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

May 2022

# G-Cloud 13 Amazon Web Services EMEA SARL, UK Branch (AWS) – AWS Managed Services (AMS) Accelerate 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 Accelerate Operations Plan. AMS Accelerate provides a range of operational services to help you achieve operational excellence on AWS. Whether you're just getting started in the cloud, looking to augment your current team, or need a long-term operational solution, AMS Accelerate can help you meet your operational goals in the cloud. Leveraging AWS services and a library of automations, configurations, and run books, we provide an end-to-end operational solution for both new and existing AWS environments.

The service leverages a suite of native AWS services and features to provide a comprehensive set of infrastructure management capabilities. Within these AWS services Accelerate creates and maintains curated sets of monitoring controls, detection guardrails, automations, and runbooks to operate infrastructure in a compliant and secure way. Whether your workloads are already in an AWS account or you're planning to migrate new ones, you can benefit from AMS Accelerate operational services such as monitoring and alerting, incident management, security management, and backup management, without going through a new migration, experiencing downtime, or changing how you use AWS. AMS Accelerate also offers an optional patch add-on for EC2 based workloads that require regular patching.

With AMS Accelerate you have the freedom to use, configure, and deploy all AWS services natively, or with your preferred tools. You can continue using your existing access and change mechanisms while AMS consistently applies proven practices that help scale your team, optimize costs, increase security and efficiency, and improve resiliency.

While AMS Accelerate can simplify your operations, you remain responsible for application development, deployment, test and tuning, and management. AMS Accelerate only makes changes in your account as a result of incidents, alarms, remediation, and some service requests. AMS Accelerate doesn't provision resources in the account on your behalf. AMS Accelerate provides troubleshooting assistance for infrastructure issues that impact applications, but AMS Accelerate doesn't access or validate your application configurations without your knowledge and approval. AMS Accelerate services and changes are provided

directly in the AWS console and APIs, so you continue to leverage your existing accounts with AWS and available AWS Marketplace solutions. AMS Accelerate doesn't modify code in your infrastructure-as-code templates (for example, AWS CloudFormation templates), but can guide your teams on which changes are required to follow best operational and security practices.

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 (AMS) builds and maintains a growing repository of compliance, operational, and security guardrails that help keep you aligned with your controls. AMS reduces the burden of meeting compliance program requirements (GDPR, SOC, NIST, ISO, PCI) through automated detection and remediation automations.
- **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.
- **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.

## 1.2. Service Description

The AMS features are:

- **Incident Management:** AMS Accelerate proactively detects and responds to incidents and assists your team in resolving issues. You can reach out to AMS Accelerate operations engineers 24x7 using AWS Support Center, with response time SLAs depending on the level of response you selected for your account.
- **Monitoring:** Accounts enrolled in AMS Accelerate are configured with a baseline deployment of CloudWatch events and alarms that have been optimized to reduce noise and to identify a possible upcoming incident. After receiving the alerts, the AMS team uses automated remediations, people, and processes, to bring the resources back to a healthy state and engage with your teams when appropriate to provide insights into learnings on the behavior and how to prevent it. If remediation fails, AMS starts the incident management process. You can change the baselines by updating the default configuration file.
- **Security Management:** In addition, AMS Accelerate leverages Amazon GuardDuty to identify potentially unauthorized or malicious activity in your AWS environment.

GuardDuty findings are monitored 24x7 by AMS. AMS collaborates with you to understand the impact of the findings and remediations based on best practice recommendations. AMS also supports Amazon Macie to protect your sensitive data such as personal health information (PHI), personally identifiable information (PII), and financial data.

