Architecture Diagrams

AWS Managed Services (AMS) for Operational Excellence

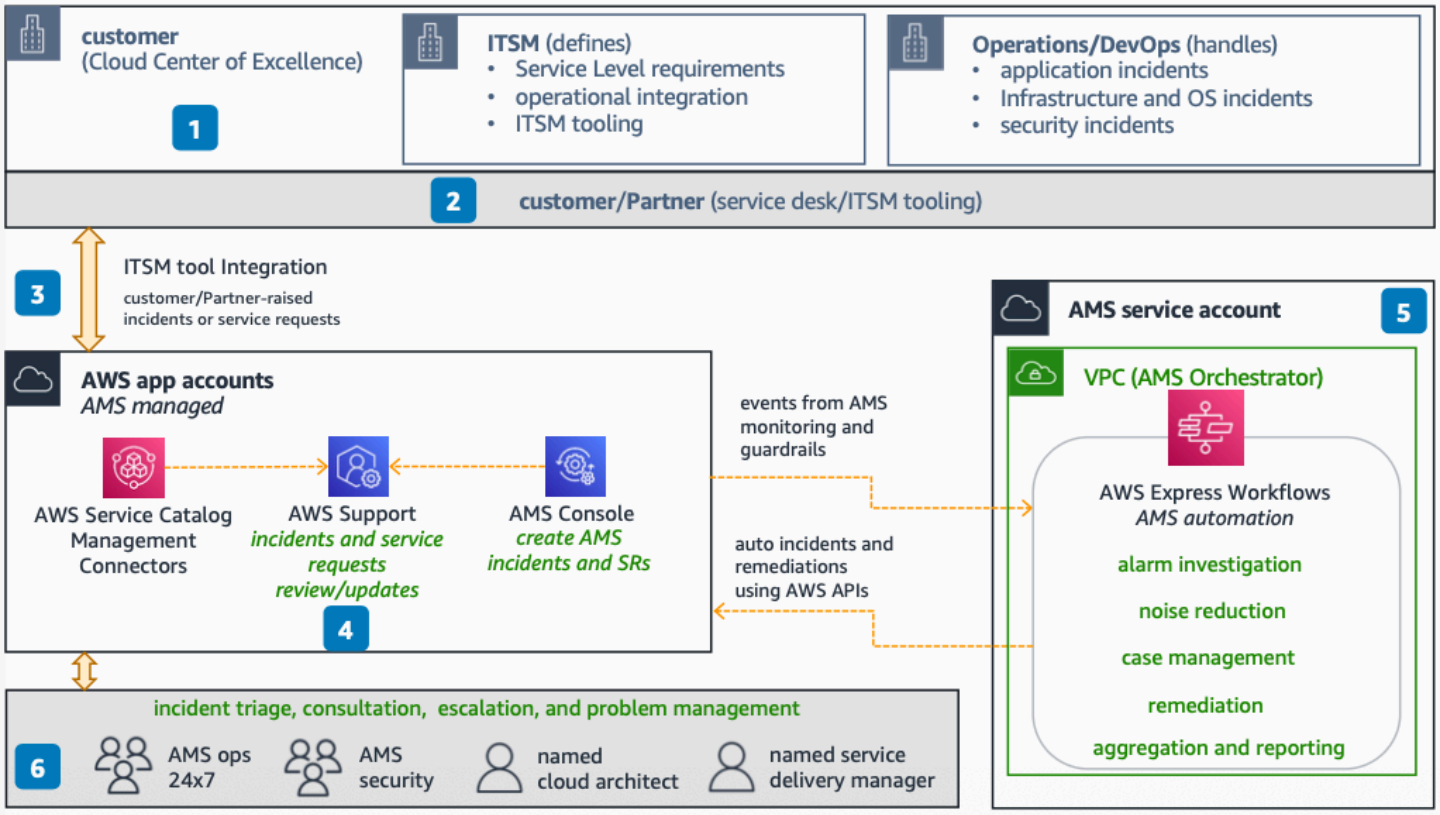
AWS Managed Services (AMS) for Operational Excellence: Architecture Diagrams

Table of Contents

AMS for Helpdesk

Use this reference architecture to understand how AWS Managed Services (AMS) provides 24x7 helpdesk in an AWS environment. AMS reduces operational burden by providing incident management, service requests, and problem management for all AWS services.

