G-Cloud 13 Amazon Web Services EMEA SARL, UK Branch (AWS) – AWS Managed Services (AMS) Advanced Operations Plan Service Definition Document

May 2022

G-Cloud 13 Amazon Web Services EMEA SARL, UK Branch (AWS) – AWS Managed Services (AMS) Advanced Operations Plan Service Definition Document

Table of Contents

1. AWS Managed Services (AMS)

The following subsections provide service definition information in accordance with the requirements identified in the ITT.

1.1. Service Overview

AMS is an enterprise service that provides ongoing management of your AWS infrastructure. AMS implements best practices and maintains your infrastructure to reduce your operational overhead and risk. AMS provides full-lifecycle services to provision, run, and support your infrastructure, and automates common activities such as change requests, monitoring, patch management, security, and backup services. AMS enforces your corporate and security infrastructure policies, and enables you to develop solutions and applications using your preferred development approach.

AWS Managed Services is available with two operations plans: AMS Accelerate and AMS Advanced. An operations plan offers a specific set of features and has differing levels of service, technical capabilities, requirements, price, and restrictions. Our operations plans give you the flexibility to select the right-sized operational capabilities for each of your AWS workloads. This section outlines the capabilities and differences, as well as the responsibilities, features, and benefits associated with each plan, so that you can understand which operations plan is best for your accounts.

A detailed feature comparison of the two operations plans can be found here: https://aws.amazon.com/managed-services/features/

This document provides detail for the AMS Advanced Operations Plan. AMS Advanced provides full-lifecycle services to provision, run, and support your infrastructure and also includes additional services, such as landing zone management, infrastructure changes and provisioning, access management, and endpoint security. AMS Advanced deploys a landing zone to which you migrate your AWS workloads and receive AMS operational services. Our managed multi-account landing zones are pre-configured with the infrastructure to facilitate authentication, security, networking, and logging.

AMS Advanced also includes a change and access management system that protects your workloads by preventing unauthorized access or the implementation of risky changes to your AWS infrastructure. Customers need to create a Request for Change (RFC) using our Change Management system to implement most changes in your AMS Advanced accounts. You create RFCs from a library of automated changes that are pre-vetted by our security and operations teams or request manual changes that are reviewed and implemented by our operations team if they are deemed both safe and supported by AMS Advanced.

Key benefits include:

- **Operational Flexibility.** AWS Managed Services (AMS) provides you with flexibility in selecting the right level of operations assistance, whether you are migrating to the cloud or just need extra help with monitoring, incidents, or patch management. AMS cloud experts, who are deeply integrated with AWS service teams, work alongside your existing operations team to provide proven operational assistance.
- **Enhanced Security and Compliance.** AWS Managed Services offers a step-by-step process for extending your security, identity, and compliance perimeter to the cloud, including the critical tasks of Active Directory integration and AMS reduces the burden of meeting compliance program requirements (GDPR, SOC, NIST, ISO, PCI) through automated detection and remediation automations. Our rigour and controls help to

enforce your corporate and security infrastructure policies, and enable you to develop solutions and applications using your preferred development approach. AMS builds and maintains a growing repository of compliance, operational, and security guardrails that help keep you aligned with your controls.

- **Accelerate Migration to the Cloud.** AWS Managed Services provides an enterprise-ready, proven operating environment, enabling you to migrate production workloads in days versus months. Working with AWS Partners and AWS Professional Services, AMS leverages the minimum viable refactoring approach of making only necessary modifications to your applications to meet security and compliance requirements. AMS then takes responsibility for operating your cloud environment post migration, such as analyzing alerts and responding to incidents, enabling your internal resources to focus on the more strategic areas of your business.
- **Remove Innovation Barriers.** Enterprise DevOps is the convergence of modern development best practices (i.e. DevOps) and existing IT process frameworks (i.e. ITIL ®) to give you speed and agility while maintaining governance, security, and compliance control. AMS enables Enterprise DevOps by packaging AWS IaaS services into a secure, compliant development platform that works with most enterprise workloads – not just cloud-native or heavily refactored workloads. AMS-powered Enterprise DevOps helps your development teams focus on their applications and innovate faster.
- **Cost Optimization.** AWS Managed Services (AMS) helps with financial and capacity optimization across your AWS estate, and any savings identified reduces your AMS fee without impacting operational outcomes or security. AMS customers have enjoyed up to 30% in operational savings and up to 25% in AWS infrastructure savings while also improving operational SLAs, security, and compliance posture. AMS also provides a flexible consumption-based pricing model and month-to-month contracting. Pay for what you use and take back operational control when you are ready.

1.2. Service Description

The AMS features are:

- **Logging, Monitoring, Guardrails, and Event Management:** AMS configures and monitors your managed environment for logging activity and defines alerts based on a variety of health checks. Alerts are investigated by AMS for applicable AWS services, and those that negatively impact your usage of those services result in the creation of incidents. AMS aggregates and stores all logs generated as a result of all operations in CloudWatch, CloudTrail, and system logs in S3. Upon request, you can ask for additional alerts to be put in place. In addition to AMS' preventative controls, AMS deploys configuration guardrails and detective controls to provide ongoing protection for you from misconfigurations that could reduce the operational and security integrity of the managed accounts, to enforce your controls such as tagging and compliance. When a monitored control is detected an alarm is generated that results in notification, modification, or termination of resources based on pre-defined AMS defaults that can be modified by you.
- **Continuity Management (Backup and Restore):** AMS provides backups of resources using standard, existing AWS Backup functionality on a scheduled interval determined by you. Restore actions from specific snapshots can be performed by AMS with your RFC. Data changes that occur between snapshot intervals are the responsibility of you to backup. You can submit an RFC for backup or snapshot requests outside of scheduled intervals. In the case of Availability Zone (AZ) unavailability in an AWS

Region, with your permission, AMS restores the managed environment by recreating new stack(s) based on templates and available EBS snapshots of the impacted Stacks.

- **Security and Access Management:** AMS provides endpoint security (EPS) such as configuring anti-virus and anti-malware protection. You can also use your own EPS tool and processes and not use AMS for EPS using a feature called bring your own EPS (BYOEPS). AMS also configures default AWS security capabilities that are approved by you during onboarding, such as identity access management (IAM) roles and EC2 security groups, and uses standard AWS tools (e.g. SecurityHub, Macie, GuardDuty) to monitor and respond to security issues. You manage your users through an approved directory service provided by you. For a list of approved directory services, see Supported configurations. AMS includes endpoint security (EPS), which is inclusive of antivirus (AV), and anti-malware protection, malware and intrusion detection (Trend Micro). Security groups are defined per stack template and are modified at launch depending on the visibility of the application (public/private) security groups. Access to systems is requested through change management requests for change (RFCs). Access management provides access to distinct resources, such as Amazon EC2 instances, the AWS Management Console, and APIs. After establishing a one-way trust with an AMS Microsoft Active Directory deployment during onboarding and federating to AWS, you can use your existing corporate credentials for all interactions.
- **Patch Management:** AMS applies and installs updates to EC2 instances for supported operating systems (OSs) and software pre-installed with supported operating systems. For a list of supported operating systems, see Supported configurations. AMS offers two models for patching:
    - AMS standard patch for traditional account-based patching, and
    - AMS Patch Orchestrator, for tag-based patching.

  In AMS standard patch, a monthly maintenance window is chosen by you for AMS to perform most patching activities. AMS applies critical security updates outside of the selected maintenance window (with appropriate notifications) and important updates during the selected maintenance window. AMS additionally applies updates to infrastructure management tools during the selected maintenance window. You can exclude stacks from patch management or reject updates, if you want.

