AMS Advanced User Guide

AMS Advanced Concepts and Procedures

Version November 11, 2021

AMS Advanced User Guide: AMS Advanced Concepts and Procedures

Table of Contents

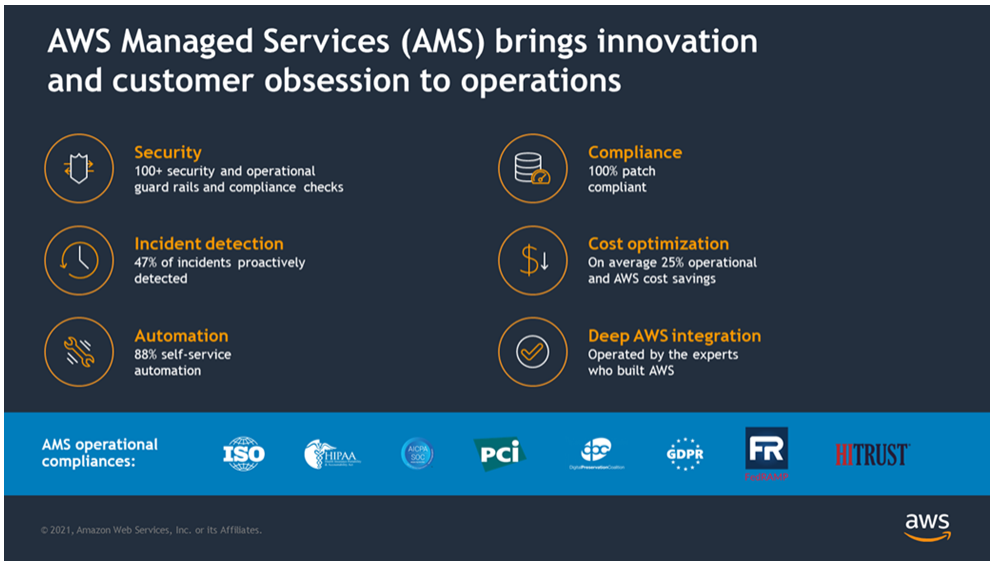
What is AWS Managed Services?

Topics

Welcome to AWS Managed Services (AMS), infrastructure operations management for Amazon Web Services (AWS). AMS is an enterprise service that provides ongoing management of your AWS infrastructure.

This user guide is intended for IT and application developer professionals. A basic understanding of IT functionality, networking, and application deployment terms and practices is assumed.

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.

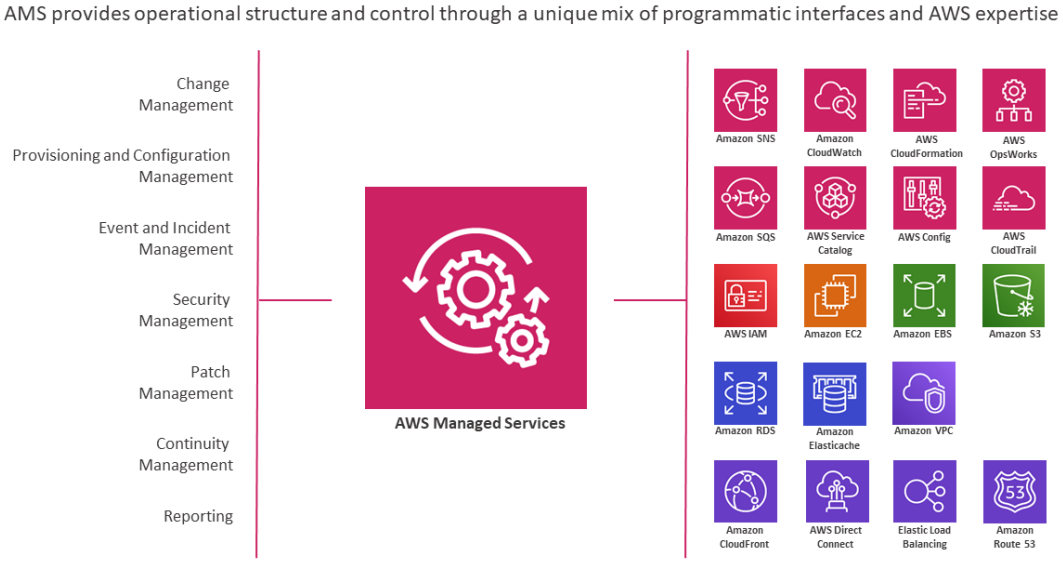


Note
New regions are added frequently. For the most recent AMS-supported AWS Regions, and the most recent AMS-supported operating systems, see Supported configurations (p. 15).

AMS seeks to continuously improve our services based on your feedback. We use several mechanisms to enable your self-service, to automate repetitive tasks, and to implement new AWS services and features as they are released. You can submit an AMS service request at any time to suggest new features or feature improvements.

AMS business hours are 24 hours a day, 7 days a week, 365 days a year.

AMS follows a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of your business.



About this guide

This user guide is intended for AMS Advanced customers with either a multi-account or single-account landing zone. Previously, AMS Advanced offered two separate user guides, one for each type of landing zone. The content was mostly the same, therefore, we have merged the content into one, consolidated user guide. You will notice that multi-account landing zone content is more prominent and single-account landing zone content is called out as different where needed. For more details about the AMS landing zone offerings, see the AMS Key Terms; also see Multi-Account Landing Zone architecture and Single-Account Landing Zone architecture.

Getting started

For details about getting started with the multi-account landing zone AMS service, see the AWS Managed Services Onboarding Introduction. The two onboarding guides provide descriptions of the service and questions to consider to help you get started. Review the feature set AWS Managed Services Features and current resources AWS Managed Services Resources.

AMS operations plans

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.

For a detailed feature comparison of the two operations plans, see AWS Managed Services Features.

AMS Accelerate operations plan

AMS Accelerate is the AMS operations plan that helps you operate the day-to-day infrastructure management of your new or existing AWS environment. AMS Accelerate provides operational services, such as monitoring, incident management, and security. AMS Accelerate also offers an optional patch add-on for EC2-based workloads that require regular patching.

With AMS Accelerate, you decide which AWS accounts you want AMS Accelerate to operate, the AWS Regions you want AMS Accelerate to operate in, the add-ons you require, and the service-level agreements (SLAs) you need. For more details, see Using the AMS Accelerate operations plan and Service Description.

AMS Advanced operations plan

AMS Advanced provides full-lifecycle services to provision, run, and support your infrastructure. In addition to the operational services provided by AMS Accelerate, AMS Advanced also includes additional services, such as landing zone management, infrastructure changes and provisioning, access management, and endpoint security.

AMS Advanced deploys a landing zone to which you migrate your AWS workloads and receive AMS operational services. Our managed multi-account landing zones are pre-configured with the infrastructure to facilitate authentication, security, networking, and logging.

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

AMS Advanced also offers different SLAs. For more information, see the AWS Managed Services AMS Advanced service description.

Key terms

- *AMS Advanced*: The services described in the "Service Description" section of the AMS Advanced Documentation. See Service Description.
- *AMS Advanced Accounts*: AWS accounts that at all times meet all requirements in the AMS Advanced Onboarding Requirements. For information on AMS Advanced benefits, case studies, and to contact a sales person, see AWS Managed Services.

- *AMS Accelerate Accounts*: AWS accounts that at all times meet all requirements in the AMS Accelerate Onboarding Requirements. See Getting Started with AMS Accelerate.
- *AWS Managed Services*: AMS and or AMS Accelerate.
- *AWS Managed Services Accounts*: the AMS Accounts and or AMS Accelerate Accounts.
- *Customer-Requested Configuration*: Any software, services or other configurations that are not identified in:
  - Accelerate: Supported Configurations or AMS Accelerate; Service Description.
  - AMS Advanced: Supported Configurations or AMS Advanced; Service Description.
- *Incident Communication*: AMS communicates an Incident to you or you request an Incident with AMS via an Incident created in Support Center for AMS Accelerate and in the AMS Console for AMS. The AMS Accelerate Console provides a summary of Incidents and Service Requests on the Dashboard and links to Support Center for details.
- *Managed Environment*: The AMS Advanced accounts and or the AMS Accelerate accounts operated by AMS.
- *Billing start date*: AWS Managed Services accounts are activated once you have granted access to AMS to a compatible account and AMS Activation notification occurs as defined in the AWS Managed Services Documentation. If the activation of the AWS Managed Services accounts, Add-on Service Request, or Account tier Service Request is received by AWS on or prior to the 20th day of the month, then the change will be effective as of the first day of the calendar month following the AMS Activation notification or such Service Request. If the activation or Service Request is received by AWS after the 20th day of the month, then the change will be effective as of the first day of the second calendar month following AMS Activation notification or such Service Request.

  AMS Activation Notification to the customer occurs when:

  1. Customer grants access to a compatible AWS account and hands it over to AWS Managed Services.
  2. AWS Managed Services designs and builds the AWS Managed Services Account.
- *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 via 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 creates 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 is that all components stay in a synchronous state since they are always generated from the same base. Immutability is independent of any tool or workflow for building the AMI.
- *Mutable infrastructure*: An infrastructure maintenance model typical for stacks that are not EC2 Auto Scaling groups and contain a single instance or just a few instances. This model most closely represents traditional, hardware-based, system deployment where a system is deployed at the beginning of its life cycle and then updates are layered onto that system over time. Any updates to the system are applied to the instances individually, and may incur system downtime (depending on the stack configuration) due to application or system restarts.
- *Security groups*: Virtual firewalls for your instance to control inbound and outbound traffic. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could have a different set of security groups assigned to it.
- *Service Level Agreements (SLAs)*: Part of AMS contracts with you that define the level of expected service.
- SLA *Unavailable* and *Unavailability*:
  - An API request submitted by you that results in an error .
  - A Console request submitted by you that results in a 5xx HTTP response (the server is incapable of performing the request).
  - Any of the AWS service offerings that constitute stacks or resources in your AMS-managed infrastructure are in a state of "Service Disruption" as shown in the Service Health Dashboard.

  - Unavailability resulting directly or indirectly from an AMS exclusion is not considered in determining eligibility for service credits. Services are considered available unless they meet the criteria for being unavailable.
- *Service Level Objectives (SLOs)*: Part of AMS contracts with you that define specific service goals for AMS services.

Patching terms:

- *Mandatory patches*: Critical security updates to address issues that could compromise the security state of your environment or account. A "Critical Security update" is a security update rated as "Critical" by the vendor of an AMS-supported operating system.
- *Patches announced versus released*: Patches are generally announced and released on a schedule. Emergent patches are announced when the need for the patch has been discovered and, usually soon after, the patch is released.
- *Patch add-on*: Tag-based patching for AMS instances that leverages AWS Systems Manager (SSM) functionality so you can tag instances and have those instances patched using a baseline and a window that you configure.
- *Patch methods*:
  - *In-place patching*: Patching that is done by changing existing instances.
  - *AMI replacement patching*: Patching that is done by changing the AMI reference parameter of an existing EC2 Auto Scaling group launch configuration.
- *Patch provider* (OS vendors, third party): Patches are provided by the vendor or governing body of the application.
- *Patch Types*:
  - *Critical Security Update (CSU)*: A security update rated as "Critical" by the vendor of a supported operating system.
  - *Important Update (IU)*: A security update rated as "Important" or a non-security update rated as "Critical" by the vendor of a supported operating system.
  - *Other Update (OU)*: An update by the vendor of a supported operating system that is not a CSU or an IU.
- *Supported patches*: AMS supports operating system level patches. Upgrades are released by the vendor to fix security vulnerabilities or other bugs or to improve performance. For a list of currently supported OSs, see Support Configurations.

Security terms:

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

Service Request terms:

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

Miscellaneous terms:

- *AWS Managed Services Interface*: For AMS: The AWS Managed Services Advanced Console, AMS CM API, and AWS Support API. For AMS Accelerate: The AWS Support Console 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.
- *Namespace*: When you create IAM policies or work with Amazon Resource Names (ARNs), you identify an AWS service by using a namespace. You use namespaces when identifying actions and resources.

Service description

Topics

AWS Managed Services (AMS) is a service for managing operations of your AWS infrastructure. AMS provides routine infrastructure operations such as patch, continuity management, security management, and IT management processes such as incident, change and service request management. For a list of supported services, see Supported AWS services (p. 25).

YouTube Video: What is AWS Managed Services and how can it benefit my business?

AMS features

AMS offers the following features for supported AWS services:

- **Logging, Monitoring, Guardrails, and Event Management**:

AMS configures and monitors your managed environment for logging activity and defines alerts based on a variety of health checks. Alerts are investigated by AMS for applicable AWS services, and those that negatively impact your usage of those services result in the creation of incidents. AMS aggregates and stores all logs generated as a result of all operations in CloudWatch, CloudTrail, and system logs in S3. Upon request, you can ask for additional alerts to be put in place. In addition to AMS' preventative controls, AMS deploys configuration guardrails and detective controls to provide ongoing protection for you from misconfigurations that could reduce the operational and security integrity of the managed accounts, to enforce your controls such as tagging and compliance. When a monitored control is detected an alarm is generated that results in notification, modification, or termination of resources based on pre-defined AMS defaults that can be modified by you.

- **Continuity management** (Backup and Restore):

  AMS provides backups of resources using standard, existing AWS Backup functionality on a scheduled interval determined by you. Restore actions from specific snapshots can be performed by AMS with your RFC. Data changes that occur between snapshot intervals are the responsibility of you to backup. You can submit an RFC for backup or snapshot requests outside of scheduled intervals. In the case of Availability Zone (AZ) unavailability in an AWS Region, with your permission, AMS restores the managed environment by recreating new stack(s) based on templates and available EBS snapshots of the impacted Stacks.

- **Security and access management**:

  AMS provides security management services such as configuring anti-virus and anti-malware protection. AMS also configures default AWS security capabilities that are approved by you during onboarding, such as identity access management (IAM) roles and EC2 security groups, and uses standard AWS tools (e.g. SecurityHub, Macie, GuardDuty) to monitor and respond to security issues. You manage your users through an approved directory service provided by you. For a list of approved directory services, see Supported configurations (p. 15).

  AMS includes endpoint security (EPS), which is inclusive of antivirus (AV), and anti-malware protection, malware and intrusion detection (Trend Micro). Security groups are defined per stack template and are modified at launch depending on the visibility of the application (public/private) security groups.

  Access to systems is requested through change management requests for change (RFCs). Access management provides access to distinct resources, such as Amazon EC2 instances, the AWS Management Console, and APIs. After establishing a one-way trust with an AMS Microsoft Active Directory deployment during onboarding and federating to AWS, you can use your existing corporate credentials for all interactions.

- **Patch management**:

  AMS applies and installs updates to EC2 instances for supported operating systems (OSs) and software pre-installed with supported operating systems. For a list of supported operating systems, see Supported configurations (p. 15).

  AMS offers two models for patching:

  - AMS standard patch for traditional account-based patching, and
  - AMS Patch Orchestrator, for tag-based patching.

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

  With AMS Patch Orchestrator, a default maintenance window per account, is defined by you for AMS to perform patching activities. You can schedule additional custom maintenance windows for AMS to

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

- **Change management**:

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

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

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

- **Automated and self-service provisioning management**:

  You can provision AWS resources on AMS in several ways:

  - Submit provisioning and configuration change types
  - Deploy AMS-provided security-hardened AMIs inclusive of your application
  - Deploy full stacks using CloudFormation templates
  - Deploy through your integrated IT service management (ITSM)
  - Deploy through AWS Service Catalog
  - Configure AWS services directly using self-service provisioning for select AWS services (see Supported AWS services (p. 25)).

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

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

- **Incident management**:

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

- **Problem management**:

  AMS performs trend analysis to identify and investigate problems and to identify the root cause. Problems are remediated either with a workaround or a permanent solution that prevents recurrence of similar future service impact. A post incident report (PIR) may be requested for any "High" incident, upon resolution. The PIR captures the root cause and preventative actions taken, including implementation of preventative measures.

- **Reporting**:

  AMS provides you with a monthly service report that summarizes key performance metrics of AMS, including an executive summary and insights, operational metrics, managed resources, AMS service level agreement (SLA) adherence, and financial metrics around spending, savings, and cost optimization. Reports are delivered by the AMS cloud service delivery manager (CSDM) assigned to you.

- **Service request management** :

  You can request information about your managed environment, AMS, or AWS service offerings by submitting service requests using the AMS interface. Service request types also include "How to" questions about AWS services and features, troubleshooting API issues, and technical support cases.

- **Service Desk** :

  AMS staffs engineering operations with full-time Amazon employees to fulfill non-automated requests including incident management, service request management, and change management. The Service Desk operates 24 x 7 365 days a year.

- **Designated resources**:

  Each customer is assigned a Cloud Service Delivery Manager (CSDM) and a Cloud Architect (CA).

  - CSDMs can be contacted directly. They perform service reviews, and delivery reporting and insights through all phases of the implementation, migration and operational life cycle. CSDMs conduct monthly business reviews and detail items such as financial spend, cost-saving recommendations, service utilization, and risk reporting. They dive deep into operational performance statistics and provide recommendations of areas of improvements.
  - CAs can be contacted directly and provide technical expertise to help you optimize your use of the AWS cloud. Example CA activities include, selecting workloads for migration, assisting with the onboarding additional accounts and workloads, acting as the technical lead in operational activities such as game days, disaster recovery testing, problem management, and technical advice to get the most out of AMS and AWS. CAs drive technical discussions at all levels of your organization and assist with incident management, making trade-offs, establishing best practices, and technical risk mitigation.

- **Developer mode** :

  This feature enables you to iterate infrastructure designs and deployments quickly within AMS-configured accounts[1] by allowing direct access to AWS service APIs and the AWS console in addition to access to the AMS change management process. Resources provisioned or configured with developer mode permissions outside of the change management process are your responsibility to manage (See "Automated and Self-Service Provisioning Management"). Resources provisioned through the AMS change management process are supported like other change management-provisioned workloads on AMS.

- **AWS support**:

AMS customers can choose the level of AWS Support they require to complement their AMS Operations plan. Accounts enrolled in AMS can be subscribed to either Business Support or Enterprise Support. To learn about the differences in Support Plans, see AWS Support Plans.

- **Customer-managed account**:

  This feature enables you to request AWS accounts within the same managed environment but the ongoing operations of workloads and AWS resources within those accounts are your responsibility. AMS provisions customer-managed accounts, but once the accounts are created, no other AMS features or services are provided to those accounts. AWS will not enroll customer-managed accounts in enterprise-level premium support. It will be your responsibility to enroll customer-managed accounts in AWS support at the support rate you choose.

- **Firewall management**:

  AMS provides an optional managed firewall solution for Supported Firewall Services, which enables internet-bound egress traffic filtering for networks in your managed environment. This excludes public-facing services that do not use the AWS network infrastructure and whose traffic goes directly to the internet. The solution combines industry-leading firewall technology with AMS infrastructure management capabilities to deploy, monitor, manage, scale, and restore the firewall infrastructure.

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

AMS environment basic components

MALZ

This is an estimate of the components, and potential costs, of the infrastructure in the core accounts. This does not include other costs such as bandwidth, CloudWatch detailed monitoring, logging, alarms, Route53, Amazon S3, Simple Notification Service (Amazon SNS), snapshots, or reserved Amazon EC2 instances.

You pay for the components required by the AMS-Managed AWS landing zone infrastructure. Estimates place the cost of a plain AMS multi-account landing zone environment at $2,450 per month and $50 for a plain application account.

For information about pricing, see AWS pricing.

Basic Environment Components

Component	Est. Cost	Description
Management account	$60	An AWS Organizations Management account; creates and financially manages member accounts. It contains the AWS Landing Zone (ALZ) framework, account configuration stack sets, and AWS Organization service control policies (SCPs). • Directory Service: $35 • CloudTrail: $7 • CloudWatch: $6 • Others: $12

Component	Est. Cost	Description
Shared Services Account	$2000	Contains infrastructure and resources required for access management (i.e., Active Directory), end-point security management (Trend Micro), and your bastions (SSH/RDP); estimate is $2400 a month. This estimate does not include the cost of the Trend Micro licenses. • EC2: $800 (with the minimum number of Bastions) • RDS: $300 (EPS) • VPC (endpoints): $400 • Directory Service: $300 • CloudWatch: $100 • GuardDuty : $15 • Secrets Manager: $10 • Data Transfer: $10 • Config: $10 • Others: $45
Networking Account	$350	The central hub for network routing between AMS accounts, your on-premise network, and egress traffic to the Internet. Additionally, contains public DMZ bastions (the entry point for AMS engineers to access hosts in your AMS environment). Price may increase depending on traffic traversing the Transit Gateway and Direct Connect. • EC2: 250 (Bastions) • VPC: 80 • Others: $20
Log Archive Account	$20	An S3 bucket with copies of AWS CloudTrail and AWS Config log files from each of your AMS environment accounts. Costs increase as more logs are collected. • S3: $10 • CloudWatch: $5 • Others: $5
Security Account	$20	The central hub for security related operations, and the main point for funneling notifications and alerts to AMS control plane services. Additionally, houses the Amazon Guard Duty management account. Costs increase as more events are analyzed using Amazon GuardDuty. • CloudWatch: $15 • Others: $5

SALZ

The following table lists the components of an example AMS-managed infrastructure.

Basic Environment Components, Last Updated 2020/07/09

Name	Instance Type	OS	# of Components	
mc-eps-dsm	m4.large	Linux	2	
mc-management	m4.large	Windows	2	
mc-bastion-dmz-ssh	m4.large	Linux	2	
mc-bastion-customer-rdp	m4.large	Windows	2	
mc-eps-relay	m4.large	Linux	2	
directory services	N/A	N/A		
additional components	N/A	N/A		

For information about pricing, see AWS Pricing.

AMS account limits

There are three distinct types of limits to consider within AMS multi-account landing zone: AMS API limits, AMS resource limits, and AWS limits.

There are two distinct types of limits to consider within AMS single-account landing zone: AMS API limits, and AWS limits.

AMS account API limits

This section describes the account level limits after which AMS throttles the API service. This means, if you call any of the listed APIs more than 10 times in a second, one of the calls is "throttled" (you receive a `ThrottleException`). Note that under rare situations, an external or downstream dependency might throttle the AMS API and then AMS may throttle your API calls at a possibly lower rate.

For each AMS SKMS API listed, the operation is throttled after 10 TPS (transactions per second):

- `GetStack`
- `GetSubnet`
- `GetVpc`
- `ListAmis`
- `ListStackSummaries`
- `ListSubnetSummaries`
- `ListVpcSummaries`

AMS multi-account landing zone account resource limits

Account resource limits relate to AMS multi-account landing zone application accounts and VPCs and subnets.

Application account resource limits

There is a soft limit of 50 application accounts per organization. If you have a use case for more than 50 application accounts, contact your cloud service delivery manager (CSDM) to relay your requirements.

VPCs and subnets resource limits

There is a soft limit of 10 VPCs per application account within the pre-defined AWS Region for the organization.

Each VPC may have 1 to 10 private subnet tiers spanned across 2 to 3 availability zones. Additionally, each VPC may have 0 to 5 public subnet tiers spanned across 2 to 3 availability zones. If you have requirements beyond these limits, inform your CSDM or Cloud Architect to review your use case.

AMS multi-account landing zone application to account ratio

One account per application is supported in AMS multi-account landing zone; however, each Application account has a small cost, and you are charged for the number of connections to the Transit Gateway per hour, and the amount of traffic that flows through AWS Transit Gateway. So, the more segregated applications are into accounts or VPCs, the higher the costs.

To reduce costs and still ensure an appropriate segregation of duties, AMS recommends that you 1) group applications by teams with tightly coupled business processes, and 2) do not mix applications that are in different stages (prod vs. non-prod) or managed by different teams. In this way, you will have fewer accounts, access management and the segregation of duties will be easier, and traffic cost could be mitigated.

For example: An enterprise has in production a Trading application and a Portfolio Management application, both applications are managed by the Investments IT team and exchange a lot of traffic with each other. In this scenario the company can benefit from grouping both applications in the same account and same the VPC, because the Investments IT team won't have to request access to multiple Application accounts and the company will save on traffic costs. In this case, the company should create another account for the same applications in development stage and provide access to the development team.

In another scenario, the enterprise has in production a Payroll application and an Accounting application, managed by the Human Resources IT and Accounting IT teams respectively. Although the Payroll application has to exchange information with the Accounting application, we recommend segregating both applications in different accounts, one per team, and establishing a connection between both application's VPCs using the Networking account. In this way, the company will prevent HR IT team request changes affecting the accounting application infrastructure, of which they would have no knowledge.

Tips on how to group accounts into organizational units (OUs). An OU is logical grouping mechanism that enables you to categorize (group) accounts and apply policies and configurations to based on those groups. The recommended approach for creating OUs is to base them on policies that need to be applied to a specific group of accounts, not on the internal hierarchy of teams within your reporting structure. An OU is not equivalent to an Active Directory's OU, and attempting to replicate the AD OU structure in AWS Orgs is discouraged and results in a difficult to maintain and/or operate structure.

AWS account limits

AWS account limits apply to your AMS accounts. The easiest method to determine default and current limits for AWS Services is by leveraging AWS Service Quotas. AMS recommends right-sizing individual service limits to the appropriate size to run the service(s) in the account. Limits act like guard-rails to protect your accounts for security and cost runaways. If you would like to raise a specific limit, submit a service request with AMS, and AMS Operations will raise the limit on your behalf. For example, the default limit (or quota) for RDS instances is 40; if your workload requires 50 RDS instances, raise a service request for AMS Operations to raise the limit to your needed value.

AMS service level objectives (SLOs)

The following table describes the goals of the AMS service. Service Level Agreements (SLAs) for other aspects of the AMS service, including incident management, are covered in the SLA document shared with you when you subscribed to AMS. For more information, speak to your CSDM.

AMS Service Level Objectives

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

Supported configurations

These are the configurations AMS supports:

- Language: AMS is available in English.
- Firewall Services: Palo Alto VM-Series Next-Generation Firewall
- Security software: Deep Security from Trend Micro (Required). AWS Marketplace: Trend Micro Deep Security
- Approved directory services: Microsoft Active Directory (AD)
- Supported AWS services (p. 25).
- 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)

New regions are added frequently. To learn more about AWS Regions and availability zones, see Regions and Zones.

- Supported AWS operating systems:
  - Amazon Linux 2 and Amazon Linux
  - CentOS 7.x, CentOS 6.5-6.10
  - Oracle Linux 7.5 and later minor versions
  - Red Hat Enterprise Linux (RHEL) 8.x, 7.x, 6.5-6.10
  - SUSE Linux Enterprise Server 15 SPx and SAP specific versions, SUSE Linux Enterprise Server 12 SP4 and later minor versions and SAP specific versions.
  - Microsoft Windows Server 2019, 2016, 2012 R2, 2012

    Note
    Operating systems (OSs) that are outside of the general support period of the operating system manufacturer ("end of support" (EOS)) have an increased security risk and are considered as supported configuration, only if 1) you have extended support with the OS vendor that allows you to receive updates, or 2) any instances using EOS OS follow the security controls as specified by AMS in the user guide, or 3) you comply with any other compensating security controls required by AMS.

AMS responsibility matrix (RACI)

Note
In order to fulfill its obligations in a timely manner, AMS may require inputs from you for deciding an appropriate course of action. AMS will contact the designated customer contact for all such clarifications and inputs. AMS will expect a response to such queries within 24 business hours. In case there is no reply within 24 business hours, AMS may choose an action on your behalf.

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

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

- **C** stands for consulted; a party whose opinions are sought, typically as subject matter experts; and with whom there is bilateral communication.
- **I** stands for informed; a party which is informed on progress, often only on completion of the task or deliverable.
- **Self-service Provisioning** refers to resources that are provisioned by the customer via self-service through the AWS API or Console including Developer Mode and Self-Service Provisioned Services.

Activity	Customer	AWS Managed Services
Application lifecycle		
Application development	R	I
Application infrastructure requirements analysis and design	R	C
Design and optimization for non-standard AMS stacks	R	C
Design and optimization of AMS standard stack	I	R
Application deployment	R	C
AWS Infrastructure deployment	C	R
Application monitoring	R	I
Application testing/optimization	R	I
AWS infrastructure optimization guidance	I	R
AWS infrastructure monitoring	I	R
Troubleshoot and resolve application issues	R	C
Troubleshoot and resolve AWS network issues	C	R
Troubleshoot and resolve operating system and infrastructure issues	C	R
Self-Service Provisioning	R	C
Application and ITSM Integration		
Application integration with AWS Service Offerings	R	C
ITSM integration with the AWS Managed Services Interface	R	C
Networking		
Managed Environment VPC and VPC set-up and configuration	C	R
Allocate private address space for VPCs (e.g. /16)	R	C
Configure & Operate non-AWS Managed Services, Customer managed Firewalls/Proxy/Bastions/ HOSTs	R	C

Activity	Customer	AWS Managed Services
Configure & Operate AWS Security Groups/NAT/ Customer Bastions/NACL inside the Managed Environment	I	R
Networking (e.g. DirectConnect) configuration and implementation within customer network	R	C
Networking configuration and implementation within the Managed Environment	C	R
Managed environment configuration		
Define default Auto Scaling settings for baseline Stack templates	I	R
Recommend RI optimization	C	R
Purchase RI and PIOP capacity	R	C
Remove capacity when capacity is over provisioned (when supported by customer application)	C	R
Create/update AWS customer specific information for AWS Managed Services	C	R
S3 configuration	C	R
Self-service provisioning	R	C
Glacier configuration	C	R
Define archival policy	R	C
Archival policy configuration	C	R
Selecting customer maintenance window	R	I
AWS RDS Management		
Monitor source/replica/RO replication health	I	R
Identify RCA of source failover	I	R
Automated snapshot (backup) configuration	C	R
Self-service provisioning	R	C
Coordinate and schedule DB engine patch management	C	R
Self-service provisioning	R	C
Recommend DB storage and PIOP capacity	C	R
Self-service provisioning	R	C
Recommend instance sizing for running databases	C	R
Self-service provisioning	R	C

Activity	Customer	AWS Managed Services
Recommend RI optimization for Managed Environment	C	R
Self-service provisioning	R	C
RDS performance monitoring (CloudWatch)	C	R
Self-service provisioning	R	C
RDS event subscription configuration (SNS)	C	R
Self-service provisioning	R	C
RDS security group configuration	C	R
Self-service provisioning	R	C
RDS engine parameter/option configuration	R	C
DB table design	R	I
DB indexing	R	I
DB log analysis	R	I
AMS Change Management		
Creating customer RFCs (e.g. access to resources creating/updating/deleting managed stacks, deploying/updating applications, changes to configuration of AWS Service Offerings)	R	I
Approving Customer RFCs	I	R
Creating AWS Managed Services RFCs (e.g. access to resources, creating resources on customer's behalf, applying updates to OS as part of Patch Management)	I	R
Approving non-automated RFCs	R	I
Submitting request for new Change Types	R	C
Creating new Change Types	I	R
Maintenance of application change calendar	R	C
Notice of upcoming Maintenance Window	I	R
AWS Service Catalog		
Create portfolios and products	R	I
Distribute products to end users	R	I
Create tags and tag option library	R	C
Sharing portfolios and products with end users	R	I
Revise / update portfolios and products	R	I

Activity	Customer	AWS Managed Services
Create and assign constraints to portfolios and products	R	C
Associate Service Actions to products	R	C
Update provisioned resources with new version of product	R	I
Provisioning		
Customer specific additions to AWS Managed Services baseline AMI	R	C
Configure additional approved Change Types used to provision Stack templates	C	R
Launch managed Stacks and associated AWS resources submitted through AMS change management process or AWS Service Catalog. *Self-service provisioning*	I	R
	R	I
Install/Update custom and 3rd party applications on Instances provisioned through AMS change management process or AWS Service Catalog.	R	I
Provisioning - Stack Architecture		
Providing OS licenses (including usage fees for the applicable AWS services – e.g. EC2 and RDS) *Self-service provisioning*	I	R
	R	I
Define baseline infrastructure templates (Stacks) for application deployment through AMS change management system. *Self-service provisioning*	I	R
	R	I
Creating baseline approved AMIs[8]	I	R
Evaluate customer application inventory and determine fit with available infrastructure templates (Stacks)	R	C
Define unique Stacks that are in addition to the baseline template offerings	R	C
Logging, Monitoring and Event Management		
Recording AWS infrastructure change logs	I	R
Recording all application change logs	R	C

Activity	Customer	AWS Managed Services
Installation and configuration of agents and scripts for patching, security, monitoring, etc. of AWS infrastructure provisioned through the AMS change management process. *Self-service provisioning*	I	R
	R	C
Define customer specific monitoring and incident requirements	R	C
Configuring alerts for Managed Environment	I	R
Monitoring all AMS configured alerts *Self-service provisioning*	I	R
	R	C
Investigating infrastructure Alerts for Incident notification *Self-service provisioning*	I	R
	R	C
Investigating application alarms	R	C
Incident Management		
Proactively notify Incidents on AWS infrastructure based on monitoring *Self-service provisioning*	I	R
	R	C
Handle application performance issues and outages	R	I
Categorize Incident priority	I	R
Provide Incident response	I	R
Provide Incident resolution / infrastructure restore **Note** SLAs do not apply to instance-based resources provisioned outside AMS change management, including those provisioned using self-service provisioning and developer mode.	C	R
Problem Management		
Identify Problems in Managed Environment	C	R
Perform RCA for Problems in Managed Environment	C	R
Remediation of Problems in Managed Environment	C	R
Identify and remediate application problems	R	I
Security Management		

Activity	Customer	AWS Managed Services
Customer infrastructure security and/or establishing baseline for security compliance process as determined and agreed to during customer onboarding.	C	R
Self-service provisioning	R	C
Maintaining valid licenses for Managed Security Software	R	C
Configure Managed Security Software	I	R
Self-service provisioning	R	C
Update Managed Security Software	I	R
Self-service provisioning	R	C
Monitoring malware on instances provisioned through the AMS CM process.	I	R
Self-service provisioning	R	C
Maintaining and updating virus signatures.	I	R
Self-service provisioning	R	C
Remediating instances infected with malware.	C	R
Self-service provisioning	R	C
Security event management	C	R
Security - Access Management		
Manage the lifecycle of users, and their permissions for local directory services, which are used to access AWS Managed Services	R	I
Operate federated authentication system(s) for customer access to AWS console/APIs	R	C
Accept and maintain Active Directory (AD) trust from AWS Managed Services AD to customer managed AD	R	C
During onboarding, create cross-account IAM Admin roles within each managed account	R	C
Secure the AWS root credential for each account	I	R
Define IAM resources for Managed Environment	C	R
Manage privileged credentials for OS access for AMS engineers	I	R
Manage privileged credentials for OS access provided to customer by AMS	R	I

Activity	Customer	AWS Managed Services
Patch Management[9]		
Monitor for applicable updates to supported OS and software preinstalled with supported OS for EC2 instances. *Self-service provisioning*	I	R
	R	C
Notify customer of upcoming updates (*applies to AMS Standard Patch only*)	I	R
Exclude certain updates and/or certain Stacks from patching activities	R	I
Define default and custom maintenance windows schedules and other parameters (e.g. maintenance window duration) to apply patches (*applies to AMS Patch* *Orchestrator only*)	R	I
Define custom Patch Baselines to filter and exclude specific patches (*applies to AMS Patch Orchestrator only*)	R	I
Tag instances to associate them with custom maintenance windows and Patch Baselines (*applies to AMS Patch Orchestrator only*)	R	I
Track the patch status of resources and highlight systems that aren't current in the monthly business review.	C	R
Apply updates to EC2 instances per Customer instructions. *Self-service provisioning*	I	R
	R	C
Patch development software (.NET, PHP, Perl, Python)	R	I
Patch, and monitor middleware applications (e.g. BizTalk, JBoss, WebSphere). *Self-service provisioning*	R	I
	C	I
Patch, and monitor custom and 3rd party applications *Self-service provisioning*	R	I
	C	I
Continuity Management		
Specify backup schedules	R	I
Execute backups per schedule. *Self-service provisioning*	I	R
	R	C

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

Activity	Customer	AWS Managed Services
Monitoring all AMS-Managed Firewall configured alerts	I	R
Execute Backups of firewall configuration	I	R
Request backup restoration activities	R	I
Update provisioned resources with new version of product	I	R
Recording AMS-Managed Firewall logs	I	R
Forward logs from AMS-Managed Firewall to CloudWatch	I	R
Request configuration changes in the AMS-Managed Firewall	R	I
Approve configuration changes in the AMS-Managed Firewall	I	R
Execute configuration changes in the AMS-Managed Firewall	I	R

[8]AMS provides AMIs for AWS EC2 only

[9]AMS is responsible for End of Life OSs only when the customer signs an extended support agreement with OS vendor

Supported AWS services

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

> **Note**
> In the following table, one star (*) indicates services that are deployed within an AMS managed environment by a customer using the AWS Console and APIs. See 'Automated and self-service provisioning management' in AMS features (p. 7) for additional details on customer responsibilities when provisioning and configuring services in this manner.
> Two stars (**) indicates that EC2 on AWS Outposts will be billed as a Group B service; all other resources hosted on AWS Outposts will be billed at their standard rate.

Supported AWS services

Group A	Group B	Group C
Amazon Alexa for Business* Amazon Managed Streaming for Apache Kafka* Amazon Simple Storage Service Amazon CloudFront Amazon Elastic File System Amazon Glacier	Amazon API Gateway* Amazon AppStream* Amazon Athena* Amazon CloudSearch* Amazon Cognito* Amazon Comprehend* Amazon Connect*	Amazon Aurora Amazon CloudWatch Amazon Elastic Block Store (EBS) Amazon Elastic Compute Cloud** Amazon Elastic Load Balancing (classic,

Group A	Group B	Group C
Amazon Simple Storage Service AWS Amplify* AWS AppMesh* AWS Auto Scaling AWS Backup AWS CloudFormation AWS Compute Optimizer AWS Global Accelerator* AWS Identity and Access Management AWS License Manager* AWS Management Console AWS Marketplace AWS Lake Formation* AWS Well Architected Tool* VM Import/ Export*	Amazon Document DB (with MongoDB compatibility)* Amazon DynamoDB* Amazon EC2 Container Registry (ECR)* Amazon ECS Fargate* Amazon Elastic Container Service for Kubernetes* Amazon EKS on AWS Fargate* Amazon Elemental MediaConvert* Amazon Elemental MediaPackage* Amazon Elemental MediaStore* Amazon Elemental MediaTailor* Amazon Elastic MapReduce* AmazonEventBridge* Amazon Forecast* Amazon FSx* Amazon Inspector* Amazon Kinesis Analytics* Amazon Kinesis Firehose* Amazon Kinesis* Amazon Kinesis Video Streams* Amazon Lex* AWS Migration Hub Amazon MQ* Amazon Personalize** Amazon QuickSight* Amazon Rekognition* Amazon SageMaker* Amazon SimpleDB* Amazon Simple Workflow* Amazon Textract* Amazon Transcribe* Amazon Translate* Amazon WorkDocs* Amazon WorkSpaces* AWS AppSync* AWS Audit Manager* AWS Batch* AWS Certificate Manager* AWS CloudEndure* AWS CloudHSM* AWS CodeBuild* AWS CodeCommit* AWS CodeDeploy* AWS CodePipeline* AWS DataSync* AWS Elemental MediaLive* AWS Glue* AWS Lambda* AWS MigrationHub* AWS Outposts** AWS Secrets Manager* AWS Security Hub* AWS Service Catalog AWS Transfer for SFTP* AWS Shield* AWS Snowball* AWS Step Functions*	application, and network; not gateway) Amazon ElastiCache Amazon OpenSearch Service Amazon GuardDuty Amazon Macie Amazon Redshift Amazon Relational Database Service Amazon Route 53 Amazon Simple Email Service Amazon Simple Notification Service Amazon Simple Queue Service Amazon Virtual Private Cloud (VPC) AWS CloudTrail AWS Config AWS Database Migration Service AWS Data Transfer AWS Direct Connect AWS Directory Service AWS Key Management Service AWS Systems Manager (SSM)

Group A	Group B	Group C
	AWS Transit Gateway* AWS WAF* AWS X-Ray*	

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

AMS multi-account landing zone service control policy restrictions

This section has been redacted because it contains sensitive AMS security-related information. This information is available through the AMS console **Documentation**. To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.

AMS protected namespaces

The list of protected namespaces for AMS. When you work with AWS resources, prevent conflict with AMS by not using these namespaces. For details on other AWS service namespaces, see Amazon Resource Names (ARNs) and AWS Service Namespaces.

- `ams-*` (this is the preferred naming standard for new resources)
- `AWSManagedServices*` (this is the preferred naming standard for resources where CamelCase is appropriate)
- `/ams/*` (this is the preferred naming standard for path-based resources)
- `ams*` and `AMS*` and `Ams*`
- `sentinel*` and `Sentinel*`
- `Managed_Services*`
- `NewAMS*`
- `AWS_*` and `aws*`
- `VPC_*`
- `CloudTrail*` and `Cloudtrail*`
- `*/aws_reserved/*`
- `INGEST*`
- `EPSDB*`
- `MMS*`
- `TemplateId*`
- `StackSet-ams*`
- `StackSet-AWS-Landing-Zone`
- `IAMPolicy*`
- `customer-mc-*`
- `Root*`
- `LandingZone*`
- `StateMachine*`

- `codedeploy_service_role`
- `managementhost`
- `sentinel.int.`
- `eps`
- `UnhealthyInServiceBastion`
- `ms-`

AMS maintenance window

The AWS Managed Services Maintenance Window (or Maintenance Window) performs maintenance activities for AWS Managed Services (AMS) and recurs the second Thursday of every month from 3 PM to 4 PM Pacific Time. AMS may change the maintenance window with 48 hours notice. This is for AMS to perform maintenance activities for managed infrastructures, such as deploying new AMS AMIs.

Your maintenance window is when AMS will apply patching and you determine your maintenance window at onboarding. You can also agree to the proposed patching window provided in your patching service notification, or suggest a different window.

For guidance on creating a maintenance window, see Maintenance Window.

What we do, what we do not do

AMS gives you a standardized approach to deploying AWS infrastructure and provides the necessary ongoing operational management. For a full description of roles, responsibilities, and supported services, see Service Description.

> **Note**
> To request that AMS provide an additional AWS service, file a service request. For more information, see Making Service Requests.

- **What we do**:

  After you complete onboarding, the AMS environment is available to receive requests for change (RFCs), incidents, and service requests. Your interaction with the AMS service revolves around the lifecycle of an application stack. New stacks are ordered from a preconfigured list of templates, launched into specific virtual private cloud (VPC) subnets, modified during their operational life through requests for change (RFCs), and monitored for events and incidents 24/7.

  Active application stacks are monitored and maintained by AMS, including patching, and require no further action for the life of the stack unless a change is required or the stack is decommissioned. Incidents detected by AMS that affect the health and function of the stack generate a notification and may or may not need your action to resolve or verify. How-to questions and other inquiries can be made by submitting a service request.

  Additionally, AMS allows you to enable compatible AWS services that are not managed by AMS. For information about AWS-AMS compatible services, see Self-service provisioning mode.

- **What we DON'T do**:

  While AMS simplifies application deployment by providing a number of manual and automated options, you're responsible for the development, testing, updating, and management of your application. AMS provides troubleshooting assistance for infrastructure issues that impact applications, but AMS can't access or validate your application configurations.

AMS Amazon Machine Images (AMIs)

AMS produces updated Amazon Machine Images (AMIs) every month for a variety of operating systems. The AMS AMIs are based on updated Amazon Machine Images that are modified for AMS.

To receive alerts when new AMS AMIs are released, you can subscribe to an Amazon Simple Notification Service (Amazon SNS) notification topic called "AMS AMI". For details, see AMS AMI notifications with SNS.

The AMS AMI naming convention is: `customer-ams-<operating system>-<release date> - <version>`. (for example, `customer-ams-rhel6-2018.11-3`)

Only use AMS AMIs that start with `customer`.

AMS recommends always using the most recent AMI. You can find the most recent AMIs by either:

- Looking in the AMS console, on the **AMIs** page.
- Viewing the latest AMS AMI CSV file, available from your CSDM or through the AMS Release Notes.
- Running this AMS `SKMS` command (AMS SKMS SDK required):

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?
 starts_with(Name,'customer')].[Name,AmiId,CreationTime]" --output table
```

AMS AMI content added to base AWS AMIs, by operating system (OS)

- Linux AMIs:
  - AWS CLI Tools
  - NTP
  - Trend Micro Endpoint Protection Service Agent
  - Code Deploy
  - PBIS / Beyond Trust AD Bridge
  - SSM Agent
  - Yum Upgrade for critical patches
  - AMS custom scripts / management software (controlling boot, AD join, monitoring, security, and logging)
- Windows Server AMIs:
  - Microsoft .NET Framework 4.5
  - PowerShell 5.1
  - AWS Tools for Windows PowerShell
  - AMS PowerShell Modules controlling boot, AD join, monitoring, security, and logging
  - Trend Micro Endpoint Protection Service Agent
  - SSM Agent
  - CloudWatch Agent
  - EC2Config service (through Windows Server 2012 R2)
  - EC2Launch (Windows Server 2016 and later)

Linux-based AMIs:

- Amazon Linux 2 (Latest Minor Release)
- Amazon Linux (Latest 2018.03 Release)

- Red Hat Enterprise 7 (Latest Minor Release)
- Red Hat Enterprise 8 (Latest Minor Release)
- SUSE Linux Enterprise Server 12 SP4
- SUSE Linux Enterprise Server 15 SP1
- CentOS 7 (Latest Minor Release)

  Note
  To use the CentOS AMIs, you must opt in to the no cost Cent OS license from the AWS Marketplace. To do this, go to AWS Marketplace and follow the instructions for opting in.

- Amazon Linux: For product overview, pricing information, usage information, and support information, see Amazon Linux AMI (HVM / 64-bit) and Amazon Linux 2.

  For more information, see Amazon Linux 2 FAQs.
- RedHat Enterprise Linux (RHEL): For product overview, pricing information, usage information, and support information, see Red Hat Enterprise Linux (RHEL) 7 (HVM).
- CentOS: To use the CentOS AMIs, you must opt in to the no cost Cent OS license from the AWS Marketplace. To do this, go to AWS Marketplace and follow the instructions for opting, or re-opting, in. You do not incur software charges for using this product, but you are responsible for other AWS charges, including EC2 usage.
- SUSE Linux Enterprise Server for SAP applications 15:
  - Run the following steps once per account:
    1. Navigate to the **AWS Marketplace**.
    2. Search for the respective SUSE 15 SAP product. We currently support:
       - SUSE Linux Enterprise Server for SAP Applications 15
       - SUSE Linux Enterprise Server for SAP Applications 15 SP1
    3. Click **Continue to subscribe**.
    4. Click **Accept terms**.
- Complete the following steps **every time** you need to launch a new **SUSE Linux Enterprise Server for SAP Applications 15** instance:
  1. Note the AMI ID for the subscribed **SUSE Linux Enterprise Server for SAP Applications 15** AMI.
  2. Create a manual (Management | Other | Other | Create) RFC with the following wording; replace *AMI ID* with the AWS Marketplace AMI ID you have subscribed to.

Windows-based AMIs:

Microsoft Windows Server (2012, 2012 R2, 2016, and 2019), based on latest Windows AMIs, (for example: Windows_Server-2012-R2_RTM-English-64Bit-Base-*).

Additional information: For product overview, pricing, usage, and support, see Microsoft Windows Server 2012 RTM.

For examples of creating AMIs, see Create AMI.

For details on the latest AMS AMIs, see the AMS Release Notes, Latest AMIs section.

Security enhanced AMIs

This section has been redacted because it contains sensitive AMS security-related information. This information is available through the AMS console **Documentation**. To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.

The security settings spreadsheets are available through your CSDM.

AMS information resources

AMS provides several information resources to help you succeed.

- AMS Release Notes: Lists the latest AMS service improvments for both AMS Accelerate and AMS. Also provides the AMI contents and CSV file for the latest AMS AMIs (once a month) and a list of new and updated change types. HTML index.
- AMS Accelerate User Guide: Helps you understand the components and features that AMS Accelerate provides and how to use them. Look here for AMS Accelerate background information and details on default settings, finding resources, and how-to examples. HTML index, PDF
- AMS Advanced User Guide: Helps you understand the components and features that AMS Advanced provides and how to use them. Look here for AMS Advanced background information and details on default settings, finding resources, and how-to examples. HTML index, PDF
- AMS Advanced Change Management User Guide: Helps you understand all aspects of requests for change (RFCs) and AMS change types (CTs). Look here for AMS Advanced change management information and and RFC how-to examples. HTML index, PDF
- AMS Advanced Application Guide: Describes the steps for deploying applications to AWS Managed Services infrastructure. Look here for information on application deployment and maintenance methodologies and considerations. HTML index, PDF.
- AMS Advanced Onboarding Guide: Describes the initial steps for creating the basic AWS Managed Services multi-account, or single-account, landing zone infrastructure in an AMS account. Look here for information on AMS account basics, validation, and questions to prepare you for onboarding to AMS. HTML index, PDF.
- Change Type Reference: Describes the change types that AWS Managed Services provides, including change type schemas. Look here for specifics on change types, including links to relevant information. HTML index, PDF.
- AMS CM (change management) API Reference: Describes the AWS Managed Services CM API, which provides operations for creating and monitoring change requests and provides information about your resources that are managed by Managed Services. HTML index, PDF.
- AMS SKMS (service knowledge management system) API Reference: Describes the AWS Managed Services SKMS API, which provides operations for requesting information about your resources that are managed by Managed Services.

  Private; available on the AMS **Reports** tab in the AWS Artifact Console.
- AMS Security Guides: Describe proprietary AMS security information.

  Private; available on the AMS **Reports** tab in the AWS Artifact Console.
- YouTube Videos: Key customer operations explained in video. See AWS Managed Services YouTube Instructional Videos.
- Blog posts: Specialty information on AWS Managed Services. See AWS Blogs.

AMS compliance

AMS has undergone auditing for the following standards and is eligible for use as part of solutions for which you must obtain compliance certification.

AMS Supported Compliance Standards

AMS supports AWS compliance standards. To learn more about AWS compliance programs, see AWS Compliance.

These are the current compliance standards supported by AMS.

	**FedRAMP**: The US Federal Government is dedicated to delivering its services to the American people in the most innovative, secure, and cost-efficient fashion. Cloud computing plays a key part in how the federal government can achieve operational efficiencies and innovate on demand to advance their mission across the nation. That is why many federal agencies today are using AWS cloud services to process, store, and transmit federal government data. For more information, see FedRAMP.
	**HIPAA**: AWS has expanded its Health Insurance Portability and Accountability Act (HIPAA) compliance program to include AMS as a HIPAA Eligible Service. If you have a Business Associate Agreement (BAA) with AWS, you can use AMS to help build your HIPAA-compliant applications. AWS offers a HIPAA-focused Whitepaper for customers who are interested in learning more about how they can leverage AMS for the processing and storage of health information. For more information, see HIPAA Compliance.
	**HITRUST**: The Health Information Trust Alliance Common Security Framework (HITRUST CSF) leverages nationally and internationally accepted standards and regulations such as GDPR, ISO, NIST, PCI, and HIPAA to create a comprehensive set of baseline security and privacy controls. For more information, see HITRUST CSF.
	**ISO 27001**: ISO/IEC 27001:2013 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO/IEC 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System (ISMS) which defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, see ISO/IEC 27001:2013.
	**ISO 27017**: ISO/IEC 27017:2015 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO/IEC 27002 and ISO/IEC 27001 standards. This code of practice provides additional information security controls implementation guidance specific to cloud service providers. For more information, see ISO/IEC 27017:2015 Compliance.
	**ISO 27018**: ISO/IEC 27018:2019 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO/IEC information security standard 27002 and provides implementation guidance on ISO/IEC 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO/IEC 27002 control set.

	For more information, see ISO/IEC 27018:2019 Compliance.
	ISO 9001: ISO 9001:2015 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. Specific sections of the standard contain information on topics such as: • Requirements for a quality management system, including documentation of a quality manual, document control, and determining process interactions • Responsibilities of management • Management of resources, including human resources and an organization's work environment • Service development, including the steps from design to delivery • Customer satisfaction • Measurement, analysis, and improvement of the QMS through activities like internal audits and corrective and preventive actions For more information, see ISO 9001:2015 Compliance.
	PCI: AMS has an Attestation of Compliance for Payment Card Industry (PCI) Data Security Standard (DSS) version 3.2 at Service Provider Level 1. Customers who use AWS products and services to store, process, or transmit cardholder data can use AMS as they manage their own PCI DSS compliance certification. For more information about PCI DSS, including how to request a copy of the AWS PCI Compliance Package, see PCI DSS Level 1. Importantly, you must configure fine-grained password policies in AMS to be consistent with PCI DSS version 3.2 standards. For details on which policies must be enforced, see Enable PCI Compliance for Your AWS Microsoft AD Directory.
	SOC: AMS System & Organization Control (SOC) Reports are independent, third-party examination reports that demonstrate how AMS achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the AMS controls established to support operations and compliance. There are three types of AMS SOC reports: • AWS SOC 1 Report - Download with AWS Artifact • AWS SOC 2: Security, Availability, & Confidentiality Report - Download with AWS Artifact • AWS SOC 3: Security, Availability, & Confidentiality Report For more information, see SOC Compliance.

Shared Responsibility

Security, including PCI compliance, is a shared responsibility. It is important to understand that AMS compliance status does not automatically apply to applications that you run in the AWS Cloud. You need to ensure that your use of AWS services complies with the standards. For more details on how

AMS works together with customers across specific activities, see the AMS AMS responsibility matrix (RACI) (p. 16).

AMS interfaces

There are six interfaces you can use to interact with AMS.

- *AMS Change management API* – Read/Write: Use the change management API (CM API) to request additions and specific changes to your managed infrastructure including resource monitoring, log, backup, and patch configurations. Also, use this API to request access to resources, delete resources, create AMIs, and create IAM instance profiles. You can access the CM API through the AMS CLI and SDKs.
- *AMS SKMS API* – Read-Only: Use this API to list managed resources and get information needed for reporting or preparing requests for change.
- *AMS Consoles*: AMS has a console for each of the operations plans: AMS Advanced and AMS Accelerate. Each are available through the AWS Management Console, once you have an account with that operations paln.

  You use the AMS Accelerate console to view summaries all your current incidents and service requests, and resource security status including compliance and real-time threat detection, and to quickly access configuration panels.

  You use the AMS console to create RFCs, report and respond to incidents, make service requests, and find information on existing VPCs and stacks. When in doubt of what to do, or when you need help with AMS or your managed resources, create a service request by using this interface.
- *AWS Support API*: Use the standard AWS Support API to programmatically create and respond to incidents and service requests. To learn more, see Getting Started with AWS Support.
- *AWS Management Console*: Many AWS consoles can be useful for viewing AMS information, for example:
  - *Amazon EC2 console*: Use to view instance information including bastion IP addresses, Amazon EC2 Auto Scaling groups, and load balancers.
  - *Multi-Account Landing Zone Config Rules compliance*: You can view compliance status across your accounts and identify non-compliant resources.
  - *AWS CloudFormation console*: Use to view stack information including stack IDs (you can find RDS stacks and RDS instance IDs here, and event information).
  - *RDS console*: Use to view event information such as a post made to a WordPress app on a site in your account. Note you must have the RDS instance ID.

  Depending on the mode of your login role, you have different level of access to the AWS Management Console. For more information on modes, see AMS modes.
- *AWS APIs* – Read Only: Your main IT administrator can use the AWS APIs to see all resources under management, view CloudTrail logs, billing information, and many other read functions.

AMS VPC endpoints

A VPC endpoint lets you privately connect your VPC to AWS services without requiring an Internet gateway. Instances in your VPC do not require public IP addresses to communicate with resources in the service.

Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic. To learn more, see VPC Endpoints.

There are two types of VPC endpoints: interface endpoints and gateway endpoints.

- Gateway endpoints: The VPC in the account has an S3 Gateway endpoint enabled by default.
- Interface endpoints: Instances in your AMS environment can talk to supported services without leaving the Amazon network. This is optional for **single-account landing zone** and it is not enabled in the account by default; submit a service request to AMS operations to get this enabled. However, for **multi-account landing zone**, interface endpoints are enabled by default in the shared services account.

  List of interface endpoints supported by AMS:

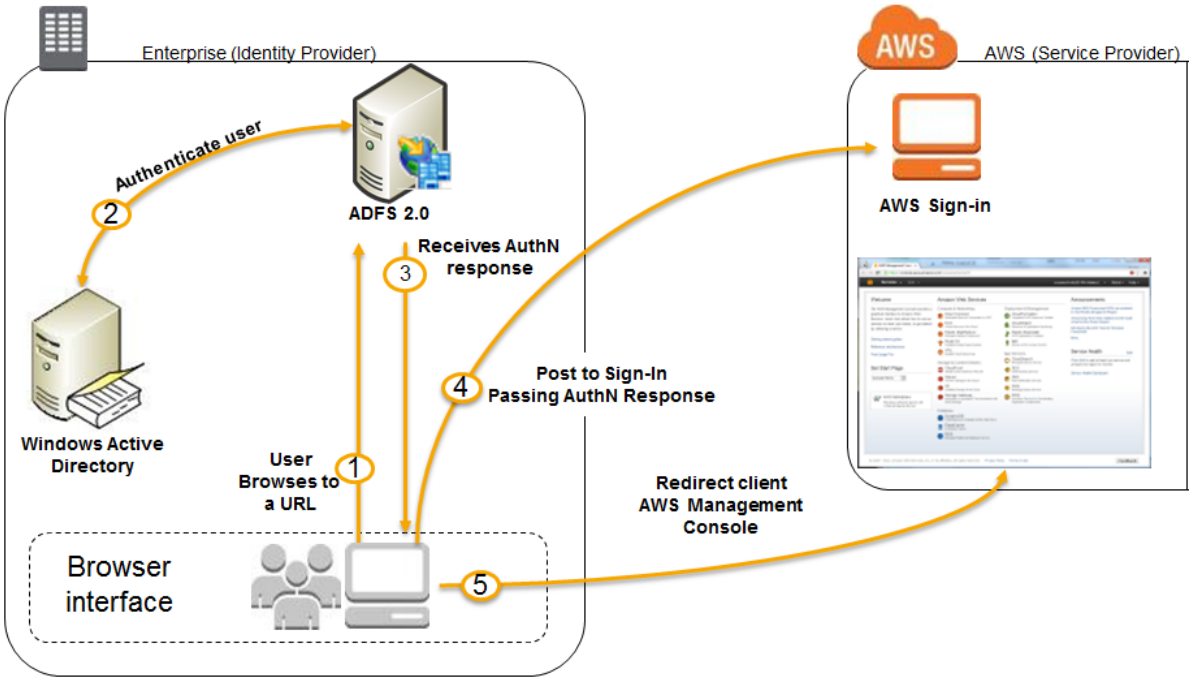
  - AWS CloudFormation
  - AWS CloudTrail
  - AWS Config
  - Amazon EC2 API
  - AWS Key Management Service
  - Amazon CloudWatch
  - Amazon CloudWatch Events
  - Amazon CloudWatch Logs
  - AWS Secrets Manager
  - Amazon SNS
  - AWS Systems Manager
  - AWS Security Token Service

How integration between AD FS and AMS works

A one-way trust between your on-premises network and the AMS domain is the default means for access to stacks and VPCs. When a VPC and stack are created, access is granted via pre-configured Active Directory security groups. In addition, access to the AWS Management Console can be configured using Active Directory Federation Service (AD FS), or any federation software that supports SAML, for a single sign-on (SSO) to the AWS Management Console.

> **Note**
> AMS can federate to many federation services, Ping, Okta, and so on. You aren't limited to AD FS. This section is an example of one federation technology available to you.

This section is duplicated from this blog post: Enabling Federation to AWS Using Windows Active Directory, AD FS, and SAML 2.0.



1. The flow is initiated when a user (let's call him Bob) browses to the AD FS sample site (https://Fully.Qualified.Domain.Name.Here/adfs/ls/IdpInitiatedSignOn.aspx) inside his domain. When you install AD FS, you get a new virtual directory named **adfs** for your default website, which includes this page.
2. The sign-on page authenticates Bob against AD. Depending on the browser Bob is using, he might be prompted for his AD username and password.
3. Bob's browser receives a SAML assertion in the form of an authentication response from AD FS.
4. Bob's browser posts the SAML assertion to the AWS sign-in endpoint for SAML (https://signin.aws.amazon.com/saml). Behind the scenes, sign-in uses the AssumeRoleWithSAML API to request temporary security credentials and then constructs a sign-in URL for the AWS Management Console.
5. Bob's browser receives the sign-in URL and is redirected to the console.

From Bob's perspective, the process happens transparently. He starts at an internal website and ends up at the AWS Management Console, without ever having to supply any AWS credentials.

> **Note**
> More information on configuring federation to the AMS console is provided in the AMS Onboarding Guide for Multi-Account Landing Zone or the AMS Onboarding Guide for Single-Account Landing Zone see Configuring Federation to the AMS Console or Configuring Federation to the AMS Console, respectively. Additionally, see Appendix: AD FS claim rule and SAML settings. For information about using AWS Microsoft AD to support your Active Directory–aware applications, in the AWS Cloud, that are subject to compliance requirements, see Manage Microsoft AD Compliance.

AMS Managed Active Directory

AMS is now offering a new service called Managed Active Directory (aka Managed AD) that allows AMS to take care of your Active Directory (AD) infrastructure operations, while keeping you in control of your Active Directory administration.

AMS support for Managed AD is similar to AMS support for the AWS Relational Database Service (RDS). In both cases, AWS (including AMS) supports the creation and management of the infrastructure running the service, while you perform access control and all administration functions. This model has the following advantages:

- Limits security risks: AWS and AMS don't need administrative privileges to your domain.
- Direct integrations: You can use your current authorization model and integrate it with AD without needing to interface with AMS.

Notes:

- Neither AMS nor you will have access to your Managed AD domain controllers, so no software can be installed on the domain controllers. This is important because third-party solutions that require software to be installed on domain controllers is not allowed.

  Access works like this:

  - AWS Directory Service team: Has access to domain controllers.
  - AMS: Has access to Directory Service APIs to perform certain actions on the domain. These actions include taking AD snapshots, changing AD schema, and others actions.
  - You: Have access to the domain (AD) for creating users, groups, and so on.
- We recommend that you perform a proof of concept on Managed AD before migrating your corporate AD, because not all functionality from a traditional AD environment is available in a Managed AD environment.
- AMS will not manage or provide guidance on your AD management. For example, AMS will not provide guidance on Organizational Unit structure, group policy structure, AD user naming conventions, and so forth.

It works like this:

1. AMS onboards a new AWS account for you, separate from and in addition to your AMS account, and provisions an Active Directory (AD) environment via AWS Directory Service (see also What Is AWS Directory Service?).

   The following is the information a systems integrator would need to gather from you in order for AMS to on board Managed AD:

   - Account information
     - Account ID of the AWS account that was created for your AMS-Managed AD: AWS account number
     - Region to onboard your Managed AD to: AWS Region
   - Managed Active Directory information:
     - Microsoft AD Edition: Standard/Enterprise. AWS Microsoft AD (Standard Edition) includes 1 GB of directory object storage. This capacity can support up to 5,000 users or 30,000 directory objects, including users, groups, and computers. AWS Microsoft AD (Enterprise Edition) includes 17 GB of directory object storage, which can support up to 100,000 users or 500,000 objects.

       For more information, see AWS Directory Service FAQs.
     - Domain FQDN: The FQDN for your AMS Managed AD domain.
     - Domain NetBIOS name: The NetBIOS name for your AMS Managed AD domain.
     - Account numbers of AMS-standard accounts you would like Managed AD integration to (AMS configures a one way trust from the AMS-standard account's AD to the Managed AD)
     - Are Active Directory Schema modifications required and if so, what modifications?
     - By default, two domain controllers are provisioned. Do you require more? If so, how many do you require and for what reason?

- Networking for Managed Active Directory information:
  - Managed AD VPC CIDR for domain controllers (a CIDR in your private subnet range for the Managed AD domain controllers):
    - Subnet CIDR 1 for domain controllers: [your CIDR, needs to be part of AMS Managed AD VPC CIDR]
    - Subnet CIDR 2 for domain controllers: [your CIDR, needs to be part of AMS Managed AD VPC CIDR]

    For example:
    - Managed AD VPC CIDR: 192.168.0.0/16
    - CIDR 1 for domain controllers: 192.168.1.0/24
    - CIDR 2 for domain controllers: 192.168.2.0/24

    To avoid IP address conflicts, be sure that the Managed AD VPC CIDR you specify does not conflict with any other private subnet CIDR you are using in your corporate network.
  - VPN Technology (optional): [Direct Connect/Direct Connect and VPN]
    - Your gateway's BGP Autonomous System Number (ASN): [Customer-provided ASN]
    - The Internet-routable IP address for your gateway's outside interface, the address must be static: [Customer Provided IP Address]
    - Whether or not your VPN connection requires static routes: [yes/no]

2. AMS provides you with the Admin account password for the AD environment and asks you to reset the password so AMS engineers can no longer access your AD environment.
3. To reset the Admin account password, connect to your Active Directory environment using Active Directory Users and Computers (ADUC). ADUC and other Remote Server Administration Tools (RSAT) should be installed and run on Administrative hosts provisioned by you on non-AMS infrastructure. Microsoft has best practices for securing such administrative hosts. For information, see Implementing Secure Administrative Hosts. You manage your Active Directory environment using these Administrative hosts.
4. In daily operations, AMS manages the AWS account up to the AWS Directory Service side of things; for example, VPC configuration, AD backups, AD trust creation and deletion, and so forth. You use, and manage, your AD environment; for example, user creation, group creation, group policy creation, and so forth.

For the most recent RACI table, see the "Roles and Responsibilities" section in the See the AMS FAQs appendix in the User Guide.

AMS application deployments

AMS Application Deployment Guide provides detailed descriptions and walkthroughs for the following deployments:

- The AMS workload ingest CT allows you and an AMS cloud migration partner to easily move your existing workloads into an AMS-managed VPC. Using AMS workload ingest, you can create an AMS AMI by submitting an RFC with the Deployment | Ingestion | Stack from migration partner migrated instance | Create CT (ct-257p9zjk14ija). You must have an instance migrated from your on-premises to AWS by a migration partner, as well as a target AMS VPC and subnet, into which the instance will be ingested.

  For details, see the AMS Application Guide at Workload Ingest.

- The AWS CloudFormation ingest change type (ct-36cn2avfrrj9v) feature allows you to easily use an existing CloudFormation template to deploy custom stacks in an AMS-managed VPC.

  For details, see the AMS Application Guide at CloudFormation Template Ingest.
- You can import your on-premises database into a new database to your AMS-managed Amazon S3 bucket or Amazon RDS instance. You do this using a Deployment | Advanced stack components | Database Migration Service (DMS) change types, including Create replication instance (ct-27apldkhqr0ol), Create replication subnet group (ct-2q5azjd8p1ag5), Create replication task (ct-1d2fml15b9eth), Create source endpoint (ct-0attesnjqy2cx) or Create source endpoint (S3) (ct-2oxl37nphsrjz), and Create target endpoint (ct-3gf8dolbo8x9p) or Create target endpoint (S3) (ct-05muqzievnxk5).

  For details, see the AMS Application Guide at Database Migration Service.
- You can import your on-premises MS SQL database into a new database on your AMS-managed RDS SQL instance. You do this using a variety of AMS change types, and the Amazon RDS API, plus AWS consoles.

  For details, see the AMS Application Guide at Database (DB) Import to MS SQL RDS.

AMS reserved prefixes

AMS resource attributes must comply with certain patterns; for example, IAM instance profile names, BackupVault names, tag names, and so forth, must not start with AMS reserved prefixes. Those reserved prefixes are:

```
ams-*
    AWSManagedServices*
    /ams/*
    ams*
    AMS*
    Ams*
    mc*
    MC*
    Mc*
    sentinel*
    Sentinel*
    Managed_Services*
    NewAMS*
    AWS_*
    aws*
    VPC_*
    CloudTrail*
    Cloudtrail*
    */aws_reserved/*
    INGEST*
    EPSDB*
    MMS*
    TemplateId*
    StackSet-ams*
    StackSet-AWS-Landing-Zone
    IAMPolicy*
    customer-mc-*
    Root*
    LandingZone*
    StateMachine*
    codedeploy_service_role
    managementhost
    sentinel.int.
    eps
```

```
UnhealthyInServiceBastion
ms-
```

AMS service management

Topics

How the AMS service works for you.

Account governance

This section covers AMS account 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.

Service commencement

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.

Service Commencement

- **R** stands for responsible party that does the work to achieve the task.
- **I** stands for informed; a party which is informed on progress, often only on completion of the task or deliverable.

Service commencement

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

AMS customer relationship management (CRM)

The purpose of AMS's customer relationship management (CRM) process is to ensure that a well-defined relationship is established and maintained with you. The foundation of this relationship is based on AMS's insight into your business requirements. The CRM process facilitates accurate and comprehensive understanding of:

- Your business needs and how to fill those needs
- Your capabilities and constraints
- AMS and your different responsibilities and obligations

The CRM process allows AMS to use consistent methods to deliver services to you and provide governance for your relationship with AMS. The CRM process includes:

- Identifying your key stakeholders
- Establishing a governance team
- Conducting and documenting service review meetings with you
- Providing a formal service complaint procedure with an escalation procedure
- Implementing and monitoring your satisfaction and feedback process
- Managing your contract

CRM Process

The CRM process includes these activities:

- Identifying and understanding your business processes and needs. Your agreement with AMS identifies your stakeholders.
- Defining the services to be provided to meet your needs and requirements.
- Meeting with you in the service review meetings to discuss any changes in the AMS service scope, SLA, contract, and your business needs. Interim meetings may be held with you to discuss performance, achievements, issues, and action plans.

- Monitoring your satisfaction by using our customer satisfaction survey and feedback given at meetings.
- Reporting performance on monthly internally-measured performance reports.
- Reviewing the service with you to determine opportunities for improvements. This includes frequent communication with you regarding the level and quality of the AMS service provided.

CRM meetings

AMS cloud service delivery managers (CSDMs) conduct meetings with you regularly to discuss service tracks (operations, security, and product innovations) and executive tracks (SLA reports, satisfaction measures, and changes in your business needs).

Meeting	Purpose	Mode	Participants
Weekly status review (optional)	Outstanding issues or incidents, patching, security events, problem records 12-week operational trend (+/- 6) Application operator concerns Weekend schedule	On-site customer location/Telecom/ Chime	AMS: CSDM and cloud architect (CA) Customer assigned team members (ex: Cloud/ Infrastructure, Application Support, Architecture teams, etc.)
Monthly business review	Review service level performance (reports, analysis, and trends) Financial analysis Product roadmap CSAT	On-site customer location/Telecom/ Chime	AMS: CSDM, cloud architect (CA), AMS account team, AMS technical product manager (TPM) (optional), AMS OPS manager (optional) You: Application Operator representative
Quarterly business review	Scorecard and service level agreement (SLA) performance and trends (6 months) Upcoming 3/6/9/12 months plans/ migrations Risk and risk mitigations Key improvement initiatives Product roadmap items Future direction aligned opportunities	On-site customer location	AMS: CSDM, cloud architect, AMS account team, AMS service director, AMS operation manager You: Application operator representative, service representative, service director

Meeting	Purpose	Mode	Participants
	Financials Cost savings initiatives Business optimization		

CRM Meeting Arrangements

The AMS CSDM is responsible for documenting the meeting, including:

- Creating the agenda, including action items, issues, and list of attendees.
- Creating the list of action items reviewed at each meeting to ensure items are completed and resolved on schedule.
- Distributing meeting minutes and the action item list to meeting attendees by email within one business day after the meeting.
- Storing meeting minutes in the appropriate document repository.

In absence of the CSDM, the AMS representative leading the meeting creates and distributes minutes.

Note
Your CSDM works with you to establish your account governance.

CRM monthly reports

Your AMS CSDM prepares and sends out monthly service performance presentations. The presentations include information on the following:

- Report date
- Summary and Insights:
  - Key Call Outs: total and active stack count, stack patching status, account onboarding status (during onboarding only), customer-specific issues summaries
  - Performance: Stats on incident resolution, alerts, patching, requests for change (RFCs), service requests, and console and API availability
  - Issues, challenges, concerns, and risks: Customer-specific issues status
  - Upcoming items: Customer-specific onboarding or incident resolution plans
- Managed Resources: Graphs and pie charts of stacks
- AMS Metrics: Monitoring and event metrics, incident metrics, AMS SLA adherence metrics, service request metrics, change management metrics, storage metrics, continuity metrics, Trusted Advisor metrics, and cost summaries (presented several ways). Feature requests. Contact information.

Note
In addition to the described information, your CSDM also informs you of any material change in scope or terms, including use of subcontractors by AMS for operational activities.
AMS generates reports about patching and backup that your CSDM includes in your monthly report. As part of the report generating system, AMS adds some infrastructure to your account that is not accessible to you:

- An S3 Bucket, with the raw data reported
- An Athena instance, with query definitions to query the data

- A Glue Crawler to read the raw data from the S3 bucket

Updates to shared services: Multi-Account Landing Zone

AMS uses the core OU to provide shared services such as access, networking, EPS, log storage, alert aggregation in your Multi-Account Landing Zone. AMS is responsible for addressing vulnerabilities, patching, and deployments of these shared services. AMS regularly updates the resources used for providing these shared services so that users have access to latest features, and security updates. The updates typically happen on a monthly basis. Resources that are part of these updates are:

- Accounts that are part of the core OU.

  The management account, shared services account, network account, security account, and log archive account have resources for RDP and SSH bastions, proxies, management hosts, and endpoint security (EPS), that are typically updated every month. AMS uses immutable EC2 deployments as part of the shared services infrastructure.
- New AMS AMIs incorporating the latest updates.

  Note
  AMS operators utilize an internal alarm suppression change type (CT) when executing data plane changes and the RFC for that CT appears in your RFC list. This is because, as the data plane release is deployed, various infrastructure may be shut down, rebooted, taken offline, or there may be CPU spikes or other effects of the deployment that trigger alarms that, during the data plane deployment, are extraneous. Once the deployment is complete, all infrastructure is verified to be running properly and alarms are re-enabled.

AMS planned event management

AWS Managed Services (AMS) planned event management (PEM) is an AMS service offering. PEM is used to engage, plan, and run customer events and projects using AMS Change Management Services and dedicated AMS resources. Change management delivers an individual request for change (RFC). The PEM delivers a set of related RFCs that align with the scope and timeline of the PEM event or project.

AMS PEM criteria

A planned event is defined as a scope-bound and time-bound project. For example, migrations, game days, disaster recovery tests, projects, or events that require dedicated on-site or off-site AMS resources such as Operation Engineers or Cloud Architects.

The AMS PEM process

The PEM process consists of the following phases:

- **Initiation —**: You engage with the Cloud Service Deliver Managers (CSDM), Technical Delivery Managers (TDM), and Cloud Architects (CA) to provide project information and the technical details to AMS. AMS works with you to ensure that the PEM plan information is correct and complete. For PEM acceptance, AMS Operations requires a lead time of 2 weeks to allow the AMS Operations appropriate time to ensure planning, technical review and resource assignment. Additional time may be required for delivery of pre-PEM tasks.

- **Technical Review —**: AMS Cloud Architects review the technical aspects of the PEM plan. They work with AMS Security and Operations to ensure compliance, provide execution optimization and automation, and define pre-PEM execution tasks and deliverables.
- **Planning —**: AMS ensures that the necessary AMS resources are assigned.
- **Readiness and Execution —**: AMS ensures pre-execution tasks are completed, and facilitates internal and customer communications. AMS also ensures execution of the PEM plan and provides execution status and progress reporting.

Getting help

You can reach out to AMS to identify the root cause of your failure. AMS business hours are 24 hours a day, 7 days a week, 365 days a year.

AMS provides several avenues for you to ask for help or make service requests.

- To ask for information or advice, or for access to an AMS-managed IT service, or to request an additional service from AMS, 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.
- To report an AWS or AMS service performance issue that impacts your managed environment, use the AMS console and submit an incident report. For details, see Reporting an incident. For general information about AMS incident management, see Incident response.
- 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:
  1. First, if you are unsatisfied with the service request or incident report response, email your CSDM: ams-csdm@amazon.com
  2. Next, if escalation is required, you can email the AMS Operations Manager (your CSDM will most likely do this): ams-opsmanager@amazon.com
  3. Further escalation would be to the AMS Director: ams-director@amazon.com
  4. Finally, you are always able to reach the AMS VP: ams-vp@amazon.com

Customer contacts with AMS that require escalation will follow the escalation path described next.

Service hours

Feature	AMS Accelerate		AMS Advanced	
Service request	Monday to Friday: 08:00–18:00, local business hours	24/7	Monday to Friday: 08:00–18:00, local business hours	24/7
Incident management (P1)	24/7			
Incident management (P2-P3)	Monday to Friday: 08:00–18:00, local business hours	24/7	Monday to Friday: 08:00–18:00, local business hours	24/7
Backup and recovery	24/7			

Feature	AMS Accelerate	AMS Advanced	
Patch management	24/7		
Monitoring and alerting	24/7		
Automated request for change (RFC)	Not Applicable	24/7	
Non-automated request for change (RFC)	Not Applicable	Monday to Friday: 08:00–18:00, local business hours	24/7
Cloud service delivery manager (CSDM)	Monday to Friday: 08:00–17:00, local business hours		

How do I get offboard assistance from AMS Single-Account Landing Zone accounts?

AMS offers off-boarding assistance within 30 days prior to termination of AMS.

You must request off-boarding assistance at least 7 days before such assistance can be provided. Off-boarding assistance can be offered in two forms:

- Control hand-over: AMS will transfer account control back to the Customer along with access credentials for all AMS Managed Applications, or
- Resource termination and data transfer: AMS backs-up all the data, deletes all the data in customer's Managed Environment, de-provisions any active resources in the account, and hands over the data backup to the Customer. At customer's request AMS can transfer customer data in the existing format using Snowball or any other media with which AWS can interface. In addition to data backups, the following customer data can be provided as part of off-boarding assistance:
  - Data stored in storage services including logs
  - Customer-specific Change type schemas
  - CloudFormation templates for Change type schemas.

If off-boarding activities are not completed upon the termination of AMS, we hand over the controls of the account(s) to enable you to complete any pending activity.

How do I offboard from AMS Multi-Account Landing Zone accounts?

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

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

How do I offboard a Multi-Account Landing Zone environment?

Scenario:

You want to leave AMS, and close (terminate) your AMS AWS account completely (including the primary account that you provided).

Process:

1. You communicate with your CSDMs or CAs and request offboarding via email or a service request.
2. AMS works on offboarding your accounts.
3. Your CSDM or CA sends you an outbound email containing further instructions; see How do I close my AWS account?

Prerequisites: Verify that you can access the account email used for account closures.

Offboarding Conclusions:

- All components are disassociated from the AMS services, but are not yet deleted in all accounts. Account closure will eventually delete all resources.
- Billing is *not stopped* until you request the account closures.
- After the account is closed, you can still sign in and file a support case or contact AWS Support for 90 days.
- After 90 days, any content remaining in the account is permanently deleted, and AWS services that aren't already terminated, are terminated.

How do I offboard a Multi-Account Landing Zone application account?

Some offboarding scenarios.

Scenario:

You want to offboard one, or more than one, application accounts from your multi-account landing zone environment, close (terminate) those accounts completely.

Process:

1. You communicate with your CSDMs or CAs to request offboarding via email or a service request.
2. AMS works on offboarding your accounts from AMS.
3. Your CSDM or CA sends you an outbound email containing further instructions; see How do I close my AWS account?

Prerequisites: Verify that you can access the account email used for account closures.

Offboarding Conclusions:

- All components are disassociated from AMS services, and most of the resources are deleted in the requested accounts. Your resources remain in the account until you request account closure.
- Core accounts and other application accounts function normally after the offboarding request.

- Billing is *not stopped* until you request account closures.
- After the account is closed, you can still sign in and file a support case or contact AWS Support for 90 days.
- After 90 days, any content remaining in the account is permanently deleted, and AWS services that aren't already terminated, are terminated.

How do I offboard a Multi-Account Landing Zone application account VPC?

Scenario:

You want to offboard one of your VPCs from an AMS-managed application account.

Process:

1. You communicate with your CSDMs or CAs via email or a service request, to request VPC offboarding.
2. AMS works on offboarding the VPC from AMS.
3. Your CSDM and CA notify you of the completion of the offboarding.

Prerequisites:

- Verify there are *no running instance stacks* associated with this offboarding VPC.

  If there are running instance stacks associated with the offboarding VPC, you are responsible for deleting those instance stacks prior to requesting a VPC offboarding.
- Your application account should always contain at least one VPC. If you request a VPC offboarding and that VPC is the only VPC in the account, follow up with an application VPC create RFC.
- Verification email to confirm the request. Your request should contain the VPC name of the VPC that you want to delete, and the account ID that the VPC is associated with.

Offboarding Conclusions:

Application accounts function normally after VPC offboarding request.

Multi-Account Landing Zone network architecture

About Multi-Account Landing Zone network architecture

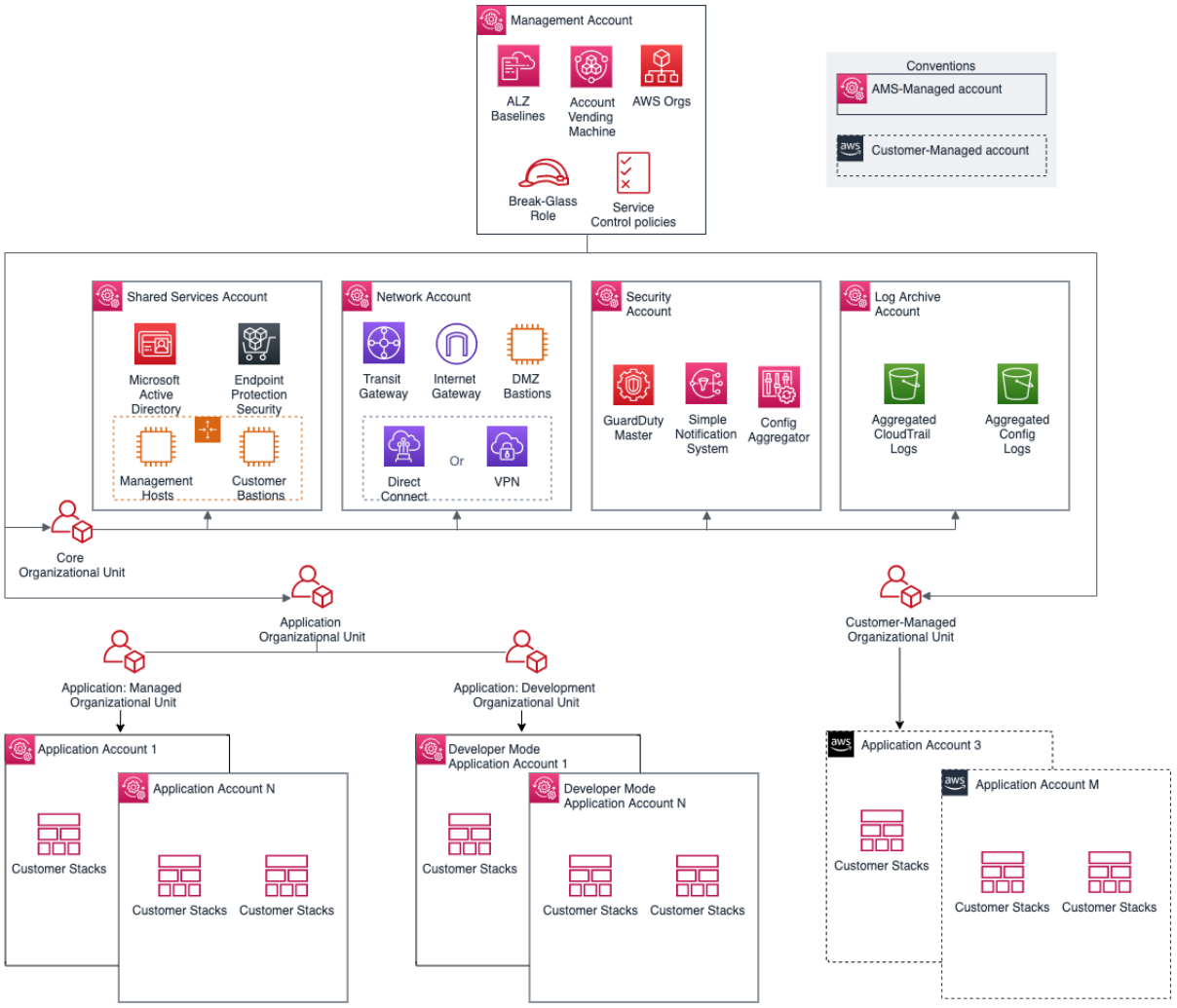
Topics

Before starting the onboarding process, it is important to understand the baseline architecture, or landing zone, that AMS creates on your behalf, its components, and functions.

AMS multi-account landing zone is a multi-account architecture, pre-configured with the infrastructure to facilitate authentication, security, networking, and logging.

> **Note**
> For estimates of costs, see AMS Multi-Account Landing Zone environment basic components.

The following diagram outlines at a high level the account structure and how infrastructure is segregated into each of the accounts:



Service region

All resources within an AMS multi-account landing zone are deployed within a single AWS Region of your choice, due to current cross region limitation with Active Directory and Transit Gateway.

Organizational units

A typical AMS multi-account landing zone consists of three top-level organizational units (OUs):

- The core Organizational unit (OU) (used to group accounts together to administer as a single unit)
- The applications OU
- The customer managed OU

AMS-managed multi-account landing zone also enables you to create custom OUs for grouping and organizing AWS Accounts and to associate custom SCPs with them; for examples on doing this, see Management account: Creating a custom OU and Management account: Creating a custom SCP, respectively. AMS provides three existing OUs under which new OUs and accounts can be requested: application > managed, application > development, and customer managed.

- Application > managed OU:

  In this sub organizational unit of the Application OU, accounts are fully managed by AMS including all operational tasks. The operational tasks include service request management, incident management, security management, continuity management, patch management, cost optimization, monitoring and event management. These tasks are carried out for your infrastructure's management. Multiple child OUs can be created as needed, until a maximum limit of nested OUs is reached for AWS organizations. For details, see Quotas for AWS Organizations.
- Application > development OU:

  Under this sub-OU of the application OU in AMS-managed landing zone, accounts are Developer mode accounts that provide you with elevated permissions to provision and update AWS resources outside of the AMS change management process. This OU also supports the creation of new children OU as needed.
- Customer Managed OU:

  This is a top-level OU in AMS multi-account landing zone. Accounts under this OU are provisioned by AMS with an RFC. In these accounts, the operations of workloads and AWS resources are your responsibility. This OU also supports the creation of new children OU as needed.

As a best practice, we recommend that accounts under these OUs and custom-requested sub-OUs be grouped based on their functionalities and policies.

Service control policies and AWS Organization

AWS provides service control policies (SCPs) for permissions management in an AWS Organization. SCPs are used to define additional guardrails for what actions users can perform in which OUs. By default, AMS provides a set of SCPs deployed in management accounts which provide protections at different default OU levels. For SCP restrictions, please contact your CSDM.

You can also create custom SCPs and attach them to specific OUs. They can be requested from your Management account using change type ct-33ste5yc7hprs. AMS then reviews the custom SCPs requested before applying them to the target OUs. For examples, see Management account: Creating a custom OU and Management account: Creating a custom SCP.

Single multi-account landing zone or multiple multi-account landing zone

The following table provides some high level considerations on deciding between a single multi-account landing zone (MALZ) vs multiple multi-account landing zones (for example, two multi-account landing zones - Prod and non-Prod). In general, the choice depends upon individual needs, legal requirements, and operating practices.

Single multi-account landing zone vs. multiple multi-account landing zones

Entity	Single AMS landing zone	Multiple (two or more) landing zones
Base cost	Lower, optimized at approximately $3,000 per month.	Higher, an additional cost of approximately $3,000 per environment.
Billing	Single bill, due to single Billing/ Management account.	Separate bill for each multi-account landing zone. Currently AWS Org does not support multi-Management accounts with a single bill.

Entity	Single AMS landing zone	Multiple (two or more) landing zones
Portability of existing reserved instances (RIs)	Low. AWS RIs are currently not convertible across multiple billing accounts. You would repurpose existing RIs for multi-account landing zone.	Lower. You would repurpose and distribute RIs across all multi-account landing zone.
Product tiering discounts	High. See Volume discounts.	Low. See Volume discounts.
Initial setup overhead (on project/ migration timelines)	Low. Active Directory, networking and single sign-on (SSO) integrations once only.	High. You would perform Active Directory, network integration, and SSO integrations for every landing zone. This could cause potential delays to any migration project.
Common services configurability	Low efforts. You configure common/ shared services like DNS, backup, monitoring, logging etc.	High efforts. Additional planning is required to address where the common infrastructure or services will be sitting. Traffic traversing across multiple transit gateways (TGWs) in each landing zone, could lead to extra cost.
Scalability	Medium. AMS has a current practical limit of 150 accounts per multi-account landing zone. Multiple teams or vendors running applications in same account could have access to stacks owned by different teams. This limitation can be mitigated by controlling access to application-specific stacks at the ServiceNow layer (by integrating the AMS ServiceNow Connector application and making use of tags). Ask AMS technical delivery managers (TDMs) or cloud architects (CAs) how to implement this.	High. Ability to leverage multiple multi-account landing zone to distribute the accounts while achieving an account or application level of segregation. Managing large numbers of accounts could lead to operational or cost overhead.
Operational Risk	(Depends) Low. Operational integration and readiness once only. Less chance of process drifts.	(Depends) Low. Multiple integration and operational activities. Drift in multiple landing zones over the period could lead to operational risks.
Multi AWS Region	Single AWS Region. AMS multi-account landing zone is restricted to a single AWS Region. To span multiple AWS Regions, use multiple multi-account landing zone.	Multi AWS Region. With multiple multi-account landing zones, you can have each MALZ deployed in one region and interconnect them using transit gateway (TGW) peering.
Account migration or portability	Yes. Moving accounts from one OU to another within the same AWS Organization is possible.	No. AMS doesn't support migration of an account across landing zones; that is, across AWS Organizations. Workloads can reach across landing zones with transit gateway (TGW) or VPC peering.

Entity	Single AMS landing zone	Multiple (two or more) landing zones
Change management	Medium. Making destructive changes to common components like TGW, Active Directory (AD), or outbound (egress) can impact all workloads in a multi-account landing zone. However, changes to AMS-managed components are tested internally and are pushed in rolling updates.	Low. Making destructive changes to common components like TGW, AD, or outbound (egress) can impact only the workloads in that specific multi-account landing zone.
Data and access controls	(Depends) Low control if you'd like to connect to different on-premise ADs and networks for Prod vs Non-Prod workloads. SAML federation, TGW domains, and security groups (SGs) can help implement required controls too.	(Depends) High control if you'd like to connect to different on-premise ADs and networks for Prod vs Non-Prod workloads. Use separate landing zones for strict compliance requirements.
Compliance and Security	(Depends) Low if there are strict compliance needs to completely segregate material vs non-material workloads. AMS standard preventative and detective controls in place.	(Depends) High as multiple multi-account landing zone could help achieve strict compliance requirements by completely segregating material vs non-material workloads. AMS standard preventative and detective controls in place.

Recommendation: Without strict Compliance or multi-Region need, starting with single AMS multi-account landing zone would strike a good balance among cost, security, operational excellence, and migration complexity. You can always setup additional landing zone, if any account or business constraints are encountered.

Single multi-account landing zone vs. Multiple multi-account landing zone FAQs

Some commonly asked questions when choosing to set up a single multi-account landing zone or multiple multi-account landing zones:

Q1: Can I start with a single multi-account landing zone and move to multiple multi-account landing zone, if any account limits or business constraints are encountered?

A: Yes. You can choose to set up another multi-account landing zone at any given time:

- A new billing payer account will be required to be setup (currently AWS doesn't support multi-payer accounts in a single AWS org).
- Multi-Account Landing Zone base build takes up to 2 weeks lead time once the multi-account landing zone questionnaire is filled out.
- Every multi-account landing zone means an addition of ~3K USD / month running cost.
- N/W, AD, DNS, and SSO integration will be required to establish for new MALZ.
- Any Reserved Instances (RIs), Cost Saving plans will be needed to be setup for the new multi-account landing zone (RIs are not transferrable).
- AMS multi-account landing zone doesn't support migration of an account across multi-account landing zone accounts; for example, across AWS Orgs. However, to move applications from one account to another is possible using standard migration methods.

Q2: What is AMS approach to MALZ updates/changes to underlying/shared infrastructure and quantify the risk to customers? Provide details on what assurances are wrapped into the process. How do Customers get comfortable that MALZ updates/changes will not impact customers? Is there any measures Customer need to take to prevent disruption?

A: AMS follows a strict change methodology using internal tools that enables us to define, review, schedule and execute changes to customers' environments.

The process to release updates enforces code reviews, integration testing, deployment in gamma and beta environments, and additional baking time and testing in beta and gamma environments before releasing to customers environments. All releases include rollback procedures and are closely monitored by the releases team and the team who created and requested the change. The scope of the releases are confined to stacks owned and provisioned by AMS. On average, we execute at least one release per week.

In addition:

- AMS SLA are applicable. As per AMS service description any incident raised post shared infra maintenance activity would adhere to entitled SLA for resolution or credits.
- No special preventive measures are required by Customers to prevent disruption to common infrastructure. Customers have Read-Only permissions at AWS Org or Core OU accounts, so customers can’t make any destructive changes to the MALZ core env. All customer’s requests to Core infrastructure requires AMS review and approval.
- Customers can test certain Org level changes like SCPs/Roles at individual non-prod account levels before propagating changes at App OU level. It is on the AMS roadmap to allow multiple APP OUs (Q2 2020), which would further alleviate risk in making some of the ORG level changes. MALZ team has already released separate OU for “Build Mode” accounts, to ensure clear segregation of customer ownership and separate controls.
- Most of these are changes that allow AMS to operate the workload in effective and efficient manner and does not necessarily impact customers workload. Where AMS believes a shared infra change can have an impact to customers’ workload they are then aligned with customers’ change window.

High level recommendation, start with multiple multi-account landing zones if:

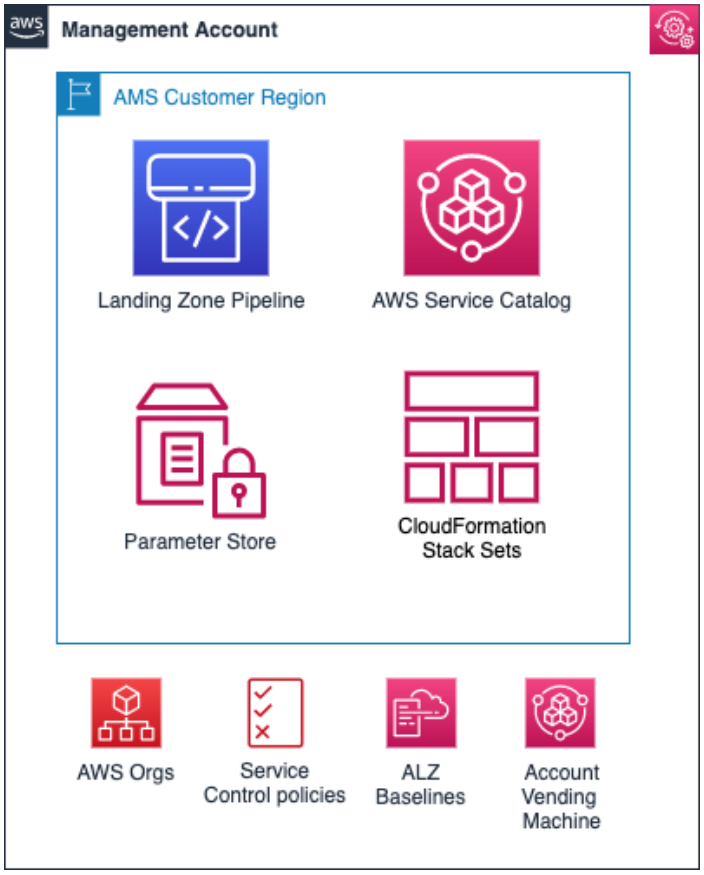
- If it helps you achieve any specific compliance.
- If you need to use Multi-Region.
- If you have different on-prem ADs and Networks for Prod/Material vs Non-Prod/Non-Material workloads, to clearly segregate b/w the workloads.

Multi-Account Landing Zone accounts

Topics

Management account

The management account is your initial AWS account when you begin onboarding with AMS. It utilizes AWS Organizations as a management account, which gives the account the ability to create and financially manage member accounts. It contains the AWS landing zone (ALZ) framework, account configuration stack sets, AWS Organization service control policies (SCPs), etc. The following diagram provides a high-level overview of the resources contained in the management account.



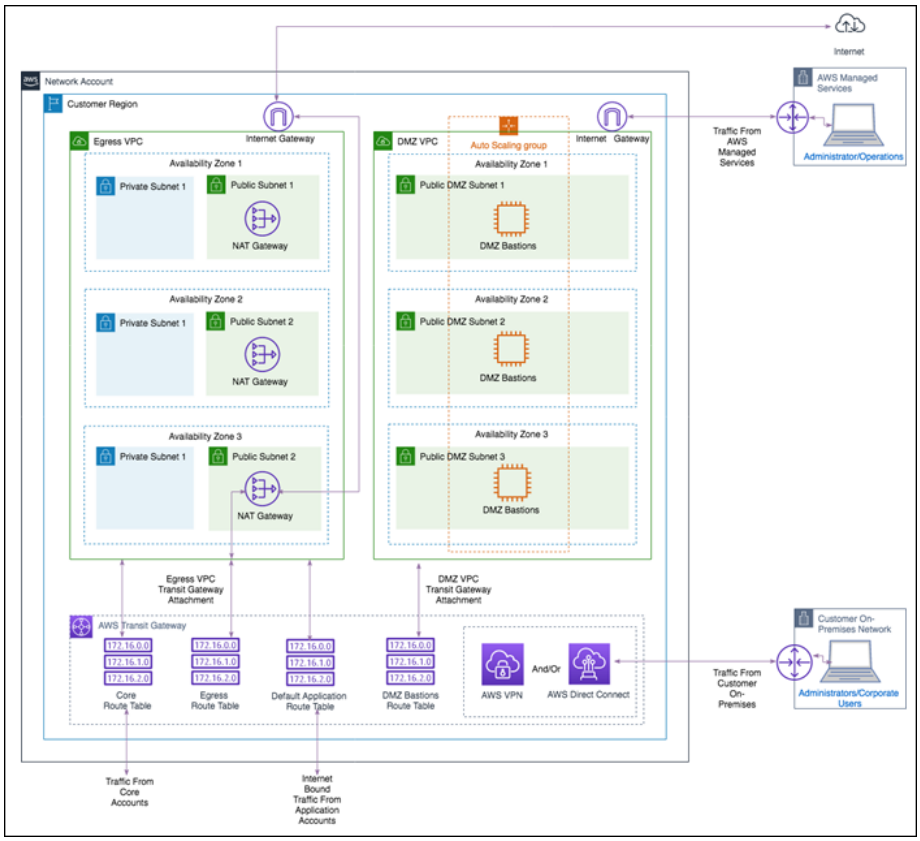
Resources in the management account

Other than the above standard services, no additional AWS resources are created in the management account during onboarding. The following inputs are required during onboarding to AMS:

- *Management account ID*: AWS Account ID that is created initially by you.
- *Core Accounts emails*: Provide the emails to be associated with each of the core accounts: Networking, Shared Services, Logging, and Security account.
- *Service Region*: Provide the AWS region to which all resources of your AMS landing zone will be deployed.

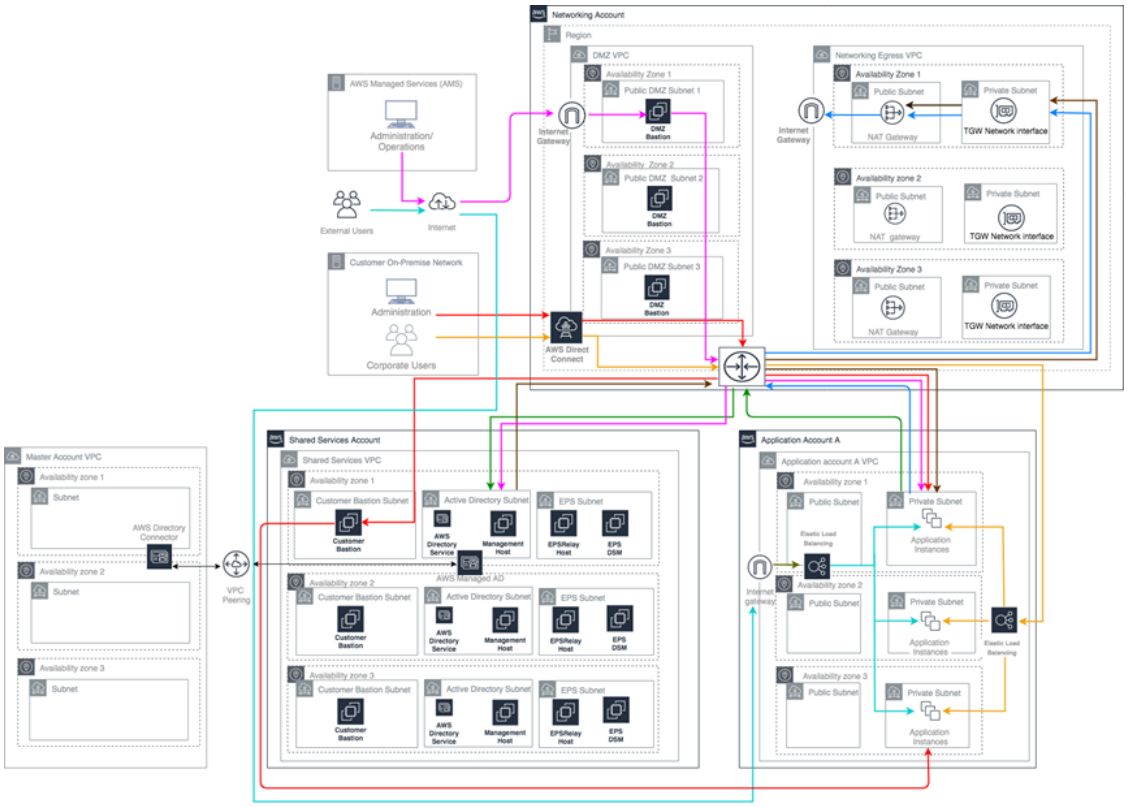
Networking account

The Networking account serves as the central hub for network routing between AMS multi-account landing zone accounts, your on-premises network, and egress traffic out to the Internet. In addition, this account contains public DMZ bastions that are the entry point for AMS engineers to access hosts in the AMS environment. For details, see the following high-level diagram of the networking account below.



Networking account architecture

The following diagram depicts the AMS multi-account landing zone environment, showcasing network traffic flows across account, and is an example of a highly-available setup.



→	Egress Internet Traffic from Application Account VPC and Shared Services VPC through Egress VPC (Networking Account) and Transit Gateway
→	Egress Traffic from an Application Account VPC to Shared Services VPC via Transit gateway (Networking Account)
→	Egress Internal Traffic from Shared Services VPC to Application and Networking Account VPCs via Transit Gateway (Networking Account).
→	Ingress through internet with managed internet gateway for AMS administrators and operators through DMZ bastions to Application VPCs and Shared Services Account VPCs via Transit Gateway (Networking Account)
→	Ingress through DirectConnect (internal customer network administrators) and Customer Bastions to Application Account's VPC instances via Transit Gateway (Networking Account)
→	Ingress through DirectConnect (internal customer network users) for Corporate Users to Application Instances in Application Account VPCs via Transit Gateway (Networking Account).
→	Ingress through Internet with managed Internet Gateway (external users), through AWS load balancers in Application (Public) Subnet and then to Application Instances in Application Account VPC.

Customer's AMS environment is categorized into multiple accounts, managed under AWS Organization. The environment is split into AMS Core Infrastructure and Application Infrastructure. Core accounts consists of Master Account, Networking Account, Shared Services Account, Logging account and Security account, whereas Application Infrastructure consists of applications accounts.

Each AMS accounts can have multiple VPCs in one region with resource subnets located in up to three availability zones. Each availability zone can have private and public subnets (depends on configuration selected). Your ("customer") corporate network is connected through a DirectConnect (VPN) tunnel, and AMS operations connects to your Application infrastructure over the internet.

Master account is the central hub to manage and configure member accounts. Landingzone framework and SSO enablement is configured in this account.

The Networking Account serves as the central hub for network routing between AMS Core Accounts, your OnPremise Network, and egress traffic out to the Internet via Transit Gateway. Transit Gateway is an AWS service that enables customers to connect their VPCs and their on-premises networks to a single gateway. Networking account consists of DMZ VPC which contain DMZ bastions hosts that serve as SSG jump boxes for AMS operations team and Egress VPC through which all network traffic is routed.

Shared Services account has a VPC with following subnets: ActiveDirectory Subnet, Customer Bastion Subnet and EPS subnet. AD Subnet consists of AMS Directory service, AD domain controller, and management hosts that automate provisioning and common tasks. And EPS subnets consists of Antivirus (Trend Micro) management servers that include EPS DSM and EPS relay (for scalability). Lastly, customer bastion subnets consists of internal (customer) bastion hosts.

Your "Customer" accounts contain your workloads, EC2 instances, RDS etc

External users connect to your applications for the internet via an AWS load balancer that is located in your application account.

AMS configures all aspects of networking for you based on our standard templates and your selected options provided during onboarding. A standard AWS network design is applied to your AWS account, and a VPC is created for you and connected to AMS by either VPN or Direct Connect. For more information about Direct Connect, see AWS Direct Connect. Standard VPCs include the DMZ, shared services, and an application subnet. During the onboarding process, additional VPCs might be requested and created to match your needs (for example, customer divisions, partners). After onboarding, you are provided with a network diagram: an environment document that explains how your network has been set up.

Note

For information about default service limits and constraints for all active services, see the AWS Service Limits documentation.

Our network design is built around the Amazon "Principle of Least Privilege". In order to accomplish this, we route all traffic, ingress and egress, through a DMZ, except traffic coming from a trusted network. The only trusted network is the one configured between your on-premises environment and the VPC through the use of a VPN and/or an AWS Direct Connect (DX). Access is granted through the use of bastion instances, thereby preventing direct access to any production resources. All of your applications and resources reside inside private subnets that are reachable through public load balancers. Public egress traffic flows through the NAT Gateways in the egress VPC (in the Networking account) to the Internet Gateway and then to the Internet. Alternatively, the traffic can flow over your VPN or Direct Connect to your on-premises environment.

Private network connectivity to AMS Multi-account landing zone environment

AWS offers private connectivity via either virtual private network (VPN) connectivity, or dedicated lines with AWS Direct Connect. Private connectivity in your multi-account environment, is set up using one of the methods described next:

- Centralized Edge connectivity using Transit Gateway
- Connecting Direct Connect (DX) and/or VPN to account virtual private clouds (VPCs)

Centralized edge connectivity using transit gateway

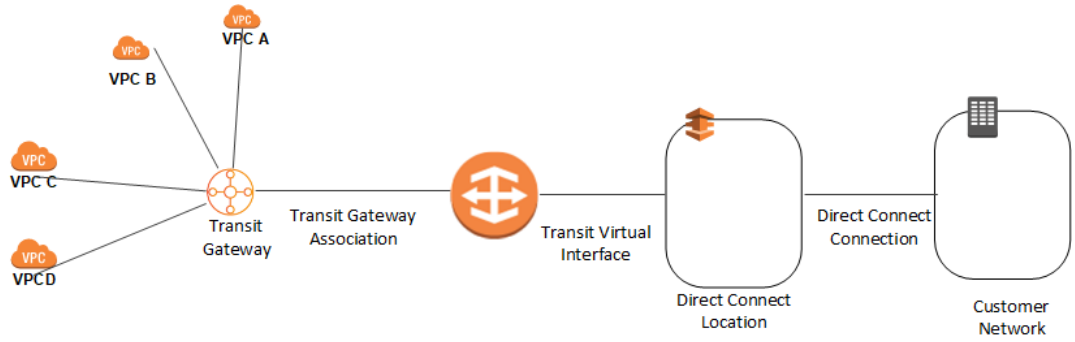
AWS Transit Gateway is a service that enables you to connect your VPCs and your on-premises networks to a single gateway. Transit gateway (TGW) can be used to consolidate your existing edge connectivity and route it through a single ingress/egress point. Transit gateway is created in the networking account of your AMS multi-account environment. For more details about transit gateway, see AWS Transit Gateway.

AWS Direct Connect (DX) gateway is used to connect your DX connection over a transit virtual interface to the VPCs or VPNs that are attached to your transit gateway. You associate a Direct Connect gateway with the transit gateway. Then, create a transit virtual interface for your AWS Direct Connect connection to the Direct Connect gateway. For information on DX virtual interfaces, see AWS Direct Connect Virtual Interfaces.

This configuration offers the following benefits. You can:

- Manage a single connection for multiple VPCs or VPNs that are in the same AWS Region.
- Advertise prefixes from on-premises to AWS, and from AWS to on-premises.

Note
For information about using a DX with AWS services, see the Resiliency Toolkit section Classic.
For more information about Transit Gateway associations, see Transit Gateway associations.



To increase the resiliency of your connectivity, we recommend that you attach at least two transit virtual interfaces from different AWS Direct Connect locations to the Direct Connect gateway. For more information, see the AWS Direct Connect resiliency recommendation.

Connecting DX or VPN to account VPCs

With this option, the VPCs in your AMS multi-account landing zone environments are directly connected to Direct Connect or VPN. The traffic directly flows from the VPCs to Direct Connect or VPN without traversing through the transit gateway.

Resources in the networking account

As shown in the networking account diagram, the following components are created in the account and require your input.

The Networking account contains two VPCs: **Egress VPC** and **DMZ VPC** also known as the **Perimeter** VPC.

AWS Network Manager

AWS Network Manager is a service that enables you to visualize your transit gateway (TGW) networks at no additional cost to AMS. It provides centralized network monitoring on both AWS resources and on on-premises networks, a single global view of their private network in a topology diagram and in a geographical map, and utilization metrics, such as bytes in/out, packets in/out, packets dropped, and alerts for changes in the topology, routing, and up/down connection status. For information, see Transit Gateway Network Manager.

Use one of the following roles to access this resource:

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

Egress VPC

The Egress VPC is primarily used for egress traffic to the Internet and is composed of public/private subnets in up to three availability zones (AZs). Network address translation (NAT) gateways are provisioned in the public subnets, and transit gateway (TGW) VPC attachments are created in the private subnets. Egress, or outbound, internet traffic from all networks enter through the private subnet via TGW, where it is then routed to a NAT via VPC route tables.

For your VPCs that contain public-facing applications in a public subnet, traffic originating from the internet is contained within that VPC. Return traffic is not routed to the TGW or Egress VPC, but routed back through the internet gateway (IGW) in the VPC.

> **Note**
> Networking VPC CIDR range: When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.16.0/24. This is the primary CIDR block for your VPC.
> The AMS multi-account landing zone team recommends the range of 24 (with more IP address) to provide some buffer in case other resources/appliances, are deployed in the future.

Managed Palo Alto egress firewall

AMS provides a Managed Palo Alto egress firewall solution, which enables internet-bound outbound traffic filtering for all networks in the Multi-Account Landing Zone environment (excluding public facing services). This solution combines industry-leading firewall technology (Palo Alto VM-300) with AMS' infrastructure management capabilities to deploy, monitor, manage, scale, and restore infrastructure within compliant operating environments. Third parties, including Palo Alto Networks, do not have access to the firewalls; they are managed solely by AMS engineers.

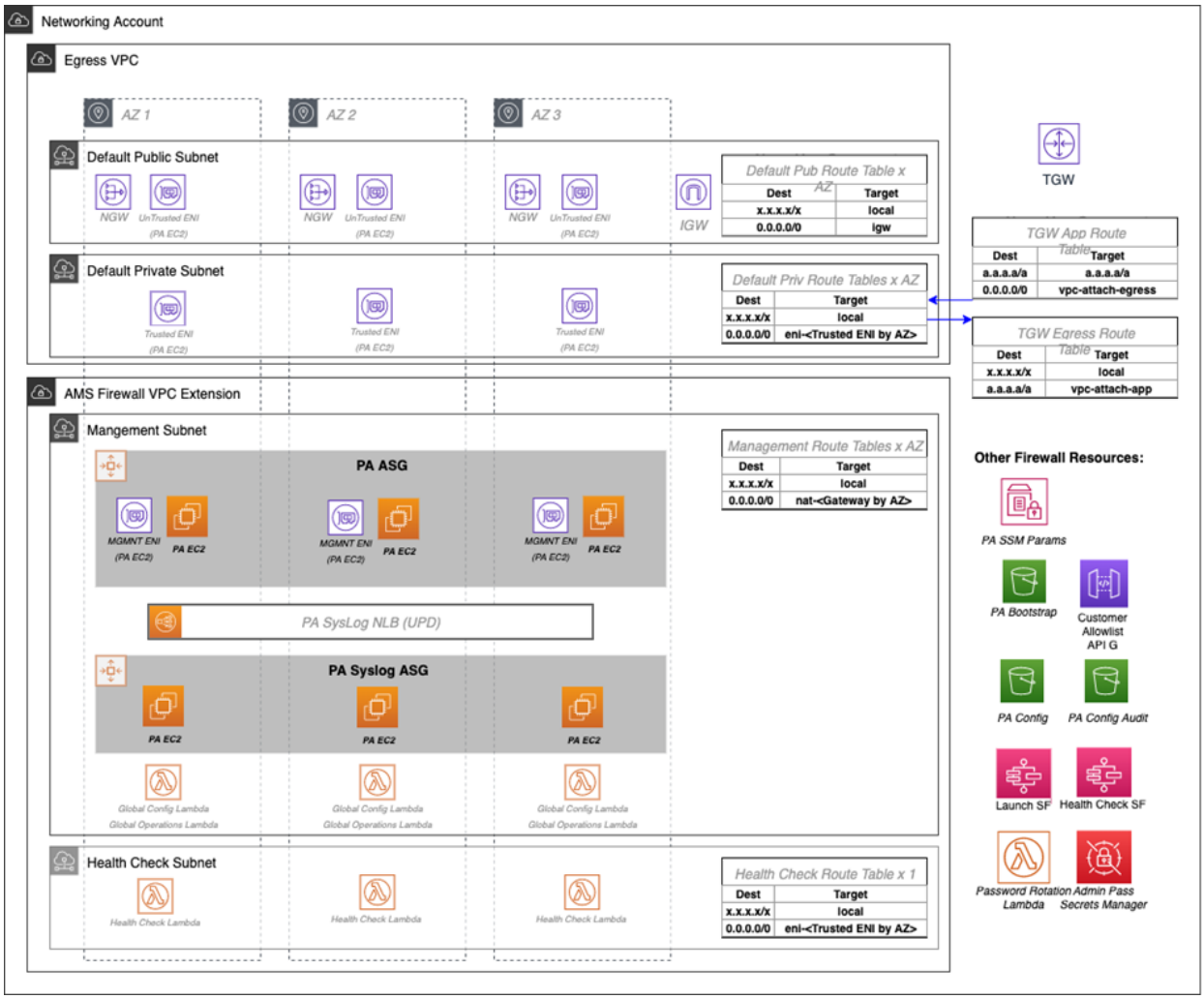
Traffic control

The managed outbound firewall solution manages a domain allow-list composed of AMS-required domains for services such as backup and patch, as well as your defined domains. When outbound

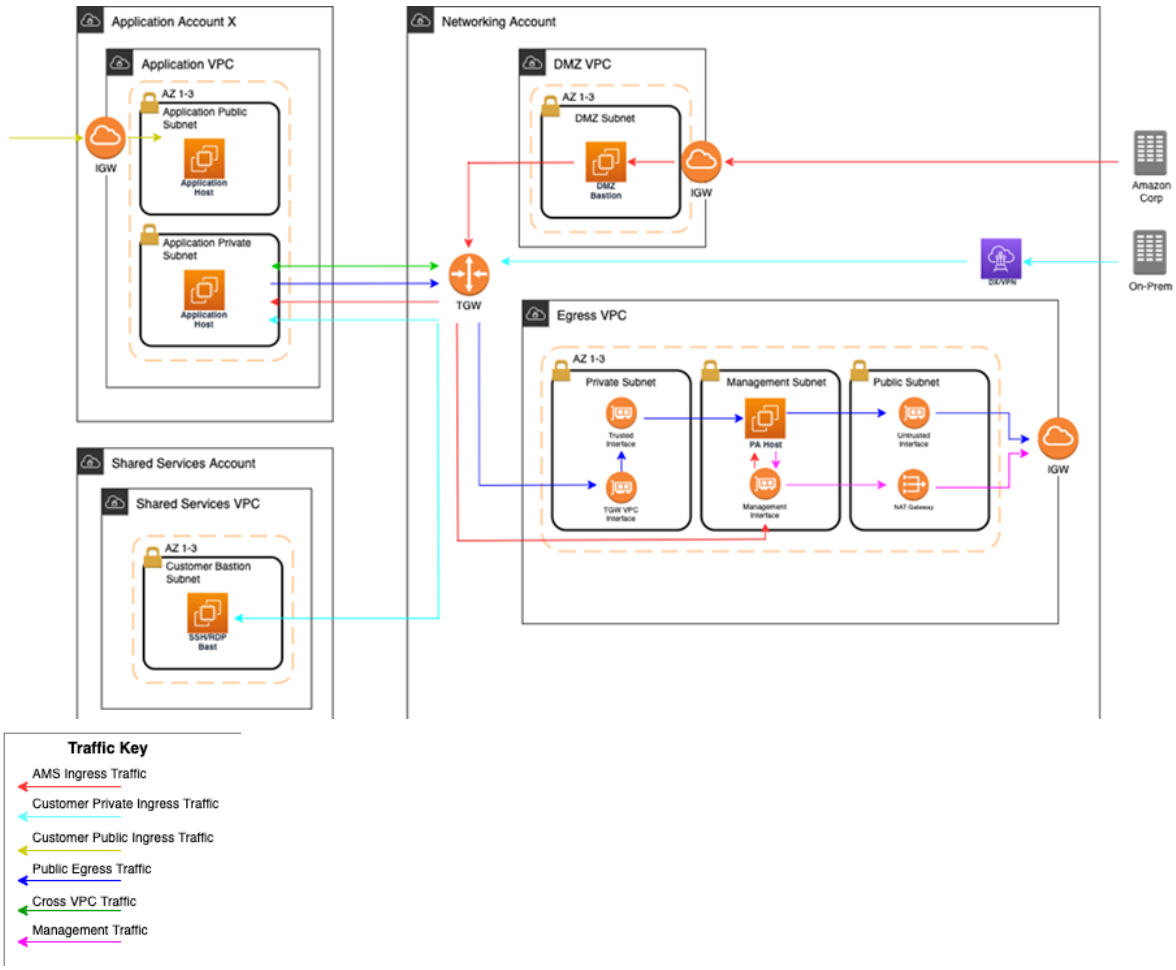
internet traffic is routed to the firewall, a session is opened, traffic is evaluated, and if it matches an allowed domain, the traffic is forwarded to the destination.

Architecture

The managed egress firewall solution follows a high-availability model, where two to three firewalls are deployed depending on number of availability zones (AZs). The solution utilizes part of the IP space from the default egress VPC, but also provisions a VPC extension (/24) for additional resources required for managing the firewalls.



Network flow



At a high level, public egress traffic routing remains the same, except for how traffic is routed to the internet from the egress VPC:

1. Egress traffic destined for the internet is sent to the Transit Gateway (TGW) through VPC route table
2. TGW routes traffic to the egress VPC via the TGW route table
3. VPC routes traffic to the internet via the private subnet route tables
   a. In the default Multi-Account Landing Zone environment, internet traffic is sent directly to a network address translation (NAT) gateway. The managed firewall solution reconfigures the private subnet route tables to point the default route (0.0.0.0/0) to a firewall interface instead.

The firewalls themselves contain three interfaces:

1. Trusted interface: Private interface for receiving traffic to be processed.
2. Untrusted interface: Public interface to send traffic to the internet.
   a. Because the firewalls perform NAT, external servers accept requests from these public IP addresses.
3. Management interface: Private interface for firewall API, updates, console, and so on.

Throughout all the routing, traffic is maintained within the same availability zone (AZ) to reduce cross-AZ traffic. Traffic only crosses AZs when a failover occurs.

Allow-list modification

After onboarding, a default allow-list named `ams-allowlist` is created, containing AMS-required public endpoints as well as public endpoints for patching Windows and Linux hosts. Once operating, you can create RFC's in the AMS console under the Management | Managed Firewall | Outbound (Palo Alto) category to create or delete allow-lists, or modify the domains. Be aware that `ams-allowlist` cannot be modified. The RFC's are handled with full automation (they are not manual).

Custom security policy

Security policies determine whether to block or allow a session based on traffic attributes, such as the source and destination security zone, the source and destination IP address, and the service. Custom security policies are supported with fully automated RFCs. CTs to create or delete security policy can be found under Management | Managed Firewall | Outbound (Palo Alto) category, and the CT to edit an existing security policy can be found under Deployment | Managed Firewall | Outbound (Palo Alto) category. You'll be able to create new security policies, modify security policies, or delete security policies.

> **Note**
> The default security policy `ams-allowlist` cannot be modified

CloudWatch PA egress dashboards

Two dashboards can be found in CloudWatch to provide an aggregated view of Palo Alto (PA). the **AMS-MF-PA-Egress-Config-Dashboard** provides a PA config overview, links to allow-lists, and a list of all security policies including their attributes. The **AMS-MF-PA-Egress-Dashboard** can be customized to filter traffic logs. For example, to create a dashboard for a security policy, you can create an RFC with a filter like:

