G-Cloud 15 Amazon Web Services EMEA SARL, UK Branch (AWS)

AWS Managed Services (AMS)

Service Definition Document

Lot 3 Cloud Support Services

30 January 2026

G-Cloud 15 Amazon Web Services EMEA SARL, UK Branch (AWS)

AWS Managed Services (AMS)

Service Definition Document

Lot 3 Cloud Support Services

This document is provided for informational purposes only. This document contains Amazon Confidential Information and is subject to the terms of the parties' agreement governing confidentiality, which include the terms governing Confidential Information in the AWS Customer Agreement (aws.amazon.com/agreement) or other agreement between you and AWS ("Service Agreement") governing Confidential Information. Where the parties have not entered into a Service Agreement, the terms of the AWS Customer Agreement control the Confidential Information provided in this document. Unless required by law, you agree not to disclose the contents of this document. Where you are required to disclose document contents by law, you will provide AWS with written notice and an opportunity to seek redactions or otherwise prevent disclosure of the information to the maximum extent permitted by law. The offerings described in this document represent AWS's current products and practices as of the date of issue of this document and are subject to change. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers. For current prices for AWS services, please refer to the AWS website at www.aws.amazon.com.

Please treat this information as private and confidential.

Table of Contents

1 Introduction 1
2 Service Description 1
2.1 AMS Accelerate Features 2
1.1 Supported Configurations 5
1.2 Supported Services 6
1.3 Roles and Responsibilities 7
2.2 Scope of Changes Performed by AMS Accelerate 15
1.4 Service Definitions 16
1.5 Pricing Overview 16
1.6 Governance 16
1.7 Contact and Escalation 16
1.8 Onboarding 17
1.9 SLAs 17
1.10 Technical Requirements 17
1.11 Operations on Demand 17
1.12 Off-Boarding Assistance 22

List of Tables

Table 1. AMS Accelerate Supported Configurations 5
Table 2. AMS Supported Services 6
Table 3. AMS Accelerate RACI Matrix 7
Table 4. AMS Accelerate Contact and Escelation Times 16
Table 5. OOD Services 18

Confidential
Confidential
Confidential

1 Introduction

This Amazon Web Services EMEA SARL, UK Branch ("Supplier") Service Definition Document provides service definition information for the AWS Support offering included in the G-Cloud 15 framework catalogue, in accordance with the requirements identified in the ITT.

2 Service Description

AMS

AMS helps Customers adopt the Supplier's cloud at scale and operate more efficiently and securely. AMS uses standard Supplier services and offers guidance and execution of operational proven practices with specialised automations, skills, and experience that are contextual to the Customer's environment and applications.

AMS offers proactive, preventative, and detective capabilities that raise the operational bar and help reduce risk without constraining agility, allowing Customers to focus on innovation. AMS extends a Customer's team with operational capabilities including monitoring, incident management, security, patch, backup, and cost optimisation.

AMS Accelerate

AMS offers the AMS Accelerate, an operations plan that helps Customers operate the day-to-day infrastructure management of their new or existing Supplier's environment. AMS Accelerate provides operational services, such as monitoring, incident management, and security. AMS Accelerate also offers an optional patch add-on for Amazon Elastic Compute Cloud (Amazon EC2)-based workloads that require regular patching.

Using the Supplier's services and a library of automations, configurations, and run books, Customers have an end-to-end operational solution for both new and existing Supplier environments. With AMS Accelerate, Customers decide which Supplier accounts they want AMS Accelerate to operate, the AWS Regions they want AMS Accelerate to operate in, the add-ons they require, and the service level agreements (SLAs) they need.

AMS provides a complete set of infrastructure management capabilities through its core Supplier services and features. Within these services, AMS Accelerate creates and maintains curated sets of monitoring controls, detection guardrails, automations, and runbooks to operate infrastructure in a compliant and secure way. Whether Customer workloads are already in a Supplier's account or are to be migrated to migrate new ones, Customers 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 the Customer uses the Supplier's environment.

With AMS Accelerate, Customers have the freedom to use, configure, and deploy all Supplier services natively, or with preferred tools. Customers can continue using their existing access and change mechanisms while AMS consistently applies proven practices that help scale teams, optimise costs, increase security and efficiency, and improve resiliency.

While AMS Accelerate can simplify operations, Customers remain responsible for application development, deployment, test and tuning, and management. AMS Accelerate only makes changes in accounts because of incidents, alarms, remediation, and some service requests. AMS Accelerate does not provide resources in the account on the Customer's behalf.

AMS Accelerate provides troubleshooting assistance for infrastructure issues that affect applications, but AMS Accelerate does not access or validate Customers application

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

configurations without Customer knowledge and approval. AMS Accelerate services and changes are provided directly in the Supplier console and APIs, so Customers continue to use their existing Supplier accounts and available AWS Marketplace solutions. AMS Accelerate does not modify code in Customer infrastructure-as-code (IaC) templates (for example, AWS CloudFormation templates) but can guide teams on the changes required to follow best operational and security practices.

