AMS Advanced Account Onboarding Information

# AMS Advanced Onboarding Guide

**Version May 08, 2024**

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AMS Advanced Onboarding Guide: AMS Advanced Account Onboarding Information

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

# Table of Contents

**AWS Managed Services Onboarding Introduction ..... 1**
Learning about AMS ..... 1
Key terms ..... 2
AMS modes ..... 8
AMS modes and applications or workloads ..... 9
AMS post-account prescriptive guidance ..... 17
What we do, what we do not do ..... 17
AMS egress traffic management ..... 18
IAM user role ..... 19
MALZ: Default IAM User Roles ..... 20
SALZ: Default IAM User Role ..... 33
Default Access Firewall Rules ..... 40
Linux Stack Instance Ports ..... 41
Windows Stack Instance Ports ..... 41
**Service management ..... 43**
Account governance ..... 43
Service commencement ..... 44
Customer relationship management (CRM) ..... 44
CRM Process ..... 45
CRM meetings ..... 46
CRM Meeting Arrangements ..... 47
CRM monthly reports ..... 48
Cost optimization ..... 49
Cost optimization framework ..... 49
Cost optimization responsibility matrix ..... 51
Service hours ..... 53
Getting help ..... 54
**Change management modes ..... 55**
Modes overview ..... 56
Types of modes and accounts in AMS ..... 56
AMS modes and applications or workloads ..... 61
Real world use cases for AMS modes ..... 69
RFC mode ..... 73
Learn about RFCs ..... 73

What are change types? ... 119
Troubleshooting RFC errors ... 131
Direct Change mode ... 142
Getting Started with Direct Change mode ... 143
Security and compliance ... 145
Change management in Direct Change mode ... 150
Creating stacks using Direct Change mode ... 153
Direct Change Mode use cases ... 156
Developer mode ... 157
Getting started with Developer mode ... 158
Security and compliance ... 160
Change management ... 162
Provisioning infrastructure ... 167
Detective controls ... 168
Logging, monitoring, and event management ... 168
Incident management ... 168
Patch management ... 168
Continuity management ... 169
Security and access management ... 169
Self-Service Provisioning mode in AMS ... 169
Getting started with SSP mode in AMS ... 170
Amazon API Gateway ... 171
Alexa for Business ... 172
Amazon AppStream 2.0 ... 173
Amazon Athena ... 176
Amazon Bedrock ... 176
Amazon CloudSearch ... 178
Amazon CloudWatch Synthetics ... 179
Amazon Cognito ... 180
Amazon Comprehend ... 181
Amazon Connect ... 182
Amazon Data Firehose ... 184
Amazon DevOps Guru ... 185
Amazon DocumentDB (with MongoDB compatibility) ... 186
Amazon DynamoDB ... 187
Amazon Elastic Container Registry ... 189

EC2 Image Builder ..... 190
Amazon ECS on AWS Fargate ..... 192
Amazon EKS on AWS Fargate ..... 194
Amazon EMR ..... 197
Amazon EventBridge ..... 200
Amazon Forecast ..... 202
Amazon FSx ..... 204
Amazon FSx for OpenZFS ..... 206
Amazon FSx for NetApp ONTAP ..... 207
Amazon Inspector Classic ..... 209
Amazon Kendra ..... 210
Amazon Kinesis Data Streams ..... 211
Amazon Kinesis Video Streams ..... 212
Amazon Lex ..... 213
Amazon MQ ..... 213
Amazon Managed Service for Apache Flink ..... 214
Amazon Managed Streaming for Apache Kafka ..... 216
Amazon Managed Service for Prometheus ..... 217
Amazon Personalize ..... 218
Amazon QuickSight ..... 220
Amazon Rekognition ..... 222
Amazon SageMaker AI ..... 223
Amazon Simple Email Service ..... 226
Amazon Simple Workflow Service ..... 227
Amazon Textract ..... 228
Amazon Transcribe ..... 229
Amazon WorkSpaces ..... 230
AMS Code services ..... 232
AWS Amplify ..... 235
AWS AppSync ..... 236
AWS App Mesh ..... 237
AWS Audit Manager ..... 237
AWS Batch ..... 239
AWS Certificate Manager ..... 240
AWS Private Certificate Authority ..... 241
AWS CloudEndure ..... 244

AWS CloudHSM ..... 245
AWS CodeBuild ..... 247
AWS CodeCommit ..... 248
AWS CodeDeploy ..... 249
AWS CodePipeline ..... 250
AWS Compute Optimizer ..... 252
AWS DataSync ..... 253
AWS Device Farm ..... 255
AWS Elastic Disaster Recovery ..... 256
AWS Elemental MediaConvert ..... 257
AWS Elemental MediaLive ..... 258
AWS Elemental MediaPackage ..... 259
AWS Elemental MediaStore ..... 260
AWS Elemental MediaTailor ..... 261
AWS Global Accelerator ..... 262
AWS Glue ..... 262
AWS Lake Formation ..... 264
AWS Lambda ..... 265
AWS License Manager ..... 266
AWS Migration Hub ..... 267
AWS Outposts ..... 268
AWS Resilience Hub ..... 269
AWS Secrets Manager ..... 270
AWS Security Hub ..... 273
AWS Service Catalog AppRegistry ..... 274
AWS Shield ..... 274
AWS Snowball Edge ..... 276
AWS Step Functions ..... 277
AWS Systems Manager Parameter Store ..... 278
AWS Systems Manager Automation ..... 279
AWS Transfer Family ..... 282
AWS Transit Gateway ..... 284
AWS WAF ..... 285
AWS Well-Architected Tool ..... 286
AWS X-Ray ..... 287
VM Import/Export ..... 288

Customer Managed mode ... 289
Getting started with Customer Managed mode ... 290
AMS and AWS Service Catalog ... 290
Getting started with Service Catalog ... 290
Service Catalog in AMS before you begin ... 291
**AMS Multi-account landing zone (MALZ) onboarding ... 295**
MALZ network architecture ... 295
About multi-account landing zone network architecture ... 295
Choosing single MALZ or multiple MALZs ... 298
Multi-Account Landing Zone accounts ... 303
MALZ: Core account onboarding ... 348
Create an AWS multi-account landing zone core account ... 349
Create an IAM role for AMS to access your account ... 350
Secure the new account with multi-factor authentication (MFA) for the root user ... 353
Subscribe to AWS Marketplace for EPS ... 353
Set up networking ... 355
Set up access management ... 359
MALZ: Application account onboarding ... 364
Requesting a new application account ... 364
Setting up Active Directory to federate access to AMS IAM roles ... 366
Setting up networking with the new Application account ... 369
Setting up additional VPCs in the Application account ... 370
Appendix: multi-account landing zone (MALZ) onboarding consideration list ... 371
Account configuration ... 371
AMS multi-account landing zone monitoring alerts ... 372
Network configuration ... 372
Active Directory configuration ... 374
Trend Micro Endpoint Protection (EPS) ... 374
Access: Bastions, SSH and RDP ... 374
Federation ... 375
**AMS Single-account landing zone (SALZ) onboarding ... 377**
AMS SALZ onboarding process ... 377
SALZ network architecture ... 378
AMS Single-account landing zone shared services ... 380
SALZ: Create a new AWS account for AMS ... 381
Create an AWS account ... 382

Set up consolidated billing–link new account to Payer account ..... 384
Configure your AWS account for AMS access ..... 385
Subscribe to AWS Marketplace for EPS ..... 388
Subscribe to AWS Marketplace for CentOS 7.6 ..... 390
Secure the new account with multi-factor authentication (MFA) for the root user ..... 390
SALZ: Set up networking ..... 390
Allocate IP Space for your AMS Environment ..... 390
Establish Private Network Connectivity to AWS ..... 392
Set up your Firewall ..... 393
AMS Bastion Options during Application Migrations/Onboarding ..... 393
SALZ: Set up access management ..... 398
Establish an Active Directory (AD) trust ..... 399
Federate your Active Directory with the AMS AWS Identity and Access Management roles ..... 405
SALZ: Default settings ..... 411
Endpoint Security (EPS) ..... 411
Security groups ..... 415
EC2 IAM instance profile ..... 420
Monitored metrics defaults ..... 427
Log retention and rotation defaults ..... 443
Continuity management defaults ..... 444
Patching defaults ..... 445
Validate the AMS service (SALZ) ..... 446
Find account settings ..... 446
Finding an instance ID or IP address ..... 450
DNS friendly bastion names ..... 453
Finding bastion IP addresses ..... 454
EC2 instances: Creating ..... 455
Access, requesting ..... 464
Other | Other RFC, creating (CLI) ..... 472
Any stack: deleting, rebooting, starting, stopping ..... 475
Access examples ..... 488
Reporting an incident ..... 499
Creating a service request ..... 504
Post-onboarding steps ..... 509
Tutorials ..... 509

Appendix: SALZ onboarding questionnaire ..... 537
Deployment summary ..... 537
Environment architecture considerations ..... 537
Single-Account Landing Zone Monitoring Alerts ..... 538
Maintenance Window ..... 539
Next Steps ..... 539
**Appendix: ActiveDirectory Federation Services (ADFS) claim rule and SAML settings ..... 540**
ADFS claim rule configurations ..... 540
Web console ..... 541
API and CLI access with SAML ..... 541
Script configuration ..... 541
Windows configuration ..... 541
Linux configuration ..... 543
**Document history ..... 545**

# AWS Managed Services Onboarding Introduction

Welcome to AWS Managed Services (AMS). AMS is an enterprise service that provides ongoing management of your AWS infrastructure. This guide is designed to help you get started using AMS, including how to set up a new account for AMS, set up networking and access to AMS, and validate your onboarding setup.

It is intended for IT administrators tasked with preparing for and carrying out the tasks required to onboard the AMS service to a new AWS account. Onboarding the AMS service requires special privileges to set up Active Directory trusts and complete other networking-level tasks. To get help in deciding whether to use multi-account landing zone accounts or single-account landing zone accounts, visit Choosing single MALZ or multiple MALZs .

> **Important**
>
> This guide is divided into two parts after this introduction: One for multi-account landing zone accounts and one for single-account landing zone accounts. The onboarding is quite different for the two, please go next to the section of the guide that applies to your situation.

**Topics**


- Learning about AMS
- AMS key terms
- AMS modes
- AMS post-account prescriptive guidance
- What we do, what we do not do
- AMS egress traffic management
- IAM user role in AMS
- Default Access Firewall Rules


## Learning about AMS

To understand AMS better, refer to these AMS User Guide sections:

- What Is AWS Managed Services introduces the AMS service and describes the key features, operations, and interfaces as well as a typical AMS-managed network architecture. This chapter also provides information on access management including how to access your AMS-managed resources and using bastions.
- Key Terms provides definitions and explanations for AMS terminology.
- Understanding AMS Defaults provides the default values AMS uses, including the defaults for basic environment components, IAM and EC2, proxies, monitored metrics, logging, endpoint security (EPS), backups, and patching.
- Change Management provides details on how requests for change (RFCs) and change types (CTs) work and includes examples of using AMS RFCs.
- Several additional chapters cover accessing the AWS console, the AMS CLI, using the AMS change management system, the AMS SKMS, security, service requests, incidents, monitoring, logs, EPS, backups, and patch management.

To learn more about AMS multi-account landing zone architecture, see Multi-Account Landing Zone network architecture

To learn more about AMS single-account landing zone architecture, see Single-Account Landing Zone network architecture

## AMS 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.
- *Critical Recommendation*: A recommendation issued by AWS through a service request informing you that your action is required to protect against potential risks or disruptions to your resources or the AWS services. If you decide not to follow a Critical Recommendation by the specified date, you are solely responsible for any harm resulting from your decision.

- *Customer-Requested Configuration*: Any software, services or other configurations that are not identified in:
  - 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.

  For AMS Advanced, these include multi-account landing zone (MALZ) and single-account landing zone (SALZ) accounts.
- *Billing start date*: The next business day after AWS receives the your information requested in the AWS Managed Services Onboarding Email. The AWS Managed Services Onboarding Email refers to the email sent by AWS to the you to collect the information needed to activate AWS Managed Services on the your accounts.

  For accounts subsequently enrolled by you, the billing start date is the next business day after AWS Managed Services sends an AWS Managed Services Activation Notification for the enrolled account. An AWS Managed Services Activation Notification occurs when:

  1. You grants access to a compatible AWS account and hand it over to AWS Managed Services.
  2. AWS Managed Services designs and builds the AWS Managed Services Account.
- *Service Termination*: You can terminate the AWS Managed Services for all AWS Managed Services accounts, or for a specified AWS Managed Services account for any reason by providing AWS at least 30 days notice through a service request. On the Service Termination Date, either:

  1. AWS hands over the controls of all AWS Managed Services accounts or the specified AWS Managed Services accounts as applicable, to you, or
  2. The parties remove the AWS Identity and Access Management roles that give AWS access from all AWS Managed Services accounts or the specified AWS Managed Services accounts, as applicable.
- *Service termination date*: The service termination date is the last day of the calendar month following the end of the 30 days requisite termination notice period. If the end of the requisite termination notice period falls after the 20th day of the calendar month, then the service

termination date is the last day of the following calendar month. The following are example scenarios for termination dates.

  - If the termination notice is provided on April 12, then the 30 days notice ends on May 12. The service termination date is May 31.
  - If a termination notice is provided on April 29, then the 30 days notice ends on May 29. The service termination date is June 30.

- *Provision of AWS Managed Services*: AWS makes available to you and you can access and use AWS Managed Services for each AWS Managed Services account from the service commencement date.
- *Termination for specified AWS Managed Services accounts*: You can terminate the AWS Managed Services for a specified AWS Managed Services account for any reason by providing AWS notice through a service request ("AMS Account Termination Request").

**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 Amazon 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 Amazon 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.

**Miscellaneous terms**:

- *AWS Managed Services Interface*: For AMS: The AWS Managed Services Advanced Console, AMS CM API, and Support API. For AMS Accelerate: The Support Console and 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 Amazon 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.

# AMS 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.

## AMS modes and applications or workloads

Consider operational and governance requirements for your applications when selecting the right mode, either by requesting a new application account or hosting the application in an existing application account. 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.

> **Note**
>
> For a descriptions of the mode types per AMS service, see Types of modes and accounts in AMS.
> For real-world use cases of the different modes, see Real world use cases for AMS modes

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 | |

| Decision issues | Standard CM mode / OOD* | AWS Service Catalog | Direct Change mode | Self-service provisioning | Developer mode | Customer Managed |
|---|---|---|---|---|---|---|
| | | | | | AMS CM system | |
| 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 | |
| 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 | |

| 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 | |
| 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 | |

| Decision issues | Standard CM mode / OOD* | AWS Service Catalog | Direct Change mode | Self-service provisioning | Developer mode | Customer Managed |
|---|---|---|---|---|---|---|
| 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 | |
| Incident Management and Audit | AMS responsibile for all managed accounts | | | | Customer responsible for resources provisioned using developer IAM role outside AMS Change Management System | |

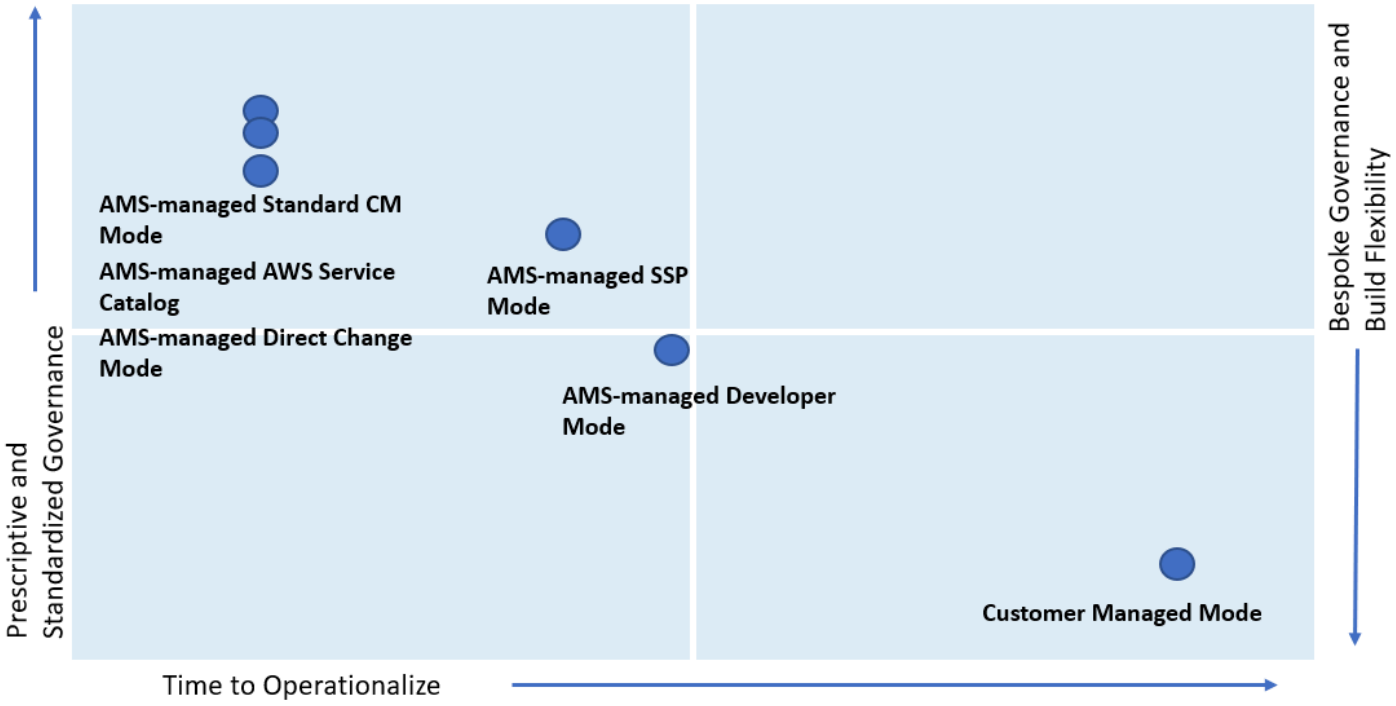
| Decision issues | Standard CM mode / OOD* | AWS Service Catalog | Direct Change mode | Self-service provisioning | Developer mode | Customer Managed |
|---|---|---|---|---|---|---|
| GuardRails and Shared infrastructure (Network) and Security Framework | Prescriptive and standardized leveraging AMS Core Accounts | | | | | Flexible and bespoke leveraging AMS Core Accounts |
| Application readiness | | | | | | |
| 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 | | | | | | |

| Decision issues | Standard CM mode / OOD* | AWS Service Catalog | Direct Change mode | Self-service provisioning | Developer mode | Customer Managed |
|---|---|---|---|---|---|---|
| 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.

# AMS post-account prescriptive guidance

As organizations adopt distributed operations and DevOps practices, there are a core set of operational capabilities that should be applied to every account prior to deployment of workloads to meet the pillars of Well Architected.

This link downloads a ZIP file containing a Word document, and a ZIP file with scripts and examples. Automated Account Setup is a set of scripts to automate, or bootstrap, the setup of a new application account.

Once a new account is vended, and before any workloads are deployed, in order to make the account ready from an operational, security and management point of view, you setup default backup plans, patch windows, and encryption (and more). To help improve the agility, consistency, and responsiveness for application account setup, the following sample "How To" is provided for your reference.

Automated Account Setup.

# 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 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 egressMgmt.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.

## IAM user role in AMS

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 Amazon 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 Amazon 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: Update Entity or IAM: Create Entity 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 MALZ: Default IAM User Roles, next.

## MALZ: Default 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 (Public AWS Managed Policy). |
| AWSManagedServicesCaseRole | ReadOnlyAccess |
| | AWSSupportAccess (Public AWS Managed Policy). |
| AWSManagedServicesChangeManagementRole (Core account version) | ReadOnlyAccess |
| | AWSSupportAccess |
| | AMSChangeManagementReadOnlyPolicy |
| | AMSChangeManagementInfrastructurePolicy |

### Core OU account: Management account roles and policies

| Role | Policy or policies |
|---|---|
| AWSManagedServicesBillingRole | AMSBillingPolicy (AMSBillingPolicy). |
| AWSManagedServicesReadOnlyRole | ReadOnlyAccess (Public AWS Managed Policy). |
| AWSManagedServicesCaseRole | ReadOnlyAccess |
| | AWSSupportAccess (Public AWS Managed Policy). |
| AWSManagedServicesChangeManagementRole (Management account version) | ReadOnlyAccess |
| | AWSSupportAccess |
| | AMSChangeManagementReadOnlyPolicy |
| | AMSChangeManagementInfrastructurePolicy |

| Role | Policy or policies |
| --- | --- |
| | AMSMasterAccountSpecificChangeManagementInfrastructure Policy |

**Core OU Account: Networking account roles and policies**

| Role | Policy or policies |
| --- | --- |
| AWSManagedServicesReadOnlyRole | ReadOnlyAccess (Public AWS Managed Policy). |
| AWSManagedServicesCaseRole | ReadOnlyAccess |
| | AWSSupportAccess (Public AWS Managed Policy). |
| AWSManagedServicesChangeManagementRole (Networking account version) | ReadOnlyAccess |
| | AWSSupportAccess |
| | AMSChangeManagementReadOnlyPolicy |
| | AMSChangeManagementInfrastructurePolicy |
| | AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy |

## Application Account Roles

Application account roles are applied to your application-specific accounts.

**Application account: Roles and policies**

| Role | Policy or policies |
| --- | --- |
| AWSManagedServicesReadOnlyRole | ReadOnlyAccess (Public AWS Managed Policy). |
| AWSManagedServicesCaseRole | ReadOnlyAccess |

| Role | Policy or policies |
| --- | --- |
| | AWSSupportAccess (Public AWS Managed Policy).<br><br>This policy provides access to all support operations and resources. For information, see Getting Started with AWS Support. |
| AWSManagedServicesSecurityOpsRole | ReadOnlyAccess |
| | AWSSupportAccess Example<br><br>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 |
| AWSManagedServicesChangeManagementRole (Application account version) | ReadOnlyAccess |
| | AWSSupportAccess (Public AWS Managed Policy).<br><br>This policy provides access to all support operations and resources. For information, see Getting Started with AWS Support. |
| | AMSSecretsManagerSharedPolicy |
| | AMSChangeManagementPolicy |
| | AMSReservedInstancesPolicy |

| Role | Policy or policies |
| --- | --- |
| | AMSS3Policy |
| AWSManagedServicesAdminRole | ReadOnlyAccess |
| | AWSSupportAccess |
| | AMSChangeManagementInfrastructurePolicy |
| | AWSMarketplaceManageSubscriptions |
| | AMSSecretsManagerSharedPolicy |
| | AMSChangeManagementPolicy |
| | AWSCertificateManagerFullAccess |
| | AWSWAFFullAccess |
| | AMSS3Policy |
| | AMSReservedInstancesPolicy |

## 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 Management 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.

JSON

```
{
    "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:*",
                "compute-optimizer:*"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostExplorerComputeOptimizer"
        },
        {
            "Action": [
                "purchase-orders:ViewPurchaseOrders",
                "purchase-orders:ModifyPurchaseOrders"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPurchaseOrders"
```

```
        },
        {
            "Action": [
                "redshift:AcceptReservedNodeExchange",
                "redshift:PurchaseReservedNodeOffering"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToRedshiftAction"
        },
        {
            "Action": "savingsplans:*",
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AWSSavingsPlansFullAccess"
        }
    ]
}
```

**AMSChangeManagementReadOnlyPolicy**

`AMSChangeManagementReadOnlyPolicy`

Permissions to see all AMS change types, and the history of requested change types.

**AMSMasterAccountSpecificChangeManagementInfrastructurePolicy**

`AMSMasterAccountSpecificChangeManagementInfrastructurePolicy`

Permissions to request the Deployment | Managed landing zone | Management account | Create application account (with VPC) change type.

**AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy**

`AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy`

Permissions to request the Deployment | Managed landing zone | Networking account | Create application route table change type.

**AMSChangeManagementInfrastructurePolicy**

`AMSChangeManagementInfrastructurePolicy` (for Management | Other | Other CTs)

Permissions to request the Management | Other | Other | Create, and Management | Other | Other | Update change types.

**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. (for example, license keys for products that need to be deployed).

JSON

```
{
 "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.

### AMSReservedInstancesPolicy

`AMSReservedInstancesPolicy`

Permissions to manage Amazon EC2 reserved instances; for pricing information, see Amazon EC2 Reserved Instances.

JSON

```
{
 "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 Amazon 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.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:PutObject"
            ],
            "Resource": "*"
        }
    ]
}
```

### AWSSupportAccess

`AWSSupportAccess`

Full access to Support. For information, see Getting Started with Support. For Premium Support information, see Support.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "support:*"
  ],
```

```
  "Resource": "*"
 }]
}
```

### AWSMarketplaceManageSubscriptions

`AWSMarketplaceManageSubscriptions` (Public AWSManaged Policy)

Permissions to subscribe, unsubscribe, and view AWS Marketplace subscriptions.

JSON

```
{
 "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 more information, see AWS Certificate Manager.

`AWSCertificateManagerFullAccess` information, (Public AWS Managed Policy).

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
```

```
  "Action": [
   "acm:*"
  ],
  "Resource": "*"
 }]
}
```

### AWSWAFFullAccess

`AWSWAFFullAccess`

Full access to AWS WAF. For more information, see AWS WAF - Web Application Firewall.

`AWSWAFFullAccess` information, (Public AWS Managed policy). This policy grants full access to AWS WAF resources.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Action": [
   "waf:*",
   "waf-regional:*",
   "elasticloadbalancing:SetWebACL"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

### ReadOnlyAccess

`ReadOnlyAccess`

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.

If you have an active AWS account, then you can use this link ReadOnlyAccess to view the entire ReadOnlyAccess policy. The whole ReadOnlyAccess policy is very long as it provides read-only access to all AWS services. The following is a partial excerpt of the ReadOnlyAccess policy.

**Single-Account Landing Zone (SALZ)**: To see the AMS single-account landing zone default, uncustomized, user role policies, see SALZ: Default IAM User Role, next.