```
fields @timestamp, @message
| filter @logStream like /pa-traffic-logs/
| filter @message like /<Security Policy Name>/
| parse @message
 "*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*"
 as x1, @x2, @x3, @x4, @type, @x6, @x7, @source_ip, @destination_ip, @source_nat_ip,
 @dest_nat_ip, @rule, @x13, @x14, @application, @x16, @from_zone, @to_zone, @x19, @x20,
 @x21, @x22, @session_id, @x24, @source_port, @destination_port, @source_nat_port,
 @destination_nat_port, @x29, @protocol, @action, @bytes, @bytes_sent, @bytes_recieved,
 @packets, @x36, @x37, @category, @x39, @x40, @x41, @source_country, @destination_country,
 @x44, @packets_sent, @packets_recieved, @session_end_reason, @x48, @x49, @x50
| display @timestamp, @rule, @action, @session_end_reason, @protocol, @source_ip,
 @destination_ip, @source_port, @destination_port, @session_id, @from_zone,
 @to_zone, @category, @bytes_sent, @bytes_recieved, @packets_sent, @packets_recieved,
 @source_country, @destination_country
```

Failover model

The firewalls solution includes two-three Palo Alto (PA) hosts (one per AZ). Healthy check canaries run on a constant schedule to evaluate the health of the hosts. If a host is identified as unhealthy, AMS is notified and the traffic for that AZ is automatically shifted to a healthy host in a different AZ via route table change. Since the health check workflow is running constantly, if the host becomes healthy again due to transient issues or manual remediation, then traffic is shifted back to the correct AZ with the healthy host.

Scaling

AMS monitors the firewall for throughput and scaling limits. When throughput limits exceed lower watermark thresholds (CPU/Networking), AMS receives an alert. A low watermaker threshold indicates that resources are approaching saturation, reaching a point where AMS will evaluate the metrics over time and reach out to suggest scaling solutions.

Backup and Restore

Backups are created during initial launch, after any configuration changes, and on a regular interval. Initial launch backups are created on a per host basis, but configuration change and regular interval backups are performed across all firewall hosts when the backup workflow is invoked. AMS engineers can create additional backups outside of those windows or provide backup details if requested.

AMS engineers can perform restoration of configuration backups if required. If a restoration is required, it will occur across all hosts to keep configuration between hosts in sync.

Restoration also can occur when a host requires a complete recycle of an instance. An automatic restoration of the latest backup occurs when a new EC2 instance is provisioned. In general, hosts are not recycled regularly, and are reserved for severe failures or required AMI swaps. Host recycles are initiated manually, and you are notified before a recycle occurs.

Other than the firewall configuration backups, your specific allow-list rules are backed up separately. A backup is automatically created when your defined allow-list rules are modified. Restoration of the allow-list backup can be performed by an AMS engineer, if required.

Updates

AMS Managed Firewall Solution requires various updates over time to add improvements to the system, additional features, or updates to the firewall operating system (OS) or software.

Most changes will not affect the running environment such as updating automation infrastructure, but other changes such as firewall instance rotation or OS update may cause disruption. When a potential service disruption due to updates is evaluated, AMS will coordinate with you to accommodate maintenance windows.

Operator access

AMS operators use their ActiveDirectory credentials to log into the Palo Alto device to perform operations (e.g., patching, responding to an event, etc.). The solution retains standard AMS Operator authentication and configuration change logs to track actions performed on the Palo Alto Hosts.

Default logs

By default, the logs generated by the firewall reside in local storage for each firewall. Overtime, local logs will be deleted based on storage utilization. The AMS solution provides real-time shipment of logs off of the machines to CloudWatch logs; for more information, see CloudWatch Logs integration (p. 67).

AMS engineers still have the ability to query and export logs directly off the machines if required. In addition, logs can be shipped to a customer-owned Panorama; for more information, see Panorama integration (p. 67).

The Logs collected by the solution are the following:

RFC Status Codes

Log Type	Description
Traffic	Displays an entry for the start and end of each session. Each entry includes the date and time, source and destination zones, addresses and ports, application name, security rule name applied to the flow, rule action (allow, deny, or drop), ingress and egress interface, number of bytes, and session end reason. The Type column indicates whether the entry is for the start or end of the session, or whether the session was denied or dropped. A "drop" indicates that the security rule that blocked the traffic specified "any" application, while a "deny" indicates the rule identified a specific application.

Log Type	Description
	If traffic is dropped before the application is identified, such as when a rule drops all traffic for a specific service, the application is shown as "not-applicable".
Threat	Displays an entry for each security alarm generated by the firewall. Each entry includes the date and time, a threat name or URL, the source and destination zones, addresses, and ports, the application name, and the alarm action (allow or block) and severity. The Type column indicates the type of threat, such as "virus" or "spyware;" the Name column is the threat description or URL; and the Category column is the threat category (such as "keylogger") or URL category.
URL Filtering	Displays logs for URL filters, which control access to websites and whether users can submit credentials to websites.
Configuration	Displays an entry for each configuration change. Each entry includes the date and time, the administrator user name, the IP address from where the change was made, the type of client (web interface or CLI), the type of command run, whether the command succeeded or failed, the configuration path, and the values before and after the change.
System	Displays an entry for each system event. Each entry includes the date and time, the event severity, and an event description.
Alarms	The alarms log records detailed information on alarms that are generated by the system. The information in this log is also reported in Alarms. Refer to "Define Alarm Settings".
Authentication	Displays information about authentication events that occur when end users try to access network resources for which access is controlled by Authentication policy rules. Users can use this information to help troubleshoot access issues and to adjust user Authentication policy as needed. In conjunction with correlation objects, users can also use Authentication logs to identify suspicious activity on the users network, such as brute force attacks. Optionally, users can configure Authentication rules to Log Authentication Timeouts. These timeouts relate to the period of time when a user needs authenticate for a resource only once but can access it repeatedly. Seeing information about the timeouts helps users decide if and how to adjust them.
Unified	Displays the latest Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering log entries in a single view. The collective log view enables users to investigate and filter these different types of logs together (instead of searching each log set separately). Or, users can choose which log types to display: click the arrow to the left of the filter field and select traffic, threat, url, data, and/or wildfire to display only the selected log types.

Event management

AMS continually monitors the capacity, health status, and availability of the firewall. Metrics generated from the firewall, as well as AWS/AMS generated metrics, are used to create alarms that are received by AMS operations engineers, who will investigate and resolve the issue. The current alarms cover the following cases:

Event Alarms:

- Firewall Dataplane CPU Utilization
  - CPU Utilization - Dataplane CPU (Processing traffic)
- Firewall Dataplane Packet Utilization is above 80%
  - Packet utilization - Dataplane (Processing traffic)
- Firewall Dataplane Session Utilization
- Firewall Dataplane Session Active
- Aggregate Firewall CPU Utilization
  - CPU Utilization across all CPUs
- Failover By AZ
  - Alarms when a fail over occurs in an AZ
- Unhealthy Syslog Host
  - Syslog host fails health check

Management Alarms:

- Health Check Monitor Failure Alarm
  - When health check workflow fails unexpectedly
  - This is for the workflow itself, not if a firewall health check fails
- Password Rotation Failure Alarm
  - When password rotation fails
  - API/Service user password is rotated every 90 days

Metrics

All metrics are captured and stored in CloudWatch in the Networking account. These can be viewed by gaining console access to the Networking account and navigating to the CloudWatch console. Individual metrics can be viewed under the metrics tab or a single-pane dashboard view of select metrics and aggregated metrics can be viewed by navigating to the Dashboard tab, and selecting **AMS-MF-PA-Egress-Dashboard**.

Custom Metrics:

- Health Check
  - Namespace: AMS/MF/PA/Egress
    - PARouteTableConnectionsByAZ
    - PAUnhealthyByInstance
    - PAUnhealthyAggregatedByAZ
    - PAHealthCheckLockState
- Firewall Generated
  - Namespace: AMS/MF/PA/Egress/<instance-id>
    - DataPlaneCPUUtilizationPct
    - DataPlanePacketBuffferUtilization
    - panGPGatewayUtilizationPct
    - panSessionActive
    - panSessionUtilization

CloudWatch Logs integration

CloudWatch Logs integration forwards logs from the firewalls into CloudWatch Logs, which mitigates the risk of losing logs due to local storage utilization. Logs are populated in real-time as the firewalls generate them, and can be viewed on-demand through the console or API.

Complex queries can be built for log analysis or exported to CSV using CloudWatch Insights. In addition, the custom AMS Managed Firewall CloudWatch dashboard will also show a quick view of specific traffic log queries and a graph visualization of traffic and policy hits over time. Utilizing CloudWatch logs also enables native integration to other AWS services such as a AWS Kinesis.

> **Note**
> PA logs cannot be directly forwarded to an existing on-prem or 3rd party Syslog collector. AMS Managed Firewall solution provides real-time shipment of logs off of the PA machines to AWS CloudWatch Logs. You can use CloudWatch Logs Insight feature to run ad-hoc queries. In addition, logs can be shipped to your Palo Alto's Panorama management solution. CloudWatch logs can also be forwarded to other destinations using CloudWatch Subscription Filters. Learn more about Panorama in the following section. To learn more about Splunk, see Integrating with Splunk.

Panorama integration

AMS Managed Firewall can, optionally, be integrated with your existing Panorama. This allows you to view firewall configurations from Panorama or forward logs from the firewall to the Panorama. Panorama integration with AMS Managed Firewall is read only, and configuration changes to the firewalls from Panorama are not allowed. Panorama is completely managed and configured by you, AMS will only be responsible for configuring the firewalls to communicate with it.

Licensing

The price of the AMS Managed Firewall depends on the type of license used, hourly or bring your own license (BYOL), and the instance size in which the appliance runs. You are required to order the instances size and the licenses of the Palo Alto firewall you prefer through AWS Marketplace.

- Marketplace Licenses: Accept the terms and conditions of the VM-Series Next-Generation Firewall Bundle 1 from the networking account in MALZ.
- BYOL Licenses: Accept the terms and conditions of the VM-Series Next-Generation Firewall (BYOL) from the networking account in MALZ and share the "BYOL auth code" obtained after purchasing the license to AMS.

Limitations

At this time, AMS supports VM-300 series or VM-500 series firewall. Configurations can be found here: VM-Series Models on AWS EC2 Instances,

> **Note**
> The AMS solution runs in Active-Active mode as each PA instance in its AZ handles egress traffic for their respected AZ. So, with two AZs, each PA instance handles egress traffic up to 5 Gbps and effectively provides overall 10 Gbps throughput across two AZs. The same is true for all limits in each AZ. Should the AMS health check fail, we shift traffic from the AZ with the bad PA to another AZ, and during the instance replacement, capacity is reduced to the remaining AZs limits.
> AMS does not currently support other Palo Alto bundles available on AWS Marketplace; for example, you cannot ask for the "VM-Series Next-Generation Firewall Bundle 2". Note that the AMS Managed Firewall solution using Palo Alto currently provides only an egress traffic filtering offering, so using advanced VM-Series bundles would not provide any additional features or benefits.

Onboarding requirements

- You must review and accept the Terms and Conditions of the VM-Series Next-Generation Firewall from Palo Alto in AWS Marketplace.
- You must confirm the instance size you want to use based on your expected workload.
- You must provide a /24 CIDR Block that does not conflict with networks in your Multi-Account Landing Zone environment or On-Prem. It must be of same class as the Egress VPC (the Solution provisions a /24 VPC extension to the Egress VPC).

Pricing

AMS Managed Firewall base infrastructure costs are divided in three main drivers: the EC2 instance that hosts the Palo Alto firewall, the software license Palo Alto VM-Series licenses, and CloudWatch Integrations.

The following pricing is based on the VM-300 series firewall.

- EC2 Instances: The Palo Alto firewall runs in a high-availability model of 2-3 EC2 instances, where instance is based on expected workloads. Cost for the instance depends on the region and number of AZs
  - Ex. us-east-1, m5.xlarge, 3AZs
    - $0.192 * 24 * 30 * 3 = $414.72
  - https://aws.amazon.com/ec2/pricing/on-demand/
- Palo Alto Licenses: The software license cost of a Palo Alto VM-300 next-generation firewall depends on the number of AZ as well as instance type.
  - Ex. us-east-1, m5.xlarge, 3AZs
    - $0.87 * 24 * 30 * 3 = $1879.20
    - https://aws.amazon.com/marketplace/pp/B083M7JPKB?ref_=srh_res_product_title#pdp-pricing
- CloudWatch Logs Integration: CloudWatch logs integration utilizes SysLog servers (EC2 - t3.medium), NLB, and CloudWatch Logs. The cost of the servers is based on region and number of AZs, and the cost of the NLB/CloudWatch logs varies based on traffic utilization.
  - Ex. us-east-1, t3.medium, 3AZ
    - $0.0416 * 24 * 30 * 3 = $89.86
  - https://aws.amazon.com/ec2/pricing/on-demand/
  - https://aws.amazon.com/cloudwatch/pricing/

Perimeter (DMZ) VPC

The Perimeter, or DMZ, VPC contains the necessary resources for AMS Operations engineers to access AMS networks. It contains public subnets across 2-3 AZs, with SSH Bastions hosts in an Auto Scaling group (ASG) for AMS Operations engineers to log into or tunnel through. The security groups attached to the DMZ bastions contain port 22 inbound rules from **Amazon Corp Networks**.

DMZ VPC CIDR range: When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.16.0/24. This is the primary CIDR block for your VPC.

> **Note**
> The AMS team recommends the range of 24 (with more IP address) to provide some buffer in case other resources, such as a firewall, are deployed in the future.

AWS Transit Gateway

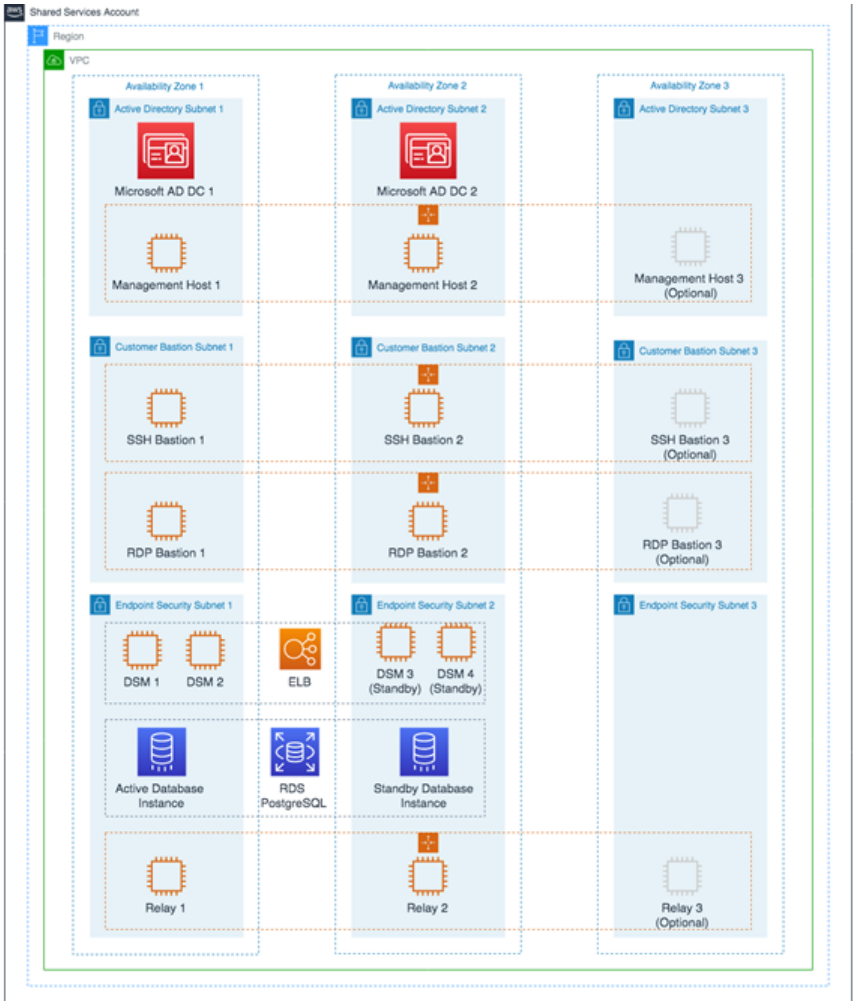
AWS Transit Gateway (TGW) is a service that enables you to connect your Amazon Virtual Private Clouds (VPCs) and your on-premises networks to a single gateway. Transit gateway is the networking backbone that handles the routing between AMS account networks and external networks. For information about Transit Gateway, see AWS Transit Gateway.

Provide the following input to create this resource:

- *Transit Gateway ASN number**: Provide the private Autonomous System Number (ASN) for your transit gateway. This should be the ASN for the AWS side of a Border Gateway Protocol (BGP) session. The range is 64512 to 65534 for 16-bit ASNs.

Shared Services account

The Shared Services account serves as the central hub for most AMS data plane services. The account contains infrastructure and resources required for access management (AD), end-point security management (Trend Micro), and it contains the customer bastions (SSH/RDP). A high-level overview of the resources contained within Shared Services Account is shown in the following graphic.



The Shared Services VPC is composed of the AD subnet, the EPS subnet, and the customer bastions subnet in the three availability zones (AZs). The resources created in the Shared Services VPC are listed below and require your input.

- *Shared Services VPC CIDR range:* When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.1.0/24. This is the primary CIDR block for your VPC.

  Note
  The AMS team recommends the range of /23.

- *Active Directory Details*: Microsoft Active Directory (AD) is utilized for user/resource management, authentication/authorization, and DNS, across all of your AMS multi-account landing zone accounts. AMS AD is also configured with a one-way trust to your Active Directory for trust-based authentication. The following input is required to create the AD:
  - Domain Fully Qualified Domain Name (FQDN): The fully qualified domain name for the AWS Managed Microsoft AD directory. The domain should not be an existing domain or child domain of an existing domain in your network.
  - Domain NetBIOS Name: If you don't specify a NetBIOS name, AMS defaults the name to the first part of your directory DNS. For example, corp for the directory DNS corp.example.com.

- *Trend Micro – endpoint protection security (EPS)*: Trend Micro endpoint protection (EPS) is the primary component within AMS for operating system security. The system is comprised of Deep Security Manager (DSM), EC2 instances, relay EC2 instances, and an agent present within all data plane and customer EC2 instances.

  You must assume the `EPSMarketplaceSubscriptionRole` in the Shared Services account, and subscribe to either the Trend Micro Deep Security (BYOL) AMI, or the Trend Micro Deep Security (Marketplace).

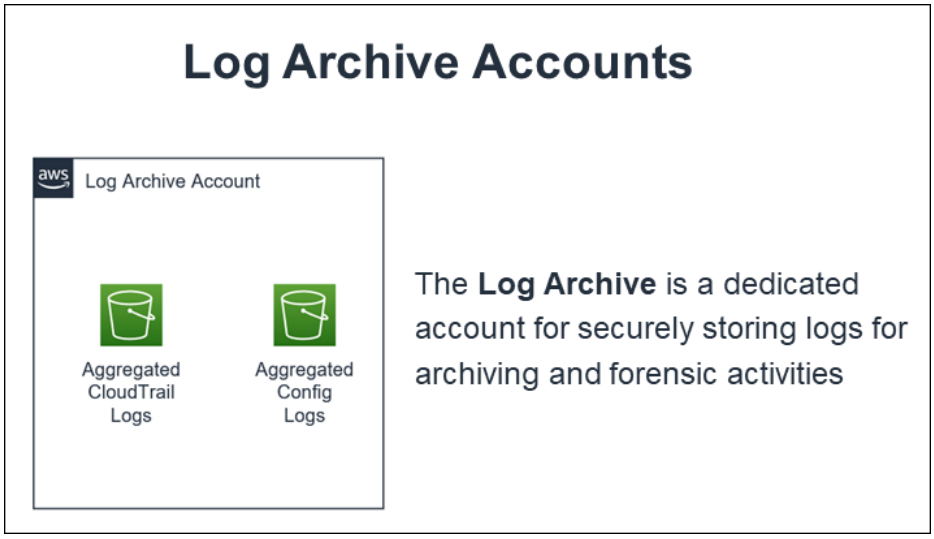
  The following default inputs are required to create EPS (if you want to change from the defaults):
  - Relay Instance Type: Default Value - m5.large
  - DSM Instance Type: Default Value - m5.xlarge
  - DB Instance Size: Default Value - 200 GB
  - RDS Instance Type: Default Value - db.m5.large

- *Customer bastions*: You are provided with SSH or RDP bastions (or both) in the Shared Services Account, to access other hosts in your AMS environment. In order to access the AMS network as a user (SSH/RDP), you must use "customer" Bastions as the entry point. The network path originates from the on-premise network, goes through DX/VPN to the transit gateway (TGW), and then is routed to the Shared Services VPC. Once you are able to access the bastion, you can jump to other hosts in the AMS environment, provided that the access request has been granted.
  - The following inputs are required for SSH bastions.
    - SSH Bastion Desired Instance Capacity: Default Value - 2.
    - SSH Bastion Maximum Instances: Default Value - 4.
    - SSH Bastion Minimum Instances: Default Value -2.
    - SSH Bastion Instance Type: Default Value - m5.large (can be changed to save costs; for example a t3.medium).
    - SSH Bastion Ingress CIDRs: IP address ranges from which users in your network access SSH Bastions.
  - The following inputs are required for Windows RDP bastions.
    - RDP Bastion Instance Type: Default Value - t3.medium.
    - RDP Bastion Desired Minimum Sessions: Default Value - 2.

- RDP Maximum Sessions: Default Value -10.
- RDP Bastion Configuration Type: You can choose one of the below configuration
  - SecureStandard = A user receives one bastion and only one user can connect to the bastion.
  - SecureHA = A user receives two bastions in two different AZ's to connect to and only one user can connect to the bastion.
  - SharedStandard = A user receives one bastion to connect to and two users can connect to the same bastion at once.
  - SharedHA = A user receives two bastions in two different AZ's to connect to and two users can connect to the same bastion at once.
- Customer RDP Ingress CIDRs: IP address ranges from which users in your network will access RDP Bastions.

Log Archive account

The Log Archive account serves as the central hub for archiving logs across your AMS multi-account landing zone environment. There is an S3 bucket in the account that contains copies of AWS CloudTrail and AWS Config log files from each of the AMS multi-account landing zone environment accounts. You could use this account for your Centralised Logging solution with AWS Firehose, or Splunk, and so forth. AMS access to this account is limited to a few users; restricted to auditors and security teams for compliance and forensic investigations related to account activity.



Security account

The Security account is the central hub for housing security related operations and the main point for funneling notifications and alerts to the AMS control plane services. In addition, the Security account houses the Amazon Guard Duty management account and the AWS Config aggregator.

Application accounts: AMS-managed, Developer mode, Customer Managed

Application accounts are AWS accounts within the AMS-managed landing zone architecture that you use to host your workloads. AMS offers three types of Application Accounts with different operational models, responsibilities and features. Each account type is grouped under an organizational unit (OU) from which you can request additional nested OUs. The three types of application accounts are described in this section.

Application Accounts are provisioned through RFC from the Management account.

AMS-managed application accounts

Application accounts that are fully managed by AMS are referred to as AMS-managed application accounts, where all operational tasks in this guide like service request management, incident management, security management, continuity management (backup), patch management, cost-optimization, or monitoring and event management, of infrastructure are performed by AMS. AMS-managed accounts are provisioned in the Application > Managed OU.

There are some AWS services that you can use in your AMS-managed account without AMS management. The list of services and how to add them into your AMS account are described in the Self-Provisioned Services section.

Developer mode application accounts

Accounts with Developer mode are a type of AMS-managed account that provide customers with elevated permissions in AMS "Plus" accounts to provision and update AWS resources outside of the AMS change management process. When using an account that has Developer mode enabled, continuity management, patch management, and change management are provided for resources provisioned through the AMS change management process, or by using an AMS Amazon Machine Image (AMI). However, you are responsible for monitoring infrastructure resources that are provisioned outside of the AMS change management process. With elevated permissions, you have an increased responsibility to ensure adherence to internal controls.

For more information, see Developer mode.

Customer Managed application accounts

You can create accounts that AMS doesn't manage in the standard way. Those accounts are called Customer Managed accounts and they give you full control to self-operate the infrastructure within the accounts while enjoying the benefits of the centralized architecture managed by AMS.

Customer Managed accounts do not have access to the AMS console or any of the services we provide (patch, backup, and so on).

Customer Managed accounts can only be provisioned from your AMS multi-account landing zone management account.

Different AMS modes work with Application accounts differently; to learn more about the modes, see AWS Managed Services modes.

To create your Customer Managed account, see Management account, customer-managed application account: Creating.

Accessing your Customer Managed account

After you provision a Customer Managed account (CMA) in multi-account landing zone, (MALZ) an Admin role, `CustomerDefaultAdminRole`, is in the account for you to assume, through SAML federation, to configure the account.

To access the CMA:

1. Log into the IAM console for the management account with the **CustomerDefaultAssumeRole** role.
2. In the IAM console, on the navigation bar, choose your username.
3. Choose **Switch Role**. If this is the first time choosing this option, a page appears with more information. After reading it, choose **Switch Role**. If you clear your browser cookies, this page can appear again.
4. On the **Switch Role** page, type the Customer Managed account ID and the name of the role to assume: **CustomerDefaultAdminRole**.

Now that you have access, you can create new IAM Roles to continue to access your environment. If you would like to leverage SAML Federation for your CMA Account, see Enabling SAML 2.0 federated users to access the AWS Management Console.

Connecting your CMA with Transit Gateway

AMS does not manage the network setup of Customer Managed accounts (CMAs). You have the option of managing your own network using AWS APIs (see Networking Solutions) or connecting to the multi-account landing zone network managed by AMS, using the existing Transit Gateway (TGW) deployed in AMS MALZ.

> **Note**
> You can only have a VPC attached to the TGW if the CMA is in the same AWS Region. For more information see Transit gateways.

To add your CMA to Transit Gateway, request a new route (use the Management | 0ther | Other | Create ct-1e1xtak34nx76) change type and include this information:

- CMA account number
- Transit Gateway ID
- TGW attachment ID from CMA account (for example, `tgw-attach-04eb40d1e14ec7272`
- CMA route table ID (for example, `rtb-0ff4d759eb28b2a05`

Create routes in the TGW route tables to connect to this VPC:

1. By default this VPC will not be able to communicate with any of the other VPCs in your MALZ network.
2. Decide with your solutions architect what VPCs you want this Customer Managed VPC to communicate with. Submit a Management | Other | Other | Update RFC against the Networking account to create the TGW routes you need. Include the CMA Account Number, Transit Gateway ID, TWG Attachment ID from the CMA account (e.g. tgw-attach-12345678901234567), and the CMA Route Table ID (e.g. rtb-12345678901234567).

Connecting a new customer-managed VPC to the AMS Multi-Account Landing Zone network (creating a TGW VPC attachment):

1. In your multi-account landing zone Networking account, open the Amazon VPC console.
2. On the navigation pane, choose **Transit Gateways**. Record the TGW ID of the transit gateway you see.
3. Open the Amazon VPC console.
4. In the navigation pane, choose **Transit Gateway Attachments** > **Create Transit Gateway Attachment**. Make these choices:
    a. For the **Transit Gateway ID**, choose the transit gateway ID you recorded in Step 2.
    b. For **Attachment type**, choose **VPC**.
    c. Under **VPC Attachment**, optionally type a name for **Attachment name tag**.
    d. Choose whether to enable **DNS Support** and **IPv6 Support**.
    e. For **VPC ID**, choose the VPC to attach to the transit gateway. This VPC must have at least one subnet associated with it.
    f. For **Subnet IDs**, select one subnet for each Availability Zone to be used by the transit gateway to route traffic. You must select at least one subnet. You can select only one subnet per Availability Zone.
5. Choose **Create attachment**. Record the ID of the newly created TGW Attachment.

Associating the TGW attachment to a route table:

Decide which TGW route table you want to associate the VPC with. We recommend creating a new application route table for Customer Managed VPCs. Submit a Management | Other | Other | Update RFC on the Networking account to associate the VPC or TGW attachment to the route table you select.

Create routes in the TGW route tables to connect to this VPC:

1. By default, this VPC will not be able to communicate with any of the other VPCs in your Multi-Account Landing Zone network.
2. Decide with your solutions architect what VPCs you want this customer-managed VPC to communicate with. Submit a Management | Other | Other | Update RFC against the networking account to create the TGW routes you need.

Configuring your VPC Route tables to point at the AMS Multi-Account Landing Zone transit gateway:

Decide with your solutions architect what traffic you want to send to the AMS Multi-Account Landing Zone transit gateway. Submit a Management | Other | Other | Update RFC against the networking account to create the TGW routes you need.

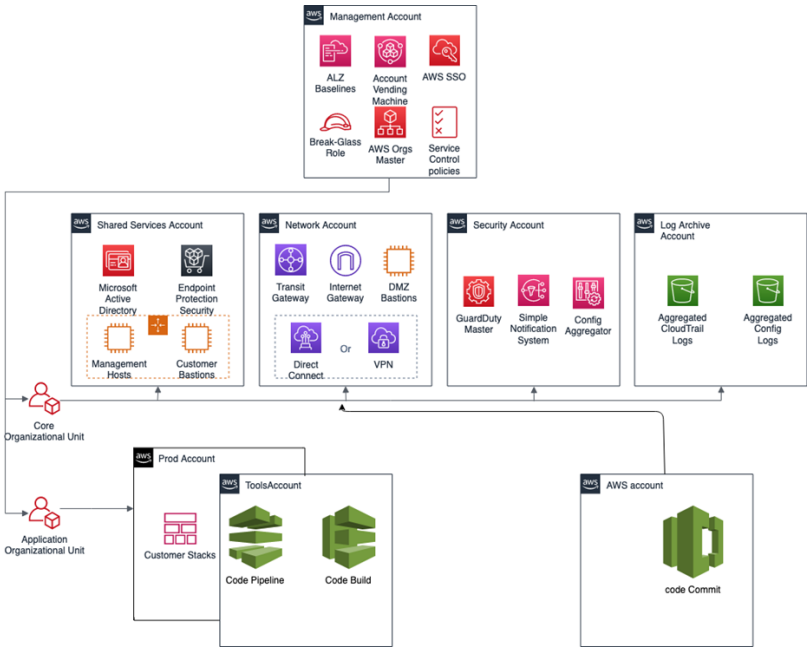
Tools account, Migrating Workloads: CloudEndure Landing Zone (MALZ)

Your Multi-Account Landing Zone tools account (with VPC) helps accelerate migration efforts, increases your security position, reduces cost and complexity, and standardizes your usage pattern.

A tools account provides the following:

- A well-defined boundary for access to replication instances for system integrators outside of your production workloads.
- Enables you to create an isolated chamber to check a workload for malware, or unknown network routes, before placing it into an account with other workloads.
- As a defined account setup, it provides faster time to onboard and get set up for migrating workloads.
- Isolated network routes to secure traffic from on-premise -> CloudEndure -> Tools account -> AMS ingested image. Once an image has been ingested, you can share the image to the destination account via an AMS Management | Advanced stack components | AMI | Share (ct-1eiczxw8ihc18) RFC.

High level architecture diagram:



Use the Deployment | Managed landing zone | Management account | Create tools account (with VPC) change type (ct-2j7q1hgf26x5c), to quickly deploy a tools account and instantiate a Workload Ingestion process within a Multi-Account Landing Zone environment. See Management account, Tools account: Creating (with VPC).

Note
We recommend having two availability zones (AZs), since this is a migration hub.
By default, AMS creates the following two security groups (SGs) in every account. Confirm the that the two SGs are present, and, if not, open a new Management | Other | Other | Create CT (ct-1e1xtak34nx76) to request them:

- SentinelDefaultSecurityGroupPrivateOnlyEgressAll
- InitialGarden-SentinelDefaultSecurityGroupPrivateOnly

Ensure that CloudEndure replication instances are created in the private subnet where there are routes back to on-premise. You can confirm that by ensuring that the route tables for the private subnet has a default route back to TGW. However, performing a CloudEndure machine cut over should go into the "isolated" private subnet where there is no route back to on-premise, only Internet outbound traffic is allowed. It is critical to ensure cutover occurs in the isolated subnet to avoid potential issues to the on-premise resources.

Prerequisites:

1. Either **Plus** or **Premium** support level.
2. The application account IDs for the KMS key where the AMIs are deployed.
3. The tools account, created as described previously.

AWS Application Migration Service (AWS MGN)

AWS Application Migration Service (AWS MGN) can be used in your MALZ Tools account through the CustomerMigrationAccessRole IAM role that is created automatically during Tools account provisioning. You can use AWS MGN to migrate applications and databases that run on supported versions of Windows and Linux operating systems.

For the most up-to-date information on AWS Region support, see the AWS Regional Services List.

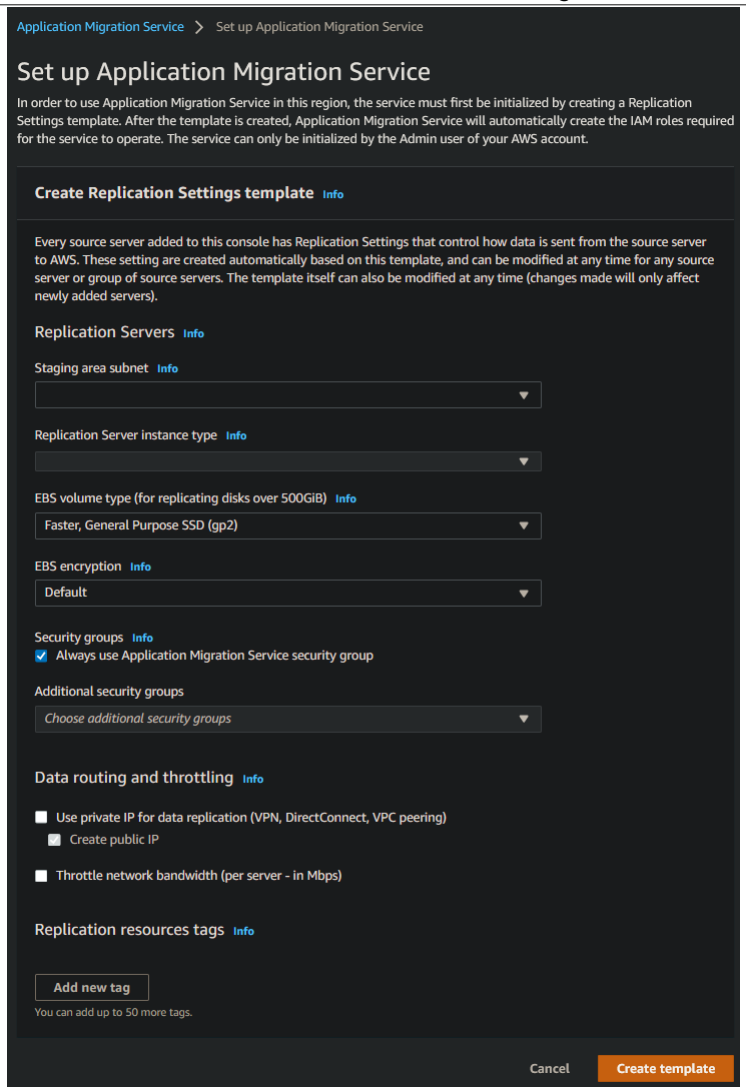
If your preferred AWS Region is not currently supported by AWS MGN, or the operating system on which your applications run is not currently supported by AWS MGN, consider using the CloudEndure Migration in your Tools account instead.

Requesting AWS MGN Initialization

AWS MGN must be initialized by AMS before first use. To request this for a new Tools account, submit a Management | Other | Other RFC from the Tools account with these details:

```
RFC Subject=Please initialize AWS MGN in this account
RFC Comment=Please click 'Get started' on the MGN welcome page here:

    https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome using all
 default values
    to 'Create template' and complete the initialization process.
```

Once AMS successfully completes the RFC and initializes AWS MGN in your Tools account, you can use CustomerMigrationAccessRole to edit the default template for your requirements.



Enable access to the new Tools account

Once the tools account is created, AMS provides you with an account ID. Your next step is to configure access to the new account. Follow these steps.

1. Update the appropriate Active Directory groups to the appropriate account IDs.

   New AMS-created accounts are provisioned with the ReadOnly role policy as well as a role to allow users to file RFCs.

   The tools account also has these additional IAM roles available:

   - AMS Migration role
   - CloudEndure user role
2. Request policies and roles to allow service integration team members to set up the next level of tools.

   Navigate to the AMS console and file the following RFCs:

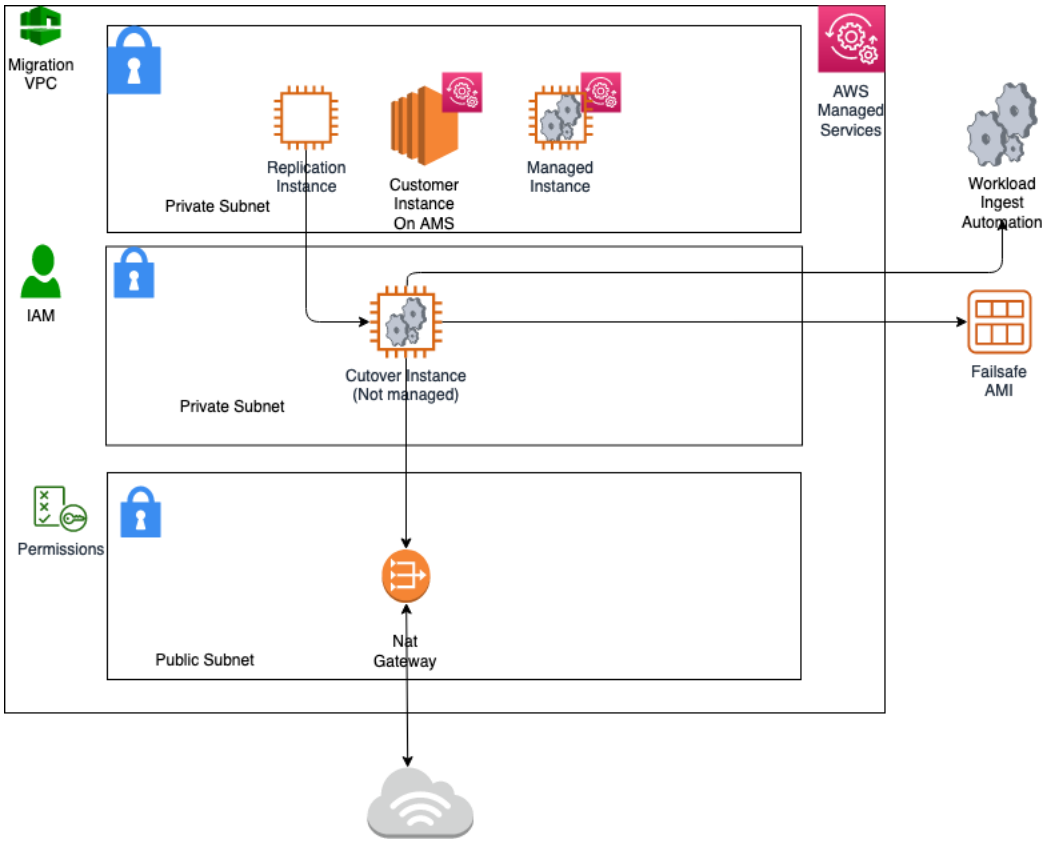
   a. Create KMS key. Use either Create KMS Key (auto) or Create KMS Key (review required).

As you use KMS to encrypt ingested resources, using a single KMS key that is shared with the rest of the Multi-Account Landing Zone application accounts, provides security for ingested images where they can be decrypted in the destination account.

b. Share the KMS key.

Use the Management | Other | Other | Create (ct-1e1xtak34nx76) change type to request that the new KMS key be shared with your application accounts where ingested AMIs will reside.

Example graphic of a final account setup:



Example policy

To see an AMS pre-approved IAM CloudEndure policy: Unpack the WIGS Cloud Endure Landing Zone Example file and open the `customer_cloud_endure_policy.json`.

Testing connectivity and end-to-end setup

To test the tools account, follow these steps.

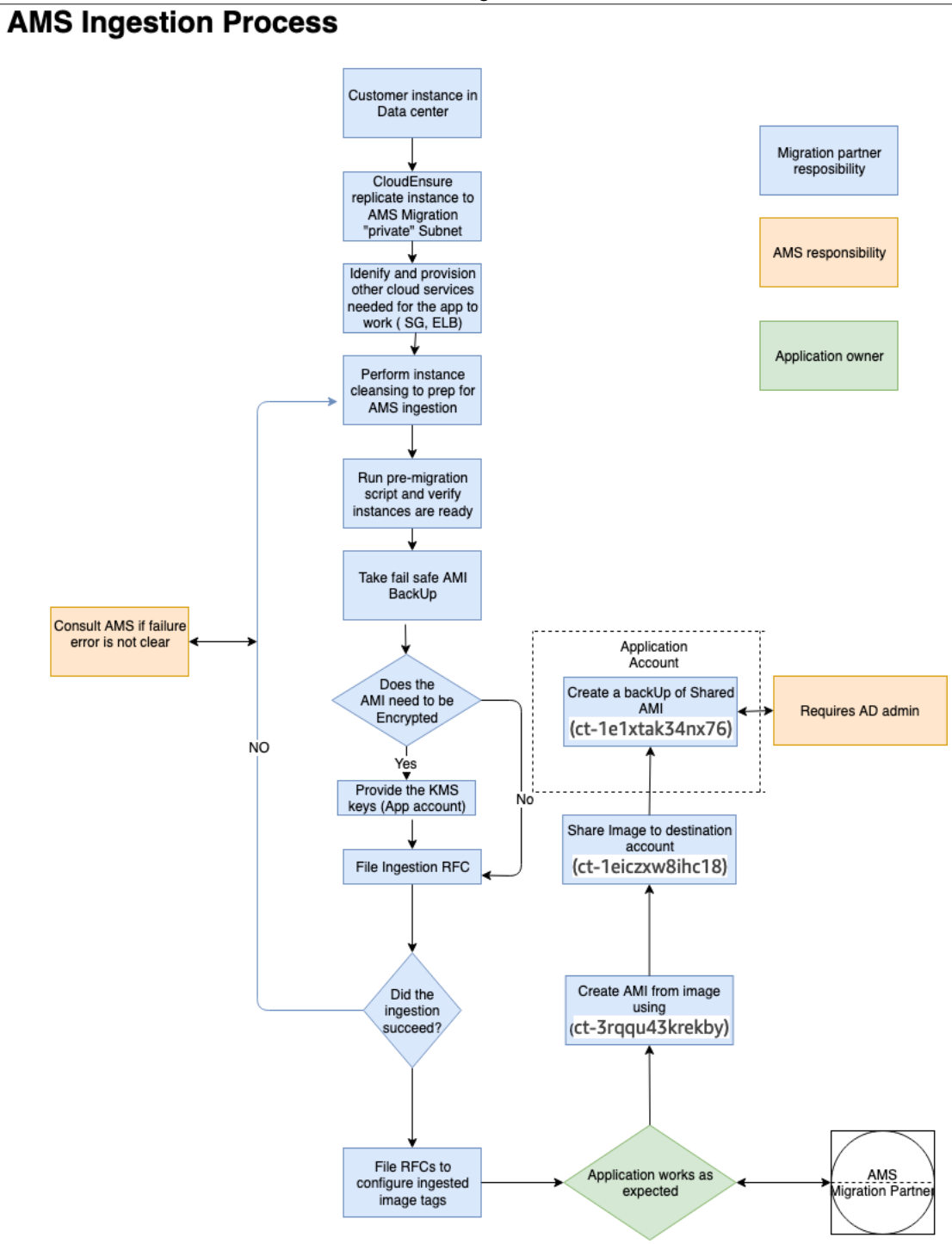
1. Start with configuring CloudEndure and installing the CloudEndure agent on a server that will replicate to AMS.
2. Create a project in CloudEndure.
3. Enter the AWS credentials shared when you performed the prerequisites, though secrets manager.
4. In **Replication settings**:
   a. Select both AMS "Sentinel" security groups (Private Only and EgressAll) for the **Choose the Security Groups to apply to the Replication Servers** option.

b. Define cutover options for the machines (instances). For information, see Step 5. Cut over

c. **Subnet**: Private subnet.

5. **Security Group**:
   a. Select both AMS "Sentinel" security groups (Private Only and EgressAll).
   b. Cutover instances have to communicate to the AMS-managed Active Directory (MAD) and to AWS public endpoints:
      i. **Elastic IP**: None
      ii. **Public IP**: no
      iii. **IAM role**: customer-mc-ec2-instance-profile
   c. Set tags as per your internal tagging convention.
6. Install the CloudEndure agent on the machine and look for the replication instance to come up in your AMS account in the EC2 console.

The AMS ingestion process:



Tools account hygiene

You'll want to clean up after you are done in the account have shared the AMI and no longer have a need for the replicated instances:

- Post instance WIGs ingestion:

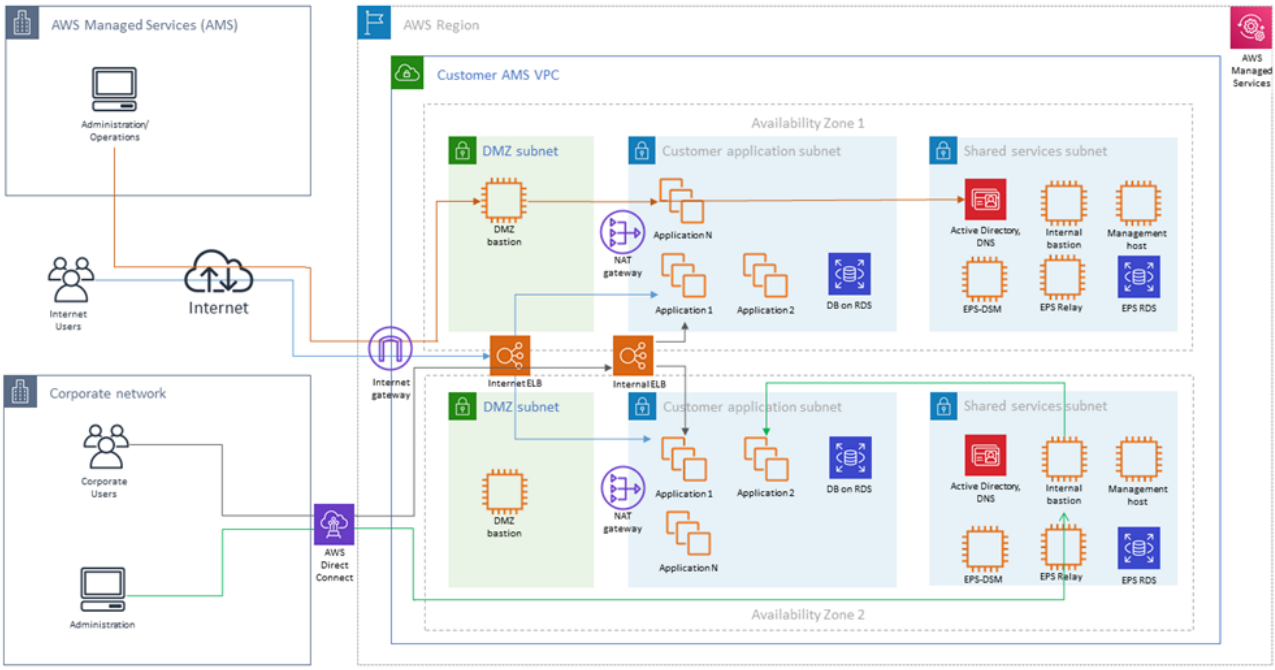
  - Cutover instance: At a minimum, stop or terminate this instance, after the work has been completed, via the AWS console
  - Pre-Ingestion AMI backups: Remove once the instance has been ingested and the on-premise instance terminated
  - AMS-ingested instances: Turn off the stack or terminate once the AMI has been shared
  - AMS-ingested AMIs: Delete once sharing with the destination account is completed
- End of migration clean up: Document the resources deployed via DevMode to ensure clean-up happens on regular basis, for example:
  - Security groups
  - Resources created via Cloud-formation
  - Network ACK
  - Subnet
  - VPC
  - Route Table
  - Roles
  - User Accounts

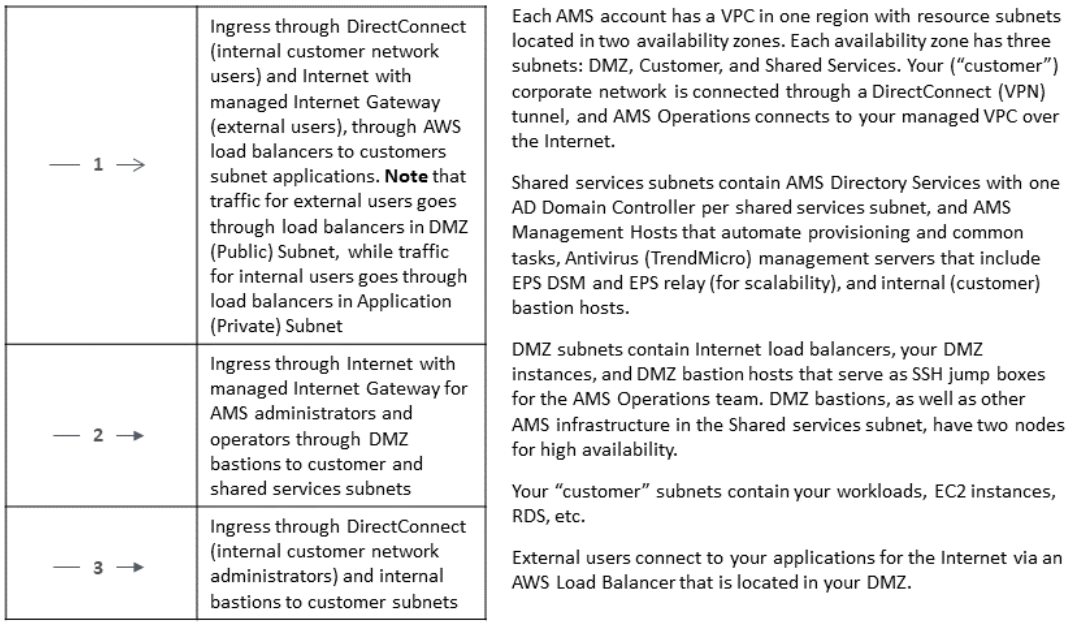
Migration at scale - Migration Factory

See Introducing AWS CloudEndure Migration Factory Solution.

Single-Account Landing Zone network architecture

The following diagram depicts the AMS single-account landing zone VPC network layout and is an example of the highly available setup.





AMS configures all aspects of networking for you based on our standard templates and your selected options provided during onboarding. A standard AWS network design is applied to your AWS account, and a virtual private cloud (VPC) is created for you and connected to AMS by either VPN or Direct Connect. Learn more about Direct Connect at AWS Direct Connect. Standard VPCs include the DMZ, shared services, and an application subnet. During the onboarding process, additional VPCs might be requested and created to match your needs (for example, customer divisions, partners). After onboarding, you're provided with a network diagram. an environment document that explains how your network has been set up.

> **Note**
> To learn about default service limits and constraints for all active services, see the AWS Service Limits documentation.

Our network design is built around the Amazon "Principle of Least Privilege". In order to accomplish this, we route all traffic, inbound and outbound, through a per, except traffic coming from a trusted network. The only trusted network is the one configured between your on-premises environment and the VPC through the use of a VPN and/or an AWS Direct Connect (DX). Access is granted through the use of bastion instances, thereby preventing direct access to any production resources. All of your applications and resources reside inside private subnets that are reachable through public load balancers. Public egress traffic flows through our forward proxies to the Internet Gateway and then to the Internet. Alternatively, the traffic can flow over your VPN or Direct Connect to your on-premises environment.

AMS Single-account landing zone shared services

Shared services subnets contain AMS Directory Services, the Management Host that automates provisioning and common tasks, antivirus (TrendMicro) management server, and internal bastion hosts:

- AMS Directory Services = AD Domain Controller

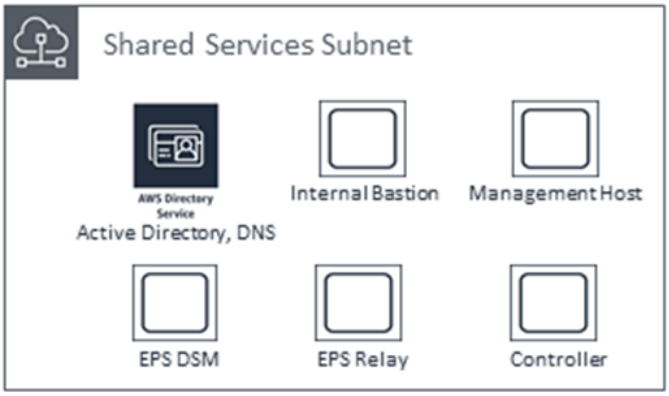
  Creates an Active Directory in AMS accounts, creates the AMS domain, joins managed stacks to the domain on launch.
- Management hosts = AMS Management Host (automate provisioning and common tasks)

Act as an API endpoint to modify AWS Directory Service, interact with AWS Directory Service domain controllers.

- Security services: Antivirus (TrendMicro) management server = EPS DSM + EPS Relay

  Leverages Trend Micro™ Deep Security software (DSM), operates in a client-server model and has a back-end database, includes Deep Security managers, agents, and relays.
- Internal bastion hosts = Customer bastions

  Special purpose servers designed to be the primary access point from the Internet and act as a proxy to your other Amazon EC2 instances.



AMS default settings

Topics

Your AWS Managed Services (AMS) network is configured in a standardized manner with defaults for most services.

This section describes the default settings that AMS uses for access, monitoring, and logging, management.

For an example of multi-account landing zone or single-account landing zone infrastructure costs, see AMS environment basic components (p. 11).

DNS resolution defaults, Multi-Account Landing Zone only

In AWS environments, domain name system (DNS) resolution between Route 53 Resolver and DNS resolvers in a VPC can be integrated by configuring Resolver forwarding rules. Before these rules can be used for forwarding DNS queries, inbound and outbound resolver endpoints need to be set up to which these queries can be forwarded.

By default, DNS queries within application account VPCs in multi-account settings in AMS are forwarded to the conditional forwarders of the AWS Directory Service for Microsoft Active Directory (also known as Managed AD) domain present in the shared services account. AMS optionally enables you to make use of the AmazonProvidedDNS; for example, AmazonProvidedDNS to forward DNS queries to. This helps you utilize VPC endpoints that today only support Amazon-provided DNS through Amazon Route 53. Correspondingly, Resolver Rules are also automatically set up for common VPC endpoints that are deployed by default in the shared services account. For more information on these common VPC endpoints, see AMS VPC endpoints (p. 34).

To configure Dynamic Host Configuration Protocol (DHCP) Option Sets in all of your application account VPCs to use Amazon-provided DNS for VPC endpoints, and have Route53 Resolver rules pointing to the common VPC endpoints in your shared services accounts (with an optional Resolver Rule for on-premises domain), create a Management | Other | Other | Create request for change (RFC) specifying the shared services account, and requesting enablement of the application account VPC local DNS and Route 53 Resolver rules for VPC endpoints.

EC2 IAM instance profile

An instance profile is a container for an IAM role that you can use to pass role information to an EC2 instance when the instance starts.

MALZ

Currently there are two AMS default instance profiles, `customer-mc-ec2-instance-profile` and `customer-mc-ec2-instance-profile-s3`, these instance profiles provide the permissions described in the following table.

Policy descriptions

Profile	Policies
`customer-mc-ec2-instance-profile`	`AMSInstanceProfileLoggingPolicy`: Allows Ec2 instances to push logs to S3 and CloudWatch.
	`AMSInstanceProfileManagementPolicy`: Allows Ec2 instances to perform booting actions, like joining Active Directory.
	`AMSInstanceProfileMonitoringPolicy`: Allows Ec2 instances to report findings to AMS monitoring services.
	`AMSInstanceProfilePatchPolicy`: Allows Ec2 instances to receive patches.
`customer-mc-ec2-instance-profile-s3`	`AMSInstanceProfileLoggingPolicy`: Allows Ec2 instances to push logs to S3 and CloudWatch.
	`AMSInstanceProfileManagementPolicy`: Allows Ec2 instances to perform booting actions, like joining Active Directory.
	`AMSInstanceProfileMonitoringPolicy`: Allows Ec2 instances to report findings to AMS monitoring services.
	`AMSInstanceProfilePatchPolicy`: Allows Ec2 instances to receive patches.
	`AMSInstanceProfileS3WritePolicy`: Allows Ec2 instances to read/write to customer S3 buckets.

SALZ

Currently there is one AMS default instance profile, `customer-mc-ec2-instance-profile`, this instance profile provides the permissions described in the following table. The profile grants permissions to the applications. running on the instance, not to users logging into the instance.

Policies often include multiple statements, where each statement grants permissions to a different set of resources or grants permissions under a specific condition.

CW = CloudWatch. ARN = Amazon Resource Name. * = wildcard (any).

EC2 default IAM instance profile permissions

CW = CloudWatch. ARN = Amazon Resource Name. * = wildcard (any).			
Amazon Elastic Compute Cloud (Amazon EC2)			
EC2 Message Actions	Allow	AcknowledgeMessage, DeleteMessage, FailMessage, GetEndpoint, GetMessages,	Allows EC2 Systems Manager messaging actions in your account.

CW = CloudWatch. ARN = Amazon Resource Name. * = wildcard (any).			
		SendReply	
Ec2 Describe	Allow	* (All)	Allows the console to display configuration details of an EC2 in your account.
Iam Get Role ID	Allow	GetRole	Allows EC2 to get your IAM ID from `aws:iam::*:role/customer-*` and `aws:iam::*:role/customer_*`.
Instance To Upload Log Events	Allow	Create Log Group	Allows logs to be created in: `aws:logs:*:*:log-group:i-*`
		Create Log Stream	Allows logs to be streamed to: `aws:logs:*:*:log-group:i-*`
CW For MMS	Allow	DescribeAlarms, PutMetricAlarm, PutMetricData	Allows CloudWatch to retrieve alarms in your account. Allows CW to create or update an alarm and associate it with the specified metric. Allows CW to publish metric data points to your account.
Ec2 Tags	Allow	CreateTags, DescribeTags,	Allows tags to be added, overwritten, and described on the specified instances in your account.
Explicitly Deny CW Logs	Deny	DescribeLogStreams, FilterLogEvents, GetLogEvents	Disallows listing, filtering, or getting the log streams for: `aws:logs:*:*:log-group:/mc/*`
Amazon EC2 Simple Systems Manager (SSM)			
SSM Actions	Allow	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	Allows a variety of SSM functions in your account.
SSM Access In S3	Allow	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadPorts, ListBucketMultipartUploads	Allows the SSM on the EC2 to get and update objects in, and to abort a multi-part object upload to, and list ports and buckets available for, multi-part uploads in `aws:s3:::mc-*-internal-*/aws/ssm*`.

CW = CloudWatch. ARN = Amazon Resource Name. * = wildcard (any).			
Amazon EC2 Simple Storage Service (S3)			
Get Object In S3	Allow	Get List	Allows EC2 applications to retrieve and list objects in S3 buckets in your account.
Customer Encrypted Log S3 Access	Allow	PutObject	Allows EC2 applications to update objects in `aws:s3:::mc-*-logs-*/encrypted/app/*`
Patch Data Put Object S3	Allow	PutObject	Allows EC2 applications to upload patching data to your S3 buckets at `aws:s3:::awsms-a*-patch-data-*`
Uploading Own Logs To S3	Allow	PutObject	Allows EC2 applications to upload custom logs to: `aws:s3:::mc-a*-logs-*/aws/instances/*/${aws:userid}/*`
Explicitly Deny MC Namespace S3 Logs	Deny	GetObject* Put*	Disallows EC2 applications getting or putting any objects from or to: `aws:s3:::mc-*-logs-*/encrypted/mc*`, `aws:s3:::mc-*-logs-*/mc/*`, `aws:s3:::mc-a*-logs-*-audit/*`
Explicitly Deny S3 Delete	Deny	* (all)	Disallows EC2 applications taking any action on objects in: `aws:s3:::mc-a*-logs-*/*`, `aws:s3:::mc-a*-internal-*/*`,
Explicitly Deny S3 CFN Bucket	Deny	Delete*	Disallows EC2 applications deleting any objects from: `aws:s3:::cf-templates-*`
Explicitly Deny List Bucket S3	Deny	ListBucket	Disallows you listing any encrypted, audit log, or reserved (mc) objects from: `aws:s3:::mc-*-logs-*`

If you're unfamiliar with Amazon IAM policies, see Overview of IAM Policies for important information.

Note
Policies often include multiple statements, where each statement grants permissions to a different set of resources or grants permissions under a specific condition.

Alerts from baseline monitoring in AMS

This section describes AMS monitoring defaults; for more information, see Monitoring and event management (p. 295).

The following table shows what is monitored and the default alerting thresholds. You can change the alerting thresholds with a Management | Other | Other | Update (ct-0xdawir96cy7k) RFC after determining what changes you want and subscribing to the relevant CloudWatch Amazon SNS topic. For information about creating and subscribing to topics, see Subscribe to a Topic. For general information, see Amazon SNS FAQs. To be notified directly when alarms cross their threshold, in addition to AMS's standard alerting process, follow these instructions about how to overwrite alarm configurations, Receiving alerts generated by AMS (p. 300).

Amazon CloudWatch provides extended retention of metrics. For more information, see CloudWatch Limits.

> **Note**
> AMS calibrates its baseline monitoring on a periodic basis. New accounts are always onboarded with the latest baseline monitoring and the table describes the baseline monitoring for an account that is newly onboarded. AMS updates the baseline monitoring in existing accounts on a periodic basis and you may experience a time lag before the updates are in place. For more information, see Viewing the monitoring configuration for an account (p. 298).

Alerts from baseline monitoring

Resource	Security alert	Alert name and trigger condition	Notes
For starred (*) alerts, AMS proactively assesses impact and remediates when possible; if remediation is not possible, AMS creates an incident. Where automation fails to remediate the issue, AMS informs you of the incident case and an AMS engineer is engaged. In addition, these alerts can be sent directly to your email (if you have opted in to the Direct-Customer-Alerts SNS topic).			
Application Load Balancer (ALB) instance	No	RejectedConnectionCount sum > 0 for 1 min, 5 consecutive times.	CloudWatch alarm if the number of connections that were rejected because the load balancer reached its maximum.
Application Load Balancer (ALB) target	No	TargetConnectionErrorCount sum > 0 for 1 min, 5 consecutive times.	CloudWatch alarm if number of connections were unsuccessfully established between the load balancer and the registered instances.
		HTTPCode_Target_5XX_Count sum > 0 for 1 min, 5 consecutive times.	CloudWatch alarm on excess number of HTTP 5XX response codes generated by the targets.
Aurora instance	No	CPUUtilization > 85% for 5 mins, 2 consecutive times.	CloudWatch alarm.
EC2 instance - all OSs	No	CPUUtilization* >= 95% for 5 mins, 6 consecutive times.	CloudWatch alarm. High CPU utilization is an indicator of a change in application state such as dead locks, infinite loops, malicious attacks, and other anomalies.
		StatusCheckFailed > 0 for 5 minutes, 3 consecutive times.	CloudWatch alarm.
		Root Volume Usage	

Resource	Security alert	Alert name and trigger condition	Notes
		>= 85% for 5 mins, 6 consecutive times.	
		Memory Free* MemoryFree < 5% for 5 minutes, 6 consecutive times.	
	Yes	EPS Malware Malware found on instance.	CloudWatch event.
Amazon EC2 instance - Linux	No	Root Volume Inode Usage Average >= 95% for 5 mins, 6 consecutive times.	CloudWatch alarm. Applied to Linux instances only.
		Swap Free* Memory Swap < 5% for 5 minutes, 6 consecutive times.	
ElastiCache Cluster	No	CurrConnections = 65000	This alarm notifies AMS of the maximum connection limit of an ElastiCache Host. CloudWatch Alarm. If you would like to update this threshold, contact AMS support.

Resource	Security alert	Alert name and trigger condition	Notes
ElastiCache Node	No	CPUUtilization Average > predefined value for 15 mins, 2 consecutive times.	CloudWatch alarm. Default is 90. If Redis, use one the following values based on instance type: • cache.t1.micro: 90% • cache.m1.small: 90% • cache.m1.medium: 90% • cache.m1.large: 45% • cache.m1.xlarge: 22.5% • cache.m2.xlarge: 45% • cache.m2.4xlarge: 11.25% • cache.c1.xlarge: 11.25% • cache.t2.micro: 90% • cache.t2.small: 90% • cache.t2.medium: 45% • cache.m3.medium: 90% • cache.m3.large: 45% • cache.m3.xlarge: 22.5% • cache.m3.2xlarge: 11.25% • cache.r3.large: 45% • cache.r3.xlarge: 22.5% • cache.r3.2xlarge: 11.25% • cache.r3.4xlarge: 5.625% • cache.r3.8xlarge: 2.8125%
ElastiCache Node - memcached	No	SwapUsage maximum > 50,000,000 bytes for 5 mins, 5 consecutive times.	CloudWatch alarm. Applied to memcached only.
OpenSearch cluster	No	ClusterStatus.red maximum is >= 1 for 1 minute, 1 consecutive time. *AMS takes pro-active actions to reduce operational impact, when this alert is triggered.*	CloudWatch alarm. At least one primary shard and its replicas are not allocated to a node. To learn more, see Red Cluster Status.
OpenSearch domain	No	KMSKeyError >= 1 for 1 minute, 1 consecutive time.	CloudWatch alarm. The KMS encryption key that is used to encrypt data at rest in your domain is disabled. Re-enable it to restore normal operations. To learn more, see Encryption of Data at Rest for OpenSearch Service Service.

Resource	Security alert	Alert name and trigger condition	Notes
		ClusterStatus.yellow maximum is >= 1 for 1 minute, 1 consecutive time *AMS takes pro-active actions to reduce operational impact, when this alert is triggered.*	At least one replica shard is not allocated to a node. To learn more, see Yellow Cluster Status.
		FreeStorageSpace minimum is <= 20480 for 1 minute, 1 consecutive time *AMS takes pro-active actions to reduce operational impact, when this alert is triggered.*	A node in your cluster is down to 20 GiB of free storage space. To learn more, see Lack of Available Storage Space.
		ClusterIndexWritesBlocked >= 1 for 5 minutes, 1 consecutive time *AMS takes pro-active actions to reduce operational impact, when this alert is triggered.*	The cluster is blocking write requests. To learn more, see ClusterBlockException.
		Nodes minimum is < x for 1 day, 1 consecutive time *AMS takes pro-active actions to reduce operational impact, when this alert is triggered.*	x is the number of nodes in your cluster. This alarm indicates that at least one node in your cluster has been unreachable for one day. To learn more, see Failed Cluster Nodes.
		CPUUtilization average is >= 80% for 15 minutes, 3 consecutive times *AMS takes pro-active actions to reduce operational impact, when this alert is triggered.*	100% CPU utilization is common, but sustained high averages are problematic. Consider using larger instance types or adding instances.
		JVMMemoryPressure maximum is >= 80% for 5 minutes, 3 consecutive times *AMS takes pro-active actions to reduce operational impact, when this alert is triggered.*	The cluster could encounter out of memory errors if usage increases. Consider scaling vertically. Amazon ES uses half of an instance's RAM for the Java heap, up to a heap size of 32 GiB. You can scale instances vertically up to 64 GiB of RAM, at which point you can scale horizontally by adding instances.

Resource	Security alert	Alert name and trigger condition	Notes
		MasterCPUUtilization average is >= 50% for 15 minutes, 3 consecutive times *AMS takes pro-active actions to reduce operational impact, when this alert is triggered.*	Consider using larger instance types for your dedicated master nodes. Because of their role in cluster stability and blue/green deployments, dedicated master nodes should have lower average CPU usage than data nodes.
		MasterJVMMemoryPressure maximum is >= 80% for 15 minutes, 1 consecutive time *AMS takes pro-active actions to reduce operational impact, when this alert is triggered.*	Consider using larger instance types for your dedicated master nodes. Because of their role in cluster stability and blue/green deployments, dedicated master nodes should have lower average CPU usage than data nodes.
OpenSearch instance	No	AutomatedSnapshotFailure maximum is >= 1 for 1 minute, 1 consecutive time.	CloudWatch alarm. An automated snapshot failed. This failure is often the result of a red cluster health status. See Red Cluster Status.
Elastic Load Balancing instance	No	SurgeQueueLength > 100 for 1 minute, 15 consecutive times.	CloudWatch alarm if an excess number of requests are pending routing.
		SpilloverCount > 1 for 1 minute, 15 consecutive times.	CloudWatch alarm if an excess number of requests that were rejected because the surge queue is full.
GuardDuty service	Yes	Not applicable; all findings (threat purposes) are monitored. Each finding corresponds to an alert.	List of supported GuardDuty finding types are on GuardDuty Active Finding Types.
Health	Varies	Changes in the GuardDuty findings. These changes include newly generated findings or subsequent occurrences of existing findings.	Notifications sent when there are changes in the status of AWS Personal Health Dashboard (AWS Health) events. Service event. Example: Scheduled EC2 instance store retirement.
AWS Managed Microsoft AD	No	Active Directory Status AWS Managed Microsoft AD instance sends an active status event.	Service event. Emitted when the directory is operating normally after an event.

Resource	Security alert	Alert name and trigger condition	Notes
		Impaired Directory Status AWS Managed Microsoft AD instance sends an impaired directory status event.	Service event. Emitted when the directory is running in a degraded state. One or more issues have been detected, and not all directory operations may be working at full operational capacity.
		Inoperable Directory Status AWS Managed Microsoft AD instance sends an inoperable status event.	Service event. Emitted when the directory is not functional. All directory endpoints have reported issues.
		Deleting Directory Status AWS Managed Microsoft AD instance sends a deleting directory status event.	Service event. Emitted when the directory is currently being deleted.
		Failed Directory Status AWS Managed Microsoft AD instance sends a failed status event.	Service event. Emitted when the directory could not be created.
		RestoreFailed Directory Status AWS Managed Microsoft AD instance sends a restore failed directory status event.	Service event. Emitted when restoring the directory from a snapshot failed.
Amazon RDS instance	No	Failover not attempted Amazon RDS is not attempting a requested failover because a failover recently occurred on the DB instance.	Service event. RDS-EVENT-0034, Amazon RDS Event Categories and Event Messages.
		DB instance partial failover recovery complete The instance has recovered from a partial failover.	Service event. RDS-EVENT-0065, Amazon RDS Event Categories and Event Messages.
		DB instance fail The DB instance has failed due to an incompatible configuration or an underlying storage issue. Begin a point-in-time-restore for the DB instance.	Service event. RDS-EVENT-0031, Amazon RDS Event Categories and Event Messages.
		Invalid subnet IDs DB instance The DB instance is in an incompatible network. Some of the specified subnet IDs are invalid or do not exist.	Service event. RDS-EVENT-0036, Amazon RDS Event Categories and Event Messages.

Resource	Security alert	Alert name and trigger condition	Notes
		DB instance invalid parameters For example, MySQL could not start because a memory-related parameter is set too high for this instance class, so the customer action would be to modify the memory parameter and reboot the DB instance.	Service event. RDS-EVENT-0035, Amazon RDS Event Categories and Event Messages.
		Error create statspack user account Error while creating Statspack user account PERFSTAT. Drop the account before adding the Statspack option.	Service event. RDS-EVENT-0058, Amazon RDS Event Categories and Event Messages.
		DB instance without enhanced monitoring Enhanced Monitoring can't be enabled without the enhanced monitoring IAM role. For information about creating the enhanced monitoring IAM role, see To create an IAM role for Amazon RDS Enhanced Monitoring.	Service event. RDS-EVENT-0079, Amazon RDS Event Categories and Event Messages.
		DB instance enhanced monitoring disabled Enhanced Monitoring was disabled due to an error making the configuration change. It's likely that the enhanced monitoring IAM role is configured incorrectly. For information about creating the enhanced monitoring IAM role, see To create an IAM role for Amazon RDS Enhanced Monitoring.	Service event. RDS-EVENT-0080, Amazon RDS Event Categories and Event Messages.
		Invalid permissions recovery S3 bucket The IAM role that you use to access your Amazon S3 bucket for SQL Server native backup and restore is configured incorrectly. For more information, see Setting Up for Native Backup and Restore.	Service event. RDS-EVENT-0081, Amazon RDS Event Categories and Event Messages.
		DB instance read replica error An error has occurred in the read replication process. For more information, see the event message. For information on troubleshooting Read Replica errors, see Troubleshooting a MySQL Read Replica Problem.	Service event. RDS-EVENT-0045, Amazon RDS Event Categories and Event Messages.

Resource	Security alert	Alert name and trigger condition	Notes
		DB instance read replication ended Replication on the Read Replica was ended.	Service event. RDS-EVENT-0057, Amazon RDS Event Categories and Event Messages.
		DB instance recovery start The SQL Server DB instance is re-establishing its mirror. Performance will be degraded until the mirror is reestablished. A database was found with non-FULL recovery model. The recovery model was changed back to FULL and mirroring recovery was started. (<dbname>: <recovery model found>[,...])".	Service event. RDS-EVENT-0066, Amazon RDS Event Categories and Event Messages.
		Low Storage alert triggers when the allocated storage for the DB instance has been exhausted.	RDS-EVENT-0007, see details at Using Amazon RDS event notification.
		Low storage alert when the DB instance has consumed more than 90% of its allocated storage	RDS-EVENT-0089, see details at Amazon RDS Event Categories and Event Messages.
		Notification service when scaling failed for the Aurora Serverless DB cluster.	RDS-EVENT-0143, see details at Amazon RDS Event Categories and Event Messages.
		CPUUtilization Average CPU utilization > 75% for 15 mins, 2 consecutive times.	CloudWatch alarm.
		DiskQueueDepth Sum is > 75 for 1 mins, 2 consecutive times.	
		FreeStorageSpace Average < 1,073,741,824 bytes for 5 mins, 2 consecutive times.	
		ReadLatency Average >= 1.001 seconds for 5 mins, 2 consecutive times.	
		WriteLatency Average >= 1.005 seconds for 5 mins, 2 consecutive times.	

Resource	Security alert	Alert name and trigger condition	Notes
		SwapUsage Average >= 104,857,600 bytes for 5 mins, 2 consecutive times.	
Amazon Redshift cluster	No	HealthStatus The health of the cluster <= 0 for 5 min, 1 consecutive times.	1 represents a healthy cluster.
		MaintenanceMode Cluster maintenance mode >= 1 for 5 min, 1 consecutive time.	1 represents ON state.
		ReadLatency The average time for disk read >= 1 for 5 min, 1 consecutive time.	None.
		WriteLatency The average time for disk write >= 1 for 5 min, 1 consecutive time.	None.
Amazon Macie	Yes	Newly generated alerts and updates to existing alerts. Macie finds any changes in the findings. These changes include newly generated findings or subsequent occurrences of existing findings.	Amazon Macie alert. For a list of supported Macie alert types, see Macie Alerts. Note that Macie is not configured for all accounts.

AMS takes pro-active actions (scaling the cluster) when this alert is triggered.

For information on remediation efforts, see AMS automatic remediation of alerts (p. 300).

Log retention and rotation defaults

This section describes AMS log management defaults; for more information, see Log Management.

- Rotation = Log turnover inside the instances
- Retention = Period of time we keep the logs in Amazon CloudWatch Logs and Amazon Simple Storage Service (S3)

The logs are retained in CloudWatch Logs as needed (you can configure this), and in S3. They don't expire or get deleted and are subject to service durability. For detailed S3 durability information, see Data protection in Amazon S3.

You can request a change to log retention for all logs, except AWS CloudTrail logs, which are kept indefinitely for audit and security reasons.

Log rotation is configured inside the instances. By default, operating system and security logs rotate hourly if they reach over 100MB, this is done to ensure that you don't run short on disk in the instances.

The log agent inside the instances uploads the log online to CloudWatch Logs, from there the logs are archived to S3.

The logs are stored in CloudWatch Logs and S3 in the raw format they are generated, there is no pre-processing.

Setting up AMS

Topics

Some AMS setup tasks might be completed at onboarding.

For a full description of roles and responsibilities, including the AMS Supported AWS services (p. 25), see AMS responsibility matrix (RACI) (p. 16).

> **Note**
> To request that AMS provide an additional AWS service, file a service request. For information about how to make this request, see Service request management (p. 275).

Using the AMS consoles

The AMS consoles in the AWS Management Console are available for you to interact with AMS and operate your AMS Advanced-managed and AMS Accelerate resources. The AMS consoles generally behave like any AWS console; however, because AMS is a private organization, only accounts enabled for AMS can access the console. Once AMS is enabled in your account, you can access the console by searching for "Managed Services" in the unified search bar.

> **Note**
> Depending on your account role, you access the AMS Advanced console or the AMS Accelerate console.

When using the AMS consoles, be aware of the following caveats:

- The AMS console is account specific. So, if you are in a "Test" account for your organization, you won't be able to see resources in the "Prod" account for that organization. Likewise, you must have an AMS Advanced role to access the AMS Advanced console.
- The AMS consoles apply an IAM policy when you authenticate that determines which console you can access and what you can do there. Your administrator may apply additional polices to the default AMS policy to restrict what you can see and do in the console.

The AMS Advanced console has these features:

- Opening page: The opening page has information boxes and links to facilitate your access to your existing RFCs, incidents, service request, and reports.

- Feature pages, links in the left-hand navigation pane:
  - **Dashboard**: Provides an overview of the current status of your account including:
    - **Requests for change**: See how many RFCs are **Awaiting your response**, and jump to the RFC list page with that filter active. See how many RFCs are **Awaiting your approval**, and jump to the RFC list page with that filter active. See how many RFCs are **Open**, and jump to the RFC list page with that filter active. Open the list page for RFCs by clicking the **View all** link.
    - **Incidents**: See how many incident cases are **Awaiting your response**, and jump to the incident list page with that filter active. See and how many are **Open**, and jump to the incident list page with that filter active. Open the incident list page by clicking the **View all** link.
    - **Service requests**: See how many service requests are **Awaiting your response**, and jump to the service request list page with that filter active. See and how many are **Open**, and jump to the service request list page with that filter active. Open the service request list page by clicking the **View all** link.
    - **Recently updated RFCs**: Date, link to the RFC details, and status
    - **Recently created incidents and service requests**: Date, link to the case details, and type (incident or service request)
  - **RFCs**: Opens a list of the existing RFCs for the account
  - **Incidents**: Opens a list of the open incidents for the account
  - **Service requests**: Opens a list of the open service requests for the account
  - **Reports**: Opens the Reports page and the default reports, **Daily Backup** and **Daily Patch** and **Monthly Billling**
  - **Resources**:
    - **VPCs**: Opens a list of the existing VPCs for the account
    - **Stacks**: Opens a list of existing stacks for the account
    - **AMIs**: Opens a list of available AMS AMIs
- **Feature spotlight**: Information on the latest updates to the console
- **Developer's Resources**: A page of downloadable files, including the AMS Advanced change management SDK and more
- **Documentation**: The AWS Managed Services documentation landing page

Using the AMS API and CLI

The AWS Managed Services (AMS) API is similar to the APIs for other AWS services. You can read about the AMS API in the AMS API Reference.

AMS API HTTP endpoints for REST calls

Besides the various SDKs, AMS provides a CLI; you can also invoke REST API calls against the AMS endpoint.

There are two AMS APIs (the endpoint for both resides in us-east-1):

- Change Management: Use this API to request access to or changes to your infrastructure, including creating and updating RFCs, deploying new instances, updating and deleting instances, getting information on CTs, and creating AMIs. The HTTP endpoint is:

  ```
  https://amscm.us-east-1.amazonaws.com
  ```
- SKMS: Use this API to get information about your infrastructure, including VPCs, stacks, subnets, and AMIs. The HTTP endpoint is:

  ```
  https://amsskms.us-east-1.amazonaws.com
  ```

Installing or upgrading the AMS CLI

The AMS CLI is an easy way to interact with the AMS API and is used in the examples in this section. For usage conventions for the AWS CLI and AMS CLI, see Using the AWS command Line Interface.

For information on installing SAML, see Appendix: ActiveDirectory Federation Services (ADFS) claim rule and SAML settings (p. 385).

To install or upgrade the AMS CLI, follow these instructions:

> **Note**
> You must have administrator credentials for this procedure.

The AWS CLI is a prerequisite for using the AMS CLIs (Change Management and SKMS).

1. To install the AWS CLI, see Installing the AWS Command Line Interface, and follow the appropriate instructions. Note that at the bottom of that page there are instructions for using different installers, Linux, MS Windows, macOS, Virtual Environment, Bundled Installer (Linux, macOS, or Unix).

   After the installation, run `aws help` to verify the installation.
2. Once the AWS CLI is installed, to install or upgrade the AMS CLI, download either the AMS **AMS CLI** or **AMS SDK** distributables zip file and unzip. You can access the AMS CLI distributables through the **Documentation** link in the left nav of the AMS console, or ask your cloud service delivery manager (CSDM) to send you the zip file.
3. The README file provides instructions for any install.

   Open either:

   - CLI zip: Provides the AMS CLI only.
   - SDK zip: Provides all of the AMS APIs and the AMS CLI.

   For **Windows**, run the appropriate installer (only 32 or 64 bits systems):

   - 32 Bits: **ManagedCloudAPI_x86.msi**
   - 64 Bits: **ManagedCloudAPI_x64.msi**

   For **Mac/Linux**, run the file named: **MC_CLI.sh** by running this command: `sh MC_CLI.sh`. Note that the **amscm** and **amsskms** directories and their contents must be in the same directory as the **MC_CLI.sh** file.
4. If your corporate credentials are used via federation with AWS (the AMS default configuration) you must install a credential management tool that can access your federation service. For example, you can use this AWS Security Blog How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS for help configuring your credential management tooling.
5. After the installation, run `aws amscm help` and `aws amsskms help` to see commands and options.

Using the AMS API in CLI, Ruby, Python, and Java

The following is a list of code snippets for the AMS API `ListChangeTypeClassificationSummaries` operation, in all available languages.

For the Python, Ruby, and Java SDKs, see Tools for Amazon Web Services and scroll down to the SDKs section. Each SDK installer contains a README with additional code snippets.

AMS API to CLI example

After you have installed the AMS CLI (requires the AWS CLI; see Installing or upgrading the AMS CLI (p. 101)), you can run any AMS API operation by reforming the call first specifying which AMS API, `aws amscm` or `aws amsskms`, and then giving the action with hyphens replacing camel case. Finally, provide credentials, such as SAML.

To learn more, see Using the AWS Command Line Interface.

Example:

- API: `'ChangeTypeClassificationSummaries[].[Category,Subcategory,Item,Operation,ChangeTypeId]'`
- CLI: `amscm list-change-type-classification-summaries --query "ChangeTypeClassificationSummaries[*].[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table`

> **Note**
> If you authenticate with SAML, add `aws --profile saml` to the beginning of the command. For example, `aws --profile saml amscm list-change-type-classification-summaries --query "ChangeTypeClassificationSummaries[*].[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table`

AMS API to Python example

In order to use the AMS API with Python, install the AMS CLI and install boto3. Follow these steps:

1. Install the AMS CLI. See Installing or upgrading the AMS CLI (p. 101).
2. Install boto3, the AWS SDK for Python. For more information, see this blog post Now Available – AWS SDK For Python (Boto3).

   ```
   import boto3
   ```
3. Get the AMS Change Management client:

   ```
   cm = boto3.client('amscm')
   ```
4. Get the AMS CTs:

   ```
   cts = cm.list_change_type_classification_summaries()

   print(cts)
   ```

Python examples

The following are some examples for using Python in AMS, to create EC2 instances, and/or use Lambda.

Python example to create an EC2

This example shows how you can use the amscm RESTFul API from within Python code to file and perform RFC processes.

1. Install the AMS CLI somewhere you have access to; you need the files it supplies.
2. Call Python libraries and create the EC2 instance:

```
import boto3
```

```
import json
import time

# Create the amscm client
cm = boto3.client('amscm')

# Define the execution parameters for EC2 Create
AMSExecParams = {
    "Description": "EC2-Create",
    "VpcId": "VPC_ID",
    "Name": "My-EC2",
    "TimeoutInMinutes": 60,
    "Parameters": {
        "InstanceAmiId": "INSTANCE_ID",
        "InstanceSubnetId": "SUBNET_ID"
    }
}

# Create the AMS RFC
cts = cm.create_rfc(
    ChangeTypeId="ct-14027q0sjyt1h",
    ChangeTypeVersion="3.0",
    Title="Python Code RFC Create",
    ExecutionParameters=json.dumps(AMSExecParams)
)

# Extract the RFC ID from the response
NewRfcID = cts['RfcId']

# Submit the RFC
RFC_Submit_Return=cm.submit_rfc(RfcId=NewRfcID)

# Check the RFC status every 30 seconds
RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']

while RFC_Status_Code != "Success":
    if RFC_Status_Code == "PendingApproval":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "InProgress":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "Failure":
        print(RFC_Status_Code)
        break
    else:
        print(RFC_Status_Code)

    RFC_Status = cm.get_rfc(RfcId=NewRfcID)
    RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']
```

Python example with Lambda

This example shows how to bundle the AMS models with your code so you can use it with Lambda, or EC2; places you won't, or can't, install `amscli`.

Note
AMS does not provide an importable AMS-specific Python SDK. The `amscli` install script installs the AMS service data models in the CLI's normal path. For CLI usage and system Python usage, that is fine, because both `awscli` and `boto3` read their service models from the same default locations (`~/.aws/models`). However, when you want to use AMS services via boto3 in Lambda

(or any other non-local runtime), it breaks, because you no longer have the data models. The following is a method to fix this by packaging the data models with the function.

There are simple steps that you can take to run your AMS-integrated Python code in Lambda or another runtime like EC2, Fargate, etc. The following workflow shows the steps necessary for AMS-integrated Lambda functions.

By adding the data models to the code's deployment package and updating the SDK search path, you can simulate an SDK experience.

Important
This example and all of the non-python commands shown were tested on a Mac computer.

Example Workflow:

1. Install the `amscli`. This creates a folder at `~/.aws/models` on your computer (Mac).
2. Copy the models to a local directory: `cp ~/.aws/models ./models`.
3. Include the models into your code's deployment package.
4. Update your function code to add the new models to the SDK path. Note that this code must run before boto3 or botocore are imported!

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note
Because the example models are in a directory named `models`, we add `./models` to AWS_DATA_PATH. If the directory was named `/ams/boto3models`, we would add the following code:

```
import os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

Your code should successfully find the AMS models. As a more specific example re: packaging, here's the Lambda specific workflow.