This reference architecture was validated by the AWS Managed Services team for technical accuracy on September 20, 2022.



The following steps describe the architecture:

1. The Helpdesk capability primarily falls under the information technology service management (ITSM) team. They define policies, provide guidelines, SLA requirements, and implement operational integration and ITSM tooling.
2. You or your partners can rely on AMS Helpdesk 24x7 for incidents at OS, infrastructure, and security levels. This frees your workforce for more value-added activities.
3. You and your partners are responsible for ITSM tooling and integration to the AWS ticketing system. With AMS, you can rely on AWS Service Management Connector (for ServiceNow or Jira SD) or use AWS Support APIs to integrate.

4. When you or your partners raise incidents and service requests, they end up in the standard AWS Support console. AMS then provides updates and resolutions.
5. The AMS service account receives events from AMS proactive monitoring and AMS security guardrails. AMS automation raises incidents, triggers remediations, and updates you through the AWS Support portal.
6. AMS acts as a single interface for all AWS related incidents. The AMS Operations team monitors your environments 24x7 (with email, phone, and chat support), backed by dedicated AMS security engineers.

Deploy the architecture

AWS Managed Services deploys and manages this architecture on your behalf as part of the AMS operations plan. You do not need to deploy CloudFormation templates or write custom code. To get started with AMS, see the What is AWS Managed Services? section in the AMS User Guide.

For onboarding details and account setup, see AMS onboarding.

Further reading

For additional information, refer to the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected
- AWS Managed Services product page

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagrams first published.	September 20, 2022

Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022

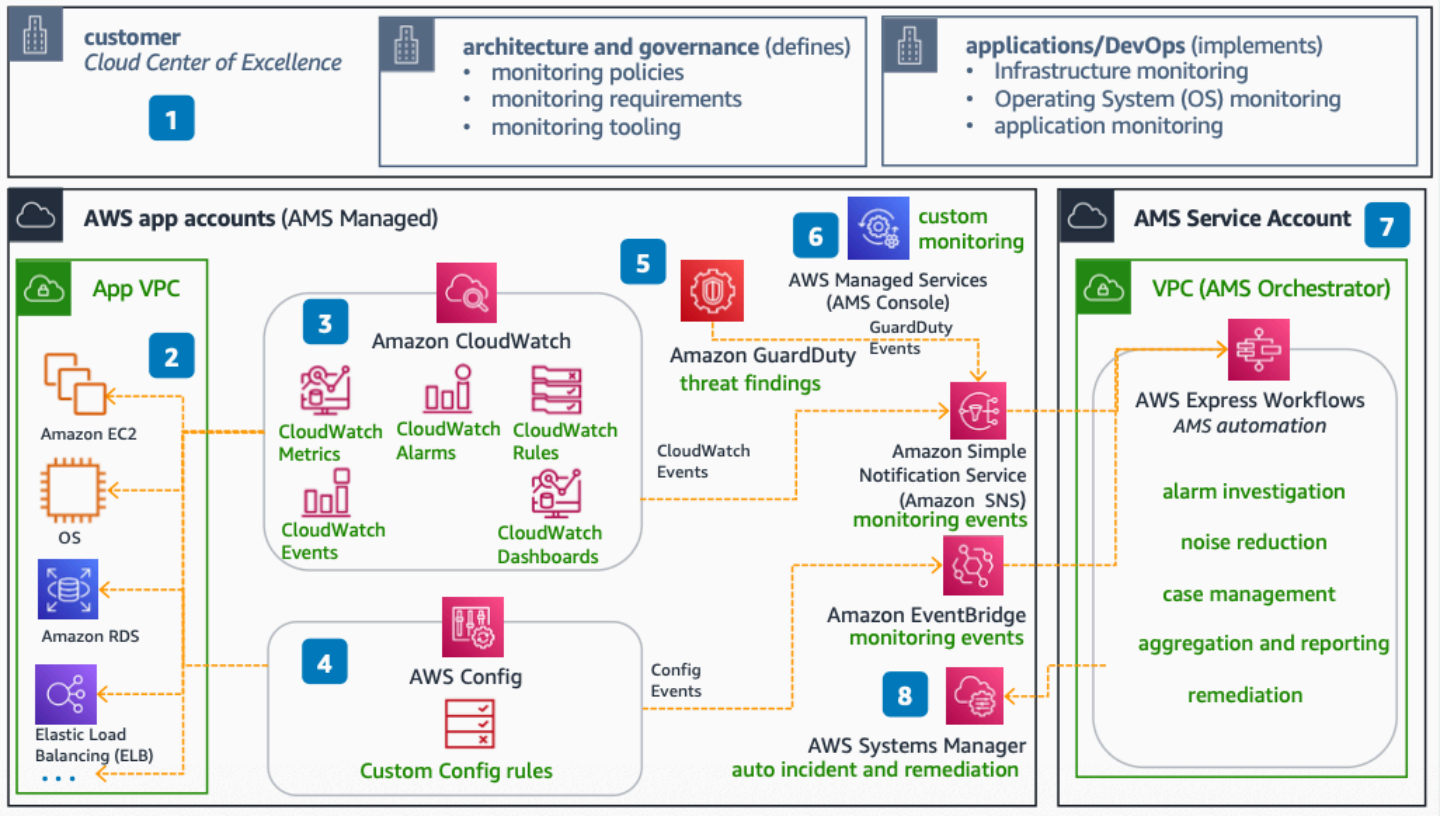
Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