## SALZ: Default 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:

Managed Services IAM ReadOnly Policy

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

JSON

```
{
  "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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

# Default Access Firewall Rules

These are the default firewall rules required to access your instances.

> **Note**
>
> For information on firewall rules and ports required for establishing an AD one-way trust, see the AMS Security Guide by going to the AWS Artifact console -> Reports tab and search for AWS Managed Services.

## Linux Stack Instance Ports

These rules are required for your authentication into AMS Linux stacks.

**Linux Instance Ports Rules FROM: Linux Stack Instance TO: CORP Domain Controller**

| Port | Protocol | Service | Direction |
|---|---|---|---|
| 389 | TCP | LDAP | Ingress |
| 389 | UDP | LDAP | Ingress |
| 88 | TCP | Kerberos | Ingress |
| 88 | UDP | Kerberos | Ingress |

## Windows Stack Instance Ports

These rules are required for your authentication into AMS Windows stacks.

**FROM: Windows Stack Instance TO: CORP Domain Controller**

| Port | Protocol | Service | Direction |
|---|---|---|---|
| 88 | TCP \| UDP | Kerberos | Ingress and Egress |
| 135 | TCP \| UDP | DCE/RPC Locator service | Ingress and Egress |
| 389 | TCP \| UDP | LDAP | Ingress and Egress |

| Port | Protocol | Service | Direction |
| --- | --- | --- | --- |
| 3268 | TCP \| UDP | msft-gc, Microsoft Global Catalog (LDAP service which contains data from Active Directory forests) | Ingress and Egress |
| 445 | TCP | Microsoft-DS Active Directory, Windows shares | Ingress and Egress |
| 49152 - 65535 | TCP | Dynamic or private ports that cannot be registered with IANA. This range is used for private, or customized services or temporary purposes and for automatic allocatio n of ephemeral ports. | Ingress and Egress |

# Service management in AWS Managed Services

**Topics**


- Account governance in AWS Managed Services
- Service commencement in AWS Managed Services
- Customer relationship management (CRM)
- Cost optimization in AWS Managed Services
- Service hours in AWS Managed Services
- Getting help in AWS Managed Services


How the AMS service works for you.

## Account governance in AWS Managed Services

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 in AWS Managed Services

*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 | Custome | 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 |

# Customer relationship management (CRM)

AWS Managed Services (AMS) provides a customer relationship management (CRM) process 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<br><br>12-week operational trend (+/- 6)<br><br>Application operator concerns<br><br>Weekend schedule | On-site customer location/ Telecom/Chime | AMS: CSDM and cloud architect (CA)<br><br>Customer assigned team members (ex: Cloud/ Infrastructure, Application Support, Architecture teams, etc.) |
| Monthly business review | Review service level performance (reports, analysis, and trends)<br><br>Financial analysis<br><br>Product roadmap<br><br>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)<br><br>You: Application Operator representative |

| Meeting | Purpose | Mode | Participants |
| --- | --- | --- | --- |
| Quarterly business review | Scorecard and service level agreement (SLA) performance and trends (6 months)<br><br>Upcoming 3/6/9/12 months plans/ migrations<br><br>Risk and risk mitigations<br><br>Key improvement initiatives<br><br>Product roadmap items<br><br>Future direction aligned opportunities<br><br>Financials<br><br>Cost savings initiatives<br><br>Business optimization | On-site customer location | AMS: CSDM, cloud architect , AMS account team, AMS service director, AMS operation manager<br><br>You: Application operator representative, service representative, service director |

## 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

# Cost optimization in AWS Managed Services

AWS Managed Services provides a detailed cost utilization and savings reports every month to you during your monthly business reviews (MBRs).

AMS follows a standard set of processes and mechanisms to identify cost saving avenues in your managed accounts and assist you to plan and roll-out the changes to optimize your AWS spend.

> **Note**
>
> AMS is developing a video to help with cost optimization. The first step is providing you with a PDF and an Excel spreadsheet of cost optimization best practices. To access these resources, open the Quick guide to cost optimization ZIP file.

## Cost optimization framework

AMS follows a three-staged approach with you to optimize your AWS costs:

1. Identify cost optimization avenues in your managed environment
2. Present a cost optimization plan to you
3. Assist in achieving cost optimization in a measurable way

### Identify cost optimization avenues in the managed environment

AMS utilizes AWS native tools like Cost explorer, and Trusted Advisor while leveraging over 20 cost savings patterns across architecture optimization, EC2 instance, and AWS account-focused optimizations to build tailored cost savings recommendations for you.

Some of the optimization recommendations include the following.

**Architectural optimization recommendations:**

- **Optimal S3 storage class use**: Amazon S3 offers a range of storage classes to meet various workload requirements based on data access, resiliency, and cost. S3 Intelligent-Tiering and S3 storage class analysis based on the workload needs allow you to manage the S3 costs efficiently.
- **Using caching architectures**: Leveraging cache instances, where applicable, can help you replace some database instances, while simultaneously meeting your IOPS requirements.

- **EBS upgrade savings**: Migrating your EBS volumes from gp2 to gp3 provides a cost savings of up to 20% and you can take advantage of predictable 3,000 IOPS baseline performance and 125 MiB/s, regardless of volume size.
- **Using elasticity**: The auto-scaling capabilities that AWS provides allow effective resource utilization and avenues for cost optimization. Reviewing and updating the instance scaling policies regularly based on need, further provides cost savings.

### EC2 instance-focused recommendations

- **Instance rightsizing**: Recommendations focused on sizing the instances and optimal configurations based on the usage. Recommendations also include utilizing Amazon EC2 Auto Scaling feature and replacing EC2 instances where applicable with AWS Lambda or static web content on Amazon S3, etc.
- **Instance scheduling**: Using AMS Resource Scheduler to automatically start and stop instances based on a time schedule helps contain costs, especially for non-production instances that are not utilized during non-business hours.
- **Subscribing to Savings plans**: Savings plan is the easiest way to save on AWS usage. The EC2 Instance Savings Plans offer up to 72% savings compared to On-Demand pricing on your Amazon EC2 instances usage. The Amazon SageMaker AI Savings Plans offer up to 64% savings on your Amazon SageMaker AI services usage. AMS provides appropriate recommendations on Savings plans based on your AWS resource usage.
- **Reserved instance (RI) usage and consumption guidance**: Amazon EC2 Reserved Instances (RI) provide a significant discount (up to 75%) compared to On-Demand pricing and provide a capacity reservation when used in a specific availability zone.
- **Spot instance usage**: Fault tolerant workloads can utilize Spot instances and reduce prices up to 90%.
- **Idle instance termination**: Identifying and reporting instances that are idle or have low utilization that can be terminated.

### Account-focused recommendations

- **Account cleanup**: At an account level, AMS also identifies un-utilized EBS volumes, duplicate CloudTrail trails, empty accounts with unused resources, and so forth, and provides recommendations for clean-up.

- **SLA recommendations**: Further, AMS regularly reviews your Plus and Premium accounts and recommends choosing the right SLA level for the accounts.
- **AMS automation optimization**: AMS continuously optmizes AMS automation and infrastructure used to provide AMS services.

### Present to customers and assist in planning

AMS conducts monthly business reviews (MBRs) with the key customer stakeholders and present the cost saving avenues, mechanisms and recommendations identified along with potential cost savings. We further work with you to plan the changes needed.

### Assist in recommendation implementation and measure the cost impact

AMS assists in achieving and measuring cost impacts and optimization changes.

You assess the application impact, risk and success criteria of the recommended changes, and raise the appropriate requests for change (RFCs) through the AMS console. AMS collaborates with you and implements the changes related to cost optimization in your managed accounts. AMS measures the cost impact and include the savings realised in the monthly business reviews (MBRs).

## Cost optimization responsibility matrix

Responsibilities in AMS cost optimization.

**Cost optimization RACI**

| Activity | Customer | AMS |
|---|---|---|
| Compiling cost saving recommendations and preparing the report | I | R |
| Presenting cost | C | R |

| Activity | Customer | AMS |
| --- | --- | --- |
| savings report | | |
| Planning changes associated with cost savings | R | C |
| Assessing the change impact and risk | R | C |
| Raising RFCs for implementing the changes | R | C |
| Reviewing the RFCs and implementing the changes | C | R |

| Activity | Customer | AMS |
|---|---|---|
| Testing the application and validating the change implementation | R | C |
| Measuring the cost impact post change and presenting to customer | I | R |

# Service hours in AWS Managed Services

| Feature | AMS Advanced |
|---|---|
| | Premium Tier |
| Service request | 24/7 |
| Incident management (P2-P3) | 24/7 |
| Backup and recovery | 24/7 |
| Patch management | 24/7 |
| Monitoring and alerting | 24/7 |

| Feature | AMS Advanced |
| --- | --- |
| | Premium Tier |
| Automated request for change (RFC) | 24/7 |
| Non-automated request for change (RFC) | 24/7 |
| Cloud service delivery manager (CSDM) | Monday to Friday: 08:00–17:00, local business hours |

## Getting help in AWS Managed Services

AMS supports you with Incident Management, Service Request Management, and Change Management 24 hours a day, 7 days a week, 365 days a year (in accordance with the AMS Service Level Agreement applied to the account).

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.

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

# Change management modes

AWS Managed Services (AMS) uses change management mode to guardrail changes in AMS Advanced. The change management modes help you maintain high operational standards for the environment, and to control risk and prevent adverse impact. AMS Advanced has different modes that provide different levels of control and risk. All modes, except for Customer-Managed mode, are managed by AMS. The following are the available change management modes:

- RFC mode (formerly Standard CM mode): Provides a "request for change" (RFC) system and AMS-custom change types (CTs)
- Direct Change mode: Same as RFC mode plus use of AWS APIs and consoles to create AMS-managed resources
- AWS Service Catalog on AMS: Similar to Direct Change mode, but instead of using the AMS change management system (RFCs), you use AWS Service Catalog to create resources that AMS then manages.
- Developer mode: Same as Direct Change mode only the resources you create with AWS APIs and consoles are not AMS-managed—you are responsible for their management
- Self Service Provisioning (SSP) mode: Same as Developer mode except there is no access to the AMS change management system (no RFCs)
- Customer Managed mode: AMS provides you with a multi-account landing zone landing zone but all resource management is your responsibility

The AWS Managed Services (AMS) change management system, using the change management (CM) API, provides operations to create and manage requests for change (RFCs) for both multi-account landing zone (MALZ) and single-account landing zone (SALZ) accounts.

A request for change (RFC) is a request created by either you or AMS through the AMS interface to make a change to your managed environment and includes a change type (CT) ID for a particular operation.

The AMS change management (CM) API provides operations to create and manage requests for change (RFCs). You can create, update, submit, approve, reject, and cancel RFCs. The AMS operators can create, update, submit, approve, reject, cancel, and mark RFCs as closed.

For a list of AMS reserved prefixes not to be used in tag or other names, see Reserved prefixes.

For information on each change type, including schemas and examples, see the AMS Change Type Reference.

> **Note**
>
> All change management API calls are recorded in AWS CloudTrail. For more information, see Accessing your logs.

# Modes overview

Use this information 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 is most useful during the foundation phase of setting up your AMS-managed platform, and 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

AWS Managed Services (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.

> **Note**
>
> For details about application deployment and choosing the right AMS mode, see AMS modes and applications or workloads.
> For real-world use cases of the different modes, see Real world use cases for AMS modes

The following table provides descriptions of the modes per AMS service.

| AMS feature | RFC mode (formerly 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 RFC mode for high-risk changes like IAM or security groups | None | | |
| Logging, Monitoring, Guardrails, and Event Management | Yes (supported resources) | | | No | |

| AMS feature | RFC mode (formerly Standard CM mode) / OOD* | Direct Change mode | AWS Service Catalog | Self-service provisioning / Developer mode | Customer Managed |
|---|---|---|---|---|---|
| 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 RFC 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**
>
> Self-Service Provisioning mode in AMS and AMS Advanced Developer mode may both appear to be a suitable fit for an application that has complex architecture rooted in native

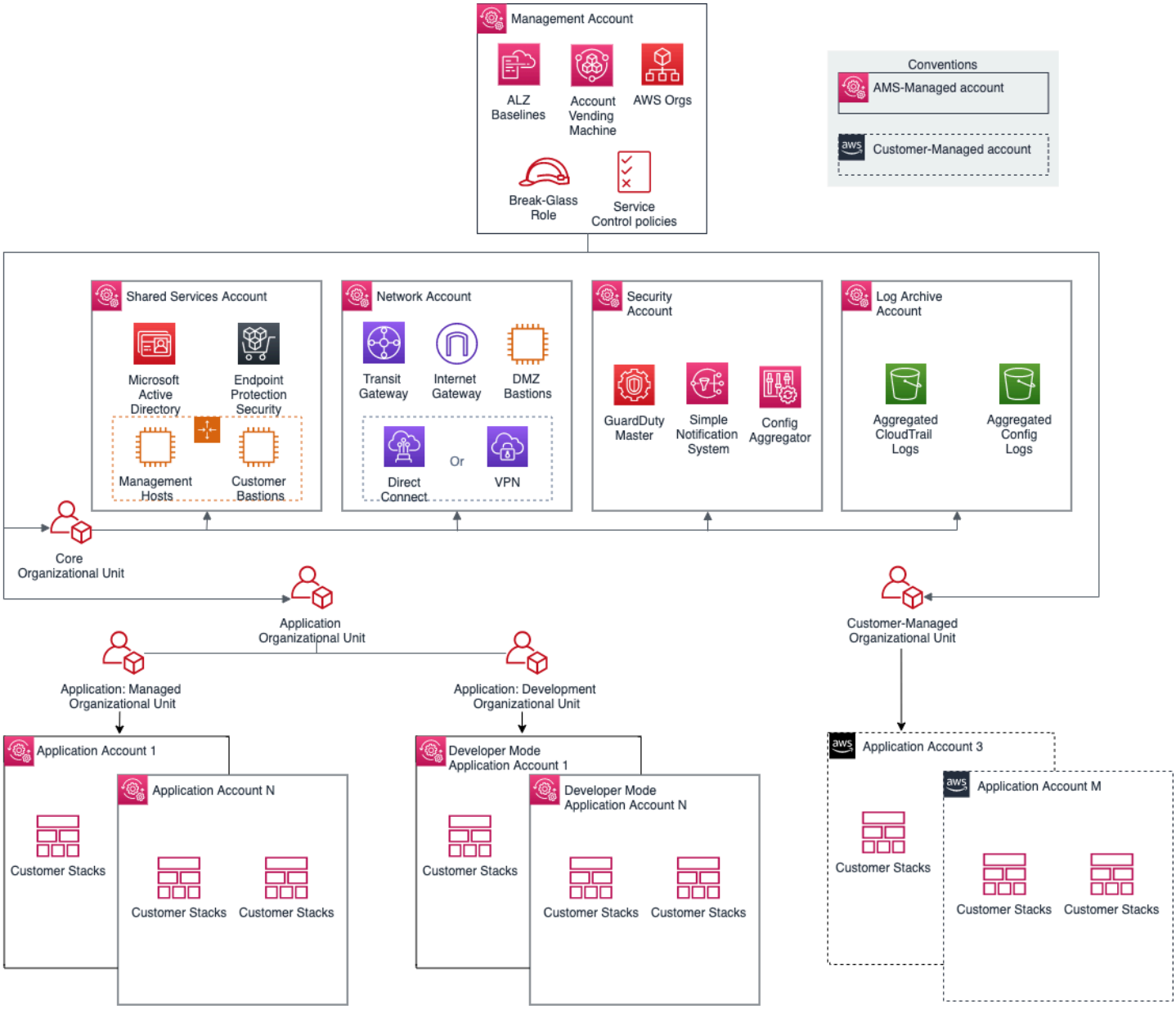
AWS Services. When architecting workloads, you make trade-offs between operational excellence and agility, based on your business context. This is a good way to think about selecting SSP mode or Developer mode for your application. The selection may also change based on the SDLC phase of the application. 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.

## MALZ architecture and associated AMS modes

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: RFC 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

| AMS Modes | Default Governance controls (Guardrails) | | Support for Customer Added Governance Controls |
|---|---|---|---|
| | Preventative Controls | Detective Controls | |
| AMS Managed – Standard CM Mode and OOD | | | Yes (Restrictive)* |
| AMS Managed - Direct Change Mode (DCM) | | | Yes (Restrictive)* |
| AMS Managed – AWS Service Catalog | | | Yes (Restrictive)* |
| AMS Managed – Self Service Provisioning (SSP) | | | Yes (Restrictive)* |
| AMS Managed – Developer Mode | | | Yes |
| Customer Managed | | | Yes |

> **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 modes and applications or workloads

Consider operational and governance requirements for your applications when selecting the right mode, either by requesting a new application account or hosting the application in an existing application account. 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.

> **Note**
>
> For a descriptions of the mode types per AMS service, see Types of modes and accounts in AMS.
> For real-world use cases of the different modes, see Real world use cases for AMS modes

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 | |
| 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 | |

| Decision issues | Standard CM mode / OOD* | AWS Service Catalog | Direct Change mode | Self-service provisioning | Developer mode | Customer Managed |
|---|---|---|---|---|---|---|
| | | | | | developer IAM role outside AMS CM system | |
| 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 | |
| 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 | |

| Decision issues | Standard CM mode / OOD* | AWS Service Catalog | Direct Change mode | Self-service provisioning | Developer mode | Customer Managed |
|---|---|---|---|---|---|---|
| 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 | |
| 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 | |

| Decision issues | Standard CM mode / OOD* | AWS Service Catalog | Direct Change mode | Self-service provisioning | Developer mode | Customer Managed |
|---|---|---|---|---|---|---|
| Incident Management and Audit | AMS responsibile for all managed accounts | | | | Customer responsible for resources provisioned using developer IAM role outside AMS Change Management System | |
| GuardRails and Shared infrastructure (Network) and Security Framework | Prescriptive and standardized leveraging AMS Core Accounts | | | | | Flexible and bespoke leveraging AMS Core Accounts |
| Application readiness | | | | | | |

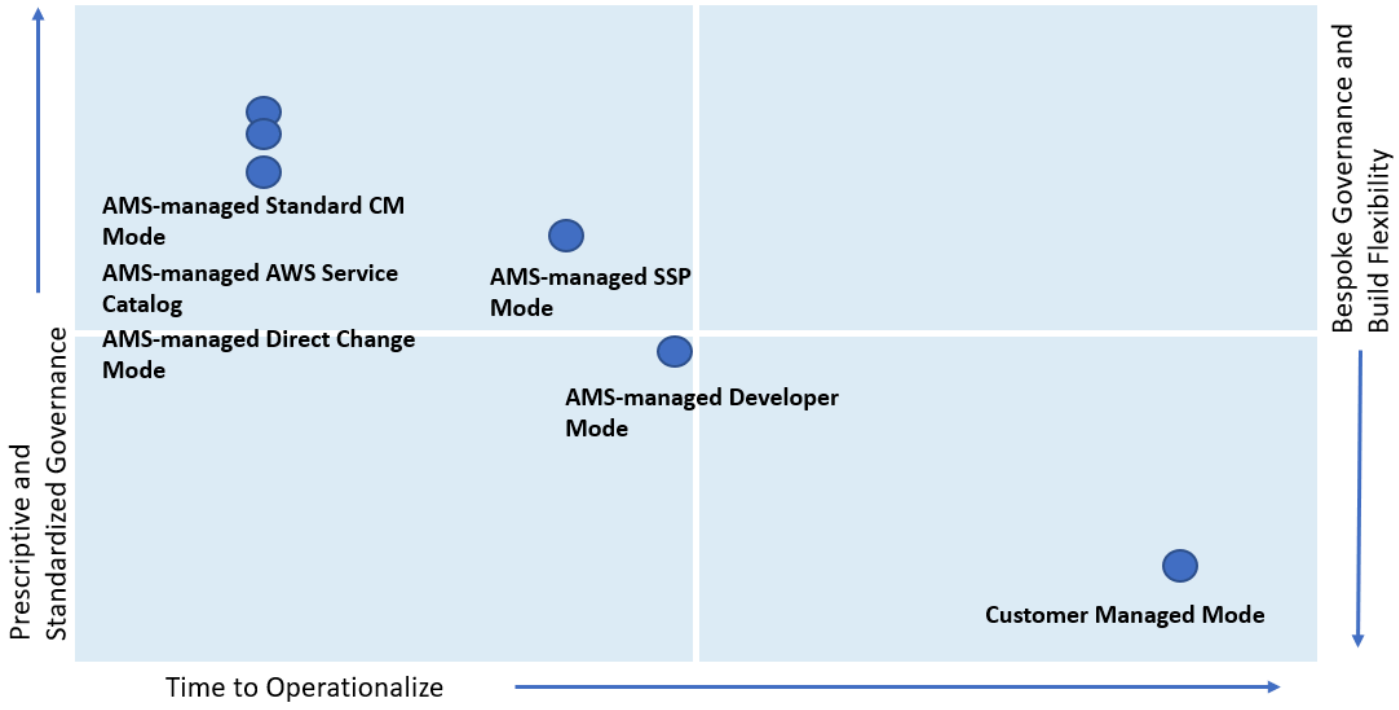
| Decision issues | Standard CM mode / OOD* | AWS Service Catalog | Direct Change mode | Self-service provisioning | Developer mode | Customer Managed |
|---|---|---|---|---|---|---|
| Application refactoring | Light refactoring is needed | | | | Light refactoring is needed (if provisioned using AMS 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 | $$$$ | | | $$$ | $$ | $ |

| Decision issues | Standard CM mode / OOD* | AWS Service Catalog | Direct Change mode | Self-service provisioning | Developer mode | Customer Managed |
|---|---|---|---|---|---|---|
| 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 RFC 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 RFC 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 RFC 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 RFC 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 RFC 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 RFC to AMS-managed Developer mode, 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 RFC 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 RFC 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 mode and AMS-managed.

# RFC mode

RFC mode is the default mode for AMS Advanced operations plan customers. It includes a change management system with requests for change or RFCs and a catalog of change types to use to request the addition or change that you need to your accounts. This change management system provides a level of security in limiting who can make changes to your accounts.

For details on AMS Advanced change types, see What Are AMS Change Types?.

For details about onboarding to AMS Advanced, see AWS Managed Services Onboarding Introduction.

For change type example walkthroughs, see the "Additional Information" section for the relevant change type in the *AMS Advanced Change Type Reference* Change Types by Classification section.

> **Note**
>
> RFC mode was previously called "Change Management mode" or "Standard CM mode."

**Topics**


- Learn about RFCs
- What are change types?
- Troubleshooting RFC errors in AMS


## Learn about RFCs

Requests for change, or RFCs, work in a two-fold manner. First, there are parameters required for the RFC itself. These are the options in the `CreateRfc` API. And second, there are parameters required for the action of the RFC (the execution parameters). To learn about the `CreateRfc` options, see the CreateRfc section of the *AMS API Reference*. These options typically appear in the **Additional configurations** area of the Create RFC pages.

You can create and submit an RFC with the `CreateRfc` API, `aws amscm create-rfc` CLI, or using the AMS console Create RFC pages. For a tutorial on creating an RFC, see Create an RFC.

**Topics**

- What are RFCs?
- Authenticate when using the AMS API/CLI
- Understand RFC security reviews
- Understand RFC change type classifications
- Understand RFC action and activity states
- Understand RFC status codes
- Understand RFC update CTs and CloudFormation template drift detection
- Schedule RFCs
- Approve or reject RFCs
- Request RFC restricted run periods
- Create, clone, update, find, and cancel RFCs
- Use the AMS console with RFCs
- Learn about common RFC parameters
- Sign up for the RFC daily email


## What are RFCs?

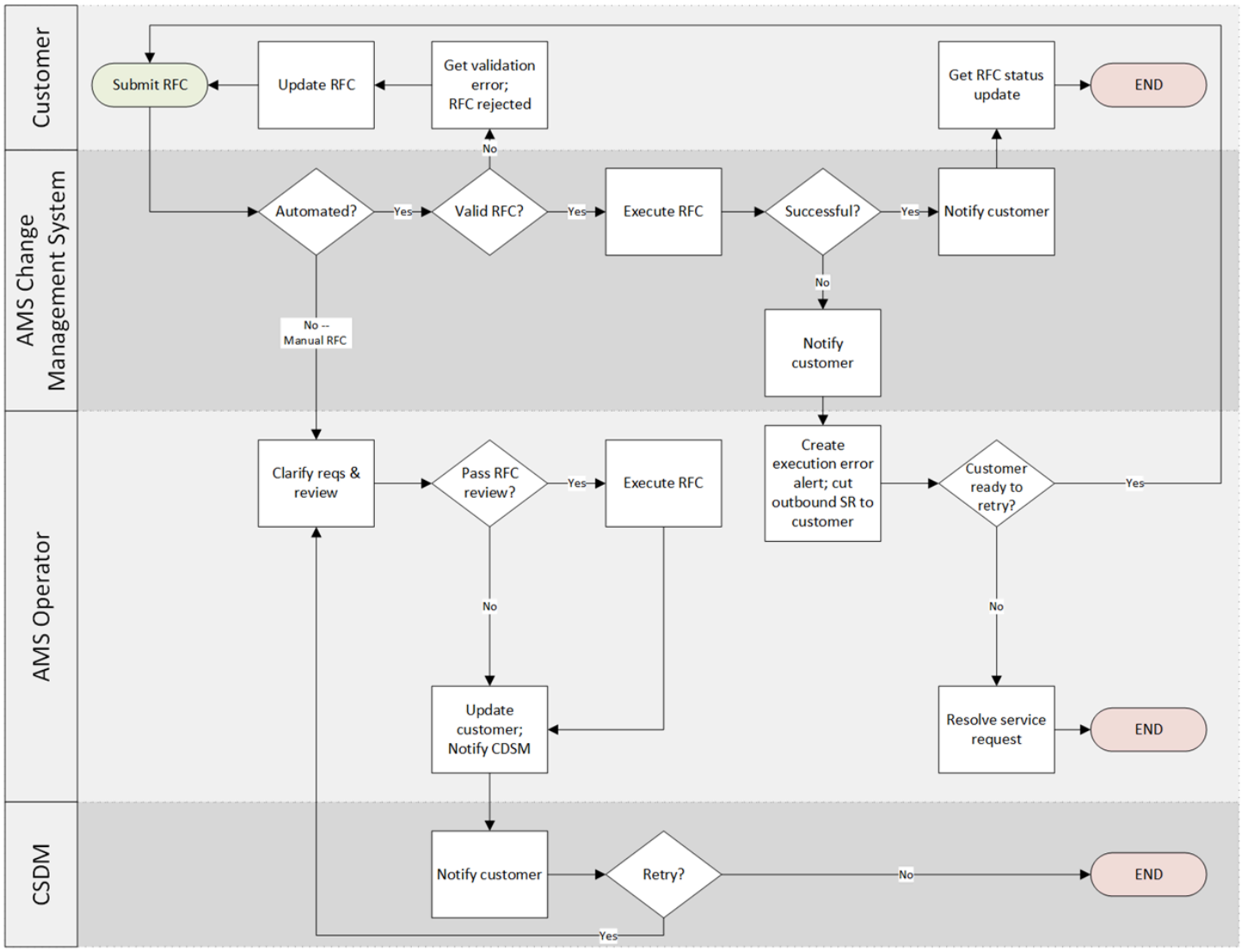
A request for change, or RFC, is how you make a change in your AMS-managed environment, or ask AMS to make a change on your behalf. To create an RFC, you choose from AMS change types, choose RFC parameters (such as schedule), and then submit the request using either the AMS console or the API commands CreateRfc and SubmitRfc.

An RFC contain two specifications, one for the RFC itself, and one for the change type (CT) parameters. At the command line, you can use an Inline RFC command, or a standard CreateRfc template in JSON format, that you fill out and submit along with the CT JSON schema file that you create (based on the CT parameters). The CT name is an informal description of the CT. A CSIO (category, subcategory, item, operation) is a more formal description of a CT. Only the CT ID must be specified when creating an RFC.

AMS notifies you when the change has completed successfully (Success) or unsuccessfully (Failure).

> **Note**
>
> For information about troubleshooting RFC failures, see Troubleshooting RFC errors in AMS.

The following graphic depicts the workflow of an RFC submitted by you.




## Authenticate when using the AMS API/CLI

When you use the AMS API/CLI, you must authenticate with temporary credentials. To request temporary security credentials for federated users, cal GetFederationToken, AssumeRole, AssumeRoleWithSAML, or AssumeRoleWithWebIdentity AWS security token service (STS) APIs.

A common choice is SAML. After set up, you add an argument to each operation that you call. For example: `aws --profile saml amscm list-change-type-categories`.

A shortcut for SAML 2.0 profiles is to set the profile variable at the start of each API/CLI with `set AWS_DEFAULT_PROFILE=saml` (for Windows; for Linux it would be `export AWS_DEFAULT_PROFILE=saml`). For information about setting CLI environment variables, see Configuring the AWS Command Line Interface, Environment Variables.

## Understand RFC security reviews

The AWS Managed Services (AMS) change management approval process ensures that we perform a security review of changes we make in your accounts.

AMS evaluates all the requests for change (RFCs) against AMS technical standards. Any change that might lower your account's security posture by deviating from the technical standards, goes through a security review. Duringthe security review, AMS highlights relevant risk and, in cases of high or very high security risk, your authorized security personnel accepts or rejects the RFC. All changes are also evaluated to assess for adverse impact on AMS's ability to operate. If potential adverse impacts are found, then additional reviews and approvals are required within AMS.

### AMS technical standards

AMS Technical Standards define the minimum security criteria, configurations, and processes to establish the baseline security of your accounts. These standards must be followed by both AMS and you.

Any change that could potentially lower the security posture of your account by deviating from the technical standards, goes through a Risk Acceptance process, where relevant risk is highlighted by AMS and accepted or rejected by the authorized security personnel from your end. All such changes are also evaluated to assess if there would be any adverse impact on AMS's ability to operate the account and, if so, additional reviews and approvals are required within AMS.

### RFC customer security risk management (CSRM) process

When someone from your organization requests a change to your managed environment, AMS reviews the change to determine whether the request might deteriorate the security posture of your account by falling outside the technical standards. If the request does lower the security posture of the account, AMS notifies your security team contact with the relevant risk, and executes the change; or, if the change introduces high or very high security risk in the environment, AMS seeks explicit approval from your security team contact in the form of risk acceptance (explained next). The AMS Customer Risk Acceptance process is designed to:

- Ensure risks are clearly identified and communicated to the right owners
- Minimize identified risks to your environment
- Obtain and document approval from the designated security contacts who understand your organization's risk profile

- Reduce ongoing operational overhead for identified risks

#### How to access technical standards and high or very high risks

We have made AMS Technical Standards documentation available for your reference in the https://console.aws.amazon.com/artifact/ as a report. Use the AMS Technical Standards documentation to understand whether a change would require risk acceptance from your authorized security contact prior to submitting a request for change (RFC).

Find the Technical Standards report by searching on "AWS Managed Services (AMS) Technical Standards" in the AWS Artifact **Reports** tab search bar after logging in with the default **AWSManagedServicesChangeManagementRole**.

> **Note**
>
> The AMS technical standard document is accessible for the Customer_ReadOnly_Role in single-account landing zone. In multi-account landing zone, the AWSManagedServicesAdminRole used by security admins and AWSManagedServicesChangeManagementRole used by application teams, can be used to access the document. If your team uses a custom role, create an Other | Other RFC to request access and we will update the specified custom role.

## Understand RFC change type classifications

The change types that you use when submitting an RFC are divided into two broad categories:

- **Deployment**: This classification is for creating resources.
- **Management**: This classification is for updating or deleting resources. The **Management** category also contains change types for accessing instances, encrypting or sharing AMIs, and starting,stopping,rebooting, or deleting stacks.

## Understand RFC action and activity states

`RfcActionState` (API) / **Activity State** (console) help you understand the status of human intervention, or action, on an RFC. Used primarily for manual RFCs, the `RfcActionState` helps you understand when there is action needed by either you or AMS operations, and helps you see

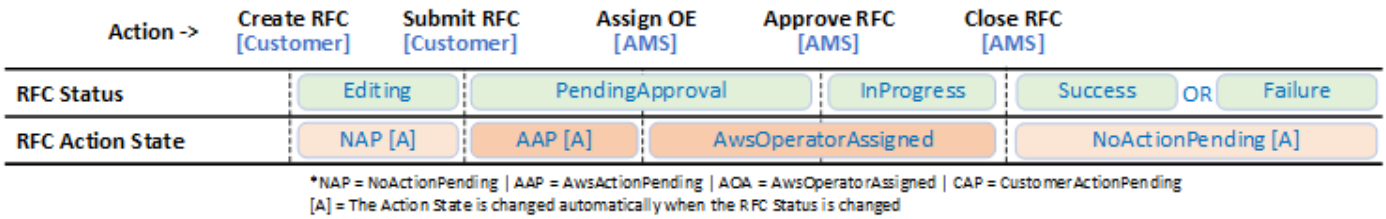
when AMS Operations is actively working on your RFC. This provides increased transparency into the actions being taken on an RFC during its lifecycle.

`RfcActionState` (API) / **Activity State** (console) definitions:

- **AwsOperatorAssigned**: An AWS operator is actively working on your RFC.
- **AwsActionPending**: A response or action from AWS is expected.
- **CustomerActionPending**: A response or action from the customer is expected.
- **NoActionPending**: No action is required from either AWS or the customer.
- **NotApplicable**: This state can't be set by AWS operators or customers, and is used only for RFCs that were created prior to this functionality being released.

RFC action states differ depending on whether the change type submitted requires manual review and has scheduling set to **ASAP** or not.

- RFC **ActionState** changes during the review, approval, and start of a manual change type with deferred scheduling:
  - After you submit a manual, scheduled, RFC, the **ActionState** automatically changes to **AwsActionPending** to indicate that an operator needs to review and approve the RFC.
  - When an operator begins actively reviewing your RFC, the **ActionState** changes to **AwsOperatorAssigned**.
  - When the operator approves your RFC, the RFC Status changes to Scheduled, and the **ActionState** automatically changes to **NoActionPending**.
  - When the scheduled start time of the RFC is reached, the RFC Status changes to **InProgress**, and the **ActionState** automatically changes to **AwsActionPending** to indicate that an operator needs to be assigned for review of the RFC.
  - When an operator begins actively running the RFC, they change the **ActionState** to **AwsOperatorAssigned**.
  - Once completed, the Operator closes the RFC. This automatically changes the **ActionState** to **NoActionPending**.



**Important**

- Action states can't be set by you. They are either set automatically based on changes in the RFC, or set manually by AMS operators.
- If you add correspondence to an RFC, the **ActionState** is automatically set to **AwsActionPending**.
- When an RFC is created, the **ActionState** is automatically set to **NoActionPending**.
- When an RFC is submitted, the **ActionState** is automatically set to **AwsActionPending**.
- When an RFC is Rejected, Canceled, or completed with a status of Success or Failure, the **ActionState** is automatically reset to **NoActionPending**.
- Action states are enabled for both automated and manual RFCs, but mostly matter for manual RFCs because those type of RFCs often require communications.

### Review RFC action states use case examples

#### Use Case: Visibility on Manual RFC Process

- Once you submit a manual RFC, the RFC action state automatically changes to `AwsActionPending` to indicate that an operator needs to review and approve the RFC. When an operator begins actively reviewing your RFC, the RFC action state changes to `AwsOperatorAssigned`.
- Consider a manual RFC that has been approved and scheduled and is ready to begin running. Once the RFC status changes to `InProgress`, the RFC action state automatically changes to `AwsActionPending`. It changes again to `AwsOperatorAssigned` once an operator starts actively running the RFC.
- When a manual RFC is completed (closed as "Success" or "Failure"), the RFC Action state changes to `NoActionPending` to indicate that no further actions are necessary from either the customer or operator.

#### Use case: RFC correspondence

- When a manual RFC is `Pending Approval`, an AMS Operator might need further information from you. Operators will post a correspondence to the RFC and change the RFC action state to

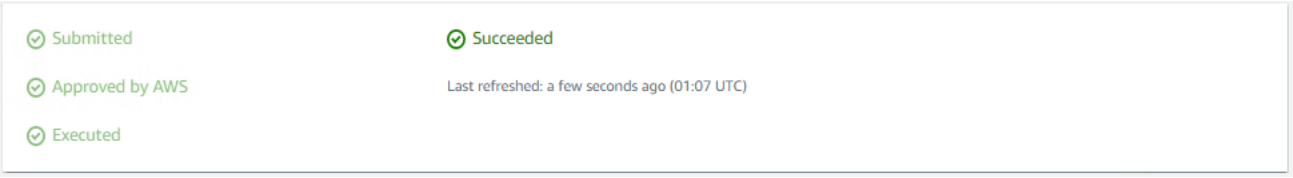
`CustomerActionPending`. When you respond by adding a new RFC correspondence, the RFC action state automatically changes to `AwsActionPending`.

- When an automated or manual RFC has failed, you can add a correspondence to the RFC details, asking the AMS Operator why the RFC failed. When your correspondence is added, the RFC action state is automatically set to `AwsActionPending`. When the AMS operator picks up the RFC to view your correspondence, the RFC action state changes to `AwsOperatorAssigned`. When the operator responds by adding a new RFC correspondence, the RFC action state may be set to `CustomerActionPending`, indicating that there is another response from the customer expected, or to `NoActionPending`, indicating that no response from the customer is needed or expected.

## Understand RFC status codes

RFC status codes help you track your requests. You can observe these status codes during an RFC run in the CLI output, or by refreshing the RFC list page in the console.

You can also see the codes for an RFC on the details page for that RFC, which might look like this:




You might see an RFC in your list that you didn't submit. When AMS operators use an internal-only CT, they submit it in an RFC and it displays in your RFC list. For more information, see Internal-only change types.

> **Important**
>
> You can request notifications of RFC state changes. For details, see RFC State Change Notifications.

**RFC status codes**

| Success | Failure |
| --- | --- |
| Editing: the RFC has been created but not submitted<br><br>PendingApproval / Submitted: The RFC has been submitted and the system is determining if it requires approval, and obtaining that approval, if required<br><br>Approved by AWS / Approved by customer: the RFC has been approved. Automated RFCs are approved by AWS, manual RFCs are approved by Operators and, sometimes, customers<br><br>Scheduled: the RFC has passed syntax and requirement checks and is scheduled for running<br><br>InProgress: the RFC is being run, note that RFCs that provision multiple resources or have long-running UserData, take longer to run<br><br>Executed: The RFC has been run<br><br>Success / Succeeded: The RFC has been successfully completed | Rejected: RFCs are rejected typically because they fail validation; for example, an unusable resource, i.e. a subnet, is specified<br><br>Canceled: RFCs are canceled typically because they do not pass validation before the configured start time has passed<br><br>Failure: The RFC has failed; see the StatusReason in the output for failure reasons, and AMS operations automatically creates a trouble ticket and communicates with you as needed |

> **Note**
>
> Canceled or rejected RFCs can be re-submitted using UpdateRfc; see also Update RFCs.

If the RFC passes all the necessary conditions (for example, all required parameters are specified), the status changes to `PendingApproval` (even automated CTs require approval, which happens automatically if syntax and parameter checks pass). If it does not pass, the status changes to

`Rejected`. The `StatusReason` provides information about rejections; the `ExecutionOutput` fields provide information about approval and completion. Error codes include:

- InvalidRfcStateException: The RFC is in a status that doesn't allow the operation that was called. For example, if the RFC has moved to the Submitted state, it can no longer be modified.
- InvalidRfcScheduleException: The StartTime, EndTime, or TimeoutInMinutes parameters were breached.
- InternalServerError: A difficulty with the system was encountered.
- InvalidArgumentException: A parameter is incorrectly specified; for example, an unacceptable value is used.
- ResourceNotFoundException: A value, such as the stack ID, cannot be found.

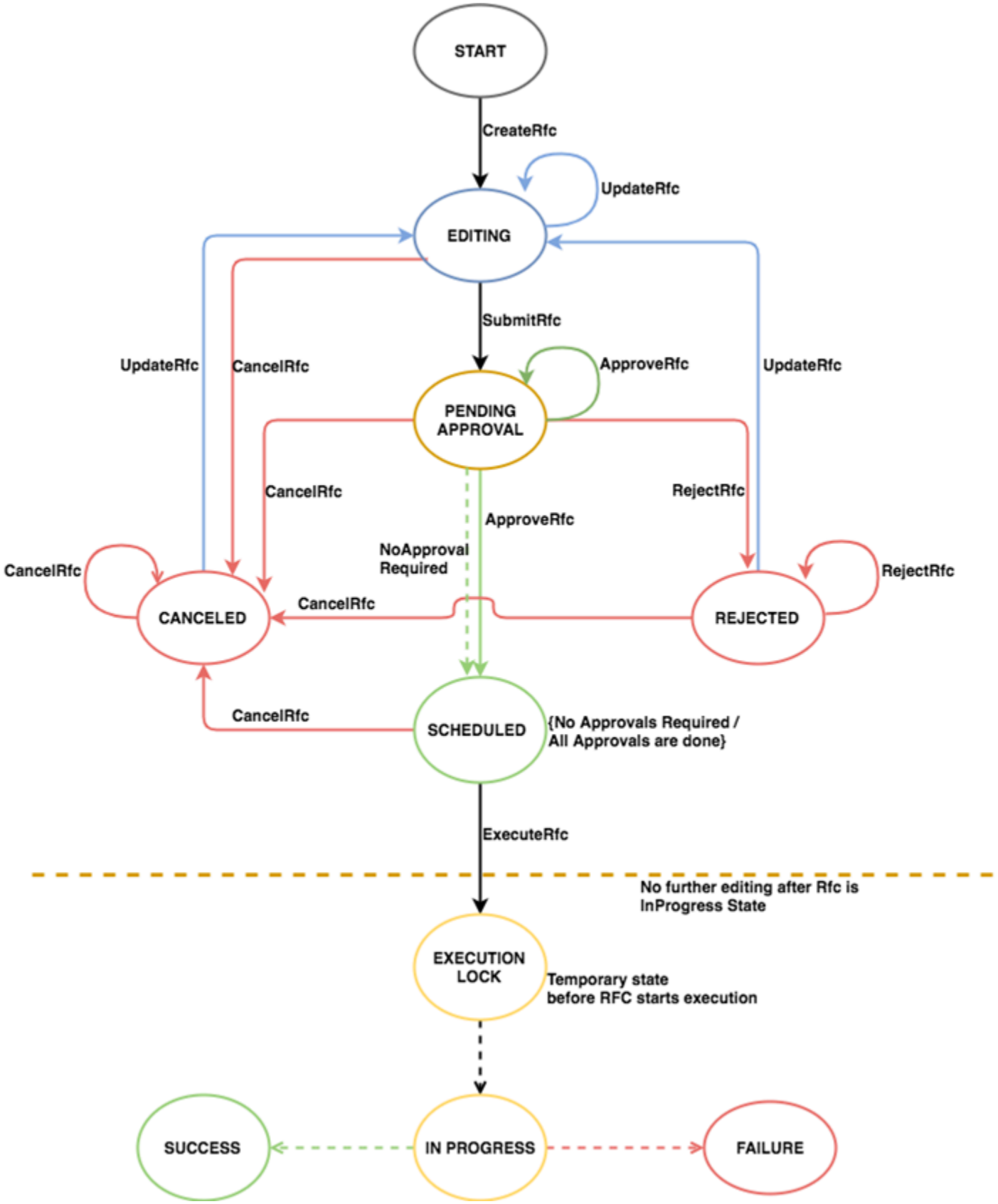
If the scheduled requested start and end times (also known as the change run window) occur before the change is approved, the RFC status changes to `Canceled`. If the change is approved, the RFC status changes to `Scheduled`. The change run window for ASAP RFCs is the submitted time plus the `ExpectedExecutionDuration` value for the CT.

At any time before the arrival of the change run window, a scheduled change (submitted with a `RequestedStartTime` in the CLI) can be modified or canceled. If the scheduled change is modified, it must then be re-submitted.

When the change start time arrives (scheduled or ASAP) and after approvals are complete, the status changes to `InProgress` and no modifications can be made. If the change is completed within the specified change run window, the status changes to `Success`. If any part of the change fails, or if the change is still in progress when the change run window ends, the status changes to `Failure`.

> **Note**
>
> During the `InProgress`, `Success`, or `Failure` change states, the RFC cannot be modified or canceled.

The following diagram illustrates the RFC statuses from the CreateRFC call through to resolution.


START
CreateRfc
UpdateRfc
EDITING
SubmitRfc
UpdateRfc
CancelRfc
ApproveRfc
UpdateRfc
PENDING APPROVAL
CancelRfc
RejectRfc
ApproveRfc
NoApproval Required
CancelRfc
CANCELED
CancelRfc
REJECTED
RejectRfc
CancelRfc
SCHEDULED
{No Approvals Required / All Approvals are done}
ExecuteRfc
No further editing after Rfc is InProgress State
EXECUTION LOCK
Temporary state before RFC starts execution
SUCCESS
IN PROGRESS
FAILURE

## Understand RFC update CTs and CloudFormation template drift detection

Resources provisioned in AMS use a modified AWS CloudFormation template. If a resource has a parameter changed directly through a service's AWS Management Console, then the CloudFormation creation record of that resource becomes out of sync. If this happens and you attempt to use an AMS update change type to update the resource in AMS, then AMS references the original resource configuration and potentially resets changed parameters. This reset might be damaging, so AMS disallows RFCs with update change types if any extra AMS configuration changes are detected.

For a list of update change types, use the console filter.

### Drift remediation FAQs

Questions and answers on AMS drift remediation. There are two change types that you can use to initiate drift remediation, one is execution mode=manual or "review required," the other is execution mode=automated.

### Drift remediation supported resources (ct-3kinq0u4l33zf)

These are the resources that are supported by the drift remediation change type, (ct-3kinq0u4l33zf). For remediation of any resource, use the "review required" (ct-34sxfo53yuzah) change type instead.

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
```

```
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

### Drift remediation change types

Questions and answers on using the AMS drift remediation change types.

For a list of supported resources for the drift remediation feature, see Drift remediation supported resources (ct-3kinq0u4l33zf).

> **Important**
>
> Drift remediation modifies the stack template and/or parameters and it is mandatory to update your local template repositories or any automation that is updating these stacks to use the latest stack template and parameters. Using old template and/or parameters without syncing can cause damaging changes to underlying resources.
> The no review required, automated, CT (ct-3kinq0u4l33zf) supports remediating only 10 resources per RFC. To remediate remaining resources in batches of 10 create new RFCs until all resources are remediated.

Which drift remediation change type should I use?

We recommend using the **no review required**, automated CT (ct-3kinq0u4l33zf) when:

- You attempt to perform an update to an existing stack resource using an automated CT and the RFC gets rejected as the stack is `DRIFTED`.
- You used an Update CT in the past and it failed as the stack was DRIFTED. You do not need to attempt an update again and can use the review required, manual, CT instead.

We recommend using the **review required**, manual CT (ct-34sxfo53yuzah) only when drifted resource types are not supported by the drift remediation no review required, automated, CT (ct-3kinq0u4l33zf), or when the drift remediation no review required, automated, CT fails.

What changes are performed to the stack during remediation?

Remediation requires updates to the stack template and/or parameters depending on the properties that are drifted. Remediation also updates the stack policy of the stack during remediation and restores the stack policy to its previous value once remediation is completed.

How can we see the changes performed to the stack template and/or parameters?

In the response to the RFC, a change summary is provided with the following information:

- `ChangeSummaryJson`: Contains change summary of Stack Template and/or Parameters as part of drift remediation. Remediation is performed in multiple phases. This change summary consists of changes for individual phases. If Remediation is successful check changes of the last phase. See ExecutionPlan in the JSON for phases executed in order. For example, RestoreReferences section when present is always executed at the end and contains JSON for post remediation changes. If remediation is run in DryRun mode none of these changes would have been applied to the stack.
- `PreRemediationStackTemplateAndConfigurationJson`: Contains configuration snapshot of CloudFormation Stack including Template, Parameters, Outputs, StackPolicyBody before remediation was triggered on the stack.

What do I need to do once remediation is performed?

> **Important**
>
> You need to update your local template repositories, or any automation, that would be updating the remediated stack, with the latest template and parameters provided in the RFC summary. It is very important to do this because using the old template and/or parameters can cause further destructive changes on the stack resources.

Will my application be effected during this remediation?

Remediation is an offline process that is performed only on the CloudFormation stack configuration. No updates are performed on the underlying resource.

Can I continue using Management | Other | Other RFCs to perform updates to resources after remediation?

We recommend that you always perform updates to stack resources using the available automated Update CTs. When the available Update CTs do not support your use case, use Management | Other | Other requests.

Does remediation create any new resources in the stack?

Remediation does not create any new resources in the stack. However, remediation creates new outputs and updates the stack template metadata section to store the remediation summary for your reference.

Will remediation always be successful?

Remediation requires careful analysis and validation of the template configuration to determine if it can be performed. In scenarios where these validations fail, the remediation process is stopped and no changes are performed to the stack template or parameters. Also, remediation can only be performed on supported resource types.

How can I perform updates to stack resources if remediation is not successful?

You can use the Management | Other | Other | Update CT (ct-0xdawir96cy7k) to request changes. AMS monitors such scenarios and works towards improving the remediation solution.

Can I remediate stacks that have both supported and unsupported resource types?

Yes. However, remediation is performed only if the supported resource types are found DRIFTED in the stack. If any unsupported resource types are DRIFTED, remediation does not continue.

Can I request remediation for stacks created through non-CFN Ingest CTs?

Yes. Remediation can be performed on stacks irrespective of the change type used for creating the stack.

Can I know the changes that would be performed to the stack before remediation?

Yes. Both change types provide a **DryRun** option that you can use to request changes that would be performed if the stack was remediated. However, the final remediation changes may differ depending on the drift present on the stack at the time of remediation.

## Schedule RFCs

The **Scheduling** feature allows you to choose a start time for RFCs. The following options are available in the **Scheduling** feature:

- **Execute this change ASAP**: AMS runs the RFC as soon as it's approved. Most CTs are automatically approved. Use this option if don't want the RFC to start at a specific time.
- **Schedule this change**: Set a day, time, and time zone for the RFC to run. For automated change types, it's a best practice to request a start time that's at least 10 minutes after you plan to submit the RFC. For review required change types, it's required that you request a start time that's at least 24 hours after you plan to submit the RFC. If the RFC isn't approved by the configured start time, then the RFC is rejected.

### Set an RFC schedule

To schedule an RFC, use one of the following methods:

**Execute this change ASAP**:

- Console: Do nothing. This uses the default RFC schedule.
- API or CLI: Remove the `RequestedStartTime` and `RequestedEndTime` options in the Create RFC operation.

**ASAP** "review required" RFCs are auto-rejected if they are not approved within thirty days of submission.

**Schedule this change**:

- Console: Select the **Schedule this change** radio button. A **Start time** area opens. Manually type in a day or use the calendar widget to pick a day. Enter a time, in UTC, expressed in ISO 8601 format, and use the drop-down list to pick a location. By default, AMS uses the ISO 8601 format YYYYMMDDThhmmssZ or YYYY-MM-DDThh:mm:ssZ, either format is accepted.

> **Note**
>
> The **Default End Time** is 4 hours from the **Start time** that you enter. To set the **End Time** of your scheduled change beyond 4 hours, use the API or CLI to run the change.

- API or CLI: Submit values for the `RequestedStartTime` and `RequestedEndTime` parameters in the Create RFC operation. Passing a configured `RequestedEndTime` doesn't stop the run for an automated change type that has already started. For a "review required" change type, if the `RequestedEndTime` is reached while AMS Operations research is still ongoing, and you're in communication with AMS, then you can request an extension, or you might be asked to re-submit the RFC.

> **Tip**
>
> For an example of a UTC time readout, see UTC on the Time-is website. Example ISO 8601 format for a date/time value of 2016-12-05 at 2:20pm: **2016-12-05T14:20:00Z** or **20161205T142000Z**.

If you provide...

- only a `RequestedStartTime`, the RFC is considered scheduled and the `RequestedEndTime` is populated using the `ExecutionDurationInMinutes` value.
- only a `RequestedEndTime`, we throw an InvalidArgumentException.
- both `RequestedStartTime` and `RequestedEndTime`, we overwrite the `RequestedEndTime` with the specified start time plus the `ExecutionDurationInMinutes` value.
- neither `RequestedStartTime` nor `RequestedEndTime`, we keep those values as null and the RFC is treated as an ASAP RFC.

> **Note**
>
> For all scheduled RFCs, an unspecified end time is written to be the time of the specified `RequestedStartTime` plus the `ExpectedExecutionDurationInMinutes` attribute of the submitted change type. For example, if the `ExpectedExecutionDurationInMinutes` is "60" (minutes), and the specified `RequestedStartTime` is `2016-12-05T14:20:00Z` (December 5, 2016 at 4:20 AM), the actual end time would be set to December 5, 2016 at 5:20 AM. To find the `ExpectedExecutionDurationInMinutes` for a specific change type, run this command:
>
> ```
> aws amscm --profile saml get-change-type-version --
> change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.
> {ExpectedDuration:ExpectedExecutionDurationInMinutes}"
> ```

### Use the RFC Priority option

Use the **Priority** option in `execution mode = manual` change types to alert AMS Operations to the urgency of the request.

**Priority** option in `execution mode = manual`:

Specify the priority of a manual RFC as **High**, **Medium**, or **Low**. RFCs classified as **High** are reviewed and approved prior to RFCs classified as **Medium**, subject to RFC service level objectives (SLOs) and their submission times. RFCs with **Low** priority or no priority specified are processed in the order they are submitted.

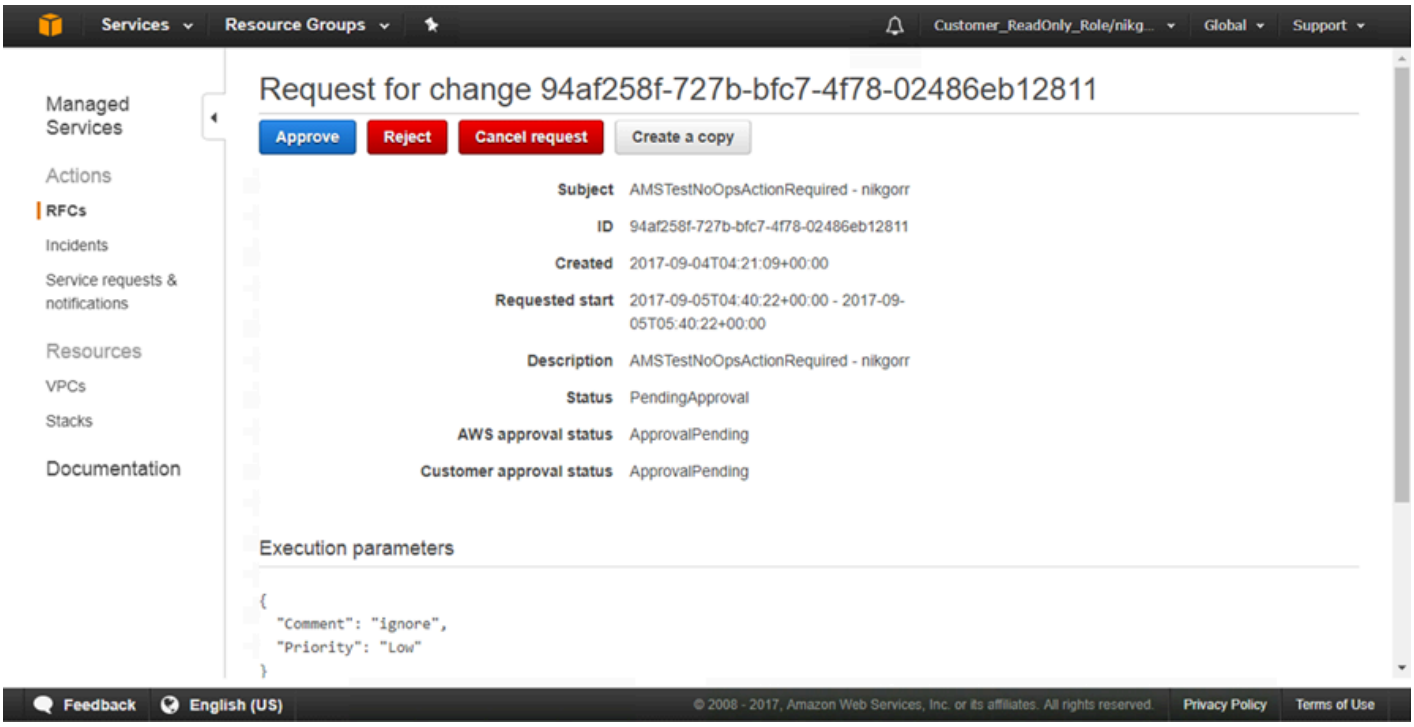
## Approve or reject RFCs

RFCs submitted with approval-required (manual) CTs must be approved by you or AMS. Pre-approved CTs are automatically processed. For more information, see CT approval requirements.

> **Note**
>
> When using "review required" CTs, AMS recommends that you use the ASAP **Scheduling** 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.

If an approval-required RFC is successfully submitted by AMS, then it must be explicitly approved by you. Or, iff you submit an approval-required RFC, then it must be approved by AMS. If you're required to approve an RFC that AMS submitted, then an email or other predetermined communication is sent to you requesting the approval. The communication includes the RFC ID. After the communication is sent, do one of the followings:

- Console Approve or Reject: Use the RFC details page for the relevant RFC:



- API / CLI Approve: ApproveRfc marks a change as approved. The action must be taken by both the owner and operator, if both are required. The following is an example CLI approve command. In the following example, replace RFC_ID with the appropriate RFC ID.

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- API / CLI Reject: RejectRfc marks a change as rejected. The following is an example CLI reject command. In the following example, replace RFC_ID with the appropriate RFC ID.

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

## Request RFC restricted run periods

Formerly known as blackout days, you can request to restrict certain time periods. No changes can be run during those times.

To set a restricted run period, use the UpdateRestrictedExecutionTimes API operation and set a specific time period, in UTC. The period that you specify overrides any previous periods that were specified. If you submit an RFC during the specified restricted run time, submission fails with the error Invalid RFC Schedule. You can specify up to 200 restricted time periods. By default, no restricted period is set. The following is an example request command (with SAML authentication configured):