  With AMS Patch Orchestrator, a default maintenance window per account, is defined by you for AMS to perform patching activities. You can schedule additional custom maintenance windows for AMS to patch a specific set of instances defined by you with tags. AMS applies all available updates, but you can filter or reject updates by creating a custom patch baseline. For both models, if you approve or reject an update provided under patch management but later change your mind, you are responsible for initiating the update via an RFC. AMS tracks the patch status of resources and highlights systems that aren't current in the monthly business review. Patch management is limited to stacks in the managed environment, including all AMS managed applications and supported AWS services with patching capabilities (for example, RDS). In order to support all types of infrastructure configurations when an update is released, AMS a) updates the EC2 instance and b) provides an updated AMS AMI for you to use. It is your responsibility to install, configure, patch, and monitor any additional applications not specifically covered above.
- **Change Management:** AMS offers Change Management, which is the mechanism for you to get access to, or affect any changes in, your managed environment. You create a

request for change (RFC) using the AMS interface. Most RFCs requested are executed automatically. AMS creates RFCs to access your resources or make changes, when needed. All RFCs follow a defined change management process. Access to your resources within a managed production environment is authorized through RFCs, while access to your resources in a managed non-production environment is authorized through RFC and, optionally, through a specialized customer-developer IAM role ("Developer Mode"), upon request. AMS approves and executes RFCs that can be executed using the features or functionalities of AWS services. You can designate a start time for the requested change to be performed through the RFC process. You can also use change management to configure AWS Service offerings in your managed environment.

All actions on your AMS resources are coordinated by the AMS change management service and logged in AWS CloudTrail, which records API calls. The AMS system manages requests for change (RFCs), scheduling to prevent overlapping activities, and change approvals. RFCs are classified, and those known to have low risk or impact are run by automated scripts.

In a multi-account landing zone (MALZ) environment, the degree of change management can differ depending on what AMS mode you are using (modes do not apply to AMS single-account landing zone environments). For more information, see AMS Modes.

- **Automated and Self-service Provisioning Management:**

  You can provision AWS resources on AMS in several ways:

  - Submit provisioning and configuration change types
  - Deploy AMS-provided security-hardened AMIs inclusive of your application
  - Deploy full stacks using CloudFormation templates
  - Deploy through your integrated IT service management (ITSM)
  - Deploy through AWS Service Catalog
  - Configure AWS services directly using self-service provisioning for select AWS services (see Supported AWS services).

  To provide self-service provisioning capabilities, AMS has created elevated IAM roles with permission boundaries to limit unintended changes from direct AWS service access. Roles do not prevent all changes and you are responsible to adhere to your internal controls, compliance, and to validate that all AWS services being used meet the required certifications. We call this the self-service provisioning mode. For details on AWS compliance requirements, see AWS Compliance.

  For resources that you provision through self-service, AMS provides incident management, detective controls and guardrails, reporting, designated resources (Cloud Service Delivery Manager and Cloud Architect), Security & access, and technical support via service requests. Additionally, where applicable, you assume responsibility for continuity management, patch management, infrastructure monitoring, and change management for resources provisioned or configured outside of the AMS change management system.

- **Incident management:** AMS proactively notifies you of incidents detected by AMS. AMS responds to both customer-submitted and AMS-generated incidents and resolves

incidents based on the incident priority. Unless otherwise instructed by you, incidents that are determined by AMS to be a risk to the security of your managed environment, and incidents relating to the availability of AMS and other AWS services, are proactively actioned. AMS takes-action on all other incidents once your authorization is received. Recurring incidents are addressed by the problem management process.

- **Problem management:** AMS performs trend analysis to identify and investigate problems and to identify the root cause. Problems are remediated either with a workaround or a permanent solution that prevents recurrence of similar future service impact. A post incident report (PIR) may be requested for any "High" incident, upon resolution. The PIR captures the root cause and preventative actions taken, including implementation of preventative measures.
- **Reporting:** AMS provides you with a monthly service report that summarizes key performance metrics of AMS, including an executive summary and insights, operational metrics, managed resources, AMS service level agreement (SLA) adherence, and financial metrics around spending, savings, and cost optimization. Reports are delivered by the AMS cloud service delivery manager (CSDM) assigned to you.
- **Service Request Management:** You can request information about your managed environment, AMS, or AWS service offerings by submitting service requests using the AMS interface. Service request types also include "How to" questions about AWS services and features, troubleshooting API issues, and technical support cases.
- **Service Desk:** AMS staffs engineering operations with full-time Amazon employees to fulfill non-automated requests including incident management, service request management, and change management. The Service Desk operates 24 x 7 365 days a year.
- **Designated Resources:** Each customer is assigned a Cloud Service Delivery Manager (CSDM) and a Cloud Architect (CA).

  CSDMs can be contacted directly. They perform service reviews, and delivery reporting and insights through all phases of the implementation, migration and operational life cycle. CSDMs conduct monthly business reviews and detail items such as financial spend, cost-saving recommendations, service utilization, and risk reporting. They dive deep into operational performance statistics and provide recommendations of areas of improvements.

  CAs can be contacted directly and provide technical expertise to help you optimize your use of the AWS cloud. Example CA activities include, selecting workloads for migration, assisting with the onboarding additional accounts and workloads, acting as the technical lead in operational activities such as game days, disaster recovery testing, problem management, and technical advice to get the most out of AMS and AWS. CAs drive technical discussions at all levels of your organization and assist with incident management, making trade-offs, establishing best practices, and technical risk mitigation.
- **Developer Mode:** This feature enables you to iterate infrastructure designs and deployments quickly within AMS-configured accounts by allowing direct access to AWS service APIs and the AWS console in addition to access to the AMS change management process. Resources provisioned or configured with developer mode permissions outside of the change management process are your responsibility to manage (See "Automated and Self-Service Provisioning Management"). Resources

provisioned through the AMS change management process are supported like other change management-provisioned workloads on AMS.

- **AWS Support:** AMS customers can choose the level of AWS Support they require to complement their AMS Operations plan. Accounts enrolled in AMS can be subscribed to either Business Support or Enterprise Support. To learn about the differences in Support Plans, see https://aws.amazon.com/premiumsupport/plans/.
- **Customer-Managed Account:** This feature enables you to request AWS accounts within the same managed environment but the ongoing operations of workloads and AWS resources within those accounts are your responsibility. AMS provisions customer-managed accounts, but once the accounts are created, no other AMS features or services are provided to those accounts. AWS will not enroll customer-managed accounts in enterprise-level premium support. It will be your responsibility to enroll customer-managed accounts in AWS support at the support rate you choose.
- **Firewall Management:** AMS provides an optional managed firewall solution for Supported Firewall Services, which enables internet-bound egress traffic filtering for networks in your managed environment. This excludes public-facing services that do not use the AWS network infrastructure and whose traffic goes directly to the internet. The solution combines industry-leading firewall technology with AMS infrastructure management capabilities to deploy, monitor, manage, scale, and restore the firewall infrastructure.

When you onboard AMS, you receive a complete list of your AMS network infrastructure. To get an updated list of services running in support of your AMS infrastructure at any time, file a service request with specifics about the information you want. To request a change to your network design, create a service request describing the changes you want to make—for example, adding a VPC or requesting a security group rule change.

AMS can also be procured through the UK AMS partner, Mobilise Cloud. Mobilise Cloud will contract with you and can provide additional services on top of the scope of AMS, with AMS delivering its service with no service change. For details, search for AMS delivered through Mobilise Cloud on the portal.

1.3. Service Definitions

The AMS Advanced Operations Plan User Guide can be found here:
https://docs.aws.amazon.com/managedservices/latest/userguide/what-is-ams.html

The Service Description in the User Guide can be found here:
https://docs.aws.amazon.com/managedservices/latest/userguide/ams-sd.html

The Service Key Terms in the User Guide can be found here:
https://docs.aws.amazon.com/managedservices/latest/userguide/key-terms.html

Selected Key Service Terms are detailed below:

AMS Advanced: The services described in the "Service Description" section of the AMS Advanced Documentation.