AMS for Proactive Monitoring

Use this reference architecture to understand how AWS Managed Services (AMS) improves observability with metrics, alarms, and automated response. AMS takes ownership of AWS infrastructure and OS monitoring, alerting, and restoration.

This reference architecture was validated by the AWS Managed Services team for technical accuracy on September 20, 2022.



The following steps describe the architecture:

1. Architecture and governance teams define high-level policies, requirements, and tooling. Your application and operations teams follow the guidelines and ensure monitoring is in place.
2. As part of account onboarding, AMS sets up multiple AWS services for monitoring. These include Amazon CloudWatch, , and to monitor at OS, infrastructure, and account levels.
3. AMS deploys various CloudWatch monitors, alerts, rules, and dashboards as baseline monitoring. This covers OS and AWS services such as Amazon EC2, Amazon RDS, Elastic Load Balancing (ELB), AWS VPN, and NAT Gateway.

4. AMS implements and monitors numerous custom rules. These rules cover PCI, NIST, CIS, and HIPAA compliance standards.
5. AMS implements threat monitoring by using . This service monitors more than 100 guardrails against Amazon EC2, Amazon S3, IAM, and Amazon EKS.
6. With AMS, you can use the AMS Service Console and an AMS-curated tool (Alarm Manager) to create custom CloudWatch alarms or change AMS monitoring thresholds.

Deploy the architecture

AWS Managed Services deploys and manages this architecture on your behalf as part of the AMS operations plan. You do not need to deploy CloudFormation templates or write custom code. To get started with AMS, see the What is AWS Managed Services? section in the AMS User Guide.

For onboarding details and account setup, see AMS onboarding.

Further reading

For additional information, refer to the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected
- AWS Managed Services product page