```
aws amscm  --profile saml update-restricted-execution-times --restricted-execution-
times="[{\"TimeRange\":{\"StartTime\":\"2018-01-01T12:00:00Z\",\"EndTime\":
\"2018-01-01T12:00:01Z\"}}]"
```

You can also view your current RestrictedExecutionTimes setting by running the ListRestrictedExecutionTimes API operation. Example:

```
aws amscm  --profile saml list-restricted-execution-times
```

If you want to submit an RFC during a specified restricted execution time, then add the **RestrictedExecutionTimesOverrideId** with the value of **OverrideRestrictedTimeRanges**, and then submit the RFC as you normally would. It's a best practice to only use this method for a critical or emergency RFC. For more information, see the API reference for SubmitRfc.

## Create, clone, update, find, and cancel RFCs

The following examples walk you through various RFC operations.

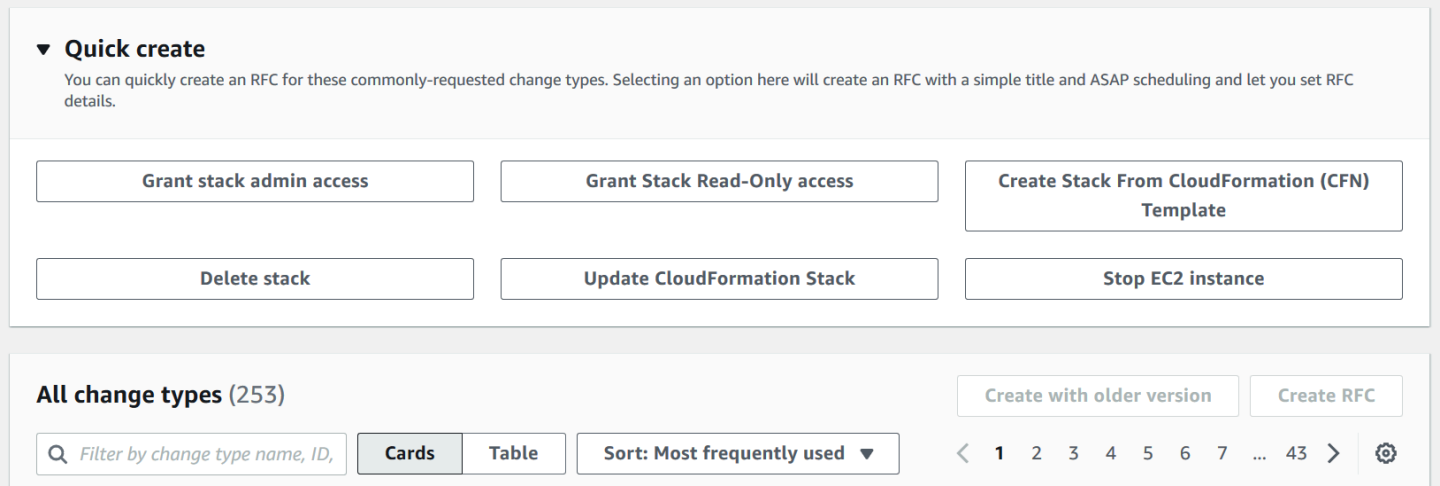
### Topics


- Create an RFC
- Clone RFCs (re-create) with the AMS console
- Update RFCs
- Find RFCs
- Cancel RFCs

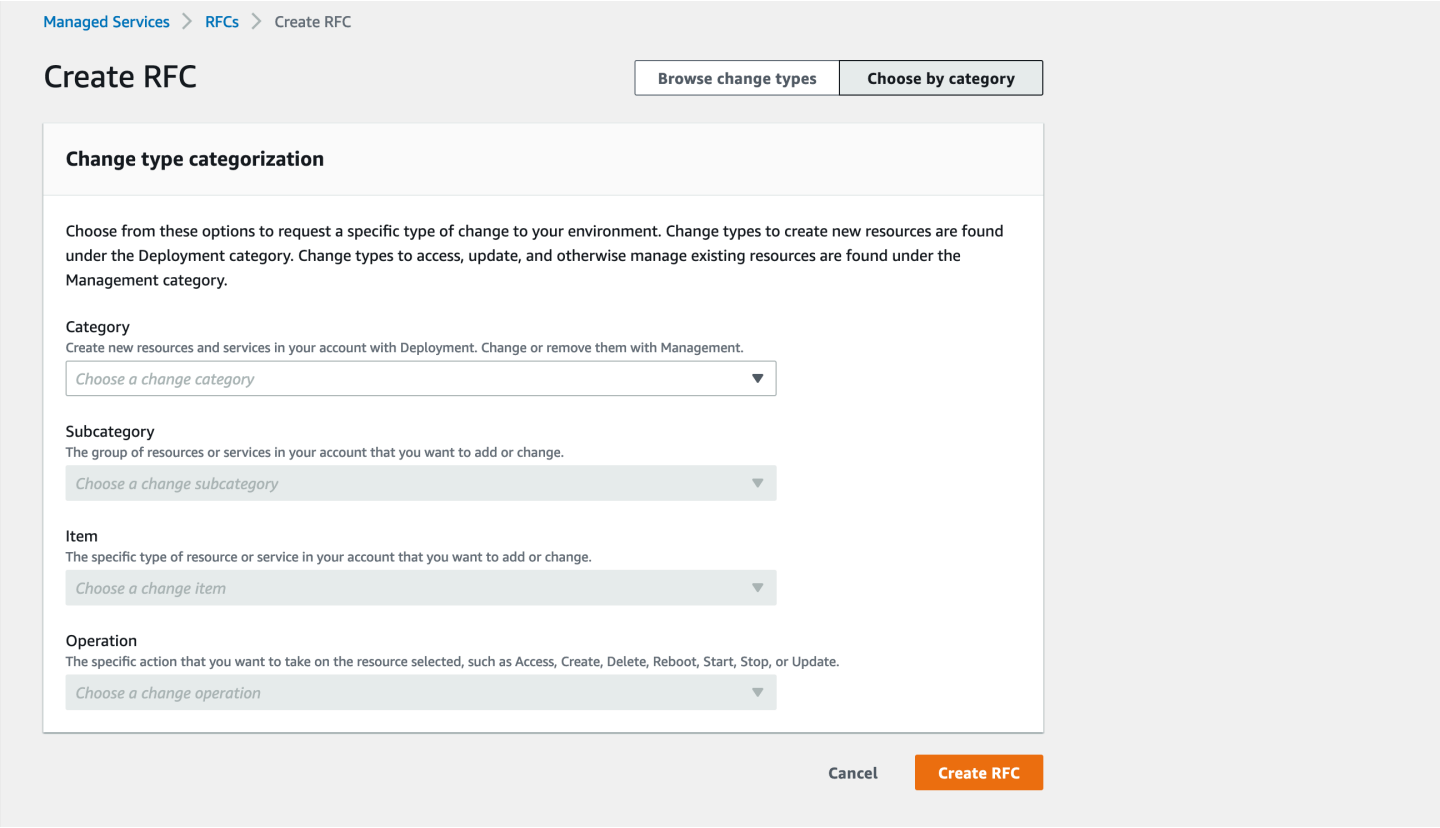

### Create an RFC

#### Creating an RFC with the console

The following is the first page of the RFC Create process in the AMS console, with **Quick cards** open and **Browse change types** active:




The following is the first page of the RFC Create process in the AMS console, with **Select by category** active:




How it works:

1. Navigate to the **Create RFC** page: In the left navigation pane of the AMS console click **RFCs** to open the RFCs list page, and then click **Create RFC**.
2. Choose a popular change type (CT) in the default **Browse change types** view, or select a CT in the **Choose by category** view.
   - **Browse by change type**: You can click on a popular CT in the **Quick create** area to immediately open the **Run RFC** page. Note that you cannot choose an older CT version with quick create.

     To sort CTs, use the **All change types** area in either the **Card** or **Table** view. In either view, select a CT and then click **Create RFC** to open the **Run RFC** page. If applicable, a **Create with older version** option appears next to the **Create RFC** button.
   - **Choose by category**: Select a category, subcategory, item, and operation and the CT details box opens with an option to **Create with older version** if applicable. Click **Create RFC** to open the **Run RFC** page.

3. On the **Run RFC** page, open the CT name area to see the CT details box. A **Subject** is required (this is filled in for you if you choose your CT in the **Browse change types** view). Open the **Additional configuration** area to add information about the RFC.

   In the **Execution configuration** area, use available drop-down lists or enter values for the required parameters. To configure optional execution parameters, open the **Additional configuration** area.
4. When finished, click **Run**. If there are no errors, the **RFC successfully created** page displays with the submitted RFC details, and the initial **Run output**.
5. Open the **Run parameters** area to see the configurations you submitted. Refresh the page to update the RFC execution status. Optionally, cancel the RFC or create a copy of it with the options at the top of the page.

### Creating an RFC with the CLI

How it works:

1. Use either the Inline Create (you issue a `create-rfc` command with all RFC and execution parameters included), or Template Create (you create two JSON files, one for the RFC parameters and one for the execution parameters) and issue the `create-rfc` command with the two files as input. Both methods are described here.
2. Submit the RFC: `aws amscm submit-rfc --rfc-id` *`ID`* command with the returned RFC ID.

   Monitor the RFC: `aws amscm get-rfc --rfc-id` *`ID`* command.

To check the change type version, use this command:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> You can use any `CreateRfc` parameters with any RFC whether or not they are part of the schema for the change type. For example, to get notifications when the RFC status changes, add this line, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` to the RFC parameters part of the request (not

the execution parameters). For a list of all CreateRfc parameters, see the AMS Change Management API Reference.

*INLINE CREATE*:

Issue the create RFC command with execution parameters provided inline (escape quotes when providing execution parameters inline), and then submit the returned RFC ID. For example, you can replace the contents with something like this::

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title
 "TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

*TEMPLATE CREATE*:

> **Note**
>
> This example of creating an RFC uses the Load Balancer (ELB) stack change type.

1. Find the relevant CT. The following command searches CT classification summaries for those that contain "ELB" in the **Item** name and creates output of the Category, Item, Operation, and ChangeTypeID in table form (Subcategory for both is `Advanced stack components`).

   ```
   aws amscm list-change-type-classification-summaries --query
    "ChangeTypeClassificationSummaries[?contains(Item,'ELB')].
   [Category,Item,Operation,ChangeTypeId]" --output table
   ```

   ```
   ----------------------------------------------------------------------
   |                            CtSummaries                             |
   +-----------+---------------------------+---------------------------+
   | Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7jl |
   | Management| Load balancer (ELB) stack | Update | ct-0ltm873rsebx9 |
   +-----------+---------------------------+---------------------------+
   ```

2. Find the most current version of the CT:

   `ChangeTypeId` and `ChangeTypeVersion`: The change type ID for this walkthrough is `ct-123h45t6uz7jl` (create ELB), to find out the latest version, run this command:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
```

3. Learn the options and requirements. The following command outputs the schema to a JSON file named CreateElbParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. Modify and save the execution parameters JSON file. This example names the file CreateElbParams.json.