AMS Advanced Accounts: AWS accounts that at all times meet all requirements in the AMS Advanced Onboarding Requirements.

Critical Recommendation: A recommendation issued by AWS through a Service Request informing you that your action is required to protect against potential risks or disruptions to your

resources or the AWS services. If you decide not to follow a Critical Recommendation by the specified date, you are solely responsible for any harm resulting from your decision.

Customer-Requested Configuration: Any software, services or other configurations that are not identified in AMS Advanced: Supported Configurations or AMS Advanced; Service Description.

Incident Communication: AMS communicates an Incident to you or you request an Incident with AMS via an Incident created in Support Center for AMS Accelerate and in the AMS Console for AMS. The AMS Accelerate Console provides a summary of Incidents and Service Requests on the Dashboard and links to Support Center for details.

Managed Environment: The AMS Advanced accounts and or the AMS Accelerate accounts operated by AMS.

Billing start date: AWS Managed Services accounts are activated once you have granted access to AMS to a compatible account and AMS Activation notification occurs as defined in the AWS Managed Services Documentation. If the activation of the AWS Managed Services accounts, Add-on Service Request, or Account tier Service Request is received by AWS on or prior to the 20th day of the month, then the change will be effective as of the first day of the calendar month following the AMS Activation notification or such Service Request. If the activation or Service Request is received by AWS after the 20th day of the month, then the change will be effective as of the first day of the second calendar month following AMS Activation notification or such Service Request.

Service Termination Date: The last day of the calendar month in which the customer provides the AMS Account Service Termination Request, or the last day of the calendar month following the end of the requisite notice period; provided that, if the Customer provides the AMS Account Service Termination Request after the 20th day of the calendar month, the Service Termination Date will be the last day of the calendar month following the calendar month that such AMS Account Service Termination Request was provided.

Provision of AWS Managed Services: AWS will make available to customer and customer may access and use AWS Managed Services for each AWS Managed Services account from the service commencement date.

Termination for specified AWS Managed Services accounts: Customer may terminate the AWS Managed Services for a specified AWS Managed Services account for any reason by providing AWS notice through a service request ("AMS Account Termination Request").

Effect of Termination of specified AWS Managed Services accounts: On the Service Termination Date, AWS will (i) hand over the controls of all AMS accounts or the specified AMS account, as applicable, to customer, or (ii) the parties will remove the AWS Identity and Access Management roles that give AWS access from all AMS Accelerate accounts or the specified AMS Accelerate account, as applicable.

Incident management terms:

Event: A change in your AMS environment.

Alert: Whenever an event from a supported AWS service exceeds a threshold and triggers an alarm, an alert is created and notice is sent to your contacts list. Additionally, an incident is created in your Incident list.

Incident: An unplanned interruption or performance degradation of your AMS environment or AWS Managed Services that results in an impact as reported by AWS Managed Services or you.

Problem: A shared underlying root cause of one or more incidents.

Incident Resolution or Resolve an Incident:

- AMS has restored all unavailable AMS services or resources pertaining to that incident to an available state, or
- AMS has determined that unavailable stacks or resources cannot be restored to an available state, or
- AMS has initiated an infrastructure restore authorized by you.

Incident Response Time: The difference in time between when you create an incident, and when AMS provides an initial response by way of the console, email, service center, or telephone.

Incident Resolution Time: The difference in time between when either AMS or you create an incident, and when the incident is resolved.

Incident Priority: How incidents are prioritized by AMS, or by you, as either Low, Medium, or High.

- Low: A non-critical problem with your AMS service.
- Medium: An AWS service within your managed environment is available but is not performing as intended (per the applicable service description).
- High: Either (1) the AMS Console, or one or more AMS APIs within your managed environment are unavailable; or (2) one or more AMS stacks or resources within your managed environment are unavailable and the unavailability prevents your application from performing its function.

AMS may re-categorize incidents in accordance with the above guidelines.

Infrastructure Restore: Re-deploying existing stacks, based on templates of impacted stacks, and initiating a data restore based on the last known restore point, unless otherwise specified by you, when incident resolution is not possible.

Infrastructure terms:

Managed production environment: A customer account where the customer's production applications reside.

Managed non-production environment: A customer account that only contains non-production applications, such as applications for development and testing.

AMS stack: A group of one or more AWS resources that are managed by AMS as a single unit.

Immutable infrastructure: An infrastructure maintenance model typical for EC2 Auto Scaling groups (ASGs) where updated infrastructure components, (in AWS, the AMI) are replaced for every deployment, rather than being updated in-place. The advantages to immutable infrastructure are that all components stay in a synchronous state since they are always generated from the same base. Immutability is independent of any tool or workflow for building the AMI.

Mutable infrastructure: An infrastructure maintenance model typical for stacks that are not EC2 Auto Scaling groups and contain a single instance or just a few instances. This model most closely represents traditional, hardware-based, system deployment where a system is deployed at the beginning of its life cycle and then updates are layered onto that system over time. Any

updates to the system are applied to the instances individually, and may incur system downtime (depending on the stack configuration) due to application or system restarts.

Security groups: Virtual firewalls for your instance to control inbound and outbound traffic. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could have a different set of security groups assigned to it.

Service Level Agreements (SLAs): Part of AMS contracts with you that define the level of expected service.

SLA Unavailable and Unavailability:

- An API request submitted by you that results in an error.
- A Console request submitted by you that results in a 5xx HTTP response (the server is incapable of performing the request).
- Any of the AWS service offerings that constitute stacks or resources in your AMS-managed infrastructure are in a state of "Service Disruption" as shown in the Service Health Dashboard
- Unavailability resulting directly or indirectly from an AMS exclusion is not considered in determining eligibility for service credits. Services are considered available unless they meet the criteria for being unavailable.

Service Level Objectives (SLOs): Part of AMS contracts with you that define specific service goals for AMS services.

Patching terms:

Mandatory patches: Critical security updates to address issues that could compromise the security state of your environment or account. A "Critical Security update" is a security update rated as "Critical" by the vendor of an AMS-supported operating system.

Patches announced versus released: Patches are generally announced and released on a schedule. Emergent patches are announced when the need for the patch has been discovered and, usually soon after, the patch is released.

Patch add-on: Tag-based patching for AMS instances that leverages AWS Systems Manager (SSM) functionality so you can tag instances and have those instances patched using a baseline and a window that you configure.

Patch methods:

- *In-place patching:* Patching that is done by changing existing instances.
- *AMI replacement patching:* Patching that is done by changing the AMI reference parameter of an existing EC2 Auto Scaling group launch configuration.

Patch provider (OS vendors, third party): Patches are provided by the vendor or governing body of the application.

Patch Types:

- Critical Security Update (CSU): A security update rated as "Critical" by the vendor of a supported operating system.
- Important Update (IU): A security update rated as "Important" or a non-security update rated as "Critical" by the vendor of a supported operating system.

- Other Update (OU): An update by the vendor of a supported operating system that is not a CSU or an IU.

Supported patches: AMS supports operating system level patches. Upgrades are released by the vendor to fix security vulnerabilities or other bugs or to improve performance. For a list of currently supported OSs, see Support Configurations.

Security terms:

Detective Controls: A library of AMS-created or enabled monitors that provide ongoing oversight of customer managed environments and workloads for configurations that do not align with security, operational, or customer controls, and take action by notifying owners, proactively modifying, or terminating resources.

Service Request terms:

Service request: A request by you for an action that you want AMS to take on your behalf.