Key benefits include:

Operational Flexibility. AMS provides Customers with flexibility in selecting the right level of operations assistance, whether new to the cloud or just need extra help with monitoring, incidents, or patch management. AMS uses a suite of native Supplier services and features to manage Customer infrastructure.

Enhanced Security and Compliance. AMS builds and maintains a growing repository of compliance, operational, and security guardrails that help keep Customers aligned with their controls. AMS can help reduce the burden of meeting compliance programme requirements, such as the National Institute of Standards and Technology (NIST) Center for Internet Security (CIS), Detective Controls Resource Confirmity Exeption, through automated detection and remediation automations.

Cost Optimisation. AMS helps with financial and capacity optimisation across the Customer's Supplier estate, and any savings identified reduces the AMS fee without impacting operational outcomes or security. AMS Customers have enjoyed up to 30% in operational savings and up to 25% in Supplier 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 is used and take back operational control when ready.

Remove Innovation Barriers. Enterprise DevOps is the convergence of modern development proven practices (i.e., DevOps) and existing IT process frameworks (i.e., ITIL ®) to give Customers speed and agility while maintaining governance, security, and compliance control. AMS transforms Enterprise DevOps by packaging Supplier IaaS services into a secure, compliant development platform that supports most enterprise workloads—including legacy systems and applications your teams already depend on. AMS-powered Enterprise DevOps helps development teams focus on their applications and innovate faster.

AMS requires Customers to have AWS Enterprise Support or AWS Unified Operations, extending the capabilities of a Technical Account Manager and aligning SLAs with the high bar Customers expect across these services

2.1 AMS Accelerate Features

AMS Accelerate offers the following features:

Incident Management

Incident management is the process the AMS service uses to respond to Customer reported incidents. AMS Accelerate proactively detects and responds to incidents and assists Customer teams in resolving issues. Customers can reach out to AMS Accelerate operations engineers 24/7 using AWS Support Center, with response time SLAs depending on the level of response selected for the account.

Monitoring

Monitoring is the process the AMS service uses to track Customer resources. Accounts enrolled in AMS Accelerate are configured with a baseline deployment of Amazon CloudWatch events and alarms optimised to reduce noise and to identify a possible

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

upcoming incident. After receiving the alerts, the AMS team automates remediation, deploys people and processes to restore resources to a healthy state, and engages with Customer teams when appropriate to share insights into what happened and how to prevent it. If remediation fails, AMS starts the incident management process. To change baselines, Customers can update the default configuration file.

Security

Security management is the process the AMS service uses to protect Customer resources. AMS protects information assets and helps keep Supplier infrastructure secure by using multiple controls, including AWS Config Rules and Amazon GuardDuty.

AMS Accelerate maintains a library of AWS Config Rules and remediation actions to help ensure that all Customer accounts comply with industry standards for security and operational integrity. AWS Config Rules continuously tracks the configuration change among Customer recorded resources. If a change violates any rule conditions, AMS reports its findings and allows Customers to remediate violations automatically or by request, according to the severity of the violation. AWS Config Rules facilitate compliance with standards set by the CIS, the NIST Cloud Security Framework, the Health Insurance Portability and Account ability Act, and the Payment Card Industry Data Security Standard.

AMS Accelerate uses Amazon GuardDuty to identify potentially unauthorised or malicious activity in the Customer's Supplier environment. GuardDuty findings are monitored 24/7 by AMS. AMS collaborates with Customers to understand the effect of the findings and remediations based on proven practice recommendations. AMS also supports Amazon Macie to protect sensitive data such as personal health information, personally identifiable information, and financial data.

Finally, AMS monitors and triages all Amazon Route 53 Resolver ALERT and BLOCK events generated in managed accounts to further inspect network traffic and augment its detective capabilities.

Patch Management

Patch management is the process the AMS service uses to update Customer resources. For a Supplier account with the patch add-on, AMS applies and installs vendor updates to Amazon EC2 instances for supported operating systems during Customer chosen maintenance windows. AMS creates a snapshot of the instance prior to patching, monitors the patch installation, and notifies the Customer of the outcome. If the patch fails, then AMS investigates the failure and recommends a course of action for the Customer to remediate the issue, or AMS restores the instance to roll back, if requested. AMS provides reports of patch compliance coverage and advises the Customer of the recommended course of action for their business.

Backup Management

AMS uses backup management to take snapshots of Customer resources. AMS creates, monitors, and stores snapshots for Supplier services supported by AWS Backup. Customers define the backup schedules, frequency, and retention period by creating AWS Backup plans while onboarding accounts and applications. Customers associate the plans with resources. AMS tracks all backup jobs, and, when a backup job fails, alerts the Supplier teams to run a remediation. AMS employs customer snapshots to conduct restoration actions during incidents, if required. AMS provides Customers with a backup coverage report and a backup status report.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

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 issues. 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.

Designated Experts

AMS Accelerate designates a Cloud Service Delivery Manager (CSDM) and a Cloud Architect (CA) to partner with the Customer and drive operational and security excellence.