- **Patch Management:** For an AWS account with the patch add-on, AWS Managed Services applies and installs vendor updates to EC2 instances for supported operating systems during your chosen maintenance windows. AMS creates a snapshot of the instance prior to patching, monitors the patch installation, and notifies you of the outcome. If the patch fails, AMS investigates the failure, tries to remediate it, or restores the instance as needed. AMS provides reports of patch compliance coverage and advises you of the recommended course of action for your business.
- **Backup Management:** AWS Managed Services creates, monitors, and stores snapshots for AWS services supported by AWS Backup. You define the backup schedules, frequency, and retention period by creating AWS Backup plans while onboarding accounts and applications. You associate the plans to resources. AMS tracks all backup jobs, and, when a backup job fails, alerts our team to run a remediation. AMS leverages your snapshots to perform restoration actions during incidents, if needed. AMS provides you with a backup coverage report and a backup status report.
- **Designated Experts:** AMS Accelerate also designates a Cloud Service Delivery Manager (CSDM) and a Cloud Architect (CA) to partner with your organization and drive operational and security excellence. Your CSDM and CA provide you guidance during and after configuration and onboarding AMS Accelerate, deliver a monthly report of your operational metrics, and work with you to identify potential cost savings using tools such as AWS Cost Explorer, Cost and Usage Reports, and Trusted Advisor.
- **Operations Tools:** AMS Accelerate can provide ongoing operations for your workload's infrastructure in AWS. Our patch, backup, monitoring, and incident management services depend on having resources tagged, and the AWS Systems Manager (SSM) and CloudWatch agents installed and configured on your EC2 instances with an IAM instance profile that authorizes them to interact with the SSM and CloudWatch services. AMS Accelerate provides tools like Resource Tagger to help you tag your resources based on rules, and automated instance configuration to install the required agents in your EC2 instances. If you're following immutable infrastructure practices, you can complete the prerequisites directly in the console or infrastructure-as-code templates.

  All AMS Accelerate customers start with incident management, monitoring, security monitoring, log recording, prerequisite tools, backup management, and reporting capabilities. You can add AMS Patch add-on at an additional price.
- **Logging and Reporting:** AWS Managed Services aggregates and stores logs generated as a result of operations in CloudWatch, CloudTrail, and VPC Flow Logs. Logging from AMS helps in faster incident resolution and system audits. AMS Accelerate also 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) designated to you.

- **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/.

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 Accelerate Operations Plan User Guide can be found here:
https://docs.aws.amazon.com/managedservices/latest/accelerate-guide/what-is-acc.html

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

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

Selected Key Service Terms are detailed below:

*AMS Accelerate Accounts:* AWS accounts that at all times meet all requirements in the AMS Accelerate 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 Accelerate: Supported Configurations or AMS Accelerate; 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 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 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 Accelerate | |
|---|---|---|
| | **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 |
| 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

## 1.7. Supported Configuration

These are the configurations AMS supports:

- **Language:** AMS is available in English.
- **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)
- **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 Accelerate 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. If you request that AWS Managed Services provide services for any software or service that is not expressly identified as supported in the following list, any AWS Managed Services provided for such customer-requested configurations will be treated as a "Beta Service" under the Service Terms.

- **Incidents:** All AWS services
- **Service Request:** All AWS services
- **Patching:** EC2
- **Backups and Restoration:** Amazon EC2, Relational Database Service (Amazon RDS), EBS, Storage Gateway, Dynamo DB, Aurora, EFS

- **Services monitored by CloudWatch alarms:** Amazon EC2, Relational Database Service (Amazon RDS), Aurora, RedShift, ElasticSearch, NAT gateway (a Network Address Translation (NAT) service), Site-to-Site VPN, Elastic Load Balancer, Application Load Balancer, Personal Health Dashboard. To learn more about what AMS Accelerate is monitoring as part of a service, see Alerts from baseline monitoring in AMS
- **Services monitored by security Config Rules:** AWS Account, GuardDuty, Macie, API Gateway, Certificate Manager (ACM), Config, CloudTrail, CloudWatch, CodeBuild, Database Migration Service, DynamoDB, Amazon EC2, Elastic Block Store (Amazon EBS), Elastic File System (Amazon EFS), Elastic Load Balancing, ElastiCache, ElasticSearch, Amazon EMR, Identity and Access Management (IAM), Key Management Service, (KMS), Lambda, Redshift, Relational Database Service (Amazon RDS), Amazon S3, SageMaker, Secrets Manager, Simple Notification Service (Amazon SNS), Systems Manager Agent (SSM), VPC (Security group, Volume, Elastic IP, VPN connection, Internet gateways), VPC Flow Logs. For more details, see Compliance and conformance and Data protection. You can find additional AMS security information in our private Security Guide that can be accessed through AWS Artifact, on the Reports tab, for Managed Services.