Alert notification: A notice posted by AMS to your Service requests list page when an AMS alert is triggered. The contact configured for your account is also notified by the configured method (for example, email). If you have contact tags on your instances/resources, and have provided consent to your cloud service delivery manager (CSDM) for tag-based notifications, the contact information (key value) in the tag is also notified for automated AMS alerts.

Service notification: A notice from AMS that is posted to your Service request list page, usually to notify you of upcoming patching.

Miscellaneous terms:

AWS Managed Services Interface: For AMS: The AWS Managed Services Advanced Console, AMS CM API, and AWS Support API.

Customer satisfaction (CSAT): AMS CSAT is informed with deep analytics including Case Correspondence Ratings on every case or correspondence when given, quarterly surveys, and so forth.

DevOps: DevOps is a development methodology that strongly advocates automation and monitoring at all steps. DevOps aims at shorter development cycles, increased deployment frequency, and more dependable releases by bringing together the traditionally-separate functions of development and operations over a foundation of automation. When developers can manage operations, and operations informs development, issues and problems are more quickly discovered and solved, and business objectives are more readily achieved.

ITIL: Information Technology Infrastructure Library (called ITIL) is an ITSM framework designed to standardize the lifecycle of IT services. ITIL is arranged in five stages that cover the IT service lifecycle: service strategy, service design, service transition, service operation, and service improvement.

IT service management (ITSM): A set of practices that align IT services with the needs of your business.

Managed Monitoring Services (MMS): AMS operates its own monitoring system, Managed Monitoring Service (MMS), that consumes AWS Health events and aggregates AWS CloudWatch data, and data from other AWS services, notifying AMS operators (online 24x7) of any alarms created through an Amazon Simple Notification Service (Amazon SNS) topic.

1.4. Pricing Overview

Please see the AWS UK G-Cloud 13 Pricing Document affiliated with this service in the Digital Marketplace.

1.5. Governance

You are designated a cloud service delivery manager (CSDM) who provides advisory assistance across AMS, and has a detailed understanding of your use case and technology architecture for the managed environment. CSDMs work with account managers, technical account managers, AWS Managed Services cloud architects (CAs), and AWS solution architects (SAs), as applicable, to help launch new projects and give best-practices recommendations throughout the software development and operations processes. The CSDM is the primary point of contact for AMS. Key responsibilities of your CSDM are:

- Organize and lead monthly service review meetings with customers.
- Provide details on security, software updates for environment and opportunities for optimization.
- Champion your requirements including feature requests for AMS.
- Respond to and resolve billing and service reporting requests.
- Provide insights for financial and capacity optimization recommendations.

1.6. Contact and Escalation

AWS Managed Services will work on all customer requests during Business Hours as indicated below:

Feature	AMS Advanced	
	Plus Tier	Premium Tier
Service request	Monday to Friday: 08:00–18:00, local business hours	24/7
Incident management (P1)	24/7	24/7
Incident management (P2-P3)	Monday to Friday: 08:00–18:00, local business hours	24/7
Backup and recovery	24/7	24/7
Patch management	24/7	24/7
Monitoring and alerting	24/7	24/7
Automated request for change (RFC)	24/7	24/7
Non-automated request for change (RFC)	Monday to Friday: 08:00–18:00, local business hours	24/7
Cloud service delivery manager (CSDM)	Monday to Friday: 08:00–17:00, local business hours	Monday to Friday: 08:00–17:00, local business hours

For specific questions about how you or your resources or applications are working with AMS, or to escalate an incident, email one or more of the following:

- First, if you are unsatisfied with the service request or incident report response, email your CSDM: ams-csdm@amazon.com
- Next, if escalation is required, you can email the AMS Operations Manager (your CSDM will most likely do this): ams-opsmanager@amazon.com
- Further escalation would be to the AMS Director: ams-director@amazon.com
- Finally, you are always able to reach the AMS VP: ams-vp@amazon.com

The following table describes the goals of the AMS service. Service Level Agreements (SLAs) for other aspects of the AMS service, including incident management, are covered in the SLA.

Feature	Performance Indicator (PI)	**Plus** (Business Days, M-F 8AM to 6PM local time)	**Premium** (Calendar Days, 24 x 7)
Change Management	Time taken to schedule or reject automated RFCs	<=30 min	<=30 min
	Time of initiation of scheduled RFCs compared to scheduled execution time	<=1 min	<=1 min
	Time taken to approve/reject non-automated RFCs, available in CT catalogue	<=48 hours	<=24 hours
	Time taken to approve/reject non-automated RFCs not available in CT catalogue	<=5 days	<=5 days
Problem Management	Time taken to complete root cause analysis (RCA)	<=10 days	<=10 days
Service Request Management	Response time for first and every subsequent reply	<=8 hours	<=4 hours

1.7. Supported Configuration

These are the configurations AMS supports:

- **Language:** AMS is available in English.
- **Firewall Services:** Palo Alto VM-Series Next-Generation Firewall
- **Security software:** Deep Security from Trend Micro. AWS Marketplace: Trend Micro Deep Security
- **Approved directory services:** Microsoft Active Directory (AD)
- **Supported AWS Regions:**
    - AMS operates in a subset of all AWS Regions; however, the AMS API/CLI runs out of the "USA East (N. Virginia)" Region only. If you run either the AMS change management API (amscm) or the AMS service knowledge management API (amsskms), in a non-USA East Region, you must add --region us-east-1 to the command.
    - US East (Virginia), US West (N. California), US West (Oregon), US East (Ohio), Canada (Central)
    - South America (São Paulo)

  - EU (Ireland), EU (Frankfurt), EU (London), EU West (Paris)
  - Asia Pacific (Mumbai), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo)

- **Amazon machine images (AMIs):** AMS provides security enhanced images (AMIs) based on CIS Level 1 benchmark for a subset of AMS's supported operating systems. To find out which operating systems have a security enhanced image available, see the AMS Security User Guide, which is available through AWS Artifact -> Reports tab filtered for AWS Managed Services. To access AWS Artifact, can contact your CSDM for instructions or go to Getting Started with AWS Artifact
- **Supported operating systems:**
  - Amazon Linux 2
  - CentOS 7.x
  - Oracle Linux 7.5 and later minor versions
  - Red Hat Enterprise Linux (RHEL) 8.x, 7.x
  - SUSE Linux Enterprise Server 15 SP0, SP1 and SAP specific versions, SUSE Linux Enterprise Server 12 SP4, SP5 and SAP specific versions.
  - Microsoft Windows Server 2019, 2016, 2012 R2, 2012
- Supported End of Support (EOS) operating systems:
  - Amazon Linux (expected AMS support end date July 1, 2023)
  - CentOS 6.5-6.10 (expected AMS support end date Feb 1, 2023)
  - RedHat Enterprise Linux (RHEL) 6.5-6.10 (expected AMS support end date Feb 1, 2023)
  - Microsoft Windows Server 2008R2 (expected AMS support end date Feb 1, 2023)

  Note:

  - End of Support (EOS) operating systems are outside of the general support period of the operating system manufacturer and have increased security risk. EOS operating systems are considered supported configurations only if AMS-required agents support the operating system and
    - you have extended support with the operating system vendor that allows you to receive updates, or
    - any instances using an EOS operating system follow the security controls as specified by AMS in the Advanced User Guide, or
    - you comply with any other compensating security controls required by AMS.
  - In the event AMS is no longer able to support an EOS operating system, AMS issues a Critical Recommendation to upgrade the operating system.
  - AMS-required agents may include but are not limited to: AWS Systems Manager, Amazon CloudWatch, Endpoint Security (EPS) agent, and Active Directory (AD) Bridge (linux only).