   For a provisioning CT, the StackTemplateId is included in the schema and must be submitted in the execution parameters.

   For TimeoutInMinutes, how many minutes are allowed for the creation of the stack before the RFC is failed, this setting will not delay the RFC execution, but you must give enough time (for example, don't specify "5"). Valid values are "60" up to "360," for CTs with long-running UserData: Create EC2 and Create ASG. We recommend the max allowed "60" for all other provisioning CTs.

   Provide the ID of the VPC where you want the stack to be created; you can get the VPC ID with the CLI command `aws amsskms list-vpc-summaries`.

```
{
"Description":      "ELB-Create-RFC",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-sdhopv00000000000",
"Name":             "MyElbInstance",
"TimeoutInMinutes": 60,
"Parameters":   {
    "ELBSubnetIds":                      ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold":   4,
    "ELBHealthCheckInterval":           5,
    "ELBHealthCheckTarget":             "HTTP:80/",
    "ELBHealthCheckTimeout":            60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":                        false
    }
}
```

5. Output the RFC JSON template to a file in your current folder named CreateElbRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. Modify and save the CreateElbRfc.json file. Because you created the execution parameters in a separate file, remove the `ExecutionParameters` line. For example, you can replace the contents with something like this:

```
{
"ChangeTypeVersion":    "2.0",
"ChangeTypeId":         "ct-123h45t6uz7jl",
"Title":                "Create ELB"
}
```

7. Create the RFC. The following command specifies the execution parameters file and the RFC template file:

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-
parameters file://CreateElbParams.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.

### Tips

> **Note**
>
> You can use the AMS API/CLI to create an RFC without creating an RFC JSON file or a CT execution parameters JSON file. To do this, you use the `create-rfc` command and add the required RFC and execution parameters to the command, this is called "Inline Create". Note that all provisioning CTs have contained within the `execution-parameters` block a `Parameters` array with the parameters for the resource. The parameters must have quote marks escaped with a back slash (\).
>
> The other documented method of creating an RFC is called "Template Create." This is where you create a JSON file for the RFC parameters and another JSON file for the execution parameters, and submit the two files with the `create-rfc` command. These files can serve as templates and be re-used for future RFCs.

When creating RFCs with templates, you can use a command to create the JSON file with the contents you want by issuing a command as shown. The commands create a file named "parameters.json" with the shown content; you could also use these commands to create the RFC JSON file.

### Clone RFCs (re-create) with the AMS console

You can use the AMS console to clone an existing RFC.

To clone, or recreate, an RFC by using the AMS console, follow these steps:

1. Find the relevant RFC. From the left navigation, click **RFCs**.

   The RFCs dashboard opens.
2. Scroll through the pages until you find the RFC you want to clone. Use the **Filter** option to narrow the list. Choose the RFC that you want to clone.

   The RFC details page opens.
3. Click **Create a Copy**.

   The **Create a request for change** page opens with all options set as in the original RFC.
4. Make the changes you want. To set additional options, change the **Basic** option to **Advanced**. After you have set all options, choose **Submit**.

   The active RFC details page opens with a new RFC ID for the cloned RFC and the cloned RFC appears in the RFC dashboard.

### Update RFCs

You can resubmit an RFC that has been rejected or that has not yet been submitted, by updating the RFC and then submitting it, or re-submitting it. Note that most RFCs are rejected because the specified `RequestedStartTime` has passed before submission or the specified TimeoutInMinutes is inadequate to run the RFC (since TimeoutInMinutes does not prolong a successful RFC, we recommend always setting this to at least "60" and up to "360" for an Amazon EC2 or an Amazon EC2 Auto Scaling group with long-running UserData). This section describes how to use the CLI version of the `UpdateRfc` command to update an RFC with a new RFC parameter, or new parameters using either stringified JSON or an updated parameters file.

This example describes using the CLI version of the AMS UpdateRfc API (see Update RFC). While there are change types for updating some resources (DNS private and public, load balancer stacks, and stack patching configuration), there is no CT to update an RFC.

We recommend that you submit one UpdateRfc operation at a time. If you submit multiple updates, for example on a DNS stack, the updates might fail attempting to update the DNS at the same time.

REQUIRED DATA: `RfcId`: The RFC you're updating.

OPTIONAL DATA: `ExecutionParameters`: Unless you're updating a non-required field, like `Description`, you would submit modified execution parameters to address the issues that caused the RFC to be rejected or canceled. All submitted non-null values overwrite those values in the original RFC.

1. Find the relevant rejected or canceled RFC, you can use this command (you can substitute the value with `Canceled`):

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
```

2. You can modify any of the following RFC parameters :

```
{
    "Description": "string",
    "ExecutionParameters": "string",
    "ExpectedOutcome": "string",
    "ImplementationPlan": "string",
    "RequestedEndTime": "string",
    "RequestedStartTime": "string",
    "RfcId": "string",
    "RollbackPlan": "string",
    "Title": "string",
    "WorstCaseScenario": "string"}
```

Example command updating the Description field:

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
 --region us-east-1
```

Example command updating the ExecutionParameters VpcId field:

```
aws amscm update-rfc  --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id
 "RFC_ID" --region us-east-1
```

Example command updating the RFC with an execution parameters file that contains the updates; see example execution parameters file in step 2 of: EC2 stack | Create:

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --
rfc-id "RFC_ID" --region us-east-1
```

3. Resubmit the RFC using `submit-rfc` and the same RFC ID that you have from when the RFC was first created:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

If the RFC succeeds, you receive no confirmation or error messages at the command line.

4. To monitor the status of the request and to view Execution Output, run the following command.

```
aws amscm get-rfc --rfc-id RFC_ID
```

## Find RFCs

### Find a request for change (RFC) with the console

To find an RFC by using the AMS console, follow these steps.

> **Note**
> This procedure applies only to scheduled RFCs, that is, RFCs that did not use the **ASAP** option.

1. From the left navigation, click **RFCs**.

   The RFCs dashboard opens.

2. Scroll through the list or use the **Filter** option to refine the list.

The RFC list changes per filter criteria.

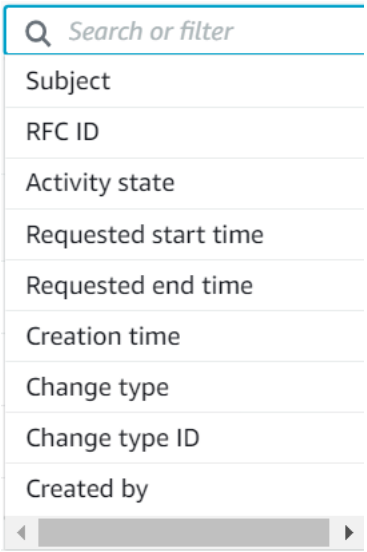
3. Choose the Subject link for the RFC you want.

   The RFC details page opens for that RFC with information including RFC ID.

4. If there are many RFCs in the dashboard, you can use the **Filter** option to search by RFC:

   - **Subject**: The subject line, or title (in the API/CLI) given to the RFC when it was created.
   - **RFC ID**: The identifier for the RFC.
   - **Activity state**: If you know the RFC state, you can choose between **AwsOperatorAssigned** meaning an operator is currently looking at the RFC, **AwsActionPending** meaning that an AMS operator must perform something before the RFC execution can proceed or **CustomerActionPending** meaning that you need to take some action before the RFC execution can proceed.
   - **Status**: If you know the RFC status, you can choose between:
     - **Scheduled**: RFCs that were scheduled.
     - **Canceled**: RFCs that were canceled.
     - **In progress**: RFCs in progress.
     - **Success**: RFCs that executed successfully.
     - **Rejected**: RFCs that were rejected.
     - **Editing**: RFCs that are being edited.
     - **Failure**: RFCs that failed.
     - **Pending approval**: RFCs that cannot proceed until either AMS or you approve. Typically, this indicates that you need to approve the RFC. You will have gotten a service notification of this in your Service Requests list.
   - **Change type**: Pick the **Category**, **Subcategory**, **Item**, and **Operation**, and the change type ID is retrieved for you.
   - **Requested start time** or **Requested end time**: This filter option lets you choose **Before** or **After**, and then enter a **Date** and, optionally, a **Time** (hh:mm and time zone). This filter operates successfully only on scheduled RFCs (not ASAP RFCs).
   - **Status**: Either **Scheduled**, **Canceled**, **In progress**, **Success**, **Rejected**, **Editing**, or **Failure**.
   - **Subject**: The subject (or title, if the RFC was created with the API/CLI) that you gave the RFC.
   - **Change type ID**: Use the identifier for the change type submitted with the RFC.

The search allows you to add the filters, as shown in the following screenshot.




5. Click on the Subject link for the RFC you want.

   The RFC details page opens for that RFC with information including RFC ID.

### Finding a request for change (RFC) with the CLI

You can use multiple filters to find an RFC.

To check the change type version, use this command:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> You can use any `CreateRfc` parameters with any RFC whether or not they are part of the schema for the change type. For example, to get notifications when the RFC status changes, add this line, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` to the RFC parameters part of the request (not the execution parameters). For a list of all CreateRfc parameters, see the AMS Change Management API Reference.

If you don't write down the RFC ID, and need to find it later, you can use the AMS change management (CM) system to search for it and narrow the results with a filter or query.

1. The CM API ListRfcSummaries operation has filters. You can Filter results based on an `Attribute` and `Value` combined in a logical AND operation, or based on an `Attribute`, a `Condition`, and `Values`.

   **RFC filtering**

| Attribute | Valid values | Valid conditions | Default condition | Notes |
|---|---|---|---|---|
| ActualEndTime | Any string representing an ISO8601 datetime (for example, "20170101T000000Z") | Before, After, Between | None | The Before or After condition only accepts one value in the Values field. The Between condition must have exactly two values in the Values field, where the first value should represent a date that happens before the second value |

| Attribute | Valid values | Valid conditions | Default condition | Notes |
|---|---|---|---|---|
| ActualStartTime | Any string representing an ISO8601 datetime (for example, “20170101T000000Z”) | Before, After, Between | None | The Before or After condition only accepts one value in the Values field. The Between condition must have exactly two values in the Values field, where the first value should represent a date that happens before the second value |
| AutomationStatusId | Manual, Automated | Equals | Equals | There are only two automation statuses |
| ChangeTypeId | Any valid change type ID; for example, ct-123h45t6uz7jl | Equals | Equals | Finding a Change Type or CSIO |
| ChangeTypeVersion | Any valid change type ID; for example, 1.0 | Equals | Equals | Finding a Change Type or CSIO |
| CreatedBy | Any string (maximum allowed length is 2048 characters) | Contains | Contains | The CreatedBy field of the RFC contains the ARN of the user who created it |

| Attribute | Valid values | Valid conditions | Default condition | Notes |
|---|---|---|---|---|
| CreatedTime | Any string representing an ISO8601 datetime (for example, “20170101T000000Z”) | Before, After, Between | None | The Before or After condition only accepts one value in the Values field. The Between condition must have exactly two values in the Values field, where the first value should represent a date that happens before the second value |
| LastModifiedTime | Any string representing an ISO8601 datetime (for example, “20170101T000000Z”) | Before, After, Between | None | The Before or After condition only accepts one value in the Values field. The Between condition must have exactly two values in the Values field, where the first value should represent a date that happens before the second value |

| Attribute | Valid values | Valid conditions | Default condition | Notes |
|---|---|---|---|---|
| LastSubmittedTime | Any string representing an ISO8601 datetime (for example, “20170101T000000Z”) | Before, After, Between | None | The Before or After condition only accepts one value in the Values field. The Between condition must have exactly two values in the Values field, where the first value should represent a date that happens before the second value |
| RequestedEndTime | Any string representing an ISO8601 datetime (for example, “20170101T000000Z”) | Before, After, Between | None | The Before or After condition only accepts one value in the Values field. The Between condition must have exactly two values in the Values field, where the first value should represent a date that happens before the second value |

| Attribute | Valid values | Valid conditions | Default condition | Notes |
|---|---|---|---|---|
| RequestedStartTime | Any string representing an ISO8601 datetime (for example, “20170101T000000Z”) | Before, After, Between | None | The Before or After condition only accepts one value in the Values field. The Between condition must have exactly two values in the Values field, where the first value should represent a date that happens before the second value |
| RfcStatusId | Canceled, Editing, Failure, InProgress, PendingApproval, Rejected, Scheduled, Success | Equals | Equals | Refresh the RFC list in the AMS console or run GetRfc |
| Title | Any valid RFC title | Contains | Contains | Regular expressions in each individual field are not supported. Case insensitive search |

Examples:

To find the IDs of all the RFCs related to SQS (where SQS is contained in the Item portion of the CT), you can use this command:

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

Which returns something like this:

```
-----------------------------------------------------------------------------
|                          ListRfcSummaries                                  |
+----------+--------------------------------+-------+-------+----------------+
|Deployment| Advanced Stack Components      |SQS    |Create |ct-123h45t6uz7jl|
|Management| Monitoring & Notification  |SQS    |Update |ct-123h45t6uz7jl|
+----------+--------------------------------+-------+-------+----------------+
```

Another filter available for `list-rfc-summaries` is `AutomationStatusId`, to look for RFCs that are automated or manual:

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

Another filter available for `list-rfc-summaries` is `Title` (**Subject** in the console):

```
 Attribute=Title,Value=RFC-TITLE
```

Example of the new request structure in JSON that returns RFCs where:

- (Title CONTAINS the phrase "Windows 2012" OR "Amazon Linux") AND
- (RfcStatusId EQUALS "Success" OR "InProgress") AND
- (20170101T000000Z <= RequestedStartTime <= 20170103T000000Z) AND (ActualEndTime <= 20170103T000000Z)

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
```

```
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

> **Note**
>
> With more advanced `Filters`, AMS intends to deprecate the following fields in an upcoming release:
>
> - Value: The Value field is part of the Filters field. Use the Values field that supports more advanced functionality.
> - RequestedEndTimeRange: Use the RequestedEndTime inside the Filters field that supports more advanced functionality
> - RequestedStartTimeRange: Use the RequestedStartTime inside the Filters field that supports more advanced functionality.

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're using the AMS console:

   Go to the **RFCs** list page. If needed, you can filter on the RFC **Subject**, which is what you entered as the RFC `Title` when you created it.

### Tips

> **Note**
>
> This procedure applies only to scheduled RFCs, that is, RFCs that did not use the **ASAP** option.

### Cancel RFCs

You can cancel an RFC using the Console or the AMS API/CLI.

To cancel an RFC with the console, find the RFC in your RFC list, open it, click **Cancel**.

Required Data:

- `Reason`: Why you are canceling the RFC.
- `RfcId`: The RFC you are canceling.

1. Typically you would cancel an RFC right after submitting it (so the RFC ID should be handy); otherwise, you would not be able to cancel it unless you scheduled it and it's before the specified start time. If you need to find the RFC ID, you can use this command (you can substitute the `Value` with `PendingApproval` for an RFC that is manually approved):

   ```
   aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
   ```

2. Example command to cancel an RFC:

   ```
   aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --
   region us-east-1
   ```

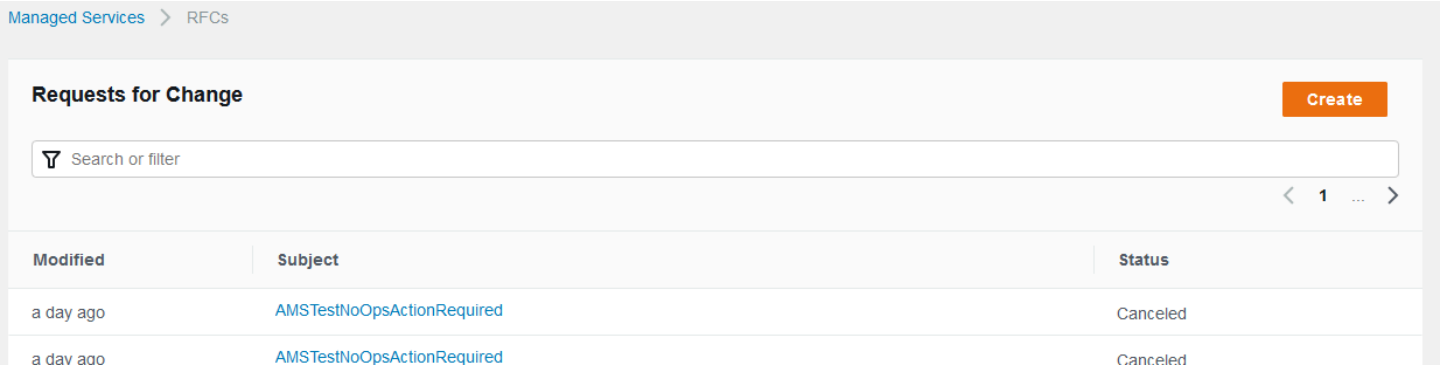
## Use the AMS console with RFCs

The AMS console provides features to help you succeed with creating and submitting RFCs.

### Use the RFC List page (Console)

The AMS console **RFCs** list page provides you with the following options:

- Advanced RFC search through a **Filter**. For information, see Find RFCs.
- Finding the last time the RFC was **Modified**. This value represents that last time that the RFC status was changed.
- Viewing RFC details with the RFC **Subject**. Choosing this link opens the details page for that RFC.
- Viewing RFC status. For information, see Understand RFC status codes




### Use RFC quick create (console)

Use the RFC quick create cards, or list table, or choose change types for RFCs by classification.

To learn more, see Create an RFC.

### Add RFC correspondence and attachments (console)

You can add correspondence to an RFC after it has been submitted and before it is approved; for example, while it's in the state of "PendingApproval". After an RFC is approved (in a state of "Scheduled" or "InProgress"), correspondence cannot be added, because it could be construed as a change to the request. After an RFC is completed (in a state of "Canceled", "Rejected", "Success", or "Failure"), correspondence is once again enabled, though correspondence is disabled once an RFC is closed for more than 30 days.

> **Note**
>
> Each correspondence is limited to 5,000 characters.

**Limitations for attachments:**

- Only three attachments per correspondence.
- Limit fifty attachments per RFC.
- Each attachment must be less than 5 MB in size.
- Only text files are accepted such as plaintext (`.txt`), comma-separated values (`.csv`), JSON (`.json`), or YAML (`.yaml`). In the case of YAML format, the file must be attached using file extension `.yaml`.

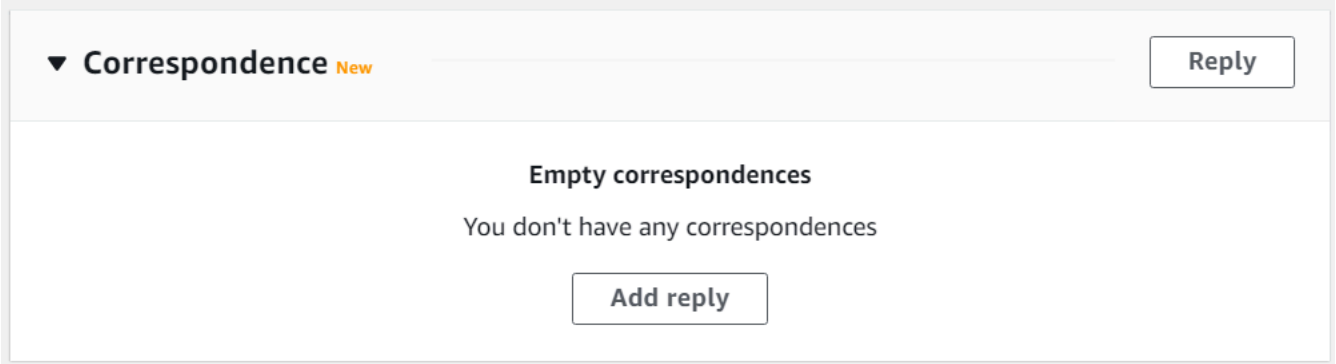
> **Note**
>
> Text files that have XML content are prohibited. If you have XML content to share with AMS, use a service request.

- File names are limited to 255 characters, with only numbers, letters, spaces, dashes (-), underscores (_), and dots (.).
- Updating and deleting attachments on an RFC is not currently supported.

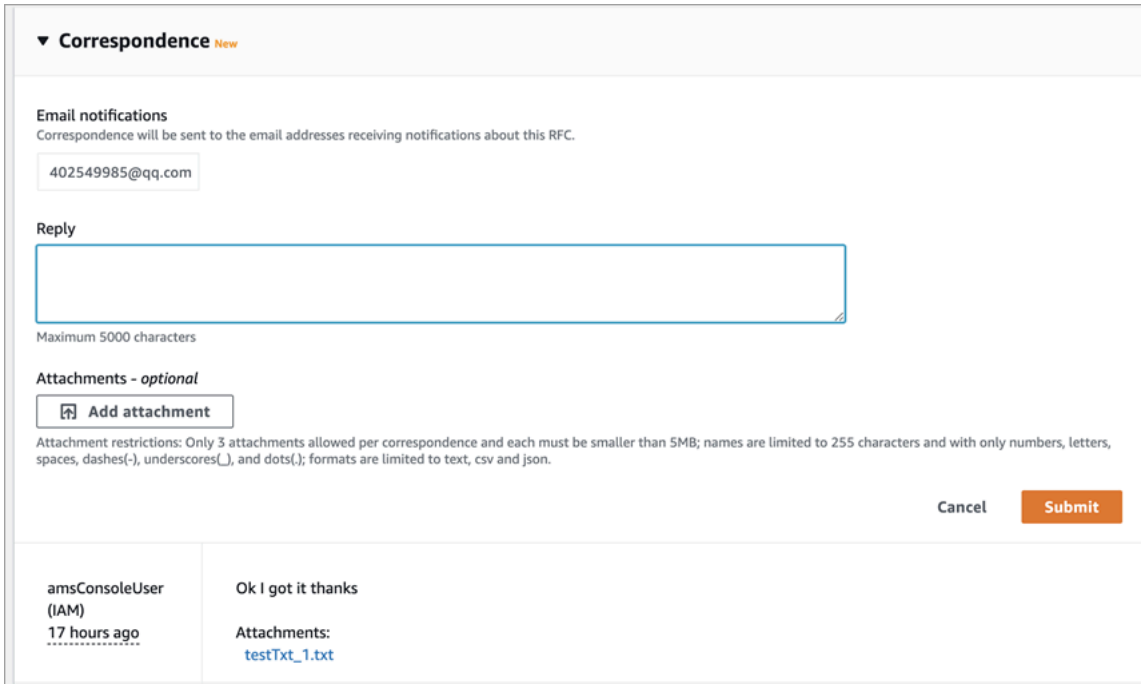
To add correspondence and attachments to an RFC, follow these steps:

1. In the AMS console, on the RFC details page for an RFC, find the **Correspondence** section at the bottom of the page.

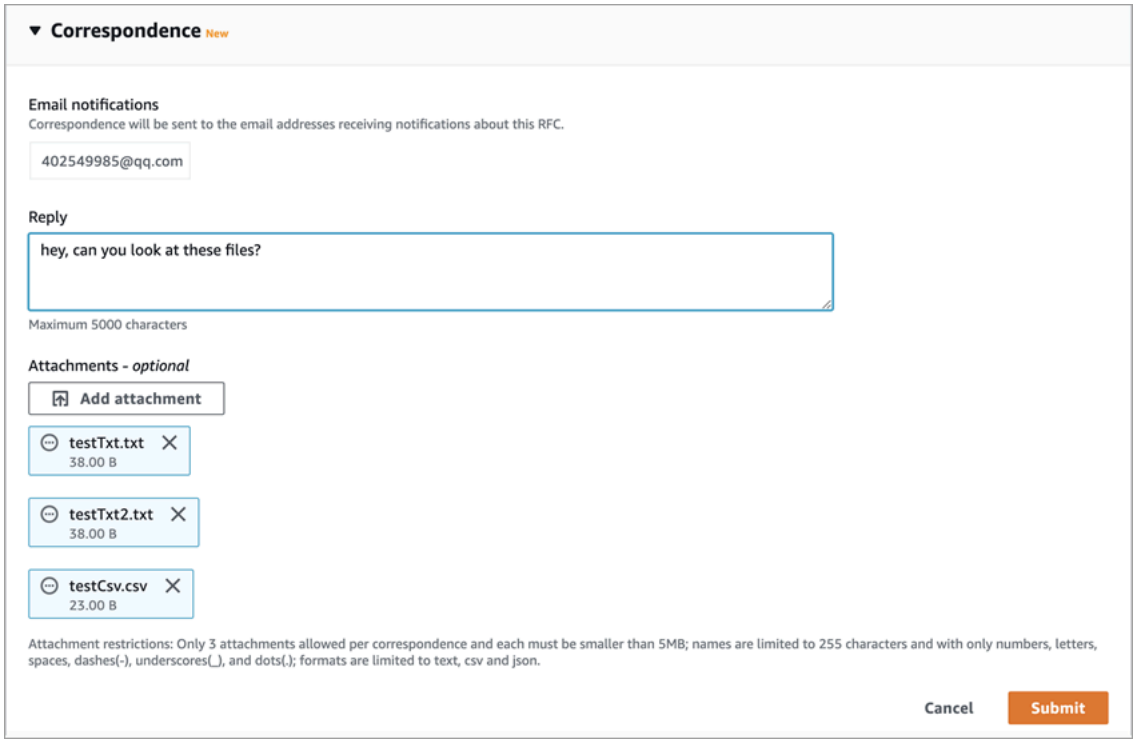
   Before any correspondence:

   After some correspondence:

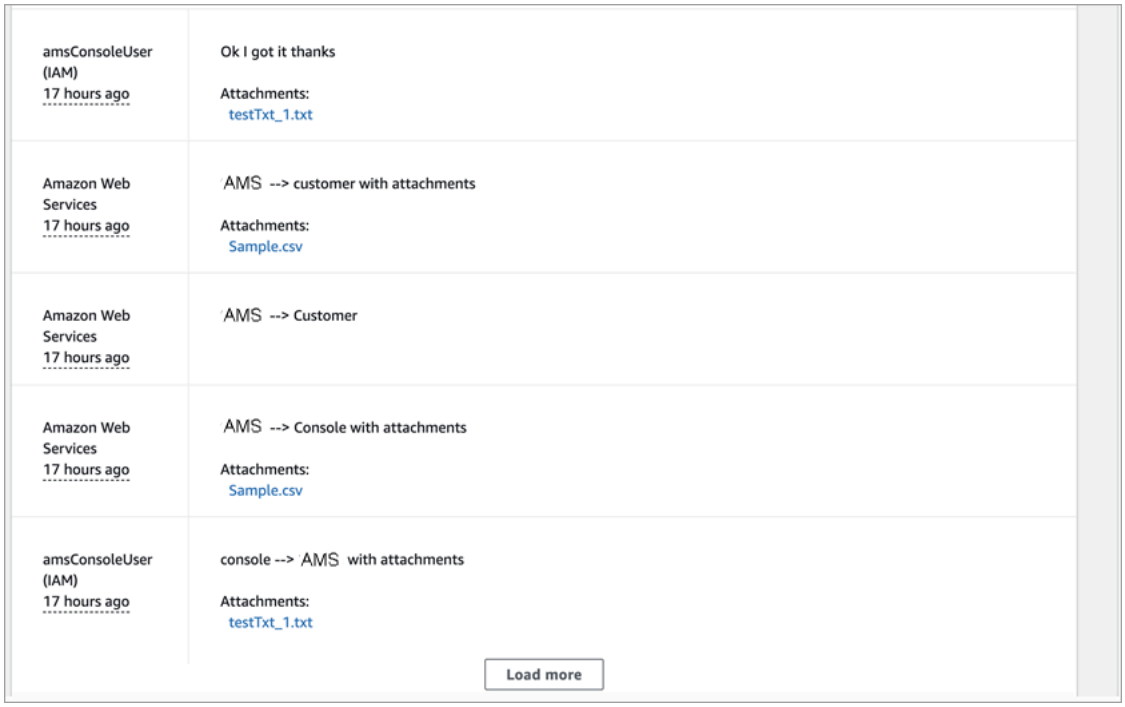



2. To add a new correspondence, type your message in the **Reply** text box. To attach files related to the correspondence, choose **Add Attachment**, and then choose the files you want.



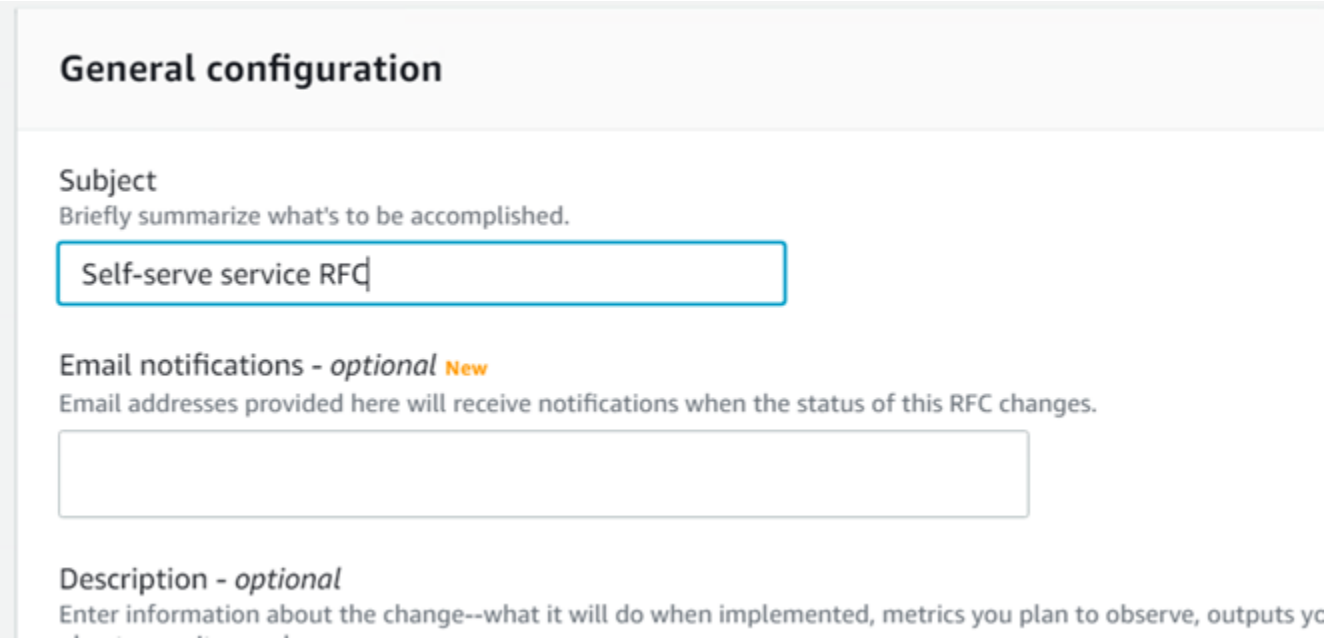

3. When you're finished, choose **Submit**.

   The new correspondence, along with links to the attached files, appear in the correspondence list on the RFC details page.




### Configure RFC email notifications (console)

The AMS console **Requests for Change** create page provides you with an option to add email addresses to receive notifications of RFC state changes:




Additionally, you can add email addresses for notifications to any change type, for example:

```
aws amscm create-rfc --change-type-id ct-1e1xtak34nx76
```

```
                    --change-type-version 1.0 --title "TITLE"
                    --notification "{\"Email\": {\"EmailRecipients\" :
[\"email@example.com\"]}}"
```

Add a similar line (`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`) to any change type inline or template request in the RFC parameters part of the request, not the parameters part.

## Learn about common RFC parameters

The following are RFC parameters that you are required to submit, and parameters that are commonly used in RFCs:

- Change type information: ChangeTypeId and ChangeTypeVersion. Ror a list of change type IDs and version numbers, see Change Type Reference.

  Run `list-change-type-classification-summaries` in the CLI with the `query` argument to narrow the results. For example, narrow results to change types that contain "Access" in the `Item` name.