Customer CSDM and CA provide guidance during and after configuration and onboarding AMS Accelerate, deliver a monthly report of the Customer's operational metrics, and work with the Customer to identify potential cost savings using tools such as AWS Cost Explorer, AWS Cost and Usage Reports, and AWS Trusted Advisor.

Operations Tools

AMS Accelerate offers ongoing operations for Customer workload's infrastructure in the Supplier environment. Supplier 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 Customer Amazon EC2 instances with an AWS Identity and Access Management (IAM) instance profile that authorises them to interact with the SSM and Amazon CloudWatch services. AMS Accelerate provides tools like resource tagger to help tag resources based on rules, and automated instance configuration to install the required agents in the Customer's Amazon EC2 instances. If the Customer is following immutable infrastructure practices, they can complete the prerequisites directly in the console or IaC templates.

Cost Optimisation

AMS Resource Scheduler automates the starting and stopping of Amazon EC2 instances, Amazon Relational Database Service (Amazon RDS) instances and Amazon EC2 Auto Scaling groups. AMS Resource Scheduler reduces operational costs for customers by stopping unused resources and starting them when needed.

Logging and Reporting

AMS aggregates and stores logs generated because of operations in Amazon CloudWatch, AWS CloudTrail, and Amazon Virtual Private Cloud (VPC) Flow Logs. Logging from AMS helps with faster incident resolution and system audits. AMS Accelerate also provides Customers with a monthly service report that summarises key performance metrics of AMS, including an executive summary and insights, operational metrics, managed resources, AMS SLA adherence, and financial metrics around spending, savings, and cost optimisation. Reports are delivered by the AMS CSDM designated to the Customer.

Service Request Management

Customers can request information about their managed environment, AMS, or Supplier service offerings by submitted service requests using the AMS Accelerate console. Customers can submit a service request for "How to" questions about Supplier services and features or to request additional AMS services.

All AMS Accelerate Customers start with incident management, monitoring, security monitoring, log recording, prerequisite tools, backup management, and reporting capabilities. Customers can add the AMS Patch management add-on at an additional price.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

1.1 Supported Configurations

AMS Accelerate supports the following configurations:

Table 1. AMS Accelerate Supported Configurations

Language	English.
Regions	See the AWS Regions supported by AWS in the AWS Regional Services webpage. AWS Regions introduced before March 20, 2019 are considered "Original" Regions and are enabled by default. Regions introduced after this date are "Opt-in" Regions and are disabled by default. If the Customer account uses multiple Regions and onboard AMS Accelerate to an account with an enabled "Opt-in" Region as the default Region, the AMS Reporting feature is only available in that Region. If Customer does not set a default Region, the last Region visited is the default Region. To activate a Region, see Enabling a Region. To set a default Region, see Choosing a Region. For a list of the Opt-in status for each Region, see Available Regions in the *Amazon Elastic Compute Cloud User Guide*.
Operating system architecture (x86-64 or ARM64)	Any supported by both Systems Manager and CloudWatch.
Supported operating systems	AlmaLinux 8.3-8.9, 9.x (AlmaLinux is only supported with x86 architecture) • Amazon Linux 2023 • Amazon Linux 2 (expected AMS support end date June 30, 2026) • Oracle Linux 9.x, 8.x • Red Hat Enterprise Linux (RHEL) 9.x, 8.x • SUSE Linux Enterprise Server 15 SP6 • SUSE Linux Enterprise Server for SAP 15 SP3 and later • Microsoft Windows Server 2022, 2019, 2016 • Ubuntu 20.04, 22.04, 24.04 Ubuntu Linux 18.04 • SUSE Linux Enterprise Server 15 SP3, SP4, and SP5 • SUSE Linux Enterprise Server for SAP 15 SP2 • SUSE Linux Enterprise Server 12 SP5 • SUSE Linux Enterprise Service for SAP 12 SP5 • Microsoft Windows Server 2012/2012 R2 • Red Hat Enterprise Linux (RHEL):7.x • Oracle Linux 7.5-7.9
Supported End of Support (EOS) operating systems	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 • Customer has extended support with the operating system vendor that allows them to receive updates, or • Any instances using an EOS OS follow the security controls as specified by AMS in the Accelerate User Guide, or • Customer complies with any other compensating security controls required by AMS. In the event AMS is no longer able to support an EOS OS, AMS issues and Critical Recommendation to upgrade the operating system.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

	AMS-required agents may include but are not limited to: AWS Systems Manager, Amazon CloudWatch, Endpoint Security (EPS) agent, and Active Directory Bridge (Linux only).
AWS Control Tower	If Customer uses AWS Control Tower to manage their multi-account environment, then they must run the latest version of AWS Control Tower for compatibility with Accelerate. Environments that use AWS Control Tower versions earlier than 2.7 (released in April 2021), are not supported. For information on how to update AWS Control Tower, see Update Your Landing Zone.