1.8. Supported AWS Services

AWS Managed Services provides operational management support services for the following AWS services. Each AWS service is distinct and as a result AMS's level of operational management support varies depending on the nature and characteristics of the underlying AWS service. Specific AWS services are grouped based on the complexity and scope of the operational management support service provided by AMS.

Note:

- In the following table, one star (*) indicates services that are deployed within an AMS managed environment by a customer using the AWS Console and APIs. See 'Automated and Self-service Provisioning Management' in 1.2 Service Description - AMS features for additional details on customer responsibilities when provisioning and configuring services in this manner.
- Two stars (**) indicates that EC2 on AWS Outposts will be billed as a Group B service; all other resources hosted on AWS Outposts will be billed at their standard rate.

Group A	Group B	Group C
Amazon Alexa for Business*	Amazon API Gateway*	Amazon Aurora
Amazon Managed Streaming for Apache Kafka*	Amazon AppStream*	Amazon CloudWatch
Amazon Simple Storage Service	Amazon Athena*	Amazon Elastic Block Store (EBS)
Amazon CloudFront	Amazon CloudSearch*	Amazon Elastic Compute Cloud**
Amazon Elastic File System	Amazon Cognito*	Amazon Elastic Load Balancing (classic, application, and network; not gateway)
Amazon Glacier	Amazon Comprehend*	Amazon ElastiCache
Amazon Simple Storage Service	Amazon Connect*	Amazon OpenSearch Service
AWS Amplify*	Amazon Document DB (with MongoDB compatibility)*	Amazon GuardDuty
AWS AppMesh*	Amazon DynamoDB*	Amazon Macie
AWS Auto Scaling	Amazon EC2 Container Registry (ECR)*	Amazon Redshift
AWS Backup	Amazon ECS Fargate*	Amazon Relational Database Service
AWS CloudFormation	Amazon Elastic Container Service for Kubernetes*	Amazon Route 53
AWS Compute Optimizer	Amazon EKS on AWS Fargate*	Amazon Simple Email Service
AWS Global Accelerator*	Amazon Elemental MediaConvert*	Amazon Simple Notification Service
AWS Identity and Access Management	Amazon Elemental MediaPackage*	Amazon Simple Queue Service
AWS License Manager*	Amazon Elemental MediaStore*	Amazon Virtual Private Cloud (VPC)
AWS Management Console	Amazon Elemental MediaTailor*	AWS CloudTrail
AWS Marketplace	Amazon Elastic MapReduce*	AWS Config
AWS Lake Formation*	Amazon EventBridge*	AWS Database Migration Service
AWS Well Architected Tool*	Amazon Forecast*	AWS Data Transfer
VM Import/ Export*	Amazon FSx*	AWS Direct Connect
	Amazon Inspector*	AWS Directory Service
	Amazon Kinesis Analytics*	AWS Key Management Service
	Amazon Kinesis Firehose*	AWS Systems Manager (SSM)
	Amazon Kinesis*	
	Amazon Kinesis Video Streams*	
	Amazon Lex*	
	AWS Migration Hub	
	Amazon MQ*	
	Amazon Personalize**	
	Amazon QuickSight*	
	Amazon Rekognition*	
	Amazon SageMaker*	
	Amazon SimpleDB*	
	Amazon Simple Workflow*	
	Amazon Textract*	
	Amazon Transcribe*	
	Amazon Translate*	
	Amazon WorkDocs*	
	Amazon WorkSpaces*	
	AWS AppSync*	

Group A	Group B	Group C
	AWS Audit Manager* AWS Batch* AWS Certificate Manager* AWS CloudEndure* AWS CloudHSM* AWS CodeBuild* AWS CodeCommit* AWS CodeDeploy* AWS CodePipeline* AWS DataSync* AWS Elemental MediaLive* AWS Glue* AWS Lambda* AWS Migration Hub* AWS Outposts** AWS Secrets Manager* AWS Security Hub* AWS Service Catalog AWS Transfer for SFTP* AWS Shield* AWS Snowball* AWS Step Functions* AWS Transit Gateway* AWS WAF* AWS X-Ray*	

If you request AWS Managed Services to provide services for any software or service that is not expressly identified as supported below, any AWS Managed Services provided for such customer requested configurations will be treated as a "Beta Service" under the Service Terms.

1.9. Roles and Responsibilities

AMS manages your AWS infrastructure. The following table provides an overview of the responsibilities of customer and AMS for activities in the lifecycle of an application running within the Managed Environment. AMS is not responsible for any of the following activities for customer-managed accounts or the infrastructure running within them, therefore this RACI is not applicable.

R stands for responsible party that does the work to achieve the task.

C stands for consulted; a party whose opinions are sought, typically as subject matter experts; and with whom there is bilateral communication.

I stands for informed; a party which is informed on progress, often only on completion of the task or deliverable.

Self-service Provisioning refers to resources that are provisioned by the customer via self-service through the AWS API or Console including Developer Mode and Self-Service Provisioned Services.

The tables below provide more details on the responsibilities of the customer and AWS Managed Services for operational activities within the Managed Environment.

Activity	Customer	AMS
Application lifecycle		
Application development	R	I
Application infrastructure requirements analysis and design	R	C
Design and optimization for non-standard AMS stacks	R	C

Activity	Customer	AMS
Design and optimization of AMS standard stack	I	R
Application deployment	R	C
AWS Infrastructure deployment	C	R
Application monitoring	R	I
Application testing/optimization	R	I
AWS infrastructure optimization guidance	I	R
AWS infrastructure monitoring	I	R
Troubleshoot and resolve application issues	R	C
Troubleshoot and resolve AWS network issues	C	R
Troubleshoot and resolve operating system and infrastructure issues *Self-Service Provisioning*	C R	R C
Application and ITSM Integration		
Application integration with AWS Service Offerings	R	C
ITSM integration with the AWS Managed Services Interface	R	C
Networking		
Managed Environment VPC and VPC set-up and configuration	C	R
Allocate private address space for VPCs (e.g. /16)	R	C
Configure & Operate non-AWS Managed Services, Customer managed Firewalls/Proxy/Bastions/HOSTs	R	C
Configure & Operate AWS Security Groups/NAT/Customer Bastions/NACL inside the Managed Environment	I	R
Networking (e.g. Direct Connect) configuration and implementation within customer network	R	C
Networking configuration and implementation within the Managed Environment	C	R
Managed environment configuration		
Define default Auto Scaling settings for baseline Stack templates	I	R
Recommend RI optimization	C	R
Purchase RI and PIOP capacity	R	C
Remove capacity when capacity is over provisioned (when supported by customer application)	C	R
Create/update AWS customer specific information for AWS Managed Services	C	R
S3 configuration *Self-Service Provisioning*	C R	R C
Glacier configuration	C	R
Define archival policy	R	C
Archival policy configuration	C	R
Selecting customer maintenance window	R	I
AWS RDS Management		
Monitor source/replica/RO replication health	I	R
Identify RCA of source failover	I	R
Automated snapshot (backup) configuration Self-service provisioning	C R	R C
Coordinate and schedule DB engine patch management Self-service provisioning	C R	R C
Recommend DB storage and PIOP capacity	C	R