  ```
  aws amscm list-change-type-classification-summaries --query
   "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
  ```

  Run `get-change-type-version` and specify the change type ID. The following command gets the CT version for ct-2tylseo8rxfsc.

  ```
  aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
  ```

- Title: A name for the RFC; this becomes the **Subject** of the RFC in the AMS console RFC list and you can search on it with the `GetRfc` command and a filter on `Title`
- Scheduling: If you want a scheduled RFC, you must include the `RequestedStartTime` and `RequestedEndTime` parameters, or use the **Schedule this change** console option. For an **ASAP** RFC (that runs as soon as it's approved), when using the CLI, leave `RequestedStartTime` and `RequestedEndTime` null. When using the console, accept the **ASAP** option.

  If the `RequestedStartTime` is missed, the RFC is rejected.
- Provisioning CTs: The execution parameters, or `Parameters` are the specific settings that are required to provision the resource. They vary widely depending on the CT.

- Non-provisioning CTs: CTs that do not provision a resource, such as access CTs or Other | Other, or delete stack, have minimal execution parameters and no `Parameters` block.
- Some RFCs also require that you specify a `TimeoutInMinutes`, or how many minutes are allowed for the creation of the stack before the RFC is failed. Valid values are 60 (minutes) up to 360, for long-running UserData. If the execution can't be completed before the `TimeoutInMinutes` is exceeded, the RFC fails. However, this setting doesn't delay the execution of the RFC.
- RFCs that create instances, such as an S3 bucket or an ELB, generally provide a schema that allows you to add up to seven tags (key/value pairs). You can add more tags to your S3 bucket by submitting an RFC using the Deployment | Advanced stack components | Tag | Create change type (ct-3cx7we852p3af). EC2, EFS, RDS, and the multi-tiered (HA Two-Tiered and HA One-Tiered) schemas allow up to fifty tags. Tags are specified in the `ExecutionParameters` part of the schema. Providing tags can be of great value. For more information, see Tagging Your Amazon EC2 Resources.

  When using the AMS console, you must open the **Additional configuration** area in order to add tags.

  > **Tip**
  >
  > Many CT schemas have a `Description` and `Name` field near the top of the schema. Those fields are used to name the stack or stack component, they don't name the resource you're creating. Some schemas offer a parameter to name the resource you're creating, and some do not. For example, the CT schema for Create EC2 stack doesn't offer a parameter to name the EC2 instance. In order to do so, you must create a tag with the key "Name" and the value of what you want the name to be. If you do not create such a tag, your EC2 instance displays in the EC2 console without a name attribute.

### Use the RFC AWS Region option

The AMS API and CLI (`amscm` and `amsskms`) endpoints are in `us-east-1`. If you federate with Security Assertion Markup Language (SAML), then scripts are provided to you at onboarding that set your AWS Region to us-east-1. If you use SAML, then you don't need to specify the `--region` option when you issue a command. If your SAML is configured to use us-east-1 but your account isn't in that AWS Region, then you must specify your account-onboarded Region when you issue other AWS commands (for example, `aws s3`).

> **Note**
>
> Most of the command examples provided in this guide don't include the `--region` option.

## Sign up for the RFC daily email

You can sign up for a daily email summarizing the RFC activity in your account over the last 24 hours using the RFC digest feature. The RFC digest feature is a streamlined process that reduces the number of email notifications you receive regarding your account's RFCs. The RFC digest might reduce the likelihood that you miss actions that are pending your response.

To turn on the RFC digest feature, contact your AMS Cloud Service Delivery Manager (CSDM). The CSDM subscribes you. You can request up to 20 email addresses (or aliases) to include on your RFC digest email list. The current email schedule is fixed at 09:00 UTC-8.

To turn off the RFC digest feature, contact your CSDM with your request.

If you don't set up RFC digest and want notifications regarding your RFCs, or if you want more detailed information on your RFCs than what the RFC digest provides, then use the Change Management System to set up CloudWatch Events notifications or email notifications for every individual RFC that you want information on. For information on setting up RFC notifications, see RFC State Change Notifications.

The topics contained in the RFC digest include the following:

- Pending Customer Approval: Lists RFCs that are in **PendingApproval** status, awaiting your approval
- Pending Customer Reply: Lists RFCs that are awaiting your reply on RFC correspondence
- Pending AWS Approval or Reply: Lists RFCs that are waiting on AMS for reply or approval
- Completed: Lists RFCs in **Success**, **Failure**, **Cancelled** and **Rejected** status

The following is an example RFC digest:

```
ACCOUNT ID: 123456789012

Total RFCs in this digest: 10
(Some RFCs may be included in more than one category below)

----

PENDING CUSTOMER REPLY - 1

RfcId:12345678-1234-5678-0912-123456789012
Title: Title of the First RFC
Activity State: Pending Customer Reply
Status: Pending AWS Approval
CreationTime: 2020-10-23T15:41:39Z

----

PENDING CUSTOMER APPROVAL - 1

RfcId:12345678-1234-5678-0912-123456789012
Title: Title of the First RFC
Activity State: Pending AWS Reply
Status: Pending Customer Approval
CreationTime: 2020-10-23T15:41:39Z

----

PENDING AWS REPLY OR APPROVAL - 2

RfcId:12345678-1234-5678-0912-123456789012
Title: Title of the First RFC
Activity State: Pending Customer Reply
Status: Pending AWS Approval
CreationTime: 2020-10-23T15:41:39Z

RfcId:12345678-1234-5678-0912-123456789012
Title: Title of the Second RFC
Activity State: Pending AWS Reply
Status: Pending Customer Approval
CreationTime: 2020-10-23T15:41:39Z

----

COMPLETED - 8

RfcId:12345678-1234-5678-0912-123456789012
Title: Title of the First RFC
Activity State: NoActionPending
Status: Success
LastUpdatedTime: 2020-10-23T15:41:39Z

RfcId:98765432-1098-7654-3210-987654321098
```

# What are change types?

Change type refers to the action that an AWS Managed Services (AMS) request for change (RFC) performs and encompasses the change action itself, and the type of change – manual vs automated. AMS has a large collection of change types not used by other Amazon web services. You use these change types when submitting a request for change (RFC) to deploy, or manage, or gain access to, resources.

**Topics**


- Automated and manual CTs
- CT approval requirements
- Change type versions
- Create change types
- Update change types
- Internal-only change types
- Change type schemas
- Managing permissions for change types
- Redacting sensitive information from change types
- Finding a change type, using the query option


## Automated and manual CTs

A constraint on change types is whether they are automated or manual, this is the change type `AutomationStatusId` attribute, called the **Execution mode** in the AMS console.

Automated change types have expected results and execution times and run through the AMS automated system, generally within an hour or less (this largely depends on what resources the CT is provisioning). Manual change types are uncommon, but they are treated differently because they require that an AMS operator act on the RFC before it can be run. That sometimes means communicating with the RFC submitter, so, manual change types require varying lengths of time to complete.

For all scheduled RFCs, an unspecified end time is written to be the time of the specified `RequestedStartTime` plus the `ExpectedExecutionDurationInMinutes` attribute of the submitted change type. For example, if the `ExpectedExecutionDurationInMinutes` is "60" (minutes), and the specified `RequestedStartTime` is `2016-12-05T14:20:00Z` (December

5, 2016 at 4:20 AM), the actual end time would be set to December 5, 2016 at 5:20 AM. To find the `ExpectedExecutionDurationInMinutes` for a specific change type, run this command:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

> **Note**
>
> Scheduled RFCs with **Execution mode**= Manual, in the Console, must be set to run at least 24 hours in the future. This caveat does not apply to the AMS API/CLI, but it is still important to schedule manual RFCs at least 8 hours ahead.

> **Note**
>
> When using "review required" CTs, AMS recommends that you use the ASAP **Scheduling** 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.

AMS aims to respond to a manual CT within four hours, and will correspond as soon as possible, but it could take much longer for the RFC to actually be run.

For a list of the CTs that are Manual and require AMS review, see the Change Type CSV file, available on the **Developer's Resources** page of the Console.

**YouTube Video**: How can I find automated change types for AMS RFCs?

To find the **Execution mode** for a CT in the AMS console, you must use the **Browse change types** search option. The results show the execution mode of the matching change type or change types.

To find the `AutomationStatus` for a specific change type by using the AMS CLI, run this command:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

You can also look up change types in the AMS Change Type Reference, which provides information about all AMS change types.

> **Note**
>
> The AMS API/CLI are not currently part of the AWS API/CLI. To access the AMS API/CLI, you download the AMS SDK through the AMS console.

## CT approval requirements

AMS CTs always have two approval conditions, **AwsApprovalId** and **CustomerApprovalId** that indicate whether the RFC requires AMS or you, or anyone, to approve the execution.

The approval condition is somewhat related to the execution mode; for details, see Automated and manual CTs.

To find out the approval condition for a CT, you can look in the AMS Change Type Reference, or run GetChangeTypeVersion. Both will also give you the CT `AutomationStatusId` or **Execution mode**.

You can approve RFCs by using the AMS console or with the following command:

```
aws amscm approve-rfc --rfc-id RFC_ID
```

### CT approval condition

| If the CT approval condition is | It requires approval from | And |
|---|---|---|
| `AwsApprovalId: Required` | The AMS change type system, | No action is required. This condition is typical for automated CTs. |
| `AwsApprovalId: NotRequiredIfSubmitter` | The AMS change type system and no one else, if the submitted RFC is for the | No action is required. This condition is typical for manual CTs because they will always be reviewed by AMS operators. |

| If the CT approval condition is | It requires approval from | And |
|---|---|---|
| | account it was submitted against, | |
| `CustomerApprovalId: NotRequired` | The AMS change type system, | If the RFC passes syntax and parameter checks, it is auto approved. |
| `CustomerApprovalId: Required` | The AMS change type system and you, | A notification is sent to you, and you must explicitly approve the RFC, either by responding to the notice, or running the ApproveRfc operation. |
| `CustomerApprovalId: NotRequiredIfSubmitter` | The AMS change type system and no one else, if you submitted the RFC. | If the RFC passes syntax and parameter checks, it is auto approved. |
| Urgent Security Incident or Patch | AMS | Is auto approved and implemented. |

## Change type versions

Change types are versioned and the version changes when a major update is made to the change type.

After selecting a change type using the AMS console, you have the option of opening the **Additional configuration** area and selecting a change type version. You can also specify a change type version at the API/CLI command line. You might want to do this for various reasons, including:

- You know that the version of the **Update** change type that you want must match the version of the **Create** change type that you used to create the resource that you now want to update. For example, you might have an Elastic Load Balancer (ELB) instance that you created with ELB Create change type version 1. To update it, choose ELB Update version 1.

- You want to use a change type version that has different options in it than the most recent change type. We don't recommend this because AMS updates change types mainly for security reasons and we recommend that you always choose the most recent version.

## Create change types

Create change types are matched version-to-version with the Update change types. That is, the change type version that you use to provision a resource must match the version of the Update change type that you would use later to modify that resource. For example, if you create an S3 bucket with the Create S3 Bucket change type version 2.0, and later want to submit an RFC to modify that S3 bucket, you must use the Update S3 Bucket change type version 2.0 as well, even if there is an Update S3 Bucket change type with version 3.0.

We recommend keeping a record of the change type ID and version that you use when provisioning a resource with a Create change type in case you later want to use an Update change type to modify it.

## Update change types

AMS provides Update change types to update resources that were created with Create change types. The Update change types must be matched version-to-version with the Create change type originally used to provision the resource.

We recommend keeping a record of the change type ID and version that you use when provisioning a resource to make it easy to update it.

**YouTube Video**: How do I use update CTs to change resources in an AWS Managed Services (AMS) account?

## Internal-only change types

You can see change types that are for internal use only. This is so you know what actions AMS can, or does, take. If there is an internal-only change type that you would like to have available for your use, submit a service request.

For example, there is a Management | Monitoring and notification | CloudWatch alarm suppression | Update CT that is internal-only. AMS uses it to deploy infrastructure updates (such as patching) to turn off alarm notifications that the updates might erroneously trigger. When this CT is submitted, you will notice the RFC for the CT in your RFC list. Any internal-only CT that is deployed in an RFC appears in your RFC list.

## Change type schemas

All change types provide a JSON schema for your input in the creation, modification, or access, of resources. The schema provides the parameters, and their descriptions, for you to create a request for change (RFC).

The successful execution of an RFC results in execution output. For provisioning RFCs, the execution output includes a "stack_id" that represents the stack in CloudFormation and can be searched in the CloudFormation console. The execution output sometimes includes output of the ID of the instance created and that ID can be used to search for the instance in the corresponding AWS console. For example, the Create ELB CT execution output includes a "stack_id" that is searchable in CloudFormation and outputs a key=ELB value=<stack-xxxx> that is searchable in the Amazon EC2 console for Elastic Load Balancing.

Let's examine a CT schema. This is the schema for CodeDeploy Application Create, a fairly small schema. Some schemas have very large `Parameter` areas.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
  resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
 vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv00000000000",
      "type": "string",
      "enum": ["stm-sft6rv00000000000"]
```

The first part of the schema provides information to AMS about the requested change type.

```
    },
    "Name":{
      "description": "A name for the stack or stack component
;
      this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
      "description": "Up to seven tags (key/value pairs) to
      categorize the resource.",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "Key": {
            "type": "string",
            "minLength": 1,
            "maxLength": 127
          },
          "Value": {
            "type": "string",
            "minLength": 1,
            "maxLength": 255
          }
        },
        "additionalProperties": false,
        "required": [
          "Key",
          "Value"
        ]
      },
      "minItems": 1,
      "maxItems": 7
    },
    "TimeoutInMinutes": {
      "description": "The maximum amount of time, in minutes,
to
      allow for execution of the change. This will not prolong
execution,
      but the RFC fails if the change is not completed in the
specified time.
```

The TimeoutIn Minutes parameter allows you to indicate a boundary time for running the change type. Valid values are 60 up to 360, for long-running UserData.

The Parameters section is where you specify settings for the resource you are creating, or the action you are requesting.

```
      Valid values are 60 up to 360, for long-running
 UserData.",
      "type": "number",
      "minimum": 0,
      "maximum": 60
    },
    "Parameters": {
      "description": "Specifications for the stack.",
      "type": "object",
      "properties": {
        "CodeDeployApplicationName": {
          "description": "The name of an AWS CodeDeploy
 application.",
          "type": "string",
          "minLength": 1,
          "maxLength": 100,
          "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
        }
      },
      "additionalProperties": false,
      "required": [
        "CodeDeployApplicationName"
      ]
    }
  },
  "additionalProperties": false,
  "required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
  ]
}
```

The "additional properties" sections let you know what parameters are required and which are optional.

**Note**

This schema allows up to seven tags; however, EC2, EFS, RDS, and the multi-tier create schemas allow up to 50 tags.

## Managing permissions for change types

You can use a custom policy to restrict which change types (CTs) are available to different groups or users.

To learn more about doing this, see the AMS User Guide section Setting Permissions.

## Redacting sensitive information from change types

AMS change type schemas offer a parameter attribute, `"metadata":"ams:sensitive":"true"` that is used for parameters that would contain sensitive information, such as a password. When this attribute is set, the input provided is obscured. Note that you cannot set this parameter attribute; however, if you are working with AMS to create a change type and have a parameter that you would like obscured at input, you can request this.

## Finding a change type, using the query option

This example demonstrates how to use the AMS Console to find the appropriate change type for the RFC that you want to submit.

You can use the console or the API/CLI to find a change type ID (CT) or version. There are two methods, either a search or choosing the classification. For both selection types, You can sort the search by choosing either **Most frequently used**, **Most recently used**, or **Alphabetical**.

**YouTube Video**: How do I create an RFC using the AWS Managed Services CLI and where can I find the CT Schema?

In the AMS console, on the **RFCs** -> **Create RFC** page:

- With **Browse by change type** selected (the default), either:
  - Use the **Quick create** area to select from AMS's most popular CTs. Click on a label and the **Run RFC** page opens with the **Subject** option auto-filled for you. Complete the remaining options as needed and click **Run** to submit the RFC.
  - Or, scroll down to the **All change types** area and start typing a CT name in the option box, you don't have to have the exact or full change type name. You can also search for a CT by change type ID, classification, or execution mode (automated or manual) by entering the relevant words.

With the default **Cards** view selected, matching CT cards appear as you type, select a card and click **Create RFC**. With the **Table** view selected, choose the relevant CT and click **Create RFC**. Both methods open the **Run RFC** page.

- Alternatively, and to explore change type choices, click **Choose by category** at the top of the page to open a series of drop-down option boxes.
- Choose **Category**, a **Subcategory**, an **Item**, and an **Operation**. The information box for that change type appears a panel appears at the bottom of the page.
- When you're ready, press **Enter**, and a list of matching change types appears.
- Choose a change type from the list. The information box for that change type appears at the bottom of the page.
- After you have the correct change type, choose **Create RFC**.

> **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. You may need to add a `--profile` option for authentication; for example, `aws amsskms` *`ams-cli-command`* `--profile SAML`. You may also need to add the `--region` option as all AMS commands run out of us-east-1; for example `aws amscm` *`ams-cli-command`* `--region=us-east-1`.

> **Note**
>
> The AMS API/CLI (amscm and amsskms) endpoints are in the AWS N. Virginia Region, `us-east-1`. Depending on how your authentication is set, and what AWS Region your account and resources are in, you may need to add `--region us-east-1` when issuing commands. You may also need to add `--profile saml`, if that is your authentication method.

To search for a change type using the AMS CM API (see ListChangeTypeClassificationSummaries) or CLI:

You can use a filter or query to search. The ListChangeTypeClassificationSummaries operation has Filters options for `Category`, `Subcategory`, `Item`, and `Operation`, but the values must match the existing values exactly. For more flexible results when using the CLI, you can use the `--query` option.

**Change type filtering with the AMS CM API/CLI**

| Attribute | Valid values | Valid/Default condition | Notes |
|---|---|---|---|
| ChangeTypeId | Any string representing a ChangeTypeId (For ex: ct-abc123xyz7890) | Equals | For change type IDs, see the Change Type Reference.<br><br>For change type IDs, see Finding a Change Type or CSIO. |
| Category | Any free-form text | Contains | Regular expressions in each individual field are not supported. Case insensitive search |
| Subcategory | | | |
| Item | | | |
| Operation | | | |

1. Here are some examples of listing change type classifications:

   The following command lists all change type categories.

   ```
   aws amscm list-change-type-categories
   ```

   The following command lists the subcategories belonging to a specified category.

   ```
   aws amscm list-change-type-subcategories --category CATEGORY
   ```

   The following command lists the items belonging to a specified category and subcategory.

   ```
   aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
   ```

2. Here are some examples of searching for change types with CLI queries:

   The following command searches CT classification summaries for those that contain "S3" in the Item name and creates output of the category, subcategory, item, operation, and change type ID in table form.

```
aws amscm list-change-type-classification-summaries --query
 "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-------------------------------------------------------------+
|               ListChangeTypeClassificationSummaries          |
+----------+-------------------------+--+------+---------------+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+----------+-------------------------+--+------+---------------+
```

3. You can then use the change type ID to get the CT schema and examine the parameters. The following command outputs the schema to a JSON file named CreateS3Params.schema.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3Params.schema.json
```

   For information about using CLI queries, see How to Filter the Output with the --query Option and the query language reference, JMESPath Specification.

4. After you have the change type ID, we recommend verifying the version for the change type to make sure it's the latest version. Use this command to find the version for a specified change type:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

   To find the `AutomationStatus` for a specific change type, run this command:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

   To find the `ExpectedExecutionDurationInMinutes` for a specific change type, run this command:

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h
 --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

## Troubleshooting RFC errors in AMS

Many AMS provisioning RFC failures can be investigated through the CloudFormation documentation. See Troubleshooting AWS CloudFormation: Troubleshooting Errors

Additional troubleshooting suggestions are provided in the following sections.

### "Management" RFC errors in AMS

AMS "Management" Category change types (CTs) allow you to request access to resources as well as manage existing resources. This section describes some common issues.

#### RFC access errors

- Make sure the Username and FQDN you specified in the RFC are correct and exist in the domain. For help finding your FQDN, see Finding your FQDN.
- Make sure the stack ID you specified for access is an EC2-related stack. Stacks such as ELB and Amazon Simple Storage Service (S3) are not candidates for access RFCs, instead, use your read only access role to get access these stacks resources. For help finding a stack ID, see Finding stack IDs
- Make sure the stack ID you provided is correct and belongs to the relevant account.

For help with other access RFC failures, see Access management.

**YouTube Video**: How do I raise a Request for Change (RFC) properly to avoid rejections and failures?

#### RFC (manual) CT scheduling errors

Most change types are ExecutionMode=Automated, but some are ExecutionMode=Manual and that affects how you should schedule them to avoid RFC failure.

Scheduled RFCs with ExecutionMode=Manual, must be set to execute at least 24 hours in the future if you are using the AMS Console to create the RFC. This caveat does not apply to the AMS API/CLI, but it is still important to schedule Manual RFCs at least 8 hours ahead.

AMS aims to respond to a manual CT within four hours, and will correspond as soon as possible, but it could take much longer for the RFC to actually be executed.

**Using RFCs with manual update CTs**

AMS Operations reject Management | Other | Other RFCs for updates to stacks, when there is an Update change type for the type of stack that you want to update.

**RFC delete stack errors**

RFC delete stack failures: If you use the Management | Standard stacks | Stack | Delete CT, you will see the detailed events in the AWS CloudFormation Console for the stack with the AMS stack name. You can identify your stack by checking it against the name it has in the AMS Console. The AWS CloudFormation Console provides more details about failure causes.

Before deleting a stack, you should consider how the stack was created. If you created the stack using an AMS CT and did not add or edit the stack resources, then you can expect to delete it without issue. However, it is a good idea for you remove any manually-added resources from a stack before submitting a delete stack RFC against it. For example, if you create a stack using the full stack CT (HA Two Tier), it includes a security group - SG1. If you then use AMS to create another security group - SG2, and reference the new SG2 in the SG1 created as part of the full stack, and then use the delete stack CT to delete the stack, the SG1 will not delete as it is referenced by SG2.

> **Important**
>
> Deleting stacks can have unwanted and unanticipated consequences. AMS prefers to *not* delete stacks or stack resources on behalf of customers for this reason. Note, that AMS will only delete resources on your behalf (through a submitted Mangement | Other | Other | Update change type) that are not possible to delete using the appropriate, automated, change type to delete. Additional considerations:
>
> - If the resources are enabled for 'delete protection', AMS can help to unblock this if you submit a Management | Other | Other | Update change type and, after the deletion protection is removed, you can use the automated CT to delete that resource.
> - If there are multiple resources in a stack, and you want to delete only a subset of the stack resources, use the CloudFormation Update change type (see CloudFormation Ingest Stack: Updating). You can also submit a Management | Other | Other | Update change type and AMS engineers can help you craft the changeset, if needed.

- If there are issues using the CloudFormation Update CT due to drifts, AMS can help if you submit a Management | Other | Other | Update to resolve the drift (as far as supported by the AWS CloudFormation Service) and provide a ChangeSet that you can then validate and execute using the automated CT, Management/Custom Stack/Stack From CloudFormation Template/Approve Changeset and Update.

AMS maintains the above restrictions to help ensure there are no unexpected or unanticipated resource deletions.

For more information, see Troubleshooting AWS CloudFormation: delete stack fails.

**RFC update DNS errors**

Multiple RFCs to update a DNS hosted zone can fail, some without reason. Creating multiple RFCs at the same time to update DNS hosted zones (private or public) can cause some RFCs to fail because they are trying to update the same stack at the same time. AMS change management rejects or fails RFCs that are not able to update a stack because the stack is already being updated by another RFC. AMS recommends that you create one RFC at a time and wait for the RFC to succeed before raising a new one for the same stack.

**RFC IAM entities errors**

AMS provisions a number of default IAM roles and profiles into AMS accounts that are designed to meet your needs. However, you may need to request additional IAM resources occasionally.

The process for submitting RFCs requesting custom IAM resources follows the standard workflow for manual RFCs, but the approval process also includes a security review to ensure appropriate security controls are in place. Therefore, the process typically takes longer than other manual RFCs. To reduce the cycle time on these RFCs, please follow the following guidelines.

For information on what we mean by an IAM review and how it maps to our Technical Standards and Risk Acceptance process, see Understand RFC security reviews.

Common IAM resources requests:

- If you are asking for a policy pertaining to a major cloud-compatible application, such as CloudEndure, see the AMS pre-approved IAM CloudEndure policy: Unpack the WIGs Cloud Endure Landing Zone Example file and open the `customer_cloud_endure_policy.json`

> **Note**
>
> If you want a more permissive policy, discuss your needs with your CloudArchitect/CSDM and obtain, if needed, an AMS Security Review and Signoff before submitting an RFC implementing the policy.

- If you want to modify a resource deployed by AMS in your account by default, we recommend that you ask for a modified copy of that resource instead of changes to the existing one.
- If you are requesting permissions for a human user (instead of attaching the permissions to the user) attach the permissions to a role, and then grant the user permission to assume that role. For details on doing this, see Temporary AMS Advanced console access.
- If you require exceptional permissions for a temporary migration or workflow, provide an end date for those permissions in your request.
- If you've already discussed the subject of your request with your security team, provide evidence of their approval to your CSDM with as much detail as possible.

If AMS rejects an IAM RFC we provide a clear reason for the rejection. For example, we might reject an IAM policy create request and explain what about the policy is inappropriate. In that case, you can make the identified changes and resubmit the request. If additional clarity on the status of a request is required, submit a service request, or contact your CSDM.

The following list describes the typical risks that AMS tries to mitigate as we review your IAM RFCs. If your IAM RFC has any of these risks, it may result in the rejection of the RFC. In cases where you require an exception, AMS asks for approvals from your security team. To seek such an exception, coordinate with your CSDM.

> **Note**
>
> AMS may, for any reason, decline any change to IAM resources inside of an account. For concerns regarding any RFC rejection, reach out to AMS Operations via a service request, or contact your CSDM.

- Privilege escalation, such as permissions that allow you to modify your own permissions, or to modify the permissions of other resources inside the account. Examples:
  - The use of `iam:PassRole` with another, more privileged role.

  - Permission to attach/detach IAM policies from a role or user.
  - The modification of IAM policies in the account.
  - The ability to make API calls in the context of management infrastructure.
- Permissions to modify resources or applications that are required to provide AMS services to you. Examples:
  - Modification of AMS infrastructure like the bastions, management host, or EPS infrastructure.
  - Deletion of log management AWS Lambda functions, or log streams.
  - The deletion or modification of the default CloudTrail monitoring application.
  - The modification of the Directory Services Active Directory (AD).
  - Disabling CloudWatch (CW) alarms.
  - The modification of the principals, policies, and namespaces deployed in the account as a part of the landing zone.
- Deployment of infrastructure outside of best practices, such as permissions that allow the creation of infrastructure in a state that endangers your information security. Examples:
  - The creation of public, or unencrypted, S3 buckets or public sharing of EBS volumes.
  - The provisioning of public IP addresses.
  - The modification of security groups to allow broad access.
- Overly broad permissions capable of causing application impact, such as permissions that can result in data loss, integrity loss, inappropriate configuration, or interruptions of service for your infrastructure and the applications inside the account. Examples:
  - Disabling, or redirecting, network traffic through APIs like `ModifyNetworkInterfaceAttribute` or `UpdateRouteTable`.
  - The disabling of managed infrastructure by detaching volumes from managed hosts.
- Permissions for services not a part of the AMS service description and not supported by AMS.

  Services not listed in the AMS Service description cannot be used in AMS accounts. To request support for a feature or service, please reach out to your CSDM.
- Permissions that do not meet your stated goal as they are either too generous, or too conservative, or are applied to the wrong resources. Examples:
  - A request for `s3:PutObject` permissions to an S3 bucket that has mandatory KMS encryption, without `KMS:Encrypt` permissions to the relevant key.
  - Permissions that pertain to resources that don't exist in the account.

- IAM RFCs where the description of the RFC does not seem to match the request.

## "Deployment" RFC errors

AMS "Deployment" Category change types (CTs) allow you to request various AMS-supported resources be added to your account.

Most AMS CTs that create a resource are based on AWS CloudFormation templates. As a customer you have read-only access to all AWS services including AWS CloudFormation, you can quickly identify the AWS CloudFormation stack that represents your stack based on the stack description using the AWS CloudFormation Console. The failed stack will likely be in a state of DELETE_COMPLETE. Once you have identified the AWS CloudFormation stack, the events will show you the specific resource that failed to create, and why.

### Using CloudFormation documentation to troubleshoot

Most AMS provisioning RFCs use a CloudFormation template and that documentation can be helpful for troubleshooting. See documentation for that AWS CloudFormation template:

- Create application load balancer failure: AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer)
- Create Auto scaling group: AWS::AutoScaling::AutoScalingGroup (Auto Scaling Group)
- Create memcached cache: AWS::ElastiCache::CacheCluster (Cache Cluster)
- Create Redis cache: AWS::ElastiCache::CacheCluster (Cache Cluster)
- Create DNS Hosted Zone (used with Create DNS private/public): AWS::Route53::HostedZone (R53 Hosted Zone)
- Create DNS Record Set (used with Create DNS private/public): AWS::Route53::RecordSet (Resource Record Sets)
- Create EC2 stack: AWS::EC2::Instance (Elastic Compute Cloud)
- Create Elastic File System (EFS): AWS::EFS::FileSystem (Elastic File System)
- Create Load balancer: AWS::ElasticLoadBalancing::LoadBalancer (Elastic Load Balancer)
- Create RDS DB: AWS::RDS::DBInstance (Relational Database)
- Create Amazon S3: AWS::S3::Bucket (Simple Storage Service)
- Create Queue: AWS::SQS::Queue (Simple Queue Service)

### RFC creating AMIs errors

An Amazon Machine Image (AMI) is a template that contains a software configuration (for example, an operating system, an application server, and applications). From an AMI, you launch an instance, which is a copy of the AMI running as a virtual server in the cloud. AMIs are very useful, and required to create EC2 instances or Auto Scaling groups; however, you must observe some requirements:

- The instance you specify for `Ec2InstanceId` must be in a stopped state for the RFC to succeed. Do not use Auto Scaling group (ASG) instances for this parameter because the ASG will terminate a stopped instance.
- To create an AMS Amazon Machine Image (AMI), you must start with an AMS instance. Before you can use the instance to create the AMI, you must prepare it by ensuring that it is stopped and dis-joined from its domain. For details, see Create a Standard Amazon Machine Image Using Sysprep
- The name you specify for the new AMI must be unique within the account or the RFC fails. How to do this is described in AMI | Create, and for more details, see and AWS AMI Design.

> **Note**
>
> For additional information for prepping for AMI creation, see AMI | Create.

### RFCs creating EC2s or ASGs errors

For EC2 or ASG failures with timeouts, AMS recommends that you confirm if the AMI used is customized. If it is, please refer to the AMI creation steps included in this guide (see AMI | Create) to ensure that the AMI was created correctly. A common mistake when creating a custom AMI is not following the steps in the guide to rename or invoke Sysprep.

### RFCs creating RDS errors

Amazon Relational Database Service (RDS) failures can occur for many different reasons because you can use many different engines when you create the RDS, and each engine has its own requirements and limitations. Before attempting to create an AMS RDS stack, carefully review AWS RDS parameter values, see CreateDBInstance.

To learn more about Amazon RDS in general, including size recommendations, see Amazon Relational Database Service Documentation.

### RFCs creating Amazon S3s errors

One common error when creating an S3 storage bucket is not using a unique name for the bucket. If you submitted an S3 bucket Create CT with the same name as one previously submitted, it would fail because an S3 bucket would already exist with that BucketName. This would be detailed in the AWS CloudFormation Console, where you will see that the stack event shows that the bucket name is already in use.

## RFC validation versus execution errors

RFC failures and related messages differ in the output messages on the AMS console RFC details page for a selected RFC:

- Validation Failures reasons are available in Status Field only
- Execution Failures reasons are available in Execution Output as well as Status Fields.

Request for change 32b01274-ee82-2d8e-b67b-cfbefda8eb0a

Cancel request | Create a copy

| | |
|---|---|
| Subject | santed - stack access |
| RFC ID | 32b01274-ee82-2d8e-b67b-cfbefda8eb0a |
| Change Type ID | ct-1dmlg9g1l91h6 |
| Created | 2017-12-05T04:23:14+00:00 |
| Requested start | 2017-12-05T04:31:06+00:00 - 2017-12-05T05:31:06+00:00 |
| Description | |
| Status | Rejected - {"errorMessage":"No domain trust found, please check DomainFQDN: A409470882227.amazonaws.com","errorType":"ClientError"} |
| AWS approval status | Rejected |
| Customer approval status | NotRequired |

Execution parameters