Example AMS Lambda Workflow:

These steps apply the preceding generic example to creating an AWS Lambda function.

1. Install the amscli. This creates a folder at `~/.aws/models` on your computer (Mac).
2. Copy the models to a local directory:

```
cp ~/.aws/models ./models
```

3. Add the models to your function's deployment zip file:

```
zip -r9 function.zip ./models
```

Important
Update your function code to add the new models to the SDK path. Note that this code must run before boto3 or botocore are imported!

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note
Because the example models are in a directory named `models`, We add `./models` to AWS_DATA_PATH. If the directory was named `/ams/boto3models`, we would add the following code:

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

Now, deploy your function:

1. Add your function code to the deployment zip file (if you haven't done so already):

```
zip -g function.zip lambda-amscm-test.py
```

2. Create or update your function with the zip file you created (console or CLI):

```
aws lambda update-function-code --function-name lambda-amscm-test --zip-file fileb://
function.zip --region us-east-1
```

Your AMS-integrated Python Lambda should now work.

Note
Your function must have IAM permissions for `amscm` or you get a permissions error.

Sample Lambda function code to test amscm (contents of lambda-amscm-test.py):

```
import json

# Force lambda to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore


def lambda_handler(event, context):
    use_session = boto3.session.Session(region_name="us-east-1")
    try:
        cm = use_session.client("amscm")
        cts = cm.list_change_type_categories()
        print(cts)
    except botocore.exceptions.UnknownServiceError:
        print("amscm not found")
```

```
    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

Test outputs (success):

Function Response:

```
{
  "statusCode": 200,
  "body": "\"Hello from Lambda!\""
}

Request ID:
"1cea13c0-ed46-43b1-b102-a8ea28529c27"
```

Function Logs:

```
START RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27 Version: $LATEST
{'ChangeTypeCategories': ['Deployment', 'Internal Infrastructure Management',
 'Management'], 'ResponseMetadata': {'RequestId': 'e27276a0-e081-408d-bcc2-10cf0aa19ece',
 'HTTPStatusCode': 200, 'HTTPHeaders': {'x-amzn-requestid': 'e27276a0-e081-408d-
bcc2-10cf0aa19ece', 'content-type': 'application/x-amz-json-1.1', 'content-length': '89',
 'date': 'Sun, 10 May 2020 23:21:19 GMT'}, 'RetryAttempts': 0}}
END RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27
```

AMS API to Ruby example

In order to use the AMS API with Ruby, install the AWS Ruby SDK and AMS CLI. Follow these steps:

1. Install the AMS CLI. See Installing or upgrading the AMS CLI (p. 101).
2. Install the AWS Ruby SDK. See Tools for Amazon Web Services.
3. Configure Ruby with these commands:

```
require 'aws-sdk'

config = {

 region: 'us-east-1',

 credentials: Aws::Credentials.new('ACCESS_KEY','SECRET_KEY')}
```

4. Get the AMS CTs:

```
ams_cm = Aws::amscm::Client.new(config)

cts = ams_cm.list_change_type_classification_summaries

print(cts)
```

AMS API to Java example

In order to use the AMS API with Java, install the AWS Java SDK and AMS CLI. Follow these steps:

1. Install the AMS CLI. See Installing or upgrading the AMS CLI (p. 101).

2. Install the AWS Java SDK. See Tools for Amazon Web Services.
3. Configure Java with these commands:

```
import com.amazonaws.auth.BasicAWSCredentials;

import com.amazonaws.services.amscm.model.AWSManagedServicesCMClient;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesRequest;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesResult;

public static void getChangeTypeClassificationSummaries() {
```

4. Set the credentials. We recommend that you do not hardcode this.

```
final BasicAWSCredentials awsCredsCm =

 new BasicAWSCredentials("ACCESS_KEY", "SECRET_KEY");
```

5. Create the AMS Change Management client:

```
final AWSManagedServicesCMClient cmClient =

 new AWSManagedServicesCMClient(awsCredsCm);
```

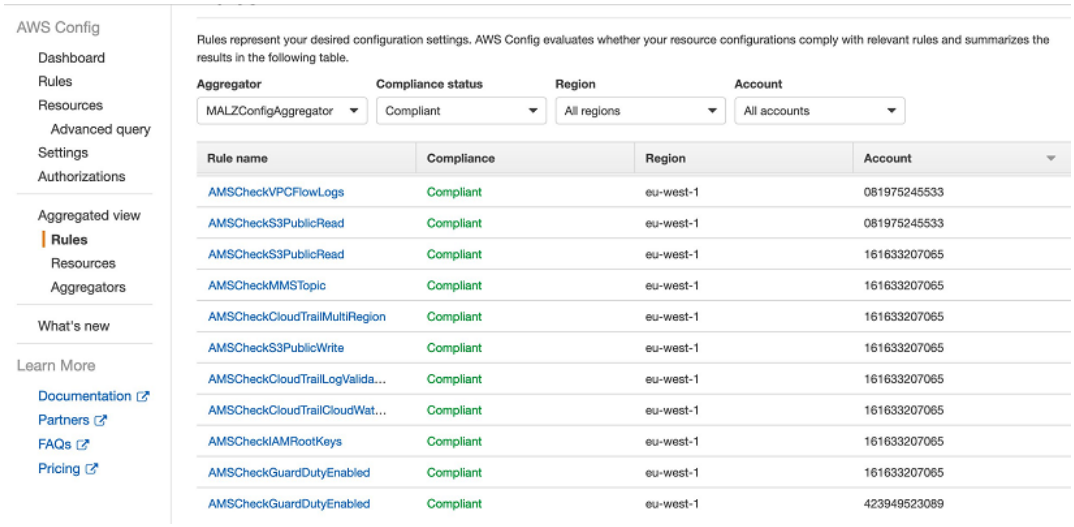
6. Get the AMS CTs:

```
final ListChangeTypeClassificationSummariesRequest listCtsRequest = new
ListChangeTypeClassification SummariesRequest();

final ListChangeTypeClassificationSummariesResult listCtsResult =

cmClient.listChangeTypeClassificationSummaries(listCtsRequest);

System.out.println("List of CTs");

listCtsResult.getChangeTypeClassificationSummaries().stream()

.map(x -> x.getCategory() + "/" + x.getSubcategory() + "/" + x.getItem() +
"/" + x.getOperation())

.forEach(System.out::println);

}
```

Multi-Account Landing Zone AWS Config aggregator

AMS multi-account landing zone utilizes the AWS Config aggregator service to create a centralized view of compliance across all your accounts. This means you can see the compliance status of all AWS Config Rules across your AMS multi-account landing zone environment under the AWS Config aggregator in your security account.

The following is a sample of the AWS Config aggregator showcasing central compliance status of AWS Config Rules across accounts.

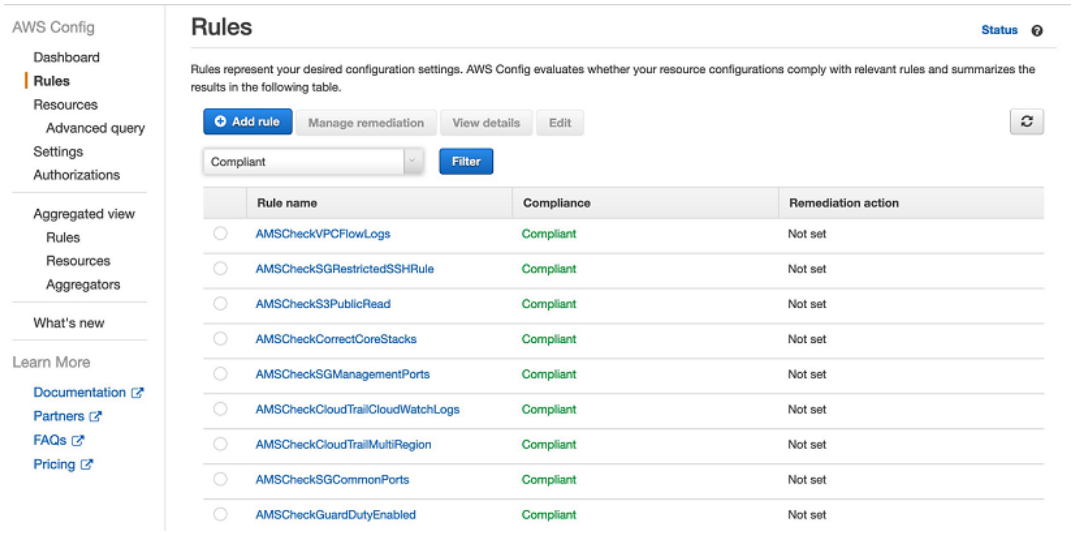


For more information, see the AWS documentation for Config Aggregator.

- How does AMS use AWS Config rules?

  AMS creates AWS Config Rules to give visibility into the configuration of your AWS resources against conditions specified in the rules. If a rule is non-compliant, you can request a change and the AMS Ops team will work with you to take corrective action.
- In that case, you see the following changes appear in your AMS accounts:
  - AWS Config Rules under AWS Config > Rules
  - Custom Config rules with their Lambda functions exist in your account
  - Config Aggregator in Security account and Config Authorization in all accounts (Multi-Account Landing Zone only)

The following is a sample of AWS Config Rules and their compliance evaluation results is shown below:



To learn more about AWS Config, see:

- AWS Config: What Is Config?
- AWS Config Rules: Evaluating Resources with Rules

- AWS Config Rules: Dynamic Compliance Checking: AWS Config Rules – Dynamic Compliance Checking for Cloud Resources
- AWS Config Aggregator: Multi-Account Multi-Region Data Aggregation

AMS bring your own EPS

You can use the AMS "bring your own end point security" (BYOEPS) feature to replace the default Trend Micro Deep Security agent with your own end point security solution, or Trend Micro license.

If you already have cost effective licenses for products other than Trend Micro Deep Security, or a team that provides your EPS, or if you want to use a specific EPS tool, use BYOEPS in your instances.

> **Note**
> The use of BYOEPS changes the AMS roles and responsibilities for security management; for details on the changes, see the AMS responsibility matrix (RACI) (p. 16)

BYOEPS works at an account level and your instances in the account either use BYOEPS or the default, AMS-managed EPS. In multi-account landing zone (MALZ), you designate application accounts where you use BYOEPS or managed EPS. If you use BYOEPS, your AWS bill reduces by the cost for Trend Micro Deep Security; however, you still incur a cost for EPS as the AMS-managed EPS is still required for protecting AMS-created and maintained EC2 instances required for access management (bastions, and management hosts). To calculate the total cost impact, you need to account for the the cost of licenses for your new tool, and the cost of managing EPS at the service levels you need.

When you use BYOEPS, you lose one of the security controls offered by AMS but have security management provided using tools such as AWS GuardDuty, AWS Macie; and process controls such as reviews of IAM configuration to ensure the security of your AWS account. AMS compliance certifications and attestations are not affected if you use BYOEPS. However, many security framework and certifications have requirements for protection from malware and malicious code. To ensure account security and compliance, evaluate and ensure that your planned controls meet the security requirements for compliance certifications needed for your workload.

Using BYOEPS

After ensuring that you want to use your own EPS solution, you are ready to request and begin using AMS BYOEPS.

Pre-requisites:

1. If you use an EC2 instance profile that is in addition to the default EC2 instance profile, `customer-mc-ec2-instance-profile`, allow the `ssm:GetParameter` action for the `/ams/end-point-security` resource, to your EC2 instance profile.
2. Update EC2 instance launch automations or processes using custom or AMS AMIs to use AMS AMIs released after December 2020.

Enable BYOEPS:

The use of BYOEPS changes the AMS responsibilities for Security Management. Consult your security and cloud platform team before enabling BYOEPS.

Request use of BYOEPS by submitting a "MOO" update RFC (Management | Other | Other | Update) with ct-0xdawir96cy7k, with the following details:

```
Please enable BYOEPS for this account/these accounts
Account IDs: IDs for the accounts for BYOEPS..
```

Accounts with EC2 instances using AMS-managed EPS:

If the accounts that you want BYOEPS for are using AMS-managed EPS, you need to work with AMS to uninstall the Trend Micro agents from those EC2 instances, and update the AMS code (i.e. boot scripts) on those instances. It is best to do this as part of a maintenance window as it may require a reboot. After AMS receives the MOO RFC, your cloud service delivery manager (CSDM) contacts you to decide on a maintenance window to perform this activity, and create a migration plan. A few things to consider as you plan:

- How many instances do you need to migrate in total? Divide the total number of instances into smaller, incremental batches.
- How would you divide the instances in batches? Options could be by resource groups, creating a list that can be shared with Operations etc.
- How much time would each batch take? How much total time is required? Consider that you might want to install your preferred EPS tooling in the same maintenance window. How much time would this take?

You will share this information with the AMS Operations engineers performing the migration. A spreadsheet, or some clear communication to your CSDM.

During the maintenance window, the following actions are performed on each instance that needs to be on-boarded to BYOEPS:

- Performed by AMS: Update AMS code (boot scripts, modules, and so forth.) to the latest. This is required because old AMS boot scripts do not have BYOEPS feature support and will re-install Trend Micro agent on every boot. Also, uninstall the Trend Micro Agent.
- Performed by You: Install, and configure your preferred EPS tooling.

Accounts with NO EC2 instances using AMS-managed EPS:

Accounts with new instance launches using the latest AMS AMIs can skip Trend Micro agent installation. Do not launch instances with AMIs older than December 2020 as they do not have the BYOEPS feature support. Update any automation using old AMIs to use the latest AMS AMIs with BYOEPS feature support. Once the feature is enabled, AMS confirms the action on the RFC.

Adding your agent on EC2 instances:

See AMS Patterns for help with deploying agents of tools such as Crowdstrike or Qualys. Submit a service request for help.

Receiving AMS notifications

Communications between you and AMS occur for many reasons:

- An RFC created by AMS that requires your approval
- An AMS case created to investigate an RFC you created that has failed
- Events created by monitoring alerts
- Patching service notifications that inform you of upcoming patching
- Service requests and incident reports
- Monthly CRM reports
- Occasional important AWS announcements (your CSDM contacts you if any action on your part is required)

All of these notifications are sent to the default contact information (the root account email) that you provided AMS when you were onboarded. Because it's difficult to keep individual emails updated, we recommend that you use a group email that can be updated on your end. All notifications sent to you are also received by AMS operations and analyzed before making a response.

AMS notification service provides two additional ways to set up contacts for notifications:

- Tag your resources with contact tags (the tag Key Value being contact information) and provide the tag Key Name to your CSDM. Alarms on those resources will be sent to the contacts provided in the Key Value, in addition to the account contact created at onboarding. This is especially useful for application owners. For more information, see Tag-based alert notification (p. 298).
- (Required at onboarding) Send to your CSDM named lists of contacts for non-resource based notifications. For example, you might have a list named "SecurityContacts" and another named "OperationsContacts", and so forth. AMS adds the list to the notification service, and alarms that apply to that list's context are sent to those contacts. This is especially useful for organizational matters.

This advanced alert routing feature is active for most of the essential CloudWatch alarms such as Amazon EC2 instance failure, Amazon Elastic Block Store (Amazon EBS) volume capacity utilization - Root usage, Amazon EBS NonRoot usage, High Memory utilization, High Swap usage, and High CPU utilization for Amazon EC2.

Additionally, when you file a service request, or incident report, you have the option of adding "CC Emails" (highly recommended) and those email addresses receive notifications about the service request or incident.

> **Important**
> While the CC email addresses provided in service requests and incident reports receive email notifications of communications, other notifications, such as patching notifications, appear in your Service Request list (an email is also sent to the default contact), *without* explicit notification to you that you have a communication awaiting your attention. This is why we strongly recommend adding a CC email where you can, and setting up the default contact email as a group to which everyone using AMS is a member.

Additionally, you can request special notifications for new AMIs, for RFC state change, and for configuration changes in your AMS account. These optional notification services are discussed next.

AMS AMI notifications with SNS

AMS provides an AMI notification service. This service allows you to subscribe to an AWS Simple Notification Service (SNS) topic that notifies you when AMS AMI updates have been released. You can choose to receive notifications for only the AMS AMIs you use, or you can sign up to receive update notifications for all AMS AMIs. For more information on SNS topics, see What is Amazon Simple Notification Service?

Whenever AMIs are released, we send notifications to the subscribers of the corresponding topic; this section describes how to subscribe to the AMS AMI notifications.

Sample message

```
{
  "Type" : "Notification",
  "MessageId" : "example messageId",
  "TopicArn" : "arn:aws:sns:us-east-1:591688410472:customer-ams-windows2019",
  "Subject" : "New AMS AMIs are Now Available",
  "Message" : "{"v1": {"Message": "A new version of the AMS Amazon Machine Images has
 been released.n nYou are now able to launch new EC2 stacks from these AMIs.n nPlease use
 this time to update any dependencies such as CloudFormation or Autoscaling groups.n n
 nRelease Notesn n nWindowsn n n- Contains latest Windows Patches:n n nMicrosoft Windows
```

```
 Server 2008 R2 Datacentern n- (KB2819745, KB3018238, KB4507004, KB4507437)n n nMicrosoft
 Windows Server 2016 Datacenter Security Enhancedn n- (KB4509091, KB4507459)n n nMicrosoft
 Windows Server 2016 Datacentern n- (KB4509091, KB4507459)n n nMicrosoft Windows Server
 2012 R2 Security Enhancedn n- (KB3191564, KB3003057, KB3013172, KB3185319, KB4504418,
 KB4506996, KB4507463)n n nMicrosoft Windows Server 2012 R2 Standardn n- (KB3003057,
 KB3013172, KB3185319, KB4504418, KB4506996, KB4507463)n n n nLinuxn n n- Contains latest
 Linux patches n- All AMIs n
ow force domainjoin-cli leave before domainjoin-cli join for better stability in
 the domain join process.nn", "images": {"images": {"image_name": "customer-ams-
windows2019-2021.08-1", "image_id": "ami-05dfa45396fddaa5e"}}, "region": "us-east-1"}}",
  "Timestamp" : "2021-09-03T19:05:57.882Z",
  "SignatureVersion" : "1",
  "Signature" : "example sig",
  "SigningCertURL" : "example url",
  "UnsubscribeURL" : "example url"
}
```


Possible AMS AMI topics to subscribe to:

- **ALL**: Use `customer-ams-all-amis`. This topic subscription notifies you when any of the AMS AMIs are updated.
- **AMS AWS Linux AMIs**: Use `customer-ams-amazon1` (Amazon Linux) or `customer-ams-amazon2` (Amazon Linux 2).
- **AMS AWS RedHat AMIs**: Use `customer-ams-rhel6`, `customer-ams-rhel6-security-enhanced`, `customer-ams-rhel7`, `customer-ams-rhel7-security-enhanced`.
- **AMS AWS CentOs AMIs**: Use `customer-ams-centos7`, `customer-ams-centos7-security-enhanced`.
- **AMS AWS Windows AMIs**: Use `customer-ams-windows2012r2`, `customer-ams-windows2012r2-security-enhanced`, `customer-ams-windows2016`, `customer-ams-windows2016-security-enhanced`.

To subscribe to AMS new AMI notifications by using the Amazon SNS console:

1. Open the Amazon SNS console to the Dashboard.
2. In the upper-right corner, change to the AWS Region for the AMIs that you are subscribing to.
3. In the left-navigation pane, choose **Subscriptions**, and then choose **Create subscription**.
4. Provide the following information:
   a. **Topic ARN**: `arn:aws:sns:{`*`REGION`*`}:287847593866:{`*`AMS_AMI_NAME`*`}` where REGION is the selected AWS Region (where the SNS notification was created) and AMS_AMI_NAME is the AMI that you want notifications about. Examples:
      - To subscribe to notifications of new AMS Amazon Linux AMIs in AWS Region us-east-1, use this **Topic ARN** = `arn:aws:sns:us-east-1:287847593866:customer-ams-amazon1`.
      - To subscribe to notifications of new AMS Window Server 2016 AMIs in AWS Region us-west-2, use this **Topic ARN** = `arn:aws:sns:us-west-2:287847593866:customer-ams-windows2016`
   b. For **Protocol**, choose **Email**.
   c. For **Endpoint**, enter an email address that you can use to receive the notifications. We recommend a distribution list rather than an individual's email.
5. Choose **Create subscription**.
6. When you receive a confirmation email with the subject line "AWS Notification - Subscription Confirmation," open the email and choose **Confirm subscription** to complete your subscription.

To unsubscribe from AMS new AMI notifications by using the AWS SNS console:

1. Open the Amazon SNS console to the Dashboard.
2. In the navigation bar, change to the AWS Region of your choice. You must use the AWS Region in which you want to receive notifications for the corresponding AMIs.
3. In the navigation pane, choose **Subscriptions**, select the subscription, and then choose **Actions** -> **Delete subscriptions**.
4. When prompted for confirmation, choose **Delete**.

To subscribe to AMS New AMI notifications using the Deployment | Ingestion | Stack from CloudFormation Template | Create (ct-36cn2avfrrj9v):

1. To subscribe to the AmazonLinuxSubscription, create and save an execution parameters JSON file; this example names it CreateSubscribeAmiParams.json:

```
{
    "AWSTemplateFormatVersion": "2010-09-09",
    "Resources": {
        "AmazonLinuxSubscription":{
              "Type" : "AWS::SNS::Subscription",
              "Properties": {
                "TopicArn": "arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}",
                "Protocol": "email",
                "Endpoint": "username@yourdomain.com"
            }
        }
      }
}
```

2. Create and save the RFC parameters JSON file with the following content; this example names it CreateSubscribeAmiRfc.json file:

```
{
   "ChangeTypeId": "ct-36cn2avfrrj9v",
   "ChangeTypeVersion": "1.0",
   "Title": "cfn-ingest-subscribe-ami"
}
```

3. Create the RFC, specifying the CreateSubscribeAmiRfc file and the CreateSubscribeAmiParams file:

```
aws amscm create-rfc --cli-input-json file://CreateSubscribeAmiRfc.json  --execution-
parameters file://CreateSubscribeAmiParams.json
```

   You receive the ID of the new RFC in the response and can use it to submit and monitor the RFC. Until you submit it, the RFC remains in the editing state and does not start.

For examples of creating AMIs, see Create AMI.

For information on consuming AMIs programmatically, see EC2 stack: creating.

Service notifications

AMS sends outbound service requests, or service notifications, when you need to act on, or be aware of, something that might impact your account or resources, including:

- Infrastructure impact: AMS sends a service notification when there is an underlying AWS service impacting your infrastructure, and you need to take action before a certain date, or you may have an outage.

- EC2 Hardware issues: AMS sends service notifications out for EC2 hardware issues that require you to reboot an EC2 instance before a certain date, or letting you know that AMS will reboot the instance for you. This is an important notice because reboot can cause an outage and you must respond with an acceptable date, or create an RFC with ct-09qbhy7kvtxqw, to reboot the instance yourself. A service notification like this automatically closes in five days if you do not respond.

RFC state change notifications

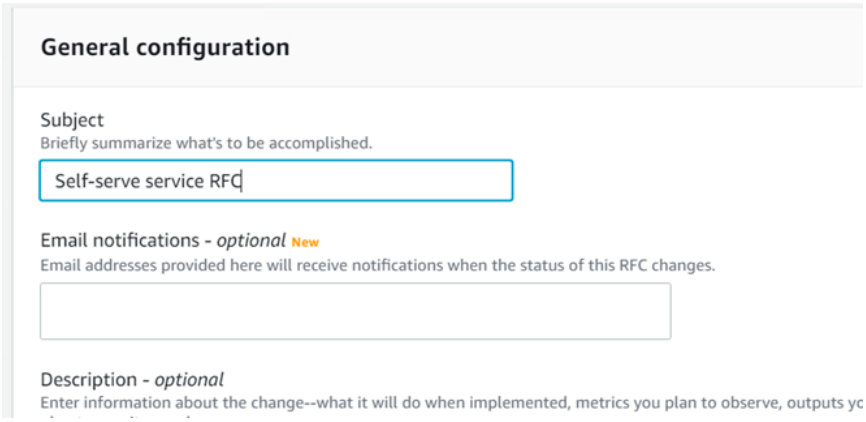
AMS offers notifications for RFC state changes by email and CloudWatch Events:

- Emails by way of the AMS Console: There is an option on the second page of the Create RFC wizard, where you can add up to five email addresses to be notified when that RFC state changes.
- CloudWatch Events: You can configure different rules and targets for CloudWatch Events to receive notifications for every RFC state change.

Email notifications

You can add email addresses to receive RFC state changes to an RFC that you create in the AMS console, or by using the AMS API/CLI.

In the AMS console, use the **Email notifications** option, on the second page of the Create RFC wizard:



In the AMS API/CLI, add a line like this to the RFC parameters section of your RFC (do not add the line to the run parameters section):

```
--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"
```

The behavior of the notifications varies depending the RFC scheduling type:

- Scheduled RFCs receive email notifications on : Submitted, Scheduled, InProgress, Completed, Rejected, Canceled, Auto-Rejected, or Auto-Canceled.
- ASAP RFCs receive email notification on: Submitted, InProgress, Completed, Rejected, Canceled, AutoRejected, or Auto-Canceled.

Note

- Email notifications are sent from this address: `no-reply@managedservices.amazonaws.com`.
- Special characters and URLs in your RFC title are redacted in the emails we send. This is a security measure.

CloudWatch Events notifications

AMS offers push notifications for the RFC State changes through CloudWatch Events. To get these notifications:

1. Create a topic and subscription where notifications will be sent. You can name the topic what you like; for information about doing this, see SNS Topic and Subscription: Creating.
2. Submit an RFC with the Management | Other | Other | Create change type and include the SNS topic and subscription in the request for RFC state change notices.

When you submit the Management | Other | Other RFC request for this feature, you can specify what RFC state changes you're interested in getting notified about and what change types, and set other filters. For example, you may want to request to be notified only when Admin Access change types are EventType = RfcSubmitted and EventType = RfcUpdated.

This is a template of CloudWatch event notifications that you can receive (with all possible values):

```
{
    "source ": "aws.managedservices",
    "detail-type": "AMS RFC State Change",
    "detail": {
        "ActionState": "null | AwsActionPending | AwsOperatorAssigned |
 CustomerActionPending | NotApplicable | NoActionPending",
        "ActualExecutionTimeRange": {
            "StartTime": "null | Actual Start Time",
            "EndTime": "null | Actual End Time"
        },
        "AutomationStatus": "Automated | Manual",
        "AwsAccountId": "AWS Account ID",
        "AwsApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending |
 Rejected | Approved",
        "ChangeTypeId": "Change_Type_ID",
        "ChangeTypeVersion": "Change_Type_Version",
        "CreatedTime": "Created_Time",
        "CustomerApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending
 | Rejected | Approved",
        "EventType": "RfcActionStateUpdated | RfcApproved | RfcAutoRejected | RfcCanceled |
 RfcCompleted | RfcCreated | RfcInProgress | RfcRejected | RfcSubmitted | RfcUpdated",
        "LastModifiedTime": "Last_Updated_Time",
        "LastSubmittedTime": "null | Last_Submitted_Time",
        "RequestedExecutionTimeRange": {
            "StartTime": "null | Expected_Start_Time",
            "EndTime": "null | Expected_End_Time"
        },
        "RfcId": "RFC_ID",
        "Status": "Editing | PendingApproval | Scheduled | Rejected | Canceled |
 ExecutionLock | InProgress | Success | Failure",
        "Title": "Title"
    }
}
```

The supported RFC state changes (EventType), as they appear in the actual CloudWatch Events notification are:

- RfcActionStateUpdated (no AMS console option): The RFC in one of the states, described later, changed.
- RfcApproved (no AMS console option): The RFC passed system and/or AMS operator validation and has been approved for completion.
- RfcAutoRejected (**Auto-Rejected**): The RFC failed system validation or AMS operator and has been rejected.

- RfcCanceled (**Canceled** or **Auto-Canceled**): The RFC was canceled by either the submitter or an AMS operator.
- RfcCompleted (**Completed**): The RFC run parameters have been completed, including UserData.
- RfcCreated (no AMS console option): The RFC was successfully created (the JSON and submitted parameters were valid).
- RfcInProgress (**InProgress**): The RFC run is still in progress.
- RfcRejected (**Rejected**): The RFC failed system or AMS operator validation has been rejected.
- RfcSubmitted (**Submitted**): The RFC has been submitted and is undergoing system validation.
- RfcUpdated (no AMS console option): The RFC has been manually updated by an AMS operator.

Additionally, you can send CloudWatch Events (CWE) notifications to any of the supported destinations and build your own systems on top of these automated notifications:

- Amazon EC2 instances
- AWS Lambda functions
- Streams in Amazon Kinesis Data Streams
- Delivery streams in Amazon Kinesis Data Firehose
- Log groups in Amazon CloudWatch Logs
- Amazon ECS tasks
- Systems Manager Run Command
- Systems Manager Automation
- AWS Batch jobs
- Step Functions state machines
- Pipelines in CodePipeline
- CodeBuild projects
- Amazon Inspector assessment templates
- Amazon SNS topics
- Amazon SQS queues
- Built-in targets: EC2 CreateSnapshot API call, EC2 RebootInstances API call, EC2 StopInstances API call, and EC2 TerminateInstances API call.
- The default event bus of another AWS account

Note
We send CloudWatch Events notification for RFC state changes, on a best-effort basis.

Setting up private and public DNS

During onboarding, AMS sets up a private DNS service for communications between your managed resources and AMS.

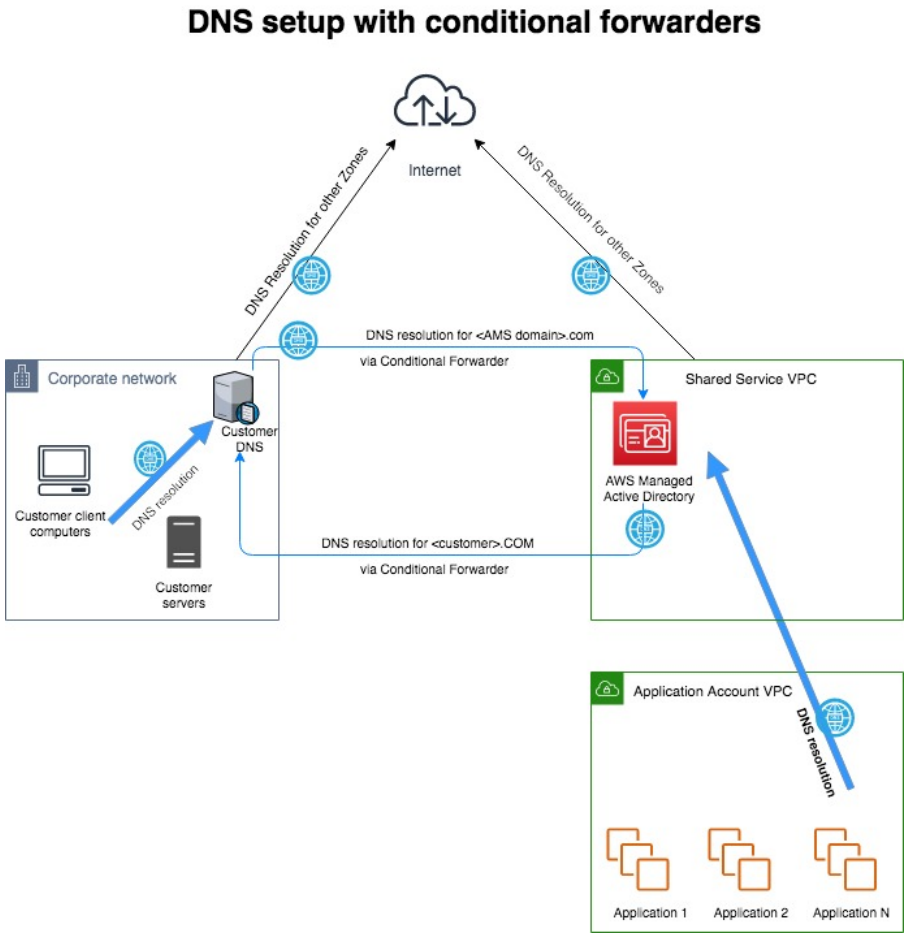
You can use AMS Route 53 to manage the internal DNS names for your application resources (web servers, application servers, databases, and so forth) without exposing this information to the public Internet. This adds an additional layer of security, and also allows you to fail over from a primary resource to a secondary one (often called a "flip") by mapping the DNS name to a different IP address.

After you create private DNS resources using the Deployment | Advanced stack components | DNS (private) | Create (ct-0c38gftq56zj6) or Deployment | Advanced stack components | DNS (public) |

Create (ct-0vzsr2nyraedl), you can use the Management | Advanced stack components | DNS (private) | Update (ct-1d55pi44ff21u) and Management | Advanced stack components | DNS (public) | Update (ct-1hzofpphabs3i), CTs to configure additional, or update existing, record sets. For multi-account landing zone (MALZ) accounts, DNS resources created in the application account VPCs can be shared with the shared services account VPC to maintain centralized DNS using AMS AD.

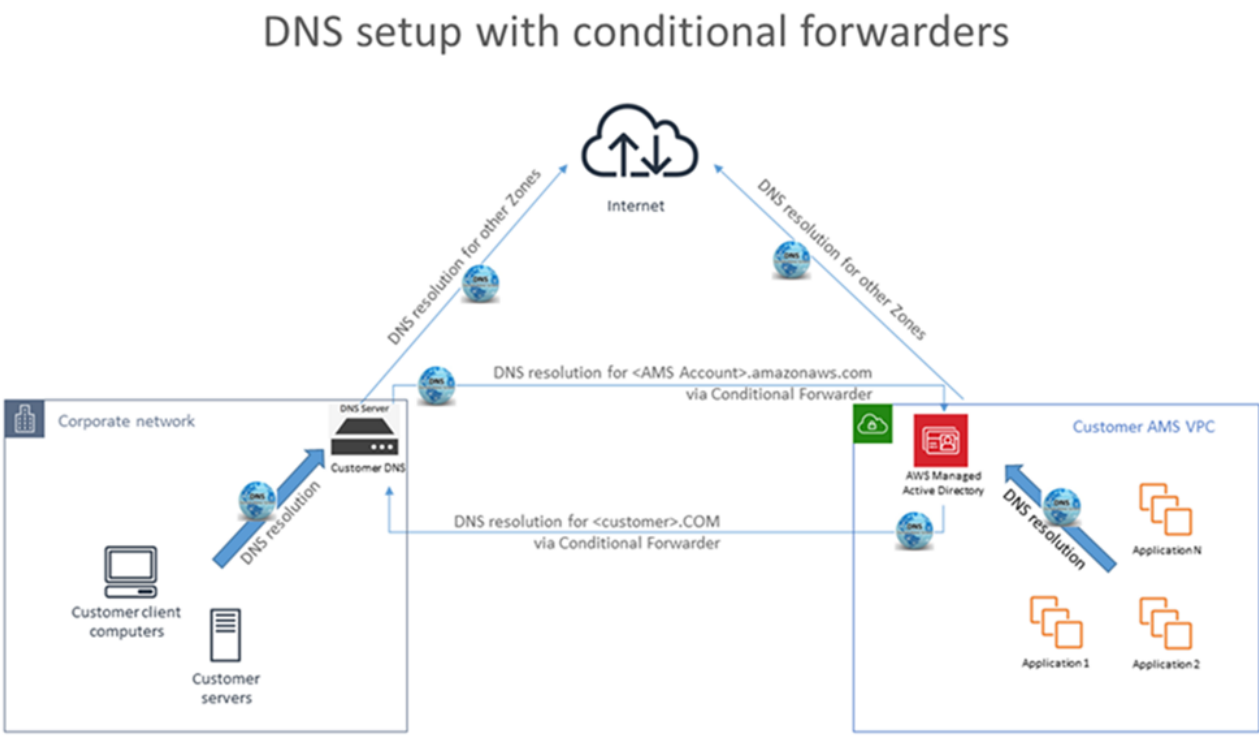
MALZ

The following graphic illustrates a possible DNS configuration for Multi-Account Landing Zone AMS. It illustrates a hybrid DNS setup between AMS and a typical customer network. A Canonical Name Record (CNAME) in the customer network DNS server forwards to the AMS AD DNS in the shared services account with a conditional forward that has the CNAME of the AMS FQDN forwarded to the A record.



SALZ

The following graphic illustrates a possible DNS configuration for single-account landing zone (SALZ). It shows a hybrid DNS setup between AMS and a typical customer network. A CNAME in the customer network DNS server forwards to the AMS AD DNS with a conditional forward which has the CNAME of the AMS FQDN forwarded to the A record.



For more information, see Using DNS with Your VPC and Working with Private Hosted Zones.

AMS egress traffic management

By default, the route with a destination CIDR of 0.0.0.0/0 for AMS private and customer-applications subnets has a network address translation (NAT) gateway as the target. AMS services, TrendMicro and patching, are components that must have egress access to the Internet so that AMS is able to provide its service, and TrendMicro and operating systems can obtain updates.

AMS supports diverting the egress traffic to the internet through a customer-managed egress device as long as:

- It acts as an implicit (for example, transparent) proxy.

  and

- It allows AMS HTTP and HTTPS dependencies (listed in this section) in order to allow ongoing patching and maintenance of AMS managed infrastructure.

Some examples are:

- The transit gateway (TGW) has a default route pointing to the customer-managed, on-premises firewall over the AWS Direct Connect connection in the Multi-Account Landing Zone Networking account.
- The TGW has a default route pointing to an AWS endpoint in the Multi-Account Landing Zone egress VPC leveraging AWS PrivateLink, pointing to a customer-managed proxy in another AWS account.
- The TGW has a default route pointing to a customer-managed firewall in another AWS account, with site-to-site VPN connection as an attachment to the Multi-Account Landing Zone TGW.

AMS has identified the corresponding AMS HTTP and HTTPS dependencies, and develops and refines these dependencies on an ongoing basis. See Egress Management ZIP. Along with the JSON file, the ZIP contains a README.

Note

- This information isn't comprehensive--some required external sites aren't listed here.
- Do not use this list under a deny list or blocking strategy.
- This list is meant as a starting point for an egress filtering rule set, with the expectation that reporting tools will be used to determine precisely where the actual traffic diverges from the list.

To ask for information about filtering egress traffic, email your CSDM: ams-csdm@amazon.com.

Setting permissions with IAM roles and profiles

AMS uses AWS Identity and Access Management (IAM) to manage users, security credentials such as access keys, and permissions that control which AWS resources users and applications can access. AMS provides a default IAM user role and a default Amazon EC2 instance profile (which includes a statement allowing the resource access to the default IAM user role).

Requesting a new IAM user role or instance profile

AMS uses an IAM role to set user permissions through your federation service and an IAM instance profile as a container for that IAM role.

You can request, with an AMS service request, or a Management | Other | Other | Create CT, a custom IAM role or instance profile. See the descriptions of each in this section.

Note
AMS has an IAM policy, `customer_deny_policy` that blocks out dangerous namespaces and actions. This policy is attached to all AMS customer roles by default and is rarely a problem for users. Your IAM user and role requests don't include this policy, but automatic inclusion of the `customer_deny_policy` in requests for IAM roles helps AMS deploy new IAM instance profiles more quickly. You can request the exclusion of the `customer_deny_policy` policy. However, this request will go through a weighty security review and is likely to be declined due to security reasons.

Deploying IAM resources

AMS can deploy IAM resources in in your multi-account landing zone (MALZ) Application and single-account landing zone (SALZ) accounts without an operator review through a request for change (RFC) with the Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entity or policy (auto) change type (ct-19jq3ulr3g9zg).

Only certain types of resources are eligible for the deployment without operator review. At the moment, only resources with a subset of actions defined in the AWS Managed IAM console **ReadOnlyAccess** managed policy are allowed. AMS supports customization of this baseline (control) policy, subject to an AMS Security review. To learn more, review RFC security reviews and reach out to your cloud service delivery manager (CSDM) or cloud architect (CA).

A number of additional validations are also executed at the deployment time. These include IAM Policy linter, and checks that the IAM resource conforms to AMS technical standards (for example, only IAM roles trust policies between AMS accounts that belong to the same customer can be configured).

Four deployment scenarios are currently supported. When submitting the ct-19jq3ulr3g9zg change type (CT), depending on the selected scenario, fill out the relevant parameters:

- Create an IAM policy - populate the `PolicyName` and `PolicyDocument` parameters.
- Create an IAM role with an IAM policy attached - populate the `RoleName`, `RoleTrustPolicy`, `PolicyName` and `PolicyDocument` parameters.
- Create an IAM policy and attach it to an existing customer IAM role - populate the `PolicyName`, `PolicyDocument` and `RoleName` parameters.
- Create an IAM role and attach it to an existing IAM policy - populate `RoleName`, `RoleTrustPolicy` and `PolicyName` parameters.

Parameters not relevant to the selected scenario are ignored.

Example parameters for Create an IAM role with an IAM policy attached scenario

UseCase: Create an IAM role with an IAM policy attached

PolicyName: example_iam_policy_name

RoleName: example_iam_role_name

PolicyDocument:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    }
  ]
}
```

Tip
Remove new lines from JSON type inputs if you request this change via AMS console.

RoleTrustPolicy:

```
{
  "Version": "2012-10-17",
  "Statement":
  [
    {
      "Effect": "Allow",
      "Principal":
      {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Note
Every IAM role deployed with the ct-19jq3ulr3g9zg change type has a Permissions boundary attached; for example, see Permissions boundaries for IAM entities . This is done to ensure the safety of AMS-managed resources. Your IAM role requests don't include this policy, but

automatic inclusion of the permission boundary in requests for IAM roles helps AMS to streamline the deployment of new IAM resources.

The ct-19jq3ulr3g9zg change type supports the creation of new resources only. To update resources created with this CT, open a request using Management | Advanced stack components | Identity and Access Management (IAM) | Update entity or policy change type (ct-27tuth19k52b4).

Restrict permissions with IAM role policy statements

AMS uses an IAM role to set user permissions through your federation service.

Single-Account Landing Zone AMS: See IAM User Role.

Multi-Account Landing Zone AMS: See Default AMS Advanced Multi-Account Landing Zone IAM User Roles.

An IAM role is an IAM entity that defines a set of permissions for making AWS service requests. IAM roles are not associated with a specific user or group. Instead, trusted entities assume roles, such as IAM users, applications, or AWS services such as Amazon EC2. For more information, see IAM Roles.

You can scope down the desired policy for a user assuming the AMS IAM user role by using the AWS Security Token Service (STS) API operation AssumeRole by passing a more restrictive IAM policy under the `Policy` request field.

Example policy statements that you can use to restrict CT access are provided next.

Using your configured Active Directory (AD) groups, and the AWS Security Token Service (STS) API operation AssumeRole, you can set permissions for certain users or groups, including restricting access to certain change types (CTs). You can use the policy statements shown below to restrict CT access in various ways.

AMS change type statement in the default IAM instance profile that allows access to all AMS API calls (amscm and amsskms) and all change types:

```
{
    "Sid": "AWSManagedServicesFullAccess",
    "Effect": "Allow",
    "Action": [
        "amscm:*",
        "amsskms:*"
    ],
    "Resource": [
        "*"
    ]
}
```

1. Statement to allow access and all actions for only two specified CTs, where "Action" is the AMS API operations (either `amscm` or `amsskms`), and "Resource" represents existing change type IDs and version number:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action":amscm:*,
      "Resource": [ "arn:aws:amscm:*:*:changetype/ct-ID1:1.0",
                    "arn:aws:amscm:*:*:changetype/ct-ID2:1.0"]
    }
  ]
```

```
}
```

2. Statement to allow access for CreateRfc, UpdateRfc, and SubmitRfc on only two specified CTs:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action":["amscm:CreateRfc",
                "amscm:UpdateRfc",
                "amscm:SubmitRfc"],
      "Resource": ["arn:aws:amscm:*:*:changetype/ct-ID1:1.0",
                   "arn:aws:amscm:*:*:changetype/ct-ID2:1.0"]
    }
  ]
}
```

3. Statement to allow access for CreateRfc, UpdateRfc, and SubmitRfc on all available CTs:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action":["amscm:CreateRfc",
                "amscm:UpdateRfc",
                "amscm:SubmitRfc"],
      "Resource":"*"
    }
  ]
}
```

4. Statement to deny access for all actions on restricted CT and allow on other CTs:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action":amscm:*"
      "Resource":"arn:aws:amscm:*:*:changetype/ct-RetrictedID:1.0"
    },
    {
      "Effect": "Allow",
      "Action":amscm:*"
      "Resource":"*"
    }
  ]
}
```

Restrict permissions with Amazon EC2 IAM instance profiles

An IAM instance profile is a container for an IAM role that you can use to pass role information to an Amazon EC2 instance when the instance starts.

Currently there is one AMS default instance profile, `customer-mc-ec2-instance-profile`, that grants permissions to the applications running on the instance, not to users logging into the instance.

You might want to modify the default instance profile, or create a new one, if you want to give an instance access to something, without granting other instances access as well. You can request a new IAM instance profile with the Management | Applications | IAM instance profile | Create change type (ct-0ixp4ch2tiu04). When submitting the RFC, you could fashion your own instance profile and include that as the InstanceProfileDescription, or you could just inform AMS (using the same field) of what changes you want. Because this is a Manual CT, AMS must approve the change and will be in contact with you about it.

If you're unfamiliar with Amazon IAM policies, see Overview of IAM Policies for important information. There is also a good blog post, Demystifying Amazon EC2 Resource-Level Permissions. Note that AMS does not currently support Resource-based access control, but does support Resource-level controls using IAM role policies (for an explanation of the difference, see AWS Services That Work with IAM.

Single-Account Landing Zone AMS:

To see a table of permissions that the default AMS IAM instance profile grants, go to EC2 IAM Instance Profile.

Restrict with network ACL

A network access control list (NACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC. For more information about the differences between security groups and network ACLs, see Comparison of security groups and network ACLs.

However, in AMS Managed Multi-Account Landing Zone, in order for AMS to effectively manage and monitor infrastructure, the use of NACLs is limited to following scope:

- NACLs are not supported in the Multi-Account Landing Zone Core accounts, i.e. Management account, Networking, Shared-Services, Logging and Security.
- NACLs are supported in Multi-Account Landing Zone Application accounts as long as they are only used as a "Deny" list and have "Allow All" to ensure AMS monitoring and management operations.

In large scale multi-account environments, you can also leverage features like centralized egress firewalls to control outbound traffic and/or AWS Transit Gateway routing tables in AMS Multi-Account Landing Zone to segregate network traffic among VPCs.

AMS on Outposts

AWS Outposts is a managed hardware solution that extends AMS managed landing zones to customer data centers. With AMS support on AWS Outposts, customers seeking the cloud expertise, cost savings and standardized platform offered by AMS, are no longer limited to hosting resources inside AWS Regions. With AMS on AWS Outposts, customers with on-premise requirements can now modernize on AWS, while enjoying the patching, backup, provisioning, incident management, business continuity, and cost optimization services offered by AMS.

Once an AWS Outposts is activated in your AMS Multi-Account Landing Zone or Single-Account Landing Zone account, you can follow existing AMS change management processes to provision and manage AWS resources. AMS-hosted infrastructure can be managed by specifying your AWS Outposts-specific subnet. AWS Outposts lifecycles can be managed directly in the AWS Outposts console using the AWS Outposts self-provision services role.

For information on the role, see AWS Outposts.

AWS Outposts installation and operational management

The onboarding to AMS on AWS Outposts process is comprised of:

1. Outposts Planning
2. Order Validation
3. Outposts Onboarding to AMS
4. Lifecycle Management

AWS Outposts planning

During AWS Outposts planning, you identify AMS on AWS Outposts use cases and engage key stakeholders, including your AMS account team and AWS Outposts representatives, to align on capacity strategy.

1. Once use cases requiring AMS on AWS Outposts have been identified, engage your AMS account team to discuss capacity planning.
2. Once your AWS Outposts capacity requirements have been determined, your AMS account team engages the AWS Outposts service team to discuss AWS Outposts onboarding plan, roles and responsibilities. During this time an AWS Outposts single point of contact (SPOC) is assigned to you. The AWS Outposts SPOC assists in finalizing AWS Outposts sizing requirements.

AWS Outposts order validation

During order validation, you create an AWS Outposts site, and order your required capacity directly in the AWS Outposts console or through your AWS Outposts account representative.

Once you, the AMS account team, the AWS Outposts team are aligned, you can request the AWS Outposts self-provisioned service role using change type ID ct-3qe6io8t6jtny, to create your site and AWS Outposts order directly in the AWS Outposts console.

Alternatively, you can work through the AWS Outposts SPOC to create Outpost Sites and orders. Your AWS Outposts SPOC remains to provide status updates to you and the AMS account team during site and order validation, and AWS Outposts installation.

AWS Outposts onboarding to AMS

Once your AWS Outposts unit is activated in your AMS managed VPC, you can request that monitors be created to track availability, capacity, exceptions and network connectivity for your Outposts hardware. By following the monitoring deployment steps described next, your AWS Outposts hardware is actively monitored by AMS.

1. Once your AWS Outposts has been installed and activated, you can request AWS Outposts-specific monitoring by submitting the following template with an RFC using the Management | Other | Other | Create (ct-1e1xtak34nx76) change type. AMS operations ensures that the AWS Outposts subnet is tracked in AMS internal tooling.
   - AWS Outposts ID
   - Subnet CIDR
   - Recommended AWS Outposts alarms:
     - InstanceFamilyCapacityAvailabilityAlert

    - InstanceTypeCapacityAvailabilityAlert
    - EBSVolumeTypeCapacityAvailabilityAlert
    - CapacityExceptionsAlert
    - Direct Connect ConnectionAlert
  - For each of the above alerts, specify the following parameters:
    - Statistic ("Average" is recommended. Other options include sum, maximum, minimum, sample count and p90)
    - Period ("5 minutes" is recommended. Other options include 10 and 30 seconds, 1, 5, and 15 minutes, 1 and 6 hours, and 1 day)
    - Threshold type ("Static" is recommended. "Anomaly" are also options.)
    - Condition ("Whenever call count is greater than", "equal to", "less than" are also options.)
    - Condition Value ("25%" is configured by default. Another other positive integer is allowable.)
    - Notification topic (AMS operations topics are automatically assigned. However any other, or custom, topic can also be added.)
2. Monitoring and operations Support
  - AMS operations monitors AWS Outposts metrics for network disconnection or component failures. AMS operations provides first response services for AWS Outposts issues, and escalates, if needed, to Premium support or EC2 support.
  - AMS operations is available to address issues related to your AWS Outposts unit.
3. When EC2 instance status or system status checks fail, AMS operations follows existing processes to bring the instance back online. If the restart fails or AWS Outposts capacity is insufficient, then an AMS operations team member notifies you directly to determine next steps.

AWS Outposts life cycle management

Once AWS Outposts has been onboarded to your AMS account, you are notified if any availability, capacity, or network exceptions, occur. You can decommission AWS Outposts directly through the AWS Outposts console or the AWS Outposts SPOC.

You can manage AWS Outposts directly in the AWS Outposts console using the AWS Outposts self-service provisioning service role or developer mode. You can also request AWS Outposts through your CSDM, or AWS Outposts single point of contact, (SPOC).

High-availability on AWS Outposts can be achieved by deploying two or more AWS Outposts. Configuring two or more AWS Outposts enables the multi-availability zone option for your Amazon Relational Database Service instances.

Provisioning AMS managed resources on AWS Outposts

Provisioning AWS resources hosted on AWS Outposts (e.g. EC2, EMR, EKS, ECS, EBS, and S3) in AMS accounts (Single-Account Landing Zone, Multi-Account Landing Zone, and Accelerate accounts) are subject to the same AMS support levels as resources in AWS Regions. You can use AMS change management, self-service provisioning services, or developer mode to create and modify the resources created on AWS Outposts.

Currently, all instance types (M5/M5d, C5/C5d, R5/R5d, I3en, G4dn), Amazon Elastic Block Store, Amazon Elastic Container Service, Amazon Elastic Kubernetes Service, Amazon EMR, Amazon Relational Database Service DBs, Application Load Balancers, and App Mesh Envoy proxy are available directly on AWS Outposts. These resources are eligible for the same AMS operations support as resources in existing regions.

Limitations of AMS on AWS Outposts

- Operational support for AWS Outposts-hosted resources is dependent on consistent network connectivity. AWS Outposts network disconnection prevents AMS operations from being able to troubleshoot any incidents or problems that occur on the disconnected AWS Outposts unit. For AMS on AWS Outposts service level contingencies, see the updated AWS Service Level Agreements (SLAs).
- Amazon Relational Database Service:
  - The create RDS change type (ct-2z60dyvto9g6c), by default, enables multi-AZ and requires a DB subnet group. DB subnet groups require two subnets in two separate Availability Zones (AZ). If you have only one AWS Outposts, creating a DB subnet group is an issue since AWS Outposts are only assigned to a single AZ. To circumvent this limitation, follow these instructions:
    1. Request a DB subnet group through an RFC with a Management | Other | Other CT, and specify the subnet on the AWS Outposts.
    2. Create a custom CFN template to deploy RDS on AWS Outposts, and specify the subnet group created in the previous step. To learn more about doing this, see Custom resources.
    3. Request that AMS deploy the CFN template containing the target RDS instance through the AMS CFN ingest CT (ct-36cn2avfrrj9v).
    4. Note that currently, RDS for AWS Outposts does not provide metrics and logs due to a limitation of RDS Service.
  - Workload ingest (WIGs): Linux WIGs only works if the pre-WIGs EC2 instance is on a non-AWS Outposts subnet. The reason is because Linux WIGs creates a WIGs node in the subnet of the first EC2 instance using m4.large, by default. As AWS Outposts doesn't have that instance type, WIGs is not able to launch its worker node. The workaround for this is to create the initial EC2 instance in a non-AWS Outposts subnet, then the target instance can be created on AWS Outposts. Moreover, currently, only Nitro-based EC2 instance types including C5, C5d, M5, M5d, R5, R5d, G4, and I3en are supported on AWS Outposts.
  - Amazon Elastic Block Store (EBS): Create EBS Volume CT (ct-16xg8qguovg2w) does not work, as volumes get created in AWS instead of AWS Outposts as we do not provide the AWS Outposts Amazon resource number (ARN) as an input parameter to the CT.
  - Network connectivity: Network connectivity is your responsibility per the AWS Outposts team.
  - Brownfield and account takeover: AWS Outposts activated in non-AMS accounts cannot be transitioned into AMS, due to the nature of AWS Outposts billing and enterprise support requirements.

AMS on AWS Outposts compliance

AMS on AWS Outposts compliance attestation

AWS Outposts control plane has been attested to HIPAA eligible, PCI and ISO compliance. However, AMS on AWS Outposts control plane has not been attested for AWS Outposts. For this reason, customers are encouraged to pursue compliance attestation AMS on AWS Outposts environment.

For controlling resource creation on the Outpost unit, customers are encouraged to segregate developer access to the Outpost, to prevent excess developer access in standard AMS managed accounts.

AMS Managed Workloads requiring FedRAMP compliance

Foremost, AMS management accounts must first be assessed for regulatory compliance, since control plane data would flow out of the AWS Outposts to AMS management accounts.

If FedRAMP certification is required and the AMS account structure is compliant, then it is recommended that you either utilize a datacenter vendor that already has the required certification and owns all of the service link appliance (or already encrypts egress data).

Finally, additional data protection can be put in place by working with your account team to deploy an SCP that restricts data to the AWS Outposts and prevents the creation of any in-region resources in the account hosting the Outpost.

Impact on existing compliance for AMS accounts

An account utilizing AWS Outposts does not need to be retested for compliance as long as no regulated data is being consumed and the account is logically separated. AMS management accounts can manage non-regulated and regulated accounts as long as cross account authentication/authorization and ingress/ egress data flows are segregated between VPCs. Therefore, even though both the non-compliant Outpost account and existing compliant application accounts are in the same organization (including shared services, networking, logging, master, security AMS services), the compliance application account still retains compliance since data is logically separated.

AMS on AWS Outposts FAQs

Which use cases qualify for AMS support on AWS Outposts?

AMS on AWS Outposts can be leveraged by enterprises needing a proven cloud operating model have workloads requiring low latency (e.g., factory robot management and mainframe migration), edge computing (e.g., remote workstations and edge data streamlining), and large data transfer loads.

Why should I use this feature?

AMS provides monitoring of AWS Outposts hardware and first response to any AWS Outposts hardware issue. Moreover, the following support features for all managed resources hosted on AWS Outposts:

- Logging, Monitoring, Guardrails, and Event Management
- Continuity Management
- Security and Access Management
- Patch Management
- Change Management
- Automated and Self-Service Provisioning Management
- Incident and Problem Management
- Reporting (Reporting for AWS Outposts hardware will not be initially supported with AMS on AWS Outposts)
- Service Request Management
- Developer Mode
- Enterprise Support

How do I use this feature?

AWS Outposts planning: During AWS Outposts planning, you have identified AMS on AWS Outposts use cases and will engage key stakeholders, including the AMS account team and AWS Outpost representatives, to align on capacity strategy.

Order validation: During order validation, you create an AWS Outposts site, and order your required capacity directly in the AWS Outposts console, or through your AWS Outposts account representative.

AWS Outposts onboarding to AMS: Once your AWS Outposts unit is activated in your AMS managed VPC, you can request that your AWS Outposts be onboarded to your AMS account by submitting a request for change (RFC) using the template in the AMS User Guide (AWS Outposts). AMS operations then creates a subnet and monitors for your Outpost using the inputs provided on the RFC.

Lifecycle management: Once AWS Outposts has been onboarded to your AMS account, you are notified of any availability, capacity, or network exceptions. You can decommission AWS Outposts directly through the AWS Outposts console or the AWS Outposts SPOC.

What are the limitations of AMS on AWS Outposts?

Data residency (e.g., country-specific data localization laws, etc.) use cases have not yet been validated for AMS on AWS Outposts.

AWS Outposts activated in non-AMS accounts cannot be transitioned into AMS, due to the nature of AWS Outposts billing and Enterprise Support requirements.

AWS Outposts control plane has been attested to HIPAA eligible, PCI and ISO compliance. However, AMS on AWS Outposts control plane has not been attested for AWS Outposts. For this reason, customers are encouraged to pursue compliance attestation AMS on AWS Outposts environment.

Can I opt out of this feature?

Provisioning AWS Outposts into your AMS environment is optional. Once deployed into your AMS account, AWS Outposts can be deprovisioned via the AWS Outposts console at any time, if no longer needed.

How will AMS on AWS Outposts be billed?

AMS uplift on AWS Outposts charges will be applied at the Group B tier.

How will the AMS Service Level Agreement change to accommodate AWS Outposts?

Incident management will be contingent on AWS Outposts availability. AWS Outposts availability is subject to customer network availability, which is the responsibility of the customer. AWS Outposts availability is also subject to AWS Outposts hardware uptime, which is dependent on AWS Outposts Service Level Agreements.

See also AWS Outposts FAQs.

AWS Systems Manager in AMS Advanced

An AWS Systems Manager document (SSM document) defines the actions that Systems Manager performs on your AWS resources. Systems Manager includes more than a dozen pre-configured documents that you can use by specifying parameters at runtime. Documents use JavaScript Object Notation (JSON) or YAML, and they include steps and parameters that you specify.

AWS Managed Services (AMS) is a trusted publisher for SSM documents. SSM documents owned by AMS are shared only with onboarded AMS accounts, always begin with a reserved prefix (AWSManagedServices-*), and show up in the Systems Manager console, as owned by Amazon. The AMS process for SSM document development and publishing follows AWS best practices and requires multiple peer reviews throughout the document life cycle. For more information on AWS best practices for sharing SSM Documents, please visit Best practices for shared SSM documents.

Available AMS Advanced SSM documents

AMS Advanced SSM documents are available exclusively to AMS Advanced customers, and are used to automate operational workflow to operate your account.

To see the available AMS Advanced SSM documents from the AWS Management Console:

1. Open the Systems Managerconsole at AWS Systems Manager console.
2. Choose **Shared with me**.
3. In the search bar, filter by **Document name prefix**, then **Equals**, and set the value to **AWSManagedServices-**.

   For AWS CLI instructions, see Using shared SSM documents.

AMS Advanced SSM document versions

SSM documents support versioning. AMS Advanced SSM documents can't be modified from the customer's account and can't be re-shared. They're centrally managed and maintained by AMS Advanced in order to operate the account.

Version numbers are incremented with each document update in a specific AWS Region. As new Regions become available, the same document content in two Regions can have different version numbers; this is typical and doesn't mean their behavior will be different. If you want to compare two AMS Advanced SSM documents, we recommend comparing their hashes with the AWS CLI:

```
aws ssm describe-document \
--name AWSManagedServices-DOCUMENTNAME \
--output text --query "Document.Hash"
```

Two SSM documents are identical if their hashes match.

Systems Manager pricing

There is no cost associated with AMS Advanced SSM document access. Runtime cost varies based on the type of SSM document, its steps, and runtime duration. For more information, refer to AWS Systems Manager pricing.

AMS and AWS Service Catalog

Topics

What is AWS Service Catalog in AMS?

AWS Service Catalog allows organizations to create and manage catalogs of AWS information technology (IT) services and enables IT administrators to create, manage, and distribute catalogs of approved products to end users in their accounts, who can then access the products they need in a personalized portal of services. Administrators can control which users have access to each product to enforce compliance with organizational business policies. Administrators can also set up roles so that end users only require IAM access to AWS Service Catalog in order to deploy approved resources. AWS Service Catalog allows your organization to benefit from increased agility and reduced costs because end users can find and launch only the products they need from a catalog that you control.

AWS Service Catalog provides you with an alternative to the AMS request for change (RFC) process for provisioning and updating resources in your AMS managed account(s). AMS manages all of the infrastructure operations tasks needed to run AWS at scale for all infrastructure resources provisioned through AWS Service Catalog including security, compliance, provisioning, availability, patch, monitoring, alerting, reporting, incident response, and cost optimization. Utilizing AWS Service Catalog in your AMS managed account provides you with a mechanism to centrally manage commonly deployed IT services and helps you achieve consistent governance while enabling users to quickly deploy only the approved IT services they need into their managed environments.

Service Catalog in AMS FAQs

Does AWS Service Catalog replace the existing AMS request for change (RFC) process?

In accounts where AWS Service Catalog is enabled, it will act as the change management system in which you provision and update IT services in your AMS account through your predefined product catalog; AMS will provide a default portfolio/product catalog, and your IT admins can create and configure your own. AWS Service Catalog will only acknowledge stacks provisioned through AWS Service Catalog. Likewise, services provisioned through AWS Service Catalog will not be modifiable through the AMS RFC process as modification outside of AWS Service Catalog will drift the stack from the approved product configuration.

Can I see stacks provisioned through service catalog in the AMS Console?

Yes. You can view all stacks provisioned through service catalog in the AMS console. Stacks provisioned through service catalog are easily identifiable by the stack ID of "SC-". Although stacks are viewable in the AMS console you will not be able to update through the AMS RFC process. Access to the AMS change management system (RFCs) is limited to access request, patch orchestration and back-up RFCs only.

If I provision and/or update a stack through AWS Service Catalog will there be a corresponding RFC in the AMS Console?

The only RFC that will show in the AMS console is an RFC to register the stack with AMS when a stack is initially provisioned. This RFC is filed automatically by the AMS validation process that is triggered when a stack is launched through AWS Service Catalog. All other provisioning and changes are tracked directly in AWS Service Catalog and are viewable in the AWS Service Catalog console. Furthermore, you can use the **Provisioned Product Plan** feature in AWS Service Catalog to view

the list of changes that will be made to the resources in advance of provisioning or updating the product.

Do I have to do anything specific for provisioning products in my AMS managed account?

Yes. All AWS Service Catalog products provisioned in AMS accounts must contain this line of JSON in the CFN template that defines that product:

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

This snippet of CloudFormation code triggers the AMS validations required before the resource can be provisioned in your AMS managed account. It is your responsibility to include this line of code as part of the product definition. If it is not included, provisioning will fail and the following error message will be displayed: "Failed to create product. This account is managed by AMS. All products in AMS accounts must have the AMS `Transform` code in the template."

Is there any AWS Service Catalog functionality not available and/or limited for AMS customers at launch?

Yes, the following SC features are not available for AMS customers at initial launch (but are planned for the future):

- Account Creation through AWS Service Catalog
- Ability to launch all AWS Services through AWS Service Catalog into an AMS-managed account. AWS Service availability is limited to AMS supported services (managed and self-provisioned). For more information on AMS-supported services, see the AMS service description.
- AWS Service Catalog IT service manager (ITSM) connectors will not communicate with AMS incident reports, and service requests.
- Ability to leverage AWS Service Catalog quick starts and reference architectures without modification. Remember that AWS Service Catalog products for AMS accounts must contain this line of JSON code:

  ```
  "Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
  {"Ref":"AWS::StackId"}}}
  ```

  in the CNF template. Note that this line is *not* part of a typical AWS CloudFormation template and must be explicitly added.
- Terraform is not currently supported by AMS for provisioning AWS Service Catalog products.
- AWS CFN stacksets are not supported in AMS.
- You cannot create custom IAM roles.
- Service Actions are limited to:
  - AWS-RebootRdsInstance
  - AWS-RestartEC2Instance
  - AWS-StartEC2Instance
  - AWS-StartRdsInstance
  - AWS-StopEC2Instance
  - AWS-StopRdsInstance
  - AWS-CreateImage
  - AWS-CreateRdsSnapshot
  - AWS-CreateSnapshot

    Note
    When creating service actions, you can configure the execution role to be the end user's permissions, the launch role, or a custom IAM role of your choosing. The

selected execution role must have sufficient permissions to perform the service action, and have a TrustPolicy that allows it to be assumed by Service Catalog, otherwise that service action will fail at execution time. We recommend using the AWSManagedServicesServiceCatalogLaunchRole, which has the correct permissions and trust policy to be used as a service action.

What will I still need to use the AMS RFC system for?

At general availability (GA) you will still need to use RFCS to run the following actions:

- Configuring Patch Orchestrator
- Configuring Back up policies
- Requesting instance access
- Creating and assigning security groups that fall outside AMS guidelines.
- Performing workload ingest (WIGS)
- Creating IAM roles

Can I use the AWS Service Catalog CLI to access AWS Service Catalog in my AMS managed account?

Yes, AWS Service Catalog APIs are available and enabled through the CLI. Actions from the management of AWS Service Catalog artifacts through the provisioning and terminating of those artifacts, are available. For more information, see AWS Service Catalog Resources, or download the latest AWS SDK or CLI.

Who creates, manages, and distributes customers' catalogs of approved products?

The customer's catalog administrator and/or IT administrator, or assigned resource, is responsible for the management of your AWS Service Catalog catalogs and approved products.

Can I use AMS AMIs?

AMS AMIs vended after March 2020 can be deployed through AWS Service Catalog.

How do I migrate to AMS using AWS Service Catalog?

To migrate your workload to AMS using AWS Service Catalog you begin by following the Workload Ingest (WIGs) process to create an AMI in AMS. You use the AMI produced by WIGS to create a product in AWS Service Catalog. How to do this is detailed in AWS Service Catalog - Getting Started.

How do I get started with AWS Service Catalog in AMS?

To get started with AWS Service Catalog in AMS, submit a service request through the AMS console to request access to AWS Service Catalog. Upon submission of the request, three IAM roles will be deployed into your account(s) along with an AMS managed stack containing the CloudFormation macro that invokes the AMS `Transform` (described previously) so we can register the products in our systems, and to perform operations against the infrastructure provisioned through AWS Service Catalog. The three IAM roles deployed include a role for IT admins to manage products as AWS Service Catalog admins; a role for application owners and end-users to configure, launch, and manage products; and a role that will be used as a launch constraint, that defines the permissions that AWS Service Catalog will use while launching or updating the your product.

AWS Managed Services Operations On Demand

Topics

Operations on Demand is an AWS Managed Services (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 catalog 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 catalog of standardized offerings and initiate a new Operations on Demand engagement through a service request. Examples of Operations on Demand offerings include assisting with the maintenance of Amazon EKS, operations of AWS Control Tower, and management of SAP clusters. New catalog offerings are added regularly based on demand and the operational use cases we see most often.

Operations on Demand is available for both AMS Advanced and AMS Accelerate Operations Plans and is available in all AWS Regions where AMS is available.

Operations on Demand catalog of offerings

Operations on Demand offers you the services described in the following table.

Title	Description	Expected Outcomes	Operations Plan
Amazon EKS Cluster Maintenance	AMS frees your container developers by handling the ongoing maintenance of your Amazon Elastic Kubernetes Service (Amazon EKS) deployments. While Amazon EKS simplifies the provisioning, scaling, and management of Kubernetes clusters and nodes, customers are still responsible for ongoing maintenance of the underlying system. For example, the Kubernetes project releases updates	Assist customer teams with the underlying operations work of updating Amazon EKS clusters.	AMS Advanced and AMS Accelerate

	regularly and will only support branches for up to a year. AMS will handle updates to the control plane, add-ons, and nodes so that your container developers can focus on their applications.		
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.	AMS Accelerate
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.	AMS Accelerate

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 (e.g. lost the source code, ISV out of business, etc.). 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.	AMS Advanced and AMS Accelerate
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.	AMS Accelerate

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

Note
For definitions of key terms refer to the AWS Managed Services Documentation Key Terms.

Requesting AMS Operations On Demand

AWS Managed Services; (AMS) Operations on Demand (Operations on Demand) is available for all AWS accounts that have been onboarded to AMS. To take advantage of Operations on Demand, request additional information from your cloud service delivery manager (CSDM), Solutions Architect (SA), account manager, or Cloud Architect (CA). Available Operations on Demand offerings are listed in the Operations on Demand catalog of offerings (p. 134). Once the engagement scoping is completed, submit a service request to AMS Operations to initiate an engagement for Operations on Demand.

Each Operations on Demand service request must contain the following detailed information pertaining to the engagement:

- The specific Operations on Demand offerings requested, and for each specific Operations on Demand 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 AWS's then-current standard rate for the applicable Operations on Demand offering) to allocate to the specific Operations on Demand offering
  - The account ID for each AWS Managed Services account for which the specific Operations on Demand offering is being requested

After the Operations on Demand service request is received, AMS Operations will review and update with their approval, partial approval, or denial.

Once approved, AMS and you coordinate to begin the engagement. No Operations on Demand offerings requested through an Operations on Demand service request are initiated until the service request is approved.

Operations on Demand service requests must be submitted by you through either:

- The AWS Managed Services account that will receive the applicable Operations on Demand offerings, or
- An AWS Managed Services account that is an AWS Organizations Management account in **all features** mode, on behalf of any of its member accounts that are AWS Managed Services accounts.

Engagements for Operations on Demand offerings begin on the first day of the first calendar month after the Operations on Demand service request is approved, except in cases where the approval occurs

after the 20th day of a given calendar month, in which case the engagement begins on the first day of the second calendar month following the month in which approval occurs, unless mutually agreed by AWS and the customer.

Making changes to Operations on Demand offerings

To request changes to ongoing engagements for Operations on Demand offerings, 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 Operations on Demand service request, AMS Operations reviews the request and either updates with their approval or requests that the assigned CSDM work with you to determine the scope and implications of the modification. If the modification is determined to require a scoping effort with the CSDM, you are required to submit a second Operations on Demand service request to initiate the modified engagement following the completion of the scoping exercise. Once approved, the modified engagement becomes effective on the first day of the first calendar month after the Operations on Demand service request is approved, except in cases where the approval occurs after the 20th day of a given calendar month in which case the engagement begins on the first day of the second calendar month following the month in which approval occurs, unless mutually agreed by AWS and the customer.

Reporting in AMS

Topics

AMS collates data from various native AWS services to provide value added reports on major AMS offerings.

AWS Managed Services (AMS) offers two types of detailed reporting:

- On request reporting: Certain reports can be requested ad hoc through your cloud service delivery manager (CSDM)
- Self-service reporting: You can generate some reports yourself

On-request reporting

Topics

AMS collates data from various native AWS services to provide value added reports on major AMS offerings. For a copy of these reports, make a request to your Cloud Service Delivery Manager (CSDM).

Patch reporting

Topics

Instance Details Summary

The objective of this report is to provide instance details gathered for instances that are onboarded to reporting. This is an informational report that helps identify all the instances onboarded, account status, instance details, maintenance window coverage, maintenance window execution time, stack details, and platform type.

This report provides:

1. Insights into Production and Non-Production Instances of an account. Note: Production and Non-Production stage is derived from the Account Name and not from the Instance Tags.

2. Insights into distribution of instances by platform type. Note: 'N/A' platform type is when AWS Systems Manager (SSM) is not able to get the platform information.
3. Insights into distribution of state of instances, number of instances running/stopped/terminating.

Field Name	Definition
Report Datetime	The date and time the report was generated.
Account Id	AWS Account ID to which the instance ID belongs
Account Name	AWS account name
Production Account	Identifier of AMS prod, non-prod accounts, depending on whether account name include value 'PROD', 'NONPROD'. Example: PROD, NONPROD, Not Available
Account Status	AMS account status. For example: ACTIVE, INACTIVE
AMS account service commitment	PREMIUM, PLUS
Landing Zone	Flag for account landing zone type. For example: MALZ, NON-MALZ
Access Restrictions	Regions to which access is restricted. For example: US SOIL
Instance Id	ID of EC2 instance
Instance Name	Name of EC2 instance
Instance Platform Type	Operating System (OS) type. For example: Windows, Linux, and so forth
Instance Platform Name	Operating System (OS) name. For example: MicrosoftWindowsServer2012R2Standard, RedHatEnterpriseLinuxServer
Stack Name	Name of stack that contains instance
Stack Type	AMS stack (AMS infrastructure within customer account) or Customer stack (AMS managed infrastructure that supports customer applications). Examples: AMS, CUSTOMER
Auto Scaling Group Name	Name of Auto Scaling Group (ASG) that contains the instance
Instance Patch Group	Patch group name used to group instances together and apply the same maintenance window. If the patch group is unassigned the value will be “Unassigned”
Instance Patch Group Type	Patch group type. DEFAULT: default patch group w/ default maintenance window, determined by AMSDefaultPatchGroup:True tag on the instance CUSTOMER: customer created patch group NOT_ASSIGNED: no patch group assigned

Field Name	Definition
Instance State	State within the EC2 instance lifecycle. Examples: TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING. For more information, see Instance lifecycle.
Maintenance Window Coverage	If there is a future Maintenance Window on this instance. Examples: COVERED or NOT_COVERED
Maintenance Window Execution Datetime	Next time the maintenance window is expected to execute. If NULL, single window execution, i.e. not recurring

Patch Details

The objective of this report is to provide patch details and maintenance window coverage of various instances.

This report provides:

1. Insights on Patch groups and its types.
2. Insights on Maintenance Windows, duration, cutoff, future dates of maintenance window executions (schedule) and instances impacted in each window.
3. Insights on all the operating systems under the account and number of instances that operating system is installed.

Field Name	Definition
Report Datetime	The date and time the report was generated.
Account Id	AWS Account ID to which the instance ID belongs
Account Name	AWS account name
Instance Id	ID of EC2 instance
Production Account	Identifier of AMS prod, non-prod accounts, depending on whether account name include value 'PROD', 'NONPROD'. If data is not available value will be “Not Available”
Account Status	AMS account status. For example: ACTIVE, INACTIVE
Instance Platform Type	Operating System (OS) type. For example: Windows, Linux
Instance Platform Name	Operating System (OS) name. For example: MicrosoftWindowsServer2012R2Standard, RedHatEnterpriseLinuxServer
Stack Type	AMS stack (AMS infrastructure within customer account) or Customer stack (AMS managed

Field Name	Definition
	infrastructure that supports customer applications). For example: AMS, CUSTOMER
Instance Patch Group	Patch group name used to group instances together and apply the same maintenance window. If the patch group is unassigned the value will be “Unassigned”
Instance Patch Group Type	Patch group type. DEFAULT: default patch group w/ default maintenance window, determined by AMSDefaultPatchGroup:True tag on the instance CUSTOMER: customer created patch group UNASSIGNED: no patch group assigned
Instance State	State within the EC2 instance lifecycle. For example: TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING For more information, see Instance lifecycle.
Maintenance Window Id	Maintenance window identifier
Maintenance Window State	Possible values are ENABLED or DISABLED.
Maintenance Window Type	Maintenance window type
Maintenance Window Next Execution Datetime	Next time the maintenance window is expected to execute. If NULL, single window execution, i.e. not recurring
Last Execution Maintenance Window	The latest time the maintenance window was executed
Maintenance Window Duration (hrs)	The duration of the maintenance window in hours
Maintenance Window Coverage	The maintenance window coverage
Patch Baseline Id	Patch baseline currently attached to instance
Patch Status	Overall patch compliance status. For example: COMPLIANT, NON_COMPLIANT. If there is at least one missing patch, instance is considered noncompliant, otherwise compliant.
Compliant - Total	Count of compliant patches (all severities)
Noncompliant - Total	Count of noncompliant patches (all severities)
Compliant - Critical	Count of compliant patches with "critical" severity
Compliant - High	Count of compliant patches with "high" severity
Compliant - Medium	Count of compliant patches with "medium" severity
Compliant - Low	Count of compliant patches with "low" severity
Compliant - Informational	Count of compliant patches with "informational" severity

Field Name	Definition
Compliant - Unspecified	Count of compliant patches with "unspecified" severity
Noncompliant - Critical	Count of noncompliant patches with "critical" severity
Noncompliant - High	Count of noncompliant patches with "high" severity
Noncompliant - Medium	Count of noncompliant patches with "medium" severity
Noncompliant - Low	Count of noncompliant patches with "low" severity
Noncompliant - Informational	Count of noncompliant patches with "informational" severity
Noncompliant - Unspecified	Count of noncompliant patches with "unspecified" severity

Instances that missed patches

The objective of this report is to provide details on instances that missed patches during the last maintenance window execution.

This report provides:

1. Insights on missing patches at the patch ID level.
2. Insights on all the instances which have at least one patch missing along with attributes such as patch severity, unpatched days, range, and release date of the patch.

Field Name	Definition
Report Datetime	The date and time the report was generated.
Account Id	AWS Account ID to which the instance ID belongs
Account Name	AWS account name
Production Account	Identifier of AMS prod, non-prod accounts, depending on whether the account name includes the value 'PROD', 'NONPROD'.
Account Status	AMS account status. For example: ACTIVE or INACTIVE
AMS account service tier	PREMIUM or PLUS
Instance Id	ID of EC2 instance
Instance Platform Type	Operating System (OS) type. For example: Windows
Instance State	State of the EC2 instance lifecycle. For example: TERMINATED, RUNNING, STOPPING, STOPPED,

Field Name	Definition
	SHUTTING-DOWN, PENDING For more information, see Instance lifecycle.
Patch Id	ID of released patch. For example: KB3172729
Patch Severity	Severity of patch per publisher. For example: CRITICAL, IMPORTANT, MODERATE, LOW, UNSPECIFIED
Patch Classification	Classification of patch per publisher. For example: CRITICALUPDATES, SECURITYUPDATES, UPDATEROLLUPS, UPDATES, FEATUREPACKS
Patch Release Datetime (UTC)	Release date of patch per publisher
Patch Install State	Install state of patch on instance per SSM. For example: INSTALLED, MISSING, NOT APPLICABLE
Days Unpatched	Number of days instance unpatched since last SSM scanning
Days Unpatched Range	Bucketing of days unpatched. For example: <30 DAYS, 30-60 DAYS, 60-90 DAYS, 90+ DAYS

Backup reporting

Topics

Backup snapshot success/failure

Backup snapshot success/failure reporting

This report provides:

1. Insights on number of distinct snapshots taken.
2. The backup success rate.

Field Name	Definition
Report Datetime	The date and time the report was generated
AWS Account ID	AWS Account ID to which the resource belongs
Account Name	AWS account name
Backup Type	The type of backup if there is a plan
Backup Plan Name	User defined backup plan name
Backup Vault Name	The name of the backup vault

Field Name	Definition
Resource Type	The type of resource that is being backed up
# of Resources	The number of resources that were backed up
Resource Region	The region of the backed up resource
Backup State	The state of the backup
Recovery Point ID	The unique identifier of the recovery point

Backup summary

Backup summary reporting

This report provides: Insights on important backup metrics.

Field Name	Definition
Customer Name	Customer name for situations where multiple sub-customers are
Backup Month	Month of the backup
Backup Year	Year of the backup
Resource Type	The type of resource that is being backed up
# of Resources	The number of resources that were backed up
Distinct Snapshots	Number of distinct snapshots
Backup Success Rate	The rate of successful backups
Max Snapshot Age	The maximum snapshot age
Backups Greater Than 30 Days Old	The count of backups that are over 30 days old

Backup snapshot aged

Backup snapshot aged reporting

This report provides:

1. Aging of backup snapshots.
2. Classify backup snapshots into different aging buckets.
3. Understand which resources are out of backup compliance.

Field Name	Definition
Report Datetime	The date and time the report was generated
AWS Account ID	AWS Account ID to which the resource belongs
Account Name	AWS account name

Field Name	Definition
Backup Type	The type of backup if there is a plan
Backup Plan Name	User defined backup plan name
Backup Vault Name	The name of the backup vault
Resource Type	The type of resource that is being backed up
# of Resources	The number of resources that were backed up
Resource Region	The region of the backed up resource
Backup State	The state of the backup
Recovery Point ID	The unique identifier of the recovery point
Distinct Snapshots	The number of distinct snapshots
Snapshot Age (days)	The age in days of the snapshot
Backups Greater Than 30 Days Old	The number of backups that are over 30 days old
Backups 15-30 Days Old	The number of backups that are between 15 and 30 days
Backups Less Than 15 Days Old	The number of backups that are less than 15 days old

Billing reporting

Topics

AMS Billing Charges Details reporting

The objective of this report is to provide details about AMS billing charges with linked accounts and respective AWS services.

This report provides:

1. Insights on AMS service-level charges, uplift percentages, account-level AMS service tiers and AMS fees.
2. Insights on linked accounts and AWS usage charges

Field Name	Definition
Billing Month	The month and year of the service billed
Payer Account Id	The 12 digit id identifying the account that will be responsible for paying the ams charges
Linked Account Id	The 12 digit id identifying the AMS account that consumes services that generates expanses

Field Name	Definition
AWS Service Name	The AWS service that was used
AWS Charges	The AWS charges for the AWS service name in AWS Service Name
Pricing Plan	The pricing plan associated with the linked account
Uplift Proportion	The uplift percentage (as a decimal V.WXYZ) based on pricing_plan, SLA, and AWS service
Adjusted AWS Charges	AWS usage adjusted for AMS
Uplifted AWS Charges	The percentage of AWS charges to be charged for AMS; adjusted_aws_charges * uplift_percent
Instances EC2 RDS Spend	Spend on EC2 and RDS instances
AMS Charges	Total ams charges for the product; uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp
Prorated Minimum Fee	The amount we charge to meet the contractual minimum
Minimum Fee	AMS Minimum Fees (if applicable)
Linked Account Total AMS Charges	Sum of all charges for the linked_account
Payer Account Total AMS Charges	Sum of all charges for payer account

Self-service reporting

Topics

AWS Managed Services (AMS) Self-Service Reporting (SSR) feature collates data from various native AWS services and provides access to reports on major AMS offerings. It also provides the information needed to support operations, configuration management, asset management, security management and compliance.

Use SSR to access the reports from the AMS console and report datasets through S3 buckets (one bucket per account) so you can plug it into your favorite Business Intelligence (BI) tool for customizing the reports based on your unique needs. AMS creates this S3 bucket in your primary AWS Region, and the data is shared from the AMS control plane hosted in us-east-1.

Important
You need one of the following role to access this feature:

- Multi-Account Landing Zone: **AWSManagedServicesReadOnlyRole**
- Single-Account Landing Zone: **Customer_ReadOnly_Role**

Daily Patch reports

These reports provide patching details.

Topics

Instance details summary (Patch Orchestrator)

This is an informational report that helps identify all the instances onboarded to Patch Orchestrator (PO), account status, instance details, maintenance window coverage, maintenance window execution time, stack details, and platform type.

This dataset provides:

- Insights into Production and Non-Production instances of an account. Production and Non-Production stage is derived from the account name and not from the instance tags.
- Insights into distribution of instances by platform type. The 'N/A' platform type is when AWS Systems Manager (SSM) is not able to get the platform information.
- Insights into distribution of state of instances, number of instances running, stopped, or terminating.

Console Field Name	Dataset Field Name	Definition
Report Datetime	dataset_datetime	The date and time the report was generated.
Account Id	aws_account_id	AWS Account ID to which the instance ID belongs
Account Name	account_name	AWS account name
Production Account	prod_account	Identifier of AMS prod, non-prod accounts, depending on whether account name include value 'PROD', 'NONPROD'.
Account Status	account_status	AMS account status
	account_sla	AMS account service commitment
Landing Zone	malz_flag	Flag for MALZ-related account
Account Type	malz_role	MALZ role
Access Restrictions	access_restrictions	Regions to which access is restricted
Instance Id	instance_id	ID of EC2 instance

Console Field Name	Dataset Field Name	Definition
Instance Name	instance_name	Name of EC2 instance
Instance Platform Type	instance_platform_type	Operating System (OS) type
Instance Platform Name	instance_platform_name	Operating System (OS) name
Stack Name	instance_stack_name	Name of stack that contains instance
Stack Type	instance_stack_type	AMS stack (AMS infrastructure within customer account) or Customer stack (AMS managed infrastructure that supports customer applications)
Auto Scaling Group Name	instance_asg_name	Name of Auto Scaling Group (ASG) that contains the instance
Instance Patch Group	instance_patch_group	Patch group name used to group instances together and apply the same maintenance window
Instance Patch Group Type	instance_patch_group_type	Patch group type
Instance State	instance_state	State within the EC2 instance lifecycle
Maintenance Window Coverage	mw_covered_flag	If an instance has at least one enabled maintenance window with a future execution date, then it's considered covered, otherwise not covered
Maintenance Window Execution Datetime	earliest_window_execution_time	Next time the maintenance window is expected to execute

Patch details

This report provides patch details and maintenance window coverage of various instances.

This report provides:

- Insights on Patch groups and its types.
- Insights on Maintenance Windows, duration, cutoff, future dates of maintenance window executions (schedule) and Instances impacted in each window.
- Insights on all the operating systems under the account and number of instances that operating system is installed.

Field Name	Dataset Field Name	Definition
Report Datetime	dataset_datetime	The date and time the report was generated.

Field Name	Dataset Field Name	Definition
Account Id	aws_account_id	AWS Account ID to which the instance ID belongs
Account Name	account_name	AWS account name
Instance Id	instance_id	ID of EC2 instance
Instance Name	instance_name	Name of EC2 instance
Production Account	prod_account	Identifier of AMS prod, non-prod accounts, depending on whether account name include value 'PROD', 'NONPROD'.
Account Status	account_status	AMS account status
	account_sla	AMS account service tier
Instance Platform Type	instance_platform_type	Operating System (OS) type
Instance Platform Name	instance_platform_name	Operating System (OS) name
Stack Type	instance_stack_type	AMS stack (AMS infrastructure within customer account) or Customer stack (AMS managed infrastructure that supports customer applications)
Instance Patch Group Type	instance_patch_group_type	DEFAULT: default patch group w/ default maintenance window, determined by AMSDefaultPatchGroup:True tag on the instance CUSTOMER: customer created patch group NOT_ASSIGNED: no patch group assigned
Instance Patch Group	instance_patch_group	Patch group name used to group instances together and apply the same maintenance window
Instance State	instance_state	State within the EC2 instance lifecycle
Maintenance Window Id	window_id	Maintenance window ID
Maintenance Window State	window_state	Maintenance window state
Maintenance Window Type	window_type	Maintenance window type
Maintenance Window Next Execution Datetime	window_next _execution_time	Next time the maintenance window is expected to execute
Last Execution Maintenance Window	last_execution_window	The latest time the maintenance window was executed

Field Name	Dataset Field Name	Definition
	window_next_exec_yyyy	Year part of window_next_execution_time
	window_next_exec_mm	Month part of window_next_execution_time
	window_next_exec_D	Day part of window_next_execution_time
	window_next _exec_HHMI	Hour:Minute part of window_next_execution_time
Maintenance Window Duration (hrs)	window_duration	The duration of the maintenance window in hours
Maintenance Window Coverage	mw_covered_flag	If an instance has at least one enabled maintenance window with a future execution date, then it's considered covered, otherwise not covered
Patch Baseline Id	patch_baseline_id	Patch baseline currently attached to instance
Patch Status	patch_status	Overall patch compliance status. If there is at least one missing patch, instance is considered noncompliant, otherwise compliant.
Compliant - Critical	compliant_critical	Count of compliant patches with "critical" severity
Compliant - High	compliant_high	Count of compliant patches with "high" severity
Compliant - Medium	compliant_medium	Count of compliant patches with "medium" severity
Compliant - Low	compliant_low	Count of compliant patches with "low" severity
Compliant - Informational	compliant_informational	Count of compliant patches with "informational" severity
Compliant - Unspecified	compliant_unspecified	Count of compliant patches with "unspecified" severity
Compliant - Total	compliant_total	Count of compliant patches (all severities)
Noncompliant - Critical	noncompliant_critical	Count of noncompliant patches with "critical" severity
Noncompliant - High	noncompliant_high	Count of noncompliant patches with "high" severity

Field Name	Dataset Field Name	Definition
Noncompliant - Medium	noncompliant_medium	Count of noncompliant patches with "medium" severity
Noncompliant - Low	noncompliant_low	Count of noncompliant patches with "low" severity
Noncompliant - Informational	noncompliant _informational	Count of noncompliant patches with "informational" severity
Noncompliant - Unspecified	noncompliant _unspecified	Count of noncompliant patches with "unspecified" severity
Noncompliant - Total	noncompliant_total	Count of noncompliant patches (all severities)

Instances that missed patches

This report provides details on instances that missed patches during the last maintenance window execution.

This report provides:

- Insights on missing patches at the patch id level.
- Insights on all the instances which have at-least one patch missing along with attributes such as patch severity, unpatched days, range, and release date of the patch.

Field Name	Dataset Field Name	Definition
Report Datetime	dataset_datetime	The date and time the report was generated.
Account Id	aws_account_id	AWS Account ID to which the instance ID belongs
Account Name	account_name	AWS account name
Customer Name Parent	customer_name_parent	
Customer Name	customer_name	
Production Account	prod_account	Identifier of AMS prod, non-prod accounts, depending on whether account name include value 'PROD', 'NONPROD'.
Account Status	account_status	AMS account status
Account Type	account_type	
	account_sla	AMS account service tier
Instance Id	instance_id	ID of EC2 instance
Instance Name	instance_name	Name of EC2 instance

Field Name	Dataset Field Name	Definition
Instance Platform Type	instance_platform_type	Operating System (OS) type
Instance State	instance_state	State within the EC2 instance lifecycle
Patch Id	patch_id	ID of released patch
Patch Severity	patch_sev	Severity of patch per publisher
Patch Classification	patch_class	Classification of patch per publisher
Patch Release Datetime (UTC)	release_dt_utc	Release date of patch per publisher
Patch Install State	install_state	Install state of patch on instance per SSM
Days Unpatched	days_unpatched	Number of days instance unpatched since last SSM scanning
Days Unpatched Range	days_unpatched_bucket	Bucketing of days unpatched

Monthly billing report

Monthly billing report.

Billing charges details

This report provides details about AMS billing charges with linked accounts and respective AWS services.

This report provides:

- Insights on AMS service-level charges, uplift percentages, account-level AMS service tiers and AMS fees.
- Insights on linked accounts and AWS usage charges.

Field Name	Dataset Field Name	Definition
Billing Date	date	The month and year of the service billed
Payer Account Id	payer_account_id	The 12 digit id identifying the account that will be responsible for paying the ams charges
Linked Account Id	linked_account_id	The 12 digit id identifying the AMS account that consumes services that generates expanses
AWS Service Name	product_name	The AWS service that was used

Field Name	Dataset Field Name	Definition
AWS Charges	aws_charges	The AWS charges for the AWS service name in AWS Service Name
Pricing Plan	pricing_plan	The pricing plan associated with the linked account
AMS Service Group	tier_uplifting_groups	AMS service group code that determines uplift percentage
Uplift Proportion	uplift_percent	The uplift percentage (as a decimal V.WXYZ) based on pricing_plan, SLA, and AWS service
Adjusted AWS Charges	adjusted_aws_usage	AWS usage adjusted for AMS
Uplifted AWS Charges	uplifted_aws_charges	The percentage of AWS charges to be charged for AMS; adjusted_aws_charges * uplift_percent
Instances EC2 RDS Spend	instances_ec2_rds_spend	Spend on EC2 and RDS instances
Reserved Instance Charges	ris_charges	Reserved instance charges
Uplifted Reserved Instance Charges	uplifted_ris	The percentage of reserved instance charges to be charged for AMS; ris_charges * uplift_percent
Savings Plan Charges	sp_charges	SavingsPlan usage charges
Uplifted Savings Plan Charges	uplifted_sp	The percentage of savings plans charges to be charged for AMS; sp_charges * uplift_percent
AMS Charges	ams_charges	Total ams charges for the product; uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp
Prorated Minimum Fee	prorated_minimum	The amount we charge to meet the contractual minimum
Linked Account Total AMS Charges	linked_account_total _ams_charges	Sum of all charges for the linked_account
Payer Account Total AMS Charges	payer_account_total _ams_charges	Sum of all charges for payer account
Minimum Fee	minimum_fees	AMS Minimum Fees (if applicable)

Field Name	Dataset Field Name	Definition
Reserved Instance and Savings Plan discount	adj_ri_sp_charges	RI/SP discount to be applied against RI/SP charges (applicable under certain circumstances)

Daily backup report

This report provides details about the status of backup (success/failure) and insights into snapshots taken.

This report provides:

- Backup status
- Number of snapshots taken
- Recovery point
- Backup plan and vault information

Field Name	Dataset Field Name	Definition
Report Datetime	dataset_datetime	The date and time the report was generated.
Account Id	aws_account_id	AWS Account ID to which the instance ID belongs
Account Name	account_name	AWS account name
Account SLA	account_sla	AMS account service commitment
	malz_flag	Flag for MALZ-related account
	malz_role	MALZ role
	access_restrictions	Regions to which access is restricted
Resource ARN	resource_arn	The Amazon resource name
Resource Id	resource_id	The unique resource identifier
Resource Region	resource_region	The region of the resource
Resource Type	resource_type	The type of resource
Recovery Point ARN	recovery_point_arn	The ARN of the recovery point
Recovery Point Id	recovery_point_id	The unique identifier of the recovery point
Backup snapshot scheduled start datetime	start_by_dt_utc	Timestamp when snapshot is scheduled to begin

Field Name	Dataset Field Name	Definition
Backup snapshot actual start datetime	creation_dt_utc	Timestamp when snapshot actually begins
Backup snapshot completion datetime	completion_dt_utc	Timestamp when snapshot is completed
Backup snapshot expiration datetime	expiration_dt_utc	Timestamp when snapshot expires
Backup Job status	backup_job_status	State of the snapshot
Backup Type	backup_type	Type of backup
Backup Job Id	backup_job_id	The unique identifier of the backup job
Backup Size In Bytes	backup_size_in_bytes	The backup size in bytes
Backup Plan ARN	backup_plan_arn	The backup plan ARN
Backup Plan Id	backup_plan_id	Backup plan unique identifier
Backup Plan Name	backup_plan_name	The Backup Plan name
Backup Plan Version	backup_plan_version	The backup plan version
Backup Rule Id	backup_rule_id	The backup rule id
Backup Vault ARN	backup_vault_arn	Backup vault ARN
Backup Vault Name	backup_vault_name	The backup vault name
IAM Role ARN	iam_role_arn	The IAM role ARN
Recovery Point Status	recovery_point_status	Recovery point status
Recovery Point Delete After Days	recovery_point_delete_after_days	Recovery point delete after days
Recovery point move to cold storage after days	recovery_point_move_to_cold_storage_after_days	Number of days after completion date when backup snapshot is moved to cold storage
Recovery Point Encryption Status	recovery_point_is_encrypted	Recovery point encryption status
Recovery Point Encryption Key ARN	recovery_point_encryption_key_arn	Recovery point encryption key ARN
Volume State	volume_state	Volume State
Instance Id	instance_id	Unique instance Id
Instance State	instance_state	Instance state
Stack Id	stack_id	Cloudformation stack unique identifier
Stack Name	stack_name	Stack Name

Field Name	Dataset Field Name	Definition
Tag: AMS Default Patch Group	tag_ams_default_patch_group	Tag Value: AMS Default Patch Group
Tag: App Id	tag_app_id	Tag Value: App ID
Tag: App Name	tag_app_name	Tag Value: App Name
Tag: Backup	tag_backup	Tag Value: Backup
Tag: Compliance Framework	tag_compliance_framework	Tag Value: Compliance Framework
Tag: Cost Center	tag_cost_center	Tag Value: Cost Center
Tag: Customer	tag_customer	Tag Value: Customer
Tag: Data Classification	tag_data_classification	Tag Value: Data Classification
Tag: Environment Type	tag_environment_type	Tag Value: Environment Type
Tag: Hours of Operation	tag_hours_of_operation	Tag Value: Hours of Operation
Tag: Owner Team	tag_owner_team	Tag Value: Owner Team
Tag: Owner Team Email	tag_owner_team_email	Tag Value: Owner Team Email
Tag: Patch Group	tag_patch_group	Tag Value: Patch Group
Tag: Support Priority	tag_support_priority	Tag Value: Support Priority

Weekly Incident report

This report provides the aggregated list of incidents along with its priority, severity and latest status, including:

- Insights on support cases categorized as incidents on the managed account
- Incident information required to visualize the incident metrics for the managed account
- Insights on incident categories and remediation status of every incident

Both visualization and data are available for the Weekly incident report.

- Visualization can be accessed through AWS Managed Services (AMS) console in the account through the **Reports** page.
- Dataset with the following schema, can be accessed through S3 bucket in the managed account.

Field Name	Dataset Field Name	Definition
Report Datetime	dataset_datetime	The date and time the report was generated
Account Id	aws_account_id	AWS Account ID to which the incident belongs
Account Name	account_name	AWS account name

Field Name	Dataset Field Name	Definition
Case Id	case_id	The ID of the incident
Created Month	created_month	The month when the incident was created
Priority	priority	The priority of the incident
Severity	severity	The severity of the incident
Status	status	The status of the incident
Category	yuma_category	The category of the incident

Data retention policy

AMS SSR has a data retention policy per report after the period reported, the data is cleared out and no longer available.

Report name	Data Retention SSR Console	Data Retention SSR S3 Bucket
Instance Details Summary (Patch Orchestrator)	2 Months	2 Years
Patch Details	2 Months	2 Years
Instances that missed patches during maintenance window execution	2 Months	2 Years
AMS Billing Charges Details	2 Years	2 Years
Daily Backup Report	1 Month	2 Years
Weekly Incident Report	2 Months	2 Years

Offboarding from SSR

To offboard from the SSR service please create a service request (SR) through the AMS console an AMS operations engineers will help you offboard from SSR. In the ticket please provide the reason for offboarding.

If you are offboarding and account and want to do a cleanup please create an SR through the AMS console and AMS operations engineers will help delete SSR S3 bucket.

If you are leaving AMS you will automatically be offboarded from the AMS SSR console. AMS will automatically stop sending data to your account. AMS deletes your SSR S3 bucket as part of offboarding process.

AMS Advanced Developer mode

Topics

AWS Managed Services (AMS) Developer mode uses elevated permissions in AMS Advanced Plus and Premium accounts to provision and update AWS resources outside of the AMS Advanced change management process. AMS Advanced Developer mode does this by leveraging native AWS API calls within the AMS Advanced Virtual Private Cloud (VPC), enabling you to design and implement infrastructure and applications in your managed environment.

When using an account that has Developer mode enabled, continuity management, patch management, and change management are provided for resources provisioned through the AMS Advanced change management process or by using an AMS Amazon Machine Image (AMI). However, these AMS management features are not offered for resources provisioned through native AWS APIs.

You are responsible for monitoring infrastructure resources that are provisioned outside of the AMS Advanced change management process. Developer mode is compatible with both production and non-production workloads. With elevated permissions, you have an increased responsibility to ensure adherence to internal controls.

> **Important**
> Resources that you create using Developer mode can be managed by AMS Advanced only if they are created using AMS Advanced change management processes.

Developer mode is one of the AMS Advanced modes you can employ. For more information, see AMS Advanced Modes.

Implementing AMS Advanced Developer mode

This section describes the kind of AMS Advanced accounts you can use with AMS Advanced Developer mode and how to successfully implement Developer mode.

Topics

Before you begin

Before implementing Developer mode, there are a few things you should know.

AMS Advanced cannot manage existing stacks or resources in a DevMode account that were created outside of the AMS Advanced change management process through requests for change (RFCs). However, while the account is in DevMode, AMS Advanced continues to manage resources provisioned through the AMS Advanced change management process with RFCs.

You cannot start with a DevMode account and later covert it to an AMS Advanced-managed application account.

Prerequisites for Developer mode

The following are the prerequisites for implementing Developer mode:

- You must be an AMS Advanced customer with at least one onboarded AMS Advanced Plus or Premium account.
- Any account you use must be an AMS Advanced Plus or Premium account.
- **Multi-Account Landing Zone (MALZ)**: You must use the `AWSManagedServicesDevelopmentRole` predefined AWS Identity and Access Management (IAM) role. You request this role. The next section describes how to acquire Developer mode permissions.
- **Single-Account Landing Zone (SALZ)**: You must use the `customer_developer_role` predefined AWS Identity and Access Management (IAM) role. You request this role. The next section describes how to acquire Developer mode permissions.

How to implement AMS Advanced Developer mode

You implement Developer mode by requesting that your eligible AMS Advanced account be provisioned with the predefined IAM role:

- **MALZ**: `AWSManagedServicesDevelopmentRole`
- **SALZ**: `customer_developer_role`

You then assign the role to the relevant users in your federated network. Use either an RFC with the Management | Other | Other change type, or a service request.

AMS Advanced recommends that you ensure that your use of Developer mode complies with your internal control frameworks and standards as Developer mode creates two vectors of change: AMS Advanced change management for AMS Advanced-managed resources and customer-managed role federation for resources that you, as our customer, manage. While AMS Advanced processes remain compliant with our declarations, customer processes and control frameworks might need to be updated.

To implement Developer mode in your AMS Advanced account

1. Confirm the account that you want to use with Developer mode meets the requirements listed in Prerequisites for Developer mode (p. 160).
2. Submit a request for change (RFC) using the change type (CT) Management | Managed account | Developer mode | Enable. For an example of how to use this CT, see Developer mode: enabling.

   After the CT is processed, the predefined IAM role, (`AWSManagedServicesDevelopmentRole` for **MALZ**, `customer_developer_role` for **SALZ**), is provisioned in the requested account.
3. Assign the appropriate role to the users that require Developer mode access using your internal federation process.

AMS Advanced recommends that you limit access to prevent unwanted or unapproved provisioning of or changes to resources.

AMS Advanced Developer mode permissions

The predefined role (`AWSManagedServicesDevelopmentRole` for **MALZ**, `customer_developer_role` for **SALZ**), grants permission to create application infrastructure resources within the AMS Advanced VPC, including IAM roles, while restricting access to *shared service* components that are operated by AMS Advanced (for example, management hosts, domain controllers, Trend Micro EPS, bastions, and unsupported AWS services). The role also restricts access to the following AWS services: Amazon GuardDuty, AWS Organizations, AWS Directory Service APIs, and AMS Advanced logs.

While the role allows you to create additional IAM roles, the same permissions boundaries included in Developer mode access are enforced on any IAM role created by the `AWSManagedServicesDevelopmentRole`.

Security and compliance in Developer mode

Security and compliance is a shared responsibility between AMS Advanced and you as our customer. AMS Advanced Developer mode shifts the shared responsibility to you for resources provisioned outside of the change management process or provisioned through change management but updated with Developer mode permissions. For more information about shared responsibility, see AWS Managed Services.

Security in Developer mode

AMS Advanced offers additional value with a prescriptive landing zone, a change management system, and access management. When using Developer mode the security value of AMS Advanced is persisted by using the same account configuration of standard AMS Advanced accounts that establishes the baseline AMS Advanced security hardened network. The network is protected by the permissions boundary enforced in the role (`AWSManagedServicesDevelopmentRole` for **MALZ**, `customer_developer_role` for **SALZ**), which restricts the user from breaking down the parameter protections established when the account is set up.

For example, users with the role can access Amazon Route 53 but AMS Advanced internal hosted zone is restricted. The same permissions boundaries are enforced on an IAM role created by the `AWSManagedServicesDevelopmentRole`, enforcing permissions boundaries on the `AWSManagedServicesDevelopmentRole` that restricts the user from breaking down the parameter protections established when the account is onboarded to AMS Advanced.

Compliance in Developer mode

Developer mode is compatible with both production and non-production workloads. It's your responsibility to ensure adherence to any compliance standards (for example, PHI, HIPAA, PCI), and to ensure that the use of Developer mode complies with your internal control frameworks and standards.

Change management in Developer mode

Change management is the process the AMS Advanced service uses to implement requests for change. A request for change (RFC) is a request created by either you or AMS Advanced through the AMS Advanced interface to make a change to your managed environment and includes a change type (CT) ID for a particular operation. For more information, see Change management (p. 282).

Change management is not enforced in AMS Advanced accounts where Developer mode permissions are granted. Users who have been granted Developer mode permission with the IAM role (`AWSManagedServicesDevelopmentRole` for **MALZ**, `customer_developer_role` for **SALZ**), can use native AWS API access to provision and make changes to resources in their AMS Advanced accounts. Users who do not have the appropriate role in these accounts must use the AMS Advanced change management process to make changes.

Important
Resources that you create using Developer mode can be managed by AMS Advanced only if they are created using AMS Advanced change management processes. Requests for changes submitted to AMS Advanced for resources created outside of the AMS Advanced change management process are rejected by AMS Advanced because they must be handled by you.

Self-service provisioning services API restrictions

All AMS Advanced self-provisioned services are supported with Developer mode. Access to self-provisioned services are subject to the limitations outlined in the respective user guide sections for each. If a self-provisioned service is not available with your Developer mode role, you can request an updated role through the Developer mode change type.

The following services do not provide full access to service APIs:

Self-Provisioned Services Restricted in Developer mode

Service	Notes
Amazon API Gateway	All Gateway APIs calls are allowed except `SetWebACL`.
Application Auto Scaling	Can only register or deregister scalable targets, and put or delete a scaling policy.
AWS CloudFormation	Can't access or modify CloudFormation stacks that have a name prefixed with `mc-`.
AWS CloudTrail	Can't access or modify CloudTrail resources that have a name prefixed with `ams-` and/or `mc-`.
Amazon Cognito (User Pools)	Can't associate software tokens. Can't create user pools, user import jobs, resource servers, or identity providers.
AWS Directory Service	Only the following AWS Directory Service actions are required by `Connect` and `WorkSpaces` services. All other Directory Service actions are denied by the Developer mode permission boundary policy: • `ds:AuthorizeApplication` • `ds:CreateAlias` • `ds:CreateIdentityPoolDirectory` • `ds:DeleteDirectory` • `ds:DescribeDirectories` • `ds:GetAuthorizedApplicationDetails` • `ds:ListAuthorizedApplications` • `ds:UnauthorizeApplication`

Service	Notes
	In single-account landing zone accounts, the boundary policy explicitly denies access to the AMS Advanced managed directory used by AMS Advanced for maintaining access to dev-mode enabled accounts.
Amazon Elastic Compute Cloud	Can't access Amazon EC2 APIs that contain the string: `DhcpOptions`, `Gateway`, `Subnet`, `VPC`, and `VPN`. Can't access or modify Amazon EC2 resources that have a tag prefixed with `AMS`, `mc`, `ManagementHostASG`, and/or `sentinel`.
Amazon EC2 (Reports)	Only view access is granted (cannot modify). Note: Amazon EC2 Reports is moving. The **Reports** menu item will be removed from the Amazon EC2 console navigation menu. To view your Amazon EC2 usage reports after it has been removed, use the AWS Billing and Cost Management console.
AWS Identity and Access Management (IAM)	Can't delete existing permission boundaries, or modify IAM user password policies. Can't create or modify IAM resources unless you are using the correct IAM role (`AWSManagedServicesDevelopmentRole` for **MALZ**, `customer_developer_role` for **SALZ**)). Can't modify IAM resources that are prefixed with: `ams`, `mc`, `customer_deny_policy`, and/or `sentinel`. When creating a new IAM resource (role, user, or group), the permission boundary (**MALZ**: `AWSManagedServicesDevelopmentRolePermissionsBound` **SALZ**: `ams-app-infra-permissions-boundary`) must be attached.
AWS Key Management Service (AWS KMS)	Can't access or modify AMS Advanced-managed KMS keys.
AWS Lambda	Can't access or modify AWS Lambda functions that are prefixed with `AMS`.
CloudWatch Logs	Can't access CloudWatch log streams that a name prefixed with: `mc`, `aws`, `lambda`, and/or `AMS`.
Amazon Relational Database Service (Amazon RDS)	Can't access or modify Amazon Relational Database Service (Amazon RDS) databases (DBs) that have a name prefixed with: `mc-`.
AWS Resource Groups	Can only access `Get`, `List`, and `Search` Resource Group API actions.
Amazon Route 53	Can't access or modify Route53 AMS Advanced-maintained resources.

Service	Notes
Amazon S3	Can't access Amazon S3 buckets that have a name prefixed with: `ams-*`, `ams`, `ms-a`, or `mc-a`.
AWS Security Token Service	The only security token service API allowed is `DecodeAuthorizationMessage`.
Amazon SNS	Can't access SNS topics that have a name prefixed with: `AMS-`, `Energon-Topic`, or `MMS-Topic`.
AWS Systems Manager (SSM)	Can't modify SSM parameters that are prefixed with `ams`, `mc`, or `svc`. Can't use the SSM API `SendCommand` against Amazon EC2 instances that have a tag prefixed with `ams` or `mc`.
AWS Tagging	You only have access to AWS Tagging API actions that are prefixed with `Get`.
AWS Lake Formation	The following AWS Lake Formation API actions are denied: • `lakeformation:DescribeResource` • `lakeformation:GetDataLakeSettings` • `lakeformation:DeregisterResource` • `lakeformation:RegisterResource` • `lakeformation:UpdateResource` • `lakeformation:PutDataLakeSettings`
Amazon Elastic Inference	You can only call the Elastic Inference API action `elastic-inference:Connect`. This permission is included in the `customer_sagemaker_admin_policy` that is attached to the `customer_sagemaker_admin_role`. This action gives you access to the Elastic Inference accelerator.
AWS Shield	No access to any of this services APIs or console.
Amazon Simple Workflow Service	No access to any of this services APIs or console.

Provisioning infrastructure in Developer mode

Users that don't have the Developer mode IAM role, `AWSManagedServicesDevelopmentRole`, in accounts where Developer mode is enabled, are required to follow the AMS Advanced change management process that leverages AMS Advanced AMIs. Users with correct role (**MALZ**: `AWSManagedServicesDevelopmentRole`, **SALZ**: `customer_developer_role`) can use the AMS Advanced change management system and AMS Advanced AMIs but are not required to.

> **Note**
> An AWS AMI, that has not been processed through AMS Advanced workload ingestion, or created in an AMS Advanced account, will not include AMS Advanced-required configurations.

Detective controls in Developer mode

This section has been redacted because it contains sensitive AMS security-related information. This information is available through the AMS console **Documentation**. To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.

Logging, monitoring, and event management in Developer mode

Logging, monitoring, and event management aren't available for resources provisioned outside of the AMS Advanced change management process, or for resources provisioned through change management and then altered by an account using Developer mode permissions.

Incident management in Developer mode

No change to incident response times. Incident resolution is a best effort for resources provisioned outside the change management process, or resources provisioned through change management and then altered by an account using Developer mode permissions.

> **Note**
> Incidents submitted in Developer mode enabled accounts are automatically degraded to a P3 and support is best effort. AMS Advanced reserves the right to downgrade incidents opened on non-manageable stacks to Sev 3.

Patch management in Developer mode

Patch management is not available for resources provisioned outside of the AMS Advanced change management process, or for resources provisioned through change management and then altered by an account using Developer mode permissions. Patching times:

- For a critical security update: Within 10 business days of release by the vendor for resources provisioned through change management and then altered by an account using Developer mode permissions.
- For an important update: Within 2 months of release by the vendor for resources provisioned through change management and then altered by an account using Developer mode permissions.

Continuity management in Developer mode

Continuity management is not available for resources provisioned outside of the AMS Advanced change management process, or for resources provisioned through change management and then altered by an account using Developer mode permissions.

Environment recovery initiation time can take up to 12 hours for resources provisioned outside of the AMS Advanced change management process, or for resources provisioned through change management and then altered by an account using Developer mode permissions.

Security and access management in Developer mode

Anti-malware protection is your responsibility for resources provisioned outside of the AMS Advanced change management process, or for resources provisioned through change management and then altered by an account using Developer mode permissions. Access to Amazon Elastic Compute Cloud (Amazon EC2) instances not provisioned through AMS Advanced change management might be controlled by key pairs instead of providing federated access.

Direct Change Mode

Topics

AWS Managed Services (AMS) Direct Change Mode (DCM) extends AMS Advanced change management by providing native AWS access to AMS Advanced Plus and Premium accounts to provision and update AWS resources. With DCM, you have the option to use native AWS API (console or CLI/SDK) or AMS Advanced change management requests for change (RFCs), and in either case the resources and changes to them are fully supported by AMS, including monitoring, patch, backup, incident response management. Resources provisioned through DCM are registered in the AMS service knowledge management system (SKMS), joined to the AMS managed Active Directory domain (when applicable), and run AMS management agents. Use existing tooling (for example, CloudFormation, AWS SDK, and CDK) to develop and deploy AMS-managed CloudFormation stacks.

Note
Direct Change mode does not remove AMS change management RFCs, you have full access to AMS RFCs with DCM.

Getting Started with Direct Change mode

Begin by submitting a request for change (RFC) in your eligible AMS Advanced account to provision the predefined IAM roles. Use an RFC with the Management | Other | Other change type as described:

1. Confirm that the account that you want to use with DCM meets the requirements: the account is AMS Advanced Plus or Premium.
2. Submit a request for change (RFC) using the Management | Other | Other | Create change type. After the CT is processed, the predefined IAM roles, `AWSManagedServicesCloudFormationAdminRole` and `AWSManagedServicesUpdateRole` are provisioned in the specified account.

   Use this template when you request the Direct Change mode role through an AMS service request:

   ```
   Direct Change Mode Access Request
   Trusted entities: The names of the trusted entity or entities to use for the roles.
   Date Range(optional): The date range to enable DCM for.
   ```

3. Assign the appropriate role to the users that require DCM access using your internal federation process.

Note
You can specify any number of SAMLIdentityProviders, AWS Services, and IAM Entities (Roles, Users etc) to assume the roles. You must provide at least one: `SAMLIdentityProviderARNs`, `IAMEntityARNs`, or `AWSServicePrincipals`. For more information, consult with your company's IAM department or with your AMS Cloud Architect.

Direct Change mode IAM roles and policies

When Direct Change mode is enabled in an account, these new IAM entities are deployed:

`AWSManagedServicesCloudFormationAdminRole`: This role grants access to the CloudFormation console, create and update CloudFormation stacks, view drift reports, and create and execute CloudFormation ChangeSets. Access to this role is managed through the your SAML provider.

Managed policies that are deployed and attached to the role `AWSManagedServicesCloudFormationAdminRole` are:

- AMS Advanced multi-account landing zone (MALZ) Application account
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
    - This policy represents the permissions granted to the `AWSManagedServicesCloudFormationAdminRole`. You and partners use this policy to grant access to an existing role in the account and allow that role to launch and update CloudFormation stacks in the account. This might require additional AMS service control policy (SCP) updates to allow other IAM entities to launch CloudFormation stacks.
- AMS Advanced single-account landing zone (SALZ) account
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
  - cdk-legacy-mode-s3-access [in-line policy]
  - AWS ReadOnlyAccess policy

`AWSManagedServicesUpdateRole`: This role grants restricted access to downstream AWS service APIs. The role is deployed with managed policies that provide mutating and non-mutating API operations, but in general restricts mutating operations (such as Create/Delete/PUT), against certain services such as IAM, KMS,GuardDuty, VPC, AMS infrastructure resources and configuration, and so forth. Access to this role is managed through the your SAML provider.

Managed policies that are deployed and attached to the role `AWSManagedServicesUpdateRole` are:

- AMS Advanced multi-account landing zone Application account
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyPolicy
  - AWSManagedServicesUpdateDenyProvisioningsPolicy
  - AWSManagedServicesUpdateEC2AndRDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy
- AMS Advanced single-account landing zone account
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyProvisioningsPolicy
  - AWSManagedServicesUpdateEC2AndRDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy1
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy2

Besides these, the managed policy `AWSManagedServicesUpdateRole` role also has the AWS managed policy `ViewOnlyAccess` attached to it.

Security and compliance

Security and compliance is a shared responsibility between AMS Advanced and you, as our customer. AMS Advanced Direct Change mode does not change this shared responsibility.

Security in Direct Change mode

AMS Advanced offers additional value with a prescriptive landing zone, a change management system, and access management. When using Direct Change mode, this responsibility model does not change. However, you should be aware of additional risks.

The Direct Change Mode "Update" role (see Direct Change mode IAM roles and policies (p. 167)) provides elevated permissions allowing the entity with access to it, to make changes to infrastructure resources of AMS-supported services within your account. With elevated permissions, varied risks exist depending on the resource, service, and actions, especially in situations where an incorrect change is made due to oversight, mistake, or lack of adherence to your internal process and control framework.

As per AMS Technical Standards, the following risks have been identified and recommendations are made as follows. Detailed information about AMS Technical Standards is available through AWS Artifact. To access AWS Artifact, contact your CSDM for instructions or go to Getting Started with AWS Artifact.

AMS-STD-001: Tagging

Standards	Does it break	Risks	Recommendations
All the AMS owned resources must have following key-value pair	Yes. Breaks for CloudFormation,CloudTrail, EFS, Elasticsearch, CloudWatch Logs, SQS, SSM, Tagging api - as these services do not support the `aws:TagsKey` condition to restrict tagging for the AMS namespace. Standard given in table **AMS-STD-003**, following, states that you can change AppId, Environment and AppName, but not for AMS-owned resources. Not achievable through IAM permissions.	Incorrect tagging of AMS resources may adversly impact the reporting, alerting and patching operations of your resources, on the AMS side.	Access must be restrticted to make any changes on the AMS default tagging requirements for anyone other than AMS teams.
All the AMS-owned tags other than those listed above must have prefixes like `AMS*` or `MC*` in upper/lower/mix case.			
Any tag on AMS-owned stacks must not be deleted based on your change requests.	Yes. CloudFormation does not support the `aws:TagsKey` condition to restrict tags for the AMS namespace.		
You are not permitted to use AMS tag naming convention in your infrastructure as mentioned in table table **AMS-STD-002**, next.	Yes. Breaks for CloudFormation,CloudTrail, EFS, Elasticsearch, CloudWatch Logs, SQS, SSM, Tagging APIO; these services do not support the `aws:TagsKey` condition to restrict		

Standards	Does it break	Risks	Recommendations
	tagging for the AMS namespace.		

AMS-STD-002: Identity and Access Management (IAM)

Standards	Does it break	Risks	Recommendations
4.7 Actions, which bypass the change management process (RFC), must not be permitted such as starting or stopping of an instance, creation of S3 buckets or RDS instances, and so forth. Developer mode accounts and Self-Service Provisioned mode services (SSPS) are exempted as long as actions are performed within the boundaries of the assigned role.	Yes. The purpose of self service actions allow you to perform actions bypassing the AMS RFC system.	The secure access model is a core technical facet of AMS and an IAM user for console or programmatic access circumvents this access control. The IAM users access is not monitored by AMS change management. Access is logged in Cloudtrail only.	The IAM user should be time-bounded and granted permissions based on least-privilege and need-to-know.

AMS-STD-003: Network Security

Standards	Does it break	Risks	Recommendations
S2. Elastic IP on EC2 instances must be used only with a formal risk acceptance agreement, or with a valid use case by internal teams.	Yes. Self service actions allow you to associate and disassociate elastic IP addresses (EIP).	Adding an elastic IP to an instance exposes it to the Internet. This increases the risk of information disclosure and unauthorized activity.	Block any unnecessary traffic to that instance through security groups, and verify that your security groups are attached with the instance to ensure that it allows the traffic only as needed for business reasons.
S14. VPC Peering and endpoint connections between accounts that belong to the same customer can be permitted.	Yes. Not possible through IAM policy.	Traffic leaving your AMS account is not monitored once egressing the account boundary.	We recommend peering only with AMS accounts that you own. If your use case requires this, use security groups and route tables to limit what traffic ranges, resources, and types can egress through the relevant connection.
AMS base AMIs can be shared between		AMIs may contain sensitive data and it	Share AMIs with only the account owned

Standards	Does it break	Risks	Recommendations
AMS-managed and unmanaged accounts as long as we can verify that they are owned by the same AWS organization.		may be exposed to unintended accounts.	by your organization or validate the use-case and account information before sharing outside the organization.

AMS-STD-007: Logging

Standards	Does it break	Risks	Recommendations
19. Any log can be forwarded from one AMS account to another AMS account of the same customer.	Yes. Potential insecurity for customer logs as verification of the customer accounts being in the same organization can not be achieved through IAM policy.	Logs may contain sensitive data and it may be exposed to unintended accounts.	Share logs with only accounts managed by your AWS Org, or validate the use-case and account information before sharing outside of your organization. We can verify this via multiple ways, check with your cloud service delivery manager (CSDM).
20. Any log can be forwarded from one AMS account to another AMS account of the same customer.			

Work with your internal IAM (Identity and Access Management) team to control the permissions to the Direct Change mode roles accordingly.

Compliance in Direct Change mode

Direct Change mode is compatible with both production and non-production workloads. It's your responsibility to ensure adherence to any compliance standards (for example, PHI, HIPAA, PCI), and to ensure that the use of Direct Change mode complies with your internal control frameworks and standards.

Change management in Direct Change mode

Change management is the process that AMS Advanced uses to implement requests for change. A request for change (RFC) is a request created by either you, or AMS Advanced through the AMS Advanced interface to make a change to your managed environment and includes an AMS Advanced change type (CT) ID for a particular operation. For more information, see Change management.

> **Note**
> Direct Change mode does not remove AMS change management RFCs, you still have full access to AMS RFCs with DCM.

AMS Direct Change mode (DCM) extends AMS Advanced change management by providing native AWS access to AMS Advanced Plus and Premium accounts to provision and update AWS resources. Users who have been granted Direct Change mode permission through the IAM roles, can use native AWS API access to provision and make changes to resources in their AMS Advanced accounts. The users can still use AMS Advanced change management RFCs using the same IAM roles. In both cases the resources and changes to them are fully supported by AMS, including monitoring, patch, backup, incident response

management. Users who do not have the appropriate role in these accounts must use the AMS Advanced change management RFC process to make changes.

Change management use cases

For security reasons, some changes in AMS Advanced can only be done through the change management (RFC):

Service	Action
AWS Certificate Manager	Create
AWS Identity and Access Management (IAM)	Any
AWS Key Management Service (KMS)	Update
AWS VPN	Any
AMS Resource Scheduler	
AWS Backup	Create backup plan
AMS Workload Ingestion (WIGs)	Any
AMS Egress Filtering (Managed Palo Alto)	
AMS Advanced MALZ account changes	
Amazon GuardDuty	
AWS Systems Manager	Create
AMS Advanced Stack Access	Any
Amazon Machine Images (AMI)	Delete, share
Amazon Elastic Block Store (EBS) volume	Delete
Amazon Elastic Block Store (EBS) default encryption	Enable default encryption
Amazon EC2	Change hostname
Amazon EC2 Security Group	Any
AMS Advanced SSPS	
AWS Managed Microsoft AD	
AMS Advanced developer mode	

Creating stacks using Direct Change mode

There are two requirements when launching stacks in CloudFormation using the `AWSManagedServicesCloudFormationAdminRole`, in order for the stack to be managed by AMS:

- The template must contain an AMS Transform.
- The stack name must start with the prefix `stack-` followed by a 17 character alphanumeric string.

Details and examples are provided.

AMS Transform

The CloudFormation template must contain the following snippet:

```
"Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  }
```

This adds a CloudFormation macro that validates and registers the stack with AMS at launch time. This snippet must also be included when updating the template of an existing stack. For example:

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
    "Transform": {
      "Name": "AmsStackTransform",
      "Parameters": {
        "StackId": {"Ref" : "AWS::StackId"}
     }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

Stack name

The stack name must start with the prefix `stack-` followed by a 17 character alphanumeric string. This is to maintain compatibility with other AMS systems that operate on AMS stack IDs.

The following are examples of ways to generate compatible stack IDs:

Bash:

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python:

```
import string
import random
```

```
'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

Powershell:

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17  | % {[char]$_}) )
```

Self-service provisioning

There are some AWS services that you can use in your AMS account without AMS management. These self-service provisioning services, or SSPS for short, how to add them into your AMS account and FAQs for each, are described here.

Self-service provisioning services are offered as is, and you're responsible for managing them. AMS provides no alerts, monitoring, logging, or patching for the resources associated with those services. AMS provides IAM roles that enable you to use the service in your AMS account safely. AMS SLAs do not apply. To add a self-service provisioning service, use the **Management | AWS service | Self-provisioned service | Add** change type (CT).

Self-service provisioning is one of the AMS modes for multi-account landing zone (MALZ) that you can employ. For more information, see AMS Modes

> **Note**
> To request that AMS provide an additional self-service provisioning service, file a service request. For details about doing that, see Service request management (p. 275).

Currently, these are the self-service provisioning service (SSPS) options, you can choose from those listed.

Amazon API Gateway

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. Using the AWS Management Console you can create REST and WebSocket APIs that act as a front door for applications to access data, business logic, or functionality from your back-end services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, any web application, or real-time communication applications.

API Gateway handles all the tasks involved in accepting and processing up-to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. API Gateway has no minimum fees or startup costs. You pay only for the API calls you receive and the amount of data transferred out and, with the API Gateway tiered pricing model, you can reduce your cost as your API usage scales. To learn more, see Amazon API Gateway.

FAQs: API Gateway in AMS

Q: How do I request access to Amazon API Gateway in my AMS account?

Request access to API Gateway by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_apigateway_author_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon API Gateway in my AMS account?

- API Gateway configuration is limited to resources without `AMS-` or `MC-` prefixes to prevent any modifications to AMS infrastructure.
- `CREATE` privileges for VPCLink are disabled in order to prevent unregulated creation of Elastic Load Balancers. If VPCLinks are required, see Application Load Balancer: creating.

Q: What are the prerequisites or dependencies to using Amazon API Gateway in my AMS account?

It depends on the type of API Gateway you want to deploy. It can be a standalone service, but it can also request access to existing services (for instance, network loadbalancer).

AWS Alexa for Business

Alexa for Business is a service that enables your organization and employees to use Alexa to get more work done. With Alexa for Business, you can use Alexa as your intelligent assistant to be more productive in meeting rooms, at your desk, and even with the Alexa devices you already use at home or on the go. IT and facilities managers can use Alexa for Business to measure and increase the utilization of the existing meeting rooms in their workplace.

To learn more, see Alexa for Business.

Alexa for Business in AMS FAQs

Q: How do I request access to Alexa for Business in my AMS account?

Request access to Alexa for Business by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_alexa_console_role`. A `customer_alexa_device_setup_user` is also created for the Device Setup Tool provided by Alexa for Business; this Device Setup Tool can then be used to set up your devices. Once provisioned in your account, you must onboard the roles in your federation solution.

The Alexa for Business gateway enables you to connect Alexa for Business to your Cisco Webex and Poly Group Series endpoints to control meetings with your voice. The gateway software runs on your on-premises hardware and securely proxies conferencing directives from Alexa for Business to your Cisco endpoint. The gateway needs two pairs of AWS credentials to communicate with Alexa for Business. We provide two limited-access IAM users: `customer_alexa_gateway_installer_user` and `customer_alexa_gateway_execution_user` for your Alexa for Business gateways, one for installing the gateway and one for operating the gateway; these can be requested by submitting an RFC with the Management | Other | Other change type.

> **Note**
> To generate usage reports and send them to Amazon S3, specify the Amazon S3 bucket name in the self-provisioned service RFC.

Q: What are the restrictions to using Alexa for Business in my AMS account?

There are no restrictions. Full functionality of Alexa for Business is available with the Alexa for Business self-provisioned service role.

Q: What are the prerequisites or dependencies to using Alexa for Business in my AMS account?

If you intend to use WPA2 Enterprise Wi-Fi to set up your shared devices, please specify this network security type in the Device Setup Tool, for which a Private Certificate Authority (PCA) in AWS Certificate Manager (ACM) is required.

What Alexa for Business functionality requires separate RFCs?

To register an Alexa Voice Service (AVS) device with Alexa for Business, provide access to the Alexa built-in device maker. To do this, an IAM role needs to be created in the Alexa for Business console that can be deployed using the Management | Other | Other change type. This allows the AVS device maker to register and manage devices with Alexa for Business on your behalf.

AppStream 2.0

Amazon AppStream 2.0 (AppStream 2.0) lets you move your desktop applications to AWS, without rewriting them. You can install your applications on AppStream 2.0, set launch configurations, and make your applications available to users. AppStream 2.0 offers a wide selection of virtual machine options so that you can select the instance type that best matches your application requirements, and set the auto-scale parameters so that you can easily meet the needs of your end users. AppStream 2.0 enables you to launch applications in your own network, which means your applications can interact with your existing AWS resources.

Amazon AppStream 2.0 enables you to quickly and easily install, test, and update your applications using the image builder. Any application that runs on Microsoft Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 is supported, and you don't need to make any modifications. When your testing is complete, you can set application launch configurations, default user settings, and publish your image for users to access.

To learn more, see AppStream 2.0.

AppStream 2.0 in AMS FAQs

Q: How do I request access to AppStream 2.0 in my AMS account?

Request access to AppStream 2.0 by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_appstream_console_role`.

A `customer_appstream_stream_role` is also deployed to stream applications that require users to be authenticated using their Active Directory login credentials.

Once provisioned in your account, you must onboard the roles in your federation solution.

Q: What are the restrictions to using AppStream 2.0 in my AMS account?

- The following functionality must be configured by the AMS Support team, and requires specific RFCs. Instruction on requesting additional functionality can be found in section 4.
  - Creating and Streaming from Interface VPC Endpoints.
  - Support for Amazon S3 endpoints for home folders and application setting persistence on a private network.
  - Creating and choosing the IAM role that will be available on all fleet streaming instances.
  - Joining AppStream 2.0 fleets and image builders Microsoft Active Directory domains.
  - Creating AppStream 2.0 Custom Usage Reports.
  - Custom branding is currently not supported.

Q: What are the prerequisites or dependencies to using AppStream 2.0 in my AMS account?

There are no prerequisites to using AppStream 2.0 in your AMS account.

Q: What AppStream 2.0 functionality requires separate RFCs?

- In order to choose an interface VPC endpoint for AppStream 2.0, submit a Management | Other | Other | Update change type RFC to create a VPC endpoint in your account. For steps to create custom endpoints for AppStream 2.0, see Creating and Streaming from Interface VPC Endpoints in the AppStream 2.0 user guide.
- Support for Amazon S3 endpoints for home folders and application setting persistence on a private network can be configured by requesting Amazon S3 VPC endpoints with a Management | Other

| Other | Create change type RFC. The RFC must include the target Amazon S3 bucket hosting the home folder contents, or application settings Amazon S3 buckets, respectively. This RFC will provide AppStream 2.0 the permissions it needs to access Amazon S3 VPC endpoints. For steps to create custom endpoints for streams, see Using Amazon S3 VPC Endpoints for Home Folders and Application Settings Persistence in the AppStream 2.0 user guide.

- In order to create and choose an IAM role that will be available on all fleet streaming instances, submit a Management | Other | Other | Create change type RFC requesting the IAM role with the required policy. The IAM role name should always start with prefix : "customer_appstream".
- Amazon AppStream 2.0 fleets and image builders can be joined to domains in Microsoft Active Directory by submitting a Management | Other | Other | Update change type RFC for the Service Account creation in Active Directory (AD). Minimal permissions required to join Microsoft Active Directory are defined in the AppStream 2.0 documentation at Granting Permissions to Create and Manage Active Directory Computer Objects.
- In order to create custom AppStream 2.0 Usage Reports, submit a Management | Other | Other | Create change type RFC requesting following:
  - "AppStreamUsageReports" CFN stack creation
  - "customer_appstream_usagereports_role" be provisioned in the account
  - Also, provide the following details:
    - Provide CRON expression to schedule Crawler run. By default it is 23:00 UTC everyday.
    - Amazon S3 bucket ARN to be used for athena query results. This bucket should have prefix : "aws-athena-query-results"
    - Amazon S3 bucket ARN for AppStream Usage Reports Logs.

  After the role is provisioned, onboard the role into your federation solution and login, then access Glue and Athena for generating custom reports using the usage report role. For details about using AppStream 2.0 Usage Reports see Create Custom Reports and Analyze AppStream 2.0 Usage Data, in the AppStream 2.0 documentation.

Amazon Athena

Amazon Athena is an interactive query service that helps you to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. You point to your data in Amazon S3, define the schema, and start querying using standard SQL. Most results are delivered within seconds. With Athena, there's no need for complex exact-trandform-load (ETL) jobs to prepare your data for analysis. This makes it straight-forward for anyone with SQL skills to quickly analyze large-scale datasets. To learn more, see Amazon Athena.

FAQs: Athena in AMS

Q: How do I request access to Amazon Athena in my AMS account?

Request access to Athena by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_athena_console_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon Athena in my AMS account?

There are no restrictions. Full functionality of Amazon Athena is available in your AMS account.

Q: What are the prerequisites or dependencies to using Amazon Athena in my AMS account?

Athena has a major dependency on the AWS Glue service, as it uses the data catalog/metastore created with AWS Glue. Therefore, AWS Glue permissions are included in the successful Athena RFC.

Amazon CloudSearch

Amazon CloudSearch is a managed service in the AWS Cloud that you use to cost-effective to set up, manage, and scale a search solution for your website or application. Amazon CloudSearch supports 34 languages and popular search features such as highlighting, autocomplete, and geospatial search. To learn more, see Amazon CloudSearch.

Amazon CloudSearch in AMS FAQs

Q: How do I request access to Amazon CloudSearch in my AMS account?

Request access to Amazon CloudSearch by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM roles to your account: `customer_csearch_admin_role` and `customer_csearch_dev_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon CloudSearch in my AMS account?

Full functionality of Amazon CloudSearch is available in your AMS account. All AMS-supported database solutions are currently supported on Amazon CloudSearch. Note that, currently, DynamoDB is the only managed AWS database solution that can’t be indexed.

Q: What are the prerequisites or dependencies to using Amazon CloudSearch in my AMS account?

Amazon CloudSearch depends on Amazon S3 working with Identity Providers to automatically analyze input data and determine the table fields. Access to Amazon S3 is not provided with this RFC, and must be requested separately in a service request.

Amazon CloudWatch Synthetics

You can use Amazon CloudWatch Synthetics to create 'canaries' to monitor your endpoints and APIs.

Canaries are configurable scripts, written in Node.js or Python, that run on a schedule. They create Lambda functions in your account that use Node.js or Python as a framework. Canaries work over both HTTP and HTTPS protocols. Canaries check the availability and latency of your endpoints and can store load time data and UI screenshots. They monitor your REST APIs, URLs, and website content, and they can check for unauthorized changes from phishing, code injection and cross-site scripting.

Canaries follow the same routes and perform the same actions as a customer, making it possible for you to continually verify your customer experience even when you don't have any customer traffic on your applications. By using canaries, you can discover issues before your customers do. To learn more, see Amazon CloudWatch: Using synthetic monitoring.

Amazon CloudWatch Synthetics in AMS FAQs

Q: How do I request access to Amazon CloudWatch Synthetics in my AMS account?

Request access to Amazon CloudWatch Synthetics by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: 'customer_cloudwatch_synthetics_role' and 'customer_lambda_canary_execution_role'. Once provisioned in your account, you must onboard the 'customer_cloudwatch_synthetics_role' role in your federation solution.

Q: What are the restrictions to using Amazon CloudWatch Synthetics in my AMS account?

There are no restrictions for the use of Amazon CloudWatch Synthetics in your AMS account. Creating roles for canaries outside of the AMS-provided service role 'customer_lambda_canary_execution_role' is prohibited.

Q: What are the prerequisites or dependencies to using Amazon CloudWatch Synthetics in my AMS account?

Canaries create and use a default Amazon CloudWatch Synthetics S3 bucket: "cw-syn-results-*${accountnumber}*-*${default-region}*"

Amazon Cognito (User Pools)

Amazon Cognito user pools provide a secure user directory that scales to hundreds of millions of users. As a fully managed service, Amazon Cognito user pools can be set up without any worries about standing up server infrastructure. This service enables you to manage a pool of final users that you can use to integrate with your internal applications. This service provides you an alternative to a customized database or a directory of final users for web or mobile applications. At the same time, Amazon Cognito user pools provides the full set of functionalities of a directory service like passwords policies, multi factor authentication, password recovery and self-sign up into services. It also allows the application to federate the access in other popular public services like OpenID, Facebook, Amazon or Google.

Amazon Cognito is divided into two main products. Amazon Cognito user pools and Amazon Cognito Identity Provider. This section focuses on Amazon Cognito user pools, which provide access to other AWS services like Amazon S3 or DynamoDB. The service allows you to use Amazon Cognito user pools, or a third party identity provider, to provide access to AWS services. It also provides access to AWS services using anonymous guest access. Because of the powerful nature of Amazon Cognito user pools, it would be managed manually on a case-by-case basis as an operation manual service, in order to avoid potential security breaks into the account. To learn more, see Amazon Cognito User Pools.

Amazon Cognito user pools in AMS FAQs

Common questions and answers:

Q: How do I request access to Amazon Cognito user pools in my AMS account?

Implementation of Amazon Cognito user pools in AMS is a 2 step process:

1. Submit a Management | Other | Other | Create (ct-1e1xtak34nx76) change type and request the creation of the Amazon Cognito user pools in your AMS Account. Include the following information:
   - AWS Region.
   - Name for the Cognito User Pool.
   - If the you want to use the Amazon Simple Email Service (Amazon SES) to send messages and notifications instead of the default internal Cognito mail service, then the customer should provide an already validated email address for the Amazon SES Service in the account. This address will be used for the "From" and "REPLY-TO" fields of the message. They must also indicate the Region where Amazon SES was activated (us-east-1, eu-west-1 or us-west-2).
   - If the you want to use SMS messages for one-time passwords and verification, then the customer should indicate so.
2. Request user access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM roles to your account: `customer_cognito_admin_role` and `customer_cognito_importjob_role`. After it's provisioned in your account, you must onboard the role in your federation solution. These roles allow you to manage the Cognito User Pool, manage your users and groups in the pool, create importjobs for users, modify the notification and subscription messages, associate applications to the user pool, add federation services to the pool in a self-managed fashion, and delete already created pools.

Q: What are the restrictions to using Amazon Cognito user pools in my AMS account?

You won't be able to create the Amazon Cognito user pools. That action requires the creation of IAM roles to leverage services used by Amazon Cognito, like Amazon SES and Amazon Simple Notification Service (Amazon SNS).

Q: What are the prerequisites or dependencies to using Amazon Cognito user pools in my AMS account?

If you want to use Amazon SES to send messages and notifications by email to your user pools, they should already activate the Amazon SES service in the account, and already validate the email address that should be used in the "FROM" and "REPLY-TO" fields of the sent emails. For more information about validating email address using Amazon SES, see Verifying Email Addresses in Amazon SES.

Amazon Comprehend

Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find insights and relationships in text, no machine learning experience is required. Amazon Comprehend uses machine learning to help you uncover the insights and relationships in your unstructured data. The service identifies the language of the text; extracts key phrases, places, people, brands, or events; understands how positive or negative the text is; analyzes text using tokenization and parts of speech; and automatically organizes a collection of text files by topic. You can also use AutoML capabilities in Amazon Comprehend to build a custom set of entities or text classification models that are tailored uniquely to your organization's needs. To learn more, see Amazon Comprehend.

Amazon Comprehend in AMS FAQs

Q: How do I request access to Amazon Comprehend in my AMS account?

Amazon Comprehend console and data access roles can be requested through the submission of two AMS Service RFCs:

Request access to Amazon Comprehend by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_comprehend_console_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon Comprehend in my AMS account?

Create New IAM Role functionality through the Amazon Comprehend console is restricted. Otherwise, full functionality of Amazon Comprehend is available in your AMS account.

Q: What are the prerequisites or dependencies to using Amazon Comprehend in my AMS account?

Amazon S3 and AWS Key Management Service (AWS KMS) are required in order to use Amazon Comprehend, if Amazon S3 buckets are encrypted with AWS KMS keys.

Amazon Connect

Amazon Connect is an omnichannel cloud contact center that helps companies provide superior customer service at a lower cost. Amazon Connect provides a seamless experience across voice and chat for customers and agents.This includes one set of tools for skills-based routing, powerful real-time and historical analytics, and easy-to-use intuitive management tools – all with pay-as-you-go pricing.

You can create one or more instances of the virtual contact center instances in either AMS multi-account landing zone or single-account landing zone accounts. You can use existing SAML 2.0 identity providers for agent access or use Amazon Connect native support for user life cycle management.

Additionally, you can claim toll free/direct dial phone numbers for each Amazon Connect instance from the Amazon Connect console. You can create rich contact flows to achieve the desired customer experience and routing using an easy-to-use graphical user interface. The contact flows can leverage AWS Lambda functions to integrate with on-premises data stores and API's. You can also enable data streaming using Kinesis Streams and Firehose.

The call recordings, chat transcripts, and reports, are stored in an Amazon S3 bucket encrypted using an AWS KMS key. The contact flow logs can be saved to CloudWatch log groups.

To learn more, see Amazon Connect.

Amazon Connect in AMS FAQs

Q: How do I request access to Amazon Connect in my AMS account?

Request access to Amazon Connect by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM roles to your account: `customer_connect_console_role` and `customer_connect_user_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon Connect in my AMS account?

There are no restrictions. Full functionality of Amazon Connect is available in your AMS account.

Q: What are the prerequisites or dependencies to using Amazon Connect in my AMS account?

- You must create an AWS KMS Key and an Amazon S3 bucket using standard AMS RFCs; the Amazon S3 bucket is required for storing call recordings and chat transcripts.
- If you want to integrate with Active Directory (AD), an AD Connector is required for integration between AMS-hosted Amazon Connect instances and your on-premises directory services. AD Connector can be configured in your account by requesting a 'Management | Other | Other' RFC.
- You can enable the following optional self-provisioned services based on your contact flow requirements.
  - **AWS Lambda**: You can use Lambda functions to extend the contact flows to leverage existing on-premises data stores or APIs. You can use the Lambda self-provisioned service to create the Lambda functions.
  - **Amazon Kinesis Data Streams**: You can create data streams to enable Data streaming to external applications. You can stream contact trace records or Agent Events.
  - **Amazon Kinesis Data Firehose**: You can create Data Firehose to stream high volume contact trace records to external applications.
  - **Amazon Lex**: You can leverage Amazon Lex Chatbots to create smart contact flows leveraging Amazon Alexa services for rich customer experience and automation.

Amazon DocumentDB (with MongoDB compatibility)

Amazon DocumentDB (with MongoDB compatibility) is a fast, scalable, highly available, and fully managed document database service that supports MongoDB workloads. Amazon DocumentDB gives you the performance, scalability, and availability you need when operating mission-critical MongoDB workloads at scale. Amazon DocumentDB implements the Apache 2.0 open source MongoDB 3.6 API

by emulating the responses that a MongoDB client expects from a MongoDB server, allowing you to use your existing MongoDB drivers and tools with Amazon DocumentDB. In Amazon DocumentDB, the storage and compute are decoupled, allowing each to scale independently, and you can increase the read capacity to millions of requests per second by adding up to 15 low latency read replicas, regardless of the size of your data. Amazon DocumentDB is designed for 99.99% availability and replicates six copies of your data across three AWS Availability Zones (AZs). You can use AWS Database Migration Service (DMS) for free (for six months) to migrate your on-premises or Amazon Elastic Compute Cloud (Amazon EC2) MongoDB databases to Amazon DocumentDB with virtually no downtime. To learn more, see Amazon DocumentDB (with MongoDB compatibility).

Amazon DocumentDB in AMS FAQs

Q: How do I request access to Amazon DocumentDB in my AMS account?

Amazon DocumentDB console and data access roles can be requested through the submission of two AMS RFCs, console access and data access:

Request access to Amazon DocumentDB by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_documentdb_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon DocumentDB in my AMS account?

Amazon DocumentDB requires Amazon RDS-specific permissions. Because AMS fully manages Amazon RDS, the IAM role for Amazon DocumentDB includes some restrictions to actions on Amazon RDS. The following restrictions apply:

- Access to the `DeleteDBInstance` and `DeleteDBCluster` APIs have been restricted. To use those deletion APIs, submit an RFC with the Management | Other | Other | Create (ct-1e1xtak34nx76) change type.
- You can't add or remove tags from Amazon RDS instances.
- You can't make your Amazon DocumentDB instance public.

Q: What are the prerequisites or dependencies to using Amazon DocumentDB in my AMS account?

Amazon S3 and AWS KMS are required in order to use Amazon DocumentDB, if Amazon S3 buckets are encrypted with AWS KMS keys.

Amazon DynamoDB

Amazon DynamoDB (DynamoDB) is a key value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multiregion, multimaster, durable database with built-in security, backup and restore, and in-memory caching for internet scale applications. DynamoDB can handle more than 10 trillion requests per day and can support peaks of more than 20 million requests per second. To learn more, see Amazon DynamoDB.

Amazon DynamoDB Accelerator (DAX) is a write-through caching service that is designed to simplify the process of adding a cache to DynamoDB tables. DAX is intended for applications that require high-performance reads.

DynamoDB in AMS FAQs

Q: How do I request access to DynamoDB and DAX in my AMS account?

Request access to DynamoDB and DAX by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM roles and policies to your account:

- DynamoDB role name: `customer_dynamodb_role`

  DAX service role name: `customer_dax_service_role`
- DynamoDB policy name: `customer_dynamodb_policy`

  DAX service policy: `customer_dax_service_policy`

Once provisioned in your account, you must onboard the `customer_dynamodb_role` in your federation solution.

Q: What are the restrictions to using DynamoDB in my AMS account?

All DynamoDB functionality are supported including DynamoDB Accelerator (DAX).

When creating alarms for any given table, the alarm name must be prefixed with "customer*"; for example, `customer-employee-table-high-put-latency`.

When creating an Amazon SNS topic for DynamoDB, it must be named: `dynamodb`.

To delete the Amazon SNS topic created by DynamoDB, submit a Management | Other | Other | Update change type RFC.

Q: What are the prerequisites or dependencies to using DynamoDB in my AMS account?

There are no prerequisites or dependencies to use DynamoDB in your AMS account.

Amazon Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images. Amazon ECR is integrated with Amazon Elastic Container Service (Amazon ECS), simplifying your development to production workflow. Amazon ECR eliminates the need to operate your own container repositories or worry about scaling the underlying infrastructure. Amazon ECS hosts your images in a highly available and scalable architecture, allowing you to reliably deploy containers for your applications. Integration with AWS Identity and Access Management (IAM) provides resource-level control of each repository. With Amazon ECR, there are no upfront fees or commitments. You pay only for the amount of data you store in your repositories and data transferred to the Internet.

To learn more, see Amazon Elastic Container Registry.

Amazon Elastic Container Registry in AMS FAQs

Q: How do I request access to Amazon ECR in my AMS account?

Request access to Amazon ECR by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_ecr_console_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon ECR in my AMS account?

There are restrictions around AMS namespaces for the use of Amazon ECR in your AMS account. Container images may not be prefixed with "AMS-" or "Sentinel-".

Q: What are the prerequisites or dependencies to using Amazon ECR in my AMS account?

There are no prerequisites or dependencies to use Amazon ECR in your AMS account.

Amazon EC2 Image Builder

EC2 Image Builder is a fully managed AWS service that makes it easier to automate the creation, management, and deployment of customized, secure, and up-to-date "golden" server images that are pre-installed and pre-configured with software and settings to meet specific IT standards.

You can use the AWS Management Console, AWS CLI, or APIs to create custom images in your AWS account. When you use the AWS Management Console, the Amazon EC2 Image Builder wizard guides you through steps to:

- Provide starting artifacts
- Add and remove software
- Customize settings and scripts
- Run selected tests
- Distribute images to AWS Regions

The images you build are created in your account and can be configured for operating system patches on an ongoing basis. To learn more, see EC2 Image Builder.

EC2 Image Builder in AMS FAQs

Common questions and answers:

Q: How do I request access to EC2 Image Builder in my AMS account?

Request access to EC2 Image Builder by submitting an RFC with the Management | AWS Service | Compatible Service change type. Through this RFC, the following IAM role will be provisioned in your account: `customer_ec2_imagebuilder_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions for EC2 Image Builder?

AMS does not support the use of Service Defaults for infrastructure configuration. You can create a new infrastructure configuration or use an existing one.

AMS does not currently support the creation of container recipes.

Q: What are the prerequisites or dependencies to enable EC2 Image Builder?

- EC2 Image Builder service-linked role: You don't need to manually create a service-linked role. When you create your first Image Builder resource in the AWS Management Console, the AWS CLI, or the AWS API, Image Builder creates the service-linked role for you.
- Instances used to build images and run tests using Image Builder must have access to the Systems Manager service. All build activity is orchestrated by SSM Automation. The SSM Agent will be installed on the source image if it is not already present, and it will be removed before the image is created.
- AWS IAM: The IAM role that you associate with your instance profile must have permissions to run the build and test components included in your image. The following IAM role policies must be attached to the IAM role that is associated with the instance profiles: `EC2InstanceProfileForImageBuilder` and `AmazonSSMManagedInstanceCore`. The IAM role name should contain the `*imagebuilder*` keyword.

- If you configure logging, the instance profile specified in your infrastructure configuration must have `s3:PutObject` permissions for the target bucket (`arn:aws:s3:::{bucket-name}/*`). For example:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::{bucket-name}/*"
        }
    ]
}
```

- Create an SNS topic with name 'imagebuilder' to receive any alerts and notification from EC2 Image Builder.

Amazon ECS on AWS Fargate

AWS Fargate is a technology that you can use with Amazon ECS to run containers (see Containers on AWS) without having to manage servers or clusters of Amazon EC2 instances. With AWS Fargate, you no longer have to provision, configure, or scale, clusters of virtual machines to run containers. This removes the need to choose server types, decide when to scale your clusters, or optimize cluster packing.

To learn more, see Amazon ECS on AWS Fargate.

Amazon ECS on Fargate in AMS FAQs

Q: How do I request access to Amazon ECS on Fargate in my AMS account?

Request access to Amazon ECS on Fargate by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM roles to your account: `customer_ecs_fargate_console_role` (if no existing IAM role is provided to associate the ECS policy to), `customer_ecs_fargate_events_service_role`, `customer_ecs_task_execution_service_role`, `customer_ecs_codedeploy_service_role`, and `AWSServiceRoleForApplicationAutoScaling_ECSService`. Once provisioned in your account, you must onboard the roles in your federation solution.

Q: What are the restrictions to using Amazon ECS on Fargate in my AMS account?

- Amazon ECS task monitoring and logging are considered your responsibility since container level activities occur above the hypervisor, and logging capabilities are limited by Amazon ECS on Fargate. As a user of Amazon ECS on Fargate, we recommend that you take the necessary steps to enable logging on your Amazon ECS tasks. For more information, see Enabling the awslogs Log Driver for Your Containers.
- Moreover, security and malware protection at the container level are also considered to be your responsibility. Amazon ECS on Fargate will not include Trend Micro or preconfigured network security components.
- This service is available for both multi-account landing zone and single-account landing zone AMS accounts.
- Amazon ECS Service Discovery is restricted by default in the self-provisioned role since elevated permissions are required to create Route 53 private hosted zones. To enable Service Discovery on a service, submit a Management | Other | Other | Update change type. To provide the information required to enable Service Discovery for your Amazon ECS Service, see the Service Discovery manual.

- AMS does not currently manage or restrict images used to deploy to containers onto Amazon ECS Fargate. You will be able to deploy images from Amazon ECR, Docker Hub, or any other private image repository. Therefore, we advised that public or any unsecured images not be deployed, since they may result in malicious activity on the account.

Q: What are the prerequisites or dependencies to using Amazon ECS on Fargate in my AMS account?

- The following are dependencies of Amazon ECS on Fargate; however, no additional action is required to enable these services with your self-provisioned role:
  - CloudWatch logs
  - CloudWatch events
  - CloudWatch alarms
  - CodeDeploy
  - App Mesh
  - Cloud Map
  - Route 53
- Depending on your use case, the following are resources that Amazon ECS relies on, and may require prior to using Amazon ECS on Fargate in your account:
  - Security group to be used with the Amazon ECS service. You can use the Deployment | Advanced stack components | Security Group | Create (auto) (ct-3pc215bnwb6p7), or, if your security group requires special rules, use Deployment | Advanced stack components | Security Group | Create (review required) (ct-1oxx2g2d7hc90). Note: The security group your select with Amazon ECS has to be created specifically for Amazon ECS where the Amazon ECS service or cluster reside. You can learn more in the **Security Group** section at Setting Up with Amazon ECS and Security in Amazon Elastic Container Service .
  - Application load balancer (ALB), network load balancer (NLB), classic load balancer (ELB) for load balancing between tasks.
  - Target Groups for ALBs.
  - App mesh resources (for instance, Virtual Routers, Virtual Services, Virtual Nodes) to integrate with your Amazon ECS Cluster.
- Currently, there is no way for AMS to automatically mitigate risk associated with supporting security groups' permissions when created outside of the standard AMS change types. We recommend that you request a specific security group for use with your Fargate cluster to limit the possibility of using a security group not designated for the use with Amazon ECS.

Amazon EKS on AWS Fargate

AWS Fargate is a technology that provides on-demand, right-sized compute capacity for containers (to understand containers, see What are Containers?). With AWS Fargate, you no longer have to provision, configure, or scale groups of virtual machines to run containers. This removes the need to choose server types, decide when to scale your node groups, or optimize cluster packing.

Amazon Elastic Kubernetes Service (Amazon EKS) integrates Kubernetes with AWS Fargate by using controllers that are built by AWS using the upstream, extensible model provided by Kubernetes. These controllers run as part of the Amazon EKS-managed Kubernetes control plane and are responsible for scheduling native Kubernetes pods onto Fargate. The Fargate controllers include a new scheduler that runs alongside the default Kubernetes scheduler in addition to several mutating and validating admission controllers. When you start a pod that meets the criteria for running on Fargate, the Fargate controllers running in the cluster recognize, update, and schedule the pod onto Fargate.

To learn more, see Amazon EKS on AWS Fargate Now Generally Available.

Amazon EKS on AWS Fargate in AMS FAQs

Q: How do I request access to Amazon EKS on Fargate in my AMS account?

Request access to Amazon EKS on Fargate by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account.

- `customer_eks_fargate_console_role`.

  After it's provisioned in your account, you must onboard the role in your federation solution.
- These service roles give Amazon EKS on Fargate permission to call other AWS services on your behalf:
  - `customer_eks_pod_execution_role`
  - `customer_eks_cluster_service_role`

Q: What are the restrictions to using Amazon EKS on Fargate in my AMS account?

- AMS will not include Trend Micro or preconfigured network security components for container images. Customers will be expected to manage their own image scanning services to detect malicious container images prior to deployment.
- EKSCTL is not supported due to CFN interdependencies.
- During cluster creation, you will have permissions to disable cluster control plane logging. For more information, see Amazon EKS control plane logging. We advise that you enable all important API, Authentication, and Audit logging on cluster creation.
- During cluster creation, cluster endpoint access for Amazon EKS clusters are defaulted to public; for more information, see Amazon EKS cluster endpoint access control. We recommend that Amazon EKS endpoints be set to private. If endpoints are required for public access, we recommend that they be set to public only for specific CIDR rangers.
- AMS does not have any method to force and restrict images used to deploy to containers on Amazon EKS Fargate. You're enabled to deploy images from Amazon ECR, Docker Hub, or any other private image repository. Therefore, there is a risk of deploying a public image that may perform malicious activity on the account.

Q: What are the prerequisites or dependencies to using Amazon EKS on Fargate in my AMS account?

In order to use the service, the following dependencies must be configured:

- For authenticating against the service, both KUBECTL and aws-iam-authenticator must be installed; for more information, see Managing cluster authentication.
- Kubernetes rely on a concept called "service accounts." In order to utilize the service accounts functionality inside of a kubernetes cluster on EKS, a Management | Other | Other | Update RFC is required with the following inputs:
  - [Required] Amazon EKS Cluster name
  - [Required] Amazon EKS Cluster namespace where service account (SA) will be deployed.
  - [Required] Amazon EKS Cluster SA name.
  - [Required] IAM Policy name and permissions/document to be associated.
  - [Required] IAM Role name being requested.
  - [Optional] OpenID Connect provider URL. For more information, see
    - Enabling IAM roles for service accounts on your cluster
    - Introducing fine-grained IAM roles for service accounts
- We recommend that Config rules be configured and monitored for
  - public cluster endpoints

- disabled API logging

Monitoring and remediating these Config rules will be your responsibility.

If you want to deploy an ALB Ingress controller, submit a Management | Other | Other Update RFC to provision the necessary IAM role to be used with the ALB Ingress Controller pod. The following inputs are required for creating IAM resources to be associated with ALB Ingress Controller (include these with your RFC):

- [Required] Amazon EKS Cluster name
- [Optional] OpenID Connect provider URL
- [Optional] Amazon EKS Cluster namespace where the application load balancer (ALB) ingress controller service will be deployed. [default: kube-system]
- [Optional] Amazon EKS Cluster service account (SA) name. [default: alb-ingress-controller]

If you want to enable envelope secrets encryption in your cluster (which we recommend), provide the KMS key ID, along with as much detail as possible (for instance, Amazon EKS Cluster Name and RFC ID) as a follow-up correspondence to the initial self-provisioned service CT request. You create a correspondence to an existing RFC after it has been submitted, by going to that RFC's details page. To learn more about envelope encryption, see Amazon EKS adds envelope encryption for secrets with AWS AWS KMS.

Amazon EMR

Amazon EMR is the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. With Amazon EMR you can run Petabyte-scale analysis at less than half of the cost of traditional on-premises solutions and over 3x faster than standard Apache Spark. For short-running jobs, you can spin up and spin down clusters and pay per second for the instances used. For long-running workloads, you can create highly available clusters that automatically scale to meet demand.

You can create one or more instances of the Amazon EMR clusters in either AMS multi-account landing zone or single-account landing zone accounts to support both transient and persistent Amazon EMR clusters. You can also enable Kerberos authentication to enable authenticate users from on-premises Active Directory domain.

You can leverage multiple data stores with the Amazon EMR clusters to support use-case specific Hadoop tools and libraries. The Amazon EMR clusters can be created using OnDemand or Spot instances and configure autoscaling to manage capacity and reduce the cost.

The cluster log files can be archived to an Amazon S3 bucket for logging and debugging. You can also access the web interfaces hosted in the Amazon EMR cluster to support hadoop administration requirements or note book experiences for customers.

To learn more, see Amazon EMR.

Amazon EMR in AMS FAQs

Q: How do I request access to Amazon EMR in my AMS account?

Request access to Amazon EMR by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM roles to your account:

- `customer_emr_cluster_instance_profile`
- `customer_emr_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

After it's provisioned in your account, you must onboard the roles in your federation solution.

Q: What are the restrictions to using Amazon EMR in my AMS account?

There are no restrictions for the use of Amazon EMR in your AMS account.

Q: What are the prerequisites or dependencies to using Amazon EMR in my AMS account?

AMS creates default security groups for the Amazon EMR master, worker, and services nodes.

If kerberos authentication is required for the Amazon EMR cluster:

- You should provide the realm name to be used for each kermerized Amazon EMR cluster and the on-premise Active Directory IP Addresses.
- Infrastructure requirements:

  Multi-Account Landing Zone (MALZ): Submit an RFC to create a new Managed application account or a new VPC in an existing application account.

  Single-Account Landing Zone (SALZ): Submit an RFC to create a new subnet in your VPC.
- Configure the incoming trust for the cluster's realm on the on-premise Active Directory.
- Submit an RFC to configure DNS zones for the realm in the Managed AD.
- Realm configuration:

  MALZ: Submit an RFC to update the VPC DHCP option set to use the realm name for domain name suffix.

  SALZ: Submit an RFC to generate a new Amazon EMR AMI to use the specific realm for domain name suffix.

Amazon EventBridge

Amazon EventBridge is a serverless event bus service that makes it easy to connect your applications with data from a variety of sources. EventBridge delivers a stream of real-time data from your own applications, Software-as-a-Service (SaaS) applications, and AWS services and routes that data to targets such as AWS Lambda. You can set up routing rules to determine where to send your data to build application architectures that react in real time to all of your data sources. EventBridge allows you to build event driven architectures, which are loosely coupled and distributed.

To learn more, see Amazon EventBridge.

EventBridge in AMS FAQs

Q: How do I request access to EventBridge in my AMS account?

Request access to EventBridge by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_eventbridge_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using EventBridge in my AMS account?

You must submit AMS RFCs and create the following resources: Service roles to trigger the batch job, SQS queue, CodeBuild, CodePipeline, and SSM commands.

Q: What are the prerequisites or dependencies to using EventBridge in my AMS account?

You must request an EventBridge service role with an RFC using the Management | Other | Other | Create change type prior to using EventBridge to trigger other AWS resources, such as AWS Batch, Lambda, Amazon SNS, Amazon SQS, or Amazon CloudWatch Logs resources. Please specify which services you wish to invoke when requesting your service role. To learn about permissions required to invoke targets, see the EventBridge documentation, Using Resource-Based Policies for EventBridge.

EventBridge is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in EventBridge. CloudTrail should be enabled and allowed to store the log files to S3 buckets. Note: All AMS Accounts have CloudTrail enabled, so no action is needed.

Amazon Forecast

Amazon Forecast (Forecast) is a fully managed service that uses machine learning to deliver highly accurate forecasts.

Based on the same technology used at Amazon.com, Forecast uses machine learning to combine time series data with additional variables to build forecasts. Forecast requires no machine learning experience to get started. You only need to provide historical data, plus any additional data that you believe may impact your forecasts. For example, the demand for a particular color of a shirt may change with the seasons and store location. This complex relationship is hard to determine on its own, but machine learning is ideally suited to recognize it. Once you provide your data, Forecast will automatically examine it, identify what is meaningful, and produce a forecasting model capable of making predictions that are up to 50% more accurate than looking at time series data alone.

To learn more, see Amazon Forecast.

Amazon Forecast in AMS FAQs

Q: How do I request access to Forecast in my AMS account?

Request access to AWS Firewall Manager by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_forecast_admin_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Forecast in my AMS account?

The default S3 bucket access only allows you to access buckets with the naming pattern 'customer-forecast-*'. If you have your own naming convention for data buckets, discuss bucket naming and related access setup with your Cloud Architect (CA). For example:

- You could define your specific Amazon Forecast service role with naming like 'AmazonForecast-ExecutionRole-*' and associated proper S3 bucket access. See the Service role - AmazonForecast-ExecutionRole-Admin and IAM policy - customer_forecast_default_s3_access_policy, in the IAM console.
- You may need to associate related S3 buckets access to IAM federation role. See the IAM policy - customer_forecast_default_s3_access_policy, in the IAM console.

Q: What are the prerequisites or dependencies to using Forecast in my AMS account?

- Proper Amazon S3 bucket(s) must be created before using Forecast. Especially, the default S3 buckets access is with naming pattern ‘customer-forecast-*’

- If you want to use naming patterns on S3 buckets other than 'customer-forecast-*', you must create a new service role with S3 access permissions on the buckets:
  1. A new service role to be created with naming 'AmazonForecast-ExecutionRole-{suffix}'.
  2. A new IAM policy to be created which is similar to customer_forecast_default_s3_access_policy and to be associated with the new service role and related federation admin role (e.g. 'customer_forecast_admin_role')

Q: How can I enhance data security while using Amazon Forecast?

- For data encryption at rest, you can use AWS KMS to provision a customer-managed CMK to protect data storage on Amazon S3 service:
  - Enable default encryption on the bucket with the provision key and set up bucket policy to accept AWS KMS data encryption while putting data.
  - Enable the Amazon Forecast service role 'AmazonForecast-ExecutionRole-*' and federation admin role (e.g. 'customer_forecast_admin_role') as the AWS KMS key user.
- For data encryption in transit, you can set up the HTTPS protocol, which is required while transferring objects on Amazon S3 bucket policy.
- Further restrictions on access control, enable a bucket policy for approved access for the Amazon Forecast service role 'AmazonForecast-ExecutionRole-*' and admin role (e.g. 'customer_forecast_admin_role').

Q: What are the best practices while using Amazon Forecast?

- You should have a good understanding of your data classification practices and map out the related data security needs while using S3 buckets with Amazon Forecast.
- For Amazon S3 bucket configuration, we strongly advise you to enable HTTPS enforcement in your S3 bucket policy.
- You must be aware of the admin role 'customer_forecast_admin_role' support permissive access (Get/Delete/Put S3 objects) on Amazon S3 buckets with naming of 'customer-forecast-*'. NOTE: If you require fine-grained access control for multiple teams, follow these practices:
  - Define your team-based access IAM identity (role/user) with least-privilege access to related Amazon S3 buckets.
  - Create team/project based AWS KMS CMKs grant proper access to corresponding IAM identities. (user access and 'AmazonForecast-ExecutionRole-{team/project}'.
  - Setup S3 bucket default encryption with the created AWS KMS CMKs.
  - Enforce S3 API traffics with HTTPS protocol on S3 bucket policy.
  - Enforce S3 bucket configuration for approved access for related IAM identities (user access and 'AmazonForecast-ExecutionRole-{team/project}' to the buckets.
- If you want to use the 'customer_forecast_admin_role' for general purpose, consider points listed previously to protect S3 buckets.

Q: Where is compliance information about Amazon Forecast?

See the AWS services Compliance Program.

Amazon FSx

Amazon FSx provides fully managed third-party file systems. Amazon FSx provides you with the native compatibility of third-party file systems with feature sets for workloads such as Windows-based storage, high-performance computing (HPC), machine learning, and electronic design automation (EDA). Amazon

FSx automates the time-consuming administration tasks such as hardware provisioning, software configuration, patching, and backups. Amazon FSx integrates the file systems with cloud-native AWS services, making them even more useful for a broader set of workloads.

Amazon FSx provides you with two file systems to choose from: Amazon FSx for Windows File Server for Windows-based applications and Amazon FSx for Lustre for compute-intensive workloads. To learn more, see Amazon FSx.

Amazon FSx in AMS FAQs

Q: How do I request access to Amazon FSx in my AMS account?

Request access to Amazon FSx by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_fsx_admin_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon FSx in my AMS account?

There are no restrictions. Full functionality of the service is available.

Q: What are the prerequisites or dependencies to using Amazon FSx in my AMS account?

There are no prerequisites. However, for advance configurations like Multi-AZ, you must install and manage the DFS Replication and DFS Namespaces services. For more information, see Deploying Multi-AZ File Systems.

Q: How do I integrate my Amazon FSx file system with my multi-account landing zone Managed AD?

When creating an Amazon FSx file system, you can specify your MALZ Managed AD as the 'AWS Managed Microsoft Active Directory' for Windows Authentication. For more information see, Using Amazon FSx with AWS Directory Service for Microsoft Active Directory

You must also share the Managed AD to the application account first. Do this by submitting an RFC with the Management | Other | Other | Create (ct-1e1xtak34nx76) change type.

Q: Which users belong in the AWS Delegated FSx Administrators group?

Only IT file server administrators. This group has **Full Access** privileges across all file shares.

Q: Should I use the default file share, share, which is created when the FSx system is provisioned?

No, we don't recommend using the the default file share, **share**, as provisioned. It grants **Full Access** to **Everyone**, which which violates the principle of least privilege. Instead, create smaller, custom file shares that match your business needs.

Q: How can I create custom file shares for specific organizations in my business?

See File Shares for instructions on creating custom file shares. Restrict access on each file share using the principle of least privilege.

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports, which are available via the Amazon Inspector console or API. To learn more, see Amazon Inspector.

Amazon Inspector in AMS FAQs

Q: How do I request access to Amazon Inspector in my AMS account?

Request access to Amazon Inspector by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the `customer_inspector_admin_role` IAM role to your account. The role includes the AWS-managed AmazonInspectorFullAccess policy. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon Inspector in my AMS account?

There are no restrictions. Full functionality of Amazon Inspector is available in your AMS account.

Q: What are the prerequisites or dependencies to using Amazon Inspector in my AMS account?

There are no prerequisites or dependencies to use Amazon Inspector in your AMS account.

Amazon Kinesis Data Analytics

Kinesis Data Analytics (KDA) Amazon Kinesis Data Analytics is the easiest way to analyze streaming data, gain actionable insights, and respond to your business and customer needs in real time. Amazon Kinesis Data Analytics reduces the complexity of building, managing, and integrating streaming applications with other AWS services. SQL users can easily query streaming data or build entire streaming applications using templates and an interactive SQL editor. Java developers can quickly build sophisticated streaming applications using open source Java libraries and AWS integrations to transform and analyze data in real time. Amazon Kinesis Data Analytics takes care of everything required to run your real-time applications continuously and scales automatically to match the volume and throughput of your incoming data. With Amazon Kinesis Data Analytics, you only pay for the resources your streaming applications consume. There is no minimum fee or setup cost. To learn more, see Amazon Kinesis Data Analytics.

Kinesis Data Analytics in AMS FAQs

Common questions and answers:

Q: How do I request access to Amazon Kinesis Data Analytics in my AMS account?

Request access to Kinesis Data Analytics by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_kinesis_analytics_application_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon Kinesis Data Analytics in my AMS account?

- Configurations are limited to resources without 'AMS-' or 'MC-' prefixes to prevent any modifications to AMS infrastructure.
- Permission to delete or create new Kinesis Data Streams or Kinesis Data Firehose has been removed from the policy. We have another policy that allows that.

Q: What are the prerequisites or dependencies to using Amazon Kinesis Data Streams in my AMS account?

There are a few dependencies:

- Amazon Kinesis Data Analytics requires that Kinesis Data Streams or Kinesis Data Firehose must be created prior to configuring an application with Kinesis Data Analytics.
- The resource-based policy permissions should indicate a particular input data source.

Amazon Kinesis Data Firehose

Kinesis Data Firehose (KDF) is the easiest way to reliably load streaming data into data lakes, data stores, and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon OpenSearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards you're already using today. It is a fully managed service that automatically scales to match the throughput of your data and requires no ongoing administration. It can also batch, compress, transform, and encrypt the data before loading it, minimizing the amount of storage used at the destination and increasing security. To learn more, see What Is Amazon Kinesis Data Firehose?

Kinesis Data Firehose in AMS FAQs

Common questions and answers:

Q: How do I request access to Amazon Kinesis Data Firehose in my AMS account?

Request access to Amazon Kinesis Data Firehose by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_kinesis_firehose_user_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Kinesis Data Firehose in my AMS account?

There are no restrictions. Full functionality of Amazon Kinesis Data Firehose is available in your AMS account.

Q: What are the prerequisites or dependencies to using Kinesis Data Firehose in my AMS account?

New service-linked IAM roles must be requested for each delivery stream. You can also re-use a single service-linked role for all streams by updating the role policy with the required resource permissions (including S3 buckets/ KMS Keys / Lambda Functions / Kinesis streams).

After you have submitted the RFC to add Kinesis Data Firehose, an AMS Operations engineer will reach out to you through a Service Request for the ARNs of resources that you would like to connect with Data Firehose (for example, AWS KMS, S3, Lambda, and Kinesis Streams).

Amazon Kinesis Data Streams

Amazon Kinesis Data Streams (KDS) is a highly scalable, and durable, real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events. The data collected is available in milliseconds to enable real-time analytics use cases such as real-time dashboards, real-time anomaly detection, dynamic pricing, and more. To learn more, see Amazon Kinesis Data Streams.

Kinesis Data Streams in AMS FAQs

Common questions and answers:

Q: How do I request access to Amazon Kinesis Data Streams in my AMS account?

Request access to Amazon Kinesis Data Streams by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_kinesis_data_streaming_user_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon Kinesis Data Streams in my AMS account?

There are no restrictions. Full functionality of Amazon Kinesis Data Streams is available in your AMS account.

Q: What are the prerequisites or dependencies to using Amazon Kinesis Data Streams in my AMS account?

There are no prerequisites or dependencies to use Amazon Kinesis Data Streams in your AMS account.

Amazon Kinesis Video Streams

Amazon Kinesis Video Streams (KVS) helps you to securely stream video from connected devices to AWS for analytics, machine learning (ML), playback, and other processing. Kinesis Video Streams automatically provisions, and elastically scales, all the infrastructure needed to ingest streaming video data from millions of devices. It also durably stores, encrypts, and indexes video data in your streams, and allows you to access your data through easy-to-use APIs. Kinesis Video Streams enables you to playback video for live and on-demand viewing, and quickly build applications that take advantage of computer vision and video analytics through integration with Amazon Rekognition Video, and libraries for ML frameworks such as Apache MxNet, TensorFlow, and OpenCV. To learn more, see Amazon Kinesis Video Streams.

Amazon Kinesis Video Streams in AMS FAQs

Common questions and answers:

Q: How do I request access to Amazon Kinesis Video Streams in my AMS account?

Request access to Amazon Kinesis Video Streams by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_kinesis_video_streaming_user_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon Kinesis Video Streams in my AMS account?

There are no restrictions. Full functionality of Amazon Kinesis Video Streams is available in your AMS account.

Q: What are the prerequisites or dependencies to using Amazon Kinesis Video Streams in my AMS account?

There are no prerequisites or dependencies to use Amazon Kinesis Video Streams in your AMS account.

Amazon Lex

Amazon Lex is a service for building conversational interfaces into any application using voice and text. Amazon Lex provides the advanced deep learning functionalities of automatic speech recognition (ASR) for converting speech to text, and natural language understanding (NLU) to recognize the intent of the text, to enable you to build applications with highly engaging user experiences and lifelike

conversational interactions. With Amazon Lex, the same deep learning technologies that power Amazon Alexa are now available to any developer, enabling you to quickly and easily build sophisticated, natural language, conversational bots or chatbots. To learn more, see Amazon Lex.

Amazon Lex in AMS FAQs

Common questions and answers:

Q: How do I request access to Amazon Lex in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_lex_author_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon Lex in my AMS account?

Amazon Lex integration with Lambda is limited to Lambda functions without an "AMS-" prefix, in order to prevent any modifications to AMS infrastructure.

Q: What are the prerequisites or dependencies to using Amazon Lex in my AMS account?

There are no prerequisites or dependencies to use Amazon Lex in your AMS account.

Amazon MQ

Amazon MQ is a managed message broker service for Apache ActiveMQ that helps you to set up and operate message brokers in the cloud. Message brokers allow different software systems, often using different programming languages and on different platforms, to communicate and exchange information. Amazon MQ reduces your operational load by managing the provisioning, setup, and maintenance of ActiveMQ, a popular open-source message broker. Connecting your current applications to Amazon MQ uses industry standard APIs and protocols for messaging, including JMS, NMS, AMQP, STOMP, MQTT, and WebSocket. Using standards means that, in most cases, there's no need to rewrite any messaging code when you migrate to AWS. To learn more, see What Is Amazon MQ?

Amazon MQ in AMS FAQs

Common questions and answers:

Q: How do I request access to Amazon MQ in my AMS account?

Utilization of Amazon MQ in your AMS account is a two-step process:

1. Provision the Amazon MQ Broker. To do this, submit a CFN Template, with the Amazon MQ Broker included, through an RFC with the Deployment | Ingestion | Stack from CloudFormation Template | Create change type (ct-36cn2avfrrj9v), or submit an RFC with the Management | Other | Other | Create change type (ct-1e1xtak34nx76) change type requesting that Amazon MQ Broker be provisioned in your account.
2. Access the Amazon MQ console. After the Amazon MQ Broker is provisioned, obtain access to the Amazon MQ console by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_mq_console_role`.

After the role is provisioned in your account, you must onboard it in your federation solution.

Q: What are the restrictions to using Amazon MQ in my AMS account?

Full functionality of Amazon MQ is available in your AMS account; however, provisioning Amazon MQ Broker is not available through the policy due to the elevated permission required. See above for details on how to provision Amazon MQ broker in your accounts.

Q: What are the prerequisites or dependencies to using Amazon MQ in my AMS account?

There are no prerequisites or dependencies to use Amazon MQ in your AMS account.

Amazon MSK

Amazon MSK is a fully managed AWS streaming data service makes it easy for you to build and run applications that use Apache Kafka to process streaming data without needing to become an expert in operating Apache Kafka clusters. Amazon MSK manages the provisioning, configuration, and maintenance of Apache Kafka clusters and Apache ZooKeeper nodes for you. Amazon MSK also shows key Apache Kafka performance metrics in the AWS Console.

Amazon MSK provides multiple levels of security for your Apache Kafka clusters, including VPC network isolation, AWS IAM for control-plane API authorization, encryption at rest, TLS encryption in-transit, TLS based certificate authentication, SASL/SCRAM authentication secured by AWS Secrets Manager. To learn more, see Amazon MSK.

Amazon MSK in AMS FAQs

Common questions and answers:

Q: How do I request access to Amazon MSK in my AMS account?

You can request access by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM policies and role to your account:

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`
- `customer-msk-admin-role.json`

Once provisioned in your account you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon MSK?

For Amazon MSK to deliver broker logs to the destinations that you configure, ensure that the `AmazonMSKFullAccess` policy is attached to your IAM role. So full access permissions are already in place.

Q: What are the prerequisites or dependencies to using Amazon MSK?

Before creating your MSK cluster, you must have a VPC and subnets within that VPC. By default, AMS has this covered as part of default AMS VPC creation.

To learn about the limitation of Amazon MSK, refer to Amazon MSK Limits.

Amazon Personalize

Amazon Personalize is a machine learning service that makes it easy for developers to create individualized recommendations for customers using their applications.

Machine learning is being increasingly used to improve customer engagement by powering personalized product and content recommendations, tailored search results, and targeted marketing promotions. However, developing the machine-learning capabilities necessary to produce these sophisticated recommendation systems has been beyond the reach of most organizations today due to the complexity. Amazon Personalize allows developers with no prior machine learning experience to easily build sophisticated personalization capabilities into their applications, using machine learning technology perfected from years of use on Amazon.com.

With Amazon Personalize, you provide an activity stream from your application – clicks, page views, signups, purchases, and so forth – as well as an inventory of the items you want to recommend, such as articles, products, videos, or music. You can also choose to provide Amazon Personalize with additional demographic information from your users such as age, or geographic location. Amazon Personalize will process and examine the data, identify what is meaningful, select the right algorithms, and train and optimize a personalization model that is customized for your data. All data analyzed by Amazon Personalize is kept private and secure, and only used for your customized recommendations. You can start serving personalized recommendations via a simple API call. You pay only for what you use, and there are no minimum fees and no upfront commitments.

To learn more, see Amazon Personalize.

Amazon Personalize in AMS FAQs

Q: How do I request access to Amazon Personalize in my AMS account?

Request access to Amazon Personalize by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type, and you need to specify which S3 bucket contains the data to be used by AWS personalize to generate the recommendations. This RFC provisions the following IAM roles to your account: `customer_personalize_console_role` and `customer_personalize_service_role`.

- Once the `customer_personalize_console_role` is provisioned in your account, you must onboard the role in your federation solution. You can also attach the `customer_personalize_console_policy` to another existing role other than `Customer_ReadOnly_Role`.
- After the `customer_personalize_service_role` is provided to your account, then you can refer its ARN when creating a new dataset group.

At this time, AMS Operations will also deploy this service role in your account: `aws_code_pipeline_service_role_policy`.

Q: What are the restrictions to using Amazon Personalize in my AMS account?

Amazon Personalize configuration is limited to resources without 'ams-' or 'mc-' prefixes, to prevent any modifications to AMS infrastructure.

Q: What are the prerequisites or dependencies to using Amazon Personalize in my AMS account?

- If the S3 bucket where data is stored is encrypted, the KMS key ID must be provided, so we can allow the role used by Amazon Personalize to decrypt the bucket.

  Amazon Personalize does not support the default KMS S3 key. If required to use KMS, create a custom key and add the following policy to it by opening an RFC with change type KMS Key | Create (Review Required):

```
{
    "Version": "2012-10-17",
    "Id": "key-consolepolicy-3",
```

```
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "Service": "personalize.amazonaws.com"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

- An S3 bucket must be created with the following bucket policy. Do this by submitting an RFC with change type S3 Storage | Create Policy. This policy allows Amazon Personalize to access data; that bucket will contain the data to be used by Amazon Personalize.