1.2 Supported Services

AMS provides operational management support services for the following Supplier services. Each Suppler service is distinct and as a result, AMS's level of operational management support varies depending on the nature and characteristics of the underlying Supplier service. If the Customer requests that AMS provides services for any software or service that is not expressly identified as supported in the following list, any AMS provided for such Customer-requested configurations will be treated as a "Beta Service" under the Service Terms.

Table 2. AMS Supported Services

Incidents	All Supplier services
Service Request	All Supplier services
Patching	Amazon EC2
Backups And Restoration	All Supplier services are supported by AWS Backup. For a list of services supported by AWS Backup, see AWS Backup supported resources. Resource Scheduler: Amazon EC2 instances, Amazon RDS and Amazon EC2 AutoScaling groups (ASGs)
Resource Scheduler	Amazon EC2 instances, Amazon RDS, and Amazon EC2 AutoScaling groups (ASGs)
Services Monitored for Operational Events	Supported checks and Trusted Advisor, Application Load Balancer, Aurora, Amazon EC2, ELB, Amazon FSx for NetApp ONTAP, Amazon FSx for Windows File Server, NAT gateway (a Network Address Translation (NAT) service), OpenSearch, AWS Health Dashboard, Amazon Redshift, Amazon RDS Site-to-Site VPN. 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:	Supplier account, AWS GuardDuty, Amazon Macie, Amazon API Gateway, AWS Certificate Manager, AWS Config, CloudTrail, CloudWatch, AWS CodeBuild, AWS Database Migration Service, Amazon DynamoDB, Amazon EC2, Amazon ElastiCache, Amazon Elastic Block Store (Amazon EBS), Amazon Elastic File System (Amazon EFS), Amazon Elastic Kubernetes Service (Amazon EKS), Elastic Load Balancing, Amazon OpenSearch Service, Amazon EMR, AWS IAM, AWS Key Management Service, AWS Lambda, Amazon Redshift, Amazon Relational Database Service, Amazon Simple Storage Service (Amazon S3), Amazon SageMaker, AWS Secrets Manager, Amazon Simple Notification Service, AWS Systems Manager, Amazon VPC (Security group, volume, Elastic IP address, VPN connection, internet gateways), Amazon VPC Flow Logs. For more details, see Configuration compliance in Accelerate and Data protection in AMS Accelerate. Customers can find additional AMS security information in our private Security Guide that can be accessed through AWS Artefact, on the Reports tab, for AMS

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

1.3 Roles and Responsibilities

The AMS Accelerate responsible, accountable, consulted, and informed, or Responsible, Accountable, Consulted, and Informed (RACI), matrix assigns primary responsibility either to the Customer or AMS for a variety of activities. The table describes the Customer responsibilities versus AMS Accelerate (the Supplier's) responsibilities.

The AMS Accelerate section in the AMS Accelerate User Guide lists the specific circumstances when AMS can make changes to Customer accounts; and specifies the types of changes AMS never makes.

AMS Accelerate RACI Matrix

AMS Accelerate manages the Customer's Supplier infrastructure. The following table provides an overview of the roles and responsibilities for Customers and AMS Accelerate for activities in the lifecycle of an application running within the managed environment.

- **Responsible**: a party that does the work to achieve the task.
- **Consulted**: A party whose opinions are sought, typically as subject matter experts; and with whom there is bilateral communication.
- **Informed**: A party who is informed on progress, often only on completion of the task.

Some sections contain 'R' for both AMS and Customers. This is because, in the Supplier's Shared Responsibility model, both AMS and the Customer takes joint ownership to respond to infrastructure and application issues.

Table 3. AMS Accelerate RACI Matrix

Activity	Customer	AMS
AMS Patterns		
Create new patterns	I	R
Deploy and customise patterns	R	C, I
Test and remove patterns	R	I
Application Lifecycle		
Application development	R	I
Application infrastructure requirements, analysis, and design	R	I
Application deployment	R	I
Supplier resource deployment	R	I
Application monitoring	R	I
Application testing/optimisation	R	I
Troubleshoot and resolve application issues	R	I
Troubleshoot and resolve problems	R	I
Monitoring supported for Supplier infrastructure	C	R
Incident response for Supplier network issues	C	R
Incident response for Supplier resource issues	C	R

Confidential

Activity	Customer	AMS
Managed Account Onboarding		
Grant access to the AMS 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
Manage the lifecycle of users and their permissions, for local directory services, used to access Supplier accounts and instances	R	I
Recommend reserved instances optimisation	I	R
Onboard account(s) to Trusted Remediator	C,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 Amazon Machine Image (AMIs) and stacks for Autoscaling groups (ASGs)	R	C