```
{
  "DomainFQDN": "A409470882227.amazonaws.com",
  "StackIds": [
    "stack-780b8040b18007ee2"
  ],
  "TimeRequestedInHours": 1,
  "Username": "santed",
  "VpcId": "vpc-daa566a2"
}
```

Execution output

```
{
  "result": null
}
```

## RFC error messages

When you come across the following error for the listed change types (CTs), you can use these solutions to help you find the source of the problems and fix them.

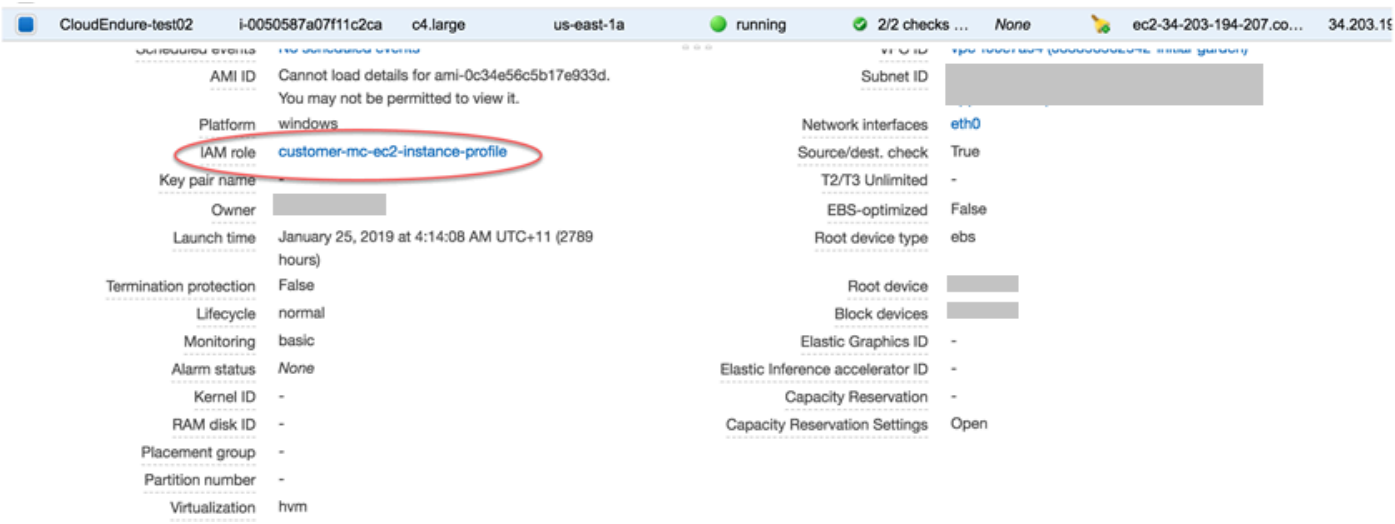
```
{"errorMessage":"An error has occurred during RFC execution. We are investigating the issue.","errorType":"InternalError"}
```

If you require further assistance after referring to the following troubleshooting options, then engage AMS via RFC correspondence or create a service request. See RFC Correspondence and Attachment (Console) and Creating a Service Request in AMS for more details.

### Workload ingestion (WIGS) errors

> **Note**
>
> Validation tools for both Windows and Linux can be downloaded and run directly on your on-premises servers, as well as EC2 instances in AWS. These can be found through the *AMS Advanced Application Developer's Guide* Migrating workloads: Linux pre-ingestion validation and Migrating workloads: Windows pre-ingestion validation.

- Make sure EC2 instance exists in target AMS account. For example, if you have shared your AMI from a non-AMS account to an AMS account, you'll have to create an EC2 instance in your AMS account with the shared AMI before you can submit a Workload Ingest RFC.
- Check to see if the security groups attached to the instance have egress traffic allowed. The SSM Agent needs to be able to connect to its public endpoint.
- Check to see if the instance has the right permissions to connect with the SSM agent. These permissions come with the `customer-mc-ec2-instance-profile`, you can check for this in the EC2 console:




### EC2 instance stack stop errors

- Check to see if the instance is already in a stopped or terminated state.
- If the EC2 instance is online and you see the `InternalError` error, then submit a service request for AMS to investigate.

- Note that you can't use the change type Management | Advanced stack components | EC2 instance stack | Stop ct-3mvvt2zkyveqj to stop an Auto Scaling group (ASG) instance. If you need to stop an ASG instance, then submit a service request.

### EC2 instance stack create errors

The `InternalError` message is from CloudFormation; a CREATION_FAILED status reason. You can find details on the stack failure in CloudWatch stack events by following these steps:

- In the AWS Management console, you can view a list of stack events while your stack is being created, updated, or deleted. From this list, find the failure event and then view the status reason for that event.

  The status reason might contain an error message from AWS CloudFormation or from a particular service that can help you understand the problem.
- For more information about viewing stack events, see Viewing AWS CloudFormation Stack Data and Resources on the AWS Management Console.

### EC2 instance volume restore errors

AMS creates an internal troubleshooting RFC when EC2 instance volume restore fails. This is done because EC2 instance volume restore is an important part of disaster recovery (DR) and AMS creates this internal troubleshooting RFC for you automatically.

When the internal troubleshooting RFC is created, a banner is displayed providing you with links to the RFC. This internal troubleshooting RFC provides your with more visibility into RFC failures and, rather than submitting retry RFCs leading to the same errors, or making you manually reach out to AMS for this failure, you can keep track of your changes and know that the failure is being worked on by AMS. This also reduces the time-to-recovery (TTR) metric for their change as AMS Operators proactively work on the RFC failure instead of waiting for your request.

## How to get help with an RFC

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 (but your CSDM will probably 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

# Direct Change mode in AMS

**Topics**


- Getting Started with Direct Change mode
- Security and compliance
- Change management in Direct Change mode
- Creating stacks using Direct Change mode
- Direct Change Mode use cases


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.

Watch Akash's video to learn more (6:30)

## Getting Started with Direct Change mode

Begin by checking prerequisites and then submitting a request for change (RFC) in your eligible AMS Advanced account.

1. Confirm that the account that you want to use with DCM meets the requirements:
   - The account is AMS Advanced Plus or Premium.
   - The account doesn't have Service Catalog enabled. We currently don't support onboarding accounts to both DCM and Service Catalog at the same time. If you are already onboarded to Service Catalog but are interested in DCM, discuss your needs with your cloud service delivery manager (CSDM). If you decide to switch from Service Catalog to DCM, offboard Service Catalog, to do that, include the ask in the request for change below. For details about Service Catalog in AMS, see AMS and Service Catalog.
2. Submit a request for change (RFC) using the Management | Managed account | Direct Change mode | Enable change type (ct-3rd4781c2nnhp). For an example walkthrough, see Direct Change mode | Enable.

   After the CT is processed, the predefined IAM roles, `AWSManagedServicesCloudFormationAdminRole` and `AWSManagedServicesUpdateRole` are provisioned in the specified account.
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 (CA).

## 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
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2AndRDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy
- AMS Advanced single-account landing zone account
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - 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) 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, OpenSearch, CloudWatch Logs, SQS, SSM, Tagging api - as these services do not support the `aws:TagsKey` condition to restrict tagging for the AMS namespace.<br><br>Standard given in table **AMS-STD-003**, following, states that you can change AppId, Environment and AppName, but not for AMS-owned resources. Not | 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. | | | |

| Standards | Does it break | Risks | Recommendations |
|---|---|---|---|
| | achievable through IAM permissions. | | |
| 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 **AMS-STD-002**, next. | Yes. Breaks for CloudFormation, CloudTrail, Amazon Elastic File System (EFS), OpenSearch, CloudWatch Logs, Amazon Simple Queue Service (SQS), Amazon EC2 Systems Manager (SSM), Tagging API; these services do not support the `aws:TagsKey` condition to restrict 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 | Yes. The purpose of self service actions allow you to perform | The secure access model is a core technical facet of | The IAM user should be time-bounded and granted permissio |

| Standards | Does it break | Risks | Recommendations |
| --- | --- | --- | --- |
| 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. | actions bypassing the AMS RFC system. | 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. | ns 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 connectio | Yes. Not possible through IAM policy. | Traffic leaving your AMS account is not | We recommend peering only with |

| Standards | Does it break | Risks | Recommendations |
|---|---|---|---|
| ns between accounts that belong to the same customer can be permitted. | | monitored once egressing the account boundary. | 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 AMS-managed and unmanaged accounts as long as we can verify that they are owned by the same AWS organization. | | AMIs may contain sensitive data and it may be exposed to unintended accounts. | Share AMIs with only the account owned by your organizat ion 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, |
| 20. Any log can be forwarded from AMS to a non-AMS account only if the | | | |

| Standards | Does it break | Risks | Recommendations |
| --- | --- | --- | --- |
| non-AMS account is owned by the same AMS customer (by confirming that they are under the same AWS Organizat ions account or by matching the email domain with the customer's company name and PAYER linked account) using internal tools. | | | check with your cloud service delivery manager (CSDM). |

Work with your internal authorization and authentication 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 request for change (RFC) process. The `AWSManagedServicesCloudFormationAdminRole` is restricted to actions taken through CloudFormation (CFN). For more about how to create stacks through DCM, see Creating stacks using Direct Change mode. The `AWSManagedServicesUpdateRole` is restricted for the following actions.

For example walkthroughs for each change type, including the Management | Managed account | Direct Change mode | Enable (ct-3rd4781c2nnhp) change type, see the "Additional Information" section for the relevant change type in the *AMS Advanced Change Type Reference* Change Types by Classification section.

| Service | Action |
| --- | --- |
| AWS Key Management Service (AWS KMS) | Update |
| AWS Certificate Manager | Create |
| AWS Identity and Access Management (IAM) | Any |
| AWS VPN | Any |

| Service | Action |
| --- | --- |
| 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 | |
| AMS Advanced Stack Access | Any |
| Amazon Elastic Block Store (EBS) volume | Delete |
| Amazon Elastic Block Store (EBS) default encryption | Enable default encryption |
| Amazon Elastic Compute Cloud (Amazon EC2) | Change hostname |
| Amazon Machine Images (AMI) | Delete, share |
| Amazon EC2 Security Group | Any |
| AMS Advanced SSPS | |
| AWS Managed Microsoft AD | |
| AMS Advanced developer mode | |
| Amazon Simple Storage Service (Amazon S3) | Create S3 bucket policies |
| AWS Systems Manager | Create |

## 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 `AmsStackTransform`.
- The stack name must start with the prefix `stack-` followed by a 17 character alphanumeric string.

> **Note**
>
> To successfully use the `AmsStackTransform`, you must acknowledge that your stack template contains the `CAPABILITY_AUTO_EXPAND` capability in order for AWS CloudFormation (CFN) to create or update the stack. You do this by passing the `CAPABILITY_AUTO_EXPAND` as part of your create-stack request. CFN rejects the request if this capability is not acknowledged when the `AmsStackTransform` is included in the template. The CFN console ensures that you pass this capability if you have the transform in your template, but this can be missed when you are interacting with CFN via their APIs. You must pass this capability whenever you use the following CFN API calls:
>
> - CreateChangeSet
> - CreateStack
> - UpdateStack

When creating or updating a stack with DCM, the same validations and augmentations of CFN Ingest and Stack Update CTs are performed on the stack, for more information see AWS CloudFormation Ingest Guidelines, Best Practices, and Limitations. The exception to this is that the AMS default security groups (SGs) will not be attached to any stand-alone EC2 instances or EC2 instances in Auto Scaling groups (ASGs). When you create your CloudFormation template, with stand-alone EC2 instances or ASGs, you can attach the default SGs.

> **Note**
>
> IAM roles can now be created and managed with the `AWSManagedServicesCloudFormationAdminRole`.

The AMS default SGs have ingress and egress rules that allow the instances to launch successfully and to be accessed later through SSH or RDP by AMS operations and you. If the you find that the AMS default security groups are too permissive, you can create your own SGs with more restrictive rules and attach them to your instance, as long as it still allows you and AMS operations to access the instance during incidents.

The AMS default security groups are the following:

- SentinelDefaultSecurityGroupPrivateOnly: Can be accessed in the CFN template through this SSM parameter `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll: Can be accessed in the CFN template through this SSM parameter `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

## AMS Transform

Add a `Transform` statement to your CloudFormation template. This adds a CloudFormation macro that validates and registers the stack with AMS at launch time.

**JSON** Example

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

**YAML** Example

```
Transform:
  Name: AmsStackTransform
  Parameters:
```

```
    StackId: !Ref 'AWS::StackId'
```

Also add the `Transform` statement when updating the template of an existing stack.

**JSON** 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"}
      }
    }
  }
}
```

**YAML** 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]$_}) )
```

## Direct Change Mode use cases

The following are uses cases for Direct Change Mode:

#### Resource provision and management through AWS CloudFormation

- Integrate existing CloudFormation-based tooling and processes.

#### Ongoing resource management and updates

- Small atomic changes with low risk.
- Changes that would otherwise run through a manual or automated RFC.

- Tooling that requires native AWS API access.
- The DCM role can be utilized if you're in the migration stage. Migration teams leverage the permissions on the DCM to create or modify stacks.
- DCM roles can be used in the CI/CD pipeline to build new AMIs, create Amazon ECS tasks, and so on.

# AMS Advanced Developer mode

**Topics**


- Getting started with AMS Advanced Developer mode
- Security and compliance in Developer mode
- Change management in Developer mode
- Provisioning infrastructure in AMS Developer mode
- Detective controls in AMS Developer mode
- Logging, monitoring, and event management in AMS Developer mode
- Incident management in AMS Developer mode
- Patch management in AMS Developer mode
- Continuity management in AMS Developer mode
- Security and access management in AMS Developer mode


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 Modes overview.

## Getting started with AMS Advanced Developer mode

Learn the various AMS Advanced accounts with AMS Advanced Developer mode and how to successfully implement Developer mode.

**Topics**


- Before you begin with AMS Developer mode
- Prerequisites for AMS Developer mode
- How to implement AMS Advanced Developer mode
- AMS Advanced Developer mode permissions


### Before you begin with AMS Developer mode

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 AMS 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.

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 AMS Developer mode.
2. Submit a request for change (RFC) using the change type (CT) Management | Managed account | Developer mode | Enable (review required). For an example of how to use this CT, see Developer Mode | Enable (Review Required).

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.

**Cautions:**

- DevMode allows you and your authorized team to bypass the deny-by-default principles at the core of AMS security. The advantages, self-service, less time waiting for AMS must be weighed against the disadvantages, anyone can perform unexpected and destructive actions without the knowledge of their security team. Automated change types to enable Dev mode and Direct

Change mode are exposed, and any authorized person in your org can run these CTs and enable these modes.

- You are responsible for managing the permissions of CT execution from your user base.
- AMS doesn't manage CT execution permissions

**Recommendations:**

- **Protect**
  - Customers can prevent access to this CT via permissioning, see Restrict permissions with IAM role policy statements
  - Prevent access to this CT by implementing a proxy such as an ITSM system
  - Utilize service control policies (SCPs) that prevent policies and behaviors as needed, see AMS Preventative and Detective Controls Library
- **Detect**
  - Monitor your RFC's for these CTs (Enable developer mode ct-1opjmhuddw194 and Direct change mode, Enable ct-3rd4781c2nnhp) being executed and respond accordingly
  - Review and/or audit your accounts for the presence of the IAM resources to identify those accounts where Developer mode or Direct Change mode have been deployed
- **Respond**
  - Remove accounts in Developer mode as needed

## 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 modes.

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.<br><br>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:<br><br>• `ds:AuthorizeApplication`<br>• `ds:CreateAlias`<br>• `ds:CreateIdentityPoolDirectory`<br>• `ds:DeleteDirectory`<br>• `ds:DescribeDirectories`<br>• `ds:GetAuthorizedApplication Details`<br>• `ds:ListAuthorizedApplications` |

| Service | Notes |
| --- | --- |
| | • `ds:UnauthorizeApplication`<br><br>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`.<br><br>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. |

| Service | Notes |
| --- | --- |
| AWS Identity and Access Management (IAM) | Can't delete existing permission boundaries, or modify IAM user password policies.<br><br>Can't create or modify IAM resources unless you are using the correct IAM role (`AWSManagedServicesDevelopmentRole` for **MALZ**, `customer_developer_role` for **SALZ**)).<br><br>Can't modify IAM resources that are prefixed with: `ams`, `mc`, `customer_deny_policy`, and/or `sentinel`.<br><br>When creating a new IAM resource (role, user, or group), the permission boundary (**MALZ**: `AWSManagedServicesDevelopmentRolePermissionsBoundary`, **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. |

| Service | Notes |
| --- | --- |
| Amazon Route 53 | Can't access or modify Route53 AMS Advanced-maintained resources. |
| 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 Manager (SSM) | Can't modify SSM parameters that are prefixed with `ams`, `mc`, or `svc`.<br><br>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`. |

| Service | Notes |
| --- | --- |
| AWS Lake Formation | The following AWS Lake Formation API actions are denied:<br>• `lakeformation:DescribeResource`<br>• `lakeformation:GetDataLakeSettings`<br>• `lakeformation:DeregisterResource`<br>• `lakeformation:RegisterResource`<br>• `lakeformation:UpdateResource`<br>• `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 AMS 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 AMS 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 AMS 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 AMS 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**
>
> AMS service level agreement (SLA) does not apply for resources created or updated outside of the AMS change management system (requests for change or RFCs), Developer mode included; therefore, resources updated or created in Developer mode are automatically degraded to a P3 and AMS support is best effort.

## Patch management in AMS 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 AMS 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 AMS 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.

# Self-Service Provisioning mode in AMS

AWS Managed Services (AMS) Self-Service Provisioning (SSP) mode provides full access to native AWS service and API capabilities in AMS managed accounts. You access services through standardized, scoped down, AWS Identity and Access Management 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 AWS CloudFormation templates to automate deployment of these services, but this isn't supported for all SSP services.

> **Important**
>
> Use SSP mode in your AWS Managed Services (AMS) accounts to access and employ AWS services, with restrictions as noted.

There are some AWS services that you can use without AMS management, in your AMS account. The Self-Service Provisioning mode services, or SSPS for short, how to add them into your AMS account and FAQs for each, are described in the section.

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.

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 and access, and technical support through 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.

## Getting started with SSP mode in AMS

Self-service provisioning is one of the AMS modes for multi-account landing zone (MALZ) that you can employ. For more information, see Modes overview.

To provide self-service provisioning capabilities, AMS has created elevated IAM roles with permission boundaries to limit unintended changes from direct AWS service access. The roles don't prevent all changes and you must adhere to your internal controls and compliance policies, and validate that all AWS services being used meet the required certifications. This is the self-service provisioning mode. For details on AWS compliance requirements, see AWS Compliance.

To add a self-service provisioning service to your multi-account landing zone Application account, use the **Management | AWS service | Self-provisioned service | Add** change type (CT), either the review-required CT or automated CT, as instructed for the service.

> **Note**
>
> To request that AMS provide an additional self-service provisioning service, file a service request.

## Use AMS SSP to provision Amazon API Gateway in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon API Gateway capabilities directly in your AMS managed account. 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.

### FAQ: 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-1w8z66n899dct) change type. This RFC provisions the following IAM roles to your account: `customer_apigateway_author_role` and `customer_apigateway_cloudwatch_role`. After provisioned in your account, you must onboard the roles 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 | Create.

**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 load balancer).

## Use AMS SSP to provision Alexa for Business in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Alexa for Business capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**Q: How do I request access to Alexa for Business in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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, then specify this network security type in the Device Setup Tool, for which an AWS Private Certificate Authority is required.
- AMS only creates secret keys that start with the namespace "A4B". This is restrictive only to this namespace.

**Q: 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.

## Use AMS SSP to provision Amazon AppStream 2.0 in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon AppStream 2.0 (AppStream 2.0) capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**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?**

While submitting the RFC to onboard AppStream 2.0, include the Amazon S3 bucket name to be used for the AppStream 2.0 usage report. The bucket name is added to the `customer-appstream-usagereports-policy` that is created when AppStream 2.0 is onboarded.

**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 2.0 Usage Reports Logs.

  After the role is provisioned, onboard the role into your federation solution and login, then access AWS GlueAWS 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.

# Use AMS SSP to provision Amazon Athena in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Athena (Athena) capabilities directly in your AMS managed account. 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 extract-transform-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.

## FAQ: 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-1w8z66n899dct) 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.

The role `customer_athena_console_role` has a prerequisite for an Amazon S3 bucket. To create a new bucket, use the automated CT `ct-1a68ck03fn98r` (Deployment | Advanced stack components | S3 storage | Create). When you use this automated CT to create an S3 bucket for Athena, the bucket name must begin with prefix `athena-query-results-*`.

# Use AMS SSP to provision Amazon Bedrock in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Bedrock capabilities directly in your AMS managed account. Amazon Bedrock is a fully managed service that makes high-

performing foundation models (FMs) from leading AI startups and AWS available for your use through a unified API. You can choose from a wide range of foundation models to find the model that is best suited for your use case. Amazon Bedrock also offers a broad set of capabilities to build generative AI applications with security, privacy, and responsible AI. Using Amazon Bedrock, you can easily experiment with and evaluate top foundation models for your use cases, privately customize them with your data using techniques such as fine-tuning and Retrieval Augmented Generation (RAG), and build agents that execute tasks using your enterprise systems and data sources.

With Amazon Bedrock's serverless experience, you can get started quickly, privately customize foundation models with your own data, and easily and securely integrate and deploy them into your applications using AWS tools without having to manage any infrastructure. For more information, see Amazon Bedrock.

## FAQ: Amazon Bedrock in AMS

### Q: How do I request access to Amazon Bedrock in my AMS account?

To request access to Amazon Bedrock submit an RFC with the Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_bedrock_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 Bedrock in my AMS account?

- Amazon Bedrock knowledge bases aren't supported by default as part of the SSPS role due to its dependency on Amazon OpenSearch Service Serverless which is not currently supported on AMS.
- Bedrock Studio isn't supported due to its dependency on unsupported services such as Amazon DataZone.

### Q: What are the prerequisites or dependencies to using Amazon Bedrock in my AMS account?

- Third-party model subscriptions that require AWS Marketplace permissions must be done by the default role (`AWSManagedServicesAdminRole` on MALZ and `Customer_ReadOnly_Role` on SALZ). This is because the default role includes AWS Marketplace permissions.
- If data encryption is used, then you must provide the AWS KMS key ARN when you request creation of the console role. Also, the Amazon S3 bucket in use must have “bedrock” in its name.

# Use AMS SSP to provision Amazon CloudSearch in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon CloudSearch capabilities directly in your AMS managed account. 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.

> **Note**
>
> AWS has closed new customer access to Amazon CloudSearch, effective July 25, 2024. Amazon CloudSearch existing customers can continue to use the service as normal. AWS continues to invest in security, availability, and performance improvements for Amazon CloudSearch, but we do not plan to introduce new features.
> To understand the differences between Amazon CloudSearch and Amazon OpenSearch Service, and how you can transition to OpenSearch Service, reach out to your cloud architect (CA) for guidance. For more information on transitioning to OpenSearch Service, see Transition from Amazon CloudSearch to Amazon OpenSearch Service service.

## Amazon CloudSearch in AWS Managed Services FAQ

### 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-1w8z66n899dct) 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.

## Use AMS SSP to provision Amazon CloudWatch Synthetics in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon CloudWatch Synthetics capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

#### 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-1w8z66n899dct) change type. This RFC provisions the following IAM role to your account: 'customer_cw_synthetics_console_role' and 'customer_cw_synthetics_canary_lambda_role'. Once provisioned in your account, you must onboard the 'customer_cw_synthetics_console_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_cw_synthetics_canary_lambda_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}*"

## Use AMS SSP to provision Amazon Cognito user pools in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Cognito user pools capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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 Amazon Cognito user pools, manage your users and groups in the pool, create importjobs for users, modify the notification and subscription messages, associate applications to the user pool, self-manage adding federation services to the pool, 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.

## Use AMS SSP to provision Amazon Comprehend in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Comprehend capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**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 by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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.

## Use AMS SSP to provision Amazon Connect in your AMS account

> **Note**
>
> After careful consideration, we decided to end support for Amazon Connect Voice ID, effective May 20, 2026. Amazon Connect Voice ID will no longer accept new customers beginning May 20, 2025. As an existing customer with an account signed up for the service

before May 20, 2025, you can continue to use Amazon Connect Voice ID features. After May 20, 2026, you will no longer be able to use Amazon Connect Voice ID.

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Connect capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**Q: How do I request access to Amazon Connect in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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.
- **Q: How do I request to add list of countries for outbound or inbound calls?**

  To add a list of countries for outbound or inbound calls, submit a service request to AMS.

## Use AMS SSP to provision Amazon Data Firehose in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Data Firehose capabilities directly in your AMS managed account. Firehose 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 Data Firehose?

### Firehose in AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request access to Amazon Data Firehose in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type. 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 Firehose in my AMS account?**

There are no restrictions. Full functionality of Amazon Data Firehose is available in your AMS account.

**Q: What are the prerequisites or dependencies to using 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 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).

## Use AMS SSP to provision Amazon DevOps Guru in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon DevOps Guru capabilities directly in your AMS managed account. Amazon DevOps Guru is a fully managed operations service that makes it easy for developers and operators to improve the performance and availability of their applications. DevOps Guru lets you offload the administrative tasks associated with identifying operational issues so that you can quickly implement recommendations to improve your application. DevOps Guru creates reactive insights you can use to improve your application now. It also creates proactive insights to help you avoid operational issues that might affect your application in the future. DevOps Guru applies machine learning to analyze your operational data and application metrics and events to identify behaviors that deviate from normal operating patterns. You are notified when DevOps Guru detects an operational issue or risk. For each issue, DevOps Guru presents intelligent recommendations to address current and predicted future operational issues.

To learn more, see What is Amazon DevOps Guru.

## Amazon DevOps Guru in AWS Managed Services FAQ

**Q: How do I request access to Amazon DevOps Guru in my AMS account?**

To request access, submit a Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_devopsguru_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 DevOps Guru in my AMS account?**

There are no restrictions. Full functionality of Amazon DevOps Guru is available in your AMS account.

**Q: What are the prerequisites or dependencies to using Amazon DevOps Guru in my AMS account?**

There are no prerequisites. DevOps Guru leverages the following AWS services: Amazon CloudWatch Logs, RDS Insights, AWS X-Ray, AWS Lambda, and AWS CloudTrail.

# Use AMS SSP to provision Amazon DocumentDB (with MongoDB compatibility) in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon DocumentDB (with MongoDB compatibility) capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**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-1w8z66n899dct) 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.

# Use AMS SSP to provision Amazon DynamoDB in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon DynamoDB (DynamoDB) capabilities directly in your AMS managed account. Amazon DynamoDB is a key value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-region, multi-active database with built-in security, backup and restore, and in-memory caching for internet scale applications. 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 AWS Managed Services FAQ

**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-1w8z66n899dct) 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.

# Use AMS SSP to provision Amazon Elastic Container Registry in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Elastic Container Registry (Amazon ECR) capabilities directly in your AMS managed account. Amazon Elastic Container Registry 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 AWS Managed Services FAQ

### 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-1w8z66n899dct) change type. This RFC provisions the following IAM roles to your account: `customer_ecr_console_role`, and `customer_ecr_poweruser_instance_profile` with associated IAM policies, `customer_ecr_console_policy` and `customer_ecr_poweruser_instance_profile_policy`, respectively. 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.

# Use AMS SSP to provision EC2 Image Builder in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access EC2 Image Builder capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request access to EC2 Image Builder in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 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. 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:

  JSON

```
{
    "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.

# Use AMS SSP to provision Amazon ECS on AWS Fargate in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon ECS on AWS Fargate capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

### 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-1w8z66n899dct) 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.
- Security and malware protection at the container level are also considered to be your responsibility. Amazon ECS on Fargate doesn't 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.

## Use AMS SSP to provision Amazon EKS on AWS Fargate in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon EKS on AWS Fargate capabilities directly in your AMS managed account. 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 and Amazon EKS Best Practices Guide for Security (includes "Recommendations" such as "Review and revoke unnecessary anonymous access" and more).

