ServiceNow® ITIL Monitoring

Enabling Problem Finding and Fixing

INTRODUCTION

IT downtime is bad for business – it not only impacts company's finances but also has a disastrous effect on the company's reputation. All of us have seen this through numerous examples all over the world.

▸ In 2016, hundreds of Delta Airlines passengers were left stranded in airports for more than six hours because of a "major system-wide network outage".[1]

▸ A fine of £56m was imposed on The Royal Bank of Scotland for an IT outage which had affected 6.5 million customers. [2]

▸ For the Fortune 1000 companies, the average total cost of unplanned application downtime per year is $1.25 billion to $2.5 billion – With the average hourly cost of an infrastructure failure being $100,000 per hour.[3]

▸ In 2015, Starbucks lost millions in sales because of the massive outage which shut down the point-of-sales systems at its stores. [4]

According to Quorum Disaster Recovery Report [4],

▸ 55 percent of the down times happen because of hardware failure

▸ 22 percent IT disasters are caused by human error

▸ Software failures cause 18 percent of the outages

▸ Natural disasters comprise 5 percent of actual causes of down time

As we see, IT outages mainly happen because of hardware or software failures or human errors. Using the right network monitoring and event management tools, companies can effectively prevent the human errors and quickly act on to repair the damage.

This guide by Alcor will help you understand the topic of ITIL event management a little more in detail.

▸ While the need for event management tools seems to be obvious, let us try and understand it in more detail -why are organizations are investing in it and what are the real costs if they don't take it seriously.

▸ Once we are convinced on the need for event monitoring, let us understand the whole process of event management – what it involves and how event management tools can play a crucial role in effective event management.

▸ Depending on the needs of the organizations, it is important that they choose the right monitoring tool – get some guidance on what to look for while choosing the right ITIL monitoring tool.

ITIL EVENT MONITORING AND MANAGEMENT – THE NEED

With the heavy dependence on technology, organizations need their IT infrastructure to be up and functioning 24x7 since their revenues and customer experiences depend on those. Considering the complexity and vastness of the systems, every day, hundreds of thousands of events and incidents happen across the IT infrastructure. To function effectively, IT needs real-time and instant information into their network performance metrics. It is not possible to have human resources deployed for this monitoring 24x7 for this.

Organizations, therefore, have started investing seriously in event management solutions which can help them in monitoring their networks in real time, troubleshoot the problems quickly and easily, enhance network security, plan for the future growth, and improve their bottom line.

Digital enterprises are moving at a very fast pace. With agile releases and continuous deployments, there is a growing demand for always-accessible applications. ITIL event management, therefore, becomes the fundamental requirement for the IT. Right from small events such as completion of a regular server maintenance script to more severe events such as a crucial server going down – all these are the events worth knowing about.

The key objectives of event management are -

▸ Detect events in time

▸ Analyze the events quickly and determine the right control action

▸ Ensure uninterrupted assurance, reporting

▸ Improve the service performance

Monitoring is the first step and a crucial component of event management. It helps in detecting the events as they occur and event management analyzes the events and helps IT in taking appropriate actions as required.

EVENT MANAGEMENT – THE PROCESS

In the context of ITIL, an event is defined as 'the change of state, that is significant to Service management'. Some of the simple examples of events include starting a service on a particular server, login of a user on a system, increase or decrease in the internet link utilization by a certain percentage, crashing of an application, completion of backup and so on. Event management involves understanding the significance of each of the events and then taking an appropriate action as required.

A solid and effective event management process helps organizations in improving their response times to incidents and exceptions, it offers them a solid basis to identify the IT components which are ideal for automation and through all these things, it helps them in reducing the down times.

ITIL identifies three different types of events:

1. Information: These are like basic status updates and do not necessarily require a response. Logs and reports typically fall in this category.

2. Warning: Warnings indicate the presence of some activity which is not normal. Warnings act as indicators to tell the IT to monitor conditions so that those don't get worse. Warnings could also trigger actions to prevent an event.

3. Exception: Exceptions indicate the presence of some problem. Exceptions could negatively impact the services and need immediate attention.

So, what exactly is event management and what is involved in the process? At a very high level, event management involves-

‣ Event detection and notification
‣ Event filtering and categorization
‣ Response selection
‣ Closing the event

EVENT MANAGEMENT – THE PROCESS

ITIL identifies three different types of events

Information

Warning

Exception
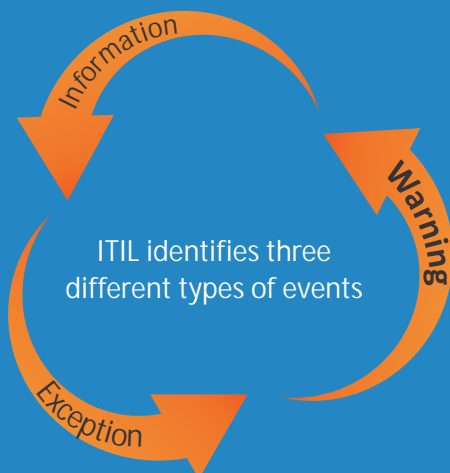
Let us understand each of these in a little more detail -

1. Event Detection and Notification

Events don't necessarily happen only during work hours. They occur all through the day (and night). Effective ITIL Event Management requires identification and detection of the significant events. Once the event is detected, the monitoring tool should send out a notification about the happening of the event.