Confidential
Confidential
Confidential

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

Activity	Customer	AMS
Patch the Windows operating system, and Microsoft packages installed on the operating system which are governed by Windows Update	I	R
Patch installed applications, software, or application dependencies not managed by Windows Update	R	I
Patch the Linux operating system and manage packages through the operating system's native package manager (for example Yum, Apt, Zypper)	I	R
Patch installed applications, software, or application dependencies not managed by the Linux operating system's native package manager	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 of supported Supplier services resources as part of incident management	R	I
Perform backup restoration activities for resources of supported Supplier services	I	R
Restore affected custom or third-party applications	R	I
Networking		
Provisioning and configuration of Managed Account VPCs, IGWs, Direct Connect, and other Supplier networking Services	R	I
Configure and operate Supplier 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 Supplier network	R	I
Monitor defined by AMS for network security, including security groups	I	R
Network-level logging configuration and management (VPC flow logs and others)	I	R

Confidential

Activity	Customer	AMS
Logging		
Record all application change logs	R	I
Record Supplier infrastructure change logs	I	R
Enable and aggregate Supplier audit trail	I	R
Aggregate logs from Supplier 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 Supplier resources using baseline CloudWatch metrics and alarms	I	R
Investigate alerts from Supplier 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
Configure Trusted Advisor checks for remediation	R	C
Automatically remediate supported Trusted Advisor checks	I	R
Manually remediate supported Trusted Advisor checks	R	C
Report remediation status	I	R
Troubleshoot remediation failures	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 Supplier services for security management of the account and its Supplier resources	I	R
Manage privileged credentials for account and OS access for AMS engineers	I	R
Security Risk Management		

Confidential

Activity	Customer	AMS
Monitor supported Supplier services for security management, like GuardDuty and Macie	I	R
Define and create AMS-defined Config Rules to detect if Supplier resources comply with CIS and NIST security proven 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 effect of remediating AMS-defined Config Rules	R	I
Request remediation of AMS-defined Config Rules in the Supplier account	R	I
Track resources exempted from AMS-defined Config Rules	R	I
Remediate supported AMS-defined Config Rules in the Supplier account	C	R
Remediate non-supported AMS-defined Config Rules in the Supplier account	R	I
Define, monitor, and investigate Customer-specific Config Rules	R	I
Incident Management		
Notify about incidents detected by AMS in Supplier resources	I	R
Notify about incidents in Supplier resources	R	I
Notify about incidents for Supplier resources based on monitoring	I	R
Handle application performance issues and outages	R	I
Categorise incident priority	I	R
Provide incident response	I	R
Provide incident resolution or infrastructure restore for resources with available backups	C	R
Security Incident Response—Prepare		
Communications		
Provide and update Customer security contact details for AMS to use during security events notifications and security escalations	R	I
Store and manage the supplied Customer security contact details to use during security events and security escalations	C	R
Training		
Provide Customer with documentation to support AMS during incident response process	I	R
Practice shared responsibility during incident response processes through security gamedays	R	R

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

Activity	Customer	AMS
Resource Management		
Configure supported security management Supplier services for alerting, alerts correlation, noise reduction and additional rules	I	R
Maintain a comprehensive inventory of Supplier resources (Amazon EC2, Amazon S3 etc.), including details on the value and criticality of each asset to the business. This information will be instrumental in determining an effective containment strategy	R	C
Employ Supplier tags to identify resources and workloads	R	C
Define and configure log retention and archival	I	R
Establish a secure baseline by defining and enforcing the organisation's security policies and configurations for Supplier accounts, services, and access management	R	I
Security Incident Response – Detect		
Logging, Indicators and Monitoring		
Configure logging and monitoring to enable event management for instance and accounts	I	R
Monitor supported Supplier services for security alerts	I	R
Deploy and manage endpoint security tools	R	I
Monitor for malware on instances using endpoint security	R	I
Notify Customer of detected events through outbound messaging	I	R
Coordinate internal stakeholder communications and leadership updates to improve response time	R	I
Define, deploy, and maintain AMS standard detection services (for example, Amazon GuardDuty and AWS Config)	C	R
Record AWS infrastructure change logs	R	I
Enable and configure logging, monitoring to enable event management for the application	R	C
Implement and maintain an allow-list, deny-list, and custom detections on supported Supplier security services (for example, Amazon GuardDuty)	R	R
Security Event Reporting		
Notify AMS of a suspicious activity or an active security investigation	R	I
Notify detected security events and incidents to the Customer	I	R
Notify planned event that might trigger Security Incident Response process	R	I
Security Incident Response – Analyse		
Investigation And Analysis		

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

Activity	Customer	AMS
Perform initial response for supported security alert generated by a supported detection source	I	R
Assess false/true positives using the available data	R	R
Generate a snapshot of affected instances to be shared with the Customer if needed	I	R
Perform forensics tasks such as chain of custody, file system analysis, memory forensics, and binary analysis	R	C
Collect application logs to aid investigation	R	I
Collect data and logs to aid investigation on security alerts	R	R
Engage subject matter experts (SMEs) within Supplier services on security investigations	C	R
Share investigation logs from supported Supplier services to Customers during an investigation	I	R
Communication		
Send alert and notifications from AMS detection sources for managed resources	I	R
Manage alert and notifications for application security events	R	I
Engage Customer security point of contact during a security incident investigation	R	I
Security Incident Response – Contain		
Containment Strategy And Execution		
Assess risks and decide the containment strategy, acknowledging potential service impacts	R	C
Make a backup of affected systems for further analysis	I	R
Contain applications and workloads (through application specific configuration or response activity)	R	C
Define the containment strategy based on the security incident and the affected resource	I	R
Enable encryption and secure storage of point in time backups of affected systems	C	R
Execute supported containment actions for Supplier resources including EC2 instances, network, and IAM	I	R
Security Incident Response – Eradicate		
Eradication Strategy And Execution		
Define eradication options based on the security incident and the affected resource on Customer application workloads	C	R
Decide on the agreed eradication strategy, timing of eradication execution and the consequences	R	I

Please treat this information as private and confidential.