> **Tip**
>
> AMS has a change type, Deployment | Advanced stack components | Identity and Access Managment (IAM) | Create OpenID Connect provider (ct-30ecvfi3tq4k3), that you can use with Amazon EKS. For an example, see Identity and Access Management (IAM) | Create OpenID Connect Provider.

## Amazon EKS on AWS Fargate in AWS Managed Services FAQ

### Q: How do I request access to Amazon EKS on Fargate in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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?

- Creating managed or self-managed EC2 nodegroups is not supported in AMS. If you have a requirement for using EC2 worker nodes, reach out to your AMS Cloud Service Delivery Manager(CSDM) or Cloud Architect(CA).
- AMS does not include Trend Micro or preconfigured network security components for container images. You are expected to manage your own image scanning services to detect malicious container images prior to deployment.
- EKSCTL is not supported due to CloudFormation interdependencies.
- During cluster creation, you 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, then it's a best practice to set them to public only for specific CIDR ranges.
- AMS doesn't have a method to force and restrict images used to deploy to containers on Amazon EKS Fargate. You can deploy images from Amazon ECR, Docker Hub, or any other private image repository. Therefore, there is a risk of deploying a public image that might perform malicious activity on the account.

- Deploying EKS clusters through the cloud development kit (CDK) or CloudFormation Ingest isn't supported in AMS.
- You must create the required security group using ct-3pc215bnwb6p7 Deployment | Advanced stack components | Security group | Create and reference in the manifest file for ingress creation. This is because the role `customer-eks-alb-ingress-controller-role` isn't authorized to create security groups.

**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

  It is your responsibility to monitor and remediate these Config rules.

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: aws-load-balancer-controller]

If you want to enable envelope secrets encryption in your cluster (which we recommend), provide the KMS key IDs you intend to use, in the description field of the RFC to add the service (Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). To learn more about envelope encryption, see Amazon EKS adds envelope encryption for secrets with AWS KMS.

## Use AMS SSP to provision Amazon EMR in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon EMR capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**Q: How do I request access to Amazon EMR in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM roles to your account:

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

After it's provisioned in your account, you must onboard the customer_emr_console_role in your federation solution.

**Q: What are the restrictions to using Amazon EMR in my AMS account?**

While creating Amazon EMR on an EC2 cluster from the AWS console, we advise you to use the **Create Cluster – Advanced** option. Amazon EMR clusters must be created by adding the tag with the Key **"for-use-with-amazon-emr-managed-policies"** with Value **"true"**. Select the following configurations in the **Security** options:

- Select custom roles for your cluster:
  - EMR Role : customer_emr_cluster_service_role
  - EC2 Instance Profile : customer_emr_cluster_instance_profile
  - Auto Scaling Role : customer_emr_cluster_autoscaling_role
- EC2 Security groups:
  - Master : ams-emr-master-security-group
  - Core & Task : ams-emr-worker-security-group
  - Service Access : ams-emr-serviceaccess-security-group

**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.

The launch templates and security groups to be used with Amazon EMR clusters must have the tag key **"for-use-with-amazon-emr-managed-policies"** with value **"true"**.

The default Amazon EMR cluster instance profile enables access to the resources such as s3 buckets and dynamodb tables with their names containing "emr". You can request additional IAM policies to use any additional resources to be used with Amazon EMR. The following resource ARN's can be used with Amazon EMR jobs using the **customer_emr_cluster_instance_profile**:

- arn:aws:dynamodb:*:*:table/*emr*
- arn:aws:kinesis:*:*:stream/*emr*
- arn:aws:sns:*:*:*emr*arn:aws:sqs:*:*:*emr*
- arn:aws:sqs:*:*:*emr*
- arn:aws:sqs:*:*:AWS-ElasticMapReduce-*
- arn:aws:sdb:*:*:domain:*emr*
- arn:aws:s3:::*emr*

If kerberos authentication is required for the Amazon EMR cluster:

- Provide the realm name to be used for each kerberized 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 a Management | Other | Other | Update (ct-0xdawir96cy7k) RFC to update the VPC DHCP option set to use the realm name for domain name suffix.

  **SALZ**: Submit a Management | Other | Other | Update (ct-0xdawir96cy7k) RFC to generate a new Amazon EMR AMI to use the specific realm for domain name suffix.

To deploy Amazon EMR studio, the role `customer_emr_cluster_service_role` has a prerequisite for an Amazon Simple Storage Service bucket. To create the bucket, use the automated CT `ct-1a68ck03fn98r` (Deployment | Advanced stack components | S3 storage | Create). When you use this automated CT to create an Amazon S3 bucket for Amazon EMR, the bucket name must begin with the prefix `customer-emr-*`. And, you must create the bucket in the same AWS Region as the Amazon EMR cluster.

## Use AMS SSP to provision Amazon EventBridge in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon EventBridge capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**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-1w8z66n899dct) change type. This RFC provisions the following IAM roles to your account: `customer_eventbridge_role` and `customer_eventbridge_scheduler_execution_role`. After it's provisioned in your account, you must onboard the role in your federation solution.

The execution role, `customer_eventbridge_scheduler_execution_role` is an IAM role that EventBridge Scheduler assumes to interact with other AWS services on your behalf. The permission policies attached to this role grant EventBridge Scheduler access to invoke targets.

> **Note**
>
> By default, EventBridge Scheduler uses AWS owned keys for EventBridge to encrypt the data. To use a customer managed key for EventBridge to encrypt the data, submit the RFC

using the Management | AWS service | Self-provisioned service | Add (review required) change type (ct-3qe6io8t6jtny) for service provisioning.

**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. Specify the services to invoke when requesting your service role. To learn about permissions required to invoke targets, see 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 must be enabled and allowed to store the log files to S3 buckets. Note: All AMS accounts have CloudTrail enabled, so no action is needed.

**Q: The role customer_eventbridge_scheduler_execution_role has a prerequisite for an AWS Key Management Service Key (optional, if used for encryption). How do I adopt AWS KMS CMKs in data encryption at rest/transit?**

By default, EventBridge Scheduler encrypts event metadata and message data that it stores under an AWS owned key (encryption at rest). EventBridge Scheduler also encrypts data that passes between EventBridge Scheduler and other services using Transport Layer Security (TLS) (encryption in transit).

If your specific use case requires that you control and audit the encryption keys that protect your data on EventBridge Scheduler, you can use a customer managed key.

You must request an RFC using the Management | AWS service | Self-provisioned service | Add (review required) change type prior to using Amazon EventBridge to onboard the AWS KMS permission.

# Use AMS SSP to provision Amazon Forecast in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Forecast (Forecast) capabilities directly in your AMS managed account. Amazon Forecast is a fully managed service that uses machine learning to deliver highly accurate forecasts.

> **Note**
>
> AWS has closed new customer access to Amazon Forecast, effective July 29, 2024. Amazon Forecast existing customers can continue to use the service as normal. AWS continues to invest in security, availability, and performance improvements for Amazon Forecast, but AWS does not plan to introduce new features.
> If you want to use Amazon Forecast, reach out to your CSDM so that they can guide you further regarding how to Transition your Amazon Forecast usage to Amazon SageMaker Canvas.

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 AWS Managed Services FAQ

### 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-1w8z66n899dct) 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.

## Use AMS SSP to provision Amazon FSx in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon FSx capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**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-1w8z66n899dct) 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.

## Use AMS SSP to provision Amazon FSx for OpenZFS in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon FSx for OpenZFS capabilities directly in your AMS managed account. FSx for OpenZFS is a fully managed file storage service that makes it easy to move data residing in on-premises ZFS or other Linux-based file servers to AWS without changing your application code or how you manage data. It offers highly reliable, scalable, performant, and feature-rich file storage built on the open-source OpenZFS file system, providing the familiar features and capabilities of OpenZFS file systems with the agility, scalability, and simplicity of a fully managed AWS service. For developers building cloud-native applications, it offers simple, high-performance storage with rich capabilities for working with data.

FSx for OpenZFS file systems are broadly accessible from Linux, Windows, and macOS compute instances and containers using the industry-standard NFS protocol (v3, v4.0, v4.1, v4.2). Powered by AWS Graviton processors and the latest AWS disk and networking technologies (including AWS Scalable Reliable Datagram networking and the AWS Nitro system), FSx for OpenZFS delivers up to 1 million IOPS with latencies of hundreds of microseconds. With complete support for OpenZFS features like instant point-in-time snapshots and data cloning, FSx for OpenZFS makes it easy for you to replace your on-premises file servers with AWS storage that provides familiar file system capabilities and eliminates the need to perform lengthy qualifications and change or re-architect existing applications or tools. And, by combining the power of OpenZFS data management capabilities with the high performance and cost efficiency of the latest AWS technologies, FSx for OpenZFS enables you to build and run high-performance, data-intensive applications.

As a fully managed service, FSx for OpenZFS makes it easy to launch, run, and scale fully managed file systems on AWS that replace the file servers you run on premises while helping to provide better agility and lower costs. With FSx for OpenZFS, you no longer have to worry about setting up and provisioning file servers and storage volumes, replicating data, installing and patching file server software, detecting and addressing hardware failures, and manually performing backups. It also provides rich integration with other AWS services, such as AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS), Amazon CloudWatch, and AWS CloudTrail.

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 for OpenZFS in AWS Managed Services FAQ

**Q: How do I request access to use FSx for OpenZFS in my AMS account?**

Request access to Amazon FSx OpenZFS by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type. This RFC provisions the following IAM role to your account: `customer_fsx_ontap_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 FSx for OpenZFS in my AMS account?**

Replacing the security group on the Amazon FSx elastic network interfaces (ENIs) requires you to submit Management | Other | Other | Update RFCs since security groups are a critical perimeter for the AMS environment. That is the only restriction.

**Q: What are the prerequisites or dependencies to using FSx for OpenZFS in my AMS account?**

There are no prerequisites. However, you must have Use AMS SSP to provision Amazon FSx in your AMS account installed.

## Use AMS SSP to provision Amazon FSx for NetApp ONTAP in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon FSx for NetApp ONTAP capabilities directly in your AMS managed account. Amazon FSx for NetApp ONTAP is a fully managed service that provides highly reliable, scalable, performant, and feature-rich file storage built on NetApp's popular ONTAP file system. It provides the familiar features, performance, capabilities, and APIs of NetApp file systems with the agility, scalability, and simplicity of a fully managed AWS service.

Amazon FSx for NetApp ONTAP provides feature-rich, fast, and flexible shared file storage that’s broadly accessible from Linux, Windows, and macOS compute instances running in AWS or on premises. FSx for ONTAP offers high-performance SSD storage with sub-millisecond latencies, and makes it quick and easy to manage your data by enabling you to snapshot, clone, and replicate your files with the click of a button. It also automatically tiers your data to lower-cost, elastic storage, eliminating the need to provision or manage capacity and allowing you to achieve SSD

levels of performance for your workload while only paying for SSD storage for a small fraction of your data. It provides highly available and durable storage with fully managed backups and support for cross-region disaster recovery, and supports popular data security and anti-virus applications that make it even easier to protect and secure your data. For customers who use NetApp ONTAP on-premises, FSx for ONTAP is an ideal solution to migrate, back up, or burst your file-based applications from on-premises to AWS without the need to change your application code or how you manage your data.

As a fully managed service, Amazon FSx for NetApp ONTAP makes it simple to launch and scale reliable, performant, and secure shared file storage in the cloud. With Amazon FSx for NetApp ONTAP, you no longer have to worry about setting up and provisioning file servers and storage volumes, replicating data, installing and patching file server software, detecting and addressing hardware failures, managing failover and failback, and manually performing backups. It also provides rich integration with other AWS services, such as AWS Identity and Access Management, Amazon WorkSpaces, AWS Key Management Service, and AWS CloudTrail.

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 for NetApp ONTAP in AWS Managed Services FAQ

**Q: How do I request access to Amazon FSx for NetApp ONTAP in my AMS account?**

Request access to Amazon FSx for NetApp ONTAP by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type. This RFC provisions the following IAM role to your account: `customer_fsx_ontap_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 for NetApp ONTAP in my AMS account?**

Replacing the security group on the Amazon FSx for NetApp ONTAP elastic network interfaces (ENIs) requires you to submit Management | Other | Other | Update RFCs since security groups are a critical perimeter for the AMS environment. That is the only restriction.

**Q: What are the prerequisites or dependencies to using Amazon FSx for NetApp ONTAP in my AMS account?**

There are no prerequisites. However, you must have Use AMS SSP to provision Amazon FSx in your AMS account installed.

# Use AMS SSP to provision Amazon Inspector Classic in your AMS account

> **Note**
>
> End of support notice: On May 20, 2026, AWS will end support for Amazon Inspector Classic. After May 20, 2026, you will no longer be able to access the Amazon Inspector Classic console or Amazon Inspector Classic resources. Amazon Inspector Classic will no longer be available to new accounts, and accounts that have not completed an assessment in the last six months. For all other accounts, access will remain valid until May 20, 2026, after which you will no longer be able to access the Amazon Inspector Classic console or Amazon Inspector Classic resources. For more information, see Amazon Inspector Classic end of support.

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Inspector Classic capabilities directly in your AMS managed account. Amazon Inspector Classic is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector Classic automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector Classic 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 Classic console or API. To learn more, see Amazon Inspector Classic.

## Amazon Inspector in AWS Managed Services FAQ

### Q: How do I request access to Amazon Inspector Classic in my AMS account?

Request access to Amazon Inspector Classic by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 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 Classic in my AMS account?

There are no restrictions. Full functionality of Amazon Inspector Classic is available in your AMS account.

**Q: What are the prerequisites or dependencies to using Amazon Inspector Classic in my AMS account?**

There are no prerequisites or dependencies to use Amazon Inspector Classic in your AMS account.

### Use the new Amazon Inspector in AMS

You can now use the new Amazon Inspector in your AMS account.

For Amazon Inspector Classic, the `customer-inspector-admin-role-ssm-inspector-agent-policy` and `AmazonInspectorFullAccess` were required. However, there has been an update to the SSPS role `customer-inspector-admin-role`, which now includes an additional `policyAmazonInspector2FullAccess`. This new policy allows API permissions for the new version of Amazon Inspector.

## Use AMS SSP to provision Amazon Kendra in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Kendra capabilities directly in your AMS managed account. Amazon Kendra is an intelligent search service that uses natural language processing and advanced machine learning algorithms to return specific answers to search questions from your data. Unlike traditional keyword-based search, Amazon Kendra uses its semantic and contextual understanding capabilities to determine if a document is relevant to a search query. Amazon Kendra returns specific answers to questions, so your experience is close to interacting with a human expert. Amazon Kendra is highly scalable, capable of meeting performance demands, is tightly integrated with other AWS services such as Amazon S3 and Amazon Lex, and offers enterprise-grade security. To learn more, see Amazon Kendra;.

### Amazon Kendra in AWS Managed Services FAQ

**Q: How do I request access to Amazon Kendra in my AMS account?**

To request access to Amazon Inspector Classic, submit an RFC with the Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) change type. This RFC provisions the `customer_kendra_console_role` IAM role to your account. After provisioned in your account, you must onboard the role in your federation solution.

**Q: What are the restrictions to using Amazon Kendra in my AMS account?**

There are no restrictions. Full functionality of Amazon Kendra is available in your AMS account.

**Q: What are the prerequisites or dependencies to using Amazon Kendra in my AMS account?**

There are no prerequisites or dependencies to get started with Amazon Kendra. However, depending on your specific use case, you might require access to other AWS services.

## Use AMS SSP to provision Amazon Kinesis Data Streams in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Kinesis Data Streams (KDS) capabilities directly in your AMS managed account. Amazon Kinesis Data Streams 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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.

# Use AMS SSP to provision Amazon Kinesis Video Streams in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Kinesis Video Streams (KVS) capabilities directly in your AMS managed account. Amazon Kinesis Video Streams 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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.

# Use AMS SSP to provision Amazon Lex in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Lex capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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.

# Use AMS SSP to provision Amazon MQ in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon MQ capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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.

## Use AMS SSP to provision Amazon Managed Service for Apache Flink in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Managed Service for Apache Flink capabilities directly in your AMS managed account. Managed Service for Apache Flink is the

easiest way to analyze streaming data, gain actionable insights, and respond to your business and customer needs in real time. Amazon Managed Service for Apache Flink 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 Managed Service for Apache Flink 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 Managed Service for Apache Flink, you only pay for the resources your streaming applications consume. There is no minimum fee or setup cost. To learn more, see Amazon Managed Service for Apache Flink.

## Managed Service for Apache Flink in AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request access to Amazon Managed Service for Apache Flink in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type. 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 Managed Service for Apache Flink 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 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 Managed Service for Apache Flink requires that Kinesis Data Streams or Firehose must be created prior to configuring an application with Managed Service for Apache Flink.
- The resource-based policy permissions should indicate a particular input data source.

# Use AMS SSP to provision Amazon Managed Streaming for Apache Kafka in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Managed Streaming for Apache Kafka (Amazon MSK) capabilities directly in your AMS managed account. Amazon Managed Streaming for Apache Kafka 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 AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request access to Amazon MSK in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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.

## Use AMS SSP to provision Amazon Managed Service for Prometheus in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Managed Service for Prometheus (AMP) capabilities directly in your AMS managed account. Amazon Managed Service for Prometheus is a serverless, Prometheus-compatible monitoring service for container metrics that makes it easier to securely monitor container environments at scale. With Amazon Managed Service for Prometheus, you can use the same open-source Prometheus data model and query language that you use today to monitor the performance of your containerized workloads, and also enjoy improved scalability, availability, and security without having to manage the underlying infrastructure.

Amazon Managed Service for Prometheusautomatically scales the ingestion, storage, and querying of operational metrics as workloads scale up and down. It integrates with AWS security services to enable fast and secure access to data. For more information, see What is Amazon Managed Service for Prometheus?

### Amazon Managed Service for Prometheus in AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request access to Amazon Managed Service for Prometheus in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer-prometheus-console-role`. After it's provisioned in your account, you must onboard the `customer-prometheus-console-role` role in your federation solution.

**Q: What are the restrictions to using Amazon Managed Service for Prometheus in my AMS account?**

All features are supported.

**Q: What are the prerequisites or dependencies to using Amazon Managed Service for Prometheus in my AMS account?**

There are no prerequisites or dependencies to get started with Amazon Managed Service for Prometheus. However, depending on your specific use case, you might require access to other AWS services.

## Use AMS SSP to provision Amazon Personalize in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Personalize capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

#### Q: How do I request access to Amazon Personalize in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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):

  JSON

```
{
    "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.

  JSON

```
{
"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/*"
]
}
]
}
```

## Use AMS SSP to provision Amazon QuickSight in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access QuickSight capabilities directly in your AMS managed account. QuickSight is a fast, cloud-powered business intelligence service that delivers insights to everyone in your organization. As a fully managed service, QuickSight lets you easily create and publish interactive dashboards that include machine learning (ML) insights. To learn more, see Amazon QuickSight.

### QuickSight in AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request access to QuickSight in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct). 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 QuickSight in my AMS account?**

- AWS resource settings on QuickSight won't be accessible to you because of the IAM policy dependency. However, the AMS team enables each resource for you in response to your request 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.
- 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 QuickSight with Active Directory (AD). QuickSight on AMS does not support integration with AD due to incompatibilities between AMS account structure and the QuickSight trust requirements.

**Q: What are the prerequisites or dependencies to using QuickSight in my AMS account?**

- When AMS receives this RFC to add QuickSight, you are sent a service request for additional information; provide them the following:
  - QuickSight account name (for example, `CustomerName-quicksight`
  - QuickSight Edition (Standard versus Enterprise)
  - The AWS Region in which to enable the QuickSight service (defaults to your AMS AWS Region).
  - A notification email address for QuickSight account.
  - (Optional) The S3 bucket where data files to be analyzed are located.
  - The VPC and subnet IDs that connect to QuickSight support a feature to add a VPC connection, which enables private connectivity between 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.

## Use AMS SSP to provision Amazon Rekognition in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Rekognition capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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 (review required) (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.

## Use AMS SSP to provision Amazon SageMaker AI in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon SageMaker AI capabilities directly in your AMS managed account. SageMaker AI provides every developer and data scientist with the ability to build, train, and deploy machine learning models quickly. Amazon SageMaker AI 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 AI.

### SageMaker AI in AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request access to SageMaker AI in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type. This RFC provisions the following IAM roles to your account: `customer_sagemaker_admin_role` and service role `AmazonSageMaker-ExecutionRole-Admin`. After SageMaker AI is provisioned in your account, you must onboard the `customer_sagemaker_admin_role` role in your federation solution. The service role cannot be accessed by you directly; the SageMaker AI service uses it while doing various actions as described here: Passing Roles.

**Q: What are the restrictions to using SageMaker AI in my AMS account?**

- The following use cases are not supported by the AMS Amazon SageMaker AI IAM role:
  - SageMaker AI Studio is not supported at this time.
  - SageMaker AI 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 AI 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 AI 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 AI related services only. To support this use case, submit a Management | Other | Other RFC to create related VPC endpoints.
- SageMaker AI endpoint auto scaling is not supported as SageMaker AI requires `DeleteAlarm` permissions on any ("*") resource. To support endpoint auto scaling, submit a Management | Other | Other RFC to setup auto scaling for a SageMaker AI endpoint.

**Q: What are the prerequisites or dependencies to using SageMaker AI 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 AI 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 AI self-provisioned service role supports your use of the SageMaker AI 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 AWS RoboMaker, Amazon Cognito, and AWS Glue resources.
- SageMaker AI 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 AWS KMS customer managed key in data encryption at rest?**

You must ensure that the key policy has been set up properly on the customer managed keys so that related IAM users or roles can use the keys. For more information, see the AWS KMS Key Policy document.

# Use AMS SSP to provision Amazon Simple Email Service in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Simple Email Service (Amazon SES) capabilities directly in your AMS managed account. Amazon Simple Email Service 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 AWS Managed Services FAQ

**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-1w8z66n899dct) 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 such as Amazon S3, Amazon 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 your Amazon 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 adds them to Secrets Manager for you.

## Use AMS SSP to provision Amazon Simple Workflow Service in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Simple Workflow Service (Amazon SWF) capabilities directly in your AMS managed account. Amazon Simple Workflow Service 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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.

## Use AMS SSP to provision Amazon Textract in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Textract capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request Amazon Textract to be set up in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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).

## Use AMS SSP to provision Amazon Transcribe in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Amazon Transcribe capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request Amazon Transcribe to be set up in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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.

## Use AMS SSP to provision Amazon WorkSpaces in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access WorkSpaces capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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 (review required) (ct-3qe6io8t6jtny) change type. 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.

## Use AMS SSP to provision AMS Code services in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AMS Code services capabilities directly in your AMS managed account. AMS Code services is a proprietary bundling of AWS code management services as detailed next. You can choose to deploy all of the services in AMS with AMS Code services, or you can deploy them in AMS individually.

AMS Code services 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

  To deploy this in your AMS account independently of AMS Code services, see Use AMS SSP to provision AWS CodeCommit in your AMS account.
- 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

  To deploy this in your AMS account independently of AMS Code services, see Use AMS SSP to provision AWS CodeBuild in your AMS account.
- 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

  To deploy this in your AMS account independently of AMS Code services, see Use AMS SSP to provision AWS CodeDeploy in your AMS account.

- 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 deploy this in your AMS account independently of AMS Code services, see Use AMS SSP to provision AWS CodePipeline in your AMS account.

## AMS Code services in AWS Managed Services FAQ

### Q: How do I request access to AMS Code services in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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 Use AMS SSP to provision AWS CodeBuild in your AMS account, Use AMS SSP to provision AWS CodeDeploy in your AMS account, and Use AMS SSP to provision AWS CodePipeline in your AMS account, respectively.

### Q: What are the restrictions to using AMS Code services 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 deploys the `customer_code_pipeline_lambda_policy` in your account; it must be attached with the Lambda execution role for Lambda invoke stage. Provide the Lambda service/execution role name that you want this policy added with. If there is no custom Lambda service/execution role, then AMS creates a new role named `customer_code_pipeline_lambda_execution_role`, that is 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 Code services 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 is done by an AMS engineer.

## Use AMS SSP to provision AWS Amplify in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Amplify capabilities directly in your AMS managed account. The AWS Amplify is a complete solution that allows frontend web and mobile developers to easily build, connect, and host fullstack applications. Amplify provides flexibility to leverage the breadth of AWS services as your use cases evolve. Amplify provides products to build fullstack iOS, Android, Flutter, Web, and React Native apps. To learn more, see AWS Amplify.

### AWS Amplify in AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request AWS Amplify to be set up in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_amplify_console_role`. After provisioned to your account, you must onboard the role in your federation solution.

Additionally, you must provide a Risk Acceptance because AWS Amplify has infrastructure-mutating permissions. To do this, work with your Cloud Service Delivery Manager (CSDM).

**Q: What are the restrictions to using AWS Amplify in my AMS account?**

You must use `'amplify*'` as the prefix for your buckets when working with Amplify, unless RA and specified otherwise.

**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.

**Malz environments only**: The default onboarded role for Amplify is "customer_amplify_console_role". To use a custom role, first deploy the IAM entities. Then, create an additional RFC to add your custom role to the Service Control Policy for Application Accounts allow list.

# Use AMS SSP to provision AWS AppSync

Use AMS Self-Service Provisioning (SSP) mode to access AWS AppSync capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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.

# Use AMS SSP to provision AWS App Mesh in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS App Mesh capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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.

# Use AMS SSP to provision AWS Audit Manager in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Audit Manager capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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 | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny). This RFC provisions the following IAM role in your account: `customer-audit-manager-admin-Role`. After 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 is 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)

# Use AMS SSP to provision AWS Batch in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Batch capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request access to AWS Batch in my AMS account?**

1. To request access to AWS Batch, submit the RFC Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). This RFC provisions the following IAM roles and policies in your account:

IAM roles:

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`
- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

Policies:

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`
- `customer_batch_events_service_role_policy`

2. After 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.

## Use AMS SSP to provision AWS Certificate Manager in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Certificate Manager (ACM) capabilities directly in your AMS managed account. AWS Certificate Manager 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 Private Certificate Authority, you pay monthly for the operation of the AWS Private CA and for the private certificates you issue. To learn more, see AWS Certificate Manager - AWS Documentation.

### ACM in AWS Managed Services FAQ

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-1w8z66n899dct). 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 | Create Public Certificate
- ACM | Create Private Certificate
- ACM Certificate with additional SANs | Create

**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.

## Use AMS SSP to provision AWS Private Certificate Authority in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Private Certificate Authority capabilities directly in your AMS managed account. Private certificates are used for identifying and securing communication between connected resources on private networks, such as servers, mobile, and IoT devices and applications. AWS Private CA is a managed private CA service that helps you easily and securely manage the lifecycle of your private certificates. AWS Private CA provides you a highly-available private CA service without the upfront investment and ongoing maintenance costs of operating your own private CA. AWS 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 AWS Private CA.

## AWS Private CA in AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request access AWS 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 AWS Private CA?**

Currently, AWS Resource Access Manager (AWS RAM) cannot be used to share your AWS Private CA cross-account.

**Q: What are the prerequisites or dependencies to using AWS Private CA?**

1. If you plan to create a CRL, you need an S3 bucket to store it in. AWS 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.

JSON

```
{
   "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. AWS 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 AWS 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.

## Use AMS SSP to provision AWS CloudEndure in your AMS account

> **Note**
>
> Following the successful launch of AWS Application Migration Service, the CloudEndure Migration service is now end of life in all AWS Regions. We recommend customers use AWS Application Migration Service for lift and shift migrations to GovCloud Regions and to the Commercial Regions. For information, see What Is AWS Application Migration Service?.
> If you want to use the AWS Application Migration Service, reach out to your CA so they can guide you.

Use AMS Self-Service Provisioning (SSP) mode to access AWS CloudEndure capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

#### Q: How do I request access to CloudEndure in my AMS account?

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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.

## Use AMS SSP to provision AWS CloudHSM in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS CloudHSM capabilities directly in your AMS managed account. AWS CloudHSM 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 AWS Managed Services FAQ

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-1w8z66n899dct) 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.

# Use AMS SSP to provision AWS CodeBuild in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS CodeBuild capabilities directly in your AMS managed account. 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 RFC, submit the Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type and request the three services: CodeBuild, CodeDeploy and CodePipeline. Then, all three roles, `customer_codebuild_service_role`, `customer_codedeploy_service_role`, and `aws_code_pipeline_service_role` are provisioned in your account. After provisioning in your account, you must onboard the role in your federation solution.

## CodeBuild in AWS Managed Services FAQ

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-1w8z66n899dct). 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.

## Use AMS SSP to provision AWS CodeCommit in your AMS account

> **Note**
>
> AWS has closed new customer access to AWS CodeCommit, effective July 25, 2024. AWS CodeCommit existing customers can continue to use the service as normal. AWS continues to invest in security, availability, and performance improvements for AWS CodeCommit, but we do not plan to introduce new features.
> To migrate AWS CodeCommit Git repositories to other Git providers, reach out to your cloud architect (CA) for guidance. For more information on migrating your Git repositories, see How to migrate your AWS CodeCommit repository to another Git provider.

Use AMS Self-Service Provisioning (SSP) mode to access AWS CodeCommit capabilities directly in your AMS managed account. 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 RFC, submit the Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type and request the three services: CodeBuild, CodeDeploy and CodePipeline. Then, all three roles, `customer_codebuild_service_role`, `customer_codedeploy_service_role`, and `aws_code_pipeline_service_role` are

provisioned in your account. After provisioning in your account, you must onboard the role in your federation solution.

## CodeCommit in AWS Managed Services FAQ

**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-1w8z66n899dct) 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.

# Use AMS SSP to provision AWS CodeDeploy in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS CodeDeploy capabilities directly in your AMS managed account. 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 RFC, submit the Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type and request the three services: CodeBuild, CodeDeploy and CodePipeline. Then, all three roles, `customer_codebuild_service_role`, `customer_codedeploy_service_role`, and `aws_code_pipeline_service_role` are provisioned in your account. After provisioning in your account, you must onboard the role in your federation solution.

### CodeDeploy in AWS Managed Services FAQ

**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-1w8z66n899dct) change type. This RFC provisions the following IAM roles to your account: `customer_codedeploy_console_role` and `customer_codedeploy_service_role`. After it's provisioned in your account, you must onboard the `customer_codedeploy_console_role` 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. Blue/Green Deployments are not supported.

**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.

## Use AMS SSP to provision AWS CodePipeline in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS CodePipeline capabilities directly in your AMS managed account. 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 RFC, submit the Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type and request the three services: CodeBuild, CodeDeploy and CodePipeline. Then, all three roles, `customer_codebuild_service_role`, `customer_codedeploy_service_role`, and `aws_code_pipeline_service_role` are provisioned in your account. After provisioning in your account, you must onboard the role in your federation solution.
> 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 AWS Managed Services FAQ

**Q: How do I request access to CodePipeline in my AMS account?**

Request access to CodePipeline by submitting a service request for the `customer_code_pipeline_console_role` in the relevant account. 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.

## Use AMS SSP to provision AWS Compute Optimizer in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Compute Optimizer capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**Q: How do I request access to Compute Optimizer in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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

## Use AMS SSP to provision AWS DataSync in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS DataSync capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**Q: How do I request access to DataSync in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_datasync_console_role`.

After 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?**

- Amazon S3 ARNs (Amazon Resource Names) are required for all S3 buckets associated with DataSync tasks that will be performed using the DataSync service role `customer_datasync_service_role`.
- 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 FAQ.

