ITIL Event Management in the Cloud

An AWS Cloud Adoption Framework Addendum

July 2015

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

Many enterprises have successfully migrated some of their on-premises IT workloads to the cloud. An enterprise must also deploy an IT Service Management (ITSM) framework so it can efficiently and effectively operate those IT capabilities. This whitepaper outlines best practices for event management in a hybrid cloud environment using Amazon Web Services (AWS).

Introduction

This whitepaper is for IT Service Management (ITSM) professionals who support a hybrid cloud environment that uses AWS. The focus is on Event Management, a core chapter of the Service Operations volume of the IT Infrastructure Library (ITIL). Many AWS enterprise customers have successfully integrated their cloud strategy with their ITIL-based IT service management practices. This whitepaper provides you with background in the following areas:

- Event Management in ITIL
- The AWS Cloud Adoption Framework
- Cloud-Specific Event Management Best Practices

What is ITIL?

The IT Infrastructure Library (ITIL) Framework, managed by AXELOS Limited, defines a commonly used, best-practice approach to IT Service Management (ITSM). It builds on ISO/IEC 20000, which provides a "formal and universal standard for organizations seeking to have their ITSM capabilities audited and certified."[1] However, the ITIL Framework goes one step further to propose operational processes required to deliver the standard.

ITIL is composed of five volumes that describe the entire ITSM lifecycle as defined by the AXELOS. To explore these volumes in detail, go to https://www.axelos.com/

The following table gives you a brief synopsis of each of the five volumes:

ITIL Volume	Description
Service Strategy	Describes how to design, develop and implement service management as a strategic asset
Service Design	Describes how to design and develop services and service management processes
Service Transition	Describes the development and improvement of capabilities for transitioning new and changed services into operations
Service Operation	Embodies practices in the management of service operation
Continual Service Improvement	Guidance in creating and maintaining value for customers

What Is the AWS Cloud Adoption Framework?

The Cloud Adoption Framework (CAF) offers comprehensive guidelines for establishing, developing, and running cloud-based IT capabilities. AWS uses the CAF to help enterprises modernize their ITSM practices so that they can take advantage of the agility, security, and cost benefits afforded by the cloud.

Like ITIL, the CAF organizes and describes the activities and processes involved in planning, creating, managing, and supporting a modern IT service. ITIL and the CAF are compatible. In fact, the CAF provides enterprises with practical operational advice for how to implement and operate ITSM in a cloud-based IT infrastructure.

The details of the AWS CAF are beyond the scope of this whitepaper, but if you want to learn more, you can read the CAF whitepaper at http://do.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf.

The CAF examines IT management in the cloud from seven core perspectives, as shown in the following table:

CAF Perspective	Description
People	Selecting and training IT personnel with appropriate skills, defining and empowering delivery teams with accountabilities and service level agreements
Process	Managing programs and projects to be on time, on target, and within budget, while keeping risks at acceptable levels
Security	Applying a comprehensive and rigorous method of describing a structure and behavior for an organization's security processes, systems and personnel
Strategy & Value	Identifying, analyzing, and measuring the effectiveness of IT investments that generate the most optimal business value
Maturity	Analyzing, defining, and anticipating demand for and acceptance of envisioned IT capabilities and services
Platform	Defining and describing core architectural principles, standards, and patterns that are required for optimal IT capabilities and services
Operation	Transitioning, operating, and optimizing the hybrid IT environment, enabling efficient and automated IT service management

Event Management in ITIL

The ITIL specification defines an event as "any detectable or discernable occurrence that has significance for the management of the IT infrastructure or the delivery of IT service." In other words, an *event* is something that happens to an IT system that has business impact.

An *occurrence* can be anything that has material impact on the business such as environmental conditions, security intrusions, warnings, errors, triggers, or even normal functioning. Occurrences are things that an enterprise needs to monitor, preferably in an automated fashion, giving you the visibility you need to run your systems more efficiently and effectively over time with minimal downtime.

The goal of Event Management is to detect events, prioritize and categorize them, and figure out what to do about them.

In practice, Event Management is used with a central monitoring tool, which registers events from services or other tools such as configuration tools, availability and capacity management tools, or specialized monitoring tools. Event Management acts as an umbrella function that sits on top of other ITIL processes such as Incident Management, Change Management, Problem

Management, or Service-Level Management and divides the work depending on the type of event or its severity.