2. Event Filtering and Categorization

Each event does not require an action. Most often than not, information events can be ignored but exceptions and warnings require action. At the filtering stage, the event management system simply filters the events as "to be ignored" or "pass on for further action".

3. Response Selection

Once the event is filtered and categorized, it requires a response. The response option could be one or a combination of – event logging, auto response, raising of an alert, escalation to require human intervention, or handling through incident/change management process. In case of an RFC, for an exception, either create an incident as soon as an exception is detected or when a specific combination of events represents and incident.

4. Closing the Event

In case the event results in an incident, problem, or change, event closure needs to be handled appropriately. The event can be marked as "closed" in the event management system – before that, it needs to be ensured that the event is properly logged along with the action taken and information about the corresponding incident, problem, or change request.

NETWORK MONITORING – A CRITICAL ELEMENT IN EVENT MANAGEMENT

In September of 2015, Facebook was down for 40 minutes – which meant that people were not able to post their updates and the Facebook ads were not running. The estimated cost of that 40 minutes of downtime was USD 500,000!

For several organizations, while the IT provides the mission-critical services which have a serious impact the business revenues and customer satisfaction, IT does not always know the real business impact of the outages. Many times, the IT teams can't even locate the exact the exact infrastructure components

which are causing the disruption and how those components are interconnected in the network.

Network monitoring tools, therefore, become an important component for monitoring the enterprise network 24X7. There are several benefits of the network monitoring tools

▸ These tools help organizations in monitoring and analyzing the network performance in real-time and help them in detecting any failure or issue immediately through alerts. With real-time detection and monitoring, it is possible to take instant corrective action and minimize the potential downtime.

▸ These tools eliminate the need for manual checks. It not only saves the company time and cost, but it also allows for 24X7 monitoring without necessarily having to deploy additional staff.

▸ The reports generated from network monitoring can help the Network Operations Center (NOC) staff in identifying trends and patterns in system performance and alert them for the need for any upgrades or replacements.

▸ These tools also help in identifying the exact areas of problems because of which, the NOC teams can quickly address the issue and save time and money.

However, having multiple tools simply complicates the matter and increases the noise – each tool generates a lot of data, they all report the same issue, a single issue creates multiple events, and many of these events could have no business impact at all. In an effort to sort through the noise of this data, it is possible that the NOC staff can miss on important issues leading to further delay in issue resolution.

To be able to efficiently manage the network availability and service performance, IT teams need much beyond a list of events on a non-updated service map. They need service-aware event management which is built around the most up-to-date service maps, offers actionable service health information (and not just a list of events), and offers a 360-degree view of how the changes and incidents affect the overview service health.

CHOOSING THE RIGHT ITIL EVENT MANAGEMENT SOLUTION

The role of the event monitoring and management solution is to accurately understand the network components and the flow of data between them. While there are hundreds of vendors with thousands of tools, as a rule, organizations should look for a solution that supports 100% of the required mandatory functional requirements which are specific to their organization and at least 80% of desired functional or nice to have requirements.

While the exact selection of the tools depends on the specific requirements of the organization, at a broad level, the event management solution should help with the following -

▶ The solution must be able to monitor and manage the crucial aspects of the business based on the business requirements. While different technologies can be monitored using different tools and ways, the solution you select must be able to interface with various other systems throughout the IT infrastructure to be able to provide the complete support. Compatibility is less of an issue when the full tool sets are purchased from the same vendor.

▶ It should support both active as well as passive monitoring as per the requirements.

▶ It should be able to filter important information from the sea of data across the network and provide the critical information focused on the organization's specific business needs.

INTRODUCTION TO SERVICENOW® EVENT MANAGEMENT

In today's age, when enterprises heavily rely on IT to provide the foundation for business services, it has become all the more important to closely monitor the infrastructure and take actions on issues. This is possible only when the monitoring is done in real-time, alters are raised at the right time, and the IT has a clear visibility between infrastructure events and business services. Only then enterprises can save themselves from the service impact created by service outages.

ServiceNow® Event Management solution helps organizations transform infrastructure events into actionable, service-aware alerts.

▸ It automatically creates actionable alerts from infrastructure events captured by the monitoring tools –With smooth integration with several third party infrastructure-monitoring tools, organizations can go with the monitoring tool of their choice.

▸ It allows organizations to apply rules to alerts to facilitate faster resolution of service-impacting issues. These rules automatically trigger various actions in ServiceNow® Incident Management, knowledge base, and more.

▸ When ServiceNow® Event Management is used with ServiceNow® Service Mapping and ServiceNow® Configuration Management Database (CMDB), it automatically maps alerts to configuration items (CIs) and services – saving a huge time for IT.