- To launch an AWS DataSync agent, submit an RFC with the Management | Other | Other | Create (ct-1e1xtak34nx76) change type, requesting the 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.

> **Note**
>
> AMS provisions the AWS DataSync agent manually on behalf of customer, and doesn't require the WIGS ingestion process on the AWS DataSync Amazon EC2 AMI.

## Use AMS SSP to provision AWS Device Farm in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Device Farm capabilities directly in your AMS managed account. AWS Device Farm is an application testing service that lets you improve the quality of your web and mobile apps by testing them across an extensive range of desktop browsers and real mobile devices; without having to provision and manage any testing infrastructure. The service enables you to run your tests concurrently on multiple desktop browsers or real devices to speed up the execution of your test suite, and generates videos and logs to help you quickly identify issues with your app.

To learn more, see AWS Device Farm.

### AWS Device Farm in AWS Managed Services FAQ

**Q: How do I request access to AWS Device Farm in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_devicefarm_role`.

Once provisioned in your account, you must onboard the roles in your federation solution.

**Q: What are the restrictions to using AWS Device Farm in my AMS account?**

Full access to the AWS Device Farm service is provided with the exception of using the AMS namespace in the 'Name' tag.

**Q: What are the prerequisites or dependencies to using AWS Device Farm in my AMS account?**

None.

## Use AMS SSP to provision AWS Elastic Disaster Recovery in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Elastic Disaster Recovery capabilities directly in your AMS managed account. AWS Elastic Disaster Recovery minimizes downtime and data loss with fast, reliable recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery. You can increase IT resilience when you use AWS Elastic Disaster Recovery to replicate on-premises or cloud-based applications running on supported operating systems. Use the AWS Management Console to configure replication and launch settings, monitor data replication, and launch instances for drills or recovery.

To learn more, see AWS Elastic Disaster Recovery.

### AWS Elastic Disaster Recovery in AWS Managed Services FAQ

**Q: How do I request access to AWS Elastic Disaster Recovery in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer_drs_console_role`.

After its provisioned in your account, you must onboard the role in your federation solution.

**Q: What are the restrictions to using AWS Elastic Disaster Recovery in my AMS account?**

There are no restrictions to use AWS Elastic Disaster Recovery in your AMS account.

**Q: What are the prerequisites or dependencies to using AWS Elastic Disaster Recovery in my AMS account?**

- After you have access to the console role, you must initialize the Elastic Disaster Recovery service to create the needed IAM roles within the account.
  - You must submit a Management | Other | Other RFC to create a clone of the `customer-mc-ec2-instance-profile` instance profile and attach the `AWSElasticDisasterRecoveryEc2InstancePolicy` policy. You must specify which machines to attach the new policy to.
  - If the instance isn't using the default instance profile, then AMS can attach `AWSElasticDisasterRecoveryEc2InstancePolicy` through automation.

- You must use a customer-owned KMS key for cross-account recovery. The source account's KMS key must be updated following the policy to allow target account access. For more information, see Share the EBS encryption key with the target account.
- The KMS key policy must be updated to allow the allow `customer_drs_console_role` to view the policy if you don't want to switch roles to view.
- For cross-account, cross-Region disaster recovery, AMS must set up the source and target account as Trusted Accounts and deploy the Failback and in-AWS right-sizing roles through AWS CloudFormation.

## Use AMS SSP to provision AWS Elemental MediaConvert in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Elemental MediaConvert capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**Q: How do I request access to MediaConvert in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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.

# Use AMS SSP to provision AWS Elemental MediaLive in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Elemental MediaLive capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**Q: How do I request access to MediaLive in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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.

## Use AMS SSP to provision AWS Elemental MediaPackage in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Elemental MediaPackage capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**Q: How do I request access to AWS Elemental MediaPackage in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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.

## Use AMS SSP to provision AWS Elemental MediaStore in your AMS account

> **Note**
>
> After careful consideration, AWS has made the decision to discontinue MediaStore, effective November 13, 2025. If you are an active customer of MediaStore, you can use MediaStore as normal until November 13, 2025, when support for the service will end. After this date, you will no longer be able to use MediaStore or any of the capabilities provided by this service.

Use AMS Self-Service Provisioning (SSP) mode to access AWS Elemental MediaStore capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**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-1w8z66n899dct) 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.

# Use AMS SSP to provision AWS Elemental MediaTailor in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Elemental MediaTailor capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**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-1w8z66n899dct) 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.

# Use AMS SSP to provision AWS Global Accelerator in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Global Accelerator capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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.

# Use AMS SSP to provision AWS Glue in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Glue capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct). This RFC provisions the following IAM roles to your account:

- `customer_glue_console_role`
- `customer_glue_service_role`

The preceding roles include the following attached policies:

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

After the roles are provisioned in your account, you must onboard them 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. For an interactive environment where you can author and test ETL scripts, use Notebooks on AWS Glue Studio. AWS Glue Interactive Sessions and Job Notebooks are serverless features of AWS Glue that you can use in AWS Glue and that make use of the AWS Glue service role.

**AWS Glue prior to 2.0:** AWS Glue Notebooks are a non-managed resource that launches Amazon EC2 instances in an account. It's a best practice to 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).

## Use AMS SSP to provision AWS Lake Formation in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Lake Formation capabilities directly in your AMS managed account. 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 FAQ) 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 AWS Managed Services FAQ

**Q: How do I request access to AWS Lake Formation in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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.

Additionally, the following two roles are optional:

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

For admin permissions, you can choose to onboard the role `customer_lakeformation_admin_role` as part of the same SSPS change type (ct-3qe6io8t6jtny).

If you want to create Blueprints in the AWS Lake Formation Console, you need to submit a Management | Other | Other RFC (ct-1e1xtak34nx76) to deploy the `customer_lakeformation_workflow_role`. In the RFC, you must provide the S3 bucket name if the bucket is a source when Blueprints are created. S3 bucket is applicable if the Blueprint type is AWS CloudTrail, Classic Load Balancer Logs or Application Load Balancer Logs.

**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.

## Use AMS SSP to provision AWS Lambda in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Lambda capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**Q: How do I request access to AWS Lambda in my AMS account?**

Request access by submitting a Management | AWS service | Self-provisioned service | Add (review required) (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 isn't available, then work with your AMS CSDM to file an exception.
- By default AMS provides 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 | AWS service | Self-provisioned service | Add (review required)(ct-3qe6io8t6jtny) change type.

**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 might require access to other AWS services 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 | AWS service | Self-provisioned service | Add (review required) change type (ct-3qe6io8t6jtny).

**Q: What do I need to do to run a Lambda function in any of my accounts?**

To deploy a Lambda function in a core account, use the following guidelines:

- Make sure that SSPS for AWS Lambda is onboarded.
- There are no specific restrictions prohibiting this deployment under the AMS responsibilities, as long as your AMS resources are protected and compliant.
- If you want AMS to create the Lambda function, then you must first use the SSPS role provided for AWS Lambda. Then, if you still want AMS assistance to deploy or support the function, contact your CA and start the out of scope (OOS) process.

## Use AMS SSP to provision AWS License Manager in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS License Manager capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct) 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.

## Use AMS SSP to provision AWS Migration Hub in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Migration Hub capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct) 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?**

None.

**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.

## Use AMS SSP to provision AWS Outposts in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Outposts capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct) 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.

# Use AMS SSP to provision AWS Resilience Hub in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Resilience Hub capabilities directly in your AMS managed account. AWS Resilience Hub helps you proactively prepare and protect your AWS applications from disruptions. The Resilience Hub offers resiliency assessment and validation that integrate into your software development lifecycle to uncover resiliency weaknesses. Resilience Hub helps you estimate whether or not your applications can meet the recovery time objective (RTO) and recovery point objective (RPO) targets, and helps resolve issues before they are released into production. After you deploy an AWS application into production, you can use Resilience Hub to continue tracking the resiliency posture of your application. If an outage occurs, Resilience Hub sends a notification to the operator to launch the associated recovery process.

## AWS Resilience Hub in AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request access to AWS Resilience Hub in my AMS account?**

Request access to Resilience Hub by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type. This RFC provisions the following IAM roles and policies to your account:

**IAM roles**

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

**Policies**

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

After the role is provisioned in your account, you must onboard the role `customer_resiliencehub_console_role` in your federation solution.

**Q: What are the restrictions to using AWS Resilience Hub in my AMS account?**

There are no restrictions. Full functionality of Resilience Hub is available in your AMS acount.

**Q: What are the prerequisites or dependencies to using AWS Resilience Hub in my AMS account?**

There are no prerequisites or dependencies to use Resilience Hub in your AMS account.

## Use AMS SSP to provision AWS Secrets Manager in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Secrets Manager capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

**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?**

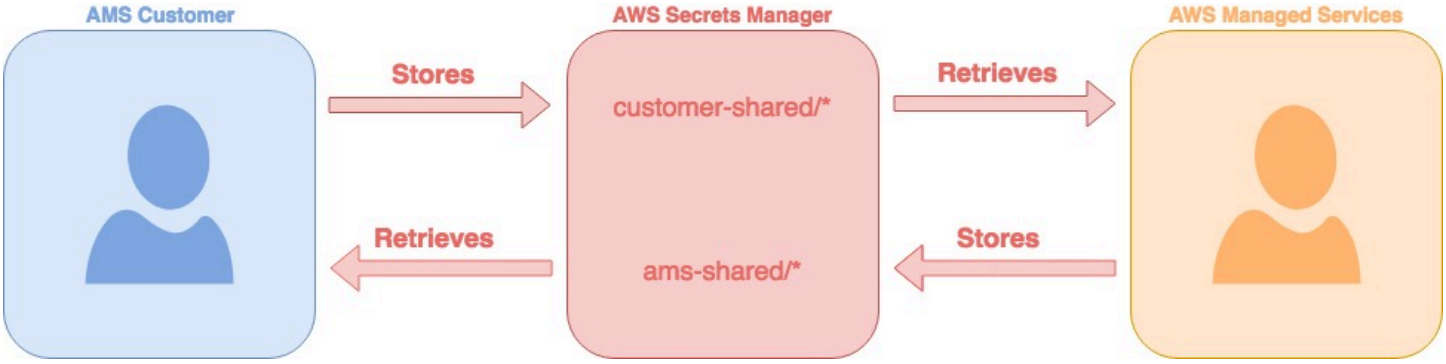
The following namespaces are reserved for use by AMS and are unavailable as part of direct access to AWS Secrets Manager:

- arn:aws:secretsmanager:*:*:secret:ams-shared/*
- arn:aws:secretsmanager:*:*:secret:customer-shared/*
- arn:aws:secretsmanager:*:*:secret:ams/*

## Sharing keys using Secrets Manager (AMS SSPS)

Sharing secrets with AMS in the plain text of an RFC, service request, or incident report, results in an information disclosure incident and AMS redacts that information from the case and requests that you regenerate the keys.

You can use AWS Secrets Manager (Secrets Manager) under this namespace, `customer-shared`.



### Sharing Keys using Secrets Manager FAQ

**Q: What type of secrets must be shared using Secrets Manager?**

A few examples are pre-shared keys for VPN creation, confidential keys such as Authentication keys (IAM, SSH), License keys and Passwords.

**Q: How can I share the keys with AMS using Secrets Manager?**

1. Login to the AWS Management console using your federated access and the appropriate role:

   for SALZ, the `Customer_ReadOnly_Role`

   for MALZ, `AWSManagedServicesChangeManagementRole`.
2. Navigate to the AWS Secrets Manager console and click **Store a new secret**.
3. Select **Other type of secrets**.
4. Enter the secret value as a plain-text and use the default KMS encryption. Click **Next**.
5. Enter the secret name and description, the name always starts with **customer-shared/**. For example **customer-shared/mykey2022**. Click **Next**.
6. Leave automatic rotation disabled, Click **Next**.
7. Review and click **Store** to save the secret.
8. Reply to us with the secret name through the Service request, RFC, or incident report, so we can identify and retrieve the secret.

**Q: What permissions are required for sharing the keys using Secrets Manager?**

**SALZ**: Look for the `customer_secrets_manager_shared_policy` managed IAM policy and verify that the policy document is the same as the one attached in the creation steps below. Confirm that the policy is attached to the following IAM Roles: `Customer_ReadOnly_Role`.

**MALZ**: Validate that the `AMSSecretsManagerSharedPolicy`, is attached to the `AWSManagedServicesChangeManagementRole` role that allows you the `GetSecretValue` action in the `ams-sharednamespace`.

Example:

```
{
```

```
"Action": "secretsmanager:*",
"Resource": [
"arn:aws:secretsmanager:*:*:secret:ams-shared/*",
"arn:aws:secretsmanager:*:*:secret:customer-shared/*"
],
"Effect": "Allow",
"Sid": "AllowAccessToSharedNameSpaces"
}
```

> **Note**
>
> The requisite permissions are granted when you add AWS Secrets Manager as a self-service provisioned service.

## Use AMS SSP to provision AWS Security Hub in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Security Hub capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

#### 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-1w8z66n899dct) 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.

## Use AMS SSP to provision AWS Service Catalog AppRegistry in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AppRegistry capabilities directly in your AMS managed account. AppRegistry enables application search, reporting, and management actions from a central location. Builders seldom create applications in a single AWS account. They typically separate application resources by lifecycle phases, such as development, test, and production. AppRegistry allows you to group and view all your resource collections across the AWS accounts that you define.

With AppRegistry, you can store your AWS applications, the collection of resources that are associated with your applications, and application attribute groups. To learn more, see What is AppRegistry.

### FAQ: AWS Service Catalog AppRegistry in AMS

**Q: How do I request access to AWS Service Catalog AppRegistry in my AMS account?**

Request access to AppRegistry by submitting an RFC with the Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) change type. This RFC provisions the following IAM role to your account: `customer-appregistry-console-role`. After provisioned in your account, you must onboard the role in your federation solution.

**Q: What are the restrictions to using AWS Service Catalog AppRegistry in my AMS account?**

Full access to the AppRegistry service is provided with the exception of using the AMS namespace in the `'Name'` tag.

**Q: What are the prerequisites or dependencies to using AWS Service Catalog AppRegistry in my AMS account?**

There are no prerequisites or dependencies to use AppRegistry in your AMS account.

## Use AMS SSP to provision AWS Shield Advanced in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Shield Advanced capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

### 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-1w8z66n899dct) 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.

## Use AMS SSP to provision AWS Snowball Edge in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access Snowball Edge capabilities directly in your AMS managed account. Snowball Edge 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 Edge addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. You can use Snowball Edge 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 Edge 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 Edge, 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 Edge.

## Snowball Edge in AWS Managed Services FAQ

Common questions and answers:

**Q: How do I request access to AWS Snowball Edge in my AMS account?**

Implementation of Snowball Edge 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 Edge for your AMS Account.
2. Request user access by submitting a Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct). This RFC provisions the following IAM roles 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 Edge in my AMS account?**

Full functionality of the AWS Snowball Edge is available in your AMS account.

**Q: What are the prerequisites or dependencies to using AWS Snowball Edge in my AMS account?**

You must have the service role account as noted above.

# Use AMS SSP to provision AWS Step Functions in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Step Functions capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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.

## Use AMS SSP to provision AWS Systems Manager Parameter Store in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Systems Manager Parameter Store capabilities directly in your AMS managed account. 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 Use AMS SSP to provision AWS Secrets Manager in your AMS account 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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.

## Use AMS SSP to provision AWS Systems Manager Automation in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Systems Manager Automation capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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 |
| 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.

## Use AMS SSP to provision AWS Transfer Family in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Transfer Family (Transfer Family) capabilities directly in your AMS managed account. AWS 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, also Create an SFTP-enabled server.

## AWS Transfer for SFTP in AWS Managed Services FAQ

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-1w8z66n899dct). 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.
- `customer_transfer_sftp_efs_user_role`. This role is designed to be attached on the SFTP users. It allows the SFTP users to interact with the EFS file system.

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 Amazon S3 bucket with a name that contains the keyword "transfer" before creating the AWS Transfer for SFTP server and users.
- To 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.

## Use AMS SSP to provision AWS Transit Gateway in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Transit Gateway capabilities directly in your AMS managed account. AWS Transit Gateway is a service that enables you to connect your Amazon Virtual Private Cloud (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.

### AWS Transit Gateway in AWS Managed Services FAQ

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-1w8z66n899dct). 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 Transit Gateway 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.

## Use AMS SSP to provision AWS WAF - Web Application Firewall in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS WAF capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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.

## Use AMS SSP to provision AWS Well-Architected Tool in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS Well-Architected Tool capabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct). 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.

## Use AMS SSP to provision AWS X-Ray in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access AWS X-Ray (X-Ray) capabilities directly in your AMS managed account. AWS 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 AWS Managed Services FAQ

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-1w8z66n899dct) change type. This RFC provisions the following IAM role to your account: `customer_xray_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_xray_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).

## Use AMS SSP to provision VM Import/Export in your AMS account

Use AMS Self-Service Provisioning (SSP) mode to access VM Import/Exportcapabilities directly in your AMS managed account. 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 AWS Managed Services FAQ

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-1w8z66n899dct). This RFC provisions the following IAM policy 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 request for change (RFC, ct-19jq3ulr3g9zg) through which the tools can perform commands from an instance.

# Customer Managed mode

AWS Managed Services (AMS) Customer Managed 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.

## Getting started with Customer Managed mode

The AMS Customer Managed mode is available through a special multi-account landing zone Application account.

For details, including how to create a Customer Managed Application account, see Customer Managed application accounts.

# AMS and AWS Service Catalog

Service Catalog in AWS Managed Services (AMS) 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 Service Catalog in order to deploy approved resources. 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.

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 Service Catalog including security, compliance, provisioning, availability, patch, monitoring, alerting, reporting, incident response, and cost optimization. Utilizing 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.

## Getting started with Service Catalog

To get started with Service Catalog in AMS, submit a service request through the AMS console to request access to 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 Service Catalog. The three IAM roles deployed include a role for IT admins to manage products as 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 Service Catalog will use while launching or updating the your product.

## Service Catalog in AMS before you begin

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

In accounts where 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. Service Catalog will only acknowledge stacks provisioned through Service Catalog. Likewise, services provisioned through Service Catalog will not be modifiable through the AMS RFC process as modification outside of 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 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 Service Catalog. All other provisioning and changes are tracked directly in Service Catalog and are viewable in the Service Catalog console. Furthermore, you can use the **Provisioned Product Plan** feature in 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 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 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:

- Account Creation through Service Catalog
- Ability to launch all AWS Services through 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.
- Service Catalog IT service manager (ITSM) connectors will not communicate with AMS incident reports, and service requests.
- Ability to leverage Service Catalog quick starts and reference architectures without modification. Remember that 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 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 Service Catalog CLI to access Service Catalog in my AMS managed account?**

Yes, Service Catalog APIs are available and enabled through the CLI. Actions from the management of 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 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 Service Catalog?

To migrate your workload to AMS using 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 Service Catalog. How to do this is detailed in AWS Service Catalog - Getting Started.

# AMS Multi-account landing zone (MALZ) onboarding

## MALZ network architecture

### About multi-account landing zone network architecture

Before you start the onboarding process to AWS Managed Services (AMS) Multi-account landing zone (MALZ), it is important to understand the baseline architecture, or landing zone, that AMS creates on your behalf, its components, and functions.

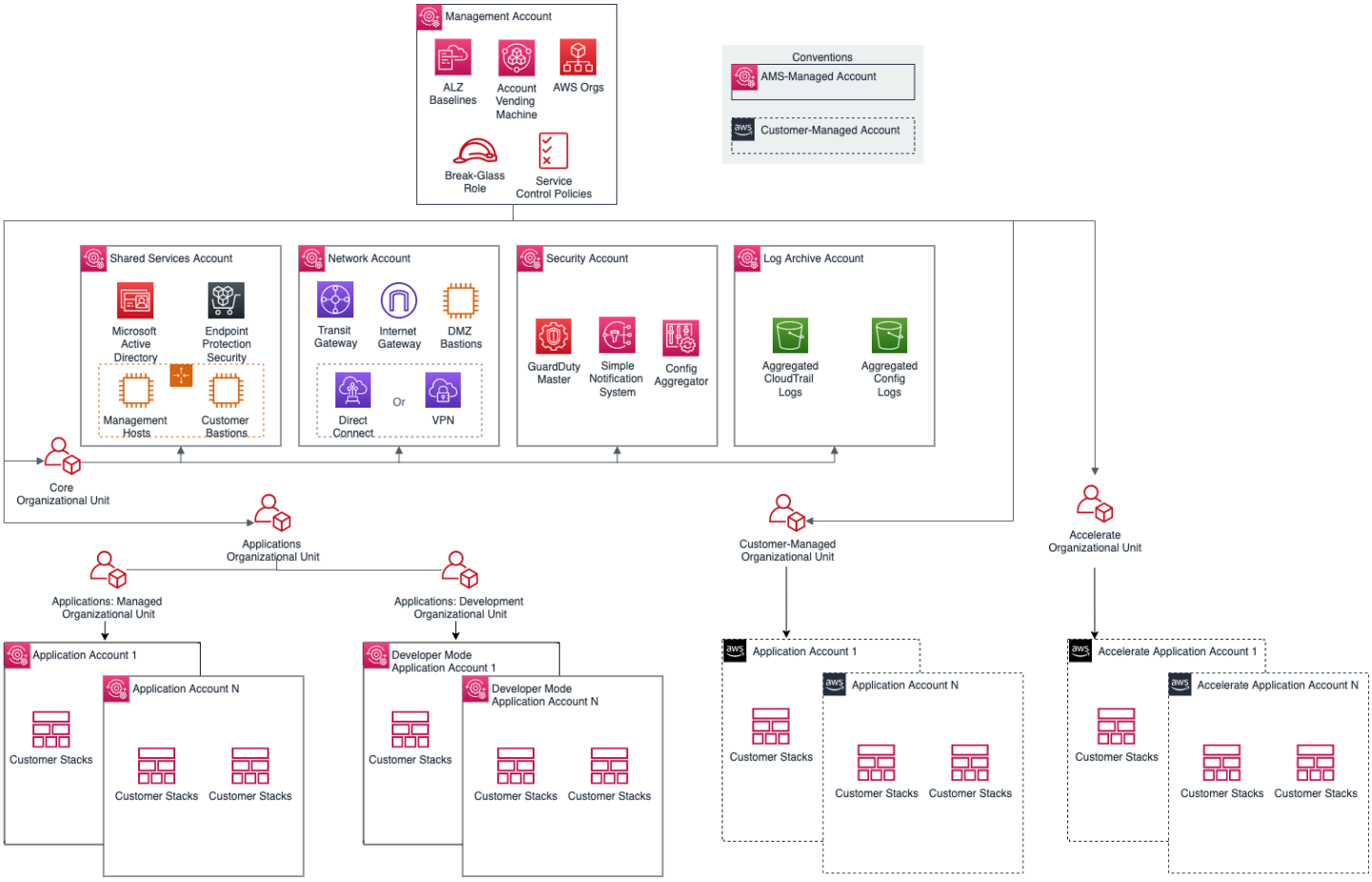
AMS multi-account landing zone is a multi-account architecture, pre-configured with the infrastructure to facilitate authentication, security, networking, and logging.

> **Note**
>
> For estimates of costs, see AMS multi-account landing zone environment basic components.

**Topics**


- Service region
- Organizational units
- Service control policies and AWS Organization


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 four 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
- The accelerate 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 | Create Custom OUs and Management account | Create Custom SCP (review required), respectively. AMS provides four existing OUs under which new OUs and accounts can be requested: accelerate, applications > managed, applications > development, and customer-managed.

- accelerate OU:

  This is a top-level OU in AMS multi-account landing zone (MALZ). Accounts under this OU are provisioned by AMS with an RFC (Deployment | Managed landing zone | Management account | Create Accelerate account, change type ID: ct-2p93tyd5angmi). In these accelerate application accounts, you can benefit from accelerate operational services such as monitoring and alerting, incident management, security management, and backup management. For more details, see AMS Accelerate accounts.

- applications > 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.

- applications > 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 | Create Custom OUs and Management account | Create Custom SCP (Review Required).

## Choosing single MALZ or multiple MALZs

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 environme nt. |
| 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. |
| 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. |

| Entity | Single AMS landing zone | Multiple (two or more) landing zones |
|---|---|---|
| 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 configura bility | 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-acc ount 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. |

| Entity | Single AMS landing zone | Multiple (two or more) landing zones |
|---|---|---|
| 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. |
| 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. |

| Entity | Single AMS landing zone | Multiple (two or more) landing zones |
|---|---|---|
| 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**

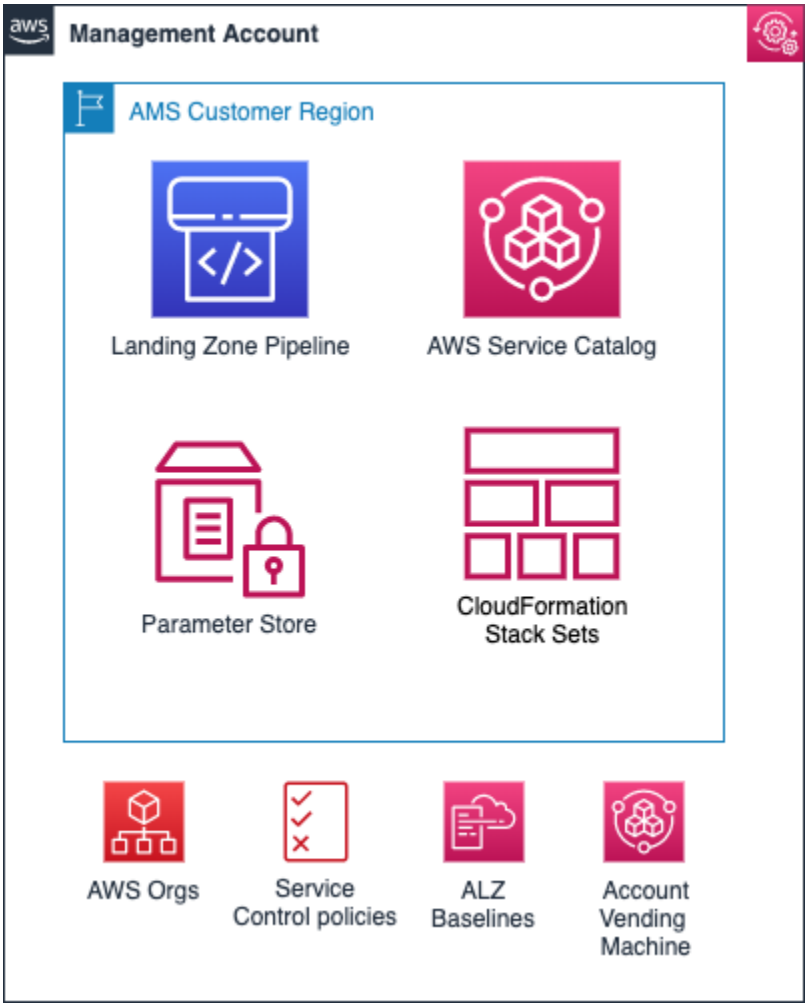

- Management account
- Networking account
- Shared Services account
- Log Archive account
- Security account
- Application account types
- AMS Tools account (migrating workloads)


### Management account

The management account is your initial AWS account when you begin onboarding with AMS. It utilizes AWS Organizations as a management account (also known as the payer account that pays the charges of all the member accounts), 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.

For more information on using a management account, see Best practices for the management account.

The following diagram provides a high-level overview of the resources contained in the management account.



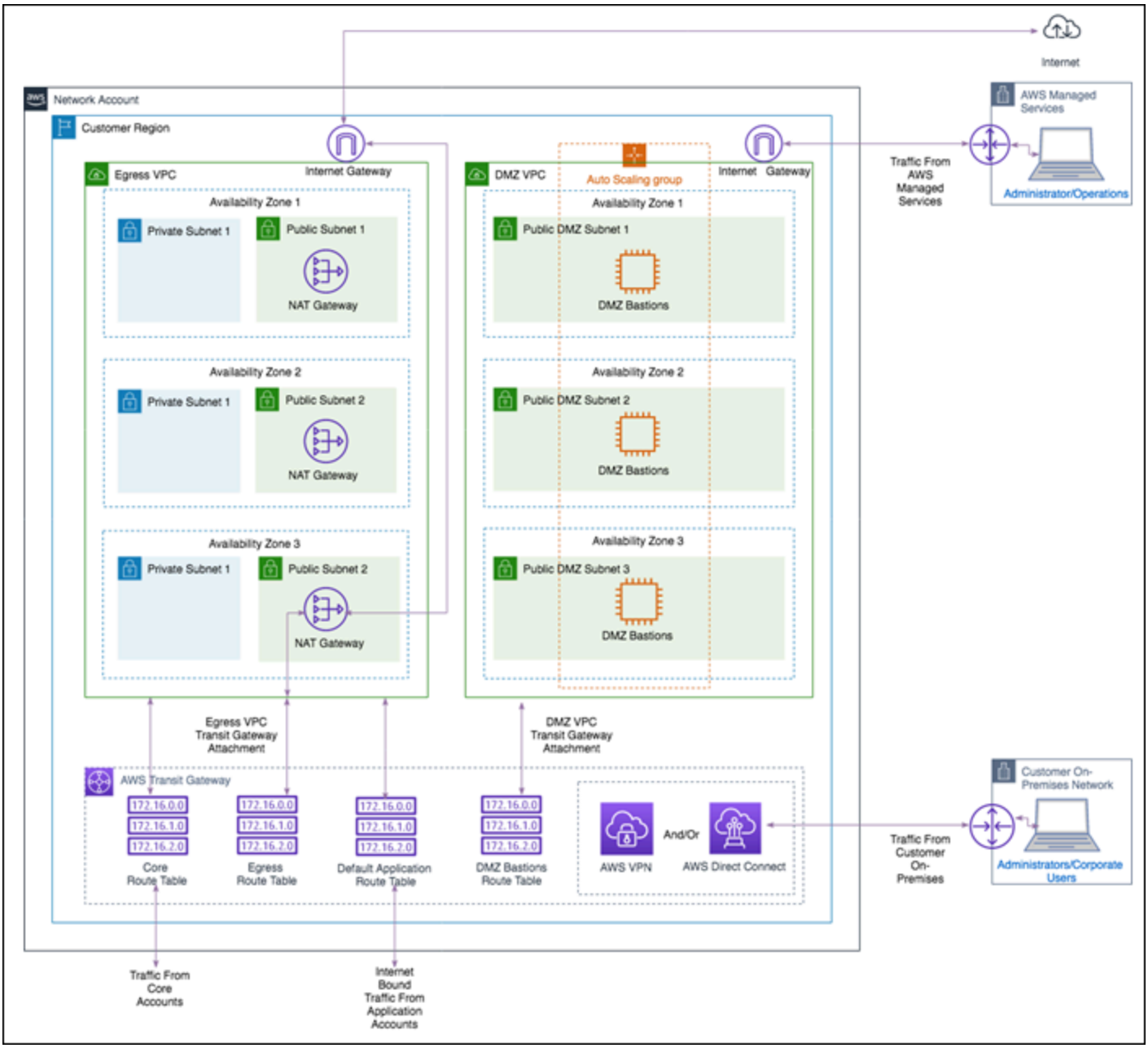

### Resources in the management account

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.