AXELOS provides the following flow chart to describe what an enterprise's Event Management process should look like:

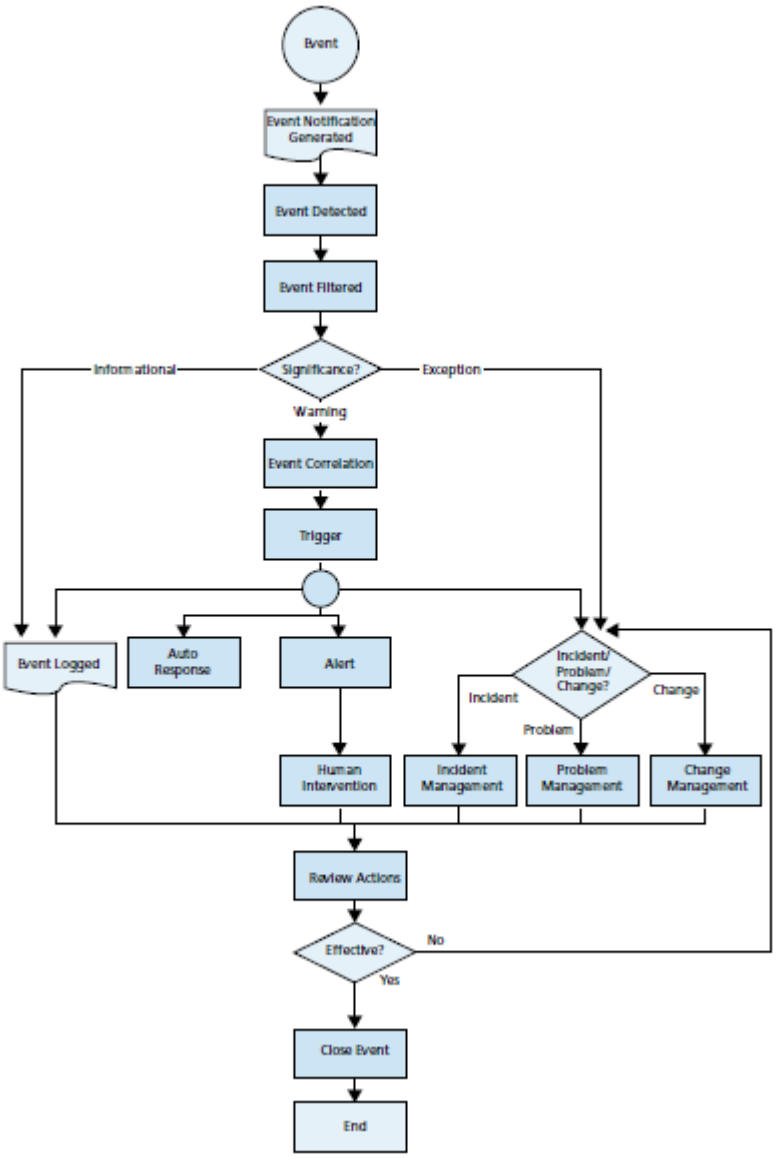

Figure 1: Event Management in ITIL

AXELOS observes that not all events are, or need to be, detected or registered. Defining the events to be managed is an explicit and important management decision. After management decides which events are relevant, service

components must be able to publish the events or the events must be pollable by a monitoring tool. Events must also be actionable. The Event Management process, whether automated or manual, must be able to determine what to do for any event. This determination can take many forms such as ignoring, logging, or escalating the event. Finally, the Event Management process must be able to review and eventually close events.

Event Management and the CAF

As with most specifications covered in the Service Operation Volume of ITIL, Event Management falls nicely into the Cloud Service Management function of the AWS CAF Operating Domain.

Of course, cloud initiatives require more than just the right technology. They also must be supported by organizational changes, including people and process changes. Such changes should be supported by a Cloud Governance Forum or Center of Excellence that has the role of managing through transition using the CAF. From the perspective of ITSM, your operations should certainly have a seat at the table.