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022

Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022

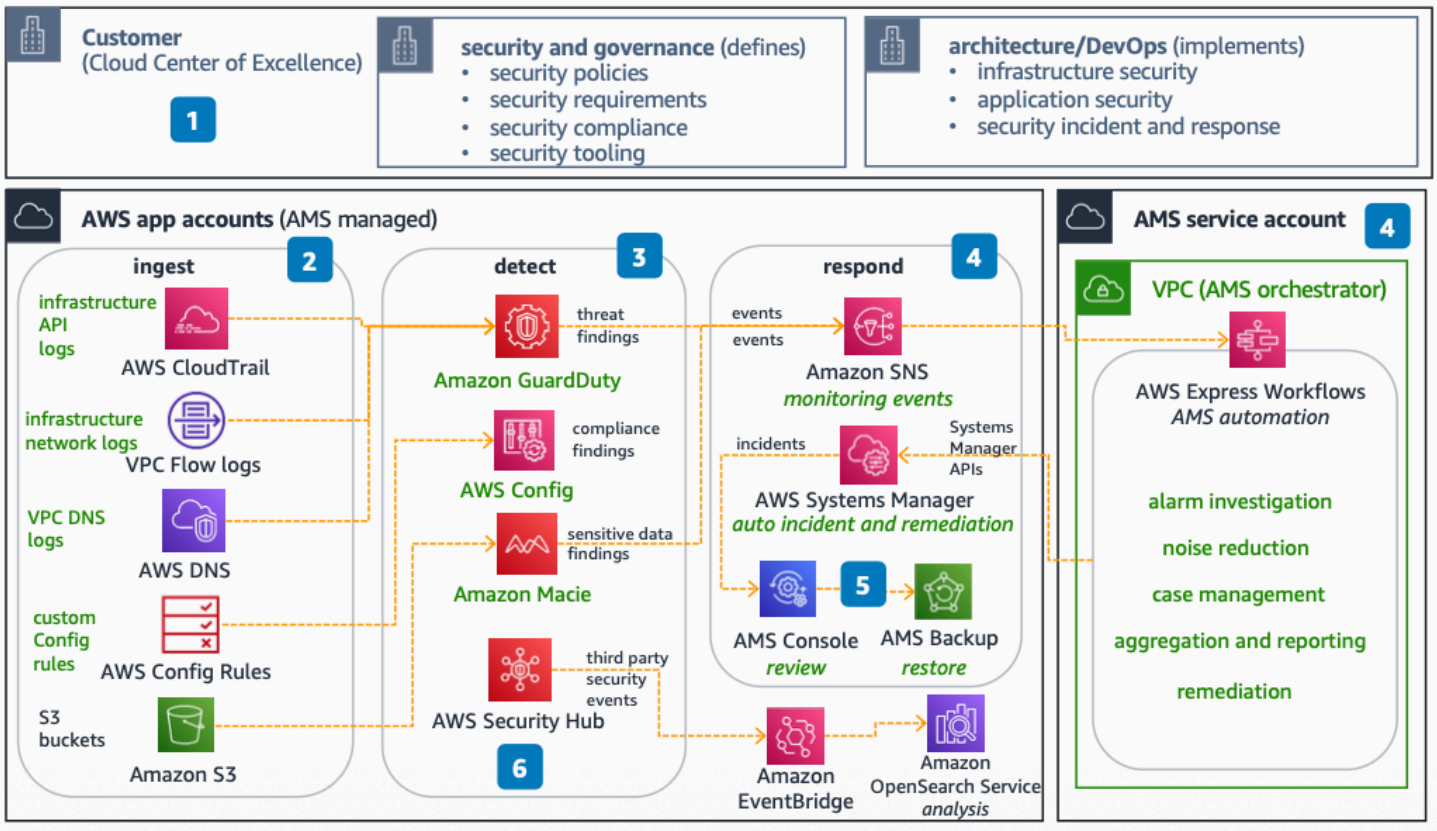
Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

AMS for Security Operations

Use this reference architecture to understand how AWS Managed Services (AMS) accelerates security and compliance in an AWS environment. AMS enables numerous security guardrails as part of account onboarding, providing a well-monitored and secure environment from day one.

This reference architecture was validated by the AWS Managed Services team for technical accuracy on September 20, 2022.



The following steps describe the architecture:

1. Security and governance teams define high-level policies, requirements, and tooling. Your application and operations teams follow the guidelines to ensure security best practices are implemented.
2. As part of account onboarding, AMS enables essential AWS services and logs to achieve the desired security posture at OS, infrastructure, and account levels.
3. AMS uses to continuously monitor threats and potential malicious activities. AMS also implements custom rules for PCI, NIST, CIS, and HIPAA compliance. Optionally, AMS can monitor for sensitive data by using AWS Macie.

4. All threat findings and non-compliant rules generate monitoring events. These events go into an AMS internal service account for investigation, noise reduction, and remediation.
5. AMS uses AWS Systems Manager to create and remediate incidents. AMS also helps restore services and data by using AWS Backup.
6. You can collate and ingest security events from multiple third-party security tools and monitor them by using AWS Security Hub.

Deploy the architecture

AWS Managed Services deploys and manages this architecture on your behalf as part of the AMS operations plan. You do not need to deploy CloudFormation templates or write custom code. To get started with AMS, see the What is AWS Managed Services? section in the AMS User Guide.

For onboarding details and account setup, see AMS onboarding.

