AWS Managed Services (AMS) for Operational Excellence

1. AMS for Helpdesk
2. AMS for Proactive Monitoring
3. AMS for Security Operations
4. AMS for Logging
5. AMS for Patching
6. AMS for Backup
AWS Managed Services (AMS) for Helpdesk

Part of Operational Excellence with AMS

Use this reference architecture to understand how AMS provides 24x7 helpdesk in an AWS environment. AMS provides unlimited access to Incident and Response, service request, and problem management for all AWS services as part of an AMS managed account.

The Helpdesk capability primarily falls under the information technology service management (ITSM) team. They define policies, provide service level agreement (SLA) requirements, implement operational integration, and ITSM tooling (if needed). The Operations teams follow the guidelines and handle incidents at App, OS, Infra, and security levels.

Customers either have in-house helpdesk or use Partners to offload the L1/L2 service desk. With AWS Managed Services (AMS), customers/Partners can rely on AMS Helpdesk 24x7 for incidents at OS, Infra, and Security levels, and use their workforce for more value-added activities and reduce staff churn.

Customers/Partners are responsible for ITSM tooling and integration to the AWS ticketing system. AMS customers can rely on AWS Service Management Connector (for ServiceNow or JiraSD) or use AWS Support APIs to integrate with the AWS/AMS ticketing system.

Incidents and service requests raised by customers or Partners, using ITSM tool or directly using AMS Console, end up in the standard AWS Support console, where AMS provides updates and resolutions.

Events from AMS proactive monitoring and AMS security guardrails are received into the AMS service account, where they are investigated and converted into incidents after discarding false positives. AMS automation raises incidents, triggers remediations where necessary, and customers are updated via the AWS Support portal.

AMS acts as a single interface for all AWS-related incidents. The AMS Operations team monitors the customers’ environment 24x7 (with email, phone, and chat support), and are backed by dedicated AMS security engineers. Customers/Partners also get access to an AMS architect and a delivery manager for ongoing tech consultations and service reviews.

Take help of AMS operations for proactive incident management in addition to achieving overall operational excellence in AWS cloud. Refer to the AMS User Guide Incident & SR section for further information.
AWS Managed Services (AMS) for Proactive Monitoring
Part of Operational Excellence with AMS

Use this reference architecture to understand how to use AMS for improved observability (such as metrics, alarms, and response). AMS takes ownership of AWS Infrastructure and OS monitoring, alerting, and restoration as part of the AMS operations plan.

The architecture and governance teams define high level policies, requirements, and tooling, whereas application and operations teams follow the guidelines and ensure monitoring is in place at the application, OS, and infrastructure levels.

As part of the account onboarding, AMS sets up and enables multiple AWS services such as Amazon CloudWatch, AWS Config, and Amazon GuardDuty to monitor at OS, infrastructure, and AWS account levels.

AMS deploys various Amazon CloudWatch monitors, alerts, rules, and dashboards as baseline monitoring to monitor OS and AWS services (such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Elastic Block Store (Amazon EBS), AWS VPN, NAT Gateway, and so on).

AMS implements and monitors numerous custom AWS Config rules to provide coverage against PCI, NIST, CIS, and HIPAA compliance standards.

AMS implements threat monitoring using Amazon GuardDuty, which in turn provides 100+ guardrails against Amazon EC2, Amazon Simple Storage Service (Amazon S3), AWS Identity and Access Management (AWS IAM), and Amazon Elastic Kubernetes Service (Amazon EKS).

AMS customers can use AMS Service Console and an AMS-curated tool (Alarm Manager) to further create custom CloudWatch alarms or change AMS monitoring thresholds.

Events or metadata from all AWS monitoring services in customer accounts go into an AMS internal service account where events are processed for investigation, noise reduction, incident/case management, aggregation, reporting, and remediation.

AMS uses heavy automation to manage and monitor AWS services and OS for customers across the globe. A high percentage of AMS alarms are auto-remediated using AWS Systems Manager (AWS SSM) and AMS-curated AWS SSM runbooks.

Use AMS operations to offload infrastructure and OS monitoring and remediation, and focus on the application layer. Refer to the AMS User Guide Monitoring section for further information. For logging (as part of observability), refer to the AMS reference architecture for Logging.
The security and governance teams define high level policies, requirements, and tooling, whereas application and operations teams follow the guidelines to ensure security best practices are implemented at the application, operating system (OS), and infrastructure levels.

As part of the account onboarding, AMS enables essential AWS services and logs to achieve desired security posture at OS, AWS infrastructure, and account levels.

AMS uses Amazon GuardDuty to continuously monitor threats and potential malicious activities (for services such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), AWS Identity and Access Management (AWS IAM), Kubernetes, and so on. In addition, AMS implements numerous custom AWS Config rules to provide visibility against PCI, NIST, CIS, and HIPAA compliance standards, and take remedial actions upon rule violations. Optionally, AMS can also monitor for sensitive data (such as PII, PHI and so on) utilizing AWS Macie.

All threat findings and non-compliant rules generate monitoring events that go into an AMS internal service account, where they are processed for investigation, noise reduction, incident/case management, aggregation, and reporting and remediations.

AMS uses heavy automation to create and remediate Incidents using AWS Systems Manager. AMS also helps restore services/data using AWS Backup from the last good backup as part of the AMS Backup service.