Figure 2 illustrates how the CAF looks at managing events and actions in a hybrid environment. Review and action is based on information comes from the on-premises environment or any number of cloud providers (private or public).

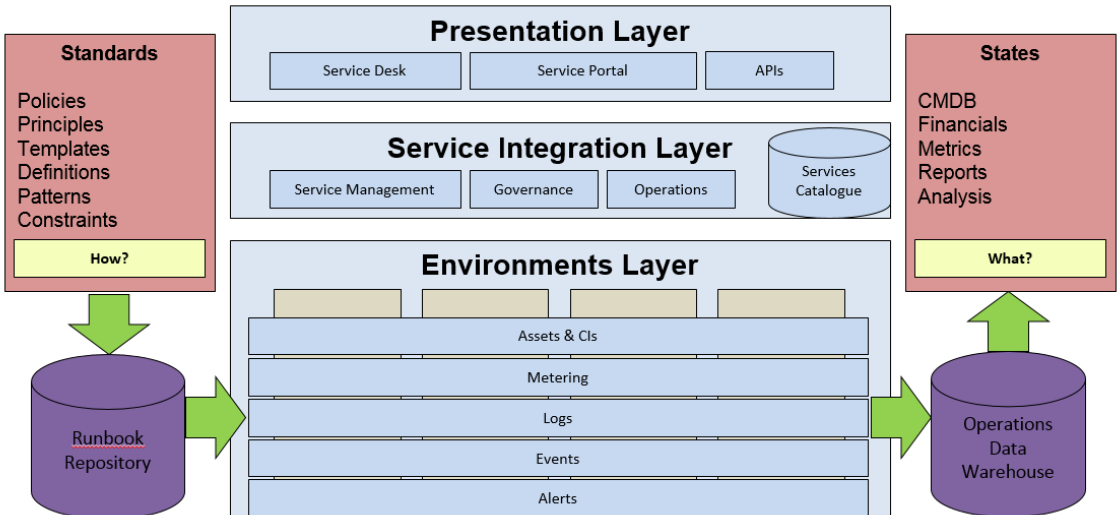

Figure 2: CAF Integration

Cloud-Specific Event Management Best Practices for IT Service Managers

AWS provides the building blocks for your enterprise to create your own Event Management Infrastructure. These building blocks allow for the integration of cloud services with on-premises or more traditional environments. In particular, AWS provides full support for ITIL Section 4.1.10: Designing for Event Management. AWS does not provide Event Management as a Service. Enterprises that enable Event Management would need to deploy and manage their own Event Management infrastructure.

Cloud Event Monitoring, Detection, and Communication Using Amazon CloudWatch

AWS supports instrumentation by providing tools to publish and poll events. In particular, you can use the Amazon CloudWatch API for automated management and integration into your Event Management infrastructure.

Amazon CloudWatch monitors your AWS resources and the applications that you run on AWS in real-time[2]. You can use Amazon CloudWatch to collect and track metrics, which are the variables you want to measure for your resources and applications. In addition, Amazon CloudWatch alarms (or monitoring scripts) can send notifications or automatically make changes to the resources that you are monitoring based on rules that you define. For information on CloudWatch pricing go to the Amazon CloudWatch pricing page.
http://aws.amazon.com/cloudwatch/pricing/

You can use CloudWatch to monitor the CPU usage and disk reads and writes of your Amazon Elastic Compute Cloud (Amazon EC2) instances. Then you can use this data to determine whether you should launch additional instances to handle increased load. You can also use this data to stop under-used instances and save money.

In addition to monitoring the built-in metrics that come with AWS, you can monitor your own custom metrics. You can publish and monitor metrics that you derive from your applications to reflect your business needs. With Amazon CloudWatch, you gain system-wide visibility into resource utilization, application performance, and operational health.[3]

By default, metrics and calculated statistics are presented graphically in the Amazon CloudWatch console. You can also retrieve these metrics using the API or command line tools. When you use Auto Scaling, you can configure alarm actions to stop, start, or terminate an Amazon EC2 instance when certain criteria are met. In addition, you can create alarms that initiate Auto Scaling and Amazon Simple Notification Service (Amazon SNS) actions on your behalf. [4]

Amazon EC2 Monitoring Detail Read more about Amazon EC2 monitoring in the AWS documentation: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html

An enterprise that does not have its own event management infrastructure can implement basic ITIL Event Management using Amazon CloudWatch. However, most large enterprises, especially those running hybrid cloud designs, will maintain their own event management infrastructure using products such as BMC Remedy, Microsoft System Center, or HP Open View.