Further reading

For additional information, refer to the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected
- AWS Managed Services product page

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022

Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022

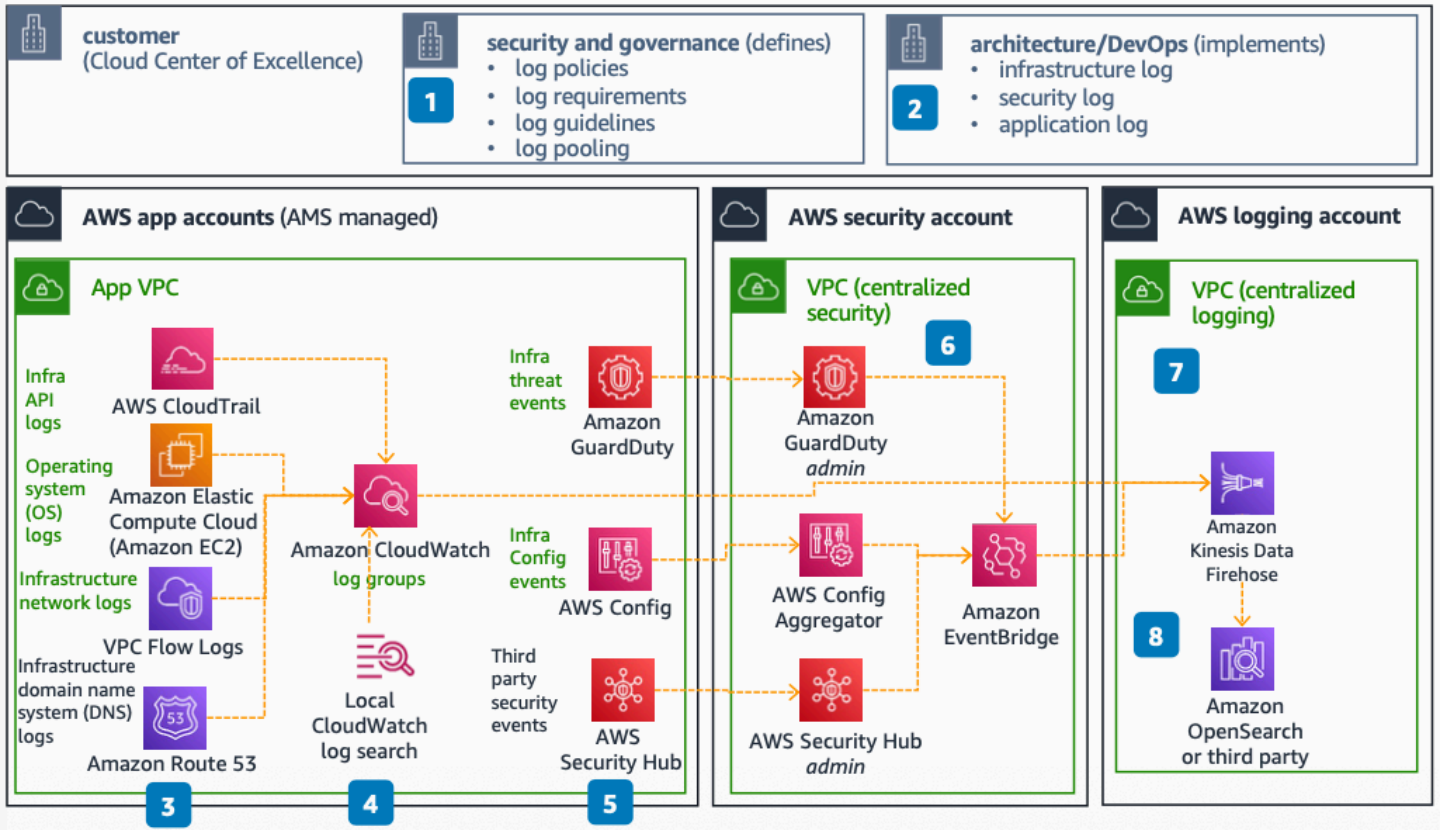
Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

AMS for Logging

Use this reference architecture to understand how AWS Managed Services (AMS) provides centralized observability with logging and tracing. AMS enables and aggregates multiple logs as part of account onboarding.

This reference architecture was validated by the AWS Managed Services team for technical accuracy on September 20, 2022.