```
{
"Version": "2012-10-17",
"Id": "PersonalizeS3BucketAccessPolicy",
"Statement": [
{
"Sid": "PersonalizeS3BucketAccessPolicy",
"Effect": "Allow",
"Principal": {
"Service": "personalize.amazonaws.com"
},
"Action": [
"s3:GetObject",
"s3:ListBucket"
],
"Resource": [
"arn:aws:s3:::bucket-name",
"arn:aws:s3:::bucket-name/*"
]
}
]
}
```

Amazon QuickSight

Amazon QuickSight is a fast, cloud-powered business intelligence service that delivers insights to everyone in your organization. As a fully managed service, Amazon QuickSight lets you easily create and publish interactive dashboards that include machine learning (ML) insights. To learn more, see Amazon QuickSight.

Amazon QuickSight in AMS FAQs

Common questions and answers:

Q: How do I request access to Amazon QuickSight in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_quicksight_console_admin_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon QuickSight in my AMS account?

- AWS resource settings on Amazon QuickSight won't be accessible to you because of the IAM policy dependency. However, the AMS team ensures that all of them are enabled when a request is submitted to enable the service.
- Resource access for individual users and groups are not supported in this model because this feature enables users to alter IAM permissions that could compromise AMS infrastructure.
- The ability to invite IAM identities from within QuickSight is not supported due to the risk involved altering IAM objects.
- Amazon QuickSight service offers two editions: Enterprise and Standard. Both provide a single sign-on (SSO) option that is supported on AMS. However, the Enterprise Edition has an option to integrate Amazon QuickSight with Active Directory (AD). Amazon QuickSight on AMS does not support integration with AD due to incompatibilities between AMS account structure and the Amazon QuickSight trust requirements.

Q: What are the prerequisites or dependencies to using Amazon QuickSight in my AMS account?

- When AMS receives this RFC to add Amazon QuickSight, you are sent a service request for additional information; provide them the following:
  - Amazon QuickSight account name (for example, *`CustomerName`*`-quicksight`
  - Amazon QuickSight Edition (Standard versus Enterprise)
  - The AWS Region in which to enable the Amazon QuickSight service (defaults to your AMS AWS Region).
  - A notification email address for Amazon QuickSight account.
  - (Optional) The S3 bucket where data files to be analyzed are located.
  - The VPC and subnet IDs that connect to Amazon QuickSight support a feature to add a VPC connection, which enables private connectivity between Amazon QuickSight and resources inside the account.

An AMS operator performs the sign up process on your behalf and configures two QuickSight functionalities:

- Auto discovery to data sources.
- VPC connections.

> **Note**
> These actions need to be performed by an AMS operator because elevated IAM and VPC permissions are required during the sign-in process.

Amazon Rekognition

Amazon Rekognition makes it easy to add image and video analysis to your applications using proven, highly scalable, deep learning technology that requires no machine learning expertise to use. With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate facial analysis and facial search capabilities that you can use to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases.

With Amazon Rekognition Custom Labels, you can identify objects and scenes in images that are specific to your business needs. For example, you can build a model to classify specific machine parts on your assembly line or to detect unhealthy plants. Amazon Rekognition Custom Labels takes care of the model development heavy lifting for you, so no machine learning experience is required. You simply need to supply images of objects or scenes you want to identify, and the service handles the rest.

To learn more, see Amazon Rekognition.

Amazon Rekognition in AMS FAQs

Common questions and answers:

Q: How do I request access to Amazon Rekognition in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_rekognition_console_role & customer_rekognition_service_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon Rekognition in my AMS account?

Full functionality of Amazon Rekognition is available with the Amazon Rekognition self-provisioned service role.

Q: What are the prerequisites or dependencies to using Amazon Rekognition in my AMS account?

If you use Kinesis Video Streams that provide the source streaming video for an Amazon Rekognition Video stream processor or a data stream as a destination to write data to Kinesis Data Streams, kindly provide AMS with a `kinesisStreamName` when creating the RFC.

Amazon SageMaker

SageMaker provides every developer and data scientist with the ability to build, train, and deploy machine learning models quickly. Amazon SageMaker is a fully-managed service that covers the entire machine learning workflow to label and prepare your data, choose an algorithm, train the model, tune and optimize it for deployment, make predictions, and take action. Your models get to production faster with much less effort and lower cost. To learn more, see Amazon SageMaker.

SageMaker in AMS FAQs

Common questions and answers:

Q: How do I request access to SageMaker in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_sagemaker_admin_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using SageMaker in my AMS account?

- The following use cases are not supported by the AMS Amazon SageMaker IAM role:
  - SageMaker Studio is not supported at this time.
  - SageMaker Ground Truth to manage private workforces is not supported since this feature requires overly permissive access to Amazon Cognito resources. If managing a private workforce is required, you can request a custom IAM role with combined SageMaker and Amazon Cognito permissions. Otherwise, we recommend using public workforce (backed by Amazon Mechanical Turk), or AWS Marketplace service providers, for data labeling.
- Creating VPC Endpoints to support API calls to SageMaker services (aws.sagemaker.{region}.notebook, com.amazonaws.{region}.sagemaker.api & com.amazonaws.{region}.sagemaker.runtime) is not supported as permissions can't be scoped down to SageMaker related services only. To support this use case, submit a Management | Other | Other RFC to create related VPC endpoints.

- SageMaker endpoint auto scaling is not supported as SageMaker requires `DeleteAlarm` permissions on any ("*") resource. To support endpoint auto scaling, submit a Management | Other | Other RFC to setup auto scaling for a SageMaker endpoint.

Q: What are the prerequisites or dependencies to using SageMaker in my AMS account?

- The following use cases require special configuration prior to use:
  - If an S3 bucket will be used to store model artifacts and data, then you must request an S3 bucket named with the required keywords ("SageMaker", "Sagemaker", "sagemaker" or "aws-glue") with a Deployment | Advanced stack components | S3 storage | Create RFC.
  - If Elastic File Store (EFS) will be used, then EFS storage must be configured in the same subnet, and allowed by security groups.
  - If other resources require direct access to SageMaker services (notebooks, API, runtime, and so on), then configuration must be requested by:
    - Submitting an RFC to create a security group for the endpoint (Deployment | Advanced stack components | Security group | Create (auto)).
    - Submitting a Management | Other | Other | Create RFC to set up related VPC endpoints.

Q: What are the supported naming conventions for resources that the `customer_sagemaker_admin_role` can access directly? (The following are for update and delete permissions; if you require additional supported naming conventions for your resources, reach out to an AMS Cloud Architect for consultation.)

- Resource: Passing `AmazonSageMaker-ExecutionRole-*` role
  - Permissions: The SageMaker self-provisioned service role supports your use of the SageMaker service role (`AmazonSageMaker-ExecutionRole-*`) with AWS Glue, AWS RoboMaker, and AWS Step Functions.
- Resource: Secrets on AWS Secrets Manager
  - Permissions: Describe, Create, Get, Update secrets with a `AmazonSageMaker-*` prefix.
  - Permissions: Describe, Get secrets when the `SageMaker` resource tag is set to `true`.
- Resource: Repositories on AWS CodeCommit
  - Permissions: Create/ delete repositories with a `AmazonSageMaker-*` prefix.
  - Permissions: Git Pull/Push on repositories with following prefixes, `*sagemaker*`, `*SageMaker*`, and `*Sagemaker*`.
- Resource: Amazon ECR (Amazon Elastic Container Registry) Repositories
  - Permissions: Permissions: Set, delete repository policies, and upload container images, when the following resource naming convention is used, `*sagemaker*`.
- Resource: Amazon S3 buckets
  - Permissions: Get, Put, Delete object, abort multipart upload S3 objects when resources have the following prefixes: `*SageMaker*`, `*Sagemaker*`, `*sagemaker*` and `aws-glue`.
  - Permissions: Get S3 objects when the `SageMaker` tag is set to `true`.
- Resource: Amazon CloudWatch Log Group
  - Permissions: Create Log Group or Stream, Put Log Event, List, Update, Create , Delete log delivery with following prefix: `/aws/sagemaker/*`.
- Resource: Amazon CloudWatch Metric
  - Permissions: Put metric data when the following prefixes are used: `AWS/SageMaker`, `AWS/SageMaker/`, `aws/SageMaker`, `aws/SageMaker/`, `aws/sagemaker`, `aws/sagemaker/`, and `/aws/sagemaker/.`.
- Resource: Amazon CloudWatch Dashboard
  - Permissions: Create/Delete dashboards when the following prefixes are used: `customer_*`.

- Resource: Amazon SNS (Simple Notification Service) topic
  - Permissions: Subscribe/Create topic when following prefixes are used: `*sagemaker*`, `*SageMaker*`, and `*Sagemaker*`.

Q: What's the difference between `AmazonSageMakerFullAccess` and `customer_sagemaker_admin_role`?

The `customer_sagemaker_admin_role` with the `customer_sagemaker_admin_policy` provides almost the same permissions as AmazonSageMakerFullAccess except:

- Permission to connect with RoboMaker, Cognito, and Glue resources.
- Sagemaker endpoint autoscaling. You must submit a Management | Other | Other | Update RFC to elevate to autoscaling permissions temporarily, or permanently, as autoscaling requires permissive access on CloudWatch service.

Q: How do I adopt KMS CMKs in data encryption at rest?

You must ensure that the key policy has been set up properly on the CMKs so that related IAM users/roles can use the keys. For more information, see the AWS KMS Key Policy document.

Amazon Simple Email Service

Amazon Simple Email Service (Amazon SES) is a cloud-based email sending service designed to help digital marketers and application developers, send marketing, notification, and transactional emails.

You can use the SMTP interface or one of the AWS SDKs to integrate Amazon SES directly into your existing applications. You can also integrate the email sending capabilities of Amazon SES into the software you already use, such as ticketing systems and email clients.

To learn more, see Amazon Simple Email Service.

Amazon SES in AMS FAQs

Q: How do I request access to Amazon SES in my AMS account?

Request access to Amazon SES by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_ses_admin_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the prerequisites or dependencies to using Amazon SES in my AMS account?

- You must configure an S3 bucket policy to allow Amazon SES to publish events to the bucket.
- You must use a default (AWS SES), or configure, a CMK key to allow Amazon SES to encrypt emails and push events to other service resources like S3, SNS, Lambda, and Firehose, belonging to the account.

Q: What are the restrictions to using Amazon SES in my AMS account?

You must raise RFCs to create the following resources:

- An SMTP user and IAM service role with PutEvents permission, to a Kinesis Firehose stream.
- You must create new AWS resources such as S3 bucket, Firehose stream, SNS topic by using AMS change types in order for yourAmazon SES rules and configuration sets' destinations to work with those resources.

- SMTP credentials. To request new SMTP credentials, use the Change Type (Management | Other | Other | Create). AMS creates the credentials and add them to Secrets Manager for you.

Amazon Simple Workflow Service

Amazon Simple Workflow Service (Amazon SWF) helps developers build, run, and scale background jobs that have parallel or sequential steps. You can think of Amazon SWF as a fully-managed state tracker and task coordinator in the Cloud. If your application's steps take more than 500 milliseconds to complete, you need to track the state of processing, or you need to recover or retry if a task fails, Amazon SWF can help you. To learn more, see Amazon Simple Workflow Service.

Amazon SWF in AMS FAQs

Common questions and answers:

Q: How do I request access to Amazon SWF in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_swf_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon SWF in my AMS account?

The Lambda `InvokeFunction` permissions have been included in this service however, the AMS `customer_deny_policy` that is added to all AMS customer roles explicitly denies access to AMS Lambda functions and AMS-owned resources. In order to tag or untag resources within Amazon SWF, submit a Management | Other | Other Change Type.

Q: What are the prerequisites or dependencies to using Amazon SWF in my AMS account?

Amazon SWF is dependent on the AWS Lambda service, therefore, permissions to invoke Lambda have been provided as a part of this role and no additional permissions are required to invoke Lambda from Amazon SWF. Otherwise, there are no prerequisites to using Amazon SWF.

Amazon Textract

Amazon Textract is a fully managed machine learning service that automatically extracts printed text, handwriting, and other data from scanned documents that goes beyond simple optical character recognition (OCR) to identify, understand, and extract data from forms and tables. To learn more, see Amazon Textract.

Amazon Textract in AMS FAQs

Common questions and answers:

Q: How do I request Amazon Textract to be set up in my AMS account?

Request access to Amazon Textract by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM roles to your account: `customer_textract_console_role`, `customer_textract_human_review_execution_role`, and `customer_ec2_textract_instance_profile`. Once provisioned in your account, you must onboard the role `customer_textract_console_role` in your federation solution.

Q: What are the restrictions to using Amazon Textract in my AMS account?

There are no restrictions for the use of Amazon Textract in your AMS account.

Q: What are the prerequisites or dependencies to using Amazon Textract in my AMS account?

You must request the creation of an S3 bucket by submitting an RFC Deployment | Advanced stack components |S3 storage | Create (ct-1a68ck03fn98r).

Amazon Transcribe

Powered by deep learning technologies, Amazon Transcribe is a fully managed and continuously trained automatic speech recognition service that automatically generates time-stamped text transcripts from audio files. Amazon Transcribe makes it easy for developers to add speech-to-text capabilities to their applications. Audio data is virtually impossible for computers to search and analyze. Therefore, recorded speech needs to be converted to text before it can be used in applications. Historically, customers had to work with transcription providers that required them to sign expensive contracts and were hard to integrate into their technology stacks to accomplish this task. Many of these providers use outdated technology that does not adapt well to different scenarios, like low-fidelity phone audio common in contact centers, which results in poor accuracy.

Amazon Transcribe uses a deep learning process called automatic speech recognition (ASR) to convert speech into text, quickly and accurately. Amazon Transcribe can be used to transcribe customer service calls, automate closed captioning and subtitling, and generate metadata for media assets to create a fully searchable archive. You can use Amazon Transcribe Medical to add medical speech-to-text capabilities to clinical documentation applications. To learn more, see Amazon Transcribe.

Amazon Transcribe in AMS FAQs

Common questions and answers:

Q: How do I request Amazon Transcribe to be set up in my AMS account?

Request access to Amazon Transcribe by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_transcribe_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon Transcribe in my AMS account?

You must use 'customer-transcribe*' as the prefix for your buckets when working with transcribe, unless RA and specified otherwise.

You are not able to create an IAM role within Amazon transcribe.

You cannot use a service-managed S3 bucket for output data in default SSPS (if this is needed, please reach out to your account CA).

You must submit Risk Acceptance if you want to use customer-managed KMS Keys that do not fall under the AMS namespace.

Q: What are the prerequisites or dependencies to using Amazon Transcribe in my AMS account?

S3 must have access to the buckets with the name 'customer-transcribe*'. KMS is required in order to use Amazon Transcribe if your S3 buckets are encrypted with KMS keys. If a bucket doesn't need to be encrypted "KMStranscribeAllow" can be removed.

Amazon WorkDocs

Amazon WorkDocs is a fully-managed, secure content creation, storage, and collaboration service. With Amazon WorkDocs, you can easily create, edit, and share content, and because it's stored centrally on AWS, access it from anywhere on any device. Amazon WorkDocs helps you to collaborate with others, and lets you easily share content, provide rich feedback, and collaboratively edit documents. You can use Amazon WorkDocs to retire your legacy file share infrastructure by moving file shares to the cloud. Amazon WorkDocs lets you integrate with your existing systems, and offers a rich API so that you can develop your own content-rich applications. Amazon WorkDocs is built on AWS, where your content is secured on the world's largest cloud infrastructure. To learn more, see Amazon WorkDocs.

Amazon WorkDocs in AMS FAQs

Common questions and answers:

Q: How do I request access to Amazon WorkDocs in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_workdocs_console_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Amazon WorkDocs in my AMS account?

Full functionality of Amazon WorkDocs is available in your AMS account. However, you can't delete an Amazon WorkDocs site. The permissions required to de-register an Amazon WorkDocs site require modification to the AWS Managed Microsoft AD directory. To do this, submit an AMS service request for the deletion of an Amazon WorkDocs site.

Q: What are the prerequisites or dependencies to using Amazon WorkDocs in my AMS account?

Amazon WorkDocs has a dependency on AWS Directory Service for Microsoft Active Directory (MAD). AMS has MAD already implemented in AMS accounts; however, it is limited to a one-way trust. You must submit a service request to AMS to have an AD Connector set up to proxy your on-premises domain.

Amazon WorkSpaces

WorkSpaces enables you to provision virtual, cloud-based Microsoft Windows or Amazon Linux desktops for your users, known as WorkSpaces. WorkSpaces eliminates the need to procure and deploy hardware or install complex software. You can quickly add or remove users as your needs change. Users access their WorkSpaces by using a client application from a supported device or, for Windows WorkSpaces, a web browser, and they log in by using their existing on-premises Active Directory (AD) credentials.

To learn more, see Amazon WorkSpaces.

WorkSpaces in AMS FAQs

Common questions and answers:

Q: How do I request access to WorkSpaces in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account:

`customer_workspaces_console_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using WorkSpaces in my AMS account?

Full functionality of Workspaces is available with the Amazon WorkSpaces self-provisioned service role.

Q: What are the prerequisites or dependencies to using WorkSpaces in my AMS account?

- WorkSpaces are limited by AWS Region; therefore, the AD Connector must be configured in the same AWS Region where the WorkSpaces instances are hosted.

  Customers can connect WorkSpaces to customer AD using one of the following two methods:

  1. Using AD connector to proxy authentication to on-premises Active Directory service (preferred):

     Configure Active Directory (AD) Connector in your AMS account prior to integrating your WorkSpaces instance with your on-premises directory service. The AD Connector acts as a proxy for your existing AD users (from your domain) to connect to WorkSpaces using existing on-premises AD credentials. This is preferred because WorkSpaces are directly joined to the customer's on-prem domain, which acts as both Resource and User forest, leading to more control on the customer side.

     For more information, see Best Practices for Deploying Amazon WorkSpaces (Scenario 1).
  2. Using AD Connector with AWS Microsoft AD, Shared Services VPC, and a one-way trust to on-premises:

     You can also authenticate users with your on-premises directory by first establishing a one-way outgoing trust from AMS-managed AD to your on-premises AD. WorkSpaces will join AMS-managed AD using an AD Connector. WorkSpaces access permissions will then be delegated to the WorkSpaces instances through the AMS-managed AD, without the need to establish a two-way trust with your on-premises environment. In this scenario, the User forest will be in the customer AD and the Resource forest will be in the AMS-managed AD (changes to AMS-managed AD can be requested via RFC). Note that the connectivity between WorkSpaces VPC and the MALZ Shared Services VPC running AMS-managed AD is established via Transit Gateway.

     For more information, see Best Practices for Deploying Amazon WorkSpaces (Scenario 6).

     Note
     The AD Connector can be configured by submitting a Management | Other | Other | Create change type RFC with the prerequisite AD configuration details; for more information, see Create an AD Connector. If method 2 is used to create a Resource forest in AMS-managed AD, submit another Management | Other | Other | Create change type RFC in AMS shared-services account by running the AMS-managed AD.

AMS CodeSuite

AMS CodeSuite includes the following services:

- AWS CodeCommit: A fully managed source control service that hosts secure Git-based repositories. It makes it so teams can collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. You can use CodeCommit to securely store anything from source code to binaries, and it works seamlessly with your existing Git tools. To learn more, see AWS CodeCommit
- AWS CodeBuild: A fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. With CodeBuild, you don't need to provision, manage, and scale your own build servers. CodeBuild scales continuously and processes multiple builds concurrently, so your builds are not left waiting in a queue. You can get started quickly by using prepackaged build environments, or you can create custom build environments that use your

own build tools. With CodeBuild, you are charged by the minute for the compute resources you use. To learn more, see AWS CodeBuild

- AWS CodeDeploy: A fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2 and your on-premises servers. AWS CodeDeploy helps you to rapidly release new features, helps you avoid downtime during application deployment, and handles the complexity of updating your applications. You can use AWS CodeDeploy to automate software deployments, eliminating the need for error-prone manual operations. The service scales to match your deployment needs. To learn more, see AWS CodeDeploy
- AWS CodePipeline: A fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates. CodePipeline automates the build, test, and deploy phases of your release process every time there is a code change, based on the release model you define. This enables you to rapidly and reliably deliver features and updates. You can easily integrate AWS CodePipeline with third-party services such as GitHub or with your own custom plugin. With AWS CodePipeline, you only pay for what you use. There are no upfront fees or long-term commitments. To learn more, see AWS CodePipeline

To learn more, see Tag: code-suite.

AMS CodeSuite in AMS FAQs

Q: How do I request access to AMS CodeSuite in my AMS account?

Request access to AMS CodeSuite by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_code_suite_console_role`. After provisioned in your account, you must onboard the role in your federation solution. At this time AMS Operations will also deploy the `customer_codebuild_service_role`, `customer_codedeploy_service_role`, `aws_code_pipeline_service_role` service roles in your account for CodeBuild, CodeDeploy and CodePipeline services. If additional IAM permissions for the are required for the `customer_codebuild_service_role` are needed, submit an AMS service request.

> **Note**
> You can also add these services separately; for information, see AWS CodeBuild (p. 217), AWS CodeDeploy (p. 219), and AWS CodePipeline (p. 219), respectively.

Q: What are the restrictions to using AMS CodeSuite in my AMS account?

- AWS CodeCommit: The triggers feature on CodeCommit is disabled given the associated rights to create SNS topics. Directly authenticating against CodeCommit is restricted; users should authenticate with Credential Helper. Some KMS commands are also restricted: kms:Encrypt, kms:Decrypt, kms:ReEncrypt, kms:GenereteDataKey, kms:GenerateDataKeyWithoutPlaintext, and kms:DescribeKey.
- CodeBuild: For AWS CodeBuild console admin access, permissions are limited at the resource level; for example, CloudWatch actions are limited on specific resources and the `iam:PassRole` permission is controlled.
- CodeDeploy: Currently CodeDeploy supports deployments on Amazon EC2/On-premises only. Deployments on ECS and Lambda through CodeDeploy is not supported.
- CodePipeline: CodePipeline features, stages, and providers are limited to the following:
  - Deploy Stage: Amazon S3 and AWS CodeDeploy
  - Source Stage: Amazon S3, AWS CodeCommit, Bit Bucket, and GitHub
  - Build Stage: AWS CodeBuild and Jenkins
  - Approval Stage: Amazon SNS
  - Test Stage: AWS CodeBuild, Jenkins, BlazeMeter, Ghost Inspector UI Testing, Micro Focus StormRunner Load, Runscope API Monitoring
  - Invoke Stage: Step Functions and Lambda

Note
AMS Operations will deploy the `customer_code_pipeline_lambda_policy` in your account; it must be attached with the Lambda execution role for Lambda invoke stage. Please provide the Lambda service/execution role name that you want this policy added with. If there is no custom Lambda service/execution role, AMS will create a new role named `customer_code_pipeline_lambda_execution_role`, which will be a copy of `customer_lambda_basic_execution_role` along with `customer_code_pipeline_lambda_policy`.

Q: What are the prerequisites or dependencies to using AMS CodeSuite in my AMS account?

- CodeCommit: If S3 buckets are encrypted with AWS KMS keys, S3 and AWS KMS are required to use AWS CodeCommit.
- CodeBuild: If additional IAM permissions are required for the defined AWS CodeBuild service role, request them through an AMS service request.
- CodeDeploy: None.
- CodePipeline: None. AWS supported services—AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy—must be launched prior to, or along with, the launch of CodePipeline. However this will be taken care by an AMS engineer; you don't need to do anything.

AWS Amplify

The AWS Amplify is a toolchain that includes a robust feature set for simplifying mobile and web application development. The CLI uses AWS CloudFormation and nested stacks to allow you to add or modify configurations locally before you push them for execution in your account. To learn more, see AWS Amplify.

AWS Amplify in AMS FAQs

Common questions and answers:

Q: How do I request AWS Amplify to be set up in my AMS account?

Request access through the submission of the AWS Services RFC (Management | AWS Service | Compatible Service). Through this RFC, the following IAM user will be provisioned in your account: `customer_amplify_cli_user`.

Q: What are the restrictions to using AWS Amplify in my AMS account?

There are no restrictions for the use of AWS Amplify in your AMS account.

Q: What are the prerequisites or dependencies to using AWS Amplify in my AMS account?

There are no prerequisites for the use of AWS Amplify in your AMS account.

AWS AppSync

AWS AppSync simplifies application development by letting you create a flexible API to securely access, manipulate, and combine data from one or more data sources. AWS AppSync is a managed service that uses GraphQL to make it easy for applications to get exactly the data they need.

With AWS AppSync, you can build scalable applications, including those requiring real-time updates, on a range of data sources such as NoSQL data stores, relational databases, HTTP APIs, and your custom

data sources with AWS Lambda. For mobile and web apps, AWS AppSync additionally provides local data access when devices go offline, and data synchronization with customizable conflict resolution, when they are back online. To learn more, see AWS AppSync.

AWS AppSync in AMS FAQs

Common questions and answers:

Q: How do I request access AWS AppSync in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM roles to your account: `customer_appsync_service_role` and `customer_appsync_author_role`. Once provisioned in your account, you must onboard the `customer_appsync_author_role` in your federation solution.

Q: What are the restrictions to using the AWS AppSync?

- When creating a Data Source on AppSync the customer need to specify the previously created service role, creation of a new role is not allowed and therefore will return an access denied
- AppSync roles are configured to restrict permissions to resources containing 'AMS-' or 'MC-' prefixes to prevent any modifications to AMS infrastructure.

Q: What are the prerequisites or dependencies to using AWS AppSync?

The service allows multiple other services to be used as a data source, The basic permissions to use them as such is included in the service role (`customer_appsync_service_role`), but you must manually select the service role when using the service.

AWS App Mesh

AWS App Mesh provides application level networking to make it easy for your services to communicate with each other across multiple types of compute infrastructure. App Mesh standardizes how your services communicate, giving you end-to-end visibility and ensuring high-availability for your applications.

AWS App Mesh makes it easy to run services by providing consistent visibility and network traffic controls for services built across multiple types of compute infrastructure. App Mesh removes the need to update application code to change how monitoring data is collected or traffic is routed between services. App Mesh configures each service to export monitoring data and implements consistent communications control logic across your application. This makes it easy to quickly pinpoint the exact location of errors and automatically re-route network traffic when there are failures or when code changes need to be deployed. To learn more, see AWS App Mesh.

AWS App Mesh in AMS FAQs

Common questions and answers:

Q: How do I request access AWS App Mesh in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_app_mesh_console_role`. After it is provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using the AWS App Mesh?

Full functionality of AWS App Mesh is available in your AMS account.

Q: What are the prerequisites or dependencies to using AWS App Mesh?

There are no prerequisites or dependencies to use AWS App Mesh in your AMS account.

AWS Audit Manager

Audit Manager helps you continuously audit your AWS usage to simplify how you assess risk and compliance with regulations and industry standards. Audit Manager automates evidence collection to make it easier to assess if your policies, procedures, and activities are operating effectively. When it is time for an audit, Audit Manager helps you manage stakeholder reviews of your controls and helps you build audit-ready reports with significantly less manual effort. To learn more, see Audit Manager.

AWS Audit Manager in AMS FAQs

Common questions and answers:

Q: How do I request access to AWS Audit Manager in my AMS account?

You can request access through the submission of the AWS Services RFC (Management | AWS Service | Compatible Service). Through this RFC the following IAM Role will be provisioned in your account: `customer-audit-manager-admin-Role`. Once provisioned in your account you must onboard the role in your federation solution.

Q: What are the restrictions to using AWS Audit Manager?

There are no restrictions for the use of AWS Audit Manager in your AMS account. Full functionality for AWS Audit Manager will be provided.

Q: What are the prerequisites or dependencies to using AWS Audit Manager?

1. You need to provide AMS with the s3 bucket where you want reports/assessments to reside.
2. If you want to have encryption with the service, you need to provide AMS with the KMS CMK ARN to use.
3. If you want to send an SNS notifications to a Topic, you must provide the name of the topic or arn.
4. **(Optional)** There is an additional prerequisite if you want to enable Organizations as part of your multi-account landing zone in Audit Manager and you want a delegated administrator account: In the description field for RFC (Management | AWS Service | Compatible Service| Add), mention that you want to use the delegated administrator account as part of Audit Manager Setup and provide the below details:
   - KMS CMK ARN (used to set up Audit Manager, initially)
   - Delegated administrator account ID for Audit Manager to use as part of this multi-account landing zone (can be a MALZ application account)

AWS Batch

AWS Batch enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS. AWS Batch dynamically provisions the optimal quantity and type of compute resources (such as CPU or memory optimized instances) based on the volume and specific resource requirements of the batch jobs submitted. With AWS Batch, there is no need to install and manage batch computing software or server clusters that you use to run your jobs, allowing you to focus on analyzing results and solving problems. To learn more, see AWS Batch.

AWS Batch in AMS FAQs

Common questions and answers:

Q: How do I request access to AWS Batch in my AMS account?

1. You can request access through the submission of the AWS Services RFC (Management | AWS Service | Compatible Service). Through this RFC, the following IAM roles and policies will be provisioned in your account:

IAM roles:

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`
- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer-ecs-task-role.json`

Policies:

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`
- `customer_batch_events_service_role_policy`

2. Once provisioned in your account, you must onboard the role `customer_batch_console_role` in your federation solution.

Q: What are the restrictions to using AWS Batch?

When creating the Compute Environment, you should tag EC2 instances as "customer_batch" or "customer-batch". If the instances are not tagged, instances will not be terminated by batch when the job completes.

Q: What are the prerequisites or dependencies to using AWS Batch?

There are no prerequisites or dependencies to use AWS Batch in your AMS account.

AWS Certificate Manager

AWS Certificate Manager (ACM) is a service that lets you provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks. AWS Certificate Manager removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates.

With AWS Certificate Manager, you can request a certificate, deploy it on ACM-integrated AWS resources, such as Elastic Load Balancers, Amazon CloudFront distributions, and APIs on API Gateway, and let AWS Certificate Manager handle certificate renewals. It also enables you to create private certificates for your internal resources and manage the certificate lifecycle centrally. Public and private certificates provisioned through AWS Certificate Manager for use with ACM-integrated services are free. You pay only for the AWS resources you create to run your application. With AWS Certificate Manager Private Certificate Authority, you pay monthly for the operation of the private Certificate Authority and for the private certificates you issue. To learn more, see AWS Certificate Manager - AWS Documentation.

ACM in AMS FAQs

Common questions and answers:

Q: How do I request access to AWS Certificate Manager in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_acm_create_role`. You can use this role to create and manage ACM certificates. After it's provisioned in your account, you must onboard the role in your federation solution.

ACM certificates can be created using the following change types, even if you haven't added the `customer_acm_create_role` IAM role:

- ACM certificate: creating
- ACM certificate: creating
- ACM: creating a private certificate

Q: What are the restrictions to using the AWS Certificate Manager?

You must submit a Request for Change (RFC) to AMS to delete or modify existing certificates, as those actions require full admin access (use the Management | Other | Other | Update change type (ct-0xdawir96cy7k). Note that the IAM policy can't exclude rights based on tag names (mc*, ams*, etc). Certificates do not incur a cost, so deleting unused certificates is not time sensitive.

Q: What are the prerequisites or dependencies to using Certificate Manager?

Existing public DNS name, and access to create DNS CNAME records, but those do not need to be hosted in the managed account.

AWS Certificate Manager Private Certificate Authority

Private certificates are used for identifying and securing communication between connected resources on private networks, such as servers, mobile, and IoT devices and applications. ACM Private CA is a managed private CA service that helps you easily and securely manage the lifecycle of your private certificates. ACM Private CA provides you a highly-available private CA service without the upfront investment and ongoing maintenance costs of operating your own private CA. ACM Private CA extends ACM's certificate management capabilities to private certificates, enabling you to create and manage public and private certificates centrally. You can easily create and deploy private certificates for your AWS resources using the AWS Management Console or the ACM API. For EC2 instances, containers, IoT devices, and on-premises resources, you can easily create and track private certificates and use your own client-side automation code to deploy them. You also have the flexibility to create private certificates and manage them yourself for applications that require custom certificate lifetimes, key algorithms, or resource names To learn more, see ACM Private CA.

ACM Private CA in AMS FAQs

Common questions and answers:

Q: How do I request access ACM Private CA in my AMS account?

Request access through the submission of the AWS Services RFC (Management | AWS Service | Compatible Service). Through this RFC the following IAM role will be provisioned in your account:

`customer_acm_pca_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using the ACM Private CA?

Currently, AWS Resource Access Manager (AWS RAM) cannot be used to share your ACM Private CA cross-account.

Q: What are the prerequisites or dependencies to using ACM Private CA?

1. If you plan to create a CRL, you need an S3 bucket to store it in. ACM Private CA automatically deposits the CRL in the Amazon S3 bucket you designate and updates it periodically. It is a pre requisite that the S3 bucket has the below bucket policy before you can set-up a CRL. In order to proceed with this request; create a RFC with ct-0fpjlxa808sh2 (Management | Advanced stack components | S3 storage | Update policy) as follows:

- Provide the S3 bucket name or ARN.
- Copy the below policy onto RFC and replace `bucket-name` with your desired S3 bucket name.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"acm-pca.amazonaws.com"
         },
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation"
         ],
         "Resource":[
            "arn:aws:s3:::bucket-name/*",
            "arn:aws:s3:::bucket-name"
         ]
      }
   ]
}
```

2. If the above S3 bucket is encrypted, then the Service Principal acm-pca.amazonaws.com requires permissions to decrypt. In order to proceed with this request; create a RFC with ct-3ovo7px2vsa6n (Management | Advanced stack components | KMS key | Update) as follows:

- Provide the KMS Key ARN on which the policy must be updated.
- Copy the below policy onto RFC and replace `bucket-name` with your desired S3 bucket name.

```
{
   "Sid":"Allow ACM-PCA use of the key",
   "Effect":"Allow",
   "Principal":{
      "Service":"acm-pca.amazonaws.com"
   },
   "Action":[
      "kms:GenerateDataKey",
      "kms:Decrypt"
   ],
   "Resource":"*",
```

```
   "Condition":{
      "StringLike":{
         "kms:EncryptionContext:aws:s3:arn":[
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
            "arn:aws:s3:::bucket_name/audit-report/*",
            "arn:aws:s3:::bucket_name/crl/*"
         ]
      }
   }
}
```

3. ACM Private CA CRLs don't support the S3 setting "Block public access to buckets and objects granted through new access control lists (ACLs)". You must disable this setting with the S3 account and bucket in order to allow the ACM Private CA to write CRLs as mentioned in How to securely create and store your CRL for ACM Private CA If you would like to disable, create a new RFC with ct-0xdawir96cy7k (Management | Other | Other | Update) and attach a Risk Acceptance. If you have any questions on risk acceptance, reach out to your Cloud Architect.

AWS CloudEndure

AWS CloudEndure migration simplifies, expedites, and automates large-scale migrations from physical, virtual, and cloud-based infrastructure to AWS. CloudEndure Disaster Recovery (DR) protects against downtime and data loss from any threat, including ransomware and server corruption.

AWS CloudEndure in AMS FAQs

Q: How do I request access to CloudEndure in my AMS account?

Request access to CloudEndure by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM User to your account: `customer_cloud_endure_user`. After it's provisioned in your account, the access key and secret key for the user is shared in AWS Secrets Manager.

These policies are provisioned to the account as well: `customer_cloud_endure_policy` and `customer_cloud_endure_deny_policy`.

Additionally, you must provide a Risk Acceptance as the CloudEndure DR solution for application integration has infrastructure-mutating permissions. To do this, work with your cloud service delivery manager (CSDM).

Q: What are the restrictions to using CloudEndure in my AMS account?

The cloud endure replication and conversion instances can be launched only in the subnet you indicate.

Q: What are the prerequisites or dependencies to using CloudEndure in my AMS account? Share the following via RFC bidirectional correspondence:

- VPC Subnet details for Replication and Conversion instances to be launched.
- The KMS Key Amazon Resource Name (ARN) if the EBS volumes are encrypted.

AWS CloudHSM

The AWS CloudHSM service helps you meet corporate, contractual, and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within

the AWS cloud. AWS, and AWS Marketplace partners, offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. AWS CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are designed and validated to government standards for secure key management. AWS CloudHSM allows you to securely generate, store, and manage cryptographic keys used for data encryption in a way that keys are accessible only by you. To learn more, see AWS CloudHSM.

AWS CloudHSM in AMS FAQs

Common questions and answers:

Q: How do I request access to AWS CloudHSM in my AMS account?

Utilization of in your AMS account is a two-step process:

1. Request an AWS CloudHSM cluster. Do this by submitting an RFC with the Management | Other | Other | Create (ct-1e1xtak34nx76) change type. Include the following details:
   - AWS Region.
   - VPC ID/ARN. Provide a VPC ID/VPC ARN that is in the same account as the RFC that you submit.
   - Specify at least two Availability Zones for the cluster.
   - Amazon EC2 instance ID that will connect to the HSM cluster.
2. Access the AWS CloudHSM console. Do this by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_cloudhsm_console_role`.

After the role is provisioned in your account, you must onboard it in your federation solution.

Q: What are the restrictions to using AWS CloudHSM in my AMS account?

Access to the AWS CloudHSM console doesn't provide you with the ability to create, terminate or restore your cluster. To do those things, submit a Management | Other | Other | Create change type (ct-1e1xtak34nx76) change type.

Q: What are the prerequisites or dependencies to using AWS CloudHSM in my AMS account?

You must allow TCP traffic using port 2225 through a client Amazon EC2 instance within a VPC, or use Direct Connect VPN for on-premise servers that want access to the HSM cluster. AWS CloudHSM is dependent on Amazon EC2 for security groups and network interfaces. For log monitoring or auditing, HSM relies on CloudTrail (AWS API operations) and CloudWatch Logs for all local HSM device activity.

Q: Who will apply updates to the AWS CloudHSM client and related software libraries?

You are responsible for applying the library and client updates. You'll want to monitor the CloudHSM version history page for releases, and then apply updates using the CloudHSM client upgrade.

> **Note**
> Software patches for the HSM appliance are always automatically applied by the AWS CloudHSM service.

AWS CodeBuild

AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. With CodeBuild, you don’t need to provision, manage, and scale your own build servers. CodeBuild scales continuously and processes multiple

builds concurrently, so your builds are not left waiting in a queue. You can get started quickly by using prepackaged build environments, or you can create custom build environments that use your own build tools. With CodeBuild, you are charged by the minute for the compute resources you use. To learn more, see AWS CodeBuild.

> **Note**
> To onboard CodeCommit, CodeBuild, CodeDeploy, and CodePipeline with a single federated role see AMS CodeSuite (p. 208).

CodeBuild in AMS FAQs

Common questions and answers:

Q: How do I request access to AWS CodeBuild in my AMS account?

Utilization of AWS CodeBuild in your AMS account is a two-step process:

1. Provision the `CodeBuild Service Role` for build process to coordinate with AWS S3 buckets, Amazon CloudWatch and Log groups
2. Request access to the CodeBuild console

You can request that both be set up in your AMS account by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using AWS CodeBuild in my AMS account?

For AWS CodeBuild console administrator access, permissions are limited at resource level; for example, CloudWatch actions are limited on specific resources and the `iam:PassRole` permission is controlled.

Q: What are the prerequisites or dependencies to using CodeBuild in my AMS account?

If additional IAM permissions are required for the defined AWS CodeBuild service role, request them through an AMS service request.

AWS CodeCommit

AWS CodeCommit is a fully managed source control service that hosts secure Git-based repositories. It helps teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. You can use CodeCommit to securely store anything from source code to binaries, and it works seamlessly with your existing Git tools. To learn more, see AWS CodeCommit.

> **Note**
> To onboard CodeCommit, CodeBuild, CodeDeploy, and CodePipeline with a single federated role, see AMS CodeSuite (p. 208).

CodeCommit in AMS FAQs

Q: How do I request access to CodeCommit in my AMS account?

AWS CodeCommit console and data access roles can be requested through the submission of two AWS Service RFCs, console access, and data access:

- Request access to AWS CodeCommit by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role

to your account: `customer_codecommit_console_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Data access (such as Training and Entity Lists) require separate CTs for each data source specifying the S3 data source (mandatory), output bucket (mandatory) and KMS (optional). There are no limitations to AWS CodeCommit job creation as long as all data sources have been granted access roles. To request data access, submit an RFC with the Management | Other | Other | Create (ct-1e1xtak34nx76).

Q: What are the restrictions to using AWS CodeCommit in my AMS account?

Triggers feature on CodeCommit are disabled given the associated rights to create SNS topics. Directly authenticating against CodeCommit is restricted, users should authenticate with Credential Helper. Some KMS commands are also restricted: `kms:Encrypt`, `kms:Decrypt`, `kms:ReEncrypt`, `kms:GenereteDataKey`, `kms:GenerateDataKeyWithoutPlaintext`, and `kms:DescribeKey`.

Q: What are the prerequisites or dependencies to using AWS CodeCommit in my AMS account?

If S3 buckets are encrypted with KMS keys, S3 and KMS are required to use AWS CodeCommit.

AWS CodeDeploy

AWS CodeDeploy is a fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers. AWS CodeDeploy helps you to rapidly release new features, helps you avoid downtime during application deployment, and handles the complexity of updating your applications. You can use AWS CodeDeploy to automate software deployments, eliminating the need for error-prone manual operations. The service scales to match your deployment needs. To learn more, see AWS CodeDeploy.

Note
To onboard CodeCommit, CodeBuild, CodeDeploy, and CodePipeline with a single federated role, see AMS CodeSuite (p. 208).

CodeDeploy in AMS FAQs

Q: How do I request access to CodeDeploy in my AMS account?

Request access to CodeDeploy by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_codedeploy_console_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using CodeDeploy in my AMS account?

Currently we are only supporting Compute Platform as — Amazon EC2/On-premises.

Q: What are the prerequisites or dependencies to using CodeDeploy in my AMS account?

There are no prerequisites or dependencies to use CodeDeploy in your AMS account.

AWS CodePipeline

AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates. CodePipeline automates the build, test, and deploy phases of your release process every time there is a code change, based on the release model you define. This enables you to rapidly and reliably deliver features and updates. You can

easily integrate AWS CodePipeline with third-party services such as GitHub or with your own custom plugin. With AWS CodePipeline, you only pay for what you use. There are no upfront fees or long-term commitments. To learn more, see AWS CodePipeline.

> **Note**
> To onboard CodeCommit, CodeBuild, CodeDeploy, and CodePipeline with a single federated role, see AMS CodeSuite (p. 208).
> CodePipeline in AMS does not support "Amazon CloudWatch Events" for Source Stage because it needs elevated permissions to create the service role and policy, which bypasses the least-privileges model and AMS change management process.

CodePipeline in AMS FAQs

Q: How do I request access to CodePipeline in my AMS account?

Request access to CodePipeline by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_code_pipeline_console_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

At this time, AMS Operations will also deploy this service role in your account: `aws_code_pipeline_service_role_policy`.

Q: What are the restrictions to using CodePipeline in my AMS account?

Yes. CodePipeline features, stages, and providers are limited to the following:

1. Deploy Stage: Limited to Amazon S3, and AWS CodeDeploy
2. Source Stage: Limited to Amazon S3, AWS CodeCommit, BitBucket, and GitHub
3. Build Stage: Limited to AWS CodeBuild, and Jenkins
4. Approval Stage: Limited to Amazon SNS
5. Test Stage: Limited to AWS CodeBuild, Jenkins, BlazeMeter, Ghost Inspector UI Testing, Micro Focus StormRunner Load, and Runscope API Monitoring
6. Invoke Stage: Limited to Step Functions, and Lambda

> **Note**
> AMS Operations will deploy `customer_code_pipeline_lambda_policy` in your account; it must be attached with the Lambda execution role for Lambda invoke stage. Please provide the Lambda service/execution role name that you want this policy added with. If there is no custom Lambda service/execution role, AMS will create a new role named `customer_code_pipeline_lambda_execution_role`, which will be a copy of `customer_lambda_basic_execution_role` along with `customer_code_pipeline_lambda_policy`.

Q: What are the prerequisites or dependencies to using CodePipeline in my AMS account?

AWS supported services AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy must be launched prior to, or along with, the launch of CodePipeline.

AWS Compute Optimizer

AWS Compute Optimizer recommends optimal AWS Compute resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics. Over-provisioning compute (Amazon EC2 and ASGs) can lead to unnecessary infrastructure cost and under-provisioning compute can lead to poor application performance. Compute Optimizer helps you choose

the optimal Amazon EC2 instance types, including those that are part of an Amazon EC2 Auto Scaling group, based on your utilization data. To learn more, see AWS Compute Optimizer.

Compute Optimizer in AMS FAQs

Q: How do I request access to Compute Optimizer in my AMS account?

Request access to Compute Optimizer by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_compute_optimizer_readonly_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Compute Optimizer in my AMS account?

There are no restrictions. Full functionality of AWS Compute Optimizer is available in your AMS account.

Q: What are the prerequisites or dependencies to using Compute Optimizer in my AMS account?

- You must submit an RFC (Management | Other | Other | Update) authorizing AMS Ops to enable the service in the account. During deployment, a service linked role (SLR) is created to allow metrics gathering and report generation. The SLR is labeled "AWSServiceRoleForComputeOptimizer". For more information, see Using Service-Linked Roles for AWS Compute Optimizer
- CloudWatch metrics must be enabled for the following metrics:
  - **CPU utilization**: The percentage of allocated Amazon EC2 compute units that are in use on the instance. This metric identifies the processing power required to run an application upon a selected instance.
  - **Memory utilization**: The amount of memory that has been used in some way during the sample period. This metric identifies the memory required to run an application upon a selected instance. Memory utilization is analyzed only for resources that have the unified CloudWatch agent installed on them. For more information, see Enabling Memory Utilization with the CloudWatch Agent (p. 10).
  - **Network in**: The number of bytes received on all network interfaces by the instance. This metric identifies the volume of incoming network traffic to a single instance.
  - **Network out**: The number of bytes sent out on all network interfaces by the instance. This metric identifies the volume of outgoing network traffic from a single instance.
  - **Local disk input/output (I/O)**: The number of input/output operations for the local disk. This metric identifies the performance of the root volume of an instance

AWS DataSync

AWS DataSync moves large amounts of data online between on-premises storage and Amazon S3, Amazon Elastic File System (Amazon Elastic File System) or Amazon FSx. Manual tasks related to data transfers can slow down migrations and burden IT operations. DataSync eliminates or automatically handles many of these tasks, including scripting copy jobs, scheduling and monitoring transfers, validating data, and optimizing network utilization. The DataSync software agent connects to your Network File System (NFS) and Server Message Block (SMB) storage, so you don't have to modify your applications. DataSync can transfer hundreds of terabytes and millions of files at speeds up to 10 times faster than open-source tools, over the internet or AWS Direct Connect links. You can use DataSync to migrate active data sets or archives to AWS, transfer data to the cloud for timely analysis and processing, or replicate data to AWS for business continuity.

To learn more, see AWS DataSync.

DataSync in AMS FAQs

Q: How do I request access to DataSync in my AMS account?

Request access to DataSync by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_datasync_console_role`.

Once provisioned in your account, you must onboard the roles in your federation solution.

The CloudWatch log group to use in order to stream task logs is "/aws/datasync".

Q: What are the restrictions to using DataSync in my AMS account?

Full functionality of AWS DataSync is available in your AMS account.

Q: What are the prerequisites or dependencies to using DataSync in my AMS account?

- S3 ARNs (Amazon Resource Names) are required for all S3 buckets associated with DataSync tasks that will be performed using the DataSync service role. All bucket names must have the prefix `datasync-`, as these are the only buckets the DataSync service-linked role (`customer_datasync_service_role`) will be able to access.
- VPC Endpoints and security groups for DataSync agents must be requested with an RFC with the Management | Other | Other | Create (ct-1e1xtak34nx76) change type prior to using VPC Endpoints.
- AWS DataSync agents run in AMS as an appliance. The AWS DataSync agent is patched and updated by the service; for details, see AWS DataSync FAQs. To launch an agent, submit an RFC with the Management | Other | Other | Create (ct-1e1xtak34nx76) change type requesting the AWS DataSync agent be deployed. Provide the AWS DataSync Amazon EC2 AMI ID, instance type, subnet, security group, and either reference an existing Amazon EC2 keypair or request the creation of a new keypair.

AWS Elemental MediaConvert

AWS Elemental MediaConvert is a file-based video transcoding service with broadcast-grade features. It enables you to create video-on-demand (VOD) content for broadcast and multiscreen delivery at scale. The service combines advanced video and audio capabilities with a simple web services interface and pay-as-you-go pricing. With AWS Elemental MediaConvert, you can focus on delivering compelling media experiences without having to worry about the complexity of building and operating your own video processing infrastructure.

To learn more, see AWS Elemental MediaConvert.

MediaConvert in AMS FAQs

Q: How do I request access to MediaConvert in my AMS account?

Request access to MediaConvert by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_mediaconvert_author_role`. Once provisioned in your account, you must onboard the role in your federation solution.

A second role will be provided, `customer_MediaConvert_Default_Role`, that is used by MediaConvert in order to read from the source S3 bucket and write the output to the destination S3 bucket, and also to invoke the API gateway in case you need digital rights management (DRM).

Q: What are the restrictions to using MediaConvert in my AMS account?

There are no restrictions for the use of MediaConvert in AMS.

Q: What are the prerequisites or dependencies to using MediaConvert in my AMS account?

There are no prerequisites or dependencies to use MediaConvert in your AMS account.

AWS Elemental MediaLive

AWS Elemental MediaLive is a broadcast-grade live video processing service. It enables you to create high-quality video streams for delivery to broadcast televisions and internet-connected multiscreen devices, like connected TVs, tablets, smartphones, and set-top boxes. The service works by encoding your live video streams in real-time, taking a larger-sized live video source and compressing it into smaller versions for distribution to your viewers. With AWS Elemental MediaLive, you can easily set up streams for both live events and 24x7 channels with advanced broadcasting features, high availability, and pay-as-you-go pricing. AWS Elemental MediaLive lets you focus on creating compelling live video experiences for your viewers without the complexity of building and operating broadcast-grade video processing infrastructure.

To learn more, see AWS Elemental MediaLive.

MediaLive in AMS FAQs

Q: How do I request access to MediaLive in my AMS account?

Request access to MediaLive by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_medialive_author_role`.

As a part of this RFC, a second role is deployed into your account; `customer_medialive_service_role` role, this role can be assigned to your Media Live channels and inputs to interact with other services such as Amazon S3, MediaStore, and CloudWatch Logs.

After the roles are provisioned in your account, you must onboard the roles in your federation solution.

Q: What are the restrictions to using MediaLive in my AMS account?

There are no restrictions for the use of MediaLive in AMS.

Q: What are the prerequisites or dependencies to using MediaLive in my AMS account?

There are no prerequisites or dependencies to use MediaLive in your AMS account.

AWS Elemental MediaPackage

AWS Elemental MediaPackage reliably prepares and protects your video for delivery over the internet. From a single video input, AWS Elemental MediaPackage creates video streams formatted to play on connected TVs, mobile phones, computers, tablets, and game consoles. It makes it easy to implement popular video features for viewers (start-over, pause, rewind, and so on.), like those commonly found on DVRs. AWS Elemental MediaPackage can also protect your content using Digital Rights Management (DRM). AWS Elemental MediaPackage scales automatically in response to load, so your viewers will always get a great experience without you having to accurately predict in advance the capacity you'll need.

To learn more, see AWS Elemental MediaPackage.

MediaPackage in AMS FAQs

Q: How do I request access to AWS Elemental MediaPackage in my AMS account?

Request access to MediaPackage by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to

your account: `customer_mediapackage_author_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

A second role will be provided, `customer_mediapackage_service_role`, that can be assigned to your Media Live channels and inputs to interact with other services such as S3 and Secrets Manager.

Q: What are the restrictions to using MediaPackage in my AMS account?

There are no restrictions for the use of MediaPackage in AMS.

Q: What are the prerequisites or dependencies to using MediaPackage in my AMS account?

There are no prerequisites or dependencies to use MediaPackage in your AMS account.

AWS Elemental MediaStore

AWS Elemental MediaStore is an AWS storage service optimized for media. It gives you the performance, consistency, and low latency required to deliver live streaming video content. AWS Elemental MediaStore acts as the origin store in your video workflow. Its high performance capabilities meet the needs of the most demanding media delivery workloads, combined with long-term, cost-effective storage. To learn more, see AWS Elemental MediaStore.

MediaStore in AMS FAQs

Q: How do I request access to MediaStore in my AMS account?

Request access to MediaStore by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_mediastore_author_role`. As a part of this RFC, a second role is deployed into your account; `MediaStoreAccessLogs` role, which is used by the MediaStore service to log activity in CloudWatch, if you choose to enable that feature. After it's provisioned in your account, you must onboard the roles in your federation solution.

At this time, AMS Operations will also deploy this service role in your account: `aws_code_pipeline_service_role_policy`.

Q: What are the restrictions to using MediaStore in my AMS account?

There are no restrictions for the use of MediaStore in AMS.

Q: What are the prerequisites or dependencies to using MediaStore in my AMS account?

There are no prerequisites or dependencies to use MediaStore in your AMS account.

AWS Elemental MediaTailor

AWS Elemental MediaTailor lets video providers insert individually targeted advertising into their video streams without sacrificing broadcast-level quality-of-service. With AWS Elemental MediaTailor, viewers of your live or on-demand video each receive a stream that combines your content with ads personalized to them. But unlike other personalized ad solutions, with AWS Elemental MediaTailor your entire stream – video and ads – is delivered with broadcast-grade video quality to improve the experience for your viewers. AWS Elemental MediaTailor delivers automated reporting based on both client and server-side ad delivery metrics, to accurately measure advertising impressions and viewer behavior. You can easily monetize unexpected high-demand viewing events with no up-front costs using AWS Elemental MediaTailor. It also improves ad delivery rates, helping you make more money from every video, and it works with a wider variety of content delivery networks, ad decision servers, and client devices.

To learn more, see AWS Elemental MediaTailor.

MediaTailor in AMS FAQs

Q: How do I request access to MediaTailor in my AMS account?

Request access to MediaTailor by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer-mediatailor-role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using MediaTailor in my AMS account?

There are no restrictions for the use of MediaTailor in AMS.

Q: What are the prerequisites or dependencies to using MediaTailor in my AMS account?

There are no prerequisites or dependencies to use MediaTailor in your AMS account.

AWS Global Accelerator

Global Accelerator is a network layer service in which you create accelerators to improve availability and performance for internet applications used by a global audience. To learn more, see Global Accelerator.

Global Accelerator in AMS FAQs

Common questions and answers:

Q: How do I request Global Accelerator to be set up in my AMS account?

Request access through the submission of the AWS Services RFC (Management | AWS Service | Self-provisioned Service). Through this RFC, the following IAM roles will be provisioned in your account: `customer_global_accelerator_console_role`. Once provisioned in your account you must onboard the console role in your federation solution.

Q: What are the restrictions to using Global Accelerator in my AMS account?

Global Accelerator is a global service that supports endpoints in multiple AWS Regions, which are listed in the AWS Region Table.

Q: What are the prerequisites or dependencies to using Global Accelerator in my AMS account?

When you set up your accelerator with Global Accelerator, you associate the static IP addresses to regional endpoints in one or more AWS Regions. For standard accelerators, the endpoints are Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses. For custom routing accelerators, endpoints are virtual private cloud (VPC) subnets with one or more EC2 instances.

AWS Glue

AWS Glue is a fully managed extract, transform, and load (ETL) service that helps you to prepare and load your data for analytics. You can create and run an ETL job with a few clicks in the AWS Management Console. You point AWS Glue to your data stored on AWS, and AWS Glue discovers your data and stores the associated metadata (e.g. table definition and schema) in the AWS Glue Data Catalog. Once cataloged, your data is immediately searchable, queryable, and available for ETL actions. To learn more, see AWS Glue.

AWS Glue in AMS FAQs

Common questions and answers:

Q: How do I request AWS Glue to be set up in my AMS account?

Request access to AWS Glue by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_glue_console_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

For access to Crawlers, Jobs, and Development endpoints (roles needed for specific use cases), submit an RFC with the Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entity or policy (ct-3dpd8mdd9jn1r).

Q: What are the restrictions to using AWS Glue in my AMS account?

There are no restrictions. Full functionality of AWS Glue is available in your AMS account with the exception of Notebooks. AWS Glue Notebooks are a non-managed resource that launches Amazon EC2 instances in an account. AMS recommends that you launch your own Amazon EC2 instances and install the software necessary to support a notebook environment and development. For more information, see Tutorial: Set Up a Local Apache Zeppelin Notebook to Test and Debug ETL Scripts and Using Development Endpoints for Developing Scripts.

Q: What are the prerequisites or dependencies to using AWS Glue in my AMS account?

AWS Glue has a dependency on Amazon S3, CloudWatch, and CloudWatch Logs. Transitive dependencies vary based on data sources, and other AWS Glue service features may be interacting with (example: Amazon Redshift, Amazon RDS, Athena).

AWS Lake Formation

AWS Lake Formation is a service that makes it easy to set up a secure data lake in days. A data lake is a centralized, curated, and secured repository that stores all your data, both in its original form and prepared for analysis. A data lake enables you to break down data silos and combine different types of analytics to gain insights and guide better business decisions.

Creating a data lake with Lake Formation is as simple as defining data sources and what data access and security policies you want to apply. Lake Formation then helps you collect and catalog data from databases and object storage, move the data into your new Amazon S3 data lake, clean and classify your data using machine learning algorithms, and secure access to your sensitive data. Your users can access a centralized data catalog (for details, see AWS Glue FAQs) that describes available data sets and their appropriate usage. Your users then leverage these data sets with their choice of analytics and machine learning services, like Amazon Redshift, Amazon Athena, and (in beta) Amazon EMR for Apache Spark. Lake Formation builds on the capabilities available in AWS Glue.

To learn more, see AWS Lake Formation.

Lake Formation in AMS FAQs

Q: How do I request access to AWS Lake Formation in my AMS account?

Request access to Lake Formation by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_lakeformation_data_analyst_role`. After it's provisioned in your account, you must onboard the roles in your federation solution.

Q: What are the restrictions to using AWS Lake Formation in my AMS account?

Full functionality of Lake Formation is available in AMS.

Q: What are the prerequisites or dependencies to using AWS Lake Formation in my AMS account?

Lake Formation integrates with the AWS Glue service, therefore AWS Glue users can access only the databases and tables on which they have Lake Formation permissions. Additionally AWS Athena and Amazon Redshift users can only query the AWS Glue databases and tables on which they have Lake Formation permissions.

AWS Lambda

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume, there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or back-end service, all with zero administration. upload your code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services, or call it directly from any Web or mobile app. To learn more, see AWS Lambda.

Lambda in AMS FAQs

Q: How do I request access to AWS Lambda in my AMS account?

Request access to Lambda by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM roles to your account: `customer_lambda_admin_role` and `customer_lambda_basic_execution_role`. After it's provisioned in your account, you must onboard the roles in your federation solution.

Q: What are the restrictions to using AWS Lambda in my AMS account?

- A Lambda function is designed to be invoked by event sources. For a list of services that can be used as a Lambda event source, see Using AWS Lambda with Other Services. Not all of these services are currently available in AMS accounts. If you require a service that is not available, work with your AMS CSDM to file an exception.
- By default AMS will provide you with a basic Lambda initiation role containing the `AWSLambdaBasicExecutionRole` and `AWSXrayWriteOnlyAccess` permissions; for information, see AWS Lambda Initiation Role. If you require additional permissions, such as the ability to provision Lambda functions within your AMS VPC, submit an RFC with the Management | Other | Other | Create (ct-1e1xtak34nx76).

Q: What are the prerequisites or dependencies to using AWS Lambda in my AMS account?

There are no prerequisites or dependencies to get started with AWS Lambda; however, depending on your specific use case, you may require access to other AWS services in order to create event sources, or additional permissions for your function to perform various actions. If additional permissions are needed, submit an RFC with the Management | Other | Other | Create (ct-1e1xtak34nx76).

AWS License Manager

AWS License Manager integrates with AWS services to simplify the management of licenses across multiple AWS accounts, IT catalogs, and on-premises, through a single AWS account. AWS License Manager lets administrators create customized licensing rules that emulate the terms of their licensing

agreements, and then enforces these rules when an instance of Amazon EC2 gets launched. The rules in AWS License Manager enable you to limit a licensing breach by physically stopping the instance from launching or by notifying administrators about the infringement. To learn more, see AWS License Manager.

License Manager in AMS FAQs

Common questions and answers:

Q: How do I request AWS License Manager to be set up in my AMS account?

Request access to AWS License Manager by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_license_manager_role`. Once the License Manager IAM role is provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using AWS License Manager in my AMS account?

You're able to associate AWS License Manager rules to the AMIs you own (filtered under "Owned by me"). If you choose to enforce a limit association to an AMI (example: can only support 100 vCPU of this AMI) and exhaust the limit, future launches with that AMI are blocked and return an error stating "No licenses available." This is the intended behavior of this service (not allowing license exhaustion). In the event you exhaust the limit but need to launch the AMI again, you must modify the rule configured in AWS License Manager.

Q: What are the prerequisites or dependencies to using AWS License Manager in my AMS account?

There are no prerequisites or dependencies to use AWS License Manager in your AMS account.

AWS Migration Hub

AWS Migration Hub provides a single location where you can track the progress of application migrations across multiple AWS and partner solutions. Using Migration Hub allows you to choose the AWS and partner migration tools that best fit your needs, while providing visibility into the status of migrations across your application portfolio. Migration Hub also provides key metrics and progress for individual applications, regardless of which tools are being used to migrate them. This allows you to quickly get progress updates across all of your migrations, easily identify and troubleshoot any issues, and reduce the overall time and effort spent on your migration projects. To learn more, see AWS Migration Hub.

Migration Hub in AMS FAQs

Common questions and answers:

Q: How do I request access to Migration Hub in my AMS account?

Request access to Migration Hub by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer-migrationhub-author-role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions for Migration Hub?

AMS does not currently support AWS Server Migration Service (AWS SMS); therefore, the Migration Hub features that enable migration of servers using AWS SMS do not work on AMS at this time.

Q: What are the prerequisites to enable Migration Hub?

There are no prerequisites to start using Migration Hub in your AMS account. However, permissions outside Migration Hub might be required during the management of the service, such as writing permissions to Amazon S3 to upload server information.

AWS Outposts

AWS Outposts is a fully managed service that extends AWS infrastructure, AWS services, APIs, and tools to virtually any datacenter, co-location space, or on-premises facility for a consistent hybrid experience. AWS Outposts is good for workloads that require low latency access to on-premises systems, local data processing, or local data storage. To learn more, see AWS Outposts.

AWS Outposts in AMS FAQs

Common questions and answers:

Q: How do I request AWS Outposts to be set up in my AMS account?

Request access to AWS Outposts by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_outposts_role`. Once the role is provisioned in your account, you must onboard it in your federation solution.

Q: What are the restrictions to using AWS Outposts in my AMS account?

There are no restrictions for the use of AWS Outposts in your AMS account.

Q: What are the prerequisites or dependencies to using AWS Outposts in my AMS account?

There are no prerequisites or dependencies to use AWS Outposts in your AMS account.

AWS Secrets Manager

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to the Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text. Secrets Manager offers secret rotation with built-in integration for Amazon RDS, Amazon Redshift, and Amazon DocumentDB. Also, the service is extensible to other types of secrets, including API keys and OAuth tokens. To learn more, see AWS Secrets Manager.

> **Note**
> By default, AMS operators can access secrets in AWS Secrets Manager that are encrypted using the account's default AWS KMS key (CMK). If you want your secrets to be inaccessible to AMS Operations, use a custom CMK, with an AWS Key Management Service (AWS KMS) key policy that defines permissions appropriate to the data stored in the secret.

Secrets Manager in AMS FAQs

Q: How do I request access to AWS Secrets Manager in my AMS account?

Request access to Secrets Manager by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM roles to your account: `customer_secrets_manager_console_role` and `customer-rotate-secrets-lambda-role`. The `customer_secrets_manager_console_role` is used as an Admin role to

provision and manage the secrets, and `customer-rotate-secrets-lambda-role` is used as the Lambda execution role for the Lambda functions that rotate the secrets. After it's provisioned in your account, you must onboard the `customer_secrets_manager_console_role` role in your federation solution.

Q: What are the restrictions to using AWS Secrets Manager in my AMS account?

Full functionality of AWS Secrets Manager is available in your AMS account, along with automatic rotation functionality of secrets. However, note that setting up your rotation using 'Create a new Lambda function to perform rotation' is not supported because it requires elevated permissions to create the AWS CloudFormation stack (IAM Role and Lambda function creation), which bypasses the Change Management process. AMS Advanced only supports 'Use an existing Lambda function to perform rotation' where you manage your Lambda functions to rotate secrets using the AWS Lambda SSPS Admin role. AMS Advanced doesn't create or manage Lambda to rotate the secrets.

Q: What are the prerequisites or dependencies to using AWS Secrets Manager in my AMS account?

The following namespaces are reserved for use by AMS and are unavailable as part of direct access to AWS Secrets Manager:

- arn:aws:secretsmanager:*:*:secret:ams-shared/*
- arn:aws:secretsmanager:*:*:secret:customer-shared/*
- arn:aws:secretsmanager:*:*:secret:ams/*

AWS Security Hub

AWS Security Hub provides you with a comprehensive view of your security state within AWS and your compliance with security industry standards and best practices. Security Hub centralizes and prioritizes security and compliance findings from across AWS accounts, services, and supported third-party partners to help you analyze your security trends and identify the highest priority security issues. To learn more, see AWS Security Hub.

Security Hub in AMS FAQs

Q: How do I request access to AWS Security Hub in my AMS account?

Request access to Security Hub by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_securityhub_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using Security Hub in my AMS account?

Archiving functionality has been noted as a potential security and operational risk and has been restricted as a part of the self-provisioned service Security role.

Q: What are the prerequisites or dependencies to using AWS Security Hub in my AMS account?

There are no prerequisites or dependencies to use AWS Security Hub in your AMS account.

AWS Shield

AWS Shield Advanced is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. Shield Advanced provides always-on detection and automatic

inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield - Standard and Advanced; AMS offers Shield Advanced. To learn more, see Shield Advanced.

All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring, network and transport layer DDoS attacks that target your website or applications. When you use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, you receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

For higher levels of protection against attacks targeting your applications running on Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Amazon Route 53 resources, you can subscribe to AWS Shield Advanced.

In addition to the network and transport layer protections that come with AWS Shield Standard, AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall. AWS Shield Advanced also gives you 24x7 access to the AWS Shield Response Team (SRT) and protection against DDoS related spikes in your Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (Elastic Load Balancing), Amazon CloudFront, AWS Global Accelerator, and Amazon Route 53 charges.

Shield Advanced in AMS FAQs

Q: How do I request access to Shield Advanced in my AMS account?

Request access to Shield Advanced by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM roles to your account: `customer_shield_role` and `aws_drt_shield_role`. Once provisioned in your account, you must onboard the roles in your federation solution.

After the roles are deployed into your account, you can use the `customer_shield_role` to confirm your subscription to AWS Shield Advanced in your account.

> **Note**
> Note that there is a monthly fee and a one-year commitment associated with the use of AWS Shield Advanced. Additionally, using AWS Shield Advanced in AMS authorizes AMS to escalate to the AWS Shield (SRT), who may make changes to your web application firewall (AWS WAF) rules during escalated distributed denial of service (DDoS) incidents. These changes will be made in coordination with AMS.

Q: What are the restrictions to using Shield Advanced in my AMS account?

Although not a restriction, you should understand that using Shield Advanced deploys the `aws_drt_shield_role`, which allows AWS Shield teams (SRT) to make emergency changes to AWS WAF rules inside of AMS accounts during escalated DDoS incidents. This is recommended by AMS for the fastest remediation of DDoS attacks, and would occur after an AMS escalation to the SRT.

Q: What are the prerequisites or dependencies to using Shield Advanced in my AMS account?

There are no prerequisites or dependencies to use Shield Advanced in your AMS account.

AWS Snowball

Snowball is a petabyte-scale data transport solution that uses devices designed to be secure, to transfer large amounts of data into and out of the AWS Cloud. Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. You can use Snowball to migrate analytics data, genomics data, video libraries, image repositories, backups,

and to archive part of data center shutdowns, tape replacement or application migration projects. Transferring data with Snowball is simple, fast, more secure, and can be as little as one-fifth the cost of transferring data by way of high-speed Internet.

With Snowball, you don't need to write any code or purchase any hardware to transfer your data. Start by using the AWS Management Console to Create an Import Job for Snowball, and a Snowball device will be automatically shipped to you. Once it arrives, attach the device to your local network, download and run the Snowball Client ("Client") to establish a connection, and then use the Client to select the file directories that you want to transfer to the device. The Client then encrypts and transfers the files to the device at high speed. Once the transfer is complete and the device is ready to be returned, the E Ink shipping label automatically updates and you can track the job status with Amazon Simple Notification Service (Amazon SNS), text messages, or directly in the Console. To learn more, see AWS Snowball.

Snowball in AMS FAQs

Common questions and answers:

Q: How do I request access to AWS Snowball in my AMS account?

Implementation of Snowball in AMS is a two-step process:

1. Submit a Management | Other | Other | Create (ct-1e1xtak34nx76) change type and request a service role for Snowball for your AMS Account.
2. Request user access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_snowball_console_role`, `customer_snowball_export_role`, and `customer_snowball_import_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using AWS Snowball in my AMS Account?

Full functionality of the AWS Snowball is available in your AMS account.

Q: What are the prerequisites or dependencies to using AWS Snowball in my AMS account?

You must have the service role account as noted above.

AWS Step Functions

AWS Step Functions is a Web service that enables you to coordinate the components of distributed applications and microservices by using visual workflows. You build applications from individual components that each perform a discrete function, or task, allowing you to scale and change applications quickly. Step Functions provides a reliable way to coordinate components and step through the functions of your application. Step Functions offers a graphical console to visualize the components of your application as a series of steps. It automatically triggers and tracks each step, and retries when there are errors, so your application runs in order and as expected, every time. Step Functions logs the state of each step, so when things do go wrong, you can diagnose and debug problems quickly. To learn more, see AWS Step Functions.

Step Functions in AMS FAQs

Common questions and answers:

Q: How do I request access to AWS Step Functions in my AMS account?

Request access to AWS Step Functions by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_step_functions_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using AWS Step Functions in my AMS account?

Full functionality of the AWS Step Functions is available in your AMS account.

Q: What are the prerequisites or dependencies to using AWS Step Functions in my AMS account?

At runtime, the role used by Step Functions must have access to the services used by the step function. For example, a step function could depend on Lambda functions. Someone authoring a step function is likely to be creating Lambda functions at the same time and would have to request access to that service as well.

AWS Systems Manager Parameter Store

AWS Systems Manager Parameter Store provides secure, hierarchical storage for configuration data management and secrets management. You can store data such as passwords, database strings, and license codes as parameter values. You can store values as plain text or encrypted data. You can then reference values by using the unique name that you specified when you created the parameter. Highly scalable, available, and durable, Parameter Store is backed by the AWS Cloud. To learn more, see AWS Systems Manager Parameter Store.

> **Note**
> If you want a dedicated secrets store with lifecycle management, use AWS Secrets Manager (p. 229) instead of Parameter Store. Secrets Manager helps you meet your security and compliance requirements by enabling you to rotate secrets automatically. Secrets Manager offers built-in integration for MySQL, PostgreSQL, and Amazon Aurora on Amazon RDS, that's extensible to other types of secrets by customizing Lambda functions.

AWS Systems Manager Parameter Store in AMS FAQs

Common questions and answers:

Q: How do I request access to Systems Manager Parameter Store in my AMS account?

Request access to AWS Systems Manager Parameter Store by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_systemsmanager_parameterstore_console_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using AWS Systems Manager Parameter Store in my AMS account?

You are required to use AWS Managed keys; access is restricted from creating custom KMS keys. However, if a custom key is required, submit an RFC to create a customer-managed key (CMK) using the Deployment | Advanced Stack Components | KMS Key | Create change type (ct-1d84keiri1jhg) with this IAM role, `customer_systemsmanager_parameterstore_console_role` as the value for the `IAMPrincipalsRequiringDecryptPermissions` and `IAMPrincipalsRequiringEncryptPermissionsPrincipal` parameters. After the KMS Key is created, you can create a Secure String using it.

Q: What are the prerequisites or dependencies to using AWS Systems Manager Parameter Store in my AMS account?

There are no prerequisites; however, SSM Parameter Store is dependent on KMS to create a Secure String so you can encrypt and decrypt their Values stored in Parameter Store.

AWS Systems Manager Automation

AWS Systems Manager Automation simplifies common maintenance and deployment tasks of Amazon Elastic Compute Cloud instances and other AWS resources using runbooks, actions and service quotas. It enables you to build, execute and monitor automations at scale. A Systems Manager Automation is a type of Systems Manager document that defines the actions that Systems Manager performs on your managed instances. A runbook you use to perform common maintenance and deployment tasks such as running commands or automation scripts within your managed instances. Systems Manager includes features that help you target large groups of instances by using Amazon Elastic Compute Cloud tags, and velocity controls that help you roll out changes according to the limits you define. The runbooks are written using JavaScript Object Notation (JSON) or YAML. Using the Document Builder in the Systems Manager Automation console, however, you can create a runbook without having to author in native JSON or YAML. Alternatively you can use Systems Manager-provided runbooks with pre-defined steps that suits your needs. To learn more, see Working with runbooks in AWS Systems Manager documentation.

Note
Although Systems Manager Automation supports 20 action types that can be used in the runbook, a limited number of actions you can use while authoring runbook to be used in your AMS Advanced account. Similarly, a limited number of Systems Manager-provided runbook can be used either directly or from within your own runbook. For details, see the restrictions in the following FAQ.

AWS Systems Manager Automation in AMS FAQs

Common questions and answers:

Q: How do I request access to Systems Manager Automation in my AMS account?

Request access to AWS Systems Manager Automation by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_systemsmanager_automation_console_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the limitations to using AWS Systems Manager Automation in my AMS account?

You are required to author your runbook, with limited set of Systems Manager supported actions for automation, only to run commands and/or scripts within your managed instances. The actions that are available to you along with any restrictions are outlined as below.

AWS Systems Manager Automation Limitations

Action	Description	Limitation
aws:assertAwsResourceProperty –	Assert an AWS resource state or event state	Only EC2 instances
aws:aws:branch –	Run conditional automation steps	No limitation
aws:createTags –	Create tags for AWS resources	Only to SSM automation runbooks that you author
aws:executeAutomation –	Run another automation	Only the automation runbook that you author
aws:executeScript –	Run a script	Only script that does not make any API call to any services

Action	Description	Limitation
aws:pause –	Pause an automation	No limitation
aws:runCommand –	Run a command on a managed instance	Only using System Manager provided document - AWS-RunShellScript and AWS-RunPowerShellScript
aws:sleep –	Delay an automation	No limitation
aws:waitForAwsResourceProperty –	Wait on an AWS resource property	Only EC2 instances

You can also chose to run command or script directly with Systems Manager provided runbook AWS-RunShellScript and AWS-RunPowerShellScript using the 'Run Command' feature from within the Systems Manager console. You can also nest these runbooks within your runbook that caters for additional pre and/or post validation or any complex automation logic.

The role adheres to least privilege principle and only provides permission required to author, execute and retrieve execution details of runbooks aimed to executing command and/or scripts within your managed instances. It does not provide permission for any other capabilities that AWS Systems Manager service provides. While the feature allows you to author automation runbooks, execution of the runbooks can not be targeted for AMS owned resources.

Q: What are the prerequisites or dependencies to using AWS Systems Manager Automation in my AMS account?

There are no prerequisites; however, you must ensure your internal process and/or compliance controls are adhered to while authoring runbooks. We also recommend to thoroughly test runbooks before executing them against production resources.

Q: Can the Systems Manager policy `customer_systemsmanager_automation_policy` be attached to other IAM roles?

No, unlike other self-provision enabled services, this policy can only be assigned to the provisioned default role `customer_systemsmanager_automation_console_role`.

Unlike the policies of other SSPS roles, this SSM SSPS policy cannot be shared with other custom IAM roles, because this AMS service is only for running commands or automation scripts within your managed instances. If these permissions were allowed to be attached to other custom IAM roles, potentially with permissions on other services, the scope of allowed actions could extend to managed services, and potentially lower the security posture of your account.

To evaluate any requests for change (RFCs) against our AMS technical standards, work with your respective Cloud Architect or Service Delivery Manager, see RFC security reviews.

> **Note**
> AWS Systems Manager allows you to use runbooks that are shared with your account. We recommend you exercise caution and perform a due-diligence check when using shared runbooks and make sure to review the content to understand the command/scripts they run before executing the runbooks. For details refer to Best practices for shared SSM documents.

AWS Transfer Family (Transfer Family)

AWS Transfer Family (Transfer Family) is a fully managed AWS service that enables you to transfer files over Secure File Transfer Protocol (SFTP), into and out of Amazon Simple Storage Service (Amazon S3)

storage. SFTP is also known as Secure Shell (SSH) File Transfer Protocol. SFTP is used in data exchange workflows across different industries such as financial services, healthcare, advertising, and retail, among others.

With AWS SFTP, you get access to an SFTP server in AWS without the need to run any server infrastructure. You can use this service to migrate your SFTP-based workflows to AWS while maintaining your end users' clients and configurations as is. You first associate your hostname with the SFTP server endpoint, then add your users and provision them with the right level of access. After you do, your users' transfer requests are serviced directly out of your AWS SFTP server endpoint. To learn more, see AWS Transfer for SFTP.

AWS Transfer for SFTP in AMS FAQs

Common questions and answers:

Q: How do I request access to AWS Transfer for SFTP in my AMS account?

Request access to AWS Transfer for SFTP by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). Through this RFC the following IAM roles, and a policy, are provisioned in your account:

- `customer_transfer_author_role`. This role is designed for you to manage the SFTP service through the console.
- `customer_transfer_sftp_server_logging_role`. This role is designed to be attached on the SFTP Server. It allows the SFTP server to pull logs into CloudWatch.
- `customer_transfer_sftp_user_role`. This role is designed to be attached on the SFTP users. It allows the SFTP Users to interact with the S3 bucket.
- `policy customer_transfer_scope_down_policy`. This policy is a scope-down policy that can be applied to the SFTP User to limit their access on the S3 bucket to their home folders.

After it's provisioned in your account, you must onboard the roles in your federation solution.

Q: What are the restrictions to using AWS Transfer for SFTP in my AMS account?

AWS Transfer for SFTP configuration is limited to resources without "AMS-" or "MC-" prefixes to prevent any modifications to AMS infrastructure.

Q: What are the prerequisites or dependencies to using AWS Transfer for SFTP in my AMS account?

- You must have an S3 bucket before creating the AWS Transfer for SFTP server and users.
- You must submit a separate RFC (Management | Other | Other | Create) to create a VPC endpoint and have it connected to AWS Transfer for SFTP.
- ITo use a "Customer Identify Provider," you must deploy the API Gateway, Lambda function, and your user repository (AD, Secrets Manager, and so on). For more information, see Enable password authentication for AWS Transfer for SFTP using AWS Secrets Manager and Working with Identity Providers

AWS Transit Gateway

AWS Transit Gateway is a service that enables you to connect your Amazon Virtual Private Clouds (VPCs) and your on-premises networks to a single gateway. As you grow the number of workloads running on AWS, you need to be able to scale your networks across multiple accounts and Amazon VPCs to keep up with the growth. Today, you can connect pairs of Amazon VPCs using peering. However, managing point-to-point connectivity across many Amazon VPCs, without the ability to centrally manage the connectivity

policies, can be operationally costly and cumbersome. For on-premises connectivity, you need to attach your AWS VPN to each individual Amazon VPC. This solution can be time consuming to build and hard to manage when the number of VPCs grows into the hundreds. To learn more, see AWS Transit Gateway.

Transit Gateway in AMS FAQs

Common questions and answers:

Q: How do I request access to AWS Transit Gateway in my AMS account?

Request access to AWS Transit Gateway by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_tgw_console_role`. Once provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using AWS Transit Gateway in my AMS account?

Full functionality of AWS Transit Gateway is available in your AMS single-account landing zone account for the exception of route table modifications for TransitGateway routing. Request route table changes by submitting a Management | Other | Other | Create change type (ct-1e1xtak34nx76).

> **Note**
> This service is only supported for single-account landing zone (SALZ), not multi-account landing zone (MALZ).

Q: What are the prerequisites or dependencies to using AWS Transit Gateway in my AMS account?

There are no prerequisites or dependencies to use AWS Transit Gateway in your AMS account.

AWS WAF - Web Application Firewall

AWS WAF is a web application firewall (AWS WAF) that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow, or block, to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting; and rules that are designed for your specific application.

To learn more, see AWS WAF - Web Application Firewall.

AMS doesn't support monitoring (CloudWatch alarms / events / MMS alerts) for AWS WAF. Due to the nature of AWS WAF, you must create custom rules for your applications; AMS can't quantify and create alarms for you, without context of your application. To learn more, see AWS WAF - Web Application Firewall.

AWS WAF in AMS FAQs

Common questions and answers:

Q: How do I request AWS WAF to be set up in my AMS account?

Request access to AWS WAF by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_waf_role`. After the AWS WAF IAM role is provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using AWS WAF?

After permissions are provisioned, you have the full functionality of AWS WAF.

Q: What are the prerequisites or dependencies to using AWS WAF?

There are no prerequisites or dependencies to use AWS WAF in your AMS account.

AWS Well-Architected Tool

The AWS Well-Architected Tool helps you review the state of your workloads and compares them to the latest AWS architectural best practices. The tool is based on the AWS Well-Architected Framework , developed to help cloud architects build secure, high-performing, resilient, and efficient application infrastructure. This framework provides a consistent approach for you to evaluate architectures, has been used in tens of thousands of workload reviews conducted by the AWS solutions architecture team, and provides guidance to help implement designs that scale with application needs over time. To learn more, see AWS Well-Architected Tool.

AWS WA Tool in AMS FAQs

Common questions and answers:

Q: How do I request access to AWS Well-Architected Tool in my AMS account?

Request access to AWS Well-Architected Tool by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_well_architected_tool_console_admin_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

Q: What are the restrictions to using AWS Well-Architected Tool in my AMS account?

Full functionality of the AWS Well-Architected Tool is available in your AMS account.

Q: What are the prerequisites or dependencies to using AWS Well-Architected Tool in my AMS account?

There are no prerequisites or dependencies to use AWS Well-Architected Tool in your AMS account.

AWS X-Ray

AWS X-Ray (X-Ray) helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing, to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application, and shows a map of your application's underlying components. You can use X-Ray to analyze both applications in development and in production, from simple three-tier applications, to complex microservices applications consisting of thousands of services. To learn more, see AWS X-Ray.

X-Ray in AMS FAQs

Common questions and answers:

Q: How do I request access to AWS X-Ray in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your

account: `customer_AWS X-Ray_console_role`. After it's provisioned in your account, you must onboard the role in your federation solution. Additionally, you must have the `customer_xray_daemon_write_instance_profile` to push data from your Amazon EC2 instances to X-Ray. This instance profile is created when you receive the `customer_AWS X-Ray_console_role`.

You can submit a service request to AMS Operations to assign the `customer_xray_daemon_write_policy` to the existing instance profile, or you can use the instance profile that is created when AMS Operations enables X-Ray for you.

Q: What are the restrictions to using AWS X-Ray in my AMS account?

Full functionality of AWS X-Ray is available in your AMS account except for encryption with AWS KMS key (KMS key). AWS X-Ray encrypts all trace data by default. By default, X-Ray encrypts traces and related data at rest. If you need to encrypt data at rest with a key, you can choose either AWS-managed KMS key (aws/xray) or KMS Customer-Managed key. For KMS Customer-Managed key for X-Ray encryption, submit a Management | Other | Other | Create change type (ct-1e1xtak34nx76).

Q: What are the prerequisites or dependencies to using AWS X-Ray in my AMS account?

AWS X-Ray has a dependency on Amazon S3, CloudWatch, and CloudWatch Logs, which are already implemented in AMS accounts. Transitive dependencies vary based on data sources and other AWS service AWS X-Ray that features may be interacting with (for example, Amazon Redshift, Amazon RDS, Athena).

VM Import/Export

VM Import/Export enables you to easily import virtual machine images from your existing environment to Amazon EC2 instances and export them back to your on-premises environment. This offering allows you to leverage your existing investments in the virtual machines that you have built to meet your IT security, configuration management, and compliance requirements by bringing those virtual machines into Amazon EC2 as ready-to-use instances. You can also export imported instances back to your on-premises virtualization infrastructure, allowing you to deploy workloads across your IT infrastructure. To learn more, see VM Import/Export.

VM Import/Export in AMS FAQs

Common questions and answers:

Q: How do I request access to VM Import/Export in my AMS account?

Request access to VM Import/Export by submitting an RFC with the Management | AWS service | Self-provisioned service | Add change type (ct-3qe6io8t6jtny). This RFC provisions the following IAM role to your account: `customer_vmimport_policy`. After it's provisioned in your account, you must onboard the role in your federation solution.

An additional role, the **VM Import/Export Service** role, is required for the service to perform actions in your account.

Q: What are the restrictions to using VM Import/Export in my AMS account?

- Functionality to import custom machine images and data volumes is both available in AMS VM Import/Export. However, permissions to S3 have been scoped down to limit actions to buckets matching the name `customer-vmimport-*` in order to limit access to information within the account.
- Image and snapshot import is supported in AMS VM Import/Export. However, instance import and instance export functionality is not available due to security measures.

- Additionally, export functionality has been disabled to mitigate the risk of exporting restricted and sensitive data.

Q: What are the prerequisites or dependencies to using VM Import/Export in my AMS account?

- You must provide a supported disk image to import into the AWS environment. For information, see VM Import/Export Requirements.
- Note: VM Import/Export is not accessible through the AWS console. The service can only be accessed through the AWS CLI, AWS Tools for PowerShell, and the AWS SDKs. A **VM Import/Export enabled** role must be requested by an AMS RFC (Management | Other | Other | Create), and then you have to access the service directly with the previously mentioned tools. Alternatively, you can request an instance profile by RFC through which the tools can perform commands from an instance.

Access in AMS

Topics

Learn how to access resources by using SSH, or remote desktop protocol (RDP), and how to use bastions.

The AWS Managed Services (AMS) access management system is configured during onboarding. Only users with the AMS IAM user role, federated through AMS, can access AMS resources in the account.

In addition to the federated trust, described next, AMS security groups are an important element in private and public application access. For information about AMS security groups and how to change them, see Security groups (p. 348).

What is Access Management?

Access management is how AMS protects your resources by allowing only authorized and authenticated access. AMS uses a default IAM user role and instance profile, as well as multi-factor authentication, security groups, DNS-friendly bastion names, and more to keep your resources protected.

AMS focuses on three types of access that require management:

- Console access: Leveraging federation, users in the account's Active Directory can access the console using single sign-on (SSO). If you have multi-factor authentication configured for these accounts, you can continue to require MFA to gain access to the console.
- Instance access with RDP or SSH: Leveraging an Active Directory trust, users in the account's existing Active Directory can request access to an instance, and then successfully authenticate to a bastion and the instance by using their existing corporate credentials. If you have multi-factor authentication configured for those accounts, you can continue to require MFA to request access to an instance. AMS uses an MFA solution of its own to restrict AMS engineer access to instances.
- Application access: Varies by use case.

Why and When AMS Accesses Your Account

AWS Managed Services (AMS) manages your AWS infrastructure and sometimes, for specific reasons, AMS operators and administrators access your account. These access events are documented in your AWS CloudTrail (CloudTrail) logs.

Why, when, and how AMS accesses your account is explained in the following topics.

Topics

AMS Customer account access triggers

AMS customer account access activity is driven by triggers. The triggers today are the AWS tickets created in our issues management system in response to Amazon CloudWatch (CloudWatch) alarms and events, and incident reports or service requests that you submit. Multiple service calls and host-level activities might be performed for each access.

Access justification, the triggers, and the initiator of the trigger are listed in the following table.

Access Triggers

Access	Initiator	Trigger
Patching	AMS	Patch issue
Infrastructure deployments	AMS	Deployment issue
Internal problem investigation	AMS	Problem issue (an issue that has been identified as systemic)
Alert investigation and remediation	AMS	AWS Systems Manager operational work items (SSM OpsItems)
Manual RFC execution	You	Request for Change (RFC) issue. (Non-automated RFCs may require AMS access to your resources)
Incident investigation and remediation	You	Inbound support case (an incident or service request you submit)
Inbound service request fulfillment	You	

AMS customer account access IAM roles

When triggered, AMS accesses customer accounts using AWS Identity and Access Management (IAM) roles. Like all activity in your account, the roles and their usage are logged in CloudTrail.

The following are the IAM roles that AMS uses to access your account.

- The role `aws_ams_admin` is used by AMS for some automated infrastructure deployments.
- A new role, `ams-application-infra-operations`, is used for SALZ and MALZ Application/Tools-Application.

Requesting instance access

To access a resource, you must first submit a request for change (RFC) for that access. There are two types of access that you can request: admin (read/write permissions) and read-only (standard user access). Access lasts for eight hours, by default. This information is required:

- Stack ID, or set of stack IDs, for the instance or instances you want to access.
- The fully qualified domain name of your AMS-trusted domain.

- The Active Directory username of the person who wants access.
- The ID of the VPC where the stacks are that you want access to.

Once you've been granted access, you can update the request as needed.

For examples of how to request access, see Requesting Admin Access or Requesting Read-only Access.

How and when to use the root user account

AWS Managed Services (AMS) Security and Operations provide robust security of customer accounts. The "root user" account is the superuser, or administrator, account within your AWS account, and its use is strongly discouraged and watched by AMS. However, there are some tasks that require root access including changing your account settings, activating AWS Identity and Access Management (IAM) access to billing and cost management, changing your root password, and enabling multi-factor authentication (MFA). Root should not be used otherwise. For more information on when to use the root user account, see Tasks that require root user credentials. For information about how MFA is configured, see Secure New Account with Multi-Factor Authentication

> **Note**
> MFA is enabled during AMS Advanced onboarding to specifically disallow root user access. Root user access in AMS-managed accounts is different from other AWS accounts, and is critical to the security of your entire AMS-managed environment. The MFA configured is a virtual MFA and is performed using an AMS-owned device. After the virtual MFA is configured with AMS' assistance, the virtual token is immediately deleted. This ensures that neither you nor AMS retains the ability to log in to the account as root user. Root login can only be re-enabled on special requests (explained next) and AMS expects such accesses to be used only when absolutely necessary.

When root access is required, the process varies slightly between AMS account types but always triggers an AMS Security and Operations team response. AMS monitors API calls for root access, and alarms are triggered if such access is detected.

Root with AMS Advanced single-account landing zone:

If you have a single-account landing zone, contact your cloud service deliver manager (CSDM) and cloud architects (CAs) to advise them of the root access work that you require. It is best to give twenty-four hours notice before the proposed activity.

Root with AMS Advanced multi-account landing zone:

For multi-account landing zone Application, Shared Services, Security, or Networking accounts, use the Management | Other | Other (ct-1e1xtak34nx76) change type. Include the date, time, and the purpose of using the root user credentials and schedule the RFC to be sure to give twenty-four hours notice before the proposed activity. Use your multi-account landing zone Management account to submit the RFC.

Additionally, contact your CSDM and CAs twenty-four hours in advance, to advise them of the root access work you require.

Root with AMS Accelerate:

As an AMS Accelerate account, AMS cannot prohibit you from using your root user account. However, AMS Operations and Security does treat its usage as an issue to investigate and we will reach out to your Security team with every use.

If you have an AMS Accelerate account, contact your CSDM and CAs twenty-four hours in advance, to advise them of the root access work you require.

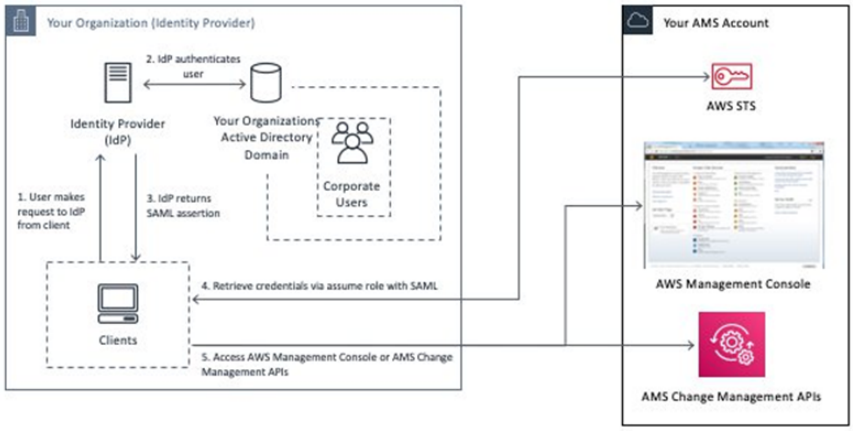
To learn about AWS root user account usage, see AWS account root user.

AMS operations and security response to root usage:

The AMS Operations team receives an alarm when the root user account is used. If the root credentials usage is unscheduled, they contact the AMS Security team, and your account team, to verify if this is expected activity. If it is not expected activity, AMS works with your Security team.

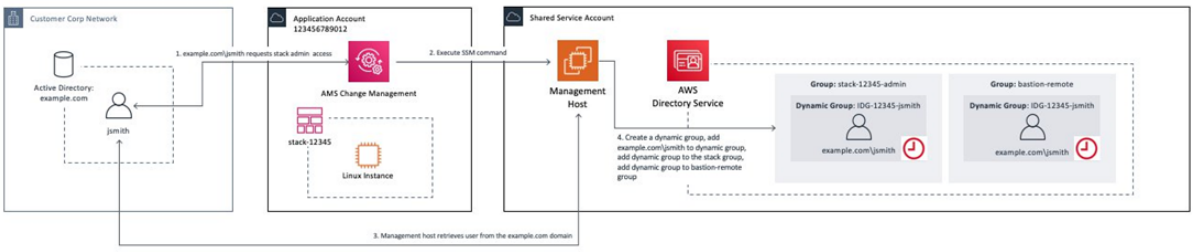
Multi-Account Landing Zone console and Amazon EC2 access

Console access for customers.

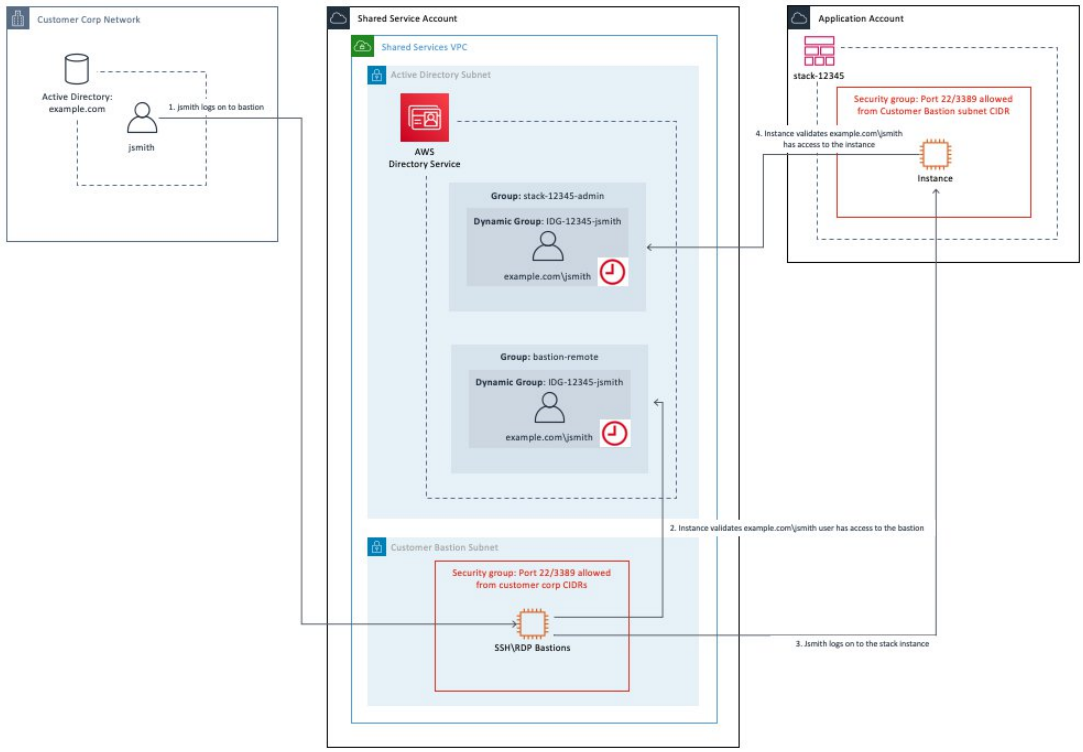


Amazon EC2 instance access for customers.

Submit access request:



Amazon EC2 instance login:



Accessing the AWS Management console and the AMS console

During onboarding, you're provided a login to the AWS Management console (with limited privileges: you can write to the AMS console, and some fields in your customer information page). You can access the AMS console by selecting the **Managed Services** link in the AWS Management console. Either federated access or shared credentials (user name/password) are prepared as agreed with your IT administration team. For further account or group creation, submit a service request to AMS.

For information about getting access to the AWS Management console, see Working with the AWS Management console.

For some tips on using the AMS console, see Using the AMS console.

Temporary AMS console access

If you haven't yet set up an identity provider (for instance, SAML) to authenticate to AMS, you can get temporary access to the AMS console. Contact your CSDM to have a Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entity or policy change request (ct-3dpd8mdd9jn1r) submitted on your behalf with these values:

- UserName: A name for the IAM user entity that you're creating
- AccessType: "Console access"
- UserPermissions: "Temporary AMS console access for *USERNAME* (the person that you want to have temporary access)"
- Email notifications: Your email address, so you can approve the request when AMS requests you to

Note
This RFC for temporary AMS Console access requires a security review and acceptance by both your internal security team and AMS Global Security.

After this request has been completed, and you're able to log in, you're required to approve the RFC that was created, to track the approval and allow the AMS team to close out the work. To approve the RFC, find it in the RFC's list page (there will be a Pending Approval flag next to it), select it to open the RFC details page for that RFC, and then choose **Approve**. Note that you won't be able to use AMS until the RFC is approved.

When the RFC successfully completes, AMS operations provides you with the new IAM user and a password. Then follow these steps:

1. Go to the AWS Management console and log in with provided user name and password. You'll be asked to create a new password. You must also, upon login, set up multi-factor authentication (MFA); to learn more about doing that, see Using Multi-Factor Authentication (MFA) in AWS.
2. In the AWS Management console, change to the provided IAM role (`customer_CustomerCode_readonly_user_role`).
3. Open the AMS **Managed Services** Console.

Note
Temporary access defaults to sixty days; however, you can request a thirty-day extension by contacting your CSDM.

Accessing instances using bastions

All access to resources inside AMS managed accounts, for both customers and AMS operators, is gated by the use of bastion hosts. We maintain both Linux and Windows RDP bastions for access.

Your bastions are accessible only over your private connection (VPN or AWS Direct Connect)DX. In addition to firewalling to prevent inbound traffic, bastions are regularly re-provisioned (with existing credentials) on a fixed schedule.

MALZ

You access your account instances by logging in to a bastion instance with your Active Directory (AD) credentials. Amazon uses bastions located in the perimeter network VPC (networking account), and you use your customer bastions, located in your Customer Bastions subnet in the shared services account.

When your AMS environment is initially onboarded, you have two SSH bastions and two RDP bastions depending on your choice.

SALZ

You access your account instances by logging in to a bastion instance with your Active Directory (AD) credentials. Amazon uses bastions located in the perimeter network subnets, and you use bastions located in your private subnets.

When your account is initially onboarded, you have two RDP and two SSH bastions, by default.

Note
As part of the single-account landing zone, AMS provides both RDP (Windows) and SSH (Linux) bastions to access your stacks; however, you can choose whether you want only RDP bastions or only SSH bastions. To request that only RDP, or only SSH bastions are maintained, submit a service request.

In order to access an instance, you need:

- Access granted to the stack. To get access granted to a stack, see Requesting Admin Access or Requesting Read-only Access.
- The stack ID that you want to access so you can be granted access to the instance. To find a stack ID, see Finding ARN IDs, instance IDs and IP addresses, and stack IDs (p. 261)
- The instance IP that you want to access. To find an instance IP, see Finding an instance ID or IP address (p. 262).
- The DNS friendly bastion name or the bastion IP. How to use DNS friendly bastion names and how to find a bastion IP are described next.

DNS friendly bastion names

MALZ

For Multi-account landing zone (MALZ), DNS records are created for the bastions in the FQDN of the AMS-managed Active Directory. AMS replaces Linux and Windows bastions as required. For example, if there is a new bastion AMI that must be deployed, the bastion DNS records dynamically update to point to new, valid bastions.

1. To access SSH (Linux) bastions, use DNS records like this:
   `sshbastion(1-4).Your_Domain.com`

   For example, where the domain is `Your_Domain`:

   - `sshbastion1.Your_Domain.com`
   - `sshbastion2.Your_Domain.com`
   - `sshbastion3.Your_Domain.com`
   - `sshbastion4.Your_Domain.com`
2. To access RDP (Windows) bastions, use DNS records like this:
   `rdp-Username.Your_Domain.com`.

   For example, where the user name is `alex`, `test`, `demo`, or `bob`, and the domain is `Your_Domain.com`:

   - `rdp-alex.Your_Domain.com`
   - `rdp-test.Your_Domain.com`
   - `rdp-demo.Your_Domain.com`
   - `rdp-bob.Your_Domain.com`

SALZ

Single-account landing zone (SALZ) replaces Linux and Windows bastions as required. For example, if there is a new bastion AMI that must be deployed, the bastion DNS records dynamically update to point to new, valid bastions.

1. To access SSH (Linux) bastions, use DNS records like this:
   `sshbastion(1-4).AAccountNumber.amazonaws.com.`

   For example, where `123456789012` is the account number:

   - `sshbastion1.A123456789012.amazonaws.com`
   - `sshbastion2.A123456789012.amazonaws.com`
   - `sshbastion3.A123456789012.amazonaws.com`

- `sshbastion4.A123456789012.amazonaws.com`

2. To access RDP (Windows) bastions, use DNS records like this: `rdpbastion(1-4).AACCOUNT_NUMBER.amazonaws.com`.

   For example, where `123456789012` is the account number:

   - `rdpbastion1.A123456789012.amazonaws.com`
   - `rdpbastion2.A123456789012.amazonaws.com`
   - `rdpbastion3.A123456789012.amazonaws.com`
   - `rdpbastion4.A123456789012.amazonaws.com`

Saving costs on Single-account landing zone (SALZ) bastions

AMS provides two SSH bastions in the default configuration for you to connect to your Amazon EC2 instances, and also deploys two DMZ bastions in the default configuration for service operations. The bastions use m4. large Amazon EC2 instances by default. You have an option to change the Amazon EC2 instances used for bastions to t3.small, and save cost.

If you are using on-demand instances, or spot instances, or a savings plan, you should consider this feature, and save costs. If you use Reserved Instances consider if using t3.small instances might lower your costs. To change the instance type, submit an RFC with Management | Other | Other | Update (ct-0xdawir96cy7k) CT from your AMS account:

- Subject: Change Amazon EC2 instance type for Linux Bastions.
- Description: Change Amazon EC2 instance type for DMZ and Customer Linux Bastions to t3.small.

Contact your cloud service delivery manager (CSDM) for additional questions, or to check if you can benefit from this feature.

Using bastion IP addresses

AMS customers can use SSH and RDP bastions, either the DNS friendly bastion names (p. 247) described previously, or bastion IP addresses.

To find bastion IP addresses, SSH and RDP, for your account:

1. For multi-account landing zone only: Log in to the Shared Services account.
2. Open the EC2 Console and choose **Running Instances**.

   The **Instances** page opens.
3. In the filter box at the top, enter either **ssh-bastion** or **rdp-bastion**.

   In the filter box at the top, enter either **customer-ssh** or **customer-rdp**.

   The SSH and/or RDP bastions for your account display.

   Note that in addition to your SSH bastions, you may see AMS perimeter network bastions in the list, which are unavailable for this.
4. Select an SSH or RDP bastion. If you're using a Windows computer and want to log in to a Linux instance, you use an SSH bastion. If you want to log in to a Windows instance, you use an RDP bastion. If you're on a Linux OS and want to log in to a Windows instance, you use an SSH bastion

through an RDP tunnel (this is so you can access the Windows desktop). To access a Linux instance from a Linux OS, you use an SSH bastion.

Instance access examples

These examples show how to log in to an instance by using a bastion after you've been granted access through an RFC. For information about getting access granted, see Requesting instance access (p. 242).

> **Note**
> An Amazon EC2 instance created through an Amazon EC2 Auto Scaling group will have an IP address that cycles in and out and you have to use your Amazon EC2 console to find that IP address.

Required data:

- **Bastion DNS friendly name or IP address**: Use a DNS friendly name as described in DNS friendly bastion names (p. 247) or find bastion IP addresses as described in Using bastion IP addresses (p. 248).
- **User name** (for example *DOMAIN_FQDN**USERNAME*) and **Password**: Credentials for the account. The *USERNAME* must be your Active Directory user account name.

  Note that a user name in the format username@customerdomain.com can be used but can cause trouble with your PBIS setup.
- **Stack IP address**: Find this by looking at the run output for the RFC that you submitted to launch the stack, or look up the Amazon EC2 instance IP address in the Amazon EC2 console. For a single Amazon EC2 instance, you can also use the AMS SKMS command ListStackSummaries to find the stack ID and then GetStack to find the stack IP address.

Access the bastion IP address, either SSH or RDP, as appropriate, and log in using one of the following procedures.

> **Note**
> RDP bastions only allow two simultaneous connections. So, in the best case scenario, only 4 admins are able to connect to windows stacks at the same time. If you require more connections for RDP, see AMS Bastion Options during Application Migrations/Onboarding in the AMS onboarding guide.

Linux computer to Linux instance

Use SSH to connect to the SSH bastion and then to the Linux instance.

MALZ

For more information about the friendly bastion names, see DNS bastions.

In order to connect to the Linux instance, you must first connect to an SSH bastion.

1. Open a shell window and enter:

```
ssh Domain_FQDN\\Username@SSH_bastion_name
    or SSH_bastion_IP
```

Which would look like this if your Domain_FQDN is "corp.domain.com", your account number is "123456789123", Your_Domain is "amazonaws.com", you choose bastion "4", and your user name is "JoeSmith":

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. Log in with your corporate Active Directory credentials.
3. When presented with a Bash prompt, SSH in to the instance, and then enter:

```
ssh Domain_FQDN\\Username@Instance_IP
```

Or, you can use the Login flag (-l):

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

For more information about the friendly bastion names, see DNS bastions.