## 1.9. Scope of Changes Performed by AMS Accelerate

AMS Accelerate only makes changes for the specific purposes and situations described below. AMS makes changes only at the infrastructure level, using the console or APIs. AMS never changes your application, control, or domain layers. You can see any changes made by AMS (or other users) using our set of pre-built queries.

AWS Resources:

AMS Accelerate deploys or updates AWS resources only in the following situations:

- to deploy and update tools and resources required by AMS;
- as part of AMS monitoring, in response to events and alarms;
- to remediate security issues found in Config Reports, to make noncompliant resources conform to security best practices;
- during remediation and restoration as part of an incident response;
- when responding to customer requests to configure AMS features, such as:
    - alarm manager
    - resource tagger
    - patch baselines and maintenance windows
    - backup plans

AMS Accelerate does not deploy or update resources outside of these situations. If you need help from AMS to execute changes in other situations, consider using Operations on Demand.

Operating system software:

AMS Accelerate can make changes to your operating system software during unavailability situations via incident resolution as defined in our Service Level Agreement. AMS can also make changes to your operating systems as part of Automated instance configuration in AMS Accelerate.

Application code and configuration:

AMS Accelerate never modifies your code (for example, AWS CloudFormation templates, other infrastructure-as-code templates, or Lambda functions), but can guide your teams on which changes are required to follow best operational and security practices. AMS Accelerate provides troubleshooting assistance for infrastructure issues that impact applications, but AMS Accelerate doesn't access or validate your application configurations.

## 1.10. Roles and Responsibilities

AMS Accelerate manages your AWS infrastructure. The following table provides an overview of the roles and responsibilities for you and AMS Accelerate for activities in the lifecycle of an application running within the managed environment.

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.

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 | I |
| Application deployment | R | I |
| AWS resource deployment | R | I |
| Application monitoring | R | I |
| Application testing/optimization | R | I |
| Troubleshoot and resolve application issues | R | I |
| Troubleshoot and resolve problems | R | I |
| AWS infrastructure monitoring | C | R |
| Incident response for AWS network issues | C | R |
| Incident response for AWS resource issues | C | R |
| **Managed Account onboarding** | | |
| Grant access to the AWS Managed Account for the AMS team and tools | R | C |
| Implement changes in the account or environment to allow the deployment of tools in the account. For example, changes in Service Control Policies (SCPs) | R | C |
| Install SSM agents in EC2 instances | R | C |
| Install and configure tooling required to provide AMS services. For example, CloudWatch agents, scripts for patching, alarms, logs, and others | I | R |
| Manage access and identity lifecycle for AMS engineers | I | R |
| Collect all required inputs to configure AMS services. For example, patch maintenance windows duration, schedule and targets | R | I |
| Request the configuration of AMS services and provide all required inputs | R | I |
| Configure AMS services as requested by the customer. For example, patch maintenance windows, resource tagger, and alarm manager | C | R |