Customers can also collate and ingest security events from multiple third party security tools, and monitor using AWS Security Hub. Events from Security Hub and AMS detective services can be further correlated for log analysis.

To achieve overall operational excellence in the AWS Cloud, in addition to security guardrails, AMS provides 24x7 Security and Incident Management, Monitoring and Logging, and Backup and OS Patching as part of its operating plans. Refer to the AMS User Guide for further information.
AWS Managed Services (AMS) for Logging
Part of Operational Excellence with AMS

Use this reference architecture to understand how to use AMS for centralized observability (such as logging and tracing). AMS enables and aggregates multiple logs as part of account onboarding.

- The logging capability primarily falls under the Security and Governance teams. They define policies, provide guidelines, requirements, and tooling (if needed).
- Architecture and DevOps teams follow the guidelines and ensure logging is enabled at application, OS, and Infrastructure (API, firewall, network) levels.
- AMS improves the overall logging posture by enabling logging of 5 of the 6 essential log types. Cloud Infra API (via AWS CloudTrail), OS and app (via Amazon CloudWatch OS agent), and network (VPC Flow Logs) are enabled as part of the account onboarding.
- All these essential logs are locally available in the CloudWatch logs for local log search, alerting or troubleshooting via built-in CloudWatch Insights. Customers can choose required retention period for local logs (for example, 3 months).
- AMS further improves the overall logging posture by enabling 2 of the 3 essential event types. Local events from 200+ AWS Config rules and Amazon GuardDuty findings are automatically enabled as part of AMS onboarding. AMS Ops monitor these findings 24x7 and remediate as needed.
- To improve access and local monitoring, customers can aggregate all security related events (or findings) into a dedicated centralized security account for GuardDuty, AWS Config, or AWS Security Hub with the help of AMS operations.
- Push consolidated event logs using Amazon EventBridge, and local CloudWatch log groups into a dedicated centralized logging account. Use Amazon Kinesis to collect, filter, and transform all logs and event streams at high scale, and index into Amazon OpenSearch for operational alerting, reporting, dashboards, and so on.

AMS helps customers set up centralized logging. Refer to the AMS User Guide Logging section for further information. For monitoring (as part of observability), refer to the AMS reference architecture for Monitoring.
AWS Managed Services (AMS) for Patching
Part of Operational Excellence with AMS

Use this reference architecture to understand how to use AMS for cross account centralized patching. AMS takes complete ownership of OS patching, notifications, rollback, and reporting as part of the AMS operations plan.

The patching capability primarily falls under the Security and Governance teams. They define policies, provide guidelines, and requirements.

Application and DevOps teams follow the guidelines to ensure regular patching is performed at the application and OS levels. App teams are responsible for defining patch windows and post-patch application testing.

AMS sets up a patch automation as part of the AWS account onboarding. Customers define the patch groups based upon environment, tiers, applications, and so on using AWS Tags. Customers can use a curated AMS Resource Tagger tool to enforce all required tags.

AMS uses AWS Systems Manager to perform OS patching. AMS works with the customer to set up patch baselines and patch maintenance windows using the AMS-provided Systems Manager automation documents (runbooks). AMS also sets up a default SSM patch maintenance window (to ensure default coverage across the EC2 fleet).

AMS further provides daily patch coverage reporting based on account, groups, patches, and so on. Reports are available to download and consume via AMS Console.

AMS implements patch alerting and monitoring using AWS Config rules and Amazon CloudWatch. The AMS internal service account runs patch orchestration and automation for all AMS customers using multiple AWS services behind the scenes. Amazon EventBridge in the AMS account receives all patch-related AWS events from the SSM services, and performs the following functions using SSM APIs:

- pre/post patch notifications
- pre-patch backup
- OS patch updates
- patch failure remediations
- patch inventory

Use the AMS operations plan to offload OS patch management to AWS. For more information, refer to the AMS User Guide Patching section.
Use this reference architecture to understand how to use AMS for data availability or continuity management. AMS takes complete ownership of backup monitoring, alerting, restoration, and reporting as part of the AMS operations plan.

The backup capability primarily falls under the Architecture and Governance teams. They define policies, and, provide guidelines and requirements. Application and DevOps teams follow the guidelines and ensure regular backup is performed at the application and operating system (OS) levels. App teams are responsible for defining backup windows/plans, along with backup, restore, and disaster recovery (DR) testing.

AMS uses AWS Backup to perform the backup and restore for all AWS services it supports. AMS sets up backup automation and vaults as part of the AWS account onboarding.

AMS provides multiple backup plans to suit different needs. Customers can set up custom backup plans or vaults based on environment, tier, recovery point objective (RPO), applications, and so on. Customers use AWS tags to define the backup target/groups. AMS provides a curated AMS Resource Tagger automation to enforce all required tags.

AMS further provides daily backup coverage reporting based on account, plan, resources, and so on. Backup reports are available to consume and export via AMS Console. Reports are powered by AMS-owned Amazon QuickSight in multiple formats.

AMS implements backup alerting and monitoring using AWS Config rules and Amazon CloudWatch. The AMS internal service account runs backup orchestration and automation for all AMS customers using multiple AWS services behind the scene. Amazon EventBridge in the AMS account receives all backup related AWS events from the backup and CloudWatch services to perform following functions:

- backup plan/vault deployment
- backup monitoring and alerting
- backup reporting
- backup failure remediations

Use the AMS operations plan to offload backup management to AWS. For more information, refer the AMS User Guide Backup section.