In order to connect to the Linux instance, you must first connect to an SSH bastion.

1. Open a shell window and enter:

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name
    or SSH_BASTION_IP
```

Which would look like this if your account number is 123456789123, you choose bastion 4, and your user name is JoeSmith:

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. Log in with your corporate Active Directory credentials.
3. When presented with a Bash prompt, SSH in to the instance, and then enter:

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Or, you can use the Login flag (-l):

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Linux computer to Windows instance

Use an SSH tunnel and an RDP client to connect to a Windows instance from your Linux computer.

MALZ

This procedure requires a Remote Desktop Connection client for Linux; the example uses Microsoft Remote Desktop (an open source UNIX client for connecting to Windows Remote Desktop Services). Rdesktop is an alternative.

Note
How you log in to Windows instances might change based on the remote desktop client being used.

First you establish an SSH tunnel, and then log in.

For more information about the friendly bastion names, see DNS friendly bastion names (p. 247).

Before you begin:

- Request access to the instance that you want to connect to; for information, see Access requests.
- Choose a friendly DNS SSH bastion name to connect to; for example:

```
sshbastion(1-4).Your_Domain
```

  Which would look like this if your Domain_FQDN is "corp.domain.com", your AMS-managed Your_Domain is "amazonaws.com", you choose bastion "4", and your user name is "JoeSmith":

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- Find the IP address of the instance that you want to connect to; for information, see Finding an instance ID or IP address.

1. Set up RDP over an SSH tunnel from a Linux desktop to a Windows instance. In order to issue the `ssh` command with the right values, there are a couple of ways to proceed:

   - In the Linux shell, set the variables, and then enter the SSH connection command:

     ```
     BASTION="sshbastion(1-4).Your_Domain""
     WINDOWS="Windows_Instance_Private_IP"
     AD="AD_Account_Number"
     USER="AD_Username"
     ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
     ```

     Example, if the following values are used:

     ```
     BASTION="sshbastion4.A123456789123.amazonaws.com"

     WINDOWS="172.16.3.254"

     AD="ACORP_example"

     USER="john.doe"
     ```

   - Add the variable values directly to the `ssh` command.

   In either case, this is what the rendered request would be (assuming the same set of variable values):

   ```
   ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
   ```

2. Either: Open your Remote Desktop Client, enter the loopback address and port, 127.0.0.1:3389, and then open the connection.

   Or, log in to the Windows instance from a new Linux desktop shell. If you use RDesktop, the command looks like this:

   ```
   rdesktop 127.0.0.1:3389
   ```

   A remote desktop window for the Windows instance appears on your Linux desktop.

Tip
If the remote desktop session fails to start, verify that network connectivity to the Windows instance from the SSH bastion is allowed on port 3389 from the shell in step 1 (replace `private_ip_address_of_windows_instance` appropriately):

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

Success:

```
nc 172.16.0.83 3389 -v -z
        Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
        netstat -anvp | grep 3389
        tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

SALZ

This procedure for a single-account landing zone requires a Remote Desktop Connection client for Linux; the example uses Microsoft Remote Desktop (an open source UNIX client for connecting to Windows Remote Desktop Services). Rdesktop is an alternative.

Note
How you log in to Windows instances might change based on the remote desktop client being used.

First you establish an SSH tunnel, and then log in.

For more information about the friendly bastion names, see DNS friendly bastion names (p. 247).

Before you begin:

- Request access to the instance that you want to connect to; for information, see Access requests.
- Choose a friendly DNS SSH bastion name to connect to; for example:

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

Which would look like this if your account number is 123456789123 and you choose bastion 4:

```
sshbastion4.A123456789123.amazonaws.com
```

- Find the IP address of the instance that you want to connect to; for information, see Finding an instance ID or IP address.

1. Set up RDP over an SSH tunnel from a Linux desktop to a Windows instance. In order to issue the `ssh` command with the right values, there are a couple of ways to proceed:

   - In the Linux shell, set the variables, and then enter the SSH connection command:

   ```
   BASTION="sshbastion(1-4).AAMSAccountNumber.amazonaws.com"
   WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"
   AD="AD_ACCOUNT_NUMBER"
   USER="AD_USERNAME"
   ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
   ```

   Example, if the following values are used:

   ```
   BASTION="sshbastion4.A123456789123.amazonaws.com"
   ```

```
WINDOWS="172.16.3.254"

AD="ACORP_example"

USER="john.doe"
```

- Add the variable values directly to the `ssh` command.

In either case, this is what the rendered request would be (assuming the same set of variable values):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. Either: Open your Remote Desktop Client, enter the loopback address and port, 127.0.0.1:3389, and then open the connection.

   Or, log in to the Windows instance from a new Linux desktop shell. If you use RDesktop, the command looks like this:

   ```
   rdesktop 127.0.0.1:3389
   ```

   A remote desktop window for the Windows instance appears on your Linux desktop.

   Tip
   If the remote desktop session fails to start, verify that network connectivity to the Windows instance from the SSH bastion is allowed on port 3389 from the shell in step 1 (replace `private_ip_address_of_windows_instance` appropriately):

   ```
   nc private_ip_address_of_windows_instance 3389 -v -z
   ```

   Success:

   ```
   nc 172.16.0.83 3389 -v -z
           Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
           netstat -anvp | grep 3389
           tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
   ```

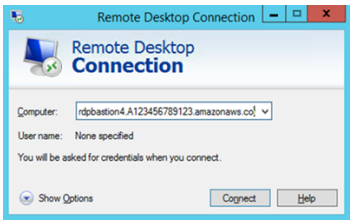
Windows computer to Windows instance

Use Windows Remote Desktop Connection client to connect to a Windows instance from your Windows computer.

MALZ

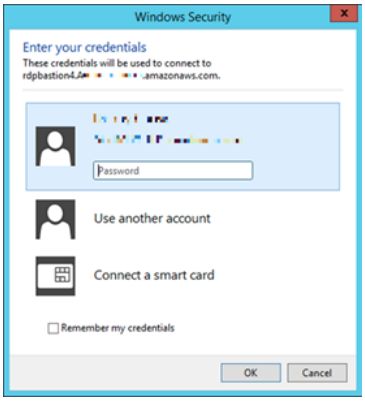
For more information about the friendly bastion names, see DNS friendly bastion names (p. 247).

1. Open the Remote Desktop Connection program, a standard Windows program, and enter the friendly DNS name of the Windows bastion in the hostname field.

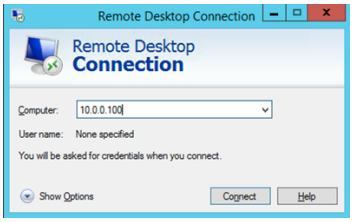


2. Choose **Connect**. The Remote Desktop Connection attempts an RDP connection to the bastion.

   If successful, a credentials dialog box opens. To gain access, use your corporate Active Directory credentials, as you would with the Windows instance.



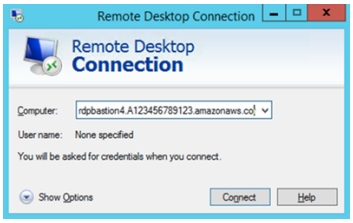
3. Open the Remote Desktop Connection program on the bastion and enter the IP address of the Windows instance you would like to connect to (for example, 10.0.0.100), and then choose **Connect**. Your corporate Active Directory credentials are again required before you connect to the Windows instance.



SALZ

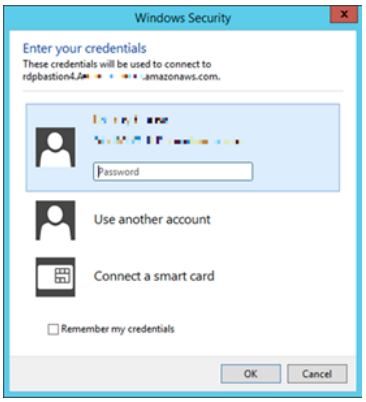
For more information about the friendly bastion names, see DNS friendly bastion names (p. 247).

1. Open the Remote Desktop Connection program, a standard Windows program, and enter the friendly DNS name of the Windows bastion in the hostname field; for example, `rdpbastion(1-4).AAMSAccountNumber.amazonaws.com`, which would look like this if your account number is 123456789123 and you choose bastion 4, `rdpbastion4.A123456789123.amazonaws.com`.

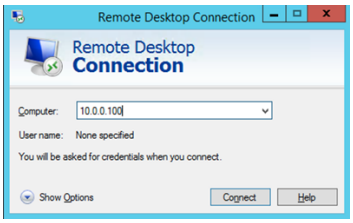


2. Choose **Connect**. The Remote Desktop Connection attempts an RDP connection to the bastion.

If successful, a credentials dialog box opens. To gain access, use your corporate Active Directory credentials, as you would with the Windows instance.



3. Open the Remote Desktop Connection program on the bastion and enter the IP address of the Windows instance you would like to connect to (for example, 10.0.0.100), and then choose **Connect**. Your corporate Active Directory credentials are again required before you connect to the Windows instance.



Windows computer to Linux instance

To RDP to an SSH bastion from a Windows environment, follow these steps.

MALZ

Before you begin:

- Request access to the instance that you want to connect to; for information, see Access requests.
- Choose a friendly DNS SSH bastion name to connect to; for example:

```
sshbastion(1-4).YOUR_DOMAIN
```

Which would look like this if YOUR_DOMAIN is myamsaddomain.com" and you choose bastion 4:

```
sshbastion4.myamsaddomain.com
```

- Find the IP address of the instance that you want to connect to; for information, see Finding an instance ID or IP address.

In order to connect to the Linux instance from your Windows machine, you must first connect to an SSH bastion.

Use the native Windows OpenSSH client or install PuTTY on your local machine. To learn more about OpenSSH, see OpenSSH in Windows.

1. Use the native Windows or open PuTTY and enter the SSH bastion hostname or the IP address of the SSH bastion. For example, 10.65.2.214 (22 is the port used for SSH; it will be set by default).
2. OpenSSH or PuTTY attempts an SSH connection to the bastion and open a shell window.
3. Use your corporate Active Directory credentials as you would with the RDP hosts to gain access.
4. When presented with a Bash prompt, SSH into the instance. Enter:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

Before you begin:

- Request access to the instance that you want to connect to; for information, see Access requests.
- Choose a friendly DNS SSH bastion name to connect to; for example:

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

  Which would look like this if your account number is 123456789123 and you choose bastion 4:

```
sshbastion4.A123456789123.amazonaws.com
```

- Find the IP address of the instance that you want to connect to; for information, see Finding an instance ID or IP address.

In order to connect to the Linux instance from your Windows machine, you must first connect to an SSH bastion.

Use the native Windows OpenSSH client or install PuTTY on your local machine. To learn more about OpenSSH, see OpenSSH in Windows.

1. Use the native Windows or open PuTTY and enter the SSH bastion hostname or the IP address of the SSH bastion. For example, 10.65.2.214 (22 is the port used for SSH; it will be set by default).
2. OpenSSH or PuTTY attempts an SSH connection to the bastion and open a shell window.
3. Use your corporate Active Directory credentials as you would with the RDP hosts to gain access.
4. When presented with a Bash prompt, SSH into the instance. Enter:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

Team, or role, based access control in an AMS account

Scenario: Two application teams A, and B, use a single AMS account for their apps "AA", and "BB", respectively. Team A wants access only to resources for app "AA", and team B wants access only to resources for app "BB". How do I set that up?

Use their ITSM's tools to implement team-based access controls (TBAC). For example, you could use the AMS ServiceNow Connector App for integration with AMS APIs. Contact your CSDM for high level guidance of this implementation.

Service knowledge management

Topics

SKMS stands for service knowledge management system and refers to all information related to the AWS Managed Services (AMS) service for a customer.

What Is service knowledge management?

Service knowledge management is the store of all information on your AMS account. Currently, information about the following is obtained from the AMS service knowledge management system (SKMS), through the AMS SKMS API:

- VPCs
- Managed subnets
- Stacks and stack components, including Amazon EC2 instances and other resources
- Amazon Machine Images (AMIs)

You can use information from the SKMS to understand the infrastructure under management and as input to change management and service requests to create, change, or remove infrastructure.

> **Note**
> All AMS SKMS API calls are recorded in AWS CloudTrail. For more information, see Accessing your logs (p. 305).

Access the SKMS through the AMS SKMS API, which provides operations for discovering information about an environment (VPCs and subnets) and the application resources (stacks, Amazon EC2 instances, and instance images or AMIs) that can be deployed there.

VPCs and instance images are set up in an account, with the necessary access permissions, during onboarding. After they have been established, you can use the change management system to populate the VPCs with working stacks.

Finding VPC, subnet, and AMI IDs

A virtual private cloud (VPC) has one or more subnets. In AMS your VPC is in an AWS Region and you have private and public subnets.

Finding a VPC ID

Most CTs require the VpcId. To find a VPC ID, you can use either the AMS console or API/CLI.

AMS Console:

1. In the navigation pane, select **Network**. The **Network** page opens.

2. Information about your VPC, or a VPC list, is shown. For more VPC details, you can open the VPC dashboard.

AMS SKMS API (see ListVpcSummaries) or CLI:

Note
The AMS CLI must be installed for these commands to work. To install the AMS API or CLI, go to the AMS console **Developers Resources** page. For reference material on the AMS CM API or AMS SKMS API, see the AMS Information Resources section in the User Guide.

1. In the following examples, the first command requests a list of summaries for all VPCs in the account. The second command requests the list of VPCs, with a query filter to list only those VPCs created in 2016, and output the CreatedTime, VpcId, and Name.

```
aws amsskms list-vpc-summaries --output table
```

```
-----------------------------------------------------
|                 ListVPCSummaries                  |
+---------------------------------------------------+
|                  VPCSummaries                     |
|+------------------+------------------------------|
|   CreatedTime     |   2016-01-15T18:50:11Z       |
|   VpcId           |   vpc-01234567890abcdef      |
|   LastModifiedTime|   2016-01-15T18:50:11Z       |
|   Name            |   952444781316-initial-vpc   |
|+------------------+------------------------------|
|                   Visibility                      |
|+------------------+------------------------------|
|   Id              |  PrivateAndPublic            |
|   Name            |  PrivateAndPublic            |
|+------------------+------------------------------|
```

2. This time with a query:

```
aws amsskms list-VPC-summaries --query "VPCSummaries[?
starts_with(@.CreatedTime,to_string(`2016`))].[CreatedTime, VpcId, Name]" --output
 table
```

```
-------------------------------------------------------------------------
|                            ListVPCSummaries                           |
+----------------------+-----------------------+--------------------------+
|2016-01-15T18:50:11Z | vpc-01234567890abcdef | 952444781316-initial-VPC |
+----------------------+-----------------------+--------------------------+
```

Finding a subnet ID

Several resources require that you specify a subnet, or list of subnets, at configuration time. To find subnets, you can use either the AMS console or API/CLI.

AMS Console:

1. In the navigation pane, select **Network**. The **Network** page opens.
2. A list of subnets is shown or, if necessary, click the VPC that you want a subnet for.

AMS SKMS API (see ListSubnetSummaries) or CLI:

Note
The AMS CLI must be installed for these commands to work. To install the AMS API or CLI, go to the AMS console **Developers Resources** page. For reference material on the AMS CM API or AMS SKMS API, see the AMS Information Resources section in the User Guide.

To find the subnets for your VPC by Visibility status, private or public, you can search with the `list-subnet-summaries` command as shown.

1. The SKMS API ListSubnetSummaries operation has parameters to narrow the results based on visibility. In addition, you can Filter results based on name. If you're using the CLI, you can also use the `--query` option to narrow the output or search on a portion of a value. For example, to find all of the subnets for a particular VPC, you can use this command:

```
aws amsskms list-subnet-summaries --query "SubnetSummaries.sort_by(@,&Visibility.Name)
[].[Visibility.Name,SubnetId,Name]" --output table
```

   Which returns something like this:

```
-------------------------------------------------------------------
|                   ListSubnetSummaries                           |
+---------+------------         -------+---------------------------+
|  Private|  subnet-01234567890abcdef  |  Demo Deployment Zone #1  |
|  Private|  subnet-01234567890abcdef  |  Demo Deployment Zone #1  |
|  Public |  subnet-01234567890abcdef  |  Demo DMZ #1              |
|  Public |  subnet-01234567890abcdef  |  Demo DMZ #1              |
+---------+----------         ---------+---------------------------+
```

   For information about using CLI queries, see How to Filter the Output with the --query Option and the query language reference, JMESPath Specification.
2. If you have multiple VPCs, include a VPC filter in the command, and then run the command for each VPC. For example:

```
list-subnet-summaries --filter Attribute=VpcId,Value=vpc-xxxxxxxx --query
 "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

For information about using CLI queries, see How to Filter the Output with the --query Option and the query language reference, JMESPath Specification..

Subnet names

Your AMS subnets are created automatically after input is gathered from you and added to the system. AMS uses a formula to create your subnet names: <A<ACCOUNT_ID>-<SUBNET-TYPE>-<AZ-IDENTIFIER>. The subnet type would be either `dmz`, `shared-services`, or `customer-application`. Should you have more than one customer-application subnet, an optional identifier may be added to the subnet name, after the account ID, to indicated that the subnet is an "additional" or "reserved" subnet.

Finding an AMI ID

An AMI is a template for Amazon EC2 instances, created from an Amazon EC2 instance. AWS provides updated AMIs (with patches, for example); however, AMS requires AMIs that have been modified for AMS use. AMS releases new AMIs that you can use every 4 - 8 weeks.

Amazon Machine Images (AMIs) are instance configuration templates that are used to create EC2 instances in AWS. AMS requires that specific AMIs be used for AMS-managed resources. The change types for creating EC2 instances and EC2 Auto Scaling groups require that you specify an AMI for AMS to use

as the basis for the instances that the change type creates. AMS recommends that you always select the most recent AMI available to you.

To learn more about AWS AMIs, see AWS AMI Design.

When creating an Amazon EC2 stack or Amazon EC2 Auto Scaling group, you must specify an Amazon machine image (AMI) by **AmiId**. You're limited to AMIs that begin with "customer-" and we recommend that you always choose the most recent AMI.

To find the most recent AMI for your account, you can search with the `list-amis` command or use the AMS console details page for relevant VPC:

- Use the AMS console: Available AMIs are listed on the **AMI** page in the AMS console. Select from AMIs with names that begin with "customer".
- Use the AMS API/CLI ListAmis operation. Here is a CLI example with a `query` option that restricts the results to customer AMIs:

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?
starts_with(Name,'customer')].[Name,AmiId]" --output table
```

  This example uses the `filter` option with the `query` option to find Windows AMIs that start with "customer":

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?
starts_with(Name,'customer')].[Name,AmiId]" --filter Attribute=Platform,Value=windows --
output table
```

- For information about using CLI queries, see How to Filter the Output with the --query Option and the query language reference, JMESPath Specification.

Finding your security groups, IAM roles and policies

How to find security group IDs, IAM role ARNs, and the IAM policies applied to your resources.

Finding your security group (SG) IDs

Amazon EC2 create and OpenSearch create domain CTs require a security group ID. This will be in the form `sg-02ce123456e7893c7`. Your account has at least two default security groups; see Security groups (p. 348). Additionally, you may have security groups that you created for specific purposes. To discover your security groups:

- Console: Use the EC2 or VPC console to view all security groups for the selected VPC.
- API/CLI (when logged into your AMS account):

  List your security groups:

```
aws ec2 describe-security-groups
```

Finding your IAM roles and policies

Your account has default IAM Roles and Policies; see IAM User Role (p. 322) and default IAM instance profiles; see EC2 IAM instance profile (p. 85) with default policies. To discover your IAM roles and policies:

- Console: Use the IAM console to view all IAM policies and roles for your account.
- API/CLI (when logged into your AMS account):

  List your roles:

```
aws --profile saml iam list-roles
```

  List your policies:

```
aws --profile saml iam list-role-policies --role-name ROLE_NAME
```

Finding ARN IDs, instance IDs and IP addresses, and stack IDs

A stack is based on a CloudFormation template that has been constructed for a particular use case; for example, an application tier or a database tier.

An instance is an Amazon EC2 instance, either a part of a stack or a standalone instance. To log in to an instance that is part of an Amazon EC2 Auto Scaling group (ASG), you request access to the ASG stack, which gives you access to all associated instances.

Finding a stack ID

Some change types require the StackId. To find a Stack ID, you can use either the AMS console, Amazon EC2 console, or API/CLI.

AMS Console:

- In the navigation pane, select **RFCs**, and then click the RFC that created the stack. Use the filter option at the top to reduce the list. The RFC details page opens and includes the run output with the stack ID.
- Alternatively, you can select **Stacks in the navigation pane** to open the stacks list page, and then page through the stack list to the stack you're interested in. This method is more useful if you know the subject of the stack you are looking for.

Amazon EC2 Console:

In the navigation pane, select **Instances** or **Load Balancers** or **Auto Scaling Groups**.

AMS SKMS API (see ListStackSummaries) or CLI:

> **Note**
> The AMS CLI must be installed for these commands to work. To install the AMS API or CLI, go to the AMS console **Developers Resources** page. For reference material on the AMS CM API or AMS SKMS API, see the AMS Information Resources section in the User Guide.

To view a list of stacks in the current account, run the ListStackSummaries operation of the SKMS API (CLI: `list-stack-summaries`). To get complete information about a particular stack instance, by StackId, run GetStack.

- In the following examples, the first command requests a list of summaries for all stack instances in the account. The second command requests the list of stack instances, with a query filter to list only those of a specific stack template, and output the VpcId, Name, and StackId.

```
aws amsskms list-stack-summaries --output table
```

```
-----------------------------------------------------------------------
|                                  ListStackSummaries                 |
|                                   StackSummaries                    |
+------------+----------------------+---------------------+---------+
|   VpcId    |         StackId      |  StackTemplateId    |  Name   |
+------------+----------------------+---------------------+---------+
|vpc-0123abcd|stack-1fb7fe2212345678|stm-sdhopvbb123456789|Test ELB|
|vpc-0123abcd|stack-8323cc0e12345678|stm-s2b72beb123456789|S3 store|
|vpc-0123abcd|stack-2309fa0712345678|stm-sdhopvbb123456789|ELB     |
|vpc-0123abcd|stack-5e61a70512345678|stm-sdpabqbb123456789|PatchSim|
|vpc-0123abcd|stack-bd0e080d12345678|stm-s2b72beb123456789|CLI demo|
+------------+----------------------+---------------------+---------+
```

For information about using CLI queries, see How to Filter the Output with the --query Option and the query language reference, JMESPath Specification..

Finding an instance ID or IP address

- To request access to an instance, to log in to an instance, or to create an AMI, you must have the instance ID. For an EC2 instance (either a standalone instance or a part of a stack), or a database instance, you can find the ID in a few different ways:
  - The AMS Console for an instance in an ASG stack: Look on the RFC detail page for the RFC that created the stack. In the Execution Output section, you will find the stack ID for the ASG stack and you can then go to the EC2 Console **Auto Scaling Groups** page and search for that stack ID and find instances for it. When you find the instance, select it and an area opens at the bottom of the page with details, including the IP address.
  - The AMS Console for a standalone EC2 or database (DB) instance: Look on the RFC detail page for the RFC that created the EC2 stack or DB instance. In the Execution Output section, you will find the Instance ID and IP address.
  - AWS EC2 Console:
    1. In the navigation pane, select **Instances**. The **Instances** page opens.
    2. Click the instance that you want the ID for. The instance details page opens and displays the ID and IP address.
  - AWS Database Console:
    1. On the Home page, select **DB Instances**. The **Instances** page opens.
    2. Filter for the DB instance that you want the ID for. The instance details page opens and displays the ID.
  - AMS CLI/API.

    Note
    The AMS CLI must be installed for these commands to work. To install the AMS API or CLI, go to the AMS console **Developers Resources** page. For reference material on the AMS CM API or AMS SKMS API, see the AMS Information Resources section in the User Guide.

    Run the following command to get stack execution output details:

    ```
    aws amsskms get-stack --stack-id STACK_ID
    ```

    The output looks similar to this with the InstanceId appearing near the bottom, under `Outputs` (values shown are examples):

```
{
    "Stack": {
        "StackId": "stack-7fa52bd5eb8240123",
        "Status": {
            "Id": "CreateCompleted",
            "Name": "CreateCompleted"
        },
        "VpcId": "vpc-01234567890abcdef",
        "Description": "Amazon",
        "Parameters": [
            {
                "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
                "Key": "SecurityGroups"
            },
            {
                "Value": "subnet-01234567890abcdef",
                "Key": "InstanceSubnetId"
            },
            {
                "Value": "t2.large",
                "Key": "InstanceType"
            },
            {
                "Value": "ami-01234567890abcdef",
                "Key": "InstanceAmiId"
            }
        ],
        "Tags": [],
        "Outputs": [
            {
                "Value": "i-0b22a22eec53b9321",
                "Key": "InstanceId"
            },
            {
                "Value": "10.0.5.000",
                "Key": "InstancePrivateIP"
            }
        ],
        "StackTemplateId": "stm-s6xvs000000000000",
        "CreatedTime": "1486584508416",
        "Name": "Amazon"
    }
}
```


Finding an Amazon Resource Name (ARN)

Amazon Resource Names (ARNs) uniquely identify AWS resources. We require an ARN when you specify a resource unambiguously across all of AWS, such as in IAM policies, Amazon Relational Database Service (Amazon RDS) tags, and API calls.

To learn more about AWS ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces.

- CodeDeployServiceRoleArn: Used for Code Deploy deployment group create CT. Follows this form `arn:aws:iam::ACCOUNT_ID:role/aws-codedeploy-role`. Find by either:
  - Console: Find by looking in the AWS Management Console -> Developer Tools -> CodeDeploy console (select an application and click the open arrow).
  - CLI:

```
aws iam get-role --role-name CodeDeployServiceRole --query "Role.Arn" --output text
```

- SSLCertificateId: Used for load balancer CTs. Follows this form `arn:aws:acm:REGION:ACCOUNT-ID:certificate/12345678-1234-1234-1234-123456789012`. Find by either:
  - Console: Find by looking in the AWS Certificate Manager Console for the relevant domain.
  - CLI:

```
aws iam list-server-certificates
```

Finding your account settings

Specific to every account are certain settings that are used to create RFCs, set schedules, and determine who receives notifications. This section describes how to find out what those settings are.

Some settings are created during onboarding and require a service request to change. You should make a note of these account details because you will use them when communicating with AMS:

- **Credentials**: If you need to retrieve your AMS user name or password, contact your local IT administrator--AMS uses your corporate Active Directory.
- **Cloud Service Delivery Manager (CSDM)**: This person is your liaison with AMS and is available to answer service questions. You are given this person's contact information at onboarding and should keep it available to all in your organization who interact with AMS. You can expect to receive monthly reports on your AMS service from this person.
- **Console access**: You access the AMS console at a URL set up specifically for your account. You can get the URL from your CSDM.
- **AMS CLI**: You can obtain the AMS CLI through the AMS console, or the distributables package that you get from your CSDM. After you have the distributables package, follow the steps outlined in Installing or upgrading the AMS CLI.
- **Maintenance window**: Your maintenance window determines when patching happens for your EC2 instances. The AWS Managed Services Maintenance Window (or Maintenance Window) performs maintenance activities for AWS Managed Services (AMS) and recurs the second Thursday of every month from 3 PM to 4 PM Pacific Time. AMS may change the maintenance window with 48 hours notice. You may have chosen a different window at onboarding--keep a record of your chosen maintenance window.
- **Monitoring**: AMS provides a set of CloudWatch metrics by default, but you can also request additional metrics. If you do, keep record of those.
- **Logs**: By default, your logs are stored at ams-a-*ACCOUNT_ID*-log-management-*REGION* where *REGION* is the region where the log was generated.
- **Mitigation**: At onboarding, AMS records the mitigation action of your choice in case a malware attack against your resources is identified. For example, contact certain people. Keep this information available to all in your organization who interact with AMS.
- **Region**: You can look at the VPC details page in the AMS console. You can also run this command (uses a SAML profile, remove if your authentication method is different):

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

Finding your FQDN

Access CTs require the fully qualified domain name, or FQDN, of your AMS-trusted domain, in the form of `C844273800838.amazonaws.com`. To discover your FQDN:

- Console: Look in the AWS Directory Service console (under Security, Identity, and Compliance category) in the **Directory name** column

- API/CLI: Use these commands while logged into your domain:

  Windows (returns user and FQDN):

```
whoami /upn
```

  or (DC+DC+DC=FQDN)

```
whoami /fqdn
```

  Linux:

```
hostname --fqdn
```

Finding your availability zones

Availability Zone: All accounts have at least two availability zones. To accurately find your availability zone names, you must first know the associated subnet ID.

- Console: In the navigation pane click **Network**, and then click the relevant VPC, if necessary. The **Network** page includes a table of subnets. Select the relevant subnet to open the subnet details page with the name of the associated availability zone.
- API/CLI:

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

Finding your SNS settings

To discover your SNS topics:

- Console: Use the SNS console to view all topics, applications, and subscriptions, and a graph of messages. Also create, delete, subscribe to, and publish to topics.
- API/CLI (when logged into your AMS account):

  List your SNS topics:

```
aws sns list-topics
```

  List your SNS subscriptions:

```
aws sns list-subscriptions
```

Finding your backup settings

Backups and Snapshots are managed by AMS through the native AWS Backup service.

The configuration is managed through AWS Backup plans. You can have multiple AWS Backup plans that associate tagged resources with backup schedules and retention policies. For more information, see Continuity Management.

Incident reports and service requests in AMS

Topics

With AWS Managed Services (AMS), you can request help with operational issues and requests at any time through the AMS console. AMS operations engineers are available to respond to your incidents and service requests 24x7, with response time Service Level Agreements (SLAs) and Service Level Objectives (SLOs), dependent on your selected account Service Tier (Plus, Premium). AMS operations engineers proactively notify you of important alerts and questions using the same mechanisms.

Incident management

Topics

Incidents are AWS service performance issues that impact your managed environment, as determined by AWS Managed Services (AMS) or you. Incidents identified by the AMS team are first received as "events": a change in system state captured by monitoring. If a configured threshold is breached, the event triggers an alarm, also called an alert. The AMS operations team determines if the event is non-impacting, an incident (a service interruption or degradation), or a problem (the underlying root cause of one or more resolved incidents).

The AMS team also receives incidents identified by you through the AWS Support center or programmatically using the AWS Support API with the service code `sentinel-report-incident`.

After your incident is received by the AMS operations team, it's reviewed to ensure that the incident is not more properly classified as a service request. If it should be classified as a service request, it's immediately reclassified and the AMS service request team takes over and you are notified. If the incident can be resolved by the receiving operator, steps are taken to immediately resolve the incident. AMS operators consult internal documentation for a resolution and, if needed, escalate the incident to other support resources until the incident is resolved. To be kept informed at each step of the incident resolution process, be sure to fill in the **CC Emails** option, and, if you'll connect by federation, log in before following the link in the email that AMS sends. After it is resolved, the AMS operations team documents the incident and resolution for future use.

For definitions of incident management terms, see AMS Key Terms.

To understand the escalation path of incidents, see Getting help.

For a description of AMS response to incidents, see AMS incident response.

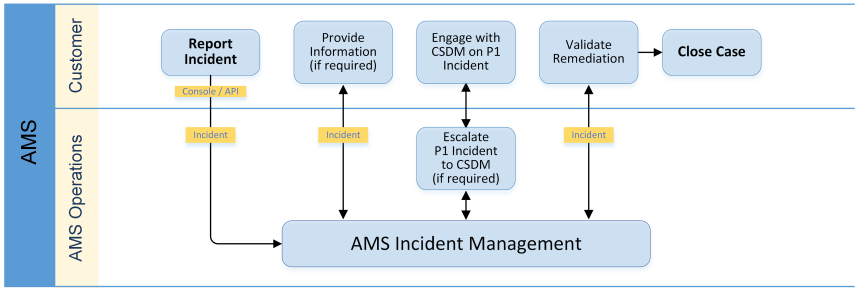
What is incident management?

Incident management is the process AMS uses to record, act on, communicate progress of, and provide notification of, active incidents.

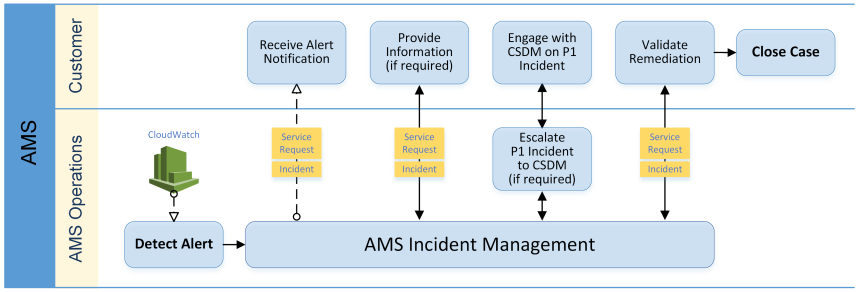
The goal of the incident management process is to ensure that normal operation of your managed service is restored as quickly as possible, the business impact is minimized, and all concerned parties are kept informed.

Examples of incidents include (but are not restricted to) loss of or degradation of network connectivity, a non-responsive process or API, or a scheduled task not being performed (for example, a failed backup).

The following graphic depicts the workflow of an incident reported by you to AMS.



This graphic depicts the workflow of an incident reported by AMS to you.



Incident priority

Incidents created in AWS Support center, console or Support API (SAPI), have different classifications than incidents created in the AMS console.

- Low: Non-critical functions of your business service, or application, related to AWS or AMS resources are impacted.
- Medium: A business service or application related to AWS and/or AMS resources is moderately impacted and is functioning in a degraded state.
- High: Your business is significantly impacted. Critical functions of your application related to AWS and/or AMS resources are unavailable. Reserved for the most critical outages affecting production systems.

> **Note**
> The AWS Support Console offers five levels of incident priority that we translate to the three AMS levels.

Problem vs incident

When AMS believes that an incident reveals a larger defect or misconfiguration and could recur, it is considered a problem rather than just an incident. In such cases, AMS undertakes analyses of the problem and offers suggestions to resolve the problem.

Incident management service commitments

Incident management service commitments

Event or action	Service commitment measurement
Case 1: An event with known impact is generated. AMS opens an incident and informs you. Case 2: AMS contacts you to confirm the impact of the event. You confirm the event is an incident. Case 3: You notice an issue and submit an incident report.	Clock for incident response and incident resolution starts when: Case 1: AMS creates an incident. Case 2: You confirm the alert is an incident. Case 3: You submit an incident. Service commitments depend on the priority of the incident created.
If you submit the incident, AMS sends a response to acknowledge it. If AMS creates the incident on your behalf, a separate incident response is not sent.	Clock for incident resolution continues ticking. Clock for incident response time stops when AMS sends the incident acknowledgement. **Note** Time spent waiting for inputs from you is excluded from incident resolution time calculations. For incidents that AMS creates, the initial response time is the time of the creation of the initial incident notification to you.
For the resources / services in question, AMS checks the health to verify if: • AMS detected event or customer submitted incident qualifies as an incident, and • the incident is correctly prioritized, and If an incident you submit is not correctly prioritized, AMS re-prioritizes it. If AMS changes an incident priority, a notification is sent to you along with reasoning behind the priority change. In certain cases, an issue you submitted may not qualify as an incident, depending on the cause. In those cases, AMS closes the incident and sends you a notification explaining the reason why. Irrespective of the event categorization, AMS works with you to assist as needed. To understand the rules for incident categorization, see Incident priority (p. 268).	In case incident priority changes, the service commitment for the new priority is applicable; clock continues ticking. In cases when an incident is closed because it does not meet the definition of an incident, service commitments are not applicable; clock stops.
AMS works on the incident to resolve it within service commitment. In certain cases, if AMS determines that unavailable stack(s) or resource(s) cannot be resolved in a timely manner, AMS will offer Infrastructure Restore as an option for resolution. Infrastructure Restore involves	Clock stops when: • AMS has restored all Unavailable services or resources pertaining to that Incident to an available state, or • an infrastructure restore is started.

Event or action	Service commitment measurement
re-deploying existing stack(s), based on the templates of the impacted stack(s), and initiating a data restore based on the last known restore point (EBS/RDS snapshot), unless otherwise specified by you. Ephemeral data on individual EC2 instances will be lost. If you do not authorize an Infrastructure Restore as recommended by AWS, you will not be eligible for a service credit for the associated Incident Resolution Time Service Commitment.	
Occasionally, AMS needs clarification from, or activity by, you to keep incident resolution efforts moving forward, unless you have a pre-defined, approved action. As a result, there is communication between AMS and you in order to resolve incidents	Clock stops when: AMS is waiting for a response or action from you. Clock restarts when: AMS receives the response from you or the action AMS requires of you is completed.

Incident management examples

Incident management examples.

Topics

The following examples describe using the AMS console to submit an incident. Once submitted, the AMS team works with you to resolve the incident per your Service Level Agreement (SLA).

Incident testing

When testing AMS incident submissions, we ask that you include in the subject text this flag: **AMSTestNoOpsActionRequired**. This flag lets AMS know that the incident submission is only for testing. When AMS operations engineers see that flag, they will not respond in any way to the incident submission.

Reporting incidents

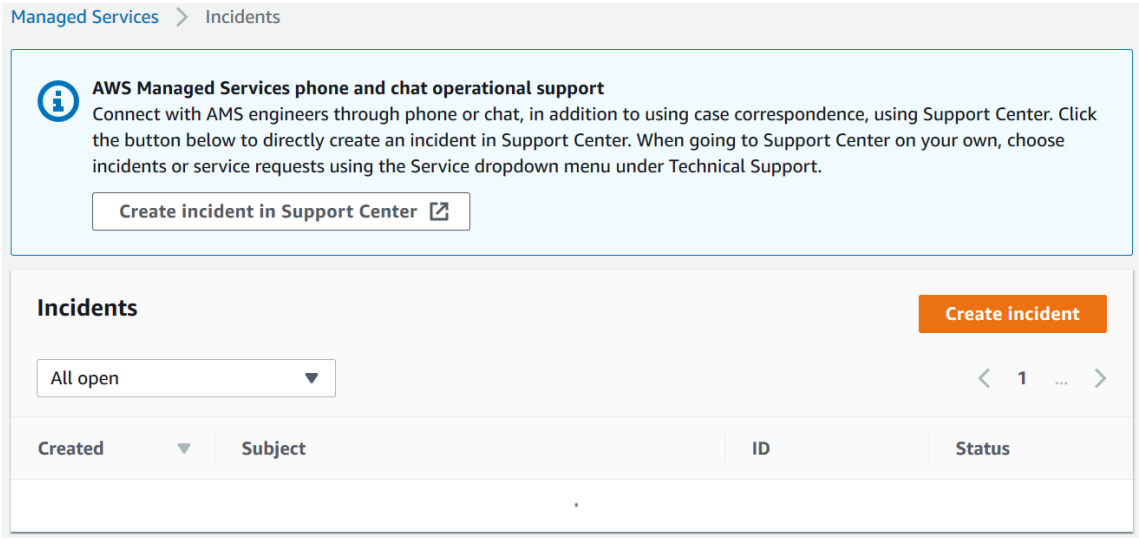
Use the AMS console to report an incident. It's important to create a new incident for each new issue or question. When opening cases related to old inquiries, it's helpful to include the related case number so we can refer to previous correspondence.

> **Note**
> If case correspondence strays from the original issue, an AMS operator might ask you to report a new incident.

To report an incident using the AMS console:

1. From the left navigation, choose **Incidents**

The **Incidents** list opens:

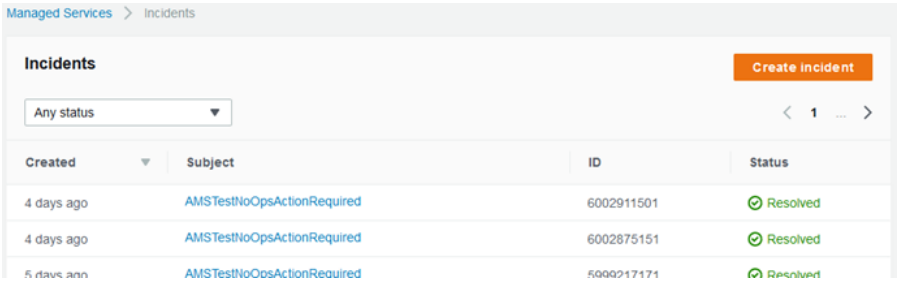


If your incident list is empty, the **Clear filter** option resets the filter to **Any status**.

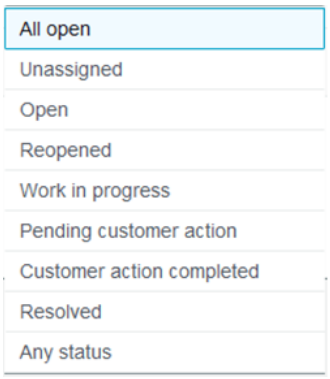
If you know you want to use phone or chat, click **Create incident in Support Center** to open the incident **Create** page in the AWS Support Center, auto-populated with the AMS service type.

> **Note**
> Phone calls initiated with AWS Support center are recorded, to better improve response. If the call drops, you must call back through the Support Center case, AWS has no mechanism for calling you back.

> **Important**
> Phone and chat support is designed to help with support cases, incidents and service requests. For RFC issues, use the correspondence option on the relevant RFC details page, to reach an AMS engineer.

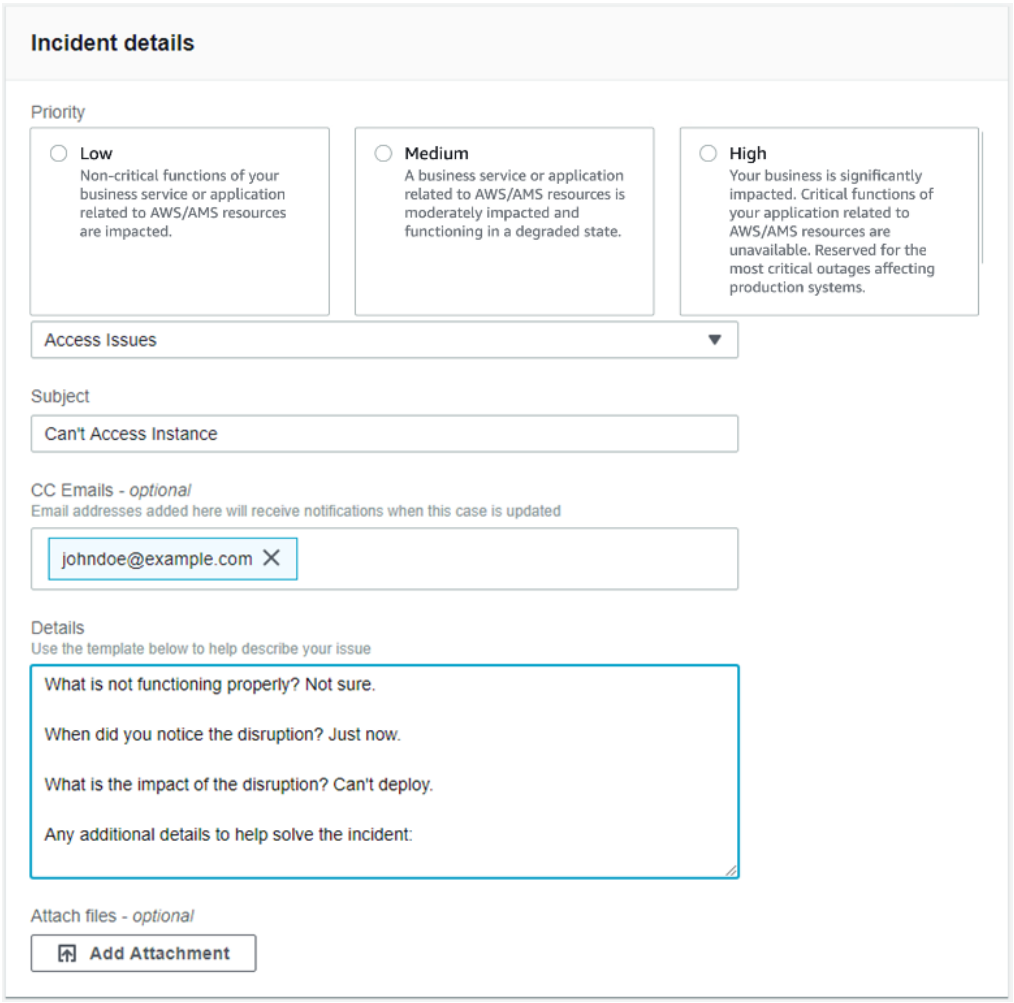


2. If you want to find an existing incident, select an incident status filter in the drop-down list.

	• All incidents that are not yet resolved. • A new incident that is not yet assigned. • An incident that has been assigned. • An incident that you reopened. • An assigned, complicated incident. • Incidents that require your feedback before the next step. • Incidents to which you have recently submitted information. • An incident that has concluded. • All incidents in the account.

3. Choose **Create**.

   The **Create an incident** page opens:



4. Select a **Priority**:

   - **Low**: Non-critical functions of your business service or application related to AWS/AMS resources are impacted.

- **Medium**: A business service or application related to AWS/AMS resources is moderately impacted and functioning in a degraded state.
- **High**: Your business is significantly impacted. Critical functions of your application related to AWS/AMS resources are unavailable. Reserved for the most critical outages affecting production systems.

5. Select a **Category**:

   - **Access Issues**: You have a question about accessing your AMS-managed resources.
   - **Availability**: A resource appears to be unavailable.
   - **Performance Issue**: A resource seems to be under-performing.
   - **Security Related**: You have a security concern about your AMS-managed resources.
   - **Other**: None of the other categories apply.

   Note
   If you are going to test incident functionality, AMS asks that you add the no-action flag (AMSTestNoOpsActionRequired) to your incident title.

6. Enter information for:

   - **Subject**: A descriptive title for the incident report.
   - **CC emails**: A list of email addresses for people you want informed about the incident report and resolution.
   - **Details**: A comprehensive description of the incident, the systems impacted, and the expected outcome of the resolution. Answer the pre-set questions, or delete them and enter any relevant information.

   To add an attachment, choose **Add Attachment**, browse to the attachment you want, and click **Open**. To delete the attachment, click the Delete icon: .

7. Choose **Submit**.

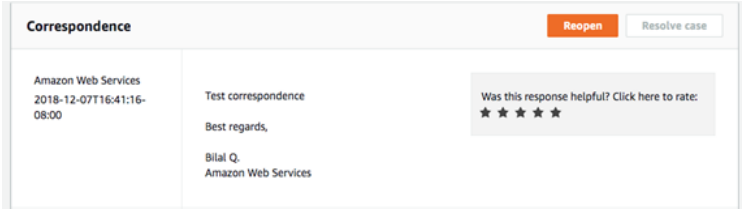
   A details page opens with information on the incident—such as **Type**, **Subject**, **Created**, **ID**, and **Status**—and a **Correspondence** area that includes the description of the request you created.

   Click **Reply** to open a correspondence area and provide additional details or updates in status.

   Click **Close Case** when the incident has been resolved.

   Click **Load More** if there is more correspondence than will fit on one page.

   Don't forget to rate the communication!



   Your incident displays on the **Incidents** list page.

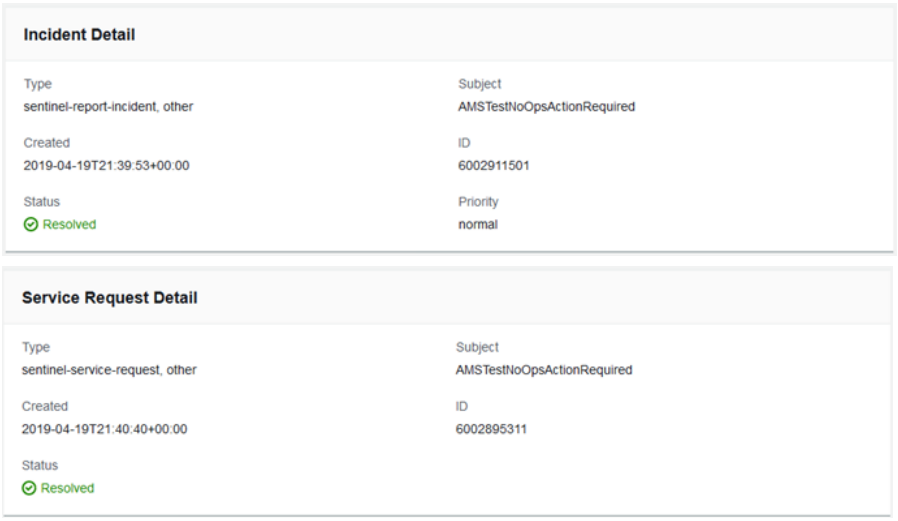
YouTube Video: How do I raise an incident from the AWS Managed Services console?

Monitoring and updating incidents

You can update, monitor, and review incident reports and service requests, both called cases, by using the AMS console, or programmatically using the AWS Support API, `DescribeCases` operation.

To monitor a case (incident or service request) by using the AMS console, follow these steps.

1. In the AMS console **Incident reports** or **Service requests** dashboard, browse to a case and choose the **Subject** to open a details page with current status and correspondences.



   When a reported incident or service request case is updated by the AMS operations team, you receive an email and a link to the incident in the AMS console so you can respond. You can't respond to incident correspondence by replying to the email.

   Important
   You must have entered an email address to receive notifications of state change for a service request or incident case. Notifications only go to the email address added to the case when it's created.
   The link in the notification email will not work unless you are using an email server on your AMS federated network. However, you can respond to the correspondence by going to your AMS console and using the case details page.

2. If there are many cases in the list, you can use the **Filter** option:

   - **All open** (default): Use this filter to see all cases that have not been resolved.
   - **Unassigned**: Use if you've just submitted the case and have not received any notice that the case state has changed. Note, incidents and service request cases are assigned at different promptness depending on the submitted priority (incidents) or your service level agreement (service requests).
   - **Open**: Use if you have received notice that the case is Pending Amazon action; this means that the case has been assigned but work has not yet begun.
   - **Reopened**: Use if you have received notice that the case was reopened (after having been resolved).
   - **Work in progress**: Use if you have received notice that an operator has begun to work on the case.
   - **Pending customer action**: Use if you have received an operator request for action on your part.
   - **Customer action completed**: Use if you have received notice that your action on the case has been processed.
   - **Resolved**: Use to view cases that you know have been resolved. Resolved cases are maintained in history for twelve months.
   - **Any status**: Use this filter to see all cases, regardless of status.

3. To check the latest status, refresh the page.
4. If there are so many correspondences that they do not all appear on the page, choose **Load More**.
5. To provide an update to the case status, choose **Reply**, enter the new correspondence, and then choose **Submit**.
6. To close out the case after it has been resolved to your satisfaction, choose **Close case**.

   Be sure to rate the service through the 1-5 star rating to let AMS know how we're doing!

Managing incidents with the AWS Support API

The AWS Support API enables you to create incidents and add correspondence to them throughout investigations of your issues and interactions with AWS Support staff. The AWS Support API models much of the behavior of the AWS Support Center. For more details about how you can use this AWS support service, see Programming an AWS Support Case.

Note
When using the AWS Support API, or SAPI, for AMS Advanced incidents, use this service code: `sentinel-report-incident`.

Responding to AMS-generated incidents

AMS proactively monitors your resources; for more information, see Monitoring and event management. Sometimes AMS identifies and creates an incident case, most often to notify you of an incident. In the event that action is required on your part to resolve an incident, AMS sends a notification to the contact information you have provided for the account. You respond to this incident in the same way as you would any other incident. You would usually respond to incidents via the AMS console; in some cases, contact by email or phone is required.

Note
AMS sends communications to your primary email address on your AWS account; we recommend adding an alternate Operations contact email alias to facilitate the incident management process. This is covered during the AMS onboarding process and related onboarding documentation. If you have provided AMS with non-resource based contacts (that you informed your CSDM of) during onboarding, those contact are used. For example, you could provide a list of contacts named "SecurityContacts" to your CSDMs/CAs to use for security-related incidents or notifications. Contact tags on your instances/resources are used for AMS-generated incidents, if you have provided your consent to CSDM for using tag information.
To learn more about this notification service, see Notifications.

Service request management

Topics

Service requests are communications to AMS created by you to ask for information or advice. A good example of a standard service request is to request guidance or help to configure an AMS service, like alarm manager, patch, and so forth. Look on the **Service requests** page of the AMS console for a list of your service requests and outbound service requests (service notifications) sent to you by AMS.

To learn more about outbound service requests, see Responding to an AMS-generated service request (notification) (p. 281).

You create an AWS Managed Services (AMS) service request by using the AMS console or programmatically by using the AWS Support API; for details, see AWS Support API. For AMS you use the service code `sentinel-service-request`.

After your service request is received by the AMS operations team and prioritized according to your service level agreement. To be kept informed at each step of the service request resolution process, be sure to fill in the **CC Emails** option, and, if you will connect by federation, log in before following the link in the email AMS sends.

What are service requests?

Service request management is the process AMS uses to record, act on, communicate progress of, and provide notification of, active service requests.

The goal of the service request management process is to ensure that your managed service is delivering what you need.

Examples of service requests include (but are not restricted to) request for a new change type, or a change in patch or log configuration.

How service request management works

Service requests are handled by the on-call AMS operations team.

After your service request is received by the AMS operations team, it's reviewed to ensure that the request is not more properly classified as an incident. If it should be classified as an incident, it's immediately reclassified and the AMS incident management team takes over and you're notified.

If the service request can be resolved with the submission of an RFC, the reviewing operator sends you an email requesting that you submit the appropriate RFC (details are provided).

If the AMS operator can resolve the service request, steps to do so are taken immediately. For example, if the service request is for architecture advice, or other information, the operator refers you to the appropriate resources or attempt to answer the question directly.

If the service request is out of scope for AMS operations, the operator either sends the request to your cloud service delivery manager so they can communicate with you, or to the appropriate AWS operations team, along with an email to you as to what steps are being taken.

The service request is not resolved until you have indicated that you're satisfied with the outcome.

> **Note**
> We recommend providing a contact email, name, and phone number in all cases to facilitate communications.

Service request management examples

Using the AMS console **Create Service Request** page, you can perform the following tasks:

- Create and update a service request
- Get a list of, and detailed information about, all of your submitted service requests
- Narrow your search for service requests by dates and incident identifiers, including requests that have been resolved
- Add communications and file attachments to your requests, and add email recipients for case correspondence
- Resolve service requests

- Rate service request communications

The following examples describe using the AMS console to create a service request.

Service request testing

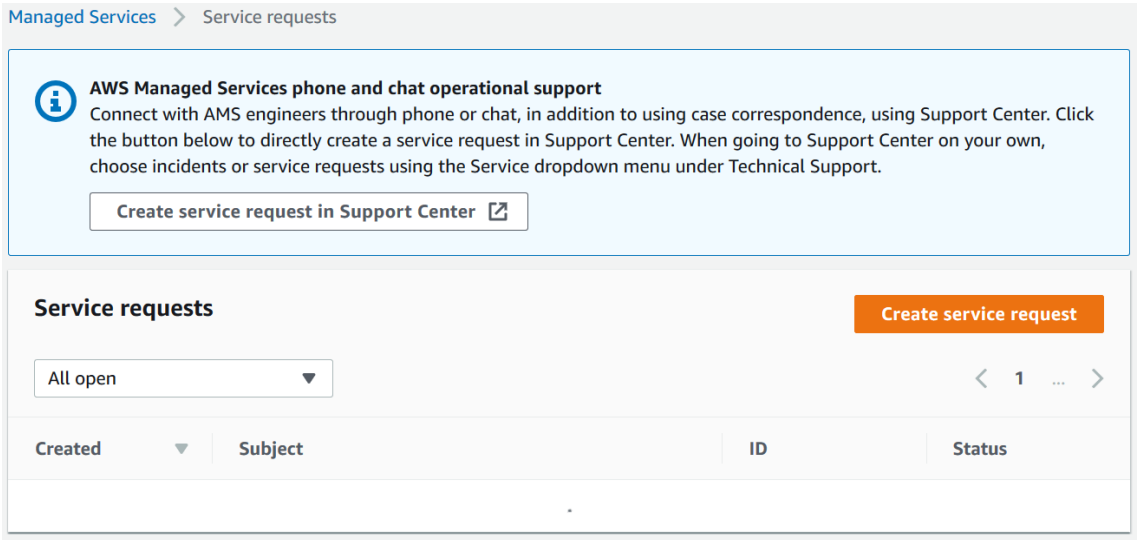
When testing AMS service requests, we ask that you include in the subject text this flag: **AMSTestNoOpsActionRequired**. This flag lets AMS know that the service request is only for testing. When AMS operations engineers see that flag, they will not respond in any way to the service request.

Creating a service request

To create a service request using the AMS console:

1. From the left navigation, choose **Service requests**.

   The **Service requests** list opens.



   If your service request list is empty, the **Clear filter** option resets the filter to **Any status**.

   If you know you want to use phone or chat, click **Create service request in Support Center** to open the service request **Create** page in the AWS Support Center, auto-populated with the AMS service type.

   Note
   Phone calls initiated with AWS Support center are recorded, to better improve response. If the call drops, you must call back through the Support Center case, AWS has no mechanism for calling you back.

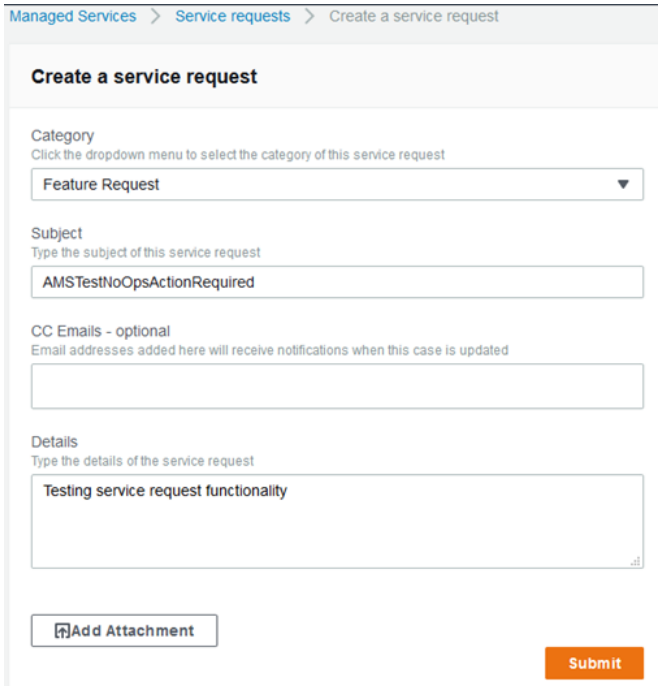
Important
Phone and chat support is designed to help with support cases, incidents and service requests. For RFC issues, use the correspondence option on the relevant RFC details page, to reach an AMS engineer.

2. If you want to find an existing service request, select a service request status filter in the drop-down list.

All open Unassigned Open Reopened Work in progress Pending customer action Customer action completed Resolved Any status	• All service requests that are not yet resolved. • A new service request that is not yet assigned. • A service request that has been assigned. • A service request that you reopened. • An assigned, complicated, service request. • Service requests that require your feedback before the next step. • Service requests to which you have recently submitted information. • A service request that has concluded. • All service requests in the account.

3. Choose **Create**.

   The **Create a service request** page opens.



4. Select a **Category**:

   - **Access**: Use this when you have a question about accessing your AMS-managed resources. To request access to an AMS-managed resource, submit an RFC with the AccessManagement category.
   - **Alert notification**: Use this when you have an alert and have not heard from AMS.
   - **Feature Request**: Use this to request that AMS add a feature.

- **General Guidance**: Use this for non-resource specific questions.
- **Security Related**: Use this when you have a security concern about your AMS-managed resources. Note that while we use encryption, you should exercise caution with the information you submit here.
- **Service Reporting Query**: Use this to request a specific report.
- **Other**: Use this when none of the other categories apply.

> **Note**
> If you are going to test service request functionality, AMS asks that you add the no-action flag (AMSTestNoOpsActionRequired) to your service request title.

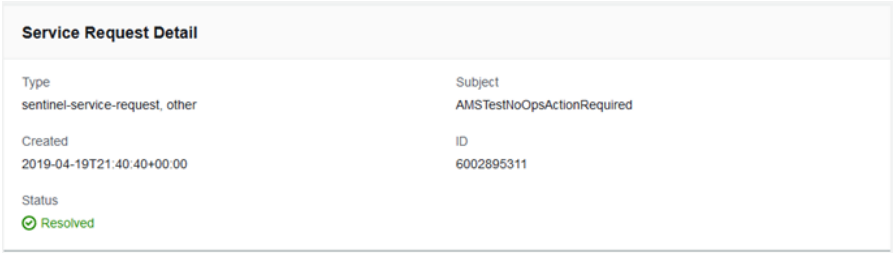
5. Enter information for:

   - **Subject**: This creates a link to the service request details on the list page.
   - **CC emails**: These emails receive correspondence in addition to your default email contacts.
   - **Details**: Provide as much information here as possible.

   To add an attachment, choose **Add Attachment**, browse to the attachment you want, and click **Open**. To delete the attachment, click the Delete icon: .

6. Choose **Submit**.

   A details page opens with information on the service request--such as **Type**, **Subject**, **Created**, **ID**, and **Status**--and a **Correspondence** area that includes the description of the request you created.



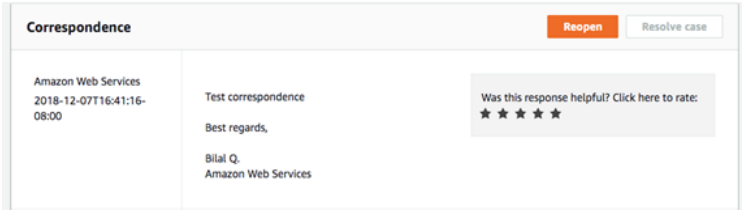
   Additionally, your service request displays on the **Service Request** list page. Use this when you have an alert but have not yet heard from AMS.

   Click **Reply** to open a correspondence area and provide additional details or status updates.

   Click **Resolve Case** when the service request has been resolved.

   Click **Load More** to view additional correspondences that do not fit on the inital page.

   Don't forget to rate the communication!



For billing-related queries, use the **Other** Category in the AMS console; the `ChangeTypeId` `ct-1e1xtak34nx76` in the AMS CM API, or the `IssueType=AMS` in the AWS Support API.

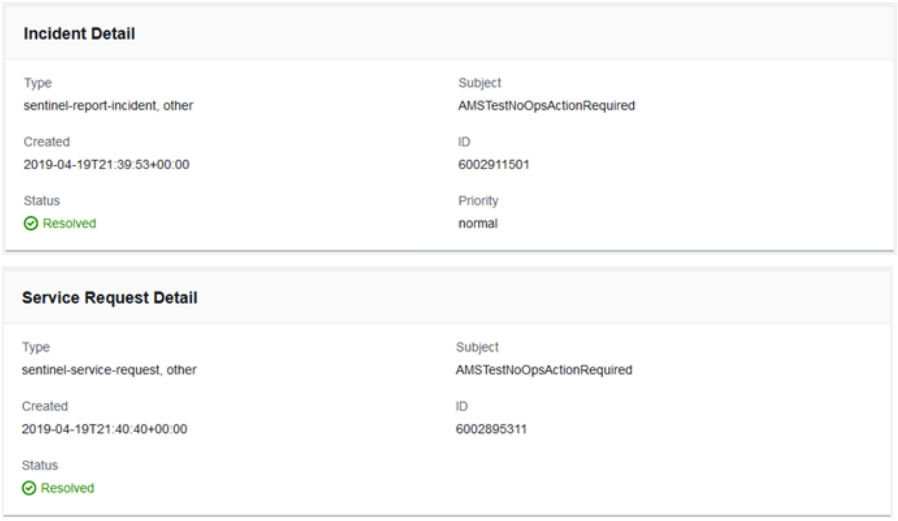
YouTube Video: How and when to raise service requests from AWS Console and what are it's Service Level Objectives?

Monitoring and updating service requests

You can update, monitor, and review incident reports and service requests, both called cases, by using the AMS console, or programmatically using the AWS Support API, `DescribeCases` operation.

To monitor a case (incident or service request) by using the AMS console, follow these steps.

1. In the AMS console **Incident reports** or **Service requests** dashboard, browse to a case and choose the **Subject** to open a details page with current status and correspondences.



   When a reported incident or service request case is updated by the AMS operations team, you receive an email and a link to the incident in the AMS console so you can respond. You can't respond to incident correspondence by replying to the email.

   Important
   You must have entered an email address to receive notifications of state change for a service request or incident case. Notifications only go to the email address added to the case when it's created.
   The link in the notification email will not work unless you are using an email server on your AMS federated network. However, you can respond to the correspondence by going to your AMS console and using the case details page.

2. If there are many cases in the list, you can use the **Filter** option:

   - **All open** (default): Use this filter to see all cases that have not been resolved.
   - **Unassigned**: Use if you've just submitted the case and have not received any notice that the case state has changed. Note, incidents and service request cases are assigned at different promptness depending on the submitted priority (incidents) or your service level agreement (service requests).
   - **Open**: Use if you have received notice that the case is Pending Amazon action; this means that the case has been assigned but work has not yet begun.
   - **Reopened**: Use if you have received notice that the case was reopened (after having been resolved).
   - **Work in progress**: Use if you have received notice that an operator has begun to work on the case.
   - **Pending customer action**: Use if you have received an operator request for action on your part.
   - **Customer action completed**: Use if you have received notice that your action on the case has been processed.

- **Resolved**: Use to view cases that you know have been resolved. Resolved cases are maintained in history for twelve months.
- **Any status**: Use this filter to see all cases, regardless of status.

3. To check the latest status, refresh the page.
4. If there are so many correspondences that they do not all appear on the page, choose **Load More**.
5. To provide an update to the case status, choose **Reply**, enter the new correspondence, and then choose **Submit**.
6. To close out the case after it has been resolved to your satisfaction, choose **Close case**.

   Be sure to rate the service through the 1-5 star rating to let AMS know how we're doing!

Responding to an AMS-generated service request (notification)

AMS patch management sends service requests (aka service notification) to you prior to your set maintenance window; for more information, see AMS maintenance window. AMS also sends service notifications to you when there is a chance that your infrastructure will be impacted by an AWS service or when an EC2 instance in your account may need to be rebooted; for more information, see Service notifications.

> **Note**
> AMS sends communications to your primary email address on your AWS account; we recommend adding an alternate Operations contact email alias to facilitate the service request/notification management process. This is covered during the AMS onboarding process and related onboarding documentation.

Change management

Important
The *Change management* chapter for AMS Advanced has been moved into a separate user guide. You can find all of the topics at the following links:

- What is change management?
- Understanding RFCs
- Understanding change types
- Resource scheduler
- Using tags
- Examples
- Tutorials
- RFC failure troubleshooting

For detailed information on RFCs and change types, or to view a complete list of change type examples, refer to the AMS Change Type Examples Guide.

For a list of AMS reserved prefixes not to be used in tag or other names, see AMS reserved prefixes (p. 39).

For information on each change type, including schemas, refer to the AMS Change Type Reference.

Note
All change management API calls are recorded in AWS CloudTrail. For more information, see Accessing your logs.

AWS Managed Services modes

Use this to help you select the appropriate AWS Managed Services (AMS) mode for hosting your applications, based on your desired combination of flexibility and prescriptive governance to achieve your business outcomes.

The intended audience for this information is:

- Customer teams responsible for the strategy and governance of their landing zone. This information will help the team lay out the foundation of an AMS-managed landing zone, with the AMS modes they'd like to offer to their internal and external customers.
- Business and application owners tasked with migrating their application to AMS. This information will help with planning application migration, with the appropriate AMS mode to migrate/host their application. Note, the same application can be hosted in more than one AMS mode during different phases of its Software Development Life Cycle (SDLC) lifecycle.
- AMS partners tasked with guiding customers on the different options to build and migrate to AMS.

This information assumes that you have already made the decision to leverage AMS to accelerate your journey to the cloud. Refer to this paper at two points in your cloud migration journey: First, during the foundation phase of setting up the AMS-managed platform. Second, when you are transitioning from

the foundation to the migration phase of your cloud adoption journey, just after onboarding to AMS is complete and you're focusing on application governance and operations.

Types of modes and accounts in AMS

AMS modes can be defined as the ways of interacting with the AMS service under the specific governance framework for each mode. The landing zone differences, multi-account landing zone or MALZ and single-account landing zone or SALZ are noted. The modes are:

- AMS-managed: Standard change management (CM) mode and Operations on demand (OOD)
- AMS-managed: Direct Change mode
- AMS-managed: AWS Service Catalog on AMS
- AMS-managed: Self Service Provisioning (SSP) mode
- AMS-managed: Developer mode
- Customer Managed mode

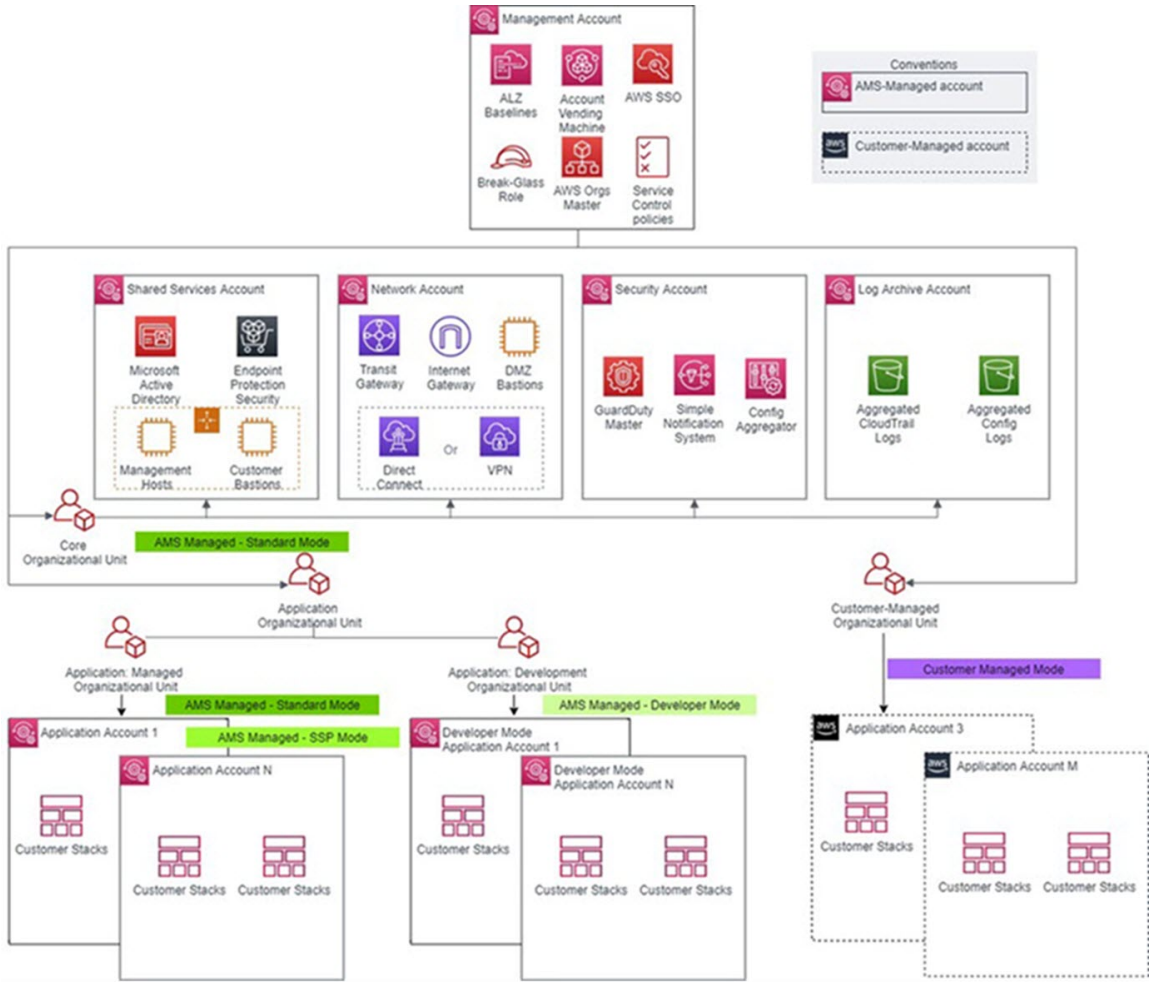
AMS feature	Standard CM mode / OOD*	Direct Change mode	AWS Service Catalog	Self-service provisioning / Developer mode	Customer Managed
Landing Zone Configuration	MALZ and SALZ	MALZ and SALZ	MALZ and SALZ		
Change Management	Change scheduling, review of manual changes, and change record	Same as Standard CM for high-risk changes like IAM or security groups	None		
Logging, Monitoring, Guardrails, and Event Management	Yes (supported resources)			No	
Continuity management	Yes (supported resources)			Not applicable / No	No
Security management	Instance level security controls and account level controls			Account level controls	AWS Org level controls
Patch management	Yes			Not applicable / No	No
Incident and problem management	Response and resolution SLA for AMS supported resources			Response SLA for resulting resources	No
Reporting	Yes			No	
Service request management	Yes			Support requests only	No

*Operations On Demand (OOD) has an offering for customers using the Standard CM mode to manage their changes through dedicated resourcing. For more details, see the Operations on Demand catalog of offerings and talk to your cloud service delivery manager (CSDM).

AMS multi-account landing zone (MALZ) gives you the option to automatically provision application accounts (or resource accounts) under the default Organizational Units (OU): Customer Managed OU, Managed OU, or Development OU. The infrastructure provisioned in the application accounts created under each of these OUs is subject to the specific AMS mode offered by those foundational OUs. It is common to find a mix of two or more modes in the same application account. For example: Standard mode and SSP mode can coexist in an AMS managed account that hosts pipeline architecture consisting of API Gateway and Lambda for trigger functions, and EC2, S3, and SQS for ingestion and orchestration. In this case, SSP mode would apply to Lambda and API Gateway.

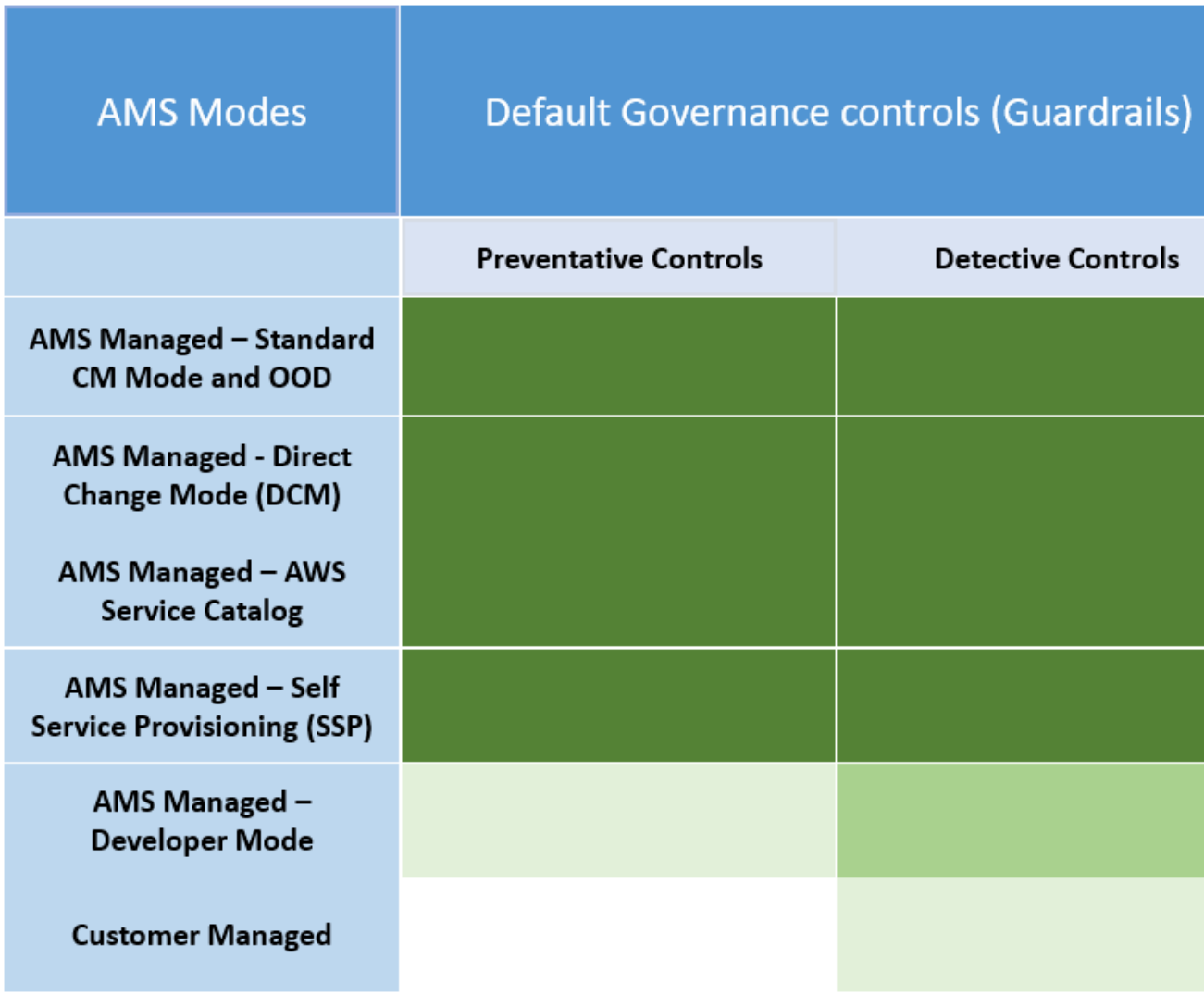
Figure 1 presents how different modes are offered through the foundational OUs in AMS. When requesting a new application account in AMS, you must select the OU for the account.

MALZ architecture and associated AMS modes



AMS leverages the foundational OUs based on AWS best practices as a way to logically manage accounts using Service Control Policies (SCPs). This serves as a way to enforce the governance framework with each AMS mode. Any governance and security guardrails (in the form of SCPs) applied to the foundational OUs also get applied to the custom/child OUs automatically. Additional SCPs can be requested for the child OUs. It is important to understand that application accounts are not the same as modes. Modes are applied to the infrastructure provisioned within the accounts and define the operational responsibilities between AMS and customers.

Figure 1: MALZ architecture and associated AMS modes



Note
"Restrictive" implies that you can request custom policies for these OUs, they are approved by AMS on a case-by-case basis to ensure they don't interfere in AMS's capabilities to provide operational excellence. For a detailed list of AMS guardrails see AMS Guardrails in the user guide.

AMS-managed Standard Change Management (CM) mode

This mode provides standardized governance supported by pre-defined guardrails and a strict set of controls that make accounts in this mode operationally secure.

There can be a learning curve in this mode as application development teams adopt the AMS processes to work within the boundaries of AMS change management, or use AWS Service Catalog to provision resources.

AMS-managed Self Service Provisioning (SSP) mode

This mode provides full access to native AWS service and API Capabilities in AMS managed accounts. You access services through standardized, scoped down, IAM roles. AMS provides service requests and incident management. Alerting, monitoring, logging, patch, back up, and change management are your responsibility. In many cases, Self-Service Provisioning services (SSPS) are self-managed, or serverless, and don't require management of certain operational tasks like patching. You benefit from using these services within the environment boundary defined by AMS guardrails and any IAM changes (including service linked roles, service roles, cross-account roles, or policy updates) need to be approved by AMS Operations to maintain the baseline security of the platform. You can leverage CloudFormation templates to automate deployment of these services but this is not supported for all SSP services currently. Examples:

- You deploy a data lake using the AMS-managed SSP mode that leverages EC2, S3, Glue and Lambda services. In this case, Glue and Lambda are considered Self Service Provisioning services and you are responsible for monitoring, logging, patch, back up, and change management.
- You deploy containerized applications using this mode; services like ECS, and EKS on Fargate, are SSP services and task monitoring, logging, container level security are the your responsibility. To use additional features like Service Accounts for EKS, you request a change with AMS to enable IAM roles and policies for the specific cluster. You do not need to explicitly request accounts to be provisioned in SSP mode. When you request any of the SSP services be enabled in your application account, SSP mode is automatically activated for those services. Not all AWS services are available as SSP services, a complete list of SSP services can be found in the AMS Service Description document.

  For information on all available self-service provisioning services, see Self-Service Provisioning Services (SSPS).

AMS-managed Developer mode

This mode provides two options for provisioning infrastructure, either AMS change management, or access to native AWS service APIs via a highly permissive IAM role ("Developer role"). Resources provisioned through the highly permissive role are managed through a less-restrictive set of guardrails, enforced through detective controls, and have fewer preventative controls.

Depending on which option is selected, you can take on more operational responsibility while also gaining flexibility. It is important to note that Developer mode does not automatically grant access to any AWS service, but only those that have been onboarded to AMS. The two most common use cases for building in this mode are described next. In both use cases, Developer mode may co-exist with Standard mode and/or SSP mode in the same application account.

- Use Case: As a way to expedite deployment or migration of applications in AMS, with the objective that production-ready workloads will operate in AMS Managed – Standard or SSP mode. In this case, you utilize a mix of Developer mode in pre-production phase, and Standard mode or SSP mode in production phase, for the same application. Working through AMS change management may be considered an impediment for application teams due to the learning curve, or the speed of processing manual RFCs. With Developer mode, you can bypass the AMS change management system, while iterating in an account that is protected by the baseline AMS security-hardened network and permissions boundaries. Once the pre-production application design and configuration is finalized, you have the option to re-deploy the production-ready application using CloudFormation templates, or custom AMIs, that are ingested via the AMS change management system. The infrastructure created as an output is consequently managed by AMS.

  Example: Setting up a CICD pipeline based on open source, or native AWS services, to deploy code to multiple accounts in AMS Managed Landing Zone can save time by building in Developer mode and leveraging the "Developer IAM role" to optimize configurations and permissions. Once finalized, you can re-deploy the infrastructure through AMS change management. Such a pipeline could also be built

and iterated upon in Standard mode or SSP mode, however you would need to plan for additional time in processing manual RFCs related to IAM permissions.

- Use Case: As a way to operationalize configurations and tools that are not supported by the AMS change management system. In this case, AMS Managed – Developer mode will be used to host production workload, with you taking over operational responsibility for the infrastructure provisioned using the "developer IAM role". It is highly recommended that you leverage the AMS change management to provision infrastructure that can be operated by AMS, like EC2, ELB, EBS, S3, etc, so that you can offload operational responsibility for those services to AMS. In this case the application operates in a mixed mode configuration with both Developer mode and Standard mode in the same application account. You can then focus on operational support for services not in scope, this includes monitoring, patching, and continuity management.
- Use Case: Extending a Terraform-based enterprise code repository in AMS can utilize Developer mode to provision infrastructure; however, you are responsible for operating any infrastructure provisioned through Terraform.
- Use Case: You want to deploy EKS on EC2 instead of EKS on Fargate (which is offered in SSP mode). In this case, you can use Developer mode to operate you desired configuration in production while leveraging the security offered by detective controls in AMS Managed Landing Zone.

  For usage information, see Developer mode.

  Note
  Self-Service Provisioning (SSP) mode and Developer mode may both appear to be a suitable fit for an application that has complex architecture rooted in native AWS Services. When architecting workloads, you make trade-offs between operational excellence and agility, based on your business context. This is a good way to think about selecting SSP mode or Developer mode for your application. The selection may also change based on the SDLC phase of the application. For example: When the application is production-ready, then SSP mode maybe a more appropriate option due to stricter AMS guardrails in this mode. The guardrails are enforced in the form of preventative controls like RFC-based change control for IAM updates and SCPs at the application OU level. These business decisions can drive your engineering priorities. You might optimize to increase flexibility for application owners in "pre-prod" phase at the expense of governance and operational support.

AMS-managed Direct Change mode

AMS Direct Change mode (DCM) extends AMS Advanced change management by providing native AWS access to AMS Advanced Plus and Premium accounts to provision and update AWS resources. Use DCM to provision AMS-managed resources using AWS CloudFormation, and to update any AMS-managed resource through the AWS Management Console, AWS APIs or AWS CloudFormation. Use DCM to accelerate migrations by deploying changes via native AWS access.

While DCM unlocks permissions to configure AMS-managed resources using the AWS Management Console, AWS APIs AWS CloudFormation, it also preserves the security boundary of the account. With DCM you can use common tool sets between AWS and AMS migration projects. Depending on use case, you can choose to use AWS CloudFormation during accelerated migrations, or RFCs when you need to leverage AMS curated deployment patterns.

Use DCM to:

- Provision and update fully managed stacks via direct AWS CloudFormation permissions
- Update AMS-managed resources through direct AWS API permissions

To see more use case details for DCM usage, see Direct Change mode.

AMS-managed AWS Service Catalog

AWS Service Catalog provides you with an alternative to the AMS Advanced request for change (RFC) process for provisioning and updating resources in your AMS-managed accounts. AMS Advanced manages all of the infrastructure operations tasks needed to run AWS at scale for all infrastructure resources provisioned through AWS Service Catalog including security, compliance, provisioning, availability, patch, monitoring, alerting, reporting, incident response, and cost optimization.

Utilizing AWS Service Catalog in your AMS-managed account provides you with a mechanism to centrally manage commonly deployed IT services, and helps you achieve consistent governance, while enabling users to quickly deploy only the approved IT services they need into their managed environments.

AMS Customer managed mode

This mode provides a governance model that is flexible and can be adapted to your requirements. This can be considered a fallback option for services and applications that AMS is unable to operate for you. AMS does not operate infrastructure hosted in accounts created under this mode. However, you can leverage centralized multi-account management in this mode. The following Multi-Account Landing Zone features can be leveraged in this mode:

- Automated Account deployment
- Connectivity through Transit Gateway in networking account
- AMS Config Rules library
- Store copies of logs in logging account
- Aggregation of customer managed Guard Duty alerts to Security account
- Consolidated Billing
- Enablement of custom Service Control Policies.

For example: If you want to run workloads on Ubuntu Pro, which is not an Operating System managed by AMS, you could use a customer managed account for hosting it. You can also consolidate workloads through customer managed accounts, to take advantage of the bulk discount on Reserved Instances/ Sharing Plans available through sharing across an AWS organization.

AMS modes and applications or workloads

Selecting the appropriate AMS mode for your applications or workloads and deciding the Organizational Unit under which you host your application. You could do this by requesting a new application account or hosting in an existing application account.

You should consider operational and governance requirements for your applications when selecting the right fit. The selection of the appropriate AMS mode for each application or workload depends on the following factors:

- The type of SDLC lifecycle function that the environment will provide (e.g., sandbox with unmoderated changes, UAT with some frequent changes, production with minimal changes and highly regulated)
- The governance policies needed (enforced through SCPs at the OU level)
- Operational Model (if you want to own the operational responsibility or want to outsource that to AMS)
- The desired business outcomes, like time to operate in the cloud, and cost of operations.

The following table outlines key considerations for application owners to help decide on the most suitable AMS mode. Application owners should include an assessment phase ahead of application migration to fully understand which mode applies to their specific application. Example: For applications based on cloud-native services or serverless architecture, the best option could be to start building

and iterating in Developer mode and deploy the final Infrastructure as Code using AMS Managed – SSP mode. In this case light re-factoring may be required to ensure that any CloudFormation templates created for automated deployment meet the ingest guidelines laid out by AMS. Additionally, any IAM permissions need to be approved by AMS Security to ensure they follow the least privilege model.

The AMS mode selected to host the application, can help enable you to build towards you desired cloud operating model.

Note
More than one cloud operating model can existing in a single AMS Managed Landing Zone based on the different AMS modes selected to host the applications.

Decision issues	Standard CM mode / OOD*	AWS Service Catalog	Direct Change mode	Self-service provisioning	Developer mode	Customer Managed
Operational readiness						
Logging, Monitoring and Event Management	AMS responsible for all managed infrastructure			Customer responsible for Self-Service Provisioned Services (SSP)	Customer responsible for resources provisioned using developer IAM role outside AMS CM system	Customer responsible
Continuity Management	AMS responsibility to execute backup plan selected by customer			Customer responsible for Self-Service Provisioned Services (SSP)	Customer responsible for resources provisioned using developer IAM role outside AMS CM system	Customer responsible
Instance Level Access Management	AMS-managed through one-way AD trust with on-prem domain. Requires managed infrastructure to join AMS domain			Not applicable	Customer responsible for resources provisioned using developer IAM role outside AMS CM system	Customer responsible
Security Management and Account Level Access Management	AMS responsibility for all managed accounts			AMS responsible for all managed accounts	Customer responsible for resources provisioned using developer IAM role outside AMS CM system	Customer responsible

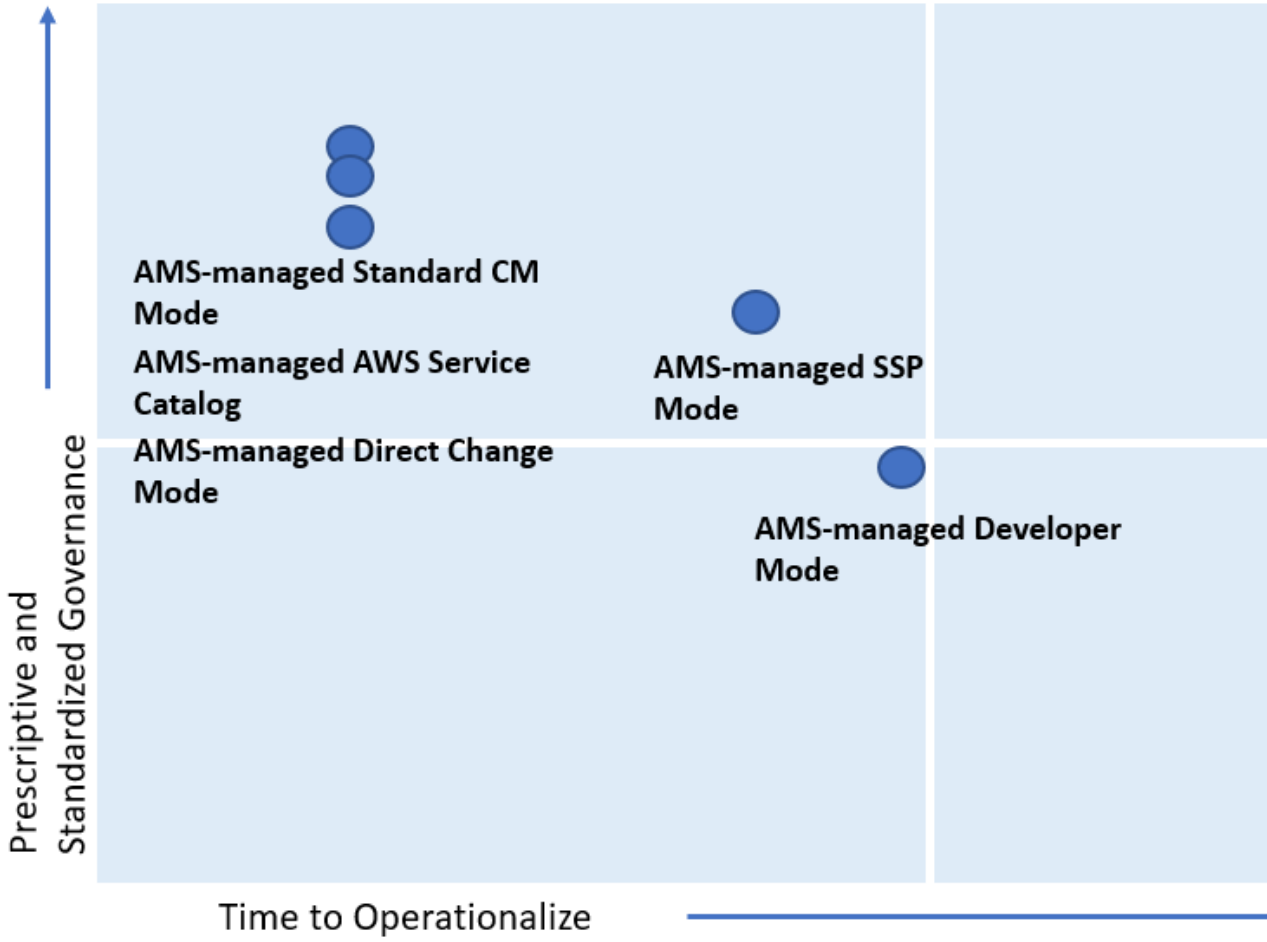
Decision issues	Standard CM mode / OOD*	AWS Service Catalog	Direct Change mode	Self-service provisioning	Developer mode	Customer Managed
Patch Management	AMS responsibility for all managed accounts			Customer responsible for Self-Service Provisioned Services (SSP)	Customer responsible for resources provisioned using developer IAM role outside AMS CM system	Customer responsible
Change Management	AMS responsibility for all managed accounts			Customer responsible for Self-Service Provisioned Services (SSP)	Customer responsible for resources provisioned using developer IAM role outside AMS CM system	Customer responsible
Provisioning Management	Prescriptive and standardized for the provisioning options offered in AMS	Flexibility to directly use AWS service API for AWS Service Catalog following AMS prescriptive standards	Flexibility to directly use AWS service API following AMS prescriptive standards	Flexibility to directly use AWS service APIs for SSP services	Flexibility to directly use AWS service API for provisioning	Customer responsibility
Incident Management and Audit	AMS responsibile for all managed accounts				Customer responsible for resources provisioned using developer IAM role outside AMS Change Management System	Customer responsible
GuardRails and Shared infrastructure (Network) and Security Framework	Prescriptive and standardized leveraging AMS Core Accounts					Flexible and bespoke leveraging AMS Core Accounts
Application readiness						

Decision issues	Standard CM mode / OOD*	AWS Service Catalog	Direct Change mode	Self-service provisioning	Developer mode	Customer Managed
Application refactoring	Light refactoring is needed				Light refactoring is needed (if provisioned using AMS Standard CM)	No need for refactoring
Support for AWS services	Limited to what is supported by AMS					Not limited
Business considerations						
Time to operational readiness	Three to six months			6 months + dependent on customer application operations competencies		6-18 months dependent on customer infrastructure and application operations competencies
Costs	$$$$			$$$	$$	$
Application examples	Webserver with 3 tier stack, apps with compliance and regulatory requirements			Webserver using API Gateway, containerized application leveraging ECS/EKS	Iterating/ optimizing on Data Lake application that uses Lambda, Glue, Athena, etc	De-centralized accounts/ applications like sandbox, third party managed applications

*Operations On Demand (OOD) has an offering for customers using the Standard CM mode to manage their changes through dedicated resourcing. For more details, see the Operations on Demand catalog of offerings and talk to your cloud service delivery manager (CSDM).

Note
The price comparison between SSP mode and Developer mode assumes that the same AWS services are provisioned.

Comparing AMS Modes against business and IT objectives



As shown, if you are looking for a highly controlled and standardized governance model for you applications, then AMS-managed Standard Change, AWS Service Catalog, or Direct Change modes are the best fit. If you require a bespoke governance model with a focus on application innovation without the need for operational readiness, select Customer Managed mode. With Customer Managed mode, it could take you a longer time to operationalize you applications as you bear the responsibility to establish people, processes, and tools to support operational capabilities such as Incident Management, Configuration Management, Provisioning Management, Security Management, Patch Management, etc.

Real world use cases for AMS modes

Examine these to help determine how to use AMS modes.

- **Use Case 1, business imperative to lower costs with a time-sensitive data center exit**: An enterprise with a compelling business event, like a data center exit, is interested in re-hosting their on-prem applications on the cloud. Most of the on-prem inventory consists of Windows and Linux servers with a mix of operating system versions. In doing so, the customer also wants to take advantage of cost savings that moving to the cloud offers and improving the technical and security posture of their applications. The customer wants to move fast but does not have the in-house cloud operations expertise built out yet. The customer has to find a balance of refactoring, too much refactoring can be risky against a tight timeline. However, with some refactoring, like updating OS versions and optimizing databases, applications can achieve the next level of performance. In this example, the customer can select AMS Managed Standard mode to re-host most of their applications. AMS provides

infrastructure operations, while also guiding the customer operations teams on best practices on securely operating in the cloud.

AMS-managed AWS Service Catalog and AMS-managed Direct Change mode gives the customer an extra flexibility while achieving the same business outcomes and objectives. In addition, the customer can use the AMS Operations On Demand (OOD) offering to have dedicated AMS operations engineers to prioritize the execution of requests for change (RFCs).

While offloading the undifferentiated infrastructure operational tasks (patching, backups, account management, etc) to AMS, the customer can continue to focus on optimizing their application and ramp-up their internal teams on cloud operations. AMS provides monthly reports to the customer on cost savings, and makes recommendations on resource optimizations. In this use case, if there were end-of-life applications hosted on legacy OS versions like Windows 2003 and 2008, that the customer decided not to re-factor, those can also be migrated to AMS and hosted in an account that leverages Customer Managed mode.

- **Use Case 2, building a data lake with Lambda, Glue, Athena within the secure AMS boundary**: An enterprise is looking to set up a Data Lake to meet the reporting needs for multiple applications in AMS. The customer wants to use S3 buckets for the storage of datasets and AWS Athena to query against the dataset for each report. S3 and AWS Athena will be deployed in separate AMS Managed accounts. The account with S3 also has other services like Glue, Lambda, and Step Functions to build a data ingestion pipeline. Glue, Lambda, Athena, and Step Functions are considered Self-Service Provisioning (SSP) services in this case. The customer also deployed an EC2 instance in the account that acts as an ad hoc tooling/scripting server. The customer starts by requesting AMS to enable the SSP services in their AMS Managed account. AMS provisions an IAM role for each service that the customer can assume, once the role is onboarded to the customer's federation solution. For ease of management, the customer can also combine the policies for the separate IAM roles into one custom role, alleviating the need to switch roles when working between the AWS services. Once the role is enabled in the account, the customer is able to configure the services as per their requirements. However, the customer must work with the AMS change management system to request additional permissions, depending on their use case.

  For example, for access to Glue Crawlers, additional permissions are needed by Glue. Additional permissions will also be needed to create event sources for Lambda. The customer will work with AMS to update IAM roles to allow cross-account access for Athena to query S3 buckets. Updates to service roles or service-linked roles will also be needed through AMS change management for Lambda to call the Step Functions service, and Glue to read and write to all S3 buckets. AMS works with customers to ensure that the least-privilege access model is followed and the IAM changes requested are not overly permissive and opening up the environment to unnecessary risk. The customer’s data lake team spends time planning for all IAM permissions needed for the services specific to the customer’s architecture and requests AMS to enable them. This is because all IAM changes are processed manually and undergo review from the AMS Security team. Time to process these requests should be accounted for in the application deployment schedule.

  As the SSP services are operational in the account, the customer can request support and report issues through AMS incident management and service requests. However, AMS will not actively monitor performance and concurrency metrics for Lambda, or job metrics for Glue. It is the customer’s responsibility to ensure appropriate logging and monitoring is enabled for SSP services. The EC2 instance and S3 bucket in the account are fully managed by AMS.

- **Use Case 3, quick and flexible set up of a CICD deployment pipeline in AMS**: A customer is looking to set up a Jenkins-based CICD pipeline to deploy code pipeline to all application accounts in AMS. The customer may find it most suitable to host this CICD pipeline in the AMS-managed Direct Change mode (DCM) or AMS-managed Developer mode because it gives them flexibility to set up the Jenkins server with required custom configuration on EC2, with the desired IAM permissions to access CloudFormation and S3 buckets that host the artifact repository. While this can also be done in the AMS Managed- Standard mode, the customer team would need to create multiple manual RFCs for IAM roles to iterate on the least permissive set of approved permissions, which are manually reviewed by AMS. DCM allows the customers to achieve their operational goals on AWS while avoiding the need

to create multiple manual RFCs for IAM roles, when using AMS-managed Standard CM mode, to iterate on the least permissive set of approved permissions, which are manually reviewed by AMS. This would take time as well as education on the customer's part to ramp up AMS processes and tools. Working with Developer mode, the customer can start with a "developer role" to provision infrastructure using native AWS APIs. The quickest and most flexible way to set up this pipeline would be to use AMS Managed-Developer mode. Developer mode gives the quickest and easiest way, while compromising on operational integration, while DCM is less flexible but does provide the same level of operational support as Standard CM mode.

- **Use Case 4, bespoke operating model within the AMS foundation**: A customer is looking at a deadline-driven data center exit and one of their enterprise applications is fully managed by a third party MSP, including application operations and infrastructure operations. Assuming that the customer does not have time in the schedule to re-factor this application so that it can be operated by AMS, Customer Managed mode is a suitable option. The customer can take advantage of the automated and quick set up of AMS managed Landing Zone. They can leverage the centralized account management that controls account vending and connectivity through the centralized networking account. It also simplifies their billing by consolidating charges for all customer managed accounts through the AMS Payer account. The customer has flexibility to set up their bespoke access management model with the MSP separate from standard access management used for AMS Managed accounts. This way, using Customer Managed mode, they can set up an AMS managed environment while meeting their business requirement of vacating their on-prem environment. In this case, if the customer also has Windows-based applications that they are migrating to the cloud, and choose to move them to a Customer Managed account, the customer is responsible for creating a cloud operating model. This can be complex, expensive, and time consuming depending on the customer's ability to transform traditional IT processes and train people. The customer can save time and cost by "lift and shift" of such workloads to an AMS Managed account and offload infrastructure operations to AMS.

  Note
  Customers may sometimes feel the need to move application accounts between the governance framework of Standard or SSP mode and Developer mode. For example, customers may host an application in AMS Managed mode as part of initial lift and shift migration, but overtime want to re-write the application to optimize it for cloud-native AWS services. They could change the mode of the pre-prod account from AMS Managed - Standard to AMS Managed-Developer, giving them the flexibility and agility for provisioning infrastructure. However, once infrastructure provisioning changes have been made using the "developer role", the same infrastructure cannot be moved back to AMS Managed – Standard mode. This is because AMS cannot guarantee operations of infrastructure that was provisioned outside of the AMS change management system. Customers may need to create a new application account that offers AMS Managed – standard mode and then re-deploy the "optimized" infrastructure configuration through CloudFormation templates or custom AMIs ingested into an AMS Managed account. This is a clean way to deploy a production ready configuration. Once deployed, the application will be under prescriptive AMS governance and operations. The same applies to switching modes between Customer Managed and AMS Managed.

Monitoring and event management

Topics

The AWS Managed Services (AMS) monitoring system monitors your AMS resources for failures, performance degradation, and security issues. The AMS monitoring system relies on AWS services such as Amazon CloudWatch (CW), Amazon GuardDuty, Amazon Macie, and AWS Health. In addition to the monitoring system, AMS also deploys TrendMicro DeepSecurity for protection against malware on Amazon Elastic Compute Cloud (Amazon EC2) instances, for information about endpoint security (EPS) defaults, see Endpoint Security (EPS) (p. 341).

AMS monitoring provides these benefits:

- A monitoring baseline so that you have a default level of protection even if you don't configure any other monitoring for your managed accounts. For information, see Alerts from baseline monitoring in AMS (p. 88).
- Investigation alerts to determine the appropriate action. For example, if GuardDuty finds activity indicating brute forcing attempts against an Amazon EC2 instance, AMS analyzes VPC flowlogs to understand the origin and context of the activity.
- Remediation of alerts, when possible, to prevent or reduce the impact for your applications. For example, if you are using a standalone Amazon EC2 instance and it fails the System health check, AMS attempts to recover the instance by stopping and restarting it. For more information, see AMS automatic remediation of alerts (p. 300).
- Transparency into active, and previously resolved, alerts using OpsCenter. For example, if you have an unexpected high CPU utilization on an Amazon EC2 instance, you can request access to the AWS Systems Manager console (includes access to the OpsCenter console) and view the OpsItem directly in the OpsCenter console.

What is monitoring?

The AMS monitoring system monitors your AWS resources for failures, performance degradation, and security issues. As a managed account, AMS configures and deploys alarms for applicable AWS resources, monitors them, and performs remediation when applicable.

The AMS monitoring system generates alerts based on the monitoring configuration in your account. The monitoring configuration of an account refers to all the resource parameters in the account that create an alert; for information about the resource parameters, see Alerts from baseline monitoring in AMS (p. 88). The monitoring configuration of an account includes CloudWatch Alarm definitions, and CloudWatch Event Rules that generate the alert (alarm or event).

The baseline monitoring configuration is the set of alarm definitions (Alerts from baseline monitoring in AMS (p. 88)) curated by AMS for monitoring resources in your managed account. The monitoring configuration of an account may differ from the baseline configuration, as a result of changes requested by you.

A notification of imminent, on-going, receding, or potential failures, performance degradation, or security issues generated by the baseline monitoring configured in an account, is called an alert. Examples of alerts are an Amazon CloudWatch Alarm, an Amazon CloudWatch Event, an Event, or a Finding from AWS service such as Amazon GuardDuty, and an event, or an alert, from Trend Micro Deep Security.

Alerts from security-related AWS services such as Amazon GuardDuty, Amazon Macie, or Trend Micro Deep Security are called security alerts to differentiate them from other types of alerts.

AMS monitoring provides these benefits:

- The ability to customize the baseline resource alarms to meet your requirements.
- Automatic remediation of alerts, when possible, to prevent or reduce the impact for your applications. For example, if you are using a standalone Amazon EC2 instance and it fails the system health check, AMS attempts to recover the instance by stopping and restarting it. For more information, see AMS automatic remediation of alerts (p. 300).
- Transparency into active, and previously resolved, alerts using OpsCenter. For example, if you have an unexpected high CPU utilization on an Amazon EC2 instance, you can request access to the AWS Systems Manager console (which includes access to the OpsCenter console) and view the OpsItem directly in the OpsCenter console.
- Investigating alerts to determine the appropriate actions.
- Alerts generated based on the configuration in your account and supported AWS services. The monitoring configuration of an account refers to all the resource parameters in the account that create an alert. The monitoring configuration of an account includes CloudWatch Alarm definitions, and EventBridge (formerly known as CloudWatch Events) that generate the alert (alarm or event). For more information about resource parameters, see Alerts from baseline monitoring in AMS (p. 88).
- Notification of imminent, on-going, receding, or potential failures; performance degradation; or security issues generated by the baseline monitoring configured in an account (known as an alert). Examples of alerts include a CloudWatch Alarm, an Event, or a Finding from an AWS service, such as GuardDuty or AWS Health.

What does the AMS monitoring system monitor?

In keeping with the AMS shared services responsibility model, the AMS monitoring system monitors your AWS infrastructure. For details on baseline monitoring in AMS, including AWS resources monitored and the type of alerts for each resource, see Alerts from baseline monitoring in AMS (p. 88). For Amazon EC2 instances, AMS monitors the operating system and provides baseline monitoring based on OS metrics such as CPU utilization and root volume usage.

We recommend supplementing AMS monitoring with additional monitoring using AWS services tailored to your application. For guidance on monitoring for availability see the "Monitoring and Alarming" section in this whitepaper Reliability Pillar. You can configure your own monitoring to suit your operational needs; how to do this is discussed in Creating additional CloudWatch alarms (p. 302) and Creating custom CloudWatch metrics and alarms (p. 303).

Single-Account Landing Zone proactive monitoring of Active Directory Trust

AMS single-account landing zone (SALZ) monitors the status of the one-way trust(s) between the Managed Active Directory (AD) in your AMS managed account and your company domain. The one-way trust with Managed AD is critical for access requests and instance logon requests. With this new monitoring, AMS now proactively responds to trust related issues, and reduces the mean time to detect access related incidents.

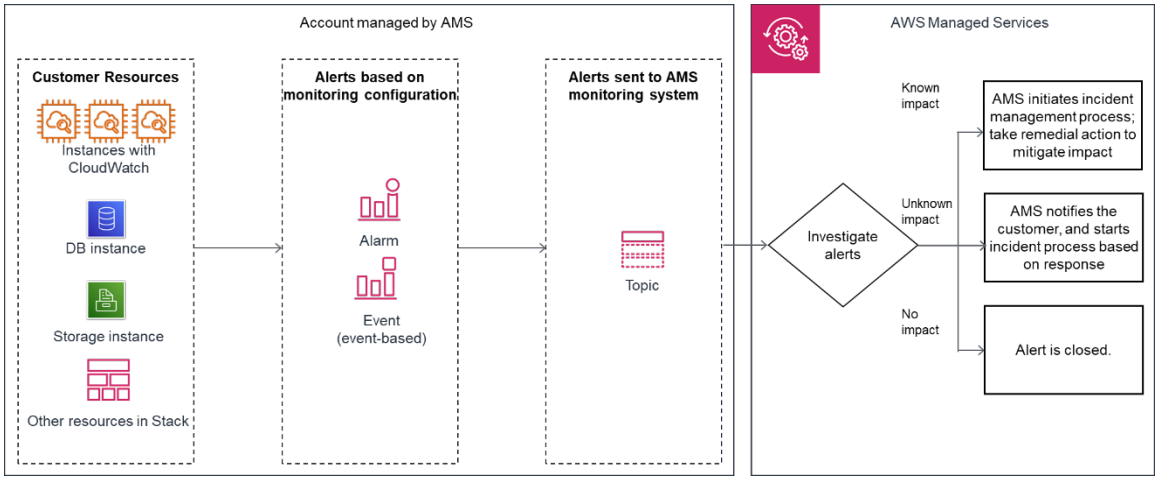
This feature is automatically enabled in your AMS accounts.

There is a small cost impact. The feature uses four AWS CloudWatch metrics, and two AWS CloudWatch alarms for one trust.

How monitoring works

See the following graphics on monitoring architecture in AMS.

The following diagram depicts a high-level overview of the **AMS multi-account landing zone** and **AMS single-account landing zone** monitoring workflow.



- Generation: At the time of account onboarding, AMS configures baseline monitoring (a combination of CloudWatch (CW) alarms, and CW event rules) for all your resources created in a managed account. The baseline monitoring configuration generates an alert when a CW alarm is triggered or a CW event is generated.
- Aggregation:
  - **Multi-Account Landing Zone**: Alerts are generated by your resources within Application and Core Organizational Unit accounts and sent to the AMS monitoring system by directing them through the Security account.
  - **Single-Account Landing Zone**: All alerts generated by your resources are sent to the AMS monitoring system by directing them to an SNS topic in the account.
- Processing: AMS analyzes the alerts and processes them based on their potential for impact. Alerts are processed as described next.
  - Alerts with known customer impact: These lead to the creation of a new incident report and AMS follows the incident management process; for information about incident management, see AMS incident response (p. 346).

Example alert: An Amazon EC2 instance fails a system health check, AMS attempts to recover the instance by stopping and restarting it.

- Alerts with uncertain customer impact: For these types of alerts, AMS sends a service notification that posts to your **Service Requests** page, asking you to verify the impact before we classify the alert as an incident.

  For example: An alert for >85% CPU utilization for more than 10 minutes on an Amazon EC2 instance can't be immediately categorized as an incident since this behavior may be expected based on usage. For such alerts, AMS sends an alert notification with the details and checks if the alert needs mitigating action. Alert notifications are discussed in detail in this section. We offer options for mitigating actions in the notification, and your reply that confirms that the alert is an incident triggers the creation of a new incident report and the AMS incident management process. Any service notification that receives a response of "no customer impact," or no response at all for three days, is marked as resolved and the corresponding alert is marked as resolved.
- Alerts with no customer impact: If, after evaluation, AMS determines that the alert doesn't have customer impact, the alert is closed.

  For example, AWS Health notifies of an EC2 instance requiring replacement but that instance has since been terminated.

Alert notification

As a part of the alert processing, based on the impact analysis, AMS creates an incident and initiates the incident management process for remediation, when impact can be determined. If impact can't be determined, AMS sends an alert notification to the email address associated with your account by way of a service notification; see the diagram on AMS monitoring architecture for alert handling process in How monitoring works (p. 297).

Tag-based alert notification

We recommend tag-based alert notifications because notifications sent to a single email address can cause confusion when multiple teams use the same account. You can use tags to get alert notifications for different resources sent to different email addresses. For resources with alerts that need to be sent to a specific email address, tag that resource with the key = OwnerTeamEmail, value = EMAIL_ADDRESS (use a group email; do not put personal information in tags). You can also use a custom tag key, but you must provide the custom tag key name to your CSDM with your explicit consent to use it in an email in order to activate automated notification for the tag-based communication. We recommend using the same tagging strategy for contact tags across all your instances and resources.

Note
The tag key value **OwnerTeamEmail** does not have to be in camel case. However, tags are case sensitive and it's best to use the recommended format. The email address must be specified in full, with the "at sign" (@) to separate the local part from the domain. Examples of invalid email addresses: Team.AppATabc.xyz or john.doe. For general guidance on your tagging strategy, see Tagging AWS resources. Do not add personally identifiable information (PII) in your tags, use distribution lists or aliases wherever possible.

Viewing the monitoring configuration for an account

There are two key parts to the monitoring configuration of an account that you can view:

- CloudWatch Alarms: You can view all the CW alarms in the account by going to the CloudWatch console and selecting different services of interest.
- CloudWatch Events:
  - **Multi-Account Landing Zone**: CloudWatch Events monitored in the account can be found by filtering for all CW event rules with the string `"ams-"`.
  - **Single-Account Landing Zone**: CloudWatch Events monitored in the account can be found by filtering for all CW event rules with the string `"mc-"`.

Changing the monitoring configuration for an account

You can change your baseline monitoring configuration for Amazon EC2 resources. For the alerts that can be configured, see Alerts from baseline monitoring in AMS (p. 88). You can change the alarm definition, alarm destination, or opt-out of the alarm notification for the baseline monitors so that the alerts meet your application's operational requirements. You can request any or all of the previously mentioned changes by submitting a Management | Other | Other | Update CT (ct-0xdawir96cy7k) with the following details.

- Instance ids [optional, if not mentioned, all instances in the account will be in-scope]
- CloudWatch metric name, for example, CPU utilization / swap free / IOwait
- Target - email id / phone number for SMS / SNS topic

To learn more about the type of changes you can request in the baseline monitoring configuration, see the Amazon CloudWatch Documentation.

Using OpsCenter

The AMS Operations team uses AWS Systems Manager OpsCenter for diagnosing and remediating many alerts related to your resources.

Using OpsCenter reduces mean time to resolution (MTTR), while providing a transparent view into the operational queues of the AMS operations teams.

With OpsCenter, AMS provides you with a transparent view of operational work items, also known as OpsItems, actively being worked upon by AMS teams, in addition to automated solutions.

To learn more about OpsCenter and OpsItems, see AWS Systems Manager OpsCenter. For information about getting access to the AWS Management Console, see Working with the AWS Management Console. From the AWS Management Console you can navigate to the AWS Systems Manager Console, and OpsCenter; to learn more, see AWS Systems Manager Session Manager. OpsCenter also provides an API that you can use; for information, see Learn More About OpsCenter.

OpsCenter is a priced feature with ~1000 OpsItems that cost under $10. For information, see AWS Systems Manager pricing.

Alert notifications from AMS

As a part of the alert processing, based on the impact analysis, AMS creates an incident and initiates the incident management process for remediation, when impact can be determined. In case impact cannot

be determined, AMS sends an alert notification to the email address associated with your account via a service notification; see the diagram on AMS monitoring architecture for alert handling process in How monitoring works (p. 297).

Receiving alerts generated by AMS

AMS enables you to receive alert notifications for Amazon EC2 resources directly to reduce communication delays. To receive Amazon EC2 alerts directly, subscribe your target (preferred email) to the SNS topic **Direct-Customer-Alerts** using the Management | Monitoring and notification | SNS | Subscribe change type (ct-3rcl9u1k017wu).

> **Note**
> Not all baseline alerts are sent to the **Direct-Customer-Alerts** topic by default. To see all alerts that are generated by the AMS monitoring system, subscribe to the SNS topic for the AMS monitoring system (in the request, ask for the "AMS Monitoring Topic"), specify a subscription channel that should receive the alerts (lambda, SQS, HTTP/S, email, or SMS), and specify the endpoints (for example, email addresses, if you choose the email protocol) that should receive the alerts.
> The AMS monitoring topic gets alerts that are used by AMS shared services, so it can be noisy.

To do this, submit an RFC with the Management | Other | Other | Create change type (ct-1e1xtak34nx76) with the parameters required to complete the action as described in the Amazon Simple Notification Service Subscribe API reference, Subscribe section.

For a list of baseline alerts AMS provides, see Alerts from baseline monitoring in AMS (p. 88).

Tag-based alert notifications

Using tag-based alert notifications are recommended because notifications sent to a single email address can cause confusion when multiple developer teams use the same account. AMS allows you to use tags to get alert notifications for different resources sent to different email addresses. For resources with alerts that need to be sent to a specific email address, tag that resource with the `key = OwnerTeamEmail`, `value = EMAIL_ADDRESS`. You can also use a custom tag key, but you must provide the custom tag key name to your CSDM with an email consent, to activate automated notification for the tag-based communication. We recommended using the same tagging strategy for contact tags across all your instances/resources.

> **Note**
> The key value `OwnerTeamEmail` does not have to be in camel case. However, tags are case sensitive and it's best to use the recommended format. The email address must be specified in full, with the "at sign" (@) to separate the local part from the domain. Examples of invalid email addresses: `Team.AppATabc.xyz` or `john.doe`. For general guidance on your tagging strategy, please refer to Using tags. Please do not add personally identifiable information (PII) in your tags. To tag an existing resource, submit an RFC with the Management | Other | Other | Update change type.

> **Important**
> Tag-based alert notifications only work for notifications related to Amazon EC2, Amazon EBS, Elastic Load Balancing, Network Load Balancer, Application Load Balancer, Amazon RDS, Amazon Redshift, and OpenSearch.

AMS automatic remediation of alerts

Some alerts are automatically remediated by AMS. This section describes how this remediation works and the conditions that must be met for the remediation to take place.

Alert name	Description	Remediation
Status Check Failed	This alarm indicates that the instance is running on degraded hardware or entered a fault state.	Our remediation first validates instance accessibility. If confirmed that accessibility is impacted, it stops the instance and starts it again so it can be migrated to new underlying hardware.
Root Volume Usage	This alarm indicates that the root volume (C: Drive in Windows) of your EC2 instance is filling up.	The remediation first deletes temporary files. If this does not free up required space, it extends the volume to prevent downtime if the volume were to get full.
Non-Root Volume Usage	This alarm indicates that an attached volume (not root or C:) is filling up.	The remediation first deletes temporary files. If this does not free up required space, it extends the volume to prevent downtime if the volume were to get full.
RDS-EVENT-0089	This alarm indicates that the DB instance has consumed more than 90% of its allocated storage.	The remediation first validates the DB is in a modifiable and available/storage-full state. It will attempt to increase the allocated storage via cloudformation changeset, if stack drift is already detected it will fall back to RDS API to prevent downtime.
RDS-EVENT-0007	This alarm indicates that the allocated storage for the DB instance has been exhausted.	The remediation first validates the DB is in a modifiable and available/storage-full state. It will attempt to increase the allocated storage via cloudformation changeset, if stack drift is already detected it will fall back to RDS API to prevent downtime.

EC2 status check failure remediation automation

These are some notes about how AMS auto-remediation works with EC2 status check failure issues.

- Your EC2 instance has become unreachable. In order to recover it, it must be stopped and started again so it's migrated to new hardware.
- The automation is not able to recover your instance if the root of the problem is within the OS.; for example, missing devices in fstab, kernel corruption, and so on.
- If your instance belongs to an Auto Scaling group, the automation takes no action. The autoscaling replaces the instance.
- The remediation doesn't take action if EC2 Auto Recovery is enabled for this instance.

EC2 volume usage remediation automation

How AMS auto-remediation works with EC2 volume usage issues.

- Before trying to extend the volume, the automation performs cleanup tasks (Windows: Disk Cleaner Linux: Logrotate + Simple Service Manager Agent Log removal) on the instance to try to free up space.

- This cleanup step will not be run on EC2 "T" family instances due to its reliance on CPU credits for continued functionality.
- The automation doesn't take action if the affected volume is already bigger than 2 TiB.
- The automation doesn't extend volumes that are part of Logical Volume Manager (LVM) or RAID.
- On Linux, the automation only supports extending file systems of type EXT2, EXT3, EXT4 and XFS.
- On Windows, the automation only supports New Technology File System (NTFS) and Resilient File System (ReFS).
- The automation doesn't extend instance stored backed volumes.
- The capacity expansion portion of the automation only occurs once every 6 hours with a 3-time volume expansion lifetime limit.

Under these EC2 volume usage issues, AMS reaches out to you through an outbound service request to determine the next actions to take.

Amazon RDS low storage event remediation automation

How AMS auto-remediation works with Amazon RDS low storage event issues.

- Before trying to extend the Amazon RDS instance storage, the automation performs several checks to ensure the Amazon RDS instance is in a modifiable and available, or storage-full, state.
- Where CloudFormation stack drift is detected, remediation occurs through Amazon RDS API.
- The remediation action does not run in the following scenarios:
  - The Amazon RDS instance status is not "available" or "storage-full".
  - The Amazon RDS instance storage is not currently modifiable (such as when the storage has been modified in the last 6 hours).
  - The Amazon RDS instance has auto-scaling storage enabled.
  - The Amazon RDS instance is not a resource within a CloudFormation stack.
- Remediation is limited to 1 expansion per 6 hours and no more than 3 expansions within a rolling fourteen day period.
- Where the above states are met, AMS reaches out to you with an outbound incident to determine next actions.

Creating additional CloudWatch alarms

You can create new CloudWatch alarms using the Deployment | Monitoring and notification | CloudWatch | Create alarms change type.

> **Important**
> AMS does not monitor CloudWatch alarms created by you.

Using CW custom CloudWatch metrics and alarms for Amazon EC2 instances (works only for mutable deployments that do not rely on updated AMIs deployed to Auto Scaling groups):

1. Produce your application monitoring script and custom metric. For more information and access to example scripts, see Monitoring Memory and Disk Metrics for Amazon EC2 Linux Instances. The Amazon CloudWatch monitoring scripts for Linux Amazon EC2 instances demonstrate how to produce and consume Amazon CloudWatch custom metrics. These sample Perl scripts comprise a fully functional example that reports memory, swap, and disk space utilization metrics for a Linux instance.
2. Upload your monitoring script. To upload the monitoring script to your Auto Scaling group or Amazon EC2 instance configuration, you can use UserData when configuring your Auto Scaling group or Amazon EC2 instance, or, if your application was deployed with CodeDeploy, you can

modify the configuration with a Deployment | Applications | CodeDeploy application | Deploy CT (ct-2edc3sd1sqmrb).

3. Publish your custom metric to CloudWatch (the first time you publish a data point for a new custom metric, it is created), see Publishing Custom Metrics.
4. Create the CloudWatch alarm, see Create a CloudWatch Alarm for an Instance.

Important
Monitoring data must be sent to this path [`infra/INSTANCE_ID/YOUR_CUSTOM_METRIC`]

To modify or delete a CloudWatch alarm, submit an RFC with the Management | Other | Other | Create change type (ct-1e1xtak34nx76) with the parameters required to complete the action as described in the Amazon CloudWatch API reference PutMetricAlarm.

You can use the CloudWatch event stream. AMS is integrated with CloudWatch and you can request that any AWS API call trigger a CloudWatch event.

To do this, submit a Management | Other | Other | Update CT (ct-0xdawir96cy7k) with the API calls that you are interested in. An AMS operator will talk to you to gather requirements. To learn more, see the Amazon CloudWatch Documentation.

To get access to the CloudWatch event stream, submit a Management | Other | Other | Update CT (ct-0xdawir96cy7k) to add a party to the SNS notification topic. An AMS operator will talk to you to gather requirements.

Creating custom CloudWatch metrics and alarms

You can store your business and application metrics in Amazon CloudWatch. You can view graphs, and set alarms based on these metrics, just as you can for the metrics that CloudWatch already stores for your AMS resources. To learn more about CloudWatch, see Amazon CloudWatch Concepts.

Amazon SNS allows applications to send time-critical messages to multiple subscribers through a "push" mechanism," in this case, MMS and your SQS queues, against the MMS SNS topic that the alarms are published to. You can use CloudWatch to create custom metrics and, via an SNS topic, have AMS alarm you appropriately. To do this, follow these steps.

Note
This process doesn't work for immutable deployments that rely on updated AMIs deployed to Auto Scaling groups, it is suitable for mutable application (not ASG) deployments.

1. Produce your application monitoring script and custom metric. For more information and access to example scripts, see Monitoring Memory and Disk Metrics for Amazon EC2 Linux Instances. The Amazon CloudWatch Monitoring Scripts for Linux Amazon EC2 instances demonstrate how to produce and consume Amazon CloudWatch custom metrics. These sample Perl scripts comprise a fully functional example that reports memory, swap, and disk space utilization metrics for a Linux instance.
2. Upload your monitoring script. To upload the monitoring script to your Auto Scaling group or Amazon EC2 instance configuration, you can use **UserData** when configuring your Auto Scaling group or Amazon EC2 instance, or, if your application was deployed with CodeDeploy, you can modify the configuration with a Deployment | Applications | CodeDeploy application | Deploy CT (ct-2edc3sd1sqmrb).
3. Publish your custom metric to CloudWatch (the first time you publish a data point for a new custom metric, it is created), see Publish Custom Metrics.
4. To integrate your customer metric to your application monitoring system, request AMS create an SNS topic for the metric by submitting an RFC with the Management | Other | Other | Create CT (ct-1e1xtak34nx76).

5. Create the CloudWatch alarm, see Creating Amazon CloudWatch Alarms.

Important
Monitoring data must be sent to this path [infra/*INSTANCE_ID*/*YOUR_CUSTOM_METRIC*].

Using CloudWatch application insights for .Net and SQL server

You can use Amazon CloudWatch Application Insights to set up the monitors for your application resources to continuously analyze data for signs of problems with your applications and reduce your mean time to repair (MTTR) when troubleshooting application issues. For details about CloudWatch Application Insights, see Amazon CloudWatch Application Insights for .NET and SQL Server.

Important
AMS does not monitor problems from CloudWatch Application Insights because they are for application code controlled by you.

To use CloudWatch Application Insights, submit an RFC with the Management | Other | Other | Create change type (ct-1e1xtak34nx76) with a request to create an IAM role that provides you with permission to configure CloudWatch Application Insights. There are two options to receive the problems identified: through an SNS topic or with a target in CloudWatch Event rules. In the RFC, specify which you want. If you plan to use CloudWatch Event rules, also specify the rule definition in the RFC. After you're set up with CloudWatch Application Insights, you receive notice of potential problems including insights that point to a possible root cause.

To learn how you can assume the role, see the AMS Onboarding Guide Federate your Active Directory with the AMS IAM Roles.

Log management

Topics

AMS log management collects, aggregates, and controls retention of the logs from the managed account. AWS log management aggregates logs from Amazon EC2 instances and AWS resources deployed within your account into CloudWatch Logs. The full list of services from which logs are currently aggregated can be found in AMS aggregated service logs (p. 306).

What Is log management?

Log management is the process of dealing with log events generated by instances, applications, and AWS services. This feature defines how AMS processes, stores, and rotates the log events generated in your managed AWS account. Infrastructure logs are used during incident resolution and to support system audits.

How AMS logging works

AMS single-account landing zone (SALZ) log management uses a variety of pre-installed agents and tools that are implemented when instances and applications are onboarded or provisioned.

Logging is configured during the account onboarding process and when a stack is launched.

AMS multi-account landing zone (MALZ) logs produced by instances and AWS services are available in CloudWatch Logs or Amazon Simple Storage Service (Amazon S3), within each account managed by AMS. AMS multi-account landing zone provides a central Logging Account that acts as a central aggregation location for some logs produced by individual application accounts.

The table in the Accessing your logs (p. 305) section describes which logs are available in individual accounts, and which are available in the central Logging Account.

Accessing your logs

MALZ

Provides five default IAM roles, each of which allow access to all logs within your account (all are prefaced with `AWSManagedServices`):

- `AdminRole`
- `CaseRole`
- `ChangeManagementRole`
- `ReadOnlyRole`
- `SecurityOpsRole`

Access to these roles is configured via federation, with each role being mapped to a group within your Active Directory domain.

To learn more about these roles, see IAM User Role (p. 322).

SALZ

The default `Customer_ReadOnly_Role` for AMS single-account landing zone allows your access to all logs within your account. Access to the logs is controlled using AWS Identity and Access Management (IAM) roles mapped to Active Directory groups.

AMS aggregated service logs

Each AWS service logs to either CloudWatch Logs or a specific location in an Amazon S3 bucket. How you access logs depends on their storage location. The following table defines how you can access the logs for each service.

Note
Unless specifically stated, all log locations are local to the account that generated the logs, and are not aggregated into the central Logging Account.

AMS single-account landing zone Aggregated Service Logs

	Service name	Log details	Log location
1	Amazon Aurora	General, slow query, and error logs.	CloudWatch LogGroup: /aws/rds/cluster/{*database_name*}/{*log_name*}
2	Amazon CloudFormation (CloudFormation or CFN)	API call logging only.	CloudFormation API calls are documented via CloudTrail, which sends its logs to the CloudWatch LogGroup and then syncs the logs into an S3 bucket. CloudWatch LogGroup: /aws/ams/cloudtrail S3 bucket: ams-a{*account_ID*}-log-management-{*region*}
3	Amazon CloudFront (CloudFront)	User request logging. You must explicitly enable CloudFront logging. For information, see Enabling logging for supported services (p. 316)	S3 bucket: ams-a{*account_ID*}-log-management-{*region*} Path: AWS/RedShift/{*CloudFront_distribution_ID*}
4	Amazon CloudWatch (CloudWatch)	API call logging only.	CloudWatch LogGroup: /aws/ams/cloudtrail
5	Amazon Elastic Block Store (EBS)	No logs are produced by the EBS service.	Not applicable
6	Amazon Elastic Compute Cloud (EC2)	System and application logs. For information, see the Amazon Elastic Compute Cloud (Amazon EC2) - system level logs (p. 314).	CloudWatch Logs: /{*instance_ID*}

	Service name	Log details	Log location
7	Amazon Elastic File System (Amazon EFS)	API call logging only.	CloudWatch LogGroup: /aws/ams/cloudtrail
8	Elastic Load Balancing (ELB)	Access and error log entries. Elastic load balancers log all requests sent to them, including requests that aren't routed to back-end instances. For example, if a client sends a malformed request, or there are no healthy instances to respond, the request is still logged. For more information about elastic load balancer log entries, see Access Log Entries for Classic Load Balancers, or Access Log Entries for Application Load Balancers.	CloudWatch LogGroup: /aws/ams/cloudtrail S3 bucket: mc-a{*account_ID*}-logs-{*region*} Path: aws/elbaccess
9	Amazon OpenSearch Service (OpenSearch Service)	Service error logs. You must explicitly enable OpenSearch logging. For information, see Enabling logging for supported services (p. 316)	CloudWatch LogGroup: /aws/ams/cloudtrail
10	Amazon ElastiCache	API call logging only.	CloudWatch LogGroup: /aws/ams/cloudtrail
11	Amazon GuardDuty		
12	Amazon Inspector		
13	Amazon Macie		
14	Amazon Redshift	Connection, user, and activity logs. Logging is enabled by default when you create your Redshift cluster by invoking the Create Redshift cluster CT (ct-1malj7snzxrkr). For information, see Database Audit Logging.	S3 bucket: ams-a{*account_ID*}-log-management-{*region*} Path: /AWS/RedShift/{*CloudFront_Distribution_ID*}
15	Amazon Relational Database Service (RDS)	Logs specific to database type. RDS logging must be explicitly enabled. For information, see Enabling logging for supported services (p. 316) You can only access MSSQL logs through a stored procedure; for information, see Archiving Log Files.	CloudWatch LogGroup: /aws/rds/(instance|cluster)/{database name}/{log name}

	Service name	Log details	Log location
16	Amazon S3 (S3)	Bucket access logs. Each access log record provides details about a single access request, such as: requester, bucket name, request time, request action, response status, and error code (if any). Access log information can be useful in security and access audits; it can also help you learn about your customer base and understand your Amazon S3 bill. For more information on S3 Access Log entries, see S3 Server Access Log Format.	S3 bucket: mc-a{*account_ID*}-log-management-{*region*} Path: /aws/s3access/{*bucket_name*}
17	Amazon Simple Email Service (SES)	SES API service calls.	CloudWatch LogGroup: /aws/ams/cloudtrail S3 bucket: ams-a{*account_ID*}-log-management-{*region*} Path: AWS/CloudTrail/AWSLogs/{*account_ID*}/CloudTrail/{*region*}
18	Amazon Virtual Private Cloud (VPC)	VPC flow data (information about the IP traffic going to and from your VPC's network interfaces).	CloudWatch LogGroup: /aws/vpcflow/{vpc_id}
19	Auto Scaling	API call logging only.	CloudWatch LogGroup: /aws/ams/cloudtrail
20	AWS Certificate Manager		
21	AWS CodeDeploy	Instance specific deployment logs.	On instance
22	AWS Config	AWS Config API service calls.	CloudWatch LogGroup: /aws/ams/cloudtrail S3 bucket: ams-a{*account_ID*}-log-management-{*region*} Path: AWS/CloudTrail/AWSLogs/{*account_ID*}/CloudTrail/{*region*}
23	AWS Database Migration Service	Database migration logs. For information, see Introducing log management in AWS Database Migration Service.	Database migration console
24	AWS Direct Connect (DX)	API call logging only.	CloudWatch LogGroup: /aws/ams/cloudtrail
25	AWS Glacier		
26	AWS IAM (IAM)		

	Service name	Log details	Log location
27	AWS Key Management Service		
28	AWS Management Console (console or AWS Console)		
29	AWS Simple Notification Service (SNS)		
30	AWS Simple Queueing Service (SQS)		

AMS multi-account landing zone Aggregated Service Logs

	Service name	Log details	Log location
1	Amazon Aurora	General, slow query, and error logs.	CloudWatch LogGroup: /aws/rds/cluster/{*database_name*}/{*log_name*}
2	Amazon CloudFormation (CloudFormation or CFN)	API call logging only.	CloudFormation API calls are documented via CloudTrail, which sends its logs to the CloudWatch LogGroup and then syncs the logs into an S3 bucket. Logs are retained for 14 days by default in the CloudWatch LogGroup, and are retained indefinitely in the S3 bucket. CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs S3 bucket [in the central Logging Account]: aws-landing-zone-logs-ams-a{*account_ID*}-log-management-{*region*} Path: /AWSLogs/{*account_ID*}/CloudTrail/
3	Amazon CloudFront (CloudFront)	User request logging. CloudFront logging must be explicitly enabled. For information, see Enabling logging for supported services (p. 316).	S3 bucket: ams-a{*account_ID*}-log-management-{*region*} Path: AWS/RedShift/{*CloudFront distribution ID*}
4	Amazon CloudWatch (CloudWatch)	API call logging only.	CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs

	Service name	Log details	Log location
			S3 bucket [in the central Logging Account]: aws-landing-zone-logs-{*account_ID*}-{*region*} Path: /AWSLogs/{*account_ID*}/CloudTrail/
5	Amazon Elastic Block Store (EBS)	No logs are produced by the EBS service.	Not applicable
6	Amazon Elastic Compute Cloud (EC2)	System and application logs. For information, see the Amazon Elastic Compute Cloud (Amazon EC2) - system level logs (p. 314).	CloudWatch Logs: /{*instance ID*}
7	Amazon Elastic File System (EFS)	API call logging only.	CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs S3 bucket [in the central Logging Account]: aws-landing-zone-logs-{*account_ID*}-{*region*} Path: /AWSLogs/{*account_ID*}/CloudTrail/
8	Amazon Elastic Load Balancing (ELB)	Access and error log entries. Elastic load balancers log all requests sent to them, including requests that aren't routed to back-end instances. For example, if a client sends a malformed request, or there are no healthy instances to respond, the request is still logged. For more information about elastic load balancer log entries, see Access Log Entries for Classic Load Balancers, or Access Log Entries for Application Load Balancers.	API call logs: CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs S3 bucket [in the central Logging Account]: aws-landing-zone-logs-{*account_ID*}-{*region*} Path: /AWSLogs/{*account_ID*}/CloudTrail/ Access logs: S3 bucket: mc-a{*account_ID*}-logs{*region*} Path: aws/elbaccess
9	Amazon OpenSearch Service (OpenSearch Service)	Service error logs. You must explicitly enable OpenSearch logging. For information, see Enabling logging for supported services (p. 316)	CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs S3 bucket [in the central Logging Account]: aws-landing-zone-logs-{*account_ID*}-{*region*} Path: /AWSLogs/{*account_ID*}/CloudTrail/

	Service name	Log details	Log location
10	Amazon ElastiCache	API call logging only.	CloudWatch LogGroup: //CloudTrail/Landing-Zone-Logs S3 bucket [in the central Logging Account]: aws-landing-zone-logs-{*account_ID*}-{*region*} Path: /AWSLogs/{*account_ID*}/CloudTrail/
11	Amazon GuardDuty		
12	Amazon Inspector		
13	Amazon Macie		
14	Amazon Redshift	Connection, user, and activity logs. Logging is enabled by default when you create your Redshift cluster by invoking the Create Redshift cluster CT (ct-1malj7snzxrkr). For information, see Database Audit Logging.	S3 bucket: ams-a{*account_ID*}-log-management-{*region*} Path: /AWS/RedShift/{*CloudFront Distribution ID*}
15	Amazon Relational Database Service (RDS)	Logs specific to database type. You must explicitly enable RDS logging. For information, see Enabling logging for supported services (p. 316) You can only access MSSQL logs through a stored procedure; for information, see Archiving Log Files.	CloudWatch LogGroup: /aws/rds/(*instance* or *cluster*)/{*database_name*}/{*log_name*}
16	Amazon S3 (S3)	Bucket access logs. Each access log record provides details about a single access request such as the requester, bucket name, request time, request action, response status, and error code (if any). Access log information can be useful in security and access audits. It can also help you learn about your customer base and understand your Amazon S3 bill. For more information about S3 Access Log entries, see S3 Server Access Log Format.	S3 bucket: mc-a{*account_ID*}-log-management-{*region*} Path: /aws/s3access/{*bucket_name*} S3 bucket [in the central Logging Account]: aws-landing-zone-s3-access-logs-{*account_ID*}-{*region*} Path: /
17	Amazon Simple Email Service (SES)	SES API service calls.	CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs S3 bucket [in the central Logging Account]: aws-landing-zone-logs-{*account_ID*}-{*region*} Path: /AWSLogs/{*account_ID*}/CloudTrail/

	Service name	Log details	Log location
18	Amazon Virtual Private Cloud (VPC)	VPC flow data (information about the IP traffic going to and from your VPC's network interfaces).	CloudWatch LogGroup: /aws/vpcflow/{*VPC_ID*}
19	Auto Scaling	API call logging only.	CloudWatch LogGroup: /CloudTrail/ Landing-Zone-Logs S3 bucket [in the central Logging Account]: aws-landing-zone-logs-{*account_ID*}-{*region*} Path: /AWSLogs/{*account_ID*}/ CloudTrail/
20	AWS Certificate Manager		
21	AWS CodeDeploy	Instance-specific deployment logs.	On Instance
22	AWS Config	AWS Config API service calls.	CloudWatch LogGroup: /CloudTrail/ Landing-Zone-Logs S3 bucket [in the central Logging Account]: aws-landing-zone-logs-{*account_ID*}-{*region*} Path: /AWSLogs/{*account_ID*}/ CloudTrail/
		Resource configuration changes, as tracked by AWS Config.	S3 bucket [in the central Logging Account]: aws-landing-zone-logs-{*account_ID*}-{*region*} Path: /AWSLogs/{*account_ID*}/ Config/
23	AWS Database Migration Service	Database migration logs. For information, see Introducing log management in AWS Database Migration Service.	Database migration console
24	AWS Direct Connect (DX)	API call logging only.	CloudWatch LogGroup: /CloudTrail/ Landing-Zone-Logs S3 bucket [in the central Logging Account]: aws-landing-zone-logs-{*account_ID*}-{*region*} Path: /AWSLogs/{*account_ID*}/ CloudTrail/
25	AWS Glacier		
26	AWS IAM (IAM)		
27	AWS Key Management Service		
28	AWS Management Console (console or AWS Console)		
29	AWS Simple Notification Service (SNS)		

	Service name	Log details	Log location
30	AWS Simple Queueing Service (SQS)		

AMS shared services logs

The following table describes the logs, and log location, for the AMS Shared Services in your account.

AMS single-account landing zone Shared Services Logging

	Shared service name	Log details	Log location
1	Bastion Hosts	Information regarding users accessing the bastion host.	**Linux Bastions**: CloudWatch Logs: /{instance id}/var/log/secure CloudWatch Logs: /{instance id}/var/log/audit/audit.log **Windows Bastions**: CloudWatch Logs: /{instance id}/SecurityEventLog
2	Management Hosts	Output of scripts, which assist in automated access management actions within the account.	CloudWatch Logs: /{instance id}/ApplicationEventLog
4	EPS Hosts (DSM)	Information regarding the enrollment of instances onto the Deep Security Management platform.	CloudWatch Logs: /{instance id}/var/log/DSM.log
5	Directory Services	Information regarding account login, account management, detailed tracking, object access, policy change, and privilege use within the account's directory. You must explicitly enable Directory Services logging. For information, see Enabling logging for supported services (p. 316).	CloudWatch Logs: /aws/directoryservice/{directory id}-{directory dns name}
6	Lambdas	Output of various lambdas, which assist in automated operational actions within the account.	CloudWatch Logs: /aws/lambda/{lambda name}

AMS multi-account landing zone Shared Services Logging

	Shared service name	Log details	Log location
1	Bastions	Output of instance logins and authentication failures.	**Linux Bastions** CloudWatch Logs: /{*instance_ID*}/var/log/secure.log **Windows Bastions** CloudWatch Logs: /{*instance_ID*}/SecurityEventLog
2	Management Hosts	Output of scriptsy, which assist in automated access management actions within the account.	CloudWatch Logs: /{*instance_ID*}/ApplicationEventLog
3	EPS Hosts (DSM)	Information regarding the enrollment of instances onto the Deep Security Management platform.	CloudWatch Logs: /{*instance_ID*}/var/log/DSM.log
4	Directory Services	Information regarding account login, account management, detailed tracking, object access, policy change, and privilege use within the account's directory. You must explicitly enable Directory Services logging. For information, see Enabling logging for supported services (p. 316).	CloudWatch Logs: /aws/directoryservice/{*directory_ID*}-{*directory_DNS_name*}
5	Lambdas	Output of various lambdas, which assist in automated operational actions within the account.	CloudWatch Logs: /aws/lambda/{*Lambda_name*}

Amazon Elastic Compute Cloud (Amazon EC2) - system level logs

Instance logs are collected by a CloudWatch Logs agent running on the instance and can be accessed through a CloudWatch Log group of the same name as the instance. For example, if the instance ID is i-0123456789abcdef0 and the log file name is /var/log/messages, the Log Group would be i-0123456789abcdef0 and the Log Stream /var/log/messages.

See also AMS aggregated service logs (p. 306).

The following logs are collected by default.

Amazon Linux / Red Hat Linux / Centos Linux

Log file / Log stream
/var/log/audit/audit.log
/var/log/cron

Log file / Log stream
/var/log/amazon/ssm/amazon-ssm-agent.log
/var/log/secure
/var/log/aws/ams
/var/log/maillog
/var/log/yum.log
/var/log/messages
/var/log/cloud-init-output.log
/var/log/cloud-init.log (Amazon Linux 1 / Amazon Linux 2 only)

Windows

Log file / Log stream
SecurityEventLog
SystemEventLog
AmazonSSMAgentLog
MicrosoftWindowsAppLockerMSIAndScriptEventLog
MicrosoftWindowsAppLockerEXEAndDLLEventLog
AmazonCloudWatchAgentLog
EC2ConfigServiceEventLog (Windows Server 2012 R2 Only)
ApplicationEventLog
AmazonCloudFormationLog
MicrosoftWindowsGroupPolicyOperationalEventLog
AmazonSSMErrorLog

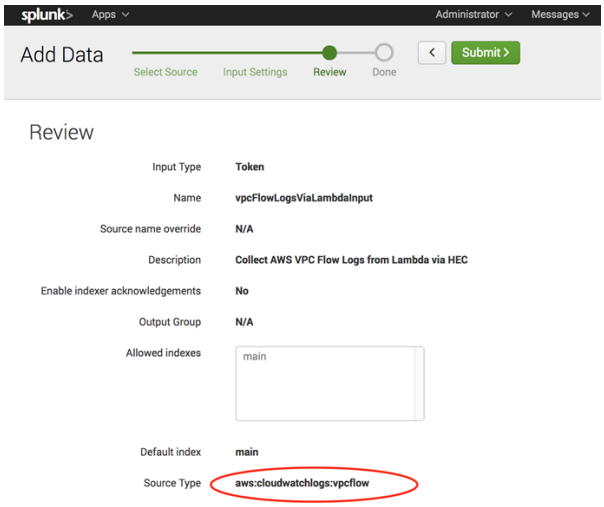
Integrating with Splunk

AMS supports AWS Lambda-based push to customer log analytics services, such as Splunk.

AMS leverages the Splunk Add-on for Amazon Web services, which allows AWS data to be streamed to Splunk. See Hardware and software requirements.

Refer to this Splunk blog post How to stream AWS CloudWatch Logs to Splunk (Hint: it's easier than you think). Because CloudWatch log streaming is enabled by default for AMS customers, and AMS configures the AWS Lambda function for you, though you need to configure the Splunk HTTP Event Collector (HEC) input and submit a request to AMS for the added functionality.

Here's how the data input settings might look:



Customizing your log configuration

You can alter log data retention for CloudWatch logs, and you can enable logging for additional AWS services.

Altering CloudWatch log retention

You can change the log data retention setting for CloudWatch logs. By default, logs are kept indefinitely and never expire. You can adjust the retention policy for each log group, keeping the indefinite retention, or you can choose a retention period between 10 years and one day. To do this, see Change Log Data Retention in CloudWatch Logs.

Enabling logging for supported services

Some services do not have logging enabled by default and require explicit enablement.

To enable logging for CloudFront, OpenSearch, Amazon RDS and Route53, submit an RFC with the Management | Other | Other | Create change type (ct-1e1xtak34nx76) with the following values, replacing *variables* as appropriate:

```
Subject: Enable logging for SERVICE_NAME
Description: Service ARN: SERVICE_ARN
```

Security in AMS

Security management is the process by which AMS identifies an organization's assets and implements policies and procedures to protect those assets.

> **Note**
> AMS now has a change type (CT), Deployment | Advanced stack components | ACM certificate with additional SANs | Create (ct-3l14e139i5p50), that you can use to submit a request for an AWS Certificate Manager certificate. For information, see What is AWS Certificate Manager?, and AWS::CertificateManager::Certificate. This CT provides for the creation of additional subject alternative name (SAN).

To better understand general AWS security, see Best Practices for Security, Identity, & Compliance.

AMS categorizes security risks as follows:

- Known risks detected by anti-malware, which the malware mitigation process handles.
- Security events including access breaches, which the security event management process handles.

Topics

Data protection in AMS

AMS continuously monitors your managed accounts by leveraging native AWS services such as Amazon GuardDuty, Amazon Macie (optionally), and other internal proprietary tools and processes. After an alarm is triggered, AMS assumes responsibility for the initial triage and response to the alarm. Our response processes are based on NIST standards. AMS regularly tests its response processes using

Security Incident Response Simulation with you to align your workflow with existing customer security response programs.

When AMS detects any violation, or imminent threat of violation, of AWS or your security policies, we gather information, including impacted resources and any configuration-related changes. AMS provides 24/7/365 follow-the-sun support with dedicated operators actively reviewing and investigating monitoring dashboards, incident queue, and service requests across all of your managed accounts. AMS investigates the findings with our security experts to analyze the activity and notify you through the security escalation contacts listed in your account.

Based on our findings, AMS engages with you proactively. If you believe the activity is unauthorized or suspicious, AMS works with you to investigate and remediate or contain the issue. There are certain finding types generated by GuardDuty that require you to confirm the impact before AMS is able to take any action. For example, the GuardDuty finding type **UnauthorizedAccess:IAMUser/ConsoleLogin**, indicates that one of your users has logged in from an unusual location; AMS notifies you and asks that you review the finding to confirm if this behavior is legitimate.

Amazon Macie

We recommend, and AMS Accelerate supports, Macie to detect a large and comprehensive list of sensitive data, such as personal health information (PHI), personally identifiable information (PII), and financial data.

Macie can be configured to run periodically on any Amazon S3 bucket, automating the evaluation of any new or modified objects within a bucket over time. As security findings are generated, AMS will notify you and work with you to remediate as needed.

For more information, see Analyzing Amazon Macie findings.

Amazon Macie security

Macie is an artificial intelligence/AI powered security service that helps you prevent data loss by automatically discovering, classifying, and protecting sensitive data stored in AWS. Macie uses machine learning to recognize sensitive data such as personally identifiable information (PII) or intellectual property, assigns a business value, and provides visibility into where this data is stored and how it is being used in your organization. Macie continuously monitors data access activity for anomalies, and delivers alerts when it detects risk of unauthorized access or inadvertent data leaks. Macie service supports Amazon S3 and AWS CloudTrail data sources.

AMS continuously monitors for alerts from Macie and, if alerted, takes quick actions to protect your resources and account. With the addition of Macie to the list of services AMS supports, we are also now responsible for enabling and configuring Macie in all of your accounts, per your instructions. You can view Macie alerts and our actions as they unfold in the AWS console or supported integrations. During account onboarding, you can indicate accounts that you use to store PII. For all new accounts with PII, we recommend using Macie. For existing accounts with PII, contact us and we will turn it on in your account. As a result, you can have an added layer of protection available and enjoy all the benefits of Macie in your AWS environment managed by AMS.

AMS Macie FAQs

- Why do I need Macie when all AMS accounts have Trend Micro and GuardDuty enabled?

  Macie helps you protect your data in Amazon S3 by helping you classify what data you have, the value that data has to the business, and the behavior associated with access to that data. Amazon GuardDuty provides broad protection of your AWS accounts, workloads, and data by helping to identify threats such as threat actor reconnaissance, instance issue, and problematic account activity. Both services incorporate user behavior analysis, machine learning, and anomaly detection to detect threats in their respective categories. Trend Micro does not focus on identifying PII and threats from them.

- How do I turn Macie on in my AMS account?

  If you have PII/PHI stored in your accounts or are planning to store it, contact your CSDM or raise a service request to enable Macie for your new or existing accounts managed by AMS.
- What are the cost implications of enabling Macie in my AMS account?

  Macie pricing works for AMS similar to other services such as Amazon Elastic Compute Cloud (Amazon EC2). You pay for Amazon Macie based on usage and an AMS uplift based on your SLAs. Macie fees are based on usage, see Amazon Macie Pricing, measured based on AWS CloudTrail events and Amazon S3 storage. Please note that Macie charges tend to flatten out from the second month after it's enabled because it charges based on incremental data added to Amazon S3 buckets.

To learn more about Macie, see Amazon Macie.

GuardDuty

GuardDuty is a continuous security monitoring service that uses threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning to identify unexpected and potentially unauthorized and malicious activity within your AWS environment. This can include issues like escalations of privileges, uses of exposed credentials, or communication with malicious IP addresses, or domains. GuardDuty also monitors Amazon Web Services account access behavior for signs of compromise, such as unauthorized infrastructure deployments, like instances deployed in a Region that has never been used, or unusual API calls, like a password policy change to reduce password strength. For more information, refer to the GuardDuty User Guide.

To view and analyze your GuardDuty findings, use the following procedure.

1. Open the GuardDuty console.
2. Choose **Findings**, and then choose a specific finding to view details. The details for each finding differ depending on the finding type, resources involved, and nature of the activity.

For more information on available finding fields, see GuardDuty finding details.

GuardDuty security

Amazon GuardDuty offers threat detection that enables you to continuously monitor and protect your AWS accounts and workloads. Amazon GuardDuty analyzes continuous streams of meta-data generated from your account and network activity found in AWS CloudTrail Events, Amazon VPC flow logs, and Domain Name System (DNS) logs. It also uses integrated threat intelligence such as known malicious IP addresses, anomaly detection, and machine learning to identify threats more accurately. GuardDuty is a monitored AMS service; to learn more about Amazon GuardDuty monitoring, see GuardDuty monitoring (p. 320). To learn more about GuardDuty, see Amazon GuardDuty.

All new AMS accounts have GuardDuty enabled by default. AMS configures GuardDuty during account onboardings. You can submit change requests to modify the settings at any time. GuardDuty pricing works for AMS similarly to other services such as Amazon Elastic Compute Cloud (Amazon EC2). You pay for GuardDuty based on usage and an AMS uplift based on your SLAs. GuardDuty fees are based on usage (Amazon GuardDuty Pricing), measured based on AWS CloudTrail events and volume of your Amazon VPC Flow log.

GuardDuty generates a variety of alerts, the primary detection categories include:

- Reconnaissance -- Activity suggesting reconnaissance by a threat actor, such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known bad IP.

- Instance issue -- Problematic instance activity, such as cryptocurrency mining, malware using domain generation algorithms (DGA), outbound denial of service activity, unusually high volume of network traffic, unusual network protocols, outbound instance communication with a known malicious IP, temporary Amazon EC2 credentials used by an external IP address, and data exfiltration using DNS.
- Account activity -- Common patterns indicative of account activity include API calls from an unusual geolocation or anonymizing proxy, attempts to disable AWS CloudTrail logging, unusual instance or infrastructure launches, infrastructure deployments in an unusual AWS Region, and API calls from known malicious IP addresses.

AMS uses GuardDuty in your managed accounts to continuously monitor for findings and alerts from GuardDuty and, if alerted, AMS operations takes proactive actions to protect your resources and account. You can view GuardDuty findings and our actions as they unfold in the AWS console or supported integrations.

GuardDuty works with Trend Micro Deep Security Manager in your account. Trend Micro Deep Security Manager provides host-based Intrusion Detection / Intrusion Prevention services. Trend Micro Web Reputation services have some overlap with GuardDuty in the ability to detect when a host is attempting to communicate with a host or web service known to be a threat. However, GuardDuty provides additional threat detection categories and accomplishes this by monitoring network traffic, a method which is complementary to Trend Micro's host-based detection. Network-based threat detection allows for increased security by not allowing controls to fail if the host has been exhibiting problematic behavior. AMS recommends using GuardDuty in all your AMS accounts.

To learn more about Trend Micro, see Trend Micro Deep Security Help Center; note that non-Amazon links may change without notice to us.

GuardDuty monitoring

GuardDuty informs you of the status of your AWS environment by producing security findings that AMS captures and can alert on.

Amazon GuardDuty monitors the security of your AWS environment by analyzing and processing VPC flow logs, AWS CloudTrail event logs, and Domain Name System logs. You can expand this monitoring scope by configuring GuardDuty to also use your own custom, trusted IP lists, and threat lists.

- Trusted IP lists consist of IP addresses that you have allowed for secure communication with your AWS infrastructure and applications. GuardDuty does not generate findings for IP addresses on trusted IP lists. At any given time, you can have only one uploaded trusted IP list per AWS account per region.
- Threat lists consist of known malicious IP addresses. GuardDuty generates findings based on threat lists. At any given time, you can have up to six uploaded threat lists per AWS account per region.

To implement GuardDuty, use the AMS CT Deployment | Monitoring and notification | GuardDuty IP set | Create (ct-08avsj2e9mc7g) to create a set of approved IP addresses. You can also use the AMS CT Deployment | Monitoring and notification | GuardDuty threat intel set | Create (ct-25v6r7t8gvkq5) to create a set of denied IP addresses.

For a list of the services that AMS monitors, see What does the AMS monitoring system monitor? (p. 296).

Data encryption in AMS

AMS uses several AWS services for data encryption, notably Amazon Simple Storage Service, AWS Key Management Service (AWS KMS), and Amazon OpenSearch Service.

Amazon Simple Storage Service offers several object encryption options that protect data in transit and at rest. Server-side encryption encrypts your object before saving it on disks in its data centers and

then decrypts it when you download the objects. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For more information, see Data protection in Amazon S3.

Data encryption at rest

OpenSearch Service domains offer encryption of data at rest, a security feature that helps prevent unauthorized access to your data. The feature uses AWS Key Management Service (AWS KMS) to store and manage your encryption keys and the Advanced Encryption Standard algorithm with 256-bit keys (AES-256) to perform the encryption. For more information, see: Encryption of Data at Rest for Amazon OpenSearch Service.

Key management

AWS KMS is a managed service that makes it easy for you to create and control customer master keys (CMKs), the encryption keys used to encrypt your data. AWS KMS CMKs are protected by hardware security modules (HSMs) that are validated by the FIPS 140-2 Cryptographic Module Validation Program except in the China (Beijing) and China (Ningxia) Regions. For more information, see What is AWS Key Management Service?

Identity and access management

AWS Identity and Access Management is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources. During AMS onboarding, you are responsible for creating cross-account IAM Admin roles within each of your managed accounts.

Multi-Account Landing Zone (MALZ) IAM safeguards

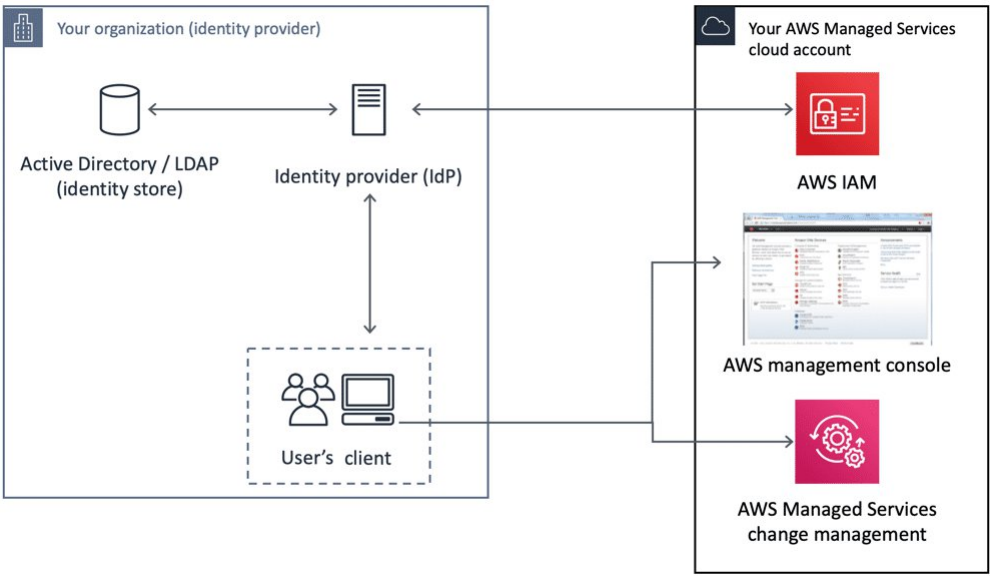
AMS multi-account landing zone (MALZ) requires an Active Directory (AD) trust as a primary design goal of AMS access management to allow each organization (both AMS, and customer) management of their own identities' life cycles. This avoids the need to have credentials in one another's directory. The one-way trust is configured, so that the Managed Active Directory within the AWS account trusts the customer owned or managed AD to authenticate users. Because the trust is only one way, it doesn't mean that the Managed AD is trusted by the Customer Active Directory.

In this configuration, the customer directory that manages user identities is known as the User Forest, and the Managed AD to which Amazon EC2 instances are attached is known as the Resource Forest. This is a commonly-leveraged Microsoft design pattern for Windows authentication; for more information, see Forest Design Models.

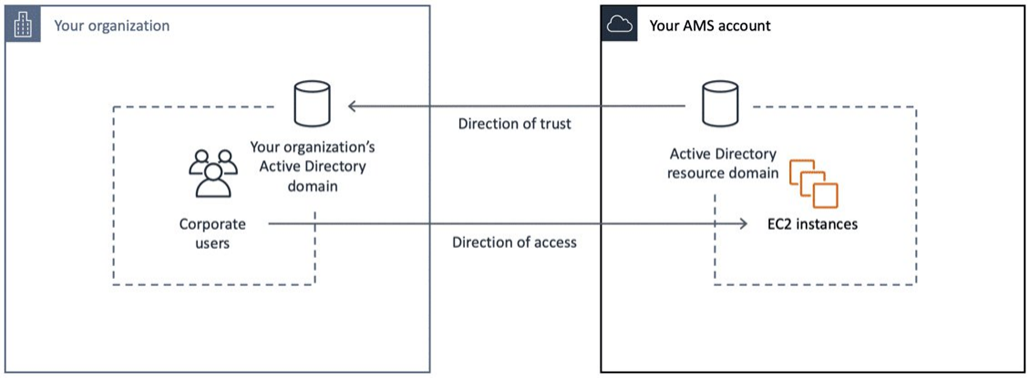
This model allows both organizations to automate their respective lifecycles and allows both AMS and you to rapidly revoke access if an employee leaves the organization. Without this model, if both organizations used a common directory (or created users/groups in one another's directories), then both organizations would have to put in additional workflows, and user syncs, to account for employees starting and leaving. This introduces risk as that process has latency and can be error-prone.

MALZ access pre-requisites

MALZ Identity Provider Integration for access to the AWS/AMS console, CLI, SDK.



One-way trust for Amazon EC2 instances in your AMS account.



Authenticating with identities

AMS uses IAM roles, which is a type of IAM identity. An IAM role is very similar to a user, in that it is an identity with permission policies that determine what the identity can and cannot do in AWS. However, a role doesn't have credentials associated with it and, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. An IAM user can assume a role to temporarily take on different permissions for a specific task.

Access roles are controlled by internal group membership, which is administered and periodically reviewed by Operations Management.

IAM User Role

An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and can't do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it.

Currently there is one AMS default user role, `Customer_ReadOnly_Role`, for standard AMS accounts and an additional role, `customer_managed_ad_user_role` for AMS accounts with Managed Active Directory.

The role policies set permissions for CloudWatch and S3 log actions, AMS console access, read-only restrictions on most AWS services, restricted access to account S3 console, and AMS change-type access.

Additionally, the `Customer_ReadOnly_Role` has mutative, reserved-instances permissions that allow you to reserve instances. It has some cost-saving values, so, if you know that you're going to need a certain number of EC2 instances for a long period of time, you can call those APIs. To learn more, see Amazon EC2 Reserved Instances.

> **Note**
> The AMS service level objective (SLO) for creating custom IAM policies for IAM users is four business days, unless an existing policy is going to be reused. If you want to modify the existing IAM user role, or add a new one, submit an IAM resource: Update or IAM resource: Create RFC, respectively.

If you're unfamiliar with Amazon IAM roles, see IAM Roles for important information.

Multi-Account Landing Zone (MALZ): To see the AMS multi-account landing zone default, un-customized, user role policies, see Default AMS multi-account landing zone (MALZ) IAM User Roles (p. 323), next.

Default AMS multi-account landing zone (MALZ) IAM User Roles

JSON policy statements for the default multi-account AMS multi-account landing zone user roles.

> **Note**
> The user roles are customizable and may differ on a per-account basis. Instructions on finding your role are provided.

These are examples of the default MALZ user roles. To make sure that you have the policies set that you need, run the AWS command `get-role` or sign in to the AWS Management -> IAM console and choose **Roles** in the navigation pane.

Core OU account roles

A core account is an MALZ-managed infrastructure account. AMS multi-account landing zone Core accounts include a management account and a networking account.

Core OU account: Common roles and policies

Role	Policy or policies
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (p. 332) (Public AWS Managed Policy).
AWSManagedServicesCaseRole	ReadOnlyAccess (p. 332)
	AWSSupportAccess (p. 331) (Public AWS Managed Policy).
AWSManagedServicesChangeManagementRole (Core account version)	ReadOnlyAccess (p. 332)
	AWSSupportAccess (p. 331)
	AMSChangeManagementReadOnlyPolicy (p. 327)
	AMSChangeManagementInfrastructurePolicy (p. 328)

Core OU account: Master account roles and policies

Role	Policy or policies
AWSManagedServicesBillingRole	AMSBillingPolicy (p. 326) (AMSBillingPolicy).

Role	Policy or policies
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (p. 332) (Public AWS Managed Policy).
AWSManagedServicesCaseRole	ReadOnlyAccess (p. 332)
	AWSSupportAccess (p. 331) (Public AWS Managed Policy).
AWSManagedServicesChangeManagementRole (Master account version)	ReadOnlyAccess (p. 332)
	AWSSupportAccess (p. 331)
	AMSChangeManagementReadOnlyPolicy (p. 327)
	AMSChangeManagementInfrastructurePolicy (p. 328)
	AMSMasterAccountSpecificChangeManagementInfrastru

Core OU Account: Networking account roles and policies

Role	Policy or policies
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (p. 332) (Public AWS Managed Policy).
AWSManagedServicesCaseRole	ReadOnlyAccess (p. 332)
	AWSSupportAccess (p. 331) (Public AWS Managed Policy).
AWSManagedServicesChangeManagementRole (Networking account version)	ReadOnlyAccess (p. 332)
	AWSSupportAccess (p. 331)
	AMSChangeManagementReadOnlyPolicy (p. 327)
	AMSChangeManagementInfrastructurePolicy (p. 328)
	AMSNetworkingAccountSpecificChangeManagementInfrastructu

Application Account Roles

Application account roles are applied to your application-specific accounts.

Application account: Roles and policies

Role	Policy or policies
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (p. 332) (Public AWS Managed Policy).
AWSManagedServicesCaseRole	ReadOnlyAccess (p. 332)
	AWSSupportAccess (p. 331) (Public AWS Managed Policy).

Role	Policy or policies
	This policy provides access to all support operations and resources. For information, see Getting Started with AWS Support.
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess (p. 332)
	AWSSupportAccess Example (p. 331) This policy provides access to all support operations and resources.
	`AWSCertificateManagerFullAccess` information, (Public AWS Managed Policy)
	`AWSWAFFullAccess` information, (Public AWS Managed policy). This policy grants full access to AWS WAF resources.
	AMSSecretsManagerSharedPolicy (p. 329)
AWSManagedServicesChangeManagementRole (Application account version)	ReadOnlyAccess (p. 332)
	AWSSupportAccess (p. 331) (Public AWS Managed Policy). This policy provides access to all support operations and resources. For information, see Getting Started with AWS Support.
	AMSSecretsManagerSharedPolicy (p. 329)
	AMSChangeManagementPolicy (p. 330)
	AMSReservedInstancesPolicy (p. 330)
	AMSS3Policy (p. 330)
AWSManagedServicesAdminRole	ReadOnlyAccess (p. 332)
	AWSSupportAccess (p. 331)
	AMSChangeManagementInfrastructurePolicy (p. 328)
	AWSMarketplaceManageSubscriptions (p. 331)
	AMSSecretsManagerSharedPolicy (p. 329)
	AMSChangeManagementPolicy (p. 330)
	AWSCertificateManagerFullAccess (p. 331)
	AWSWAFFullAccess (p. 332)
	AMSS3Policy (p. 330)
	AMSReservedInstancesPolicy (p. 330)

Policy Examples

Examples are provided for most policies used. To view the ReadOnlyAccess policy (which is pages long as it provides read-only access to all AWS services), you can use this link, if you have an active AWS account: ReadOnlyAccess. Also, a condensed version is included here.

AMSBillingPolicy

`AMSBillingPolicy`

The new Billing role can be used by your accounting department to view and change billing information or account settings in the Master account. To access information such as Alternate Contacts, view the account resources usage, or keep a tab of your billing or even modify your payment methods, you use this role. This new role comprises of all the permissions listed in the AWS Billing IAM actions web page.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToBilling"
        },
        {
            "Action": [
                "aws-portal:ViewAccount",
                "aws-portal:ModifyAccount"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountSettings"
        },
        {
            "Action": [
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountBudget"
        },
        {
            "Action": [
                "aws-portal:ViewPaymentMethods",
                "aws-portal:ModifyPaymentMethods"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPaymentMethods"
        },
        {
            "Action": [
                "aws-portal:ViewUsage"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToUsage"
        },
        {
            "Action": [
```

```
                "cur:DescribeReportDefinitions",
                "cur:PutReportDefinition",
                "cur:DeleteReportDefinition",
                "cur:ModifyReportDefinition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostAndUsageReport"
        },
        {
            "Action": [
                "pricing:DescribeServices",
                "pricing:GetAttributeValues",
                "pricing:GetProducts"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPricing"
        },
        {
            "Action": [
                "ce:CreateCostCategoryDefinition",
                "ce:DeleteCostCategoryDefinition",
                "ce:DescribeCostCategoryDefinition",
                "ce:ListCostCategoryDefinitions",
                "ce:UpdateCostCategoryDefinition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostCategories"
        }
    ]
}
```

AMSChangeManagementReadOnlyPolicy

`AMSChangeManagementReadOnlyPolicy`

Permissions to see all AMS change types, and the history of requested change types.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Sid": "AMSCoreAccountsCMAndSKMSReadOnlyAccess",
  "Effect": "Allow",
  "Action": [
   "amscm:GetChangeTypeVersion",
   "amscm:GetRfc",
   "amscm:ListChangeTypeCategories",
   "amscm:ListChangeTypeClassificationSummaries",
   "amscm:ListChangeTypeItems",
   "amscm:ListChangeTypeOperations",
   "amscm:ListChangeTypeSubcategories",
   "amscm:ListChangeTypeVersionSummaries",
   "amscm:ListRestrictedExecutionTimes",
   "amscm:ListRfcSummaries",
   "amsskms:GetStack",
   "amsskms:GetSubnet",
   "amsskms:GetVpc",
   "amsskms:ListAmis",
   "amsskms:ListStackSummaries",
   "amsskms:ListSubnetSummaries",
   "amsskms:ListVpcSummaries"
  ],
```

```
  "Resource": "*"
 }]
}
```

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

`AMSMasterAccountSpecificChangeManagementInfrastructurePolicy`

Permissions to request the Deployment | Managed landing zone | Master account | Create application account (with VPC) change type.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Sid": "AMSMasterAccountAccess",
  "Effect": "Allow",
  "Action": [
   "amscm:ApproveRfc",
   "amscm:CancelRfc",
   "amscm:CreateRfc",
   "amscm:RejectRfc",
   "amscm:SubmitRfc",
   "amscm:UpdateRfc",
   "amscm:UpdateRfcActionState",
   "amscm:UpdateRestrictedExecutionTimes"
  ],
  "Resource": [
   "arn:aws:amscm:global:*:changetype/ct-1zdasmc2ewzrs:*"
  ]
 }]
}
```

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

`AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy`

Permissions to request the Deployment | Managed landing zone | Networking account | Create application route table change type.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Sid": "AMSNetworkingAccountAccess",
  "Effect": "Allow",
  "Action": [
   "amscm:ApproveRfc",
   "amscm:CancelRfc",
   "amscm:CreateRfc",
   "amscm:RejectRfc",
   "amscm:SubmitRfc",
   "amscm:UpdateRfc",
   "amscm:UpdateRfcActionState",
   "amscm:UpdateRestrictedExecutionTimes"
  ],
  "Resource": [
   "arn:aws:amscm:global:*:changetype/ct-1urj94c3hdfu5:*"
  ]
 }]
}
```

AMSChangeManagementInfrastructurePolicy

`AMSChangeManagementInfrastructurePolicy` (for Management | Other | Other CTs)

Permissions to request the Management | Other | Other | Create, and Management | Other | Other | Update change types.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Sid": "AMSCoreAccountsAccess",
  "Effect": "Allow",
  "Action": [
   "amscm:CancelRfc",
   "amscm:CreateRfc",
   "amscm:SubmitRfc",
   "amscm:UpdateRfc",
   "amscm:UpdateRfcActionState",
   "amscm:UpdateRestrictedExecutionTimes",
  ],
  "Resource": [
   "arn:aws:amscm:global:*:changetype/ct-1e1xtak34nx76:*",
   "arn:aws:amscm:global:*:changetype/ct-0xdawir96cy7k:*",
  ]
 }]
}
```

AMSSecretsManagerSharedPolicy

`AMSSecretsManagerSharedPolicy`

Permissions to view secret passwords/hashes shared by AMS through AWS Secrets manager (e.g. passwords to infrastructure for auditing).

Permissions to create secret password/hashes to share with AMS. (e.g. license keys for products that need to be deployed).

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Sid": "AllowAccessToSharedNameSpaces",
   "Effect": "Allow",
   "Action": "secretsmanager:*",
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
   ]
  },
  {
   "Sid": "DenyGetSecretOnCustomerNamespace",
   "Effect": "Deny",
   "Action": "secretsmanager:GetSecretValue",
   "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
   "Sid": "AllowReadAccessToAMSNameSpace",
   "Effect": "Deny",
   "NotAction": [
    "secretsmanager:Describe*",
    "secretsmanager:Get*",
    "secretsmanager:List*"
   ],
   "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
 ]
}
```

AMSChangeManagementPolicy

`AMSChangeManagementPolicy`

Permissions to request and view all AMS change types, and the history of requested change types.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Sid": "AMSFullAccess",
  "Effect": "Allow",
  "Action": [
   "amscm:*",
   "amsskms:*"
  ],
  "Resource": [
   "*"
  ]
 }]
}
```

AMSReservedInstancesPolicy

`AMSReservedInstancesPolicy`

Permissions to manage EC2 reserved instances; for pricing information, see Amazon EC2 Reserved Instances.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Sid": "AllowReservedInstancesManagement",
  "Effect": "Allow",
  "Action": [
   "ec2:ModifyReservedInstances",
   "ec2:PurchaseReservedInstancesOffering"
  ],
  "Resource": [
   "*"
  ]
 }]
}
```

AMSS3Policy

`AMSS3Policy`

Permissions to create and delete files from existing S3 buckets.

> **Note**
> These permissions do not grant the ability to create S3 buckets; that must be done with the Deployment | Advanced stack components | S3 storage | Create change type.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "s3:AbortMultipartUpload",
   "s3:DeleteObject",
```

```
   "s3:PutObject",
  ],
  "Resource": "*"
 }]
}
```

AWSSupportAccess

`AWSSupportAccess`

Full access to AWS Support. For information, see Getting Started with AWS Support. For Premium Support information, see AWS Support.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "support:*"
  ],
  "Resource": "*"
 }]
}
```

AWSMarketplaceManageSubscriptions

`AWSMarketplaceManageSubscriptions` (Public AWS Managed Policy)

Permissions to subscribe, unsubscribe, and view AWS Marketplace subscriptions.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Action": [
   "aws-marketplace:ViewSubscriptions",
   "aws-marketplace:Subscribe",
   "aws-marketplace:Unsubscribe"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

AWSCertificateManagerFullAccess

`AWSCertificateManagerFullAccess`

Full access to AWS Certificate Manager. For Certificate Manager information, see AWS Certificate Manager.

`AWSCertificateManagerFullAccess` information, (Public AWS Managed Policy).

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "acm:*"
  ],
```

```
  "Resource": "*"
 }]
}
```

AWSWAFFullAccess

`AWSWAFFullAccess`

Full access to AWS Web Application Firewall (WAF). For WAF information, see AWS WAF - Web Application Firewall.

`AWSWAFFullAccess` information, (Public AWS Managed policy). This policy grants full access to AWS WAF resources.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Action": [
   "waf:*",
   "waf-regional:*",
   "elasticloadbalancing:SetWebACL"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

ReadOnlyAccess

`ReadOnlyAccess` (actions a-l only)

Read-only access to all AWS services and resources on the AWS console.

When AWS launches a new service, AMS updates the ReadOnlyAccess policy to add read-only permissions for the new service. The updated permissions are applied to all principal entities that the policy is attached to.

This doesn't grant the ability to log into EC2 hosts or database hosts.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Action": [
   "aws-marketplace:ViewSubscriptions",
   "aws-marketplace:Subscribe",
   "aws-marketplace:Unsubscribe"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

Single-Account Landing Zone (SALZ): To see the AMS single-account landing zone default, uncustomized, user role policies, see Default AMS single-account landing zone (SALZ) IAM User Role (p. 332), next.

Default AMS single-account landing zone (SALZ) IAM User Role

JSON policy statements for the default AMS single-account landing zone user role.

Note
The SALZ default user role is customizable and may differ on a per-account basis. Instructions on finding your role are provided.

This is an example of the default SALZ user role, but to make sure that you have the policies set for you, run the AWS command `get-role` or sign in to the AWS Management -> IAM console at https://console.aws.amazon.com/iam/. In the IAM console, in the navigation pane, choose **Roles**.

The customer read-only role is a combination of multiple policies. A breakdown of the role (JSON) follows.

Managed Services Audit Policy:

```
{"Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "BasicConsoleAccess",
      "Effect": "Allow",
      "Action": [
        "aws-portal:View*",
        "ec2-reports:View*",
        "support:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AuditAccessToAWSServices",
      "Effect": "Allow",
      "Action": [
        "acm:Describe*",
        "acm:List*",
        "appstream:Get*",
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codecommit:Get*",
        "codecommit:List*",
        "codedeploy:BatchGet*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:Get*",
        "codepipeline:List*",
        "config:Describe*",
        "config:Get*",
        "datapipeline:Describe*",
        "datapipeline:EvaluateExpression",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:ValidatePipelineDefinition",
        "directconnect:Describe*",
```

```
        "ds:Describe*",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "ec2:Describe*",
        "ec2:Get*",
        "ecs:Describe*",
        "ecs:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "events:Describe*",
        "events:Get*",
        "events:List*",
        "guardduty:Get*",
        "guardduty:List*",
        "kinesis:Describe*",
        "kinesis:List*",
        "kms:List*",
        "lambda:Get*",
        "lambda:List*",
        "macie:Describe*",
        "macie:Get*",
        "macie:List*",
        "opsworks:Describe*",
        "opsworks:Get*",
        "rds:Describe*",
        "rds:Download*",
        "rds:List*",
        "redshift:Describe*",
        "redshift:View*",
        "route53:Get*",
        "route53:List*",
        "route53domains:CheckDomainAvailability",
        "route53domains:Get*",
        "route53domains:List*",
        "sdb:Get*",
        "sdb:List*",
        "ses:Get*",
        "ses:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:Get*",
        "sqs:List*",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "tag:get*",
        "trustedadvisor:Describe*",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
```

```
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSManagedServicesFullAccess",
      "Effect": "Allow",
      "Action": [
        "amscm:*",
        "amsskms:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Managed Services IAM ReadOnly Policy

```
{
  "Statement": [
    {
      "Action": [
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccountAliases",
        "iam:ListAttachedRolePolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListMFADevices",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices"
      ],
      "Effect": "Allow",
      "Resource": [
        "*"
      ],
      "Sid": "IAMReadOnlyAccess"
    },
    {
      "Action": [
        "iam:*"
```

```
      ],
      "Effect": "Deny",
      "Resource": [
        "arn:aws:iam::*:group/mc-*",
        "arn:aws:iam::*:group/mc_*",
        "arn:aws:iam::*:policy/mc-*",
        "arn:aws:iam::*:policy/mc_*",
        "arn:aws:iam::*:role/mc-*",
        "arn:aws:iam::*:role/mc_*",
        "arn:aws:iam::*:role/Sentinel-*",
        "arn:aws:iam::*:role/Sentinel_*",
        "arn:aws:iam::*:user/mc-*",
        "arn:aws:iam::*:user/mc_*"
      ],
      "Sid": "DenyAccessToIamRolesStartingWithMC"
    }
  ],
```

Managed Services User Policy

```
"Version": "2012-10-17"
}
 {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomerToListTheLogBucketLogs",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "aws/*",
            "app/*",
            "encrypted",
            "encrypted/",
            "encrypted/app/*"
          ]
        }
      }
    },
    {
      "Sid": "BasicAccessRequiredByS3Console",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid": "AllowCustomerToGetLogs",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/aws/*",
```

```
      "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
    ]
  },
  {
    "Sid": "AllowAccessToOtherObjects",
    "Effect": "Allow",
    "Action": [
      "s3:DeleteObject*",
      "s3:Get*",
      "s3:List*",
      "s3:PutObject*"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "AllowCustomerToListTheLogBucketRoot",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::mc-a*-logs-*"
    ],
    "Condition": {
      "StringEquals": {
        "s3:prefix": [
          "",
          "/"
        ]
      }
    }
  },
  {
    "Sid": "AllowCustomerCWLConsole",
    "Effect": "Allow",
    "Action": [
      "logs:DescribeLogStreams",
      "logs:DescribeLogGroups"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:*"
    ]
  },
  {
    "Sid": "AllowCustomerCWLAccessLogs",
    "Effect": "Allow",
    "Action": [
      "logs:FilterLogEvents",
      "logs:GetLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/*",
      "arn:aws:logs:*:*:log-group:/infra/*",
      "arn:aws:logs:*:*:log-group:/app/*",
      "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
    ]
  },
  {
    "Sid": "AWSManagedServicesFullAccess",
    "Effect": "Allow",
    "Action": [
      "amscm:*",
      "amsskms:*"
    ],
```

```
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "ModifyAWSBillingPortal",
    "Effect": "Allow",
    "Action": [
      "aws-portal:Modify*"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "DenyDeleteCWL",
    "Effect": "Deny",
    "Action": [
      "logs:DeleteLogGroup",
      "logs:DeleteLogStream"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:*"
    ]
  },
  {
    "Sid": "DenyMCCWL",
    "Effect": "Deny",
    "Action": [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:FilterLogEvents",
      "logs:GetLogEvents",
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/mc/*"
    ]
  },
  {
    "Sid": "DenyS3MCNamespace",
    "Effect": "Deny",
    "Action": [
      "s3:*"
    ],
    "Resource": [
      "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
      "arn:aws:s3:::mc-a*-logs-*/mc/*",
      "arn:aws:s3:::mc-a*-logs-*-audit/*",
      "arn:aws:s3:::mc-a*-internal-*/*",
      "arn:aws:s3:::mc-a*-internal-*"
    ]
  },
  {
    "Sid": "ExplicitDenyS3CfnBucket",
    "Effect": "Deny",
    "Action": [
      "s3:*"
    ],
    "Resource": [
      "arn:aws:s3:::cf-templates-*"
    ]
  },
  {
    "Sid": "DenyListBucketS3LogsMC",
```

```
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "auditlog/*",
            "encrypted/mc/*",
            "mc/*"
          ]
        }
      }
    },
    {
      "Sid": "DenyS3LogsDelete",
      "Effect": "Deny",
      "Action": [
        "s3:Delete*",
        "s3:Put*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/*"
      ]
    },
    {
      "Sid": "DenyAccessToKmsKeysStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "kms:*"
      ],
      "Resource": [
        "arn:aws:kms::*:key/mc-*",
        "arn:aws:kms::*:alias/mc-*"
      ]
    },
    {
      "Sid": "DenyListingOfStacksStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/mc-*"
      ]
    },
    {
      "Sid": "AllowCreateCWMetricsAndManageDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCreateandDeleteCWDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
      ],
```

```
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Customer Secrets Manager Shared Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
        "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
      ]
    },
   {
      "Sid": "DenyCustomerGetSecretCustomerNamespace",
      "Effect": "Deny",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    },
    {
      "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
      "Effect": "Deny",
      "NotAction": [
        "secretsmanager:Describe*",
        "secretsmanager:Get*",
        "secretsmanager:List*"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
    }
  ]
}
```

Customer Marketplace Subscribe Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
```

```
}
```

AWS Certificate Manager (ACM) certificate

AMS now has a CT, Deployment | Advanced stack components | ACM certificate with additional SANs | Create (ct-3l14e139i5p50), that you can use to submit a request for an AWS Certificate Manager certificate, with up to five additional Subject alternative names (SAN) (such as example.com, example.net, and example.org). For details, see What Is AWS Certificate Manager? and ACM Certificate Characteristic.

> **Note**
> This timeout setting isn't just about the run, but also your validation of the ACM certificate through email validation. Without your validation, the RFC fails.

Security event logging and monitoring

AMS continuously monitors the managed environment for security threats. Security events might be detected by AMS or by you. AMS regularly updates its automation process—based on the Computer Security Incident Handling Guide by the National Institute of Standards and Technology (NIST)—to better detect security threats.

Endpoint Security (EPS)

Resources that you provision in your AMS Advanced environment automatically include the installation of an endpoint security (EPS) monitoring client. This process ensures that the AMS Advanced-managed resources are monitored and supported 24x7. In addition, AMS Advanced monitors all agent activity, and an incident is created if any security event is detected.

> **Note**
> Security incidents are handled as incidents; for more information, see Incident response.

Endpoint Security provides anti-malware protection, specifically, the following actions are supported:

- EC2 instances register with EPS
- EC2 instances deregister from EPS
- EC2 instances real-time anti-malware protection
- EPS agent-initiated heartbeat
- EPS restore quarantined file
- EPS event notification
- EPS reporting

AMS Advanced uses Trend Micro for endpoint security (EPS). These are the default EPS settings. To learn more about Trend Micro, see the Trend Micro Deep Security Help Center; note that non-Amazon links may change without notice to us.

AMS Advanced Multi-Account Landing Zone (MALZ) default settings are described in the following sections; for non-default AMS multi-account landing zone EPS settings, see AMS Advanced Multi-Account Landing Zone EPS non-default settings.

> **Note**
> You can bring your own EPS, see AMS bring your own EPS.

General EPS settings

Endpoint security general network settings.

EPS defaults

Setting	Default
Firewall Ports (Instances' Security Group)	EPS Deep Security Manager agents (DSMs) must have port 4120 open for the Agent/Relay to Manager communication, and port 4119 for the Manager Console. EPS Relays must have port 4122 open for the Manager/Agent to Relay communication. No specific ports should be open for customer instance inbound communication because agents initiate all requests.
Communication Direction	Agent/Appliance Initiated
Heartbeat Interval	Ten minutes
Number of missed heartbeats before an alert	Two
Maximum allowed drift (difference) between server times	Unlimited
Raise offline errors for inactive (registered, but not online) virtual machines	No
Default policy	Base policy (described next)
Activation of multiple computers with the same host name	Is allowed
Alerts for pending updates are raised	After seven days
Update source	Trend Micro Update Server (https://ipv6-iaus.trendmicro.com/iau_server.dll/)
Event or log data deletion	Events and logs are deleted from the DSM database after seven days.
Agent software versions are held	Up to five
Most recent rule updates are held	Up to ten
Logs storage	By default, log files are stored securely in Amazon S3, but you can also archive them to Amazon Glacier to help meet audit and compliance requirements.

Base policy

Endpoint security base policy default settings.

EPS base policy

Setting	Default
Enabled Modules	Anti-Malware
Disabled Modules	Web Reputation
	Firewall
	Intrusion Protection
	Integrity Monitoring
	Log Inspection
	Application Control

Anti-malware

Endpoint security anti-malware settings.

EPS anti-malware defaults

Setting	Default	Notes
Real-Time Scan	Scan everything Every Day/All Day (24 hours)	Quarantine all suspected viruses. Enable IntelliTrap and spyware/grayware protection. Spyware and Grayware trigger Anti-Malware and result in a quarantine of the item.
Manual Scan	Scan everything	Must be requested, then follows default real-time scan configuration.
Scheduled Scan	Scan everything	Set for the last Sunday of every month, 6am.
Smart Protection	Disabled	N/A
Quarantined Files	Trend Micro Deep Security Manager (DSM)	Appx 1GB of disk reserved for quarantine.
Scan Limitation	Trend Micro DSM	Scan files of all sizes.
Allowed Spyware or Grayware	None	N/A
Local Event Notification	Yes	N/A

Malware mitigation process

AMS uses Trend Micro's Deep Security Platform (anti-malware system) to detect and respond to malware on your AMS-managed instances. By default, the Trend Micro detection agent runs on all Amazon EC2 instances, including those in the shared services and private subnets, for both Windows and Linux operating systems. The anti-malware system is connected to AMS monitoring so that an event is generated whenever malware is detected. If there is customer impact, the event is escalated to the incident management process (for details, see AMS incident response (p. 346)). While AMS assesses the impact, you are notified, and attempts are made to mitigate the impact.

Trend Micro anti-malware definitions are updated automatically when Trend Micro publishes updates.

During application onboarding, you indicate the action you want AMS to take when malware is found on an instance:

- Make sure the quarantined file is on the allow list, removing it from the quarantine and releasing it back to the file system.
- Delete the quarantined file, removing it from the instance.
- Suspend the instance and replace it. The suspended instance is then available to you to mount for forensic research.

After application onboarding:

- When the anti-malware system discovers malware on an instance, AMS automatically quarantines the malware. This triggers an event and a follow-up investigation.
- AMS notifies you of the event through a service notification and starts following the default mitigation action that you selected.
- If you haven't chosen a default action, AMS asks you which action to take. After receiving your instructions, AMS runs the selected action and notifies you. AMS notifies you again after the action is complete, including details needed for forensic analysis, if applicable.

Enable IDS and IPS in Trend Micro Deep Security

You can request that AMS enable Trend Micro Intrusion Detection System (IDS) and Intrusion Protection Systems (IPS), non-default features, for your account.

To do this, submit an update request (Management | Other | Other | Update) and include a list of email addresses to receive IDS and IPS notifications. These addresses are added to an SNS topic in your account, which AMS creates for you.

> **Note**
> AMS cannot add any Trend Micro service that might interfere with our ability to provide other AMS services.

Full system malware scans

The Payment Card Industry Data Security Standard (PCI DSS) requires full system malware scans, which are enabled on your AMS-managed VPC by default. Full system scans are set to occur at 2AM (on the time zone set on the server) because they use a lot of CPU. Full system scans are in addition to regular malware scans that do not use a lot of CPU.

There is a new Management change type (CT), **Disable malware scans**, that allows you to disable full system malware scans. You can find the CT in the Management | Host security | Full system scan | Disable classification, change ID ct-1pybwg08h8qsz. To re-enable scans, use the Management | Other | Other | Update CT. Disabling full system scans does not disable your regular malware scans.

Amazon Inspector security

The Amazon Inspector service monitors the security of your AMS-managed stacks. Amazon Inspector is an automated security assessment service that helps identify gaps in the security and compliance of infrastructure deployed on AWS. Amazon Inspector security assessments enable you to automatically assess stacks for exposure, vulnerabilities, and deviations from best practices by checking for unintended network accessibility and vulnerabilities in your Amazon EC2 instances. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. Amazon Inspector assessments are offered as pre-defined rules packages mapped to common security best practices and definitions. These rules are regularly updated by AWS security researchers. For more information about Amazon Inspector go to Amazon Inspector.

AMS Amazon Inspector FAQs

- Is Amazon Inspector installed to my AMS accounts by default?

  No. Amazon Inspector is not part of the default AMI build or workload ingestion.
- How do I access and install Amazon Inspector?

  Submit an RFC (Management | Other | Other | Create) to request account access and installation to Inspector and the AMS operations team will modify the Customer_ReadOnly_Role to provide Amazon Inspector console access (without SSM access).
- Does the Amazon Inspector Agent have to be installed on all of the Amazon EC2 instances I want to assess?

  No, Amazon Inspector assessments with the network reachability rules package can be run without an agent for any Amazon EC2 instances. The agent is required for host assessment rules packages. For more information about agent installation, see Installing Amazon Inspector Agents.
- Is there an additional cost for this service?

  Yes. Amazon Inspector pricing can be found on the Amazon Inspector pricing site.
- What are Amazon Inspector findings?

  Findings are potential security issues discovered during the Amazon Inspector assessment of the selected assessment target. Findings are displayed in the Amazon Inspector console or the API, and contain both a detailed description of the security issues and recommendations for resolving them.
- Are reports of the Amazon Inspector assessment available?

  Yes. An assessment report is a document that details what is tested in the assessment run, and the results of the assessment. The results of your assessment are formatted into standard reports, which can be generated to share results within your team for remediation actions, to enrich compliance audit data, or to store for future reference. An Amazon Inspector assessment report can be generated for an assessment run once it has been successfully completed.
- Can I use tags to identify the stacks I want to run Amazon Inspector reports against?

  Yes.
- Will AMS Operations teams have access to the Amazon Inspector assessment results?

  Yes. Anyone with access to the Amazon Inspector console in AWS is able to view findings and assessment reports.
- Will AMS Operations teams recommend or take action based on the findings of the Amazon Inspector reports?

  No. If you want changes made based on the findings of the Amazon Inspector report, you must request changes through an RFC (Management | Other | Other | Update).
- Will AMS be notified when I run an Amazon Inspector report?

When you request Amazon Inspector access, the AMS Operator running the RFC notifies your CSDM of the request.

For more information, see Amazon Inspector FAQs.

AMS incident response

AMS uses traditional IT service management (ITSM) incident management best practices to restore service, when needed, as quickly as possible.

We provide 24/7/365 follow-the-sun support through multiple operations centers around the world with dedicated operators actively monitoring dashboards and incident queues.

Our operations engineers use internal incident tracking tools to identify, log, categorize, prioritize, diagnose, resolve, and close incidents and provide updates on all of these activities to you through the AMS console or through the AWS Support API. Our operators, many of whom have spent time in AWS Premium Support in various technology profiles and roles, leverage a variety of internal AWS support tools to help with all of those activities. These operators are deeply familiar with AMS supported infrastructures and have expert level technical skills to address all identified support issues. In the rare case where our operators need assistance, the Premium Support and AWS Service teams are available to assist as needed.

In cases where High priority incidents are impacting your critical workloads, AMS will recommend an infrastructure restore. There is often a tradeoff between troubleshooting an issue or restoring from a known good backup, and customer risks and impacts from service downtime are the deciding factors. If you have time to devote to troubleshooting issues, AMS will assist you, but if the urgency to restore is high, we can initiate a restore right away.

Note
Ephemeral data that is not part of the stack template or data restore is lost. AMS uses reasonable efforts to perform infrastructure restore while AWS service offerings are unavailable. Infrastructure restore is completed once AWS service offerings are available.
If you don't authorize an infrastructure restore as recommended by AMS, you won't be eligible for a service credit for the AMS service commitment for incident resolution time.

Compliance validation

AMS deploys and manages a library of AWS Config rules and remediation actions, grouped in conformance packs, to protect against misconfigurations that could reduce the security and operational integrity of your accounts.

Conformance packs are a collection of AWS Config Rules and remediation actions that AMS deploys and manages in your accounts. These conformance packs are industry-standard compliance checks that track the configuration changes that occur among your resources, and determine whether these changes violate any rule conditions.

As an example, when an Amazon S3 bucket is created, AWS Config can evaluate the Amazon S3 bucket against a rule that requires Amazon S3 buckets to deny public read access. If the Amazon S3 bucket policy or bucket access control list (ACL), allows public read access, AWS Config flags both the bucket and the rule as noncompliant. These AWS Config Rules mark resources as either Compliant, Noncompliant, or Not Applicable, based on the result of their evaluation. For more information about AWS Config service, see the AWS Config Developer Guide.

You can use the AWS Config console, AWS CLI, or AWS Config API to view the rules deployed in your account and the compliance state of your rules and resources. For more information, see the AWS Config documentation: Viewing Configuration Compliance.

Note
Additional information on this topic is available through the AMS console **Documentation**; this information is not included in this guide because it contains sensitive AMS security content. To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.

Resilience

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS global infrastructure.

Infrastructure security

Note
Additional information on this topic is available through the AMS console **Documentation**; this information is not included in this guide because it contains sensitive AMS security content. To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.

Security control for end-of-support operating systems

Operating systems that are outside of the general support period of the operating system manufacturer's "end-of-support" or EOS, and do not receive security updates, have an increased security risk.

AWS offers some services to help with handling operation system end-of-support. For information about Windows end-of-support, see End-of-Support Migration Program for Windows Server.

Note
Additional information on this topic is available through the AMS console **Documentation**; this information is not included in this guide because it contains sensitive AMS security content. To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.

Using security groups

A security group acts as a virtual firewall that controls the traffic for one or more instances. AMS security groups allow you to set inbound traffic rules and outbound traffic rules on an instance-level basis. You can create a security group and specify resources in your AMS account, Amazon EC2 instances, Amazon RDS DB instances, Load Balancers, Deep Security Manager (DSM) replication instances, EFS mount targets, and ElastiCache clusters, to associate with the security group. Once associated, traffic to or from those instances is constrained by the rules set in the security group.

To better understand general AWS security, see Best Practices for Security, Identity, & Compliance and Amazon Amazon EC2 Security Groups for Linux Instances.

AMS now has a set of change types for creating and managing security groups:

- Deployment | Advanced stack components | Security group | Create (ct-1oxx2g2d7hc90)
- Management | Advanced stack components | Security group | Delete (ct-3cp96z7r065e4)
- Management | Advanced stack components | Security group | Update (ct-3memthlcmvc1b)

For examples, see Security groups.

Security groups

In AWS VPCs, AWS Security Groups act as virtual firewalls, controlling the traffic for one or more stacks (an instance or a set of instances). When a stack is launched, it's associated with one or more security groups, which determine what traffic is allowed to reach it:

- For stacks in your public subnets, the default security groups accept traffic from HTTP (80) and HTTPS (443) from all locations (the internet). The stacks also accept internal SSH and RDP traffic from your corporate network, and AWS bastions. Those stacks can then egress through any port to the Internet. They can also egress to your private subnets and other stacks in your public subnet.
- Stacks in your private subnets can egress to any other stack in your private subnet, and instances within a stack can fully communicate over any protocol with each other.

> **Important**
> The default security group for stacks on private subnets allows all stacks in your private subnet to communicate with other stacks in that private subnet. If you want to restrict communications between stacks within a private subnet, you must create new security groups that describe the restriction. For example, if you want to restrict communications to a database server so that the stacks in that private subnet can only communicate from a specific application server over a specific port, request a special security group. How to do so is described in this section.

Default Security Groups

MALZ

The following table describes the default inbound security group (SG) settings for your stacks. The SG is named "SentinelDefaultSecurityGroupPrivateOnly-vpc-ID" where *ID* is a VPC ID in your AMS multi-account landing zone account. All traffic is allowed outbound to "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" via this security group (all local traffic within stack subnets is allowed).

All traffic is allowed outbound to 0.0.0.0/0 by a second security group "SentinelDefaultSecurityGroupPrivateOnly".

> **Tip**
> If you're choosing a security group for an AMS change type, such as EC2 create, or OpenSearch create domain, you would use one of the default security groups described here, or a security group that you created. You can find the list of security groups, per VPC, in either the AWS EC2 console or VPC console.

There are additional default security groups that are used for internal AMS purposes.