Activity	Customer	AMS
Self-service provisioning	R	C
Recommend instance sizing for running databases Self-service provisioning	C R	R C
Recommend RI optimization for Managed Environment Self-service provisioning	C R	R C
RDS performance monitoring (CloudWatch) Self-service provisioning	C R	R C
RDS event subscription configuration (SNS) Self-service provisioning	C R	R C
RDS security group configuration Self-service provisioning	C R	R C
RDS engine parameter/option configuration	R	C
DB table design	R	I
DB indexing	R	I
DB log analysis	R	I
AMS Change Management		
Creating customer RFCs (e.g. access to resources creating/updating/deleting managed stacks, deploying/updating applications, changes to configuration of AWS Service Offerings)	R	I
Approving Customer RFCs	I	R
Creating AWS Managed Services RFCs (e.g. access to resources, creating resources on customer's behalf, applying updates to OS as part of Patch Management)	I	R
Approving non-automated RFCs	R	I
Submitting request for new Change Types	R	C
Creating new Change Types	I	R
Maintenance of application change calendar	R	C
Notice of upcoming Maintenance Window	I	R
AWS Service Catalogue		
Create portfolios and products	R	I
Distribute products to end users	R	I
Create tags and tag option library	R	C
Sharing portfolios and products with end users	R	I
Revise / update portfolios and products	R	I
Create and assign constraints to portfolios and products	R	C
Associate Service Actions to products	R	C
Update provisioned resources with new version of product	R	I
Provisioning		
Customer specific additions to AWS Managed Services baseline AMI	R	C
Configure additional approved Change Types used to provision Stack templates	C	R
Launch managed Stacks and associated AWS resources submitted through AMS change management process or AWS Service Catalogue *Self-service provisioning*	I R	R I
Install/Update custom and 3rd party applications on Instances provisioned through AMS change management process or AWS Service Catalogue	R	I
Provisioning - Stack Architecture		

Activity	Customer	AMS
Providing OS licenses (including usage fees for the applicable AWS services – e.g. EC2 and RDS) *Self-service provisioning*	I R	R I
Define baseline infrastructure templates (Stacks) for application deployment through AMS change management system *Self-service provisioning*	I R	R I
Creating baseline approved AMIs[8]	I	R
Evaluate customer application inventory and determine fit with available infrastructure templates (Stacks)	R	C
Define unique Stacks that are in addition to the baseline template offerings	R	C
Logging, Monitoring and Event Management		
Recording AWS infrastructure change logs	I	R
Recording all application change logs	R	C
Installation and configuration of agents and scripts for patching, security, monitoring, etc. of AWS infrastructure provisioned through the AMS change management process *Self-service provisioning*	I R	R C
Define customer specific monitoring and incident requirements	R	C
Configuring alerts for Managed Environment	I	R
Monitoring all AMS configured alerts *Self-service provisioning*	I R	R C
Investigating infrastructure Alerts for Incident notification *Self-service provisioning*	I R	R C
Investigating application alarms	R	C
Incident Management		
Proactively notify Incidents on AWS infrastructure based on monitoring *Self-service provisioning*	I R	R C
Handle application performance issues and outages	R	I
Categorize Incident priority	I	R
Provide Incident response	I	R
Provide Incident resolution / infrastructure restore Note: SLAs do not apply to instance-based resources provisioned outside AMS change management, including those provisioned using self-service provisioning and developer mode.	C	R
Problem Management		
Identify Problems in Managed Environment	C	R
Perform RCA for Problems in Managed Environment	C	R
Remediation of Problems in Managed Environment	C	R
Identify and remediate application problems	R	I
Security Management		
Customer infrastructure security and/or establishing baseline for security compliance process as determined and agreed to during customer onboarding *Self-service provisioning*	C R	R C
Maintaining valid licenses for Managed EPS	R	C
Configure Managed EPS *Self-service provisioning*	I R	R C
Update Managed EPS *Self-service provisioning*	I R	R C

Activity	Customer	AMS
Monitoring malware on instances provisioned through the AMS CM process *Self-service provisioning*	I R	R C
Maintaining and updating virus signatures *Self-service provisioning*	I R	R C
Remediating instances infected with malware *Self-service provisioning*	C R	R C
Security event management	C	R
Security - Access Management		
Manage the lifecycle of users, and their permissions for local directory services, which are used to access AWS Managed Services	R	I
Operate federated authentication system(s) for customer access to AWS console/APIs	R	C
Accept and maintain Active Directory (AD) trust from AWS Managed Services AD to customer managed AD	R	C
During onboarding, create cross-account IAM Admin roles within each managed account	R	C
Secure the AWS root credential for each account	I	R
Define IAM resources for Managed Environment	C	R
Manage privileged credentials for OS access for AMS engineers	I	R
Manage privileged credentials for OS access provided to customer by AMS	R	I
Patch Management		
Monitor for applicable updates to supported OS and software preinstalled with supported OS for EC2 instances *Self-service provisioning*	I R	R C
Notify customer of upcoming updates (*applies to AMS Standard Patch only*)	I	R
Exclude certain updates and/or certain Stacks from patching activities	R	I
Define default and custom maintenance windows schedules and other parameters (e.g. maintenance window duration) to apply patches (*applies to AMS Patch Orchestrator only*)	R	I
Define custom Patch Baselines to filter and exclude specific patches (*applies to AMS Patch Orchestrator only*)	R	I
Tag instances to associate them with custom maintenance windows and Patch Baselines (*applies to AMS Patch Orchestrator only*)	R	I
Track the patch status of resources and highlight systems that aren't current in the monthly business review	C	R
Apply updates to EC2 instances per Customer instructions *Self-service provisioning*	I R	R C
Patch development software (.NET, PHP, Perl, Python)	R	I
Patch, and monitor middleware applications (e.g. BizTalk, JBoss, WebSphere) *Self-service provisioning*	R C	I I
Patch, and monitor custom and 3rd party applications *Self-service provisioning*	R C	I I
Continuity Management		
Specify backup schedules	R	I
Execute backups per schedule *Self-service provisioning*	I R	R C
Validate backups	R	I

Activity	Customer	AMS
Request backup restoration activities	R	I
Execute backup restoration activities *Self-service provisioning*	I R	R C
Restore affected Stacks and VPCs *Self-service provisioning*	I R	R C
Restore affected custom/3rd party application	R	C
Reporting		
Prepare and deliver monthly service report *AMS on AWS Outposts*	I R	R I
Configure and retrieve API audit history on demand (CloudTrail) *Self-service provisioning*	I R	R I
Provide access to incident history through AWS Managed Services Interface	I	R
Provide access to change history through AWS Managed Services Interface *Self-service provisioning*	I N/A	R N/A
Service Request Management		
Request information using service requests	R	I
Reply to service requests	I	R
Managed Firewall		
Request the deployment of AMS-Managed Firewall	R	I
Design and optimization of AMS-Managed Firewall architecture	I	R
Deployment of AWS Infrastructure and AMS-Managed Firewall appliance	I	R
Providing Firewall licenses (including usage fees for the applicable AWS services – e.g. EC2)	R	I
Define default domain allow-list	I	R
Request to add, modify, and delete custom allow-lists and security policies	R	I
Configuring alerts for AMS-Managed Firewall	I	R
Monitoring all AMS-Managed Firewall configured alerts	I	R
Execute Backups of firewall configuration	I	R
Request backup restoration activities	R	I
Update provisioned resources with new version of product	I	R
Recording AMS-Managed Firewall logs	I	R
Forward logs from AMS-Managed Firewall to CloudWatch	I	R
Request configuration changes in the AMS-Managed Firewall	R	I
Approve configuration changes in the AMS-Managed Firewall	I	R
Execute configuration changes in the AMS-Managed Firewall	I	R

1.10. Onboarding and Service Commencement

The AMS Advanced Operations Plan Onboarding Guide can be found here: https://docs.aws.amazon.com/managedservices/latest/onboardingguide/og-intro.html

Service Commencement: The Service Commencement Date for an AWS Managed Services account is the first day of the first calendar month after which AWS notifies you that the activities set out in the Onboarding Requirements for that AWS Managed Services account have been completed; provided that if AWS makes such notification after the 20th day of a calendar month,

the Service Commencement Date is the first day of the second calendar month following the date of such notification.

R stands for responsible party that does the work to achieve the task.

I stands for informed; a party which is informed on progress, often only on completion of the task or deliverable.