Activity	Customer	AMS
Define eradication steps based on the security incident and the affected resource on AMS managed workloads	C	R
Eradicate threats and harden Supplier resources including EC2 instances, network, and IAM eradication	R	C
Eradicate threats and harden applications and workloads (through application specific configuration or response activity)	R	I
Security Incident Response – Recover		
Recovery Preparation And Execution		
Configure backup plans and targets as requested by the Customer	I	R
Review backup plans to restore AMS managed workloads	R	I
Perform backup restoration activities for resources of supported Supplier services	I	R
Backup Customer application, APP configuration, and deployment settings, and review backup plans to restore Customer applications and workloads post incident	R	I
Restore applications and Customer workloads (through application specific restoration steps)	R	I
Security Incident Response—PIR		
Post Incident Reporting		
Share appropriate lessons learned and action items with Customer post incident as required	I	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 optimisation 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

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

Activity	Customer	AMS
Record changes made by AMS Operations	I	R
Cost Optimisation		
Collect all required inputs to configure Resource Scheduler	R	I
Request the onboarding, configuration of Resource Scheduler and provide all required inputs	R	I
Deploy Resource Scheduler per Customer configuration	C, I	R
Disable and enable the Resource Scheduler on Customer account	R	C
Create, delete, describe, and update schedules	C	R
Create, delete, describe, and update periods	C	R
Investigate and troubleshoot issues with Resource Scheduler	I	R
Request for off-boarding the Resource Scheduler	R	I
Offboard the Resource Scheduler from account	C, I	R

2.2 Scope of Changes Performed by AMS Accelerate

AMS Accelerate only makes changes for the specific purposes and situations described next. AMS makes changes only at the infrastructure level, using the console or APIs. AMS never changes the Customer's application, control, or domain layers. Customer can see any changes made by AMS (or other users) using the Supplier's set of pre-built queries; to do this, see Tracking changes in your AMS Accelerate accounts.

Supplier Resources

AMS Accelerate deploys or updates Supplier 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 as part of Responses to violations in Accelerate (making noncompliant resources conform to security proven practices).
- During remediation and restoration as part of an incident response.
- When responding to Customer requests to configure AMS features, such as the following:
  - Alarm manager
  - Resource tagger
  - Patch baselines and maintenance windows
  - Resource scheduler
  - Backup plans

AMS Accelerate does not deploy or update resources outside of these situations. If Customer needs help from AMS to make changes in other situations, they can use Operations on Demand.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

Operating System Software

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

Application Code and Configuration

AMS Accelerate never modifies Customer code (for example, AWS CloudFormation templates, other IaC templates, or Lambda functions) but can guide teams on which changes are required to follow best operational and security practices. AMS Accelerate provides troubleshooting assistance for infrastructure issues that affect applications, but AMS Accelerate does not access or validate Customer application configurations.

1.4 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

1.5 Pricing Overview

Refer to the AWS UK G-Cloud 15 Pricing Document affiliated with this service in the Digital Marketplace.

1.6 Governance

Customers have a designated CSDM who provides advisory assistance across AMS Accelerate, and has a detailed understanding of Customer use cases and technology architecture for the managed environment. CSDMs work with Account Managers, TAMs, AMS CAs, and AWS Solutions Architects (SAs), as applicable, to help launch new projects and give proven practice recommendations throughout the software development and operations processes. The CSDM is the primary point of contact for AMS. Key responsibilities of Customer CSDM are:

- Organise and lead monthly service review meetings with Customers.
- Provide details on security, software updates for environment and opportunities for optimisation.
- Champion Customer requirements including feature requests for AMS Accelerate.
- Respond to and resolve billing and service reporting requests.
- Provide insights for financial and capacity optimisation recommendations.

1.7 Contact and Escalation

AMS will work on all Customer requests during business hours as indicated below.

Table 4. AMS Accelerate Contact and Escalation Times

Feature	AMS Accelerate
Service request	24/7
Incident management (P1)	
Incident management (P2-P3)	

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

Feature	AMS Accelerate
Backup and recovery	
Patch management	
Monitoring and alerting	
CSDM	Monday to Friday 08:00—17:00, local business hours

Escalation Path

AMS supports Customers with Incident Management and Service Request Management, 24 hours a day, 7 days a week, 365 days a year; in accordance with the AMS SLAs applied to the account.

