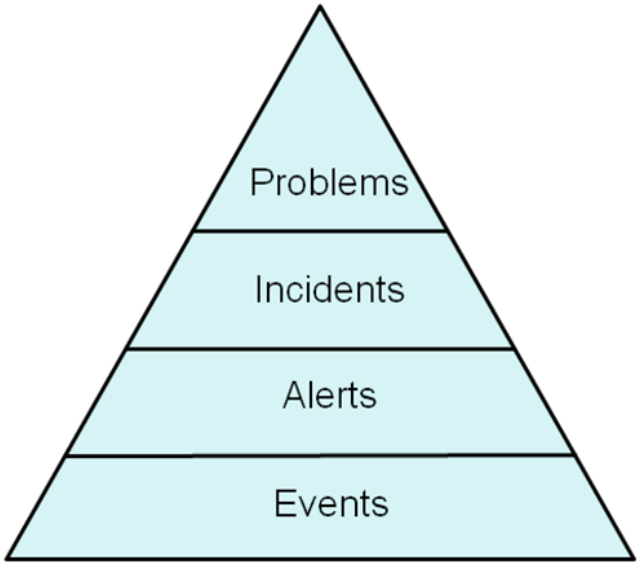
The objectives of event management

Event management is to provide the entry point for the execution of many service operation processes and activities. In addition, it provides a way of comparing actual performance and behaviour against design standards and Service Level Agreements.

Other objectives include:

- Provides the ability to detect, interpret and initiate appropriate action for events
- Basis for operational monitoring and control and entry point for many service operation activities
- Provides operational information, as well as warnings and exceptions, to aid automation
- Supports continual service improvement activities of service assurance and reporting and service improvement

"A change of state that has significance for the management of a configuration item or IT service"



It is **unusual for an organisation to appoint an 'Event Manager'**, as events tend to occur in multiple contexts and for many different reasons. However, it is important that Event Management procedures are coordinated to prevent duplication of effort and tools

The scope of event management

Event management can be applied to any aspect of service management that needs to be controlled and which can be automated. These include:

- Configuration Items (CIs):
  - Some CIs will be included because they need to stay in a constant state
  - Some CIs will be included because their status needs to change frequently and event management can be used to automate this and update the CMS
- Environmental conditions (e.g. fire and smoke detection)
- Software licence monitoring for usage to ensure optimum/legal licence utilisation and allocation
- Security (e.g. intrusion detection)
- Normal activity (e.g. tracking the use of an application or the performance of a server)

The difference between monitoring and event management – These two areas are very closely related, but slightly different in nature. Event management is focused on generating and detecting meaningful notifications about the status of the IT infrastructure and services.

Whilst monitoring is required to detect and track these notifications, monitoring is broader than event management. For example, monitoring tools will check the status of a device to ensure that it is operating within acceptable limits, even if that device is not generating events.

Examples of events

Events that signify regular operation:

- notification that a scheduled workload has completed
- a user has logged in to use an application
- an email has reached its intended recipient

Events that signify an exception:

- a user attempts to log on to an application with the incorrect password
- an unusual situation has occurred in a business process that may indicate an exception requiring further business investigation (e.g. a web page alert indicates that a payment authorisation site is unavailable – impacting financial approval of business transactions)
- a device's CPU is above the acceptable utilisation rate
- a PC scan reveals the installation of unauthorised software

Events that signify unusual, but not exceptional, operation:

- Server's memory utilization reaches within 5% of its highest acceptable performance level
- The completion time of a transaction is 10% longer than normal

The value to the organisation of event management

Event management's value to the organisation is generally indirect; however, it is possible to determine the basis for its value as follows:

- Event management provides mechanisms for early detection of incidents. In many cases, it is possible for the incident to be detected and assigned to the appropriate group for action, before any actual service outage occurs.
- Event management makes it possible for some types of automated activity to be monitored by exception – thus removing the need for expensive and resource intensive real-time monitoring, while reducing downtime.
- When integrated into other service management processes (such as, for example, availability or capacity management), event management can signal status changes or exceptions that allow the appropriate person or team to perform early response, thus improving the performance of the process. This, in turn, will allow the business to benefit from more effective and more efficient service management overall.

- Event management provides a basis for automated operations, thus increasing efficiencies and allowing expensive human resources to be used for more innovative work, such as designing new or improved functionality or defining new ways in which the business can exploit technology for increased competitive advantage.

The activities of event management

The service design phase of the service lifecycle should define which events need to be generated and then specify how this can be done for each type of CI. During the service transition phase, the event generation options would be set and tested.

Event occurs – Events occur continuously, but not all of them are detected or registered. It is, therefore, important that everybody involved in designing, developing, managing and supporting IT services and the IT infrastructure that they run on understands what types of event need to be detected.

Event notification – Most CI's are designed to communicate certain information about themselves in one of two ways:

- A device is interrogated by a management tool, which collects certain targeted data. This is often referred to as polling.
- The CI generates a notification when certain conditions are met. The ability to produce these notifications has to be designed and built into the CI, for example, a programming hook inserted into an application.

Event detection – Once an event notification has been generated, it will be detected by an agent running on the same system, or transmitted directly to a management tool, specifically designed to read and interpret the meaning of the event.

Event filtering – The purpose of filtering is to decide whether to communicate the event to a management tool or to ignore it. If ignored, the event will usually be recorded in a log file on the device, but no further action will be taken.

