Meeting the New Standard for AWS Managed Services

White Paper

April 2017

www.sciencelogic.com • info@sciencelogic.com • Phone: +1.703.354.1010 • Fax: +1.571.336.8000

Table of Contents

Meeting the New Standard for AWS Managed Services

Introduction

The AWS MSP Partner Network (MPN) Program helps MSPs develop a managed service practice around the deployment and ongoing operation of AWS services. The MSP program sets a high standard for MSPs to attain in terms of their operational capabilities and their in-house AWS technology and process expertise. MSPs who achieve MPN partner program membership are typically among the top MSPs in the world for AWS technology prowess, whether for AWS-based consulting services, or operational support services.

According to the MPN program documentation: "*The AWS MSP Partner Program Validation Checklist…. provides the criteria necessary to achieve the MSP Partner designation and represents AWS' view of the capabilities that a 'next generation managed service provider' should have to support customers through all phases of the customer engagement lifecycle: plan, design, migrate/build, run, and optimize*".

The most recent update to the checklist (version 3.1) raises the bar further for MSPs, implying they must deliver more value to customers – and in turn demand more from their monitoring vendors. This paper describes the latest program requirements related to monitoring and summarizes how the ScienceLogic platform helps MSPs meet those requirements. It is not intended as a complete work on how to pass the AWS audit, as it discusses only the monitoring aspects.

New Requirements in Version 3.1

This latest revision (3.1) to the AWS Partner Program Checklist adds several new requirements related to monitoring, including the following:

- Section 9.5 - Proactive Monitoring and Alerting
- Section 9.6 - Next Generation Monitoring Capabilities
- Section 9.7 - Service Intelligence Reporting and Dashboards for Customers
- Section 9.8 - Continuous Compliance
- Section 9.9 - Event Management

Specific monitoring requirements are documented in the following table, along with examples of how the ScienceLogic platform helps MSPs meet the new standards.

AWS MSP 3.1 Requirement	ScienceLogic Examples
9.5 Proactive Monitoring and Alerting	
Partner has systems, tools, or applications capable of monitoring the performance of all AWS services that are part of the customer's managed service agreement. Proactive Monitoring looks for patterns of events to predict possible future failures. (*ITIL Service Operation)* The monitoring and alerting functionality must also be accompanied by corresponding service desk functionality to take action on events/alerts according to SLAs/contractual obligations. Partners should show their capabilities within the following categories: Infrastructure monitoring, some examples include: □ Amazon CloudWatch out-of-the-box metrics for AWS monitoring, alerting, and automated provisioning	The ScienceLogic Monitoring platform is designed to consume, process, and manage events—and act upon them proactively. On receiving an alert from AWS for a specific fault condition, ScienceLogic automatically opens a ticket (in ScienceLogic or 3rd party service management systems). It automatically populates the incident with device details (asset name, serial number, etc.) and troubleshooting information (e.g., it automatically conducts ping/reachability/other tests and adds results to the incident). ScienceLogic can consume and process CloudWatch metrics and alerts, or custom metrics, in conjunction with alerts it generates from aspects of infrastructure that AWS does not instrument (e.g., Windows OS metrics). ScienceLogic can consume and process alerts and performance detail from APM tools (e.g., New Relic) to provide