Step #	Step Title	Description	Customer	AMS
1.	Customer AWS account handover	Customer creates a new AWS account and hands it over to AWS Managed Services	R	I
2.	AWS Managed Services Account - design	Finalize design of AWS Managed Services Account	I	R
3.	AWS Managed Services Account - build	An AWS Managed Services account is built per the design in Step 2	I	R

1.11. Service Level Agreement

The Service Level Agreement can be found here: https://s3.amazonaws.com/ams.contract.docs/AWSManagedServicesSLA.pdf and is also detailed below:

AWS Managed Services (AMS) is a standardized service for all our Enterprise customers and offers two Service Levels and associated agreements and credits.

AWS MANAGED SERVICES SERVICE LEVEL AGREEMENT

This AWS Managed Services Service Level Agreement ("SLA") is a policy governing the use of AWS Managed Services ("AMS"), including AMS Advanced and AMS Accelerate, and applies separately to each account using AWS Managed Services. In the event of a conflict between the terms of this SLA and the terms of the AWS Customer Agreement or other agreement with us governing your use of our Services (the "Agreement"), the terms and conditions of this SLA apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

Service Commitments

AWS will use commercially reasonable efforts to meet the following Service Commitments:

- **Incident Response Time** – Once an Incident is reported by you, AWS Managed Services will send an initial response to you concerning the Incident via the AMS console, e-mail, or telephone within the timeframes set out in the Service Commitment & Credit Table ("SCCT") below.
- **Incident Restoration/Resolution Time** – AWS Managed Services will Restore or Resolve Incidents reported by AWS Managed Services or you within the timeframes set out in the SCCT below.
- **AWS Console/API Availability** – AWS will make the AMS console and AMS APIs available as set out in the SCCT below.
- **Patch Management** – AWS Managed Services will attempt to apply or install new updates to EC2 instances and provision AWS Managed Services AMIs with new updates, as applicable, within your Managed Environment as set out in the SCCT below. This Service Commitment only applies to vendor updates for supported operating

systems and software pre-installed with supported operating systems. A list of supported operating systems for AMS Advanced and AMS Accelerate is available in the AWS Managed Services Documentation

- **Environment Recovery Initiation Time** – AWS will initiate a customer-authorized Environment Recovery, as needed, within the timeframes set out in the SCCT below.

In the event AWS Managed Services does not meet a Service Commitment in Conformance with the Service Commitment & Credit Table, you will be eligible to receive a Service Credit as described below.

Service Commitment & Credit Table (SCCT)

Service Commitment Category	Key Performance Indicator	Service Commitment[1]		Conformance	Service Credits***
		AMS Advanced			
		Plus Tier	Premium Tier		
Incident Management - Response Time*	1. Priority 1 Incident	<=4 hours	<=15 min	95%	3%
	2. Priority 2 Incident	<=8 hours	<=2 hours	95%	2%
	3. Priority 3 Incident	<=24 hours	<=8 hours	90%	1%
Incident Management – Restoration/Resolution Time*	4. Priority 1 Incident	<=12 hours Resolution	<=4 hours Resolution	95%	6%
	5. Priority 2 Incident	<=24 hours Resolution	<=8 hours Resolution	95%	4%
	6. Priority 3 Incident	<=48 hours Resolution	<=24 hours Resolution	90%	2%
AMS API and Console Availability**	7. API Availability Percentage	>=99.90%	>=99.90%	99%	0.5%
	8. Console Availability Percentage	>=99.90%	>=99.90%	99%	0.5%
Patch Management	9. Patch Compliance	>=90%	>=95%	95%	4%
	10. Patched baseline AMS AMIs	Within 10 business days of a critical security update being available.	Within 8 calendar days of a critical security update being available.	95%	3%
Continuity Management - Environment Recovery	11. Environment Recovery Initiation Time	<=12 hours	<=4 hours	99%	4%

* If five (5) or more Priority 1 Incidents, caused due to application issues, are reported on any individual Stack during any rolling 30 day period, any subsequent Incidents for the same Stack will be excluded for the purposes of calculating Service Credits until AWS Managed Services determines otherwise. AWS Managed Services will escalate the issue with you in your monthly service review meetings to determine what, if any, changes are needed before the Stacks are included in Service Credit Calculations.

** API Availability Percentage and Console Availability Percentage are each calculated by subtracting from 100%, the average Unavailability rate from each five minute period in the monthly billing cycle. The Unavailability rate is (i) the total number of Unavailable responses divided by (ii) the total number of requests for the applicable request type during the five-minute period.

*** The Service Credit is a percentage of the total monthly fee for either AMS Accelerate or AMS Advanced for the account that does not meet the Service Commitment, depending on which service the account is enrolled in.

[1] References to minutes or hours within the table refer to “Business Hours” as defined in the AWS Managed Services Documentation. The AWS Managed Services Maintenance Window is excluded from all Service Commitment time calculations.

Definitions

Capitalized terms are defined below:

- "**Unavailable**" and "**Unavailability**" mean:
    - For AWS Managed Services APIs, if an HTTP request submitted by you results in a 5xx HTTP response (where "x" represents any single digit number).
    - For AWS Managed Services console, if an HTTP request submitted by you results in a 5xx HTTP response (where "x" represents any single digit number).
    - For AWS resources, if any of the AWS Services that constitute the resource(s) are in a state of "Service Disruption" as indicated in http://status.aws.amazon.com/.
    - Services are considered available unless they meet the criteria for being Unavailable.
- The "**AWS Managed Services Maintenance Window**" is a time window selected by AWS to perform maintenance activities in an AWS Managed Services account. AWS Managed Services may announce a Maintenance Window by providing 48 hours' notice.
- "**Incident Resolution**" or "**Resolved**" Incident means that either (1) AWS Managed Services has restored all Unavailable services or resources pertaining to that Incident to an available state, or (2) AWS Managed Services determines that Unavailable resources cannot be restored to an available state and AWS Managed Services initiates a customer-authorized Incident Restore. If you do not authorize an Incident Restore as recommended by AWS when an Incident Restore will bring all the resources pertaining to that Incident to an available state, you will not be eligible for a Service Credit for the associated Incident Resolution Time Service Commitment.
- "**Incident Restore**" means initiating a data restore of impacted resources based on their last known restore point in AWS Backup. Ephemeral data that is not part of the backup will be lost. AWS Managed Services will use reasonable efforts to perform an Incident Restore while AWS Services are Unavailable. Incident Restore is available for resources supported by AWS Backup. Incident Restore will be completed once the impacted resource(s) are available.
- "**Incident Response Time**" means the difference in time between when you create an Incident, and when AWS Managed Services provides an initial response via console, e-mail, or telephone.
- "**Incident Resolution/Restoration Time**" means the difference in time between when either AWS Managed Services or you create an Incident, and when the Incident is Resolved. Time spent waiting for inputs or approvals from you is excluded from Incident Resolution/Restoration Time calculations. For Incidents that AWS Managed Services creates, the Incident creation time is the time of the initial customer notification.
- "**Incident Priority**" – Incidents will be categorized by AWS Managed Services or you as either Priority 1, 2, or 3.
    - "**Priority 1**" means that either (1) the AWS Managed Services Console, or one or more AWS Managed Services APIs within your Managed Environment are Unavailable; or (2) one or more AWS Managed Services Stacks or resources

within your Managed Environment are Unavailable and the Unavailability prevents your application from performing its normal function.