To report a Supplier or AMS service performance issue that impacts Customer managed environment, Customers can use the AMS console and submit an incident case. For details, see Submitting an incident. For general information about AMS incident management, see Incident management.

To ask for information or advice, or to request additional services from AMS, Customer can use the AMS console and submit a service request. For details, see Creating a service request. For general information about AMS service requests, see Service request management.

1.8 Onboarding

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

1.9 SLAs

The SLA can be found here: https://s3.amazonaws.com/ams.contract.docs/AWSManagedServicesSLA.pdf.

1.10 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/

1.11 Operations on Demand

Operations on Demand is an AMS feature that extends the standard scope of Customer AMS Operations plan by providing operational services that are not currently offered natively by the AMS operations plans or the Supplier. A combination of automation and skilled AMS resources delivers the catalogue offering after selection. There are no long-term commitments or additional contracts, allowing Customers to extend their existing AMS and Supplier operations and capabilities as needed. Customers agree to purchase blocks of hours (Operations on Demand (OOD) blocks), 20 hours per block, monthly.

Customer can select from the catalogue of standardised offerings and initiate a new OOD engagement through a service request. Examples of OOD offerings include assisting with the maintenance of Amazon EKS, operations of AWS Control Tower, and management of SAP clusters. New catalogue offerings are added regularly based on demand and the operational use cases we see most often.

OOD is available for AMS Accelerate operations plans and is available in all AWS Regions where AMS is available.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

AMS performs Customer Security Risk Management (CSRM) while implementing requested changes. To learn more about the CSRM process, see Change request security reviews.

OOD Catalogue of Offerings

OOD offers Customers the services described in the Table 5.

Table 5. OOD Services

Operations Plan	Title	Description	Expected Outcomes
AMS Accelerate	Amazon EKS cluster maintenance	AMS frees container developers by handling the ongoing maintenance of Customer 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 and a curated set of Amazon EKS and Kubernetes add-ons.	Customer teams assisted with the underlying operations work of updating Amazon EKS clusters.
AMS Accelerate	AMI Building and Vending	AMS provides ongoing management of AMI building and vending for Customers. Supplier engineers release a monthly list of subscribed AMIs, release on demand AMIs for emergent patching activities, manage changes using runbooks, and monitor AMI builds using CloudWatch Monitoring. Supplier also provides troubleshooting assistance and detailed reporting for all AMIs used in designated accounts. This offering requires AMI build Pipelines to be deployed via EC2 Image builder. AMS does not support any other automation or service that interacts with EC2 Image builder.	Customer security posture improved, and Customer time spent on building and vending AMIs reduced.
AMS Accelerate	Curated change execution	Customers can work with the Supplier's skilled operations engineers to translate business requirements into validated change requests that can be executed safely within the Supplier environment. Customer can take advantage of the Supplier's unique approach to automation and knowledge of operational proven practices (for example, impact assessment, roll backs, two-person rule), whether it is a simple change at scale or a complex action with downstream impacts.	Customers assisted with defining, creating, and executing custom change requests. Changes can be manual or automated (CloudFormation, SSM). Includes consultation with Support for configuration guidance when necessary. Not intended for changes to application code, application installation/deployment, data migration, or OS configuration changes.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

Operations Plan	Title	Description	Expected Outcomes
AMS Accelerate	AWS Network Firewall Operations	AMS collaborates with Customers to onboard firewalls and implement and manage the policies and rules for ongoing firewall operations. Supplier engineers do this by using Supplier operational proven practices and automation to configure standardised policies and rules, and by enabling monitoring to detect changes made outside of the automation process. AMS quickly notifies Customers of unwanted changes and provides options to include them, if requested, or restore the account to a previous configuration to help ensure the overall stability of Customer systems.	Customer teams assisted with reducing management overhead by quickly detecting unintentional network firewall changes, resulting in improved incident resolution and reduced RCA time for both expected and unexpected issues.
AMS Accelerate	AWS Control Tower operations	Ongoing operations and management of Customer AWS Control Tower landing zone, including AWS Transit Gateway and AWS Organizations – providing a landing zone solution. The Supplier handles account vending, SCP and OU management, drift remediation, SSO user management, and AWS Control Tower upgrades with the Supplier's library of custom controls and guardrails.	Customer teams assisted with some of the underlying operations work of managing AWS Control Tower, AWS Transit Gateway, and AWS Organizations.
AMS Accelerate	AWS landing zone Accelerate operations	AMS provides ongoing operations of AWS landing zones deployed through AWS Landing Zone Accelerator (LZA). Supplier engineers handle configuration file changes, AWS Control Tower environment management (account vending, OU creation, guardrails), service control policy management, Control Tower drift detection and remediation, network configuration management, and updates to Control Tower and the LZA framework. AWS LZA provides a means to set up and govern a secure, multi-account Supplier environment using operational proven practices and services such as AWS Control Tower.	Customer teams assisted with ongoing operations and management of the AWS LZA solution.
AMS Accelerate	SAP Cluster Assist	Dedicated alarming, monitoring, cluster patching, backup, and incident remediation for Customer	Customer or partner SAP teams assisted with some of the underlying operations work.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