□ Amazon CloudWatch custom metrics for Application monitoring, alerting, and automated provisioning □ Other 3rd party AWS infrastructure monitoring tools Service monitoring, some examples include: □ Operating system monitoring tools for OS-level monitoring □ Application monitoring tools for Application-level monitoring □ Simulated transaction monitoring tools for end-to-end system monitoring Evidence must be in the form of a technology demonstration of tooling used to carry out proactive monitoring and alerting.	comprehensive alerting on application conditions as well as underlying infrastructure conditions. Our system includes web transaction monitoring via simulated transactions.
9.6. Next Generation Monitoring Capabilities	
9.6.1 Partner must implement service intelligence monitoring capabilities which gather intelligence from heterogeneous monitoring and logging sources. One of the values a next-generation MSP brings to customers is their ability to manage AWS workloads which, if designed correctly, are dynamic, highly automated environments that can scale up down according to demand. To be effective, next gen MSPs must use new technologies that give visibility into the full environment, including application performance. Furthermore, given the dynamic and highly automated nature of AWS workloads, MSPs should leverage monitoring tools that scale instantly to adjust to changes in workloads being monitored. Evidence should be in the form of a technology demonstration with a customer use case.	ScienceLogic can consume events and log data from a range of data sources and tools. **Example:** Collect EC2 + OS conditions via AWS + our agent + SNMP/WMI + PowerShell ScienceLogic has demonstrated this at another large scale public cloud provider to deliver their cloud compute auto-scaling functionality using our runbook automation engine. Our solution can add and drop compute instances automatically according to load levels and CPU/memory utilization metrics, in compliance with user-selected policies/rules for max/min compute levels for a given service. (Roadmap) In 2017, ScienceLogic will introduce new capabilities to automatically scale the monitoring system to deal with hyper-dynamic, transient workloads. This will include high granularity data sampling—much finer than traditional 5/10/15 minute intervals—enabling detailed visibility for highly transient workloads. ScienceLogic recently introduced new application infrastructure monitoring visibility that combines full stack visibility with dependency mapping to create complete views of business services. This will be further enhanced in 2017.
9.6.2 The monitoring solution used by Partner should have the ability to use statistical analysis algorithms to identify outliers or anomalies in metrics to generate alerts rather than defined thresholds. These can identify patterns in a single metric over time, or compare a metric for a single member of a cluster against other member nodes to identify unhealthy resources for replacement before an incident occurs. Evidence should be in the form of a technology demonstration of 2 customer use cases.	ScienceLogic applies standard deviation-based statistical analysis for algorithmic anomaly detection—for single devices or device groups. Combined with IT Service visibility, ScienceLogic generates events and dynamically adjusts thresholds based on device conditions (CPU, Memory, etc.) and IT service conditions (health, availability, risk).
9.6.3 The solution should apply machine learning capabilities to monitoring and log data. Monitoring machine learning solutions can be used in a predictive fashion, identifying trends in data to trigger actions prior to an anomaly or threshold breach being detected. In logging, machine learning solutions can provide suggestions to operators investigating root cause of an incident by surfacing related log events from across an application landscape, while accepting feedback from the operator on the relevance of the data. Evidence should be in the form of a technology demonstration of 2 customer use cases.	ScienceLogic applies machine learning with runbook automation to initiate actions prior to potential outages. **Example:** With machine learning and dynamic pooling, ScienceLogic can determine when a capacity problem may occur and proactively spin up additional server capacity prior to outage conditions occurring. So, IF # of concurrent sessions exceeds X AND CPU utilization exceeds Y% THEN spin up additional EC2 capacity to ensure load stays below that same Y%. And continue to maintain this over time.

9.7 Service Intelligence Reporting and Dashboards for Customers	
Partner provides customer with dashboard and advanced reporting capabilities that showcase a service-intelligence approach to monitoring, as opposed to more traditional threshold based monitoring and handling of events and incidents. Dashboards should provide comprehensive full-stack visibility in real-time, while also offering historical analysis and trending. Evidence must be in the form of dashboards and reporting for current or past customers.	Real-time dashboarding is a standard feature that shows live and historical device and service health and performance views—in addition to events and incidents. Live dependency maps show relationships between infrastructure elements. This shows conditions across not just individual devices—but groups of devices that deliver a service, showing IT service availability, health, and risk rather than device-specific metrics that provide no insight into service conditions. ScienceLogic shows at least layer 3-4 today—more for Microsoft applications—and will add additional application level visibility in 2017, including real-time views, high granularity, and log analysis.
9.8 Continuous Compliance	
9.8.1 Next-generation MSPs adopt a continuous approach to managing and monitoring compliance, both as it relates to new policies, audit requirements, and non-compliant changes within the environment. Partner provides continuous compliance solutions to their customers which apply to AWS managed resources. Examples include use of AWS CloudTrail or AWS Config to monitor changes to network configuration, access by IAM principals, or EBS encryption settings to ensure the system remains within policy. Evidence must be in the form of customer case studies which highlight shortened time to remediation and audit reduction time as well as a demonstration of continuous compliance tools and processes with documented outcomes.	ScienceLogic can apply change detection for infrastructure such as AWS VPCs and Security Groups, to alert upon new elements joining/leaving—and then use runbook automation to enforce compliance to port rules or new instances—and remediate back into compliance. ScienceLogic also collects date/time on what was changed using AWS Config. We can provide a reference instance at an AWS MSP partner.
9.8.2 Partner provides continuous compliance solutions to their customers to ensure compliance of resource level controls. Examples include ensuring CIS hardened instances remain hardened after deployment and maintaining log and configuration file integrity. Evidence must be in the form of customer case studies which highlight shortened time to remediation and audit reduction time as well as a demonstration of continuous compliance tools and processes with documented outcomes.	N/A