  - "**Priority 2**" means that an AWS service within your Managed Environment is available but is not performing as intended by AWS.
  - "**Priority 3**" includes any Incident that is not categorized as Priority 1 or Priority 2.
  - AWS Managed Services may re-categorize Incidents in accordance with the above guidelines

- **"Patch Compliance**" means the percentage of EC2 instances in an AWS Managed Services Account that have updates installed in accordance with their "patch baselines", as defined in the user guide. Patch Compliance is calculated at the time of each customer-selected patch maintenance window. The following will not be included in Patch Compliance calculations: (1) EC2 instances that do not use SSM based patching, (2) EC2 instances that are not patched because they are pending customer action for configuration changes, (3) EC2 instances that are not patched because the customer does not provide a patch maintenance window, or (4) EC2 instances that are not patched because the patch maintenance window provided by the customer is not at least two hours in duration plus an additional hour for every 50 instances that require patching.
- "**Patched baseline AMS AMIs**" are AMIs that are published by AWS Managed Services and patched with critical security updates for supported operating systems. Non-critical security vendor updates are not included in the Service Commitment.
- "**Environment Recovery**" – In case of Availability Zone (AZ) Unavailability in a Region used by your AWS Managed Services account, "Environment Recovery" is the process of restoring one or more AWS subnets in your Managed Environment by re-deploying existing stacks, based on templates of impacted stacks, and initiating a data restore based on a last known restore point, unless otherwise advised by the customer.
- "**Environment Recovery Initiation Time**" means the difference in time between when you request or authorize an Environment Recovery and the time AWS Managed Services initiates the Environment Recovery process. Time spent waiting for inputs or approvals from you is excluded from Environment Recovery Initiation Time calculations.
- "**Conformance**" is the percentage of times that AWS Managed Services must meet a Service Commitment in any monthly billing cycle. If AWS Managed Services does not meet the Conformance percentage for any Service Commitment, you will be eligible for a Service Credit.
  - For the purpose of determining Conformance for the Patch Management Service Commitment, each release of an update or multiple updates released simultaneously by an AWS Managed Services-supported operating system vendor will be considered as a single update.
- A "**Service Credit**" is a dollar credit, calculated as set forth below, that we may credit back to an eligible AWS Managed Services account.
- "**Business Hours**" refers to the hours in local customer time that AWS Managed Services will work on all customer requests. Business Hours for Plus and Premium SLA Tiers are defined in the AWS Managed Services Documentation.

Service Credits

Service Credits are calculated as a percentage of the total charges paid by you (excluding one-time payments such as upfront payments made for on boarding) for AWS Managed Services for the monthly billing cycle and AMS Account in which the Service Commitment was not met in accordance with the Service Commitment & Credit Table and as further specified below:

- The Service Credit percent indicated in the SCCT may only be recovered once per monthly billing cycle for each Service Commitment.
- Separately reported Incidents that have the same Incident Resolution will be combined into one Incident for the purposes of calculating Service Credits. If Incidents are combined, Service Credits will be due for the individual Incident that provides the highest Service Credits for the customer.

We will apply any Service Credits only against future AWS Managed Services payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Service Commitment was not met. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the Agreement, your sole and exclusive remedy for any Unavailability, non-performance, or other failure by us to provide AWS Managed Services is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA. Notwithstanding the above, Service Credits may not individually or cumulatively exceed 30% of the total charges paid by you for AWS Managed Services on any individual account for the billing cycle in which the Service Commitment(s) was not met.

Credit Request and Payment Process

To receive a Service Credit, you must submit a claim by opening a service request in the AWS Managed Services Console. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the Service Commitment was not met and must include:

1. the words “SLA Credit Request” in the subject line;
2. the dates and times of each time you are claiming that Service Commitment was not met; and
3. your request logs and other documents that corroborate your claim (any confidential or sensitive information in these logs and other documents should be removed or replaced with asterisks).

Once we review your Service Credit Request and confirm your eligibility, we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

SLA Exclusions

The Service Commitments do not apply to any Unavailability, suspension, or termination of AWS Managed Services, or any other AWS Managed Services performance issues: (i) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of AWS Managed Services; (ii) that result from any actions or inactions of you or any third party, including your decision to postpone or not to authorize AWS Managed Services to perform or implement a change, update, patch, or other action recommended by AWS Managed Services; (iii) that result from you not following

the guidelines and best practices described in the AWS Managed Services Documentation on the AWS Site; (iv) that result from your equipment, software, or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) arising from our suspension and termination of your right to use AWS Managed Services in accordance with the Agreement; (vi) that result from resources developed using non-AWS Managed Services approved AMIs; (vii) that result from the Unavailability or degraded performance of AWS Service Offerings; (viii) that result from unauthorized use of account credentials by you or any third party (collectively, the “AWS Managed Services SLA Exclusions”). SLAs are not applicable once off-boarding assistance commences following the termination of AWS Managed Services. If availability is impacted by factors other than those included herein, then we may issue a Service Credit considering such factors at our discretion.

1.12. Technical Requirements

Comprehensive technical documentation is available as part of the engagement and Public Documentation can be found here: https://docs.aws.amazon.com/managedservices/

1.13. Operations On Demand

Operations on Demand (OOD) is an AMS service feature that extends the standard scope of your AMS operations plan by providing operational services that are not currently offered natively by the AMS operations plans or AWS. Once selected, the catalogue offering is delivered by a combination of automation and highly skilled AMS resources. There are no long term commitments or additional contracts, allowing you to extend your existing AMS and AWS operations and capabilities as needed. Customers agree to purchase blocks of hours (20 hours per block) on a monthly or one-time basis. Billing is block-based; unused whole blocks will not be billed.

You can select from the catalogue of standardized offerings https://docs.aws.amazon.com/managedservices/latest/userguide/ood-catalog.html and initiate a new OOD engagement through a service request. Examples of OOD offerings include:

Title	Description	Expected Outcomes
Amazon EKS Cluster Maintenance	AMS frees your container developers by handling the ongoing maintenance and health of your Amazon Elastic Kubernetes Service (Amazon EKS) deployments. AMS performs the end-to-end procedures necessary to update a cluster addressing the components of control plane, add-ons, and nodes. AMS performs the updating to managed node types as well as a curated set of Amazon EKS and Kubernetes add-ons.	Assist customer teams with the underlying operations work of updating Amazon EKS clusters.
Legacy OS Upgrade	Avoid an instance migration by upgrading instances to a supported operating system version. We can perform an in-place upgrade on your selected instances leveraging automation and the upgrade capabilities of the software vendors (for example, Microsoft Windows 2008 R2 to Microsoft Windows 2012 R2). This approach is ideal for legacy applications that cannot be easily re-installed on a new instance and provides additional protection from known and unmitigated security threats on older OS versions.	Solution for applications that can no longer be re-installed on a new instance (for example, lost the source code, ISV out of business, and so forth). Failed upgrades can be rolled back to their original state. From an operational perspective, this is preferred as it puts the instance in a more supportable state with the latest security patches.

Title	Description	Expected Outcomes
Priority RFC Execution	Designated AMS operations engineer capacity to prioritize the execution of your requests for change (RFC). All submissions will receive a higher level of response and priority order can be adjusted by interacting directly with engineers through an Amazon Chime meeting room.	Customers receive a response SLO of 8 hours for RFCs

New catalogue offerings are added regularly based on demand and the operational use cases we see most often.

1.14. Off-boarding Assistance

Currently AMS supports 3 types of offboarding for multi-account landing zone accounts:

- Multi-Account Landing Zone environmental offboarding
- Application account offboarding
- Application account VPC offboarding.

Details can be found here:
https://docs.aws.amazon.com/managedservices/latest/onboardingguide/offboarding-malz.html

On the Service Termination Date, AWS will (i) hand over the controls of all AMS accounts or the specified AMS account, as applicable, to customer, or (ii) the parties will remove the AWS Identity and Access Management roles that give AWS access from all AMS Accelerate accounts or the specified AMS Accelerate account, as applicable.