Many event management tools are integrated with Amazon Web Services. See the following table for some examples.

Tool	Reference
MS System Center	http://aws.amazon.com/windows/system-center/
BMC Remedy	http://media.cms.bmc.com/documents/439126_BMC_Managing_AWS_SWP.pdf
IBM Tivoli	https://aws.amazon.com/marketplace/pp/B007P7MEK0
CA APM	https://aws.amazon.com/marketplace/pp/B00GGX0N0W/ref=portal_asin_url

Tool	Reference
CA Nimsoft	http://www.ca.com/~/media/Files/DataSheets/ca-nimsoft-monitor-for-amazon-web-services.pdf
HP Sitescope	http://h30499.www3.hp.com/t5/Business-Service-Management-BAC/HP-SiteScope-integration-with-Amazon-CloudWatch-Auto-Scaling-AWS/ba-p/2408860#.VCzWTPmSzTY

This type of design is fully compatible with AWS. However, enterprises will need to deploy SNMP, AWS SNS, or other interfaces that sit between Amazon CloudWatch and their enterprise Event Management / Service Desk tool. This will ensure that AWS-generated events can pass through Amazon CloudWatch and into the enterprise Event Manager.

IT service management professionals who integrate Amazon CloudWatch into their enterprise event management infrastructure need to answer the following questions:

- Are the right events are being propagated?
- Are the events tracked at the right level of granularity?
- Is there a mechanism to review and update triggers, limits, and event-handling rules?

BEST PRACTICES FOR MONITORING IN AWS

Make monitoring a priority to head off small problems before they become big ones.

Automate monitoring tasks as much as possible.

Check the log files on your services (Amazon EC2, Amazon S3, Amazon RDS, etc.).

Create and implement a monitoring plan that collects data from all parts of your AWS solution so that you can more easily debug a multi-point failure, if one

occurs. Your monitoring plan should address, at a minimum, the following questions:

- What are your monitoring goals?
- What resources will you monitor?
- How often will you will monitor these resources?
- What monitoring tools will you use?
- Who will perform the monitoring tasks?
- Who should receive notification when something goes wrong?

Incident Management

Events classified as Warnings or Exceptions may trigger incident management processes. These processes restore normal service operation as quickly as possible and minimize any adverse impact on business operations.

In the ITIL process, first attempt to resolve warnings or exceptions by consulting a database of known errors or a configuration management database (CMDB). If the warning or exception is not in the database, then classify the incident and transfer it to Incident Management. Incident Management typically consists of first line support specialists who can resolve most of the common incidents. When they cannot resolve an incident, they escalate it to the second line support team, and the process continues until the incident is resolved. Incident Management tries to find a quick resolution to the Incident so that the service degradation or downtime is minimized."[1]