Operations Plan	Title	Description	Expected Outcomes
		SAP clusters. This catalogue item allows Customers to offload some of the ongoing operational work from their SAP operations team so that they can focus on capacity management and performance tuning.	The Customer must still provide other SAP capabilities such as capacity management, performance tuning, DBA, and SAP basis administration.
AMS Accelerate	SQL Server on EC2 Operations	AMS collaborates with the Customer to onboard, implement, and manage the ongoing operations of SQL Server databases deployed on EC2 instances. Supplier engineers use operational proven practices and automation to free up Customer database teams by performing tasks such as backup and patching, extending AMS operational support to SQL Server patching to include cluster-aware rolling updates, backup and restore services aligned with Supplier ransomware defence strategy, and monitoring adherence to Customer-provided backup and patching controls.	SQL Server Customers assisted with offloading patching and backup database operations to improve resilience, and security posture of their workloads, in addition to optimising licence costs by bringing their own licences (BYOL) to EC2.
AMS Advanced	Amazon EKS Cluster Maintenance	AMS frees Customer's container developers by handling the ongoing maintenance and health of 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 and a curated set of Amazon EKS and Kubernetes add-ons.	Customer teams assisted with the underlying operations work of updating Amazon EKS clusters.
AMS Advanced	Priority Requests for Change (RFC) Execution	Designated AMS Operations engineer capacity to prioritise the execution of Customer RFC. All submissions 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 Service Level Objective (SLO) of 8 hours for RFCs.
AMS Advanced and AMS Accelerate	Legacy OS Upgrade	Avoid an instance migration by upgrading instances to a supported operating system version. The Supplier can perform an in-place upgrade on Customer selected instances using	This solution addresses applications that users can no longer re-install on a new instance (for example, lost source code, ISV out of business, and so on).

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

Operations Plan	Title	Description	Expected Outcomes
		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. The following operating systems are supported for in-place upgrades: Microsoft Windows 2012 R2 to Microsoft Windows 2016 and above Microsoft Windows 2016 to Microsoft Windows 2022 and above Red Hat Enterprise Linux 7 to Red Hat Enterprise Linux 8 Red Hat Enterprise Linux 8 to Red Hat Enterprise Linux 9 Oracle Linux 7 to Oracle Linux 8	Customers can roll failed upgrades back to their original state. From an operational perspective, administrators prefer rolling back because it puts the instance in a more supportable state with the latest security patches.

Requesting AMS OOD

Supplier accounts onboarded to AMS can access AMS OOD. To take advantage of OOD, Customers can request additional information from their CSDM, SA, account manager, or CA. Available OOD offerings are listed in the Operations on Demand catalog of offerings table. After completing engagement scoping, customers should submit a service request to AMS Operations to start an engagement for OOD.

Each OOD service request must contain the following detailed information pertaining to the engagement:

- The specific OOD offerings requested, and for each specific OOD offering:
  - The number of blocks (one block is equal to 20 hours of operational resource time in a given calendar month, to be charged at SUPPLIER's then-current standard rate for the applicable Operations on Demand offering) to allocate to the specific OOD offering.
  - The account ID for each AMS account for which the specific OOD offering is being requested.

OOD service requests must be submitted by the Customer through either:

- The AMS account that receives the applicable OOD offerings, or
- An AMS account that is an AWS Organizations Management account in all features mode, on behalf of any of its member accounts that are AMS accounts.

AMS Operations reviews and updates accounts with their approval, partial approval, or denial after receiving the OOD service request. AMS and the Customer coordinate to begin the engagement once they approve the OOD offerings service request. The Supplier will not

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.
Please treat this information as private and confidential.

initiate any OOD offerings until approval of the service request and agreement on an engagement start date.

AMS uses a monthly subscription allocation of OOD blocks. The Supplier will allocate the approved number of blocks monthly, starting from the engagement start date, until the Customer requests to opt out through a new service request. OOD blocks are valid for a calendar month. Unused blocks, or block portions, are not rolled over or carried forward to future months.

Customers are billed a minimum of one OOD block each month, regardless of the number of hours used. Any additional, allocated, OOD block in which no hours were used, is not billed.

Making Changes to OOD Offerings

To request changes to ongoing engagements for OOD offerings, Customers can submit a service request containing the following information:

- The modification(s) being requested, and
- The requested date for the modifications to become effective.

After receiving the OOD service request, AMS Operations reviews the request and either updates with their approval or requests that the assigned CSDM work with the Customer to determine the scope and implications of the modification. If the CSDM must scope the modification, the Customer must submit a second OOD service request to initiate the modified engagement after completing the scoping exercise.

Once approved, the most recently modified block allocation becomes and continues to stay active, superseding any prior block allocations, unless agreed otherwise by the Supplier and the Customer.

1.12 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 IAM roles that give the Supplier access from all AMS Accelerate accounts or the specified AMS Accelerate account, as applicable.

Confidential
Confidential
Confidential