The following steps describe the architecture:

1. The logging capability primarily falls under the security and governance teams. They define policies, provide guidelines, requirements, and tooling.
2. Architecture and DevOps teams follow the guidelines and ensure logging is enabled at application, OS, and infrastructure (API, firewall, network) levels.
3. AMS improves the logging posture by enabling 5 of 6 essential log types. Cloud infrastructure API (through AWS CloudTrail), OS and application (through CloudWatch OS agent), and network (VPC Flow Logs) are enabled as part of account onboarding.

4. All essential logs are locally available in CloudWatch Logs for local log search, alerting, or troubleshooting through built-in CloudWatch Insights. You can choose required retention periods for local logs.
5. AMS further improves the logging posture by enabling local events from 200+ rules and findings as part of onboarding. AMS Ops monitor these findings 24x7 and remediate as needed.
6. You can aggregate all security-related events into a dedicated centralized security account for , , or AWS Security Hub with help from AMS operations.
7. Push consolidated event logs by using and local CloudWatch log groups into a dedicated centralized logging account. Use Kinesis to collect, filter, and transform all logs and event streams at high scale. Then index into for operational alerting, reporting, and dashboards.

Deploy the architecture

AWS Managed Services deploys and manages this architecture on your behalf as part of the AMS operations plan. You do not need to deploy CloudFormation templates or write custom code. To get started with AMS, see the What is AWS Managed Services? section in the AMS User Guide.

For onboarding details and account setup, see AMS onboarding.

Further reading

For additional information, refer to the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected
- AWS Managed Services product page

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date

Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022

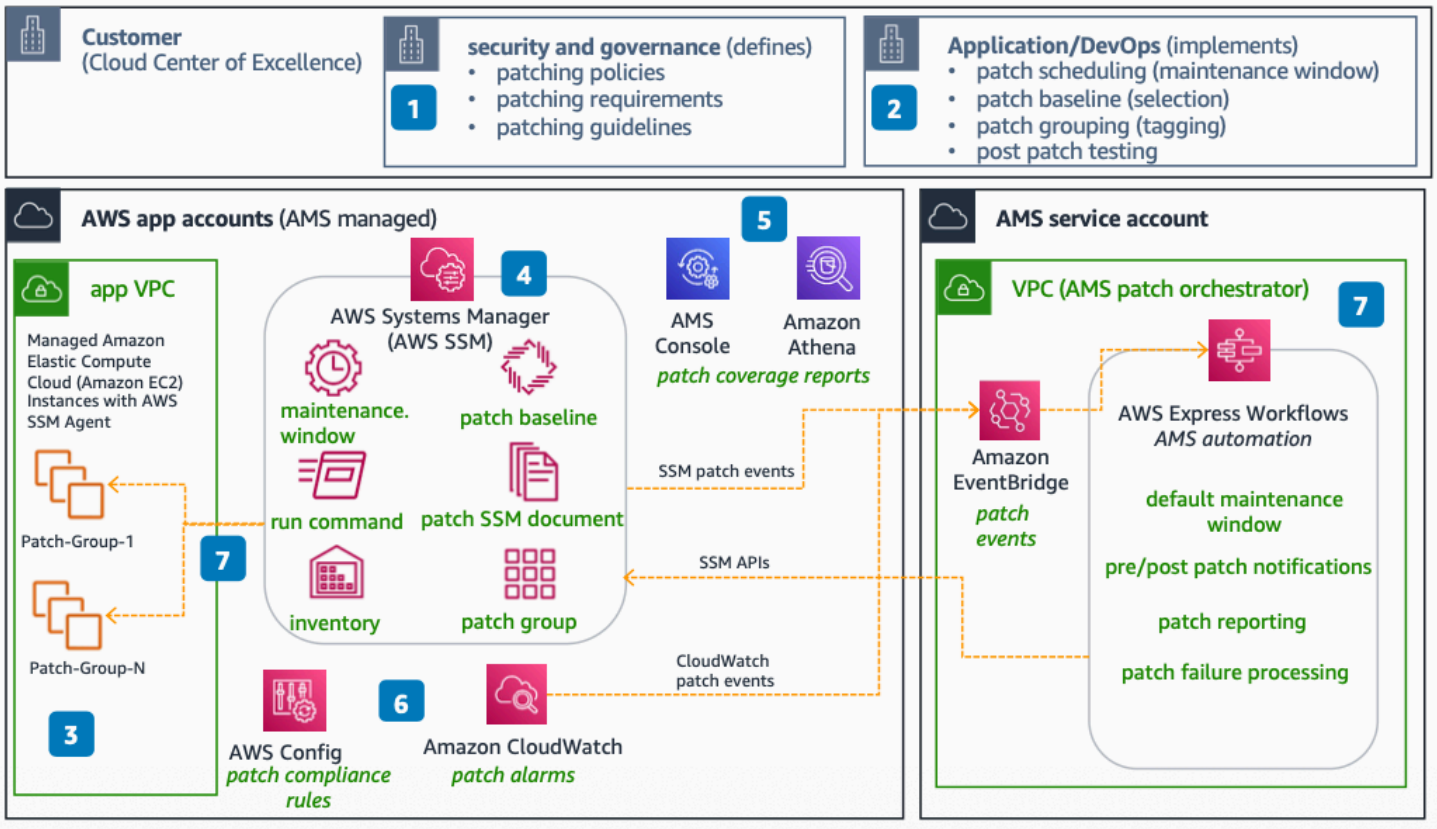
Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