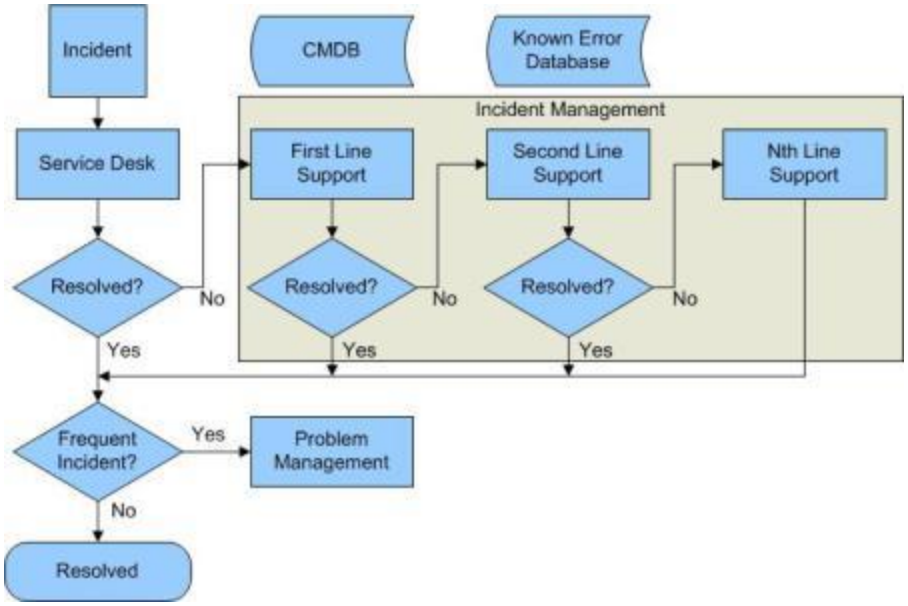

Figure 3: Incident Management in ITIL

It is worth noting that a well-designed cloud infrastructure can be far more resilient to faults. There is less likelihood of generating production incidents where faults are able to gracefully fail over. Underlying problems can be resolved through Problem Management.

INCIDENT MANAGEMENT BEST PRACTICES

As part of cloud-integrated Incident Management, enterprises should define several parameters:

- Ensure that relevant employees and staff understand which services are AWS-operated versus enterprise-operated (for example, an Amazon EC2 instance versus a business application running on that instance).
- Ensure that relevant staff and processes are aware of the SLAs associated with AWS-operated services and integrate those SLAs into the existing Enterprise Incident Management infrastructure.
- Define explicit SLAs (including resolution time scales) for services operated by the enterprise, but running on the AWS infrastructure.

- Define Incident Severity levels and Priorities for all services running on the AWS infrastructure.
- Subscribe to Enterprise Support and agree on the role the Amazon Technical Account Manager (TAM) will have during Incident Responses. For example, for Severity 1 incidents, should the TAM be part of the emergency resolution bridge / emergency response team?
- Ensure 360 degree ticket integration. Make sure that ticket opening and closing is seamless across on-premises and cloud systems.
- Define recovery runbook recipes (Incident Model) that include the recovery steps in chronological order, individual responsibilities, escalation rules, timescales and SLA thresholds, media/communications roles, and post-mortems. You should note that in a cloud environment, where infrastructure is defined as code, termination and reboot might be a faster way to recover from an incident than by using standard debugging approaches. Service can be immediately restored and root problems can be addressed offline as part of Problem Management.
- Where possible, incident remediation should occur automatically, with no human intervention. However, where human intervention is required, that intervention should be simple, with mostly automated runbook steps.

Problem Management

Problem Management is the process of managing the lifecycle of all problems with the goal of preventing repeat incidents. Whereas the goal of Incident Management is to recover, Problem Management is about resolving root causes so that incidents do not recur and maintaining information about problems and related solutions so organizations can reduce the impact of incidents.

Enterprises operating a hybrid environment will likely have their own Problem Management infrastructure. The goal of integration should be to seamlessly integrate the process for addressing problems related to AWS into the existing Problem Management infrastructure.

Enterprises have the option of purchasing AWS Enterprise Support, where they can agree on role the Amazon Technical Account Manager (TAM) will have during Problem Management. For example, where the problem explicitly involves part of the AWS infrastructure, the TAM might be involved with formal problem detection, prioritization, and diagnosis workshops and discussions or be required to log AWS-related problems with the enterprise Problem Logging platform / Known Error Database.

If AWS infrastructure is not part of the root cause, it could play a role in supporting diagnosis. Here the TAM can support the information gathering.

Conclusion

Enterprises that migrate to the cloud can feel confident that their existing investments in ITIL, and particularly Event Management, can be leveraged going forward. The Cloud Operating model is consistent with traditional IT Service Management discipline. This whitepaper gives you a proposed suite of best practices to help smooth the transition and ensure continuing compliance.

Contributors

The following individual contributed to this document:

- Eric Tachibana, AWS Professional Services

Notes

[1] ITIL Service Operation Publication, Office of Government Commerce, 2007, Page 5

[2] For up to 2 weeks!

[3] What Is Amazon CloudWatch? (http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/WhatIsCloudWatch.html)

[4] For more information about creating CloudWatch alarms, see Creating Amazon CloudWatch Alarms in the CloudWatch documentation (http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/AlarmThatSendsEmail.html).