AMS default security groups (inbound traffic)

Type	Protocol	Port range	Source
All traffic	All	All	SentinelDefaultSecurityGroupPrivateOnly (restricts outbound traffic to members of the same security group)
All traffic	All	All	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (does not restrict outbound traffic)
HTTP, HTTPS, SSH, RDP	TCP	80 / 443 (Source 0.0.0.0/0) SSH and RDP access is allowed from bastions	SentinelDefaultSecurityGroupPublic (does not restrict outbound traffic)
MALZ bastions:			
SSH	TCP	22	SharedServices VPC CIDR and DMZ VPC CIDR, plus Customer-provided on-prem CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ bastions:			
SSH	TCP	22	mc-initial-garden-LinuxBastionSG
SSH	TCP	22	mc-initial-garden-LinuxBastionDMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionDMZSG

SALZ

The following table describes the default inbound security group (SG) settings for your stacks. The SG is named "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly-*ID*" where *ID* is a unique identifier. All traffic is allowed outbound to "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" via this security group (all local traffic within stack subnets is allowed).

All traffic is allowed outbound to 0.0.0.0/0 by a second security group "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnlyEgressAll-*ID*".

> **Tip**
> If you're choosing a security group for an AMS change type, such as EC2 create, or OpenSearch create domain, you would use one of the default security groups described here, or a security group that you created. You can find the list of security groups, per VPC, in either the AWS EC2 console or VPC console.

There are additional default security groups that are used for internal AMS purposes.

AMS default security groups (inbound traffic)

Type	Protocol	Port range	Source
All traffic	All	All	SentinelDefaultSecurityGroupPrivateOnly (restricts outbound traffic to members of the same security group)
All traffic	All	All	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (does not restrict outbound traffic)
HTTP, HTTPS, SSH, RDP	TCP	80 / 443 (Source 0.0.0.0/0) SSH and RDP access is allowed from bastions	SentinelDefaultSecurityGroupPublic (does not restrict outbound traffic)
MALZ bastions:			
SSH	TCP	22	SharedServices VPC CIDR and DMZ VPC CIDR, plus Customer-provided on-prem CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ bastions:			
SSH	TCP	22	mc-initial-garden-LinuxBastionSG
SSH	TCP	22	mc-initial-garden-LinuxBastionDMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionDMZSG

Create, Change, or Delete Security Groups

You can request custom security groups. In cases where the default security groups do not meet the needs of your applications or your organization, you can modify or create new security groups. Such a request would be considered approval-required and would be reviewed by the AMS operations team.

To create a security group outside of stacks and VPCs, submit an RFC using the `Management | Other | Other | Create` CT (ct-1e1xtak34nx76).

To add or remove a user from an Active Directory (AD) security group, submit a request for change (RFC) using the `Management | Other | Other | Update` CT (ct-0xdawir96cy7k).

Note
When using manual (approval required) CTs, AMS recommends that you use the ASAP option (choose **ASAP** in the console, leave start and end time blank in the API/CLI) as these CTs require an AMS operator to examine the RFC, and possibly communicate with you before it can be approved and run. If you schedule these RFCs, be sure to allow at least 24 hours. If approval does not happen before the scheduled start time, the RFC is rejected automatically.

Find Security Groups

To find the security groups attached to a stack or instance, use the EC2 console. After finding the stack or instance, you can see all security groups attached to it.

For ways to find security groups at the command line and filter the output, see `describe-security-groups`.

Security best practices

This section has been redacted because it contains sensitive AMS security-related information. This information is available through the AMS console **Documentation**. To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.

AMS multi-account landing zone EPS non-default settings

This section has been redacted because it contains sensitive AMS security-related information. This information is available through the AMS console **Documentation**. To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.

AMS Guardrails

A guardrail is a high-level rule that provides ongoing governance for your overall AMS environment.

This section has been redacted because it contains sensitive AMS security-related information. This information is available through the AMS console **Documentation**. To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.

MALZ Service control policies

This section has been redacted because it contains sensitive AMS security-related information. This information is available through the AMS console **Documentation**. To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.

MALZ Service control policies

This section has been redacted because it contains sensitive AMS security-related information. This information is available through the AMS console **Documentation**. To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.

Continuity management

Topics

As part of continuity management, AWS Managed Services (AMS) provides automated access to AWS Backup, a native service with AWS. This facilitates access to a service that supports Amazon EBS, Amazon EC2, Amazon RDS, Amazon EFS, and more.

To learn more, see AWS Backup: How It Works.

What is continuity management?

Continuity management is the process AMS uses to provide backups and snapshots for your account.

How continuity management works

AMS uses AWS Backup for continuity management.

Backup vaults

AWS Backup organizes snapshots into logical storage units called vaults. AMS creates standard backup vaults as follows:

- `ams-automated-backups`: This is the default location for all backups from AMS-created backup plans, if no vault name is defined.
- `ams-manual-backups`: This is the default location for all backups from Start Backup Job RFC (ct-2hhud2lx01tq7) backup plans, if no vault name is defined.
- `ams-custom-backups`: This is the default location for all backups from custom backup plans, if no vault name is defined.
- `ams-patch-backups`: This is the default location for the snapshots AMS takes prior to patching an instance using Patch Orchestrator or the monthly patch activities. These are automatically removed according to the AMS patch lifecycle default policy of 60 days.

AMS backup plans

A backup plan is a policy expression that defines when and how you want to back up supported AWS resources, such as RDS databases, EBS volumes, DynamoDB tables, and EFS file systems. Scheduling and retention policies are managed via custom backup plans, which you can create using a change type (CT) with AMS Advanced or using AWS Backup with AMS Accelerate. Assign resources to your backup plans using tags and AWS Backup automatically backs up and retains backups for assigned resources according to the defined backup plan. You can create multiple backup plans if you have workloads with different backup requirements.

Note
AWS Backup can operate at the EBS volume level or at the Amazon EC2 instance level, but it is not recommended to do both at the same time, as this can lead to a race condition where the backups may clash.

A backup plan can have up to six backup rules that define a schedule and a retention period, among other details. The backup schedule determines when AWS Backup initiates a backup job and how often a backup is created. You can choose a frequency of hourly, daily, weekly, or monthly. The deletion days setting determines how many days the snapshot is stored before being automatically deleted.

Note
AMS Advanced: If you are migrated from the legacy AMS backup system, AMS creates a default backup plan for backwards compatibility. The **key:value** pair in this scenario is **Backup:True**. To support backwards compatibility, the value here is case insensitive, so **Backup:True** or **Backup:TRUE** are all valid tags. All other key:value pairs are case sensitive.

Default backup plans, AMS Advanced multi-account landing zone

During the new **Account creation** RFC, AMS ensures that there is an overarching default backup plan at the account level to safeguard your workloads. The values for the following mandatory fields are set up by default, as shown below; however, customers can change these values during or after account creation to best suit their business continuity needs.

- **Backup plan name**: default-backup-plan
- **Resource tag key**: Backup
- **Resource tag value**: True
- **Backup rule 1 schedule expression**: cron(0 2 ? * *), that is, set a daily backup for 02:00 UTC time
- **Backup rule 1 delete after days**: 7 days

Backup change types, AMS Advanced

AMS provides several CTs for you to create and use backup plans.

- **Create Backup Plan**:
  - Classification: Deployment | AWS Backup | Backup plan | Create
  - Change type ID: ct-2hyozbpa0sx0m
  - Requirements: You must have tagged the resources you want to include in the backup plan (you specify those tags when you create the backup plan). You can create up to six backup plan rules, each with different schedules and vaults.
  - For details and example, see Backup plan: creating.
- **Start Backup Job**:
  - Management | AWS Backup | Backup job | Start
  - Change type ID: ct-2hhud2lx01tq7
  - Requirements: The Amazon resource name (ARN) of the resource to back up under the existing backup plan.
  - For details and example, see Job: Starting.
- **Stop Backup Job**:
  - Management | AWS Backup | Backup job | Stop
  - Change type ID: ct-1895yr1p87noq
  - Requirements: The identifer of an existing backup job (`BackupJobId`) to stop.

  - For details and example, see Backup job: stopping.
- **Delete Recovery Point**:
  - Management | AWS Backup | Recovery point | Delete
  - Change type ID: ct-1r1vbr8ahr156
  - Requirements: The ARN of the recovery point (backup) to delete.
  - For details and example, see Backup Recovery Point: Deleting.
- **Restore Job Restore EBS**:
  - Management | AWS Backup | Restore job | Restore EBS
  - Change type ID: ct-063qsm82cfxu6
  - Requirements: The ARN (`RecoveryPointArn`) of the recovery point (backup) to restore, plus the availability zone (`AvailabilityZone:`) in which to restore the EBS snapshot, and the name of the container (`BackupVaultName`) where backups are stored.
  - For details and example, see EBS Volume: creating from backup.
- **Restore Job Restore EFS**:
  - Management | AWS Backup | Restore job | Restore EFS
  - Change type ID: ct-0g690ekkyfm79
  - Requirements: The ARN (`RecoveryPointArn`) of the recovery point (backup) to restore, and the name of the container (`BackupVaultName`) where backups are stored.
  - For details and example, see EFS: creating from backup.

Disaster recovery response

In addition to the options described in the following sections, it is good for you to know what steps to take to initiate a disaster recovery (DR) with AMS.

If you experience a disaster and need to initiate a recovery, follow these general guidelines:

1. Open a **High** priority incident with the **Availability** category. AMS will open a conference bridge and invite your team to join.
2. Know the list of resources you need to recover.
3. Know the target Landing Zone you need to recover to (for example, the same account, different AZ or different account and different region).
4. Submit recover requests for each resource in the target landing zone. Follow your existing DR plan or see the options in the following section (for example, Disaster protection for EC2 with EBS snapshots on AMS (p. 359), or Disaster protection for EC2 with CloudEndure on AMS (p. 360)).
5. Restore the application functionality and use AMS assistance to troubleshoot infrastructure-related issues.

AMS can help you with preparing for this event and with creating a DR plan for your organization to cover these questions. For more details, contact your cloud service delivery manager (CSDM) or cloud architect (CA).

Disaster recovery planning

Disaster recovery (DR) is a critical service for enterprise business continuity and compliance. AMS partners with you to help you plan, implement and maintain your DR strategy on AMS.

AMS landing zone (LZ), multi-account and single-account, provides native, multi-AZ, high-availability for AMS infrastructure components that meet most disaster protection scenarios. However, depending on

your business's geographical coverage, you might need regional protection. For cross-region availability and DR, another AMS account is required in a different region (this is so for both multi-account landing zone and single-account landing zone).

AMS aligns with AWS DR guidance as described in this blog, Rapidly recover mission-critical systems in a disaster, and supports the following four options:

- Multi Site (or Highly Available)
- Warm Standby
- Pilot Light
- Backup and Restore

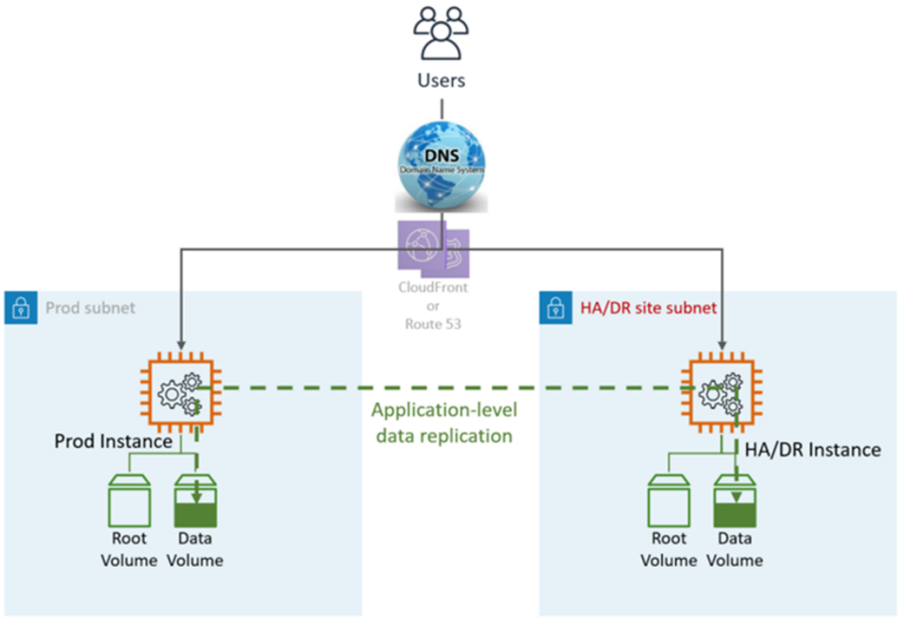
These options and AMS support for them are described in the following sections.

Multi-site or highly available (HA)

The HA solution is usually provided by the application's built-in functionality, such as clustering or synchronous replication. Users are directed to both Prod and HA/DR nodes. DNS points either to the nodes directly or through an elastic load balancer (ELB).

Your AMS cloud architect (CA) will work with you as part of your Well-Architected-Review and DR planning.

HA DR utilizes application and AWS-native services and features, as illustrated in the following graphic:



The DR site can be in the same or different AWS Region.

> **Note**
> Different region (Cross-Region) will have a different Active Directory environment.

DR (failover) steps: Automatic failover, no manual steps are required. In case of a failure in the primary LZ, the users will be automatically re-routed to the DR/HA node. This is achieved by both DNS and application configuration.

HA DR metrics:

- Recovery Point Objective (RPO): <5 min
- Recovery Time Objective and (RTO): <5 min
- Maintenance: High (Synchronous changes are required in both environments, like Application configuration, patching, SG or ALB, certificates, and so on).
- Cost: High

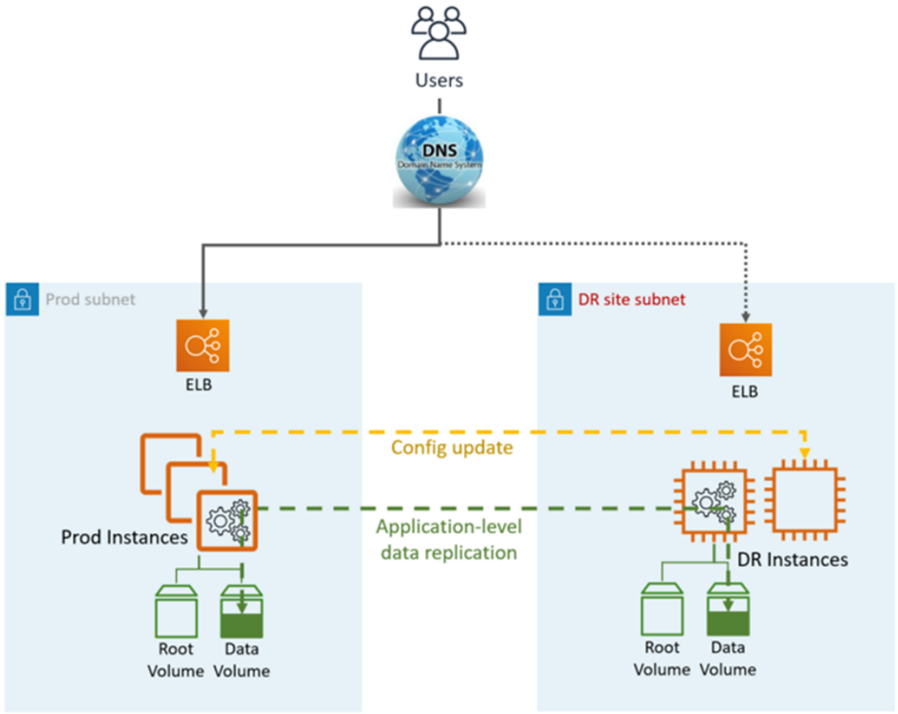
Warm standby

The term "warm standby" is used to describe a disaster recovery (DR) scenario in which a scaled-down version of the environment is running in the cloud.

Data replication is handled by the application layer, usually asynchronously, to an online instance, while the rest of the instances (for example, Application and Web tier) might be turned off to save the cost. Users are directed only to the Production site. Other AWS resources like elastic load balancer (ELB) may be pre-provisioned in the DR site as well.

Your AMS Cloud Architect (CA) will work with you as part of your Well-Architected-Review and DR planning.

Warm Standby DR utilizes application and AWS-native services and features, as illustrated in the following graphic:



DR site can be in the same or different AWS Region.

> **Note**
> Different region (Cross-Region) will have a different Active Directory environment.

DR (failover) steps:

1. Brake the data replication and make the data instance in the DR site the master
2. Update application configuration as required (new IP, server name, and so on)

3. Redirect DNS to the DR site (ELB)
4. AD Dependencies if required (Service accounts, SPNs, GPOs, and so on)

HA DR metrics:

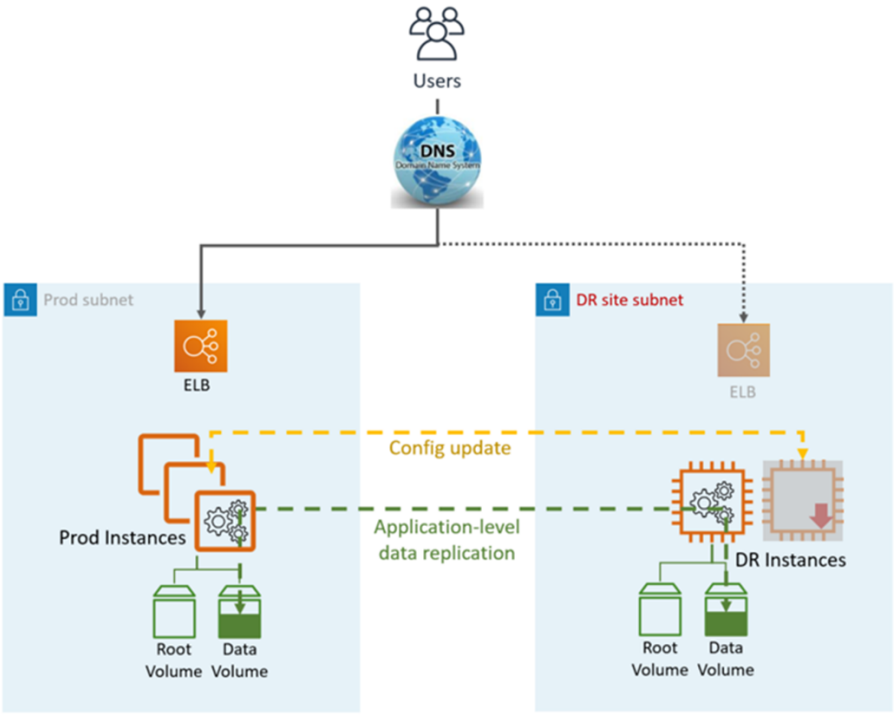
- Recovery Point Objective (RPO): <1hr
- Recovery Time Objective and (RTO): <1 hr (depends on the number of instances and orchestration)
- Maintenance: High (Synchronous changes are required in both environments, like Application configuration, patching, security groups (SG) or application load balancer (ALB), certificates, and so on).
- Cost: Medium

Pilot light

In this disaster recovery (DR) approach, you replicate part of your Prod environment for a limited set of core services. A small part of your infrastructure is always running, simultaneously syncing mutable data (such as databases or documents), while other parts of your infrastructure are switched off and used only during testing. Unlike a backup and recovery approach, you must ensure that your most critical core elements are already configured and running in the DR landing zone (the pilot light).

Your AMS Cloud Architect will work with you as part of your Well-Architected-Review and DR planning.

Pilot Light DR utilizes application and AWS-native services and features, as illustrated in the following graphic:



DR site can be in the same or different AWS Region.

> **Note**
> Different region (Cross-Region) will have a different Active Directory environment.

DR (failover) steps:

1. Brake the data replication and make the data instance in the DR site the master
2. Start the turned off instances and infrastructure
3. Update application configuration as required (new IP, server name, and so on)
4. Add the instances to the ELB as required
5. Redirect DNS to the DR site (ELB)
6. AD Dependencies, if required (Service accounts, SPNs, GPOs, and so on)

Pilot Light DR metrics:

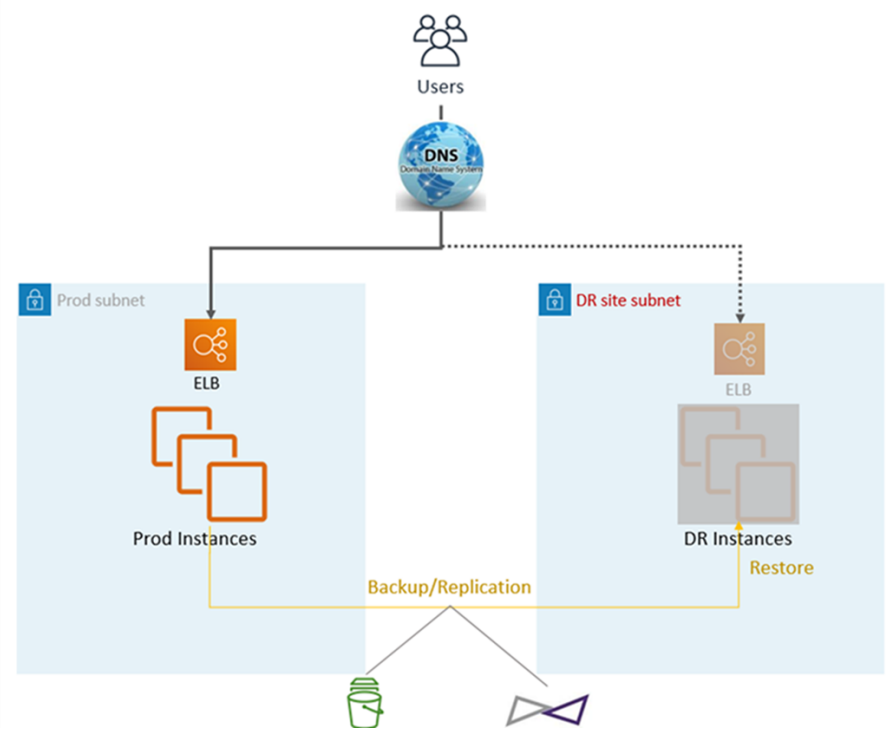
- Recovery Point Objective (RPO): <1hr
- Recovery Time Objective and (RTO): ~1 hr (depends on the number of instances and orchestration)
- Maintenance: Medium
- Cost: Medium

Backup and restore

This simple and low cost disaster recovery (DR) approach backs up your data and applications from anywhere to the DR landing zone for use during recovery from a disaster.

Your AMS Cloud Architect will work with you as part of your Backup and DR planning.

Backup and Restore DR utilizes AMS automated tooling and processes, as illustrated in the following graphic:



Two backup and replication methods can be used:

- EBS snapshot (Recovery Point Objective (RPO) > 1hr), known as "EBS"
- CloudEndure (Recovery Point Objective (RPO) ~ 0.25hrs), known as "CE"

The DR site can be in the same or different AWS Region.

> **Note**
> Different region (Cross-Region) will have a different Active Directory environment.

DR (failover) steps:

1. Restore the instances from snapshots (two-step process with placeholder instance first)
2. Update application configuration (new IP, server namea,nd so on)
3. Set up other infrastructure as required (SG, ELB, and so on)
4. Redirect DNS to the DR site (ELB)
5. Update or restore AD dependencies if required (service accounts, service principal names (SPNs), group policy objects (GPOs), and so on)

Backup and Restore DR metrics:

- Recovery Point Objective (RPO): >1hr or ~0.25hrs (depends on the solution selected - EBS or CE)
- Recovery Time Objective and (RTO): ~1 hr (depends on the number of instances and orchestration)
- Maintenance: High (Synchronous changes are required in both environments, like application configuration, patching, security groups or application load balancers, certificates, and so on.
- Cost: Medium

Disaster protection for EC2 with EBS snapshots on AMS

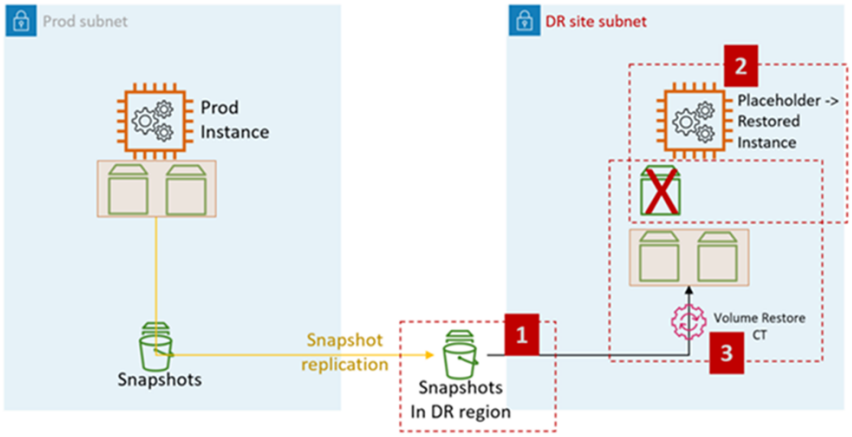
Prerequisites:

- AMS Prod Landing Zone (source)
- AMS DR Landing Zone (DR target)
- EBS snapshots are enabled for EC2 instances (AWS Backup)

Snapshot replication solution:

- **Cross AZ**: Not applicable - EBS snapshot are highly available within the Region by design
- **Cross-Region**: AWS Backup

The following diagram represents the EC2 restore process from EBS snapshots on AMS:



EC2 DR steps on AMS:

1. Raise an RFC to share the EBS snapshots with the target account (required for Cross-Region DR).

   : Management, Advanced Stack Components, EBS Snapshot, Share
2. Create a placeholder EC2 AMS stack in the destination subnet (DR site subnet). The recommendation is to use CFN ingestion to create the stack as the customer can combine the steps of assigning security groups and other (like adding the instance to an ELB) in the same stack.

   Change type: Deployment, Ingestion, Stack from CloudFormation Template, Create
3. Raise an RFC to perform EC2 stack volume restore.

   Change type: Management, Advanced Stack Components, EC2 instance stack, Restore volumes.

   The CT restores the volumes from the snapshots shared in step 1 and attaches to the placeholder instance created in step 2.

Volume Restore CT functionality:

- Shut the placeholder instance down
- Restore volumes from the snapshots
- Swap out the volumes
- Start the instance
- Leave the old domain
- Change the hostname
- Reboot. AMS bootstrap scripts join the instance to the target (DR) domain upon start up

Volume restore CT input:

- InstanceId (placeholder instance ID)
- RootDeviceSnapshotId, the EBS snapshot for the restored root volume
- KMSKeyId, the KMS key identifier, or ARN, to encrypt all restored volumes on the EC2 instance
- DeviceNames, up to 25 (optional)
- SnapshotIds, up to 25 (optional). List of snapshots of the volumes to be restored

Disaster protection for EC2 with CloudEndure on AMS

Prerequisites:

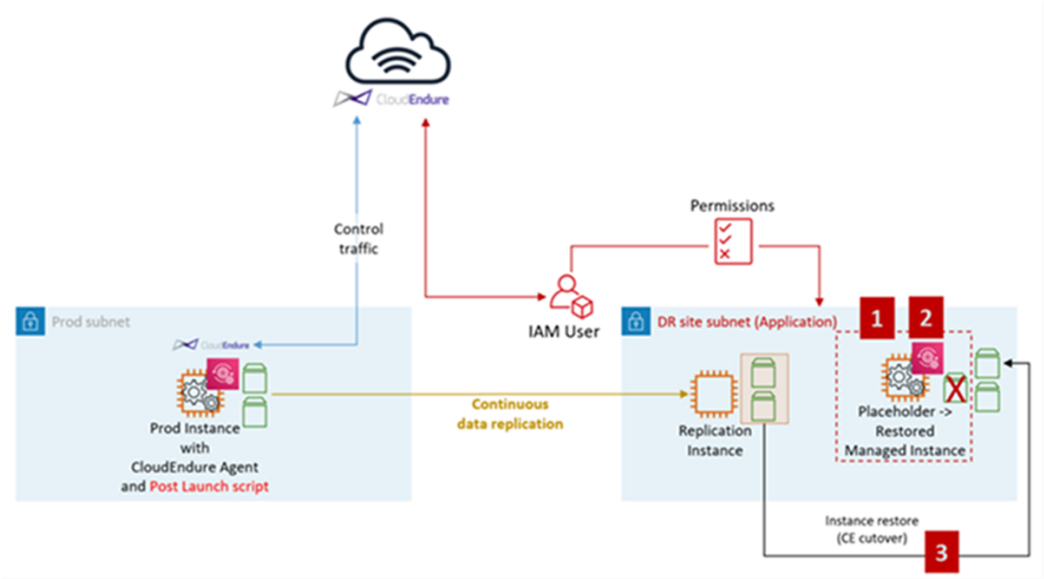
- AMS Prod Landing Zone (source)
- AMS DR Landing Zone (DR target)

Create an IAM user in the DR LZ. See Migration CloudEndure documentation for the setup details (Note: The Migration subnet is not needed for the DR setup), the main difference will be that the setup is permanent as opposed to temporary like in case of migration. Other differences:

- No Migration subnet, skip steps 2, 3, 4, 5
- IAM user should have access to application subnets in the DR zone
- Step 8 is not performed, skip
- Important: Source instance should have Post Launch script configured. See this CE guide. The script will be provided by your AMS Cloud Architect.

- Destination (Placeholder) instance and its EBS volume should have a tag key: "CloudEndure creation time", value: <Anything>. Otherwise, CloudEndure won't be able to restore on top of the Placeholder instance.

The diagram below represents the CloudEndure setup and restore process for EC2 on AMS.



EC2 DR steps with CloudEndure on AMS:

1. Create a placeholder EC2 AMS stack in the destination subnet (DR site subnet) with proper tags, for more information, see the previous section. We recommend using CFN ingestion to create the stack as you can combine the steps of assigning security groups and tagging the instance, EBS volume, and other (like adding the instance to an ELB) in the same stack.

   Change type: Deployment, Ingestion, Stack from CloudFormation Template, Create
2. Stop the placeholder instance.

   Change type: Management, Advanced stack components, EC2 instance, Stop
3. If not done in step 1, tag the placeholder instance and its EBS volume with key: "CloudEndure creation time", value: <Anything>.

   Change type: Management, Advanced stack components, Tag, Update.
4. Initiate instance restore (cutover) from the CloudEndure console. Use the placeholder instance from step 1 as the target.

   Note
   The placeholder instance volumes are retained in the account. To delete these volumes, submit a Management | Other | Other change type at the end of the disaster recovery operation.

CloudEndure restore (cutover) workflow:

- The target (placeholder) instance needs to be in the stopped state
- Swap out the volumes and delete the source (placeholder) root volume
- Start the instance
- Run the Post Launch script, which will:

- Leave the old domain
- Change the hostname
- Reboot. AMS bootstrap scripts join the instance to the target (DR) domain during the startup.

Patch management

Topics

In AMS, patch management is a service that helps you maintain OS vendor updates on your Amazon Elastic Compute Cloud (Amazon EC2) instances. You have the freedom to customize the frequency and process of patching your Amazon EC2 instances.

You configure patch management during onboarding, and you can update it by using the RFC process. Stacks created using the change management system and a patch-compatible template (for Amazon EC2, Auto Scaling group, HA one-tier or two-tier stack) are subscribed to patch management automatically.

AMS provides the following methods for configuring patching:

- Patch orchestrator – Tag-based patching
- AMS standard patch – Account-based patching

For definitions of patching terms, see Key terms (p. 3).

Important

- It's not possible for stacks or a stack's constituent instances to opt out of patch management, if the AMS template from which the stack is created is compatible with patch management. Currently, patching is compatible with the following stack templates:
  - Amazon EC2 stack | Create, and Amazon EC2 stack | Create (with additional volumes)
  - Amazon EC2 instance launched with AWS CloudFormation ingest
  - Auto Scaling group | Create (the Amazon EC2 instances in the group are patched)
  - High Availability One-Tier stack | Create, and High Availability Two-Tier stack | Create
- If there is an ongoing incident that affects a stack, AMS operators can reschedule or cancel scheduled patching.
- By default, all instances within a particular patch-compatible stack are patched in-place. To patch Auto Scaling groups with an Amazon Machine Image (AMI) replacement using the latest/patched AMS AMI, submit a service request. Updated AMIs are shared to accounts every month.

Tip
AMS recommends that you enable backups for instances that have valuable applications or services. For information about enabling backups, see Continuity management (p. 352).

AMS Patch Orchestrator: a tag-based patching model

If you have been onboarded to the new AMS Patch Orchestrator tag-based patching model, you can use tags to apply your patch configuration to a precise set of resources, called a *patch group*, ranging from

one instance to all of your instances. For information about AMS tags, see Using tags. Instructions on setting up Patch Orchestrator tags are provided in the following section.

Patches are installed during the patch windows you define with the SSM Patch Window: creating. Each patch window is an AWS Systems Manager maintenance window that runs on a schedule of your choice, has a configured duration, and applies to one patch group. Instances that are not part of an explicit patch window are patched during the default maintenance window that you define when you onboard to Patch Orchestrator.

> **Important**
> If multiple patch maintenance windows are scheduled to run at the same time, they must have fewer than 1001 instances being processed at any given time. This is an AWS Systems Manager limitation. AMS recommends at least 1 hour per every 50 instances.

By default, all operating system (OS) vendor-provided patches are installed during a maintenance window or an on-demand patch. This is called the *default patch baseline*. If you would like to restrict which patches are installed, you can define a custom patch baseline with the SSM Patch Baseline: creating. For example, you can use a custom patch baseline to ensure that only critical and important security updates are installed for one or more patch groups.

After patches are installed on an instance, the instance is rebooted. Patch notifications are sent before and after patching, and an additional reminder is sent within 96 hours before the scheduled start. In addition, AMS applies updates to infrastructure management tools (such as the AWS SSM agent) during the selected maintenance window.

> **Important**
> AMS is deprecating the monthly patch compliance reporting of instances with missing patches, and will not be sending monthly reports. This change has been made in view of the recently released self-serve operational reports that refresh every 24 hours and are available to you on demand and provide the most recent and granular data. To learn more about the reports, see Self-service reporting. To learn more about the reports, see Self-service reporting (p. 147).

For more information on the notifications, see Patch notifications (p. 368).

Using Patch Orchestrator

Enable AMS Patch Orchestrator for your account by submitting a service request that includes the following details:

- **Category**: Other
- **Subject**: Onboard to Patch Orchestrator
- **CC Emails**: CC email addresses receive notifications when the status of this onboarding RFC changes
- **Details**: Paste the following information into the email and provide your values. Note that the ThirdTagKey is optional. For recommendations and examples, see the following table.

```
Default maintenance window Schedule:
Default Maintenance Window Schedule TimeZone:
Default Maintenance Window Duration:
Default Maintenance Window Cutoff:
Default Patch Backup Retention In Days:
Default Maintenance Window Notification Emails:
First Tag Key:
Second Tag Key:
Third Tag Key:
```

The following table describes the format and recommendations for your provided values.

Patch orchestrator tag-based patching configurations

Name of parameter	Information	Recommendation or example
Default Maintenance Window Schedule	The schedule of the default maintenance window in the form of a cron or rate expression. For example: • `cron(0 3 ? * 6L *)`: 03:00 am on the last Friday of every month • `rate(7 days)`: Every seven days For more information about creating cron expressions, and links to cron and rate expression resources, see Cron and rate expressions for maintenance windows.	We recommend having the window run at least once per month on a consistent weekday.
Default Maintenance Window Schedule Time Zone	The time zone that the default maintenance window runs are based on, in Internet Assigned Numbers Authority (IANA) format.	For example: • America/Los_Angeles • etc/UTC
Default Maintenance Window Duration	The duration of the default maintenance window in hours.	At least 1 hour per every 50 instances, plus 2 hours for cutoff.
Default Maintenance Window Cutoff	The number of hours before the end of the Default Maintenance Window in which no new patching commands are started. This interval exists to allow enough time for patching to complete before the window ends.	At least 2 hours.
Default Patch Backup Retention In Days (optional)	The default time in days to keep the EBS restore points created before patching instances.	We recommend keeping the default, which is 60.
Default Maintenance Window Notification Emails	One to five email addresses or distribution lists to receive notifications about default maintenance window patching status.	We recommend using group distribution lists instead of individual emails.
First Tag Key	The first tag-key to use for creating your Patch Group tag values.	For example, AppId. Specify **null** if you already have defined your own patch groups with a Patch Group tag.

Name of parameter	Information	Recommendation or example
Second Tag Key	The second tag-key to use for creating your Patch Group tag values.	For example, Environment. Specify **null** if you have already defined your own patch groups with a Patch Group tag.
Third Tag Key (optional)	The optional third tag-key to use for creating your Patch Group tag values.	For example, Group.

After you're onboarded to the new Patch Orchestrator patching service model, all appropriately tagged instances in your account belong to a patch group with a Patch Group tag. Patch Orchestrator uses either your existing Patch Group tag, or an AMS-created tag consisting of the two or three concatenated tag values that you specified during Patch Orchestrator onboarding. For example, {*Tag Value 1*}-{*Tag Value 2*}-{*Tag Value 3*}. AMS updates these AMS-applied Patch Group tags are every 12 hours. If needed, you can update your Patch Group tag values with the Tags: updating (review required) or Tags: updating (review required) change types.

For example, if your Amazon EC2 instance has the following tag key:value pairs:

- `AppId:MyApplication`
- `Environment:Production`
- `Group:1`

During onboarding you specified the following tag keys:

- `First Tag Key = AppId`
- `Second Tag Key = Environment`
- `Third Tag Key = Group`

AMS creates the following Patch Group tag and applies it to your instances: `Patch Group:MyApplication-Production-1`.

Patch Orchestrator prerequisites

Patch Orchestrator workflow targets Amazon EC2 instances that are patched by latest version of System Manager Automation Document: AWSManagedServices-PatchInstanceFromMaintenanceWindow.

As part of the document workflow, the run command document "AWS-RunPatchBaseline" is run against each of the Amazon EC2 instances out of patch group members. To learn more, see About the SSM document AWS-RunPatchBaseline.

Requirements:

- Amazon EC2 instance deployed from AMS-provided Amazon Machine Image (AMI), or on an AMI through the "Stack from migration partner migrated instance" CT (ct-257p9zjk14ija).
- Egress internet connection enabled. For firewall/proxy solutions the requirement is to allow Windows update endpoint and/or Linux repository mirror endpoints, AWS system manager proxy settings, and metadata proxy configuration. For more information, see Configure SSM Agent to use a proxy and Using an HTTP proxy
- IAM role matching minimum permissive access for the SSM service of `customer-mc-ec2-instance-profile` IAM role.

- We recommend 10 GB available root partition space. For Linux OS, at least 2 GB available in the `/var` partition.
- Working and valid Certificate Authority for update downloads.
- Windows Server Update Services (WSUS) - Registry including but not limited to: DisableWindowsUpdateAccess, NoWindowsUpdate; Automatic Updates must not impair operation of Windows Update process.

Validation:

- For Linux OS instances using yum package manager you can validate availability of updates by running `#yum check-update`
- For Linux OS RedHat 5.7 and newer, 6.1 and newer, and 7.0 and newer; Amazon EC2 instances migrated to your AMS account via the "Stack from migration partner migrated instance" CT (ct-257p9zjk14ija), you need to validate subscription manager status for update performance.
- On Windows OS, enable Windows Server Update Services (WSUS). No local policy should block WSUS ability to scan or install updates. Once logged as administrator you can validate it by performing a scan for available updates from Windows Update Service console. Windows Server OS releases including 2012R2, 2016 and 2019 have default Windows Update settings to download and install. You can configure desired settings prior to scan. On later releases of OS, this operation can trigger installation; configure desired behavior beforehand.
- Request validation from the AMS Operations team by submitting a service request: "AWSManagedServices-CheckPatchingPrerequisites Automation document to run against Amazon EC2 instance for assessment of patch readiness."

Patch windows

Instances in a specific patch group are patched during one or more patch windows. Patch windows run on a schedule defined as a cron or rate expression, and have a configurable duration intended to keep patching-related disruption within a chosen time interval. AMS recommends creating multiple patch windows that collectively cover all of your instances, to match your organization's specific patching routines, and to use the default maintenance window as a fallback. Patch windows are created with the RFC change type Deployment | Patching | SSM patch window | Create (ct-0el2j07llrxs7). All instances that are not part of a patch window are patched during the default maintenance window created during onboarding.

Normally, a patch window does not need to be updated to include new instances. Typically, this is done by modifying instance tags. For example, consider the following sequence of events:

1. Two instances are tagged with AppId:MyApplication, Environment:Production, Group:1.

   This produces a tag for Patch Group:MyApplication-Production-1 on these instances (assuming First Tag Key = AppId, Second Tag Key = Environment, Third Tag Key = Group).
2. Patch window for MyApplication-Production-1 patch group is created.
3. Three more instances are created and tagged with AppId:MyApplication, Environment:Production, Group:1.

   Again, this produces a tag for Patch Group:MyApplication-Production-1.

No change to the patch window is needed because it picks up all five instances at the time of the next scheduled run.

For a more detailed discussion and a walkthrough on using this change type, see SSM Patch Window: creating.

Patch notifications

The subscribed email addresses (up to five) receive an email similar to the following just before the patch maintenance window start:

```
Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME was started at:
 2020-02-21T12:02:18.196Z.
Details:
    Maintenance Window AccountId:   YOUR_ACCOUNT_ID
    Maintenance Window Region:      YOUR_ACCOUNT_REGION
    Maintenance Window Id:          THE_MAINTENANCE_WINDOW_ID
    Maintenance Window Name:        THE_MAINTENANCE_WINDOW_NAME
    Maintenance Window Description: MaintenanceWindow for patching patch
 Group PATCH_GROUP_NAME
    Maintenance Window Patch Group: PATCH_GROUP_NAME
    Maintenance Window ExecutionId: THE_EXECUTION_ID
Targets:
    InstanceId           InstanceName        StackId
    -------------------  --------------      ----------------------
    THE_INSTANCE_ID      THE_INSTANCE_NAME   THE_STACK_NAME

A follow-up message with a detailed report is sent as soon as the maintenance window is
 over.

Please raise a service request if you have any inquires about AMS Patch Orchestrator by
 following this URL:
https://console.aws.amazon.com/managedservices/servicerequest/new

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team
```

At the end of the patch activity, the subscribed email addresses receive an email similar to the following:

```
Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME ended at:
 2020-02-21T12:03:20.058Z, with status: SUCCESS.
Details:
    Maintenance Window AccountId:   YOUR_ACCOUNT_ID
    Maintenance Window Region:      YOUR_ACCOUNT_REGION
    Maintenance Window Id:          THE_MAINTENANCE_WINDOW_ID
    Maintenance Window Name:        THE_MAINTENANCE_WINDOW_NAME
    Maintenance Window Description: MaintenanceWindow for patching patch
 Group PATCH_GROUP_NAME
    Maintenance Window Patch Group: PATCH_GROUP_NAME
    Maintenance Window ExecutionId: THE_EXECUTION_ID
Targets:
    RfcId                       InstanceId        InstanceName          StackId
   Status
    ----------------------  -------------------  --------------    ----------------------
  --------
    THE_RFC_ID        THE_INSTANCE_ID     THE_INSTANCE_NAME THE_STACK_NAME           STATUS

You can view the current Patch Compliance of your Amazon EC2 Instances by following this
 URL:
https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

Please raise an Incident if an issue is impacting one of your production applications by
 following this URL:
https://console.aws.amazon.com/managedservices/incident/new
```

```
Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team
```

Every 96 hours AMS verifies the upcoming patch runs, and sends a reminder notification to the subscribed email addresses. For example:

```
Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME will start at:
 2020-05-06T16:35:36.523Z.
Details:
    Maintenance Window AccountId:   YOUR_ACCOUNT_ID
    Maintenance Window Region:      YOUR_ACCOUNT_REGION
    Maintenance Window Id:          THE_MAINTENANCE_WINDOW_ID
    Maintenance Window Name:        THE_MAINTENANCE_WINDOW_NAME
    Maintenance Window Description: MaintenanceWindow for patching patch
 Group PATCH_GROUP_NAME
    Maintenance Window Patch Group: PATCH_GROUP_NAME
    Maintenance Window Next Start Time: 2020-05-06T16:35:36.523Z
    Maintenance Window Schedule:        rate(24 hours)
    Maintenance Window Timezone:        THE_TIMEZONE
At this time, these are the instances in the "PATCH_GROUP_NAME" Patch Group:
    InstanceId           InstanceName    StackId                  InstanceState

-------------------------------------------------------------------------------------------------

    THE_INSTANCE_ID      THE_INSTANCE_NAME   THE_STACK_NAME  running/stopped
    THE_INSTANCE_ID      THE_INSTANCE_NAME   THE_STACK_NAME  running/stopped
    THE_INSTANCE_ID      THE_INSTANCE_NAME   THE_STACK_NAME  running/stopped

A notification message is sent as soon as the maintenance window starts.

You can view the current Patch Compliance of your Amazon EC2 Instances by following this
 URL:
https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

If you would like to disable this maintenance window or you have inquires about the AMS
 Patch Orchestrator click on the following URL:
https://console.aws.amazon.com/managedservices/servicerequest/new

If you would like to delete this maintenance window, you can run the CT with id
 "ct-0q0bic0ywqk6c" against the stack id "stack-rctyznutkyj4tkkzq".

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team
```

Patch baselines

By default, all operating system (OS) vendor-provided patches are installed using the AMS-default patch baseline. If you want to restrict which patches are installed, you can optionally create a patch baseline using the RFC change type Deployment | Patching | SSM patch baseline | Create *OS* (CT ID varies per operating system).

For information about using this change type, see SSM Patch Baseline: creating.

Patch Orchestrator reserved tags

Patch Orchestrator also generates the following tags that can't be modified:

- **AMSPatchGroup** – This tag is used for Patch Group tag value generation. You shouldn't modify the AMSPatchGroup. You can modify the "Patch Group" tag if you want to use a custom "Patch Group" value. Patch Orchestrator continues generating a value for AMSPatchGroup based on the tag-keys provided during onboarding, but won't modify the "Patch Group" tag value if it has been set to a custom value by you. To stop using a custom "Patch Group" value, you can set the value of "Patch Group" to match the AMSPatchGroup tag value.
- **AMSDefaultPatchGroup** – This tag indicates whether an instance is part of the default maintenance window, with a value of either True or False. If an instance's Patch Group is not assigned to a maintenance window this value is set to True.

On-demand patching

AMS has a change type that works with your patch baseline, to enable you to run a patch on instances on demand. This can be either the default baseline you set at on boarding, or the Patch Orchestrator Systems Manager patch baseline that you set with the Patch Baseline change type (CT ID varies per operating system).

You can use the on-demand patching change type with or without Patch Orchestrator.

For information about using this change type, see On-demand Patching: Run.

> **Note**
> You can't use instances that are part of an Auto Scaling group in an on-demand patching change type.
> For information about having your Auto Scaling groups patched with the latest AMI, see AMI updates patching (using patched AMIs for Auto Scaling groups) (p. 375).

AMS standard patching

AMS supports existing customers using the AMS standard patching model, but this model is not available for new customers and is being retired in favor of AMS Patch Orchestrator.

Typical patch contents for AMS standard patching include vendor updates for supported operating systems and software preinstalled with supported operating systems (for example, IIS and Apache Server).

During AMS onboarding, you specify patching requirements, policy, frequency, and preferred patch windows. When AMS determines that there are new patches available, a notice is sent to you requesting the best dates and times for applying patches. This enables you to avoid taking applications offline for infrastructure patching all at once, so you can control which infrastructure gets patched when.

> **Note**
> The patching process described in this topic applies only to your stacks. AMS infrastructure is patched during a separate process. The AWS Managed Services Maintenance Window (or Maintenance Window) performs maintenance activities for AWS Managed Services (AMS) and recurs the second Thursday of every month from 3 PM to 4 PM Pacific Time. AMS may change the maintenance window with 48 hours notice. You configure the AMS patch window at onboarding, or you approve or reject the monthly patch service notification.

AMS regularly scans managed Amazon EC2 instances for updates available through the operating system update functionality. We also provide regular updates to the AMS base Amazon Machine Images (AMIs) supported in our environment.

After they are validated, AMS AMI releases are shared with all AMS accounts. You can view the available AWS AMI releases by using the DescribeImages Amazon EC2 API call or using the Amazon EC2 console. To find available AMS AMIs, see Finding an AMI ID (p. 259).

AMS performs patching on an ad hoc schedule that is communicated to you and requires your approval to proceed. You're notified of upcoming patches and proposed patch windows, and must respond to the notification. If you don't respond, patching doesn't occur.

Note
By default, AMS uses Systems Manager to apply patches by having the package manager (Linux) or System Update service (Windows) query its default repository to see which new packages are available. If, during the course of your day-to-day operations, you have installed a package on a Linux host using the default package manager, that package manager also picks up new packages for that software when they're available. In such a case, you may want to take a patching action (described in this section) to opt-out for that instance.

Supported operating systems

- Amazon Linux 2 and Amazon Linux
- CentOS 7.x, CentOS 6.5-6.10
- Oracle Linux 7.5 and later minor versions
- Red Hat Enterprise Linux (RHEL) 8.x, 7.x, 6.5-6.10
- SUSE Linux Enterprise Server 15 SPx and SAP specific versions, SUSE Linux Enterprise Server 12 SP4 and later minor versions and SAP specific versions.
- Microsoft Windows Server 2019, 2016, 2012 R2, 2012

Supported patches

AWS Managed Services supports patching primarily at the operating system level. The patches that are installed may differ by operating system.

Important
All updates are downloaded from the Systems Manager patch baseline service remote repositories configured on the instance, and described later in this topic. The instance must be able to connect to the repositories so the patching can be performed.
To opt-out of the patch baseline service for repositories that deliver packages that you want to maintain yourself, run the following command to disable the repository:

```
yum-config-manager --disable REPOSITORY_NAME
```

Retrieve the list of currently configured repositories with the following command:

```
yum repolist
```

- **Amazon Linux** preconfigured repositories (usually four):

Repository ID	Repository name
amzn-main/latest	amzn-main-Base
amzn-updates/latest	amzn-updates-Base
epel/x86_64	Extra Packages for Enterprise Linux 6 - x86_64

Repository ID	Repository name
pbis	PBIS Packages Updates

- **Red Hat Enterprise Linux** preconfigured repositories (five for Red Hat Enterprise Linux 7 and five for Red Hat Enterprise Linux 6):

Repository ID	Repository name
rhui-REGION-client-config-server-7/x86_64	Red Hat Update Infrastructure 2.0 Client Configuration Ser
rhui-REGION-rhel-server-releases/7Server/x86_64	Red Hat Enterprise Linux Server 7
rhui-REGION-rhel-server-releases/7Server/x86_64	Red Hat Enterprise Linux Server 7 RH Common(RPMs)
epel/x86_64	Extra Packages for Enterprise Linux 7 - x86_64
pbis	PBIS Packages Updates

Repository ID	Repository name
rhui-REGION-client-config-server-6	Red Hat Update Infrastructure 2.0
rhui-REGION-rhel-server-releases	Red Hat Enterprise Linux Server 6 (RPMs)
rhui-REGION-rhel-server-rh-common	Red Hat Enterprise Linux Server 6 RH Common (RPMs)
epel	Extra Packages for Enterprise Linux 6 - x86_64
pbis	PBIS Packages Updates

- **CentOS 7** preconfigured repositories (usually five):

Repository ID	Repository Name
base/7/x86_64	CentOS-7 - Base
updates/7/x86_64	CentOS-7 - Updates
extras/7/x86_64	CentOS-7 - Extras
epel/x86_64	Extra Packages for Enterprise Linux 7 - x86_64
pbis	PBIS Packages Updates

- For **Microsoft Windows Server**, all updates are detected and installed using the Windows Update Agent, which is configured to use the Windows Update catalog (this doesn't include updates from Microsoft Update).

  On Microsoft Windows operating systems, Patch Manager uses Microsoft's cab file wsusscn2.cab as the source of available operating system security updates. This file contains information about the security-related updates that Microsoft publishes. Patch Manager downloads this file regularly from Microsoft and uses it to update the set of patches available for Windows instances. The file contains only updates that Microsoft identifies as being related to security. As the information in

the file is processed, Patch Manager also removes updates that have been replaced by later updates. Therefore, only the most recent update is displayed and made available for installation. For example, if KB4012214 replaces KB3135456, only KB4012214 is made available as an update in Patch Manager.

To read more about the wsusscn2.cab file, see the Microsoft article Using WUA to Scan for Updates Offline.

Patching and infrastructure design

AMS employs different patching methods depending on your infrastructure design: mutable or immutable (for detailed definitions, see Key terms (p. 3)).

With mutable infrastructures, patching is done using a traditional in-place methodology of installing updates directly to the Amazon EC2 instances, individually, by AMS operations engineers. This patching method is used for stacks that are not Auto Scaling groups, and contain a single Amazon EC2 instance or a few instances. In this scenario, replacing the AMI that the instance or stack was based on would destroy all of the changes made to that system since it was first deployed, so that is not done. Updates are applied to the running system, and you may experience system downtime (depending on the stack configuration) due to application or system restarts. This can be mitigated with a Blue/Green update strategy. For more information, see AWS CodeDeploy Introduces Blue/Green Deployments.

With immutable infrastructures, the patching method is AMI replacement. Immutable instances are updated uniformly using an updated AMI that replaces the AMI specified in the Auto Scaling group configuration. AMS releases updated (that is, patched) AMIs every month, usually the week of Patch Tuesday. The following section describes how this works.

How AMS standard patching works

AMS uses the Systems Manager Run Command service for regularly scheduled monthly and as-needed critical patching, with two principal patching methods, in-place and AMI replacement, depending on your infrastructure deployment strategy (mutable vs. immutable). This section describes the AMS patching service, types, methods, and processes as directed to the two different infrastructure deployment strategies.

AMS defines two patch types, which are scheduled differently. Important or critical updates (that is, *critical patching*) and other updates (that is, *standard patching*) are the regular OS vendor updates and are applied monthly. Critical updates are applied as quickly as possible, after acceptance of the notice. Patches are applied through either in-place patching or AMI replacement (upon request).

Update scanning

AMS uses the Amazon EC2 Run Command Service to contact your Amazon EC2 stacks and deploy the required scanning and patching scripts. AMS uses the native package management component already installed on the supported operating system to perform all the required scanning and patching behavior on the Amazon EC2 stack. For Red Hat and Amazon Linux, the service uses yum. For Windows, the service uses the Windows Update Agent.

Scans are performed daily using SSM Maintenance Windows and the AMS default AWS-RunPatchBaseline document. Every reachable Amazon EC2 stack is scanned, using the update repositories for Linux and Windows. The AMS patching process detects all reachable Amazon EC2 stacks and then performs the scans in a batch process that ensures the stack always remains in a healthy state, even if a failure occurs while running the scan. The scan results are then saved for each Amazon EC2 stack.

To view the scan results for a stack or instance, submit a service request with the stack ID or instance ID.

The default AMS patching process is to install all available patches regardless of patch classification or severity (for example, critical versus standard). The exception to this are patches that have been explicitly excluded for the stack (patches defined as mandatory by AMS should not be excluded).

You're sent a patching service notification 14 days before the proposed maintenance window. This gives you time to test the proposed patches and accept or reject them. If you don't reply to the patching service notification, your instances aren't patched. When the time comes to install the patches, AMS creates a Request for Change (RFC) for each stack, and that RFC appears in your account's RFC list.

AMS configured maintenance window and notice

With AMS configured patching, each account has a monthly maintenance window, which you define when you onboard your account. The AWS Managed Services Maintenance Window (or Maintenance Window) performs maintenance activities for AWS Managed Services (AMS) and recurs the second Thursday of every month from 3 PM to 4 PM Pacific Time. AMS may change the maintenance window with 48 hours notice.

The patching window is different. The patching outbound service request (also known as a *service notification*) includes a suggested patch window.

> **Note**
> For information about replying to the patching service notification, see Actions you can take in AMS standard patching (p. 377).

The patching service notification is sent by email to the contact email address on file for your account. The notification includes a link to the AWS Support console where you can respond to it. You can also respond to the notification using the AMS Service Request page. The service notification includes:

- A list of update IDs (CSUs, IUs, and OUs) that apply to the stack, and those updates that you have requested be excluded from patching (if any).
- IDs of instances that will be affected.
- A proposed patching window when the updates will be applied. You can request a different patching window.
- A request that you accept the proposed patching, or ask for additional information. AMS gives you time to test the impact of the updates and approve or reject the patching, or ask that specific updates be excluded. If you need more time to test, and want the updates to be applied after your testing, respond to the service notification and describe what you want, or submit a service request for a new patch RFC based on the details of the previous RFC. If you don't reply to the service notification at all, no patching action is taken and the RFC is cancelled.

If you approve the service notification, AMS runs the patch RFC and applies the updates within the agreed-to patch window, as per the service commitment.

When patching is finished, AMS sends you a correspondence in the Service Request, with a summary of the outcome of the patching activity (that is, success or failed).

In-place patching

In-place patching refers to a method where AMS logs into each stack instance and applies patches.

In-place patching occurs on mutable infrastructures using Amazon EC2 instances running a supported operating system. Patching applies all non-excluded updates available up to that point. When critical patches are released, there is an additional critical patching process.

Standard patching: in-place

Standard patching occurs on the agreed-to patch schedule suggested in the patch service notification, and includes regular patch updates that are not deemed critical.

Prior to the proposed patching window, and with your affirmative response to the notification, a patch RFC is created and appears in your RFC dashboard.

Critical patching: in-place

When an OS vendor releases a critical security update, AMS notifies you of the patch RFC by sending you a service notification (to the contact email for your account) for each stack, according to the AMS service commitment. The service notification includes the following for each update:

- Update release date
- Update criticality
- Update details (KB reference, etc.)
- IDs of stacks affected

You can test the updates listed in the notification, and approve or reject the patches by replying to the service notification. If you approve the notification, you need to provide a specific patch window per stack for installing the updates.

> **Note**
> Patch windows that are within 24 hours of reply to the service notification may be rescheduled based on available capacity.

If you don't reply within 10 days or if you reject the proposed patching, the patching is canceled.

If you want to apply the updates after the allowed period (provided in the notification), submit a service request for a new patch schedule based on the details of the previous notification.

If you approve the service notification, AMS applies the updates within your specified patch window, according to the service commitment.

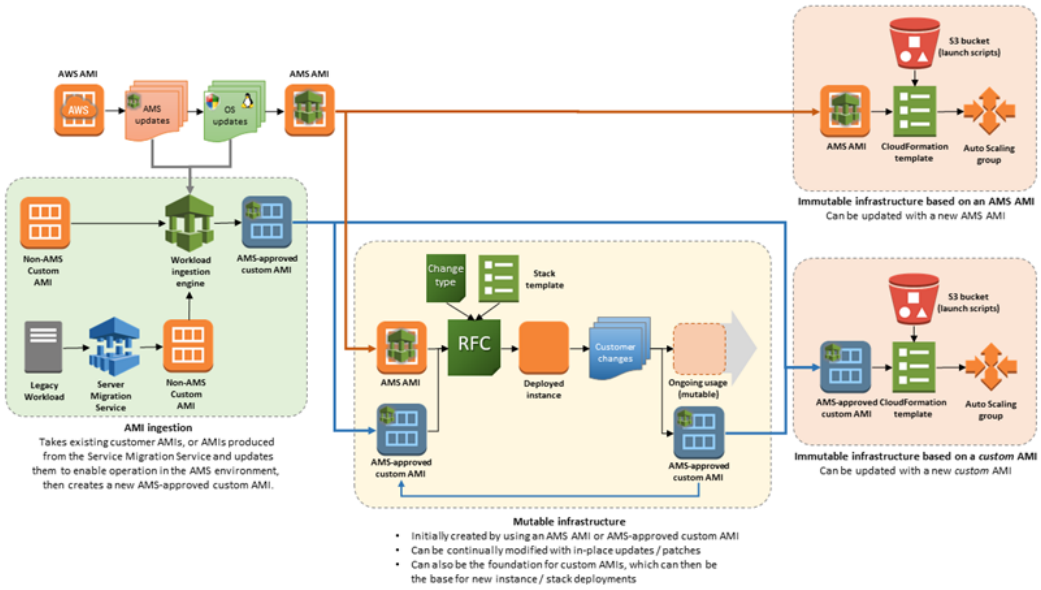
In the case of multiple updates, you can exclude specific updates from the patching by specifying the updates to be excluded in your response to the service notification.

AMS sends you a service notification for each stack, of the outcome of each update (that is, success or fail).

AMI updates patching (using patched AMIs for Auto Scaling groups)

AMI-replacement patching is done on immutable infrastructures by updating the AMI ID that is configured to deploy new Amazon EC2 instances in an Auto Scaling group.

Amazon Machine Images (AMIs) are released on a regular basis for the supported operating systems. Operating system vendors release new patches on a periodic basis. AMS takes the Amazon-provided AMI, updates it with the latest patches, and then adds the appropriate components to enable it to operate in the AMS environment. Then, it makes the new AMS AMI available to all AMS customers by sharing the AMI to the accounts. Your Auto Scaling group stacks can be refreshed on a monthly basis with these newly released AMS AMIs. The following graphic illustrates how AMIs are used in AMS your environments.



Auto Scaling groups create their instances based on the configured AMI for the Auto Scaling group. When AMS shares updated AMIs, you have the following options depending on how you are managing AMI updates:

- If you are using an application deployment tool (for example, UserData, CodeDeploy, and so forth) that customizes your instances automatically after they are created, you can do the following:
  - Reply to the patching service notification, or submit a service request, for the latest AMS AMI to replace your current Auto Scaling group's configuration AMI. After the AMI ID in your Auto Scaling groups' configuration is replaced, AMS kicks off rolling updates of your instances and your Auto Scaling group instance configurations (for example, installing applications, boot scripts, etc.) are applied to the new instances created with the new AMS AMI automatically.
- If you are using a custom/golden AMI in your Auto Scaling groups' configuration, you can:
  - Create an instance with the new AMS AMI, customize the instance and create a new golden AMI. Share the new golden AMI with AMS using the Amazon EC2 console, and submit a service request to AMS to update your Auto Scaling groups' configuration to use your new custom AMI.
  - Share your existing golden AMI with AMS by using the Amazon EC2 console, and submit a service request for AMS to update your golden AMI. To do this, AMS creates an instance from your golden AMI, applies the patches to that instance, creates a new golden AMI for you, and then updates your Auto Scaling groups' configuration to use the new AMI. The drawback here is that AMS cannot test that your new custom AMI works the way you want it to. Instead, you should test the instance created with the new AMI and verify that everything works correctly before creating a new golden AMI, sharing it, and requesting that AMS update your Auto Scaling groups. AMS does not recommend this option.

Standard patching: AMI updates

Every month AMS releases new Amazon Machine Images (AMIs) with service improvements and new patches that apply to the AMIs.

> **Note**
> New AMS AMIs are generated after Patch Tuesday from updated AWS AMIs. Then, AMS tests them before making them available. After the new AMIs pass testing, AMS shares updated AMIs to managed accounts.

Critical patching: AMI updates

When needed, AMS provides AMIs updated with critical security patches released since the last monthly AMI release.

The process for critical security updates to immutable infrastructures is identical to the monthly AMI process for immutable infrastructures, except that a new AMS AMI is created outside the normal schedule (Patch Tuesday), based on the release of new critical updates. AMS makes available a new AMI with the critical security patches according to the service level agreements (SLAs) defined for your account. AMS updates of Auto Scaling groups by request only. Use a service request to submit AMI replacement requests.

AMS standard patching failures

In case of failed updates, AMS performs an analysis to understand the cause of failure and communicates the outcome of the analysis to you. If the failure is attributable to AMS, we retry the updates if it's within the maintenance window. Otherwise, AMS creates service notifications for the failed instance update and waits for your instructions.

For failures attributable to your system, you can submit a service request with a new patch RFC to update the instances.

Actions you can take in AMS standard patching

In addition to testing new AMIs, there are several actions you can take to manage the patching of your infrastructure:

- If it took longer to test the updates than the patch window allowed, you can request that AMS apply the updates that were canceled when you're ready by submitting a service request (use the details in the original service notification as the basis).
- You can request that an important update (IU) or other update (OU) be applied before the next automated update window by submitting a service request providing a list of the updates, the applicable instances, and other details as appropriate. Since this CT is not automated, it takes longer to schedule and run. Check the service level objectives (SLOs) for the appropriate time. For more information, see AMS service level objectives (SLOs) (p. 15).

Additionally, you can use existing, patched, AMS AMIs to create custom AMIs. For information, see Create AMI.

> **Note**
> You can't request a new AMS AMI based on an important update or other update before the next maintenance window because the AMS AMI release process follows a uniform cadence for the benefit of all AMS customers.

Changing what gets patched/opting out

With AMS configured patching, in your response to the patching service notification or in a Service Request, you can change what resources get patched. You can do the following:

- Define a list of patches that should be excluded from remediation, per stack and per operating system.
- Define a list of resources that should be excluded from certain patches or all patching.
- Define a list of resources that should be always be excluded from all patching.
- Define a list of resources that should be patched on a certain day and certain time (good if you haven't defined a maintenance window).

To exclude one or more patches, submit a service request, or respond to the patching service notification using the template provided next. Do not submit an RFC. Include in the request the patch name or names that you want excluded and why. Include this information in a Service Request as follows:

- Name: The name of the patch. For Windows patches, this is the KB name, such as `KB3145384`. For Linux patches, this is the package name, such as `openssh-6.6.1p1-25.61.amzn1.x86_64`.
- Reason: A comment indicating why the patch is being excluded.
- Expiration Time: The date/time when the exclusion expires.

If an excluded patch is already installed, it is removed.

The request is reviewed by an operator who will discuss it with you if excluding those patches poses a significant security risk. The expiry date for excluded patches is also negotiated. After the agreed upon expiry date, the exclusion expires, and the patch is installed on any subsequent patching.

Patches on the exclusion list are still returned in scan results, if applicable.

> **Note**
> Unlike Windows, Linux patches are version-specific. This distinction is important because new versions of an excluded patch are not automatically excluded. It is your responsibility to notify AMS to exclude new versions of a Linux patch if that's what you want to do.

Patch service notification reply templates

You must reply to patching service notifications in order for patching to be performed on your instances. By using the specified format, you ensure that the correct patching occurs. You should do this if you haven't already set a maintenance window with AMS.

When you reply to a service notification, use the format given.

If no maintenance window is set, let us know when to patch what as shown following:

```
UTC                 StartTime       StackId                     InstanceId (Optional)
2019-04-01          15:00           stack-123456789012          i-1234566789
2019-04-01          15:00           stack-123456789013          i-1234566784
2019-04-01          15:00           stack-123456789014          i-1234566783
2019-04-01          15:00           stack-123456789015          i-1234566782
```

If you have a set maintenance window and want certain resources to be excluded from certain patches, use the following format:

```
StackId                     InstanceId (Optional)       Exclude Patches
stack-123456789012          i-1234566789                PATCH
stack-123456789013          i-1234566784                PATCH
stack-123456789014          i-1234566783                PATCH
stack-123456789015          i-1234566782                PATCH
```

If you have a set maintenance window and want certain resources to always be excluded from all patching, use the following format:

```
StackId                     InstanceId (Optional)       Exclude Patches
stack-123456789012          i-1234566789                ALL
stack-123456789015          i-1234566782                ALL
```

Preparing for patching

To prepare your environment for automated patching, we recommend the following:

- Be sure you have a complete inventory of all instances to be patched.
- Ensure that your resources are backed up regularly as part of your Continuity of Business strategy. Additional backups are created as part of the patch sequence, and these are automatically deleted according to your configured Patch Orchestrator retention policy (default is 60 days).
- Ensure that all relevant licenses are up to date.
- Modify your stack maintenance windows to stagger patching so that testing stacks are patched before production stacks. That way, any errors with patching are found in the testing stacks and can be identified before production stacks are patched.

Viewing patch settings

To find out what your current patching configuration is you can do the following:

- Submit a service request to AMS with the query.
- Wait for a patch service notification. The patching notice advises you of all patches to be applied and instances to be patched, and also suggests a patch window.

You can submit a service request to modify the following:

- Scan Interval: The amount of time, in minutes, between compliance scans performed on instances of this stack.

  Default is `240` (4 hours).
- NotificationWindow: How far in advance (in minutes) of a scheduled change (patch) the notification should be sent to you.
  Default is `10080` (7 days).

AMS standard patching FAQs

This section provides answers to some frequently asked questions.

- Q: How do I opt out of patching globally?

  A: To globally opt out of patching, file a service request. Note that you can't opt out of AMS mandatory patches. All stacks will continue to be scanned so that we can report on vulnerabilities.

- Q: How do I exclude specific stacks from patching?

  A: To permanently exclude specific stacks from patching, submit a service request. To exclude certain stacks from a particular patch cycle, respond to the upcoming patching notice with the list of stacks to exclude. For information, see Changing what gets patched/opting out (p. 377). Note that you can't opt out of mandatory patches.

- Q: What happens if I don't approve a patching service notification?

  A: You have 14 days to approve a standard patching service request and 10 days to approve a critical patching notice. If you don't approve the service request within the time period, the service commitment is nullified and no patching occurs. In the case of mandatory patching, patches are applied regardless of response to the service request.

- Q: How do I exclude specific patches and packages from being installed?

A: To permanently exclude specific patches or packages, submit a service request. To exclude certain patches or packages from a particular patch cycle, respond to the upcoming patching notice with the list of patches or packages to exclude. For details, see Changing what gets patched/opting out (p. 377). Note that you can't opt out of mandatory patches.

- Q: What happens if a system fails as a result of patching?

  A: AMS monitors each system. AMS sends a service notification to you of the outcome of each update (that is, success or fail) per stack and instance. If a failure is detected, AMS investigates, works to restore the instance, and then an AMS operations engineer attempts to manually patch. For information, see AMS standard patching failures (p. 377).

- Q: What updates are managed by AMS?

  A: AMS manages operating system level updates that AMS is notified of by the vendor. For more information, see Supported patches (p. 371).

- Q: What updates are not managed by AMS?

  A: Application-level updates are not managed by AMS.

- Q: How are Auto Scaling groups updated?

  A: Auto Scaling groups are updated with an AMI replacement in the Auto Scaling group configuration and preform a rolling update. A rolling update observes the HealthyHostThreshold setting of your patching configuration, which determines how many Amazon EC2 instances in a stack must be maintained active during patching. For more information, see AMI updates patching (using patched AMIs for Auto Scaling groups) (p. 375).

- Q: How do I get updates installed outside the normal cycle?

  A: For OS-level updates that you want installed outside of the normal patching schedule, submit a service request by using the patching notification that you received. This might happen if your testing of a proposed patch took longer than 21 days (for a standard patch) or 14 days (for a critical patch). Out-of-band patching can be done in-place for standalone Amazon EC2 instances.

- Q: How are newly deployed stacks or instances patched?

  A: When creating a new Amazon EC2 stack instance or Auto Scaling group, you should always specify the latest AMS AMI, which will have the latest patches on it already. For mutable infrastructures, inline patching should be performed as soon as the stack is deployed.

Patching service commitments

Based on your type of infrastructure deployment, and criticality of the update, we provide service commitments for critical security updates for mutable and immutable infrastructures, and important updates for mutable and immutable infrastructures.

Standard patching

These are AMS service commitments for standard patching.

Standard patching, mutable infrastructure (in-place patching)

Event/Action	Service commitment measurement
Important Updates are released in a month.	Clock starts
Fourteen days from when the standard patch notification is created, AMS notifies you of upcoming planned patching through a service notification and by email for each stack. The service notification includes: • A list of update IDs (CSUs and IUs) that are applicable (needed and not applied) for the stack, and those updates excluded from patching • IDs of stacks affected • The maintenance window when the updates will be applied	Clock stops after service notification is sent.
You test the impact of the updates and approve or reject the RFC. If you do not reply within 14 days or you reject the patching in your response to the service notification, no action is taken. If you take longer than 14 days to test, and want the updates to be applied after the 14-day period, submit a service request for a new patch RFC based on the details of the previous RFC.	If you don't approve or reply within 14 days, the pending change is canceled and the service commitment for the updates is not applicable.
If you approve the service notification within 14 days, AMS applies the updates. You can choose to exclude specific updates from an RFC by specifying the updates to be excluded in your response to the service notification.	The clock starts if you approve service notification within 14 days of the receipt. The clock stops after the update installation has been attempted.
AMS sends a service notification to you of the outcome of each update that was attempted. The service notification includes the following details: • Amazon EC2 instance ID • Update 1 Success/Failed: ARN a1, ARN a2... • Update 2 Success/Failed: ARN b1, ARN b2... • Update N Success/Failed: ARN c1, ARN c2...	Not applicable.
In case of failed updates, AMS performs an analysis to understand the cause of failure and communicates the outcome of the analysis to you. If the failure is attributable to AMS, AMS retries the updates if within the maintenance window, otherwise AMS creates service notifications for	Not applicable.

Event/Action	Service commitment measurement
the failed instance-update combination and waits for your instructions on a maintenance window.	
For failures attributable to you, submit a service request for a new patch RFC to update the instances.	Not applicable.

Standard patching, immutable infrastructure (AMI replacement patching)

Event/Action	Service commitment measurement	Action owner
Important updates are released in a month.	Clock starts	OS vendor
Seven days prior to the Amazon Machine Image (AMI) release window, AMS notifies you of the following through a service notification. • Updates (CSUs and IUs) released since last release window and are applicable to AMS AMIs • Update details: KB reference, and so on • AMS AMIs impacted • Anticipated release date and time for new updated AMIs	Clock continues to run.	AMS Ops engineer
AMS releases updated AMIs in managed account.	Clock stops.	
AMS notifies you of the AMIs shared in your account through a service notification and by email.	Not applicable.	
If testing the new AMIs takes longer than the allotted time (one week), you can submit a service request to AMS to update your Auto Scaling groups with the new AMS AMI (as is). If you want to modify the new AMS AMI with your configurations, use an RFC with the Management | Other | Other | Update CT (ct-0xdawir96cy7k) to request that we update your Auto Scaling groups.	Not applicable.	

Critical patching

These are AMS service commitments for critical security updates.

Critical security updates, mutable infrastructure

Event/Action	Service commitment measurement
CSU is released.	Clock starts
AMS notifies you of the patch RFC through a service notification (which also sends an email) for each stack. The service notification includes: • Updates release date • Update criticality • Update details: KB reference, and so on • IDs of stacks affected	The clock stops after the service notification is sent.
You test the updates listed in the RFC, and approve or reject the RFC within 10 days by replying to the service notification. You provide a specific maintenance window (per stack) for installing the updates. Maintenance windows specified that are within 24 hours of reply to the service notification may be rescheduled based on available capacity. If you don't reply within 10 days, or if you reject the patch RFC, the pending action is canceled. If you want to apply the updates after the 14-day period, submit a service request for a new patch RFC based on the details of the previous RFC.	If you don't approve or reply within 14 days, the pending change is canceled and the service commitment for the update is not applicable.
If you approve the service notification, AMS applies the updates. For multiple updates, you can choose to exclude specific updates from the change by specifying the updates to be excluded in your response to the service notification.	If the desired maintenance window is not within the service commitment time frame, the service commitment for the update is missed only if the RFC is not run within the desired maintenance window.
AMS sends a service notification to you of the outcome of each update that was applied. The service notification includes the following details: • Amazon EC2 instance ID • Update Success: ARN a1, ARN a2... • Update Failed: ARN c1, ARN c2...	Not applicable.
In case of failed updates, AMS performs an analysis to understand the cause of failure and communicates the outcome of the analysis to you. If the failure is attributable to AMS, AMS retries the updates if within the maintenance window, otherwise AMS creates service notifications for the failed instance-update combination and waits for your instructions on a new maintenance window.	Not applicable.

Event/Action	Service commitment measurement
For failures attributable to you, submit a service request for a new patch RFC to update the instances.	Not applicable.

Critical security updates, immutable infrastructure

Event/Action	Service commitment measurement
CSU is released.	Clock starts
AMS notifies you of the following via a service notification: • Update release date • Update criticality • Update details (KB reference,and so on) • AMS Amazon Machine Images (AMI) impacted • Anticipated release date and time for new updated AMIs	Clock continues to run.
AMS releases updated AMIs in managed account.	Clock stops.
If you approve the service notification, AMS applies the updates. AMS notifies you of the AMIs shared in your account, through a service notification and by email.	Not applicable.
If testing the new AMIs takes longer than the allotted time (one week), you can submit a service request to AMS to update your Auto Scaling groups with the new AMS AMI (as is). If you want to modify the new AMS AMI with your configurations, use an RFC with the Management | Other | Other | Update CT (ct-0xdawir96cy7k) to request that we update your Auto Scaling groups.	Not applicable.

Appendix: ActiveDirectory Federation Services (ADFS) claim rule and SAML settings

For detailed step-by-step instructions on how to install and configure AD FS see Enabling Federation to AWS Using Windows Active Directory, ADFS, and SAML 2.0.

ADFS claim rule configurations

If you already have an ADFS implementation, configure following:

- Relying party trust
- Claims rules

The relying party trust and claims rules steps are taken from Enabling Federation to AWS Using Windows Active Directory, AD FS, and SAML 2.0blog

- Claims rules:
  - **Nameid**: Configuration per blog post
  - **RoleSessionName**: Configure as follows
    - **Claim rule name**: **`RoleSessionName`**
    - **Attribute store**: **`Active Directory`**
    - **LDAP Attribute**: **`SAM-Account-Name`**
    - **Outgoing Claim Type**: **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**
    - **Get AD Groups**: Configuration per blog post
    - **Role claim**: Configure as follows

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-", "arn:aws:iam::$1:saml-provider/customer-
readonly-saml,arn:aws:iam::$1:role/"));
```

Web console

You can access the AWS Web console by using the link below replacing *`[ADFS-FQDN]`* with the FQDN of your ADFS implementation.

https://*`[ADFS-FQDN]`*/adfs/ls/IdpInitiatedSignOn.aspx

Your IT department can deploy the above link to the user population via a Group Policy.

API and CLI access with SAML

How to configure API and CLI access with SAML.

The python packages are sourced from the blog posts below:

- NTLM: How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS
- Forms: How to Implement a General Solution for Federated API/CLI Access Using SAML 2.0
- PowerShell: How to Set Up Federated API Access to AWS by Using Windows PowerShell

Script configuration

1. Using Notepad++, change the default region to the correct region
2. Using Notepad++, disable SSL verification for test and dev environments
3. Using Notepad++, configure idpentryurl

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?
loginToRp=urn:amazon:webservices
```

Windows configuration

The instructions below are for the python packages. The credentials generated will be valid for 1 hour.

1. Download and install python (2.7.11)
2. Download and install AWS CLI tools
3. Install the AMS CLI:

   a. Download the AMS distributables zip file provided by your cloud service delivery manager (CSDM) and unzip.

      Several directories and files are made available.

   b. Open either the **Managed Cloud Distributables -> CLI -> Windows** or the **Managed Cloud Distributables -> CLI -> Linux / MacOS** directory, depending on your operating system, and:

      For **Windows**, execute the appropriate installer (this method only works on Windows 32 or 64 bits systems):

      - 32 Bits: ManagedCloudAPI_x86.msi
      - 64 Bits: ManagedCloudAPI_x64.msi

      For **Mac/Linux**, execute the file named: **MC_CLI.sh**. You can do this by running this command: `sh MC_CLI.sh`. Note that the **amscm** and **amsskms** directories and their contents must be in the same directory as the **MC_CLI.sh** file.

   c. If your corporate credentials are used via federation with AWS (the AMS default configuration) you must install a credential management tool that can access your federation service. For example, you can use this AWS Security Blog How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS for help configuring your credential management tooling.

   d. After the installation, run `aws amscm help` and `aws amsskms help` to see commands and options.

4. Download the required SAML script

   Download to c:\aws\scripts
5. Download PIP

   Download to c:\aws\downloads
6. Using PowerShell, install PIP

   <pythondir>.\python.exe c:\aws\downloads\get-pip.py
7. Using PowerShell, install boto module

   <pythondir\scripts>pip install boto
8. Using PowerShell, install requests module

   <pythondir\scripts>pip install requests
9. Using PowerShell, install requests security module

   <pythondir\scripts>pip install requests[security]
10. Using PowerShell, install beautifulsoup module

    <pythondir\scripts>pip install beautifulsoup4
11. Using PowerShell, create a folder called .aws in the users profile (%userprofile%\.aws)

    mkdir .aws
12. Using PowerShell, create a credential file in the .aws folder

    New-Item credentials -type file –force

    The credentials file mustn't have a file extension

    The filename must be all lowercase and have the name credentials
13. Open the credentials file with notepad and paste in the following data, specifying the correct region

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

14. Using PowerShell, the SAML script and logon

    <pythondir>.\python.exe c:\aws\scripts\samlapi.py

    Username: [USERNAME]@upn

    Choose the role you would like to assume

Linux configuration

The credentials generated will be valid for 1 hour.

1. Using WinSCP, transfer the SAML script
2. Using WinSCP, transfer the Root CA certificate (ignore for test and dev)
3. Add the ROOT CA to the trusted root certificates (ignore for test and dev)

$ openssl x509 -inform der -in [certname].cer -out certificate.pem (ignore for test and dev)

Add contents of certificate.pem to end of /etc/ssl/certs/ca-bundle.crt file ((ignore for test dev)

4. Create .aws folder in home/ec2-user 5

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

5. Using WinSCP, transfer the credentials file to .aws folder
6. Install boto module

   $ sudo pip install boto
7. Install requests module

   $ sudo pip install requests
8. Install beautifulsoup module

   $ sudo pip install beautifulsoup4
9. Copy the script to home/ec2-user

   Set the required permissions

   Execute the script: samlapi.py

Document history

The following table describes the important changes to the documentation since the last release of AMS.

- **API version: 2019-05-21**
- **Latest documentation update:** November 11, 2021

Change	Description	Date
New or Updated CTs and Walkthroughs: AMS Change Management User Guide Document History.		
Find AMI Command Syntax	When using the find AMI commands, you must use a single quote and not a tick mark. See Finding an AMI ID (p. 259) and AMS Amazon Machine Images (AMIs) (p. 29).	November 11, 2021
Direct Change Mode (DCM)	DCM now supports customized trusted entities in addition to SAML, values allowed are SAMLIdentityProviderARNs, IAMEntityARNs, or AWSServicePrincipals. See note at Getting Started with Direct Change mode (p. 167). Also, the suggested request template was updated. See Getting Started with Direct Change mode (p. 167)	November 11, 2021
Using Root Account	The note was updated with a better warning. See How and when to use the root user account (p. 243)	November 11, 2021
AMS Modes	AMS has a new mode, Direct Change mode. See AMS modes and applications or workloads (p. 288) and Direct Change Mode (p. 167).	October 28, 2021
Developer Mode	Content updated with current information. See Security and compliance in Developer mode (p. 161).	October 28, 2021
New AMS Report	The Weekly Incident report provides an aggregated list of incidents along with its priority, severity and latest status. See Weekly Incident report (p. 157).	October 14, 2021
New Supported Services	AWS Compute Optimizer, Amazon Personalize, and AWS Systems Manager (SSM), were added to the list of Supported Services in the AMS Service Description. See Supported AWS services (p. 25)	October 14, 2021
Extra IAM deployment options	Additional information has been added. See "Deploying IAM Resources" at Setting permissions with IAM roles and profiles (p. 119)	October 14, 2021

Change	Description	Date
New MALZ feature. AWS Application Migration Service (AWS MGN) for Tools accounts.	AWS Application Migration Service (AWS MGN) can be used in MALZ Tools account via the CustomerMigrationAccessRole IAM role. You use AWS MGN to migrate applications and databases that run on supported versions of Windows and Linux operating systems. See AWS Application Migration Service (AWS MGN) (p. 76).	September 30, 2021
New video links.	YouTube video links were added to several sections. See Incident management (p. 267) Service request management examples (p. 276) Service description (p. 7)	September 30, 2021
AMI notifications with SNS.	An example notice was added. See AMS AMI notifications with SNS (p. 111)	September 30, 2021
Self service provisioning service FAQs.	The FAQs were updated to AWS standards.	September 30, 2021
Application account access.	The information was updated and clearer instructions were added. See Accessing your Customer Managed account (p. 73) and Connecting your CMA with Transit Gateway (p. 73)	September 30, 2021
New feature. Operations on Demand	Operations on Demand provides you with a curated catalog of operations activities. See AWS Managed Services Operations On Demand (p. 134).	September 16, 2021
New section. Disaster recovery execution	A new section was added detailing the steps you take to initiate a disaster recovery. See Disaster recovery response (p. 354).	September 16, 2021
Self-Service Provisioning, Service Updates	ACM FAQs updated to use an RFC and not a service request. See ACM in AMS FAQs (p. 214). Amazon SES FAQs updated to list SMTP credentials as a required ask. See Amazon SES in AMS FAQs (p. 204). Systems Manager FAQs updated for the Systems Manager "customer_systemsmanager_automation_policy," can it be attached to other IAM roles? See AWS Systems Manager Automation in AMS FAQs (p. 234). Amazon FSx FAQs updated to note that the default settings are not suitable for business use. See Amazon FSx in AMS FAQs (p. 193).	September 16, 2021

Change	Description	Date
Root account	New section on using the root credentials. See How and when to use the root user account (p. 243).	August 26, 2021
Planned Event Management (PEM)	Updated information on the PEM initiation process. See AMS planned event management (p. 45).	August 26, 2021
AMS reserved prefixes	Some attributes must comply with certain patterns; for example, IAM instance profile names, BackupVault names, tag names, and so forth, must not start with AMS reserved prefixes. See AMS reserved prefixes (p. 39).	August 12, 2021
Service description	Windows 2008 R2 is removed from the list of supported OSes. See Supported configurations (p. 15).	August 12, 2021
Self-provisioned service mode	The description for AWS CodePipeline SSPS was updated to mention that CodePipeline in AMS does not support "Amazon CloudWatch Events" for Source Stage. See AWS CodePipeline (p. 219).	August 12, 2021
Patching	Added note about the upcoming deprecation of monthly patch compliance reports in light of the new self-service patch reports. See AMS Patch Orchestrator: a tag-based patching model (p. 363).	August 12, 2021
Alert automatic remediation	New feature in alert remediation that auto-remediates RDS Low Storage events. See AMS automatic remediation of alerts (p. 300).	August 12, 2021
July 2021		
SLOs	Updated business hours to align with SLOs. "Plus (Business Days, M-F 8AM to 6PM local time)", "Premium (Calendar Days, 24 x 7)." See Service description (p. 7).	July 29, 2021
Information resources	Updated with new information resources including private AMS security information on AWS Artifact and AWS Managed Services YouTube Instructional Videos. See also AMS information resources (p. 31).	July 15, 2021
Incident management	Added note about how AMS consolidates the five priorites. See What is incident management? (p. 267).	July 15, 2021

Change	Description	Date
Support experience	Added missing SAPI service codes. See Incident reports and service requests in AMS (p. 267).	July 15, 2021
AMI contents	Updated AMI content notes. See AMS Amazon Machine Images (AMIs) (p. 29).	July 15, 2021
Service description	Added AWS CloudEndure* and Amazon Translate* to the list of Group B supported services. See Service description (p. 7).	July 15, 2021
June 2021		
New feature: Self-service reporting	AMS now offers self-service reporting through a new **Reporting** page in the AMS Console. See Self-service reporting (p. 147).	June 17, 2021
New feature: AMS Public GitHub	See GitHub repo.	June 17, 2021
Updated the alerts from baseline monitoring table. See Alerts from baseline monitoring in AMS (p. 88).	June 17, 2021	
Clarified and added more detail to instructions on how to connect to linux bastions from Windows. See Windows computer to Linux instance (p. 255).	June 17, 2021	
Updated the Windows AMI contents list, including adding 'Amazon Unified CloudWatch Agent'. See AMS Amazon Machine Images (AMIs) (p. 29).	June 17, 2021	
Clarified differences between MALZ and SALZ with respect to DNS bastions. See DNS friendly bastion names (p. 247).	June 17, 2021	
Updated the RACI table. See AMS responsibility matrix (RACI).	June 17, 2021	
Updated role names and allowances in step 2 of the implementation instructions for Amazon Cognito user pools. See Amazon Cognito (User Pools) (p. 180).	June 17, 2021	

Change	Description	Date
Moved the 'AMS Advanced service control policy restrictions' and 'AMS Advanced detective controls Config rules' tables to the new private security guide, which is available on AWS Artifact.	To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.	May 31, 2021
Moved the 'Security best practices', 'AMS Advanced Guardrails', 'MALZ Service control policies', 'Security control for end-of-support operating systems', 'AMS Advanced detective controls', 'Detective controls in developer mode', and 'Security enhanced AMIs' sections to the new private security guide, which is available on AWS Artifact.	To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.	May 31, 2021
Redacted the 'Compliance validation', 'Security event logging and monitoring', 'Security alerts defaults', 'How do I offboard a Multi-Account Landing Zone environment', and 'How do I offboard a Multi-Account Landing Zone application account?' sections and put the redacted content in the new private security guide, which is available on AWS Artifact.	To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.	May 31, 2021
Moved the Single-Account Landing Zone network architecture from a section within the introduction to a chapter.	See Single-Account Landing Zone network architecture.	May 13, 2021
Moved the Change management chapter to a new guide dedicated to change management, change types, and examples.	See AWS Managed Services Change Management User Guide.	May 13, 2021

Change	Description	Date
Added new section to Self-service provisioning: AWS CloudEndure. AWS CloudEndure migration simplifies, expedites, and automates large-scale migrations from physical, virtual, and cloud-based infrastructure to AWS. CloudEndure Disaster Recovery (DR) protects against downtime and data loss from any threat, including ransomware and server corruption.	See AWS CloudEndure (p. 216).	May 13, 2021
This user guide is no longer dedicated to multi-account landing zone content; instead, single-account landing zone content has been merged into the guide. The two user guides, multi-account landing zone and single-account landing zone shared most content and they have been merged into one guide. All differences between the two landing zone accounts is called out. Additionally, the Change Management chapter is removed, that content has been moved into a separate user guide. Finally, there is a greatly updated security chapter and some sections have been moved from other chapters into it. This was done to conform to AWS Documentation standards.	See What is change management?	May 13, 2021
Added new section to Self-service provisioning: AWS Systems Manager Automation Runbook. AMS Self-service provisioning has enabling AWS Systems Manager Automation Runbook as service (SSPS) so you can now author automation runbooks yourself and execute them against your fleet of managed instances.	See AWS Systems Manager Automation (p. 234).	May 13, 2021

Change	Description	Date
Updated the AMS CodeSuite entry in the Self-service provisioning section: added an invoke stage to CodePipeline limitations for AMS CodeSuite.	See AMS CodeSuite (p. 208).	May 13, 2021
Updated AMS Advanced contact (business) hours on the AMS Advanced account governance page.	See Account governance (p. 41).	May 13, 2021
Updated the screenshots on the RFC correspondence and attachment page.	See RFC correspondence.	May 13, 2021
AMS VPC endpoints section for Multi-Account Landing Zone has moved to the introduction chapter and out of the Multi-Account Landing Zone architecture chapter.	See AMS VPC endpoints (p. 34).	May 13, 2021
Added Amazon Alexa for Business and Amazon Rekognition to list of supported AWS services.	See Supported AWS services (p. 25).	May 13, 2021
Updated the AMS contact hours.	See Account governance (p. 41).	April 15, 2021
Updated AMS management account page with an updated graphic.	See Management account (p. 56).	April 15, 2021
Added a section linking to the Single-Account Landing Zone Onboarding Guide.	See Getting started (p. 2).	April 15, 2021
Added a section linking to the Multi-Account Landing Zone Onboarding Guide.	See Getting started (p. 2).	April 15, 2021
Updated AWS Backup change type descriptions.	See AWS Backup.	April 15, 2021
AMS added descriptions for the following services: AWS Batch, Managed Streaming for Apache Kafka (MSK), AWS Audit Manager, AWS Global Accelerator, Amazon Transcribe, Amazon Textract, AWS Amplify, and AWS Certificate Manager - Private Certificate Authority.	See Self-service provisioning (p. 175).	April 15, 2021

Change	Description	Date
New CTs and walkthroughs:	Directory service: accept sharing. Allows user to accept a directory sharing request sent from the directory owner account. Redshift cluster: resuming. Describes how to resume an Amazon Redshift cluster. Redshift cluster: pausing. Describes how to pause an Amazon Redshift cluster. RDS DB stack: restoring DB instances. Describes how to restore an AWS Relational Database Service (RDS) database (DB) instance to a previous point in time using the AMS Advanced console or the AMS Advanced API/CLI. EBS Volume: modifying. Modify an EBS Volume that is not attached to an EC2 instance in an Auto Scaling group.	April 15, 2021
Updated CTs and walkthroughs:	EBS volume: creating. Describes how to request the provisioning of up to five Elastic Block Store (EBS) volumes and attach them to an existing EC2 instance. EBS volume: updating. Describes how to request the update of up to five Elastic Block Store (EBS) volumes and attachments to an existing EC2 instance. SSM Patch Baseline: Creating. Describes how to create an SSM resource, Patch Baseline by operating system (OS), using the AMS Advanced console or the AMS Advanced API/CLI. Backup plan: configuring a cross region. Configure a cross region in an AWS Backup backup plan, using the AMS Advanced console or the AMS Advanced API/CLI.	April 15, 2021
Updated information on configuring and deploying AMS Resource Scheduler.	See AMS Resource Scheduler.	March 18, 2021
Updated information on configuring and deploying AMS Resource Scheduler.	See AMS Resource Scheduler	March 18, 2021
Updated information on reporting in AMS.	See Reporting in AMS (p. 139).	March 18, 2021
Updated Certificate Manager content under Self-service provisioning services.	See AWS Certificate Manager (p. 213).	March 18, 2021

Change	Description	Date
Updates to graphics and terminology in Management account and Architecture pages.	See Management account (p. 56) and Multi-Account Landing Zone network architecture (p. 50).	March 18, 2021
Updated AMS key terms page.	See Key terms (p. 3).	March 18, 2021
Updated SSPS Documentation for EC2 Image Builder.	See Amazon EC2 Image Builder (p. 185).	March 18, 2021
Updated SSPS Documentation for Migration Hub.	See AWS Migration Hub (p. 228).	March 18, 2021
Updated SSPS Documentation for CloudWatch Synthetics.	See Amazon CloudWatch Synthetics (p. 179).	March 18, 2021
Updated SSPS Documentation for AWS Secrets Manager.	See AWS Secrets Manager (p. 229).	March 18, 2021
New CTs and Walkthroughs:	EBS Volume: modifying.	March 18, 2021
Updated CTs and walkthroughs:	Tags: bulk updating (auto). Increased CsvS3Url input parameter length to avoid RFC failure because generated pre-signed URL is over the allowed value. On-demand patching: run. Added optional parameters. AMS Resource Scheduler. Resource Scheduler CTs are now compatible with multi-account landing zone.	March 18, 2021
Updated CTs and walkthroughs:	Tags: bulk updating (auto). Increased CsvS3Url input parameter length to avoid RFC failure because generated pre-signed URL is over the allowed value. On-demand patching: run. Added optional parameters. AMS Resource Scheduler. Resource Scheduler CTs are now compatible with multi-account landing zone. Management account application account (with VPC): creating. The minimum value for the PatchOrchestratorDefaultPatchBackupRetentionInDays parameter changed from 60 to 1.	March 18, 2021

Change	Description	Date
New RFC Digest feature in Change Management. AMS added a new feature page, RFC digest, to the 'Change Management, RFCs, change types, and examples' section of the user guides.	See RFC digest.	February 11, 2021
Updates to EC2 IAM Instance Profile. AMS has updated the policy statement description for "Instance To Upload Log Events".	See EC2 IAM instance profile (p. 85).	February 11, 2021
Updated On-demand patching. SSM automation concurrent runs per account increased from 25 to 100 and the pending queue limit increased from 75 to 1,000.	See On-demand patching: run.	February 11, 2021
Updated Self-service provisioning services. AMS added two new services to the SSPS page in the user guides: Alexa for Business and Amazon Rekognition.	See Self-service provisioning (p. 175), AWS Alexa for Business (p. 176), and Amazon Rekognition (p. 201).	February 11, 2021
Updated MALZ offboarding page. AMS removed "The service level agreement (SLA) for all offboarding is 7 business days."	See How do I offboard from AMS Multi-Account Landing Zone accounts? (p. 47)	February 11, 2021
Updates to managed Palo Alto egress firewall.	See Managed Palo Alto egress firewall (p. 60).	February 11, 2021
Updated SSPS Documentation for AWS DataSync: AMS replaced the erroneous reference to MediaLive with DataSync.	See AWS DataSync (p. 221).	February 11, 2021
Updates to table in Alerts from Baseline Monitoring. AMS removed a duplicate row under the resource column (for ALB instance).	See Alerts from baseline monitoring in AMS (p. 88).	February 11, 2021
Updated 'Continuity management' chapter in MALZ user guide. AMS added a new 'default backup' subsection that describes what the default parameters are and informs the client that these defaults can be modified.	See Continuity management (p. 352).	February 11, 2021

Change	Description	Date
New CTs and Walkthroughs:	Amazon EC2 stack: replace instance profile. KMS alias: creating. KMS alias: deleting. EC2 stack: updating termination protection. EC2 stack: resize instance.	February 11, 2021
New CTs and Walkthroughs:	Amazon EC2 stack: replace instance profile. KMS alias: creating. KMS alias: deleting. EC2 stack: updating termination protection. EC2 stack: resize instance.	February 11, 2021
Updated CTs and walkthroughs:	Stack: deleting. Management account application account (with VPC): creating. Target group (for ALB): updating.	February 11, 2021
Updated CTs and walkthroughs:	Stack: deleting. Target group (for ALB): updating.	February 11, 2021
Updated section: Terms and Conditions requirements for VM-Series Next-Generation Firewall "Bundle-1" from Palo Alto.	See Managed Palo Alto egress firewall (p. 60).	January 14, 2021
Updated section: Replaced CDSM with CA in "CAs can be contacted directly and provide technical expertise to help you optimize your use of the AWS Cloud. Example CSDM activities include, workload selection for migration, a...".	See AMS features (p. 7).	January 14, 2021
Updated: AMS changed the way developer mode is enabled.	See Implementing AMS Advanced Developer mode (p. 159).	January 14, 2021
Updated section: AMS added a note ("Events are emitted on a best effort basis") to CloudWatch Event documentation.	See CloudWatch Events notifications (p. 115).	January 14, 2021
Updated RFC Scheduling: AMS updated the auto-rejection time for manual RFCs from 5 days to 30 days.	See RFC scheduling.	January 14, 2021

Change	Description	Date
Updated the list of restrictions in CodePipeline FAQs.	See CodePipeline in AMS FAQs (p. 220).	January 14, 2021
New CTs and Walkthroughs:	EBS volume: encrypt EBS by default. SSM Patch window: set status. AMIs: copying. Application account VPC: deleting. EC2 stack: change hostname (Linux). EC2 stack: change hostname (Windows).	January 14, 2021
New CTs and Walkthroughs:	EBS volume: encrypt EBS by default. SSM Patch window: set status. AMIs: copying. EC2 stack: change hostname (Linux). EC2 stack: change hostname (Windows).	January 14, 2021
Updated CTs and walkthroughs:	RDS DB stack: creating from Snapshot.	January 14, 2021

AWS glossary

For the latest AWS terminology, see the AWS glossary in the *AWS General Reference*.