AMS for Patching

Use this reference architecture to understand how AWS Managed Services (AMS) provides cross-account centralized patching. AMS takes complete ownership of OS patching, notifications, rollback, and reporting.

This reference architecture was validated by the AWS Managed Services team for technical accuracy on September 20, 2022.



The following steps describe the architecture:

1. The patching capability primarily falls under the security and governance teams. They define policies, provide guidelines, and requirements.
2. Your application and DevOps teams follow the guidelines to ensure regular patching at the application and OS levels. Your application teams are responsible for defining patch windows and post-patch application testing.
3. AMS sets up patch automation as part of AWS account onboarding. You define patch groups based on environment, tiers, and applications by using AWS Tags.

4. AMS uses AWS Systems Manager to perform OS patching. AMS works with you to set up patch baselines and patch maintenance windows by using AMS-provided Systems Manager automation documents (runbooks).
5. With AMS, you get daily patch coverage reporting based on account, groups, and patches. Reports are available to download through the AMS Console.
6. AMS implements patch alerting and monitoring by using rules and Amazon CloudWatch.
7. The AMS internal service account runs patch orchestration and automation. receives all patch-related events from Systems Manager. These events trigger pre-patch and post-patch notifications, pre-patch backup, OS patch updates, patch failure remediations, and patch inventory.

Deploy the architecture

AWS Managed Services deploys and manages this architecture on your behalf as part of the AMS operations plan. You do not need to deploy CloudFormation templates or write custom code. To get started with AMS, see the What is AWS Managed Services? section in the AMS User Guide.

For onboarding details and account setup, see AMS onboarding.

Further reading

For additional information, refer to the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected
- AWS Managed Services product page