| Activity | Customer | AMS |
|---|---|---|
| Manage the lifecycle of users and their permissions, for local directory services, used to access AWS accounts and instances | R | I |
| Recommend reserved instances optimization | I | R |
| **Patch management** | | |
| Collect all required inputs to configure patch maintenance windows, patch baselines, and target | R | I |
| Request the configuration of patch maintenance windows and baselines, and provide all required inputs | R | I |
| Configure patch maintenance windows, patch baselines, and targets as requested by the customer | C | R |
| Monitor for applicable updates to supported OS and software preinstalled with supported OS for EC2 instances | I | R |
| Report for missing updates to supported OS and maintenance window coverage | I | R |
| Take snapshots of instances before applying updates | I | R |
| Apply updates to EC2 instances per customer configuration | I | R |
| Investigate failed updates to EC2 instances | C | R |
| Update AMIs and stacks for Auto-Scaling groups (ASGs) | R | C |
| Patch development software (.NET, PHP, Perl, Python) | R | I |
| Patch and monitor middleware applications (for example, BizTalk, JBoss, WebSphere). | R | I |
| Patch and monitor custom and third-party applications | R | I |
| **Backup** | | |
| Collect all required inputs to configure backup plans and target resources | R | I |
| Request the configuration of Backup plans and provide all required inputs | R | I |
| Configure backup plans and targets as requested by the customer | C | R |
| Specify backup schedules and target resources | R | I |
| Perform backups per plan | I | R |
| Investigate failed backup jobs | I | R |
| Report for backup jobs status and backup coverage | I | R |
| Validate backups | R | I |
| Request backup restoration for resources supported AWS services resources as part of incident management | R | I |
| Perform backup restoration activities for resources of supported AWS services | I | R |
| Restore affected custom or third-party applications | R | I |
| **Networking** | | |
| Provisioning and configuration of Managed Account VPCs, IGWs, DirectConnect, and other AWS networking Services | R | I |
| Configure and operate AWS Security Groups/NAT/NACL inside the Managed account | R | I |
| Networking configuration and implementation within customer network (for example DirectConnect) | R | I |
| Networking configuration and implementation within AWS network | R | I |
| Monitor defined by AMS for network security, including security groups | I | R |
| Network-level logging configuration and management (VPC flow logs, ELB access log, and others) | I | R |
| **Logging** | | |
| Record all application change logs | R | I |

| Activity | Customer | AMS |
|---|---|---|
| Record AWS infrastructure change logs | I | R |
| Enable and aggregate AWS audit trail | I | R |
| Aggregate logs from AWS resources | I | R |
| **Monitoring and Remediation** | | |
| Collect all required inputs to configure alarm manager, resource tagger, and alarm thresholds | R | I |
| Request the configuration of alarm manager and provide all required inputs | R | I |
| Configure alarm manager, resource tagger, and alarm thresholds as requested by the customer. | C | R |
| Deploy AMS CloudWatch baseline metrics and alarms per customer configuration | I | R |
| Monitor supported AWS resources using baseline CloudWatch metrics and alarms | I | R |
| Investigate alerts from AWS resources | C | R |
| Remediate alerts based on defined configuration, or create an incident | I | R |
| Define, monitor, and investigate customer-specific monitors | R | I |
| Investigate alerts from application monitoring | R | C |
| **Security Architecture** | | |
| Review AMS resources and code for security issues and potential threats | I | R |
| Implement security controls in AMS resources and code to mitigate security risks | I | R |
| Enable supported AWS services for security management of the account and its AWS resources | I | R |
| Manage privileged credentials for account and OS access for AMS engineers | I | R |
| **Security Risk Management** | | |
| Monitor supported AWS services for security management, like GuardDuty and Macie | I | R |
| Define and create AMS-defined Config Rules to detect if AWS resources comply with Center for Internet Security (CIS) and NIST security best practices. | I | R |
| Monitor AMS-defined Config Rules | I | R |
| Report conformance status of Config Rules | I | R |
| Define a list of required Config Rules and remediate them | I | R |
| Evaluate the impact of remediating AMS-defined Config Rules | R | I |
| Request remediation of AMS-defined Config Rules in the AWS account | R | I |
| Track resources exempted from AMS-defined Config Rules | R | I |
| Remediate supported AMS-defined Config Rules in the AWS account | C | R |
| Remediate non-supported AMS-defined Config Rules in the AWS account | R | I |
| Define, monitor, and investigate customer-specific Config Rules | R | I |
| **Security monitoring and response** | | |
| Configure supported security management AWS services for alerting, alerts correlation, noise reduction, and additional rules | I | R |
| Monitor supported AWS services for security alerts | I | R |
| Install, update, and maintain endpoint security tools | R | I |
| Monitor for malware on instances using endpoint security | R | I |
| **Incident Management** | | |