9.9 Event Management	
9.9.1 Partner has a process for detecting, categorizing, and taking action on all events. Events are generally: □ Informational in nature (and should be logged) □ Related to warnings (and should create alerts) □ Exception-based; dealing with something acting out of normal pattern (and should trigger an incident) An event is defined as a change of state that has significance for the management of an IT service or other configuration item. The term is also used to mean an alert or notification created by any IT service, configuration item or monitoring tool. Events typically require IT operations personnel to take actions, and often lead to incidents being logged. Event management is the process responsible for managing events throughout their lifecycle. (*ITIL Service Operation)*	An audit trail is core functionality within the ScienceLogic system. We provide extensive event correlation and de-duplication so that the MSP only needs to focus troubleshooting on the root cause of an issue—not the associated symptoms—which can cause multiple events, alerts, and incidents. Actions can be informational (events), warnings (email, pager notifications), and exception-based (notify only after a condition persists for a given length of time or occurs multiple times—or after other events in sequence)
9.9.2 Partner can demonstrate the ability to programmatically add value to customers' operations by differentiating between monitoring events that require customer engagement and those that don't. Partner must provide an example of filtering and sending event information to customers.	ScienceLogic enables operations teams to classify and prioritize events according to policies, devices, or other criteria/rules. Events can be correlated and de-duplicated to avoid operations teams receiving multiple incidents and wasting time investigating symptoms of the same problem. ScienceLogic can create and manage incidents directly in service management systems (ServiceNow, Remedy, etc.) or send root cause events to avoid incident/event storms and false positives. In some cases, customers have saved multiple $M in operations productivity.

ScienceLogic and MSPs

ScienceLogic has long been a provider of multi-tenanted monitoring system software to service providers. Unlike many monitoring solutions that were built for enterprises, ScienceLogic was designed and built from the ground up to meet the specific needs of MSPs—with a highly scalable, multi-tenanted monitoring platform. The platform helps MSPs generate new revenue streams through advanced services, including real-time visualization of customer infrastructure under management, and the creation of premium-tier Managed AWS offerings or dedicated advanced monitoring services.

Overview of ScienceLogic for Monitoring AWS Environments

ScienceLogic is a Hybrid IT service assurance solution for monitoring and managing all aspects of private and public cloud technologies, such as AWS, as well as on-premises network, storage, and compute elements. ScienceLogic discovers, classifies, maps relationships, and monitors IT elements regardless of technology, vendor, or location. Customer-facing dashboards provide simple visualization of any configuration, health, performance, or availability metrics on individual devices, groups of devices, or complete services. ScienceLogic provides rich event management, and can automatically initiate actions upon error conditions or policy violations.

MSPs adopt ScienceLogic for its deep monitoring visibility into AWS configuration status and performance, as well as its hybrid IT capability that includes extensive automation plus service and application visibility. For more detailed descriptions of ScienceLogic please visit our website at www.sciencelogic.com