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date

Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022

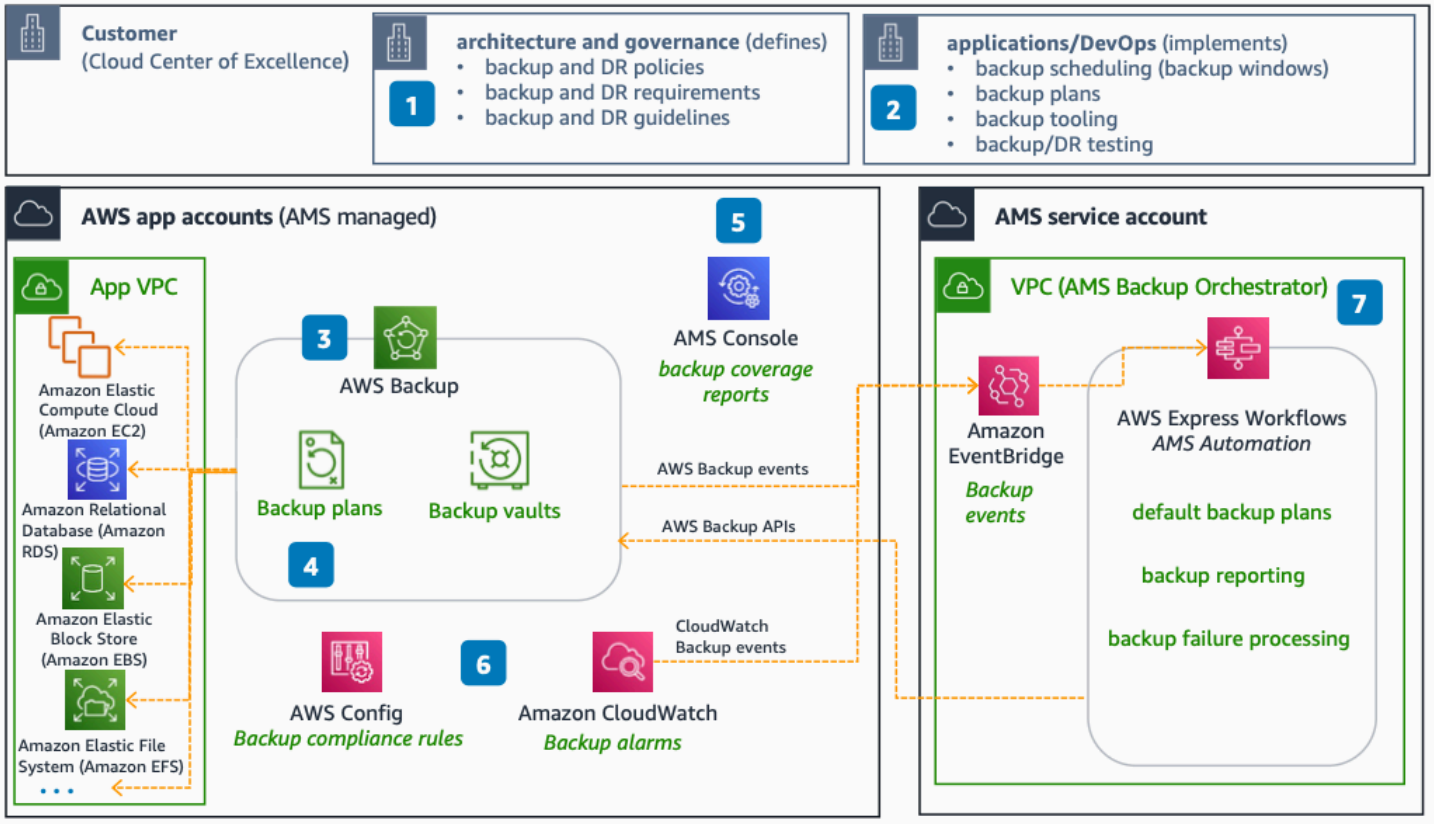
Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

AMS for Backup

Use this reference architecture to understand how AWS Managed Services (AMS) manages data availability and continuity. AMS takes complete ownership of backup monitoring, alerting, restoration, and reporting.

This reference architecture was validated by the AWS Managed Services team for technical accuracy on September 20, 2022.



The following steps describe the architecture:

1. The backup capability primarily falls under the architecture and governance teams. They define policies, provide guidelines, and requirements.
2. Your application and DevOps teams follow the guidelines and ensure regular backup at the application and OS levels. Your application teams are responsible for defining backup windows, backup plans, and disaster recovery (DR) testing.
3. AMS uses AWS Backup to perform backup and restore for all AWS services it supports. AMS sets up backup automation and vaults as part of AWS account onboarding.

4. AMS offers multiple backup plans to suit different needs. You set up custom backup plans or vaults based on environment, tier, recovery point objective (RPO), and applications by using AWS tags.
5. With AMS, you get daily backup coverage reporting based on account, plan, and resources. Backup reports are available to consume and export through the AMS Console.
6. AMS implements backup alerting and monitoring by using rules and Amazon CloudWatch.
7. The AMS internal service account runs backup orchestration and automation. receives all backup-related events to perform backup deployment, monitoring, alerting, reporting, and failure remediations.

Deploy the architecture

AWS Managed Services deploys and manages this architecture on your behalf as part of the AMS operations plan. You do not need to deploy CloudFormation templates or write custom code. To get started with AMS, see the What is AWS Managed Services? section in the AMS User Guide.

For onboarding details and account setup, see AMS onboarding.

Further reading

For additional information, refer to the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected
- AWS Managed Services product page

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagrams first published.	September 20, 2022

Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022
Initial publication	Reference architecture diagrams first published.	September 20, 2022

Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.