| Activity | Customer | AMS |
|---|---|---|
| Notify about incidents detected by AMS in AWS resources | I | R |
| Notify about incidents in AWS resources | R | I |
| Notify about incidents for AWS resources based on monitoring | I | R |
| Handle application performance issues and outages | R | I |
| Categorize incident priority | I | R |
| Provide incident response | I | R |
| Provide incident resolution or infrastructure restore for resources with available backups | C | R |
| **Problem Management** | | |
| Correlate incidents to identify problems | I | R |
| Perform root cause analysis (RCA) for problems | I | R |
| Remediate problems | I | R |
| Identify and remediate application problems | R | I |
| **Service Management** | | |
| Request information using service requests | R | I |
| Reply to service requests | I | R |
| Provide cost-optimization recommendations | I | R |
| Prepare and deliver monthly service report | I | R |
| **Change Management** | | |
| Change management processes and tooling for provisioning and updating resources in the managed environment | R | I |
| Maintenance of application change calendar | R | I |
| Notice of upcoming maintenance Window | R | I |
| Record changes made by AMS Operations | I | R |

## 1.11. Onboarding and Service Commencement

The AMS Accelerate Onboarding approach can be found here: https://docs.aws.amazon.com/managedservices/latest/accelerate-guide/acc-get-mgmt-resource-onboard.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.

## 1.12. 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 Accelerate | | | |
| | | Plus Tier | Premium Tier | | |
| Incident Management - Response Time* | 1. Priority 1 Incident | <=4 hours | <=15 min | 95% | 3% |
| | 2. Priority 2 Incident | <=8 hours | <=4 hours | 95% | 2% |
| | 3. Priority 3 Incident | <=24 hours | <=12 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 | N/A | N/A | 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 | N/A | N/A | 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.

## 1.13. 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/

## 1.14. 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 and Health Checks | 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.<br>AMS also provides a set of Amazon EKS cluster health checks that leverage automation and operation engineers to detect, alert, and remediate issues that can impact cluster and workloads. | Assist customer teams with the underlying operations work of updating Amazon EKS clusters and monitoring foundational cluster health. |
| AWS Control Tower Operations | Ongoing operations and management of your AWS Control Tower landing zone, including AWS Transit Gateway and AWS Organizations - providing a comprehensive landing zone solution. We handle account vending, SCP and OU management, drift remediation, SSO user management, and AWS Control Tower upgrades with our library of custom controls and guardrails. | Assist customer teams with some of the underlying operations work of managing AWS Control Tower, AWS Transit Gateway, and AWS Organizations. |

| Title | Description | Expected Outcomes |
|---|---|---|
| SAP Cluster Assist | Dedicated alarming, monitoring, cluster patching, backup, and incident remediation for your SAP clusters. This catalog item allows you to offload some of the ongoing operational work from your SAP operations team so that they can focus on capacity management and performance tuning. | Assist customer or partner SAP teams with some of the underlying operations work. Still requires the customer to provide other SAP capabilities such as capacity management, performance tuning, DBA, and SAP basis administration. |
| 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. |
| Curated Change Execution | Work with our skilled operations engineers to translate your business requirements into validated change requests that can be executed safely within your AWS environment. Take advantage of our unique approach to automation and knowledge of operational best practices (e.g. impact assessment, roll backs, two-person rule), whether it is a simple change at scale or a complex action with downstream impacts. | Work with customers to define, create, and execute custom change requests. Changes can be manual or automated (CFN, SSM). Includes consultation with AWS Support for configuration guidance when necessary. Not intended for changes to application code, application installation/deployment, data migration, or OS configuration changes. |

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

## 1.15. Off-boarding Assistance

AMS will support off-boarding either account by account or in totality.

On the Service Termination Date, 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.