Significance of events – Every organisation will have its own categorisation of the significance of an event, but it is suggested that at least these three broad categories be represented:

- **Informational**: This refers to an event that does not require any action and does not represent an exception. They are typically stored in the system or service log files and kept for a predetermined period.

  Examples of informational events include:

  - A device has come online
  - A transaction is completed successfully

- **Warning**: A warning is an event that is generated when a service or device is approaching a threshold. Warnings are intended to notify the appropriate person, process or tool so that the situation can be checked and appropriate action taken to avoid an exception.

  Examples of warning events are:

  - Memory utilisation on a server is currently at 65% and increasing. If it reaches 75%, response times will be unacceptably long and the Operational Level Agreement for that department will be breached.
  - The collision rate on a network has increased by 15% in a short period of time (which is defined, i.e. an hour).

- **Exception**: An exception means that a service or device is currently operating abnormally. Typically this means that an Operational Level Agreement or Service Level Agreement has been breached and the business has been impacted. Exceptions could represent a total failure, impaired functionality or degraded performance.

  Examples of exception events include:

  - A server is down
  - Response time of a standard transaction across the network has slowed to more than 15 seconds

Event correlation – If an event is significant, a decision has to be made about exactly what the significance is and what actions need to be taken to deal with it. It is here that the meaning of the event is determined.

Trigger – If the correlation activity recognises an event, a response will be required. The mechanism used to initiate that response is also called a trigger. There are many different types of triggers, each designed specifically for the task it has to initiate. Some examples could include:

- Incident triggers that generate a record in the incident management system
- Change triggers that generate a request for change
- A trigger resulting from an approved request for change that has been implemented but caused the event, or from an authorised change that has been detected
- Scripts that execute specific actions
- Paging systems that will notify a person or team of an event
- Database triggers that restrict access of a user to specific records or fields, or that create or delete entries in the database

Response selection – At this point of the process, there are a number of response options available:

- Event logged – There will be a record of the event and any subsequent actions.
- Auto response – Some events are understood well enough that the appropriate response has already been defined and automated. This is normally a result of good design or previous experience (within problem management). The trigger will initiate the action and then evaluate whether it was completed successfully. If not, an incident or problem record will be created. Examples of auto responses include rebooting a device, restarting a service, locking a device or application to protect it against unauthorised access.
- Alert and human intervention – If the event requires human intervention, it will need to be escalated. The purpose of the alert is to ensure that the person with the skills appropriate to deal with the event is notified. The alert will contain all the information necessary for the person to determine the appropriate action
- Incident, problem or change? – Some events will represent a situation where the appropriate response will need to be handled through the incident, problem or change management process.
- Open an RFC.
- Open an incident record – As with an RFC, an incident can be created as soon as an exception is detected, or when the correlation engine determines that a specific type or combination of events represents an incident.
- Open or link to a problem record – It is rare for a problem record to be opened without related incidents. In most cases this step refers to linking an incident to an existing problem record. This will assist the problem management teams to reassess the severity and impact of the problem, and may result in a changed priority to an outstanding problem.
- Special types of incident – In some cases an event will indicate an exception that does not directly impact any IT service, e.g. unauthorized entry to a data centre. In this case, the incident will be logged using an incident model that is appropriate for this type of exception, e.g. a security incident. The incident should be escalated to the group that manages that type of incident. As there is no outage, the incident model used should reflect that this was an operational issue rather than a service issue. These incidents should not be used to calculate downtime, and can, in fact, be used to demonstrate how proactive IT has been in making services available.

Review actions – As thousands of events are generated on a daily basis, it is not possible to review every one. However, it is important to check that any significant events or exceptions have been handled appropriately, or to track trends or counts of event types etc. In many cases, this can be done automatically.

Close event – Some events will remain open until a certain action takes place, for example an event that is linked to an open incident. However, most events are not opened or closed. informational events are simply logged and then used as input to other processes, such as backup and storage management. Auto response events will typically be closed by the generation of a second event. For example, a device generates an event and is rebooted through auto response – as soon as that device is successfully back online, it generates an event that effectively closes the loop and clears the first event.

The terminology of event management

Event – A change of state that has significance for the management of a configuration item or IT service.

Trigger – An indication that some action or response to an event may be needed.

Alert – A warning that a threshold has been reached or something has been changed. (An event has occurred).

Event management relationship with other ITIL processes

The primary process relationships are with incident, problem and change management which are an exception event and are detailed within the event management process.

Capacity and availability management are critical in defining what events are significant, what appropriate thresholds should be and how to respond to them. In return, event management will improve the performance and availability of services by responding to events when they occur and by reporting on actual events and patterns of events to determine (by comparison with Service Level Agreement targets and KPIs) if there is some aspect of the infrastructure design or operation that can be improved.

Configuration management is able to use events to determine the current status of any CI in the infrastructure. Comparing events with the authorised baselines in the Configuration Management System (CMS) will help to determine whether there is unauthorised change activity taking place in the organisation.

Asset management can use event management to determine the lifecycle status of assets. For example, an event could be generated to signal that a new asset has been successfully configured and is now operational.

Events can be a rich source of information that can be processed for inclusion in Knowledge Management Systems. For example, patterns of performance can be correlated with business activity and used as input into future design and strategy decisions.

Event management can play an important role in ensuring that potential impact on Service Level Agreements is detected early, and any failures are rectified as soon as possible so that impact on service targets is minimised.