▸ Using dashboards, it also shows how business services are impacted because of the events.

ServiceNow® Event Management helps organizations reduce the business impact of service outages. The key benefits include -

Increased Service Availability: ServiceNow® Event Management automatically filters incoming events and generates qualified alerts enabling faster action. It automatically creates incidents and triggers IT processes for rapid remediation of service-impacting issues.

Linkage to Business Services: Through intuitive dashboards and interactive views, it shows how the events impact services. This helps in prioritizing the issues appropriately according to the business criticality of the services.

Easy Third Party Integrations: ServiceNow® Event Management can easily integrate with the several third-party monitoring tools or out-of-the-box connectors. This enables a single management console for combining multiple event sources.

ALCOR'S EXPERTISE IN SERVICENOW®

Alcor takes a strategic ITSM implementation approach and focuses on solving the business problems of their clients by leveraging an integrated business process design and technology implementation capability. Alcor's ITSM solutions with ServiceNow® leverage a business view of IT services. The objective is to enable the IT support organization to:

- Quickly resolve or escalate issues and problems
- Improve root cause isolation, and
- Provide higher levels of business user satisfaction.

Alcor brings substantial process expertise, ServiceNow® experience and depth of organizational governance modeling to build solutions that are effective and provide complete life cycle support for Incident Management, Problem Management, Change Management and Configuration Management. Alcor has experience in Automating ServiceNow® with external applications like emails, active directories, Adobe, assets, and Amazon Cloud Provision (LABS). This includes real-world experience of having worked with enterprises in the banking and financial services and retail sector where we have helped orchestrate transaction volumes running into the 100's of thousands.

Alcor has specific expertise in ServiceNow® IT Operations Management across the three levels, Orchestration, Release Management and Service Analytics. Through effective Orchestration Alcor helps clients launch the right automated process consistently and to codify best practices into the process workflows to save time and money. Alcor's expertise in helping their clients manage Release Management better allows optimal usage of the IT assets, hardware and software, available to the client to ensure effective, timely, un-interrupted and on-demand service delivery. Alcor helps their clients put in place Service Analytics Solutions that gives them the capability to keep track of each and every infrastructure component that impacts overall service delivery.

Alcor achieves this by leveraging their integrated business process design and technology implementation capability. Their professionals are the top talents in the business with deep personal understanding of the business verticals they service. This allows them to deliver flexible solutions that work in the real world. Their strength lies in delivering solutions that are customized to the specific requirements of their customers including complex integrations with the other systems in the eco-system like Financial and Procurement Management systems.

Building effective Enterprise Service Management Solutions is one of Alcor's key business focus areas. Alcor consultants have deep expertise around implementing and managing key IT Service Management processes such as Incident, Change, Release, Problem, Configuration Management & Asset Management. Alcor provides process maturity & technological sophistication when implementing ESM solutions.

CONCLUSION

When IT technologies fail, it has a serious impact on the organization's finances, reputation, and integrity. As a result, today's digital enterprises take ITIL monitoring and event management quite seriously. They have started to implement sophisticated monitoring systems to help them identify the overall health of their IT infrastructure. Deploying a monitoring system is a first step towards ensuring the business continuity and service performance. However, once the event alert is raised, it needs to be quickly categorized and acted upon. Event management solutions help in the appropriate categorization and remediation of the events. To gain the best results from the event management solution, organizations need to ensure that the solution is able to link the events to business impact – only then the IT can prioritize the events and resolve them for service continuity and reduce the overall business impact.

ABOUT ALCOR SOLUTIONS

Alcor is a global cloud advisory and implementation services company serving Fortune 500, Government Agencies, and other leading organizations in multiple industry verticals across the Americas, Canada and India. Alcor is a ServiceNow® Gold Services Partner and also partners to Salesforce®, FireEye™, Microsoft® , Dell, BOMGAR®, and BigPanda® amongst others. They advise leading businesses on cloud platforms, architecture, enterprise service management and integrating IT service delivery. They also provide business process consulting to capture, re-engineer and improve processes that can easily be automated to deliver real value. The Alcor consulting team is derived from a combination of experts in Business strategy, Cloud Technology and Organizational Change Management.

For more information, connect with us at information@alcortech.com.

REFERENCES

1. http://www.datacenterdynamics.com/content-tracks/security-risk/tens-of-thousands-of-delta-passengers-grounded-by-outage/96749.article

2. https://www.theguardian.com/business/2014/nov/20/royal-bank-of-scotland-it-breakdown-56m-pounds-fine

3. https://devops.com/real-cost-downtime/

4. http://www.geekwire.com/2015/starbucks-lost-millions-in-sales-because-of-a-system-refresh-computer-problem/

5. Quorum Disaster Recovery Report, Q1 2013

Alcor is a technology implementation company focusing on Enterprise and Government technology needs in ITSM, systems integration, web development and mobility space. We provide a strategic ITSM implementation approach to our clients and focus on solving business problems by leveraging an integrated business process design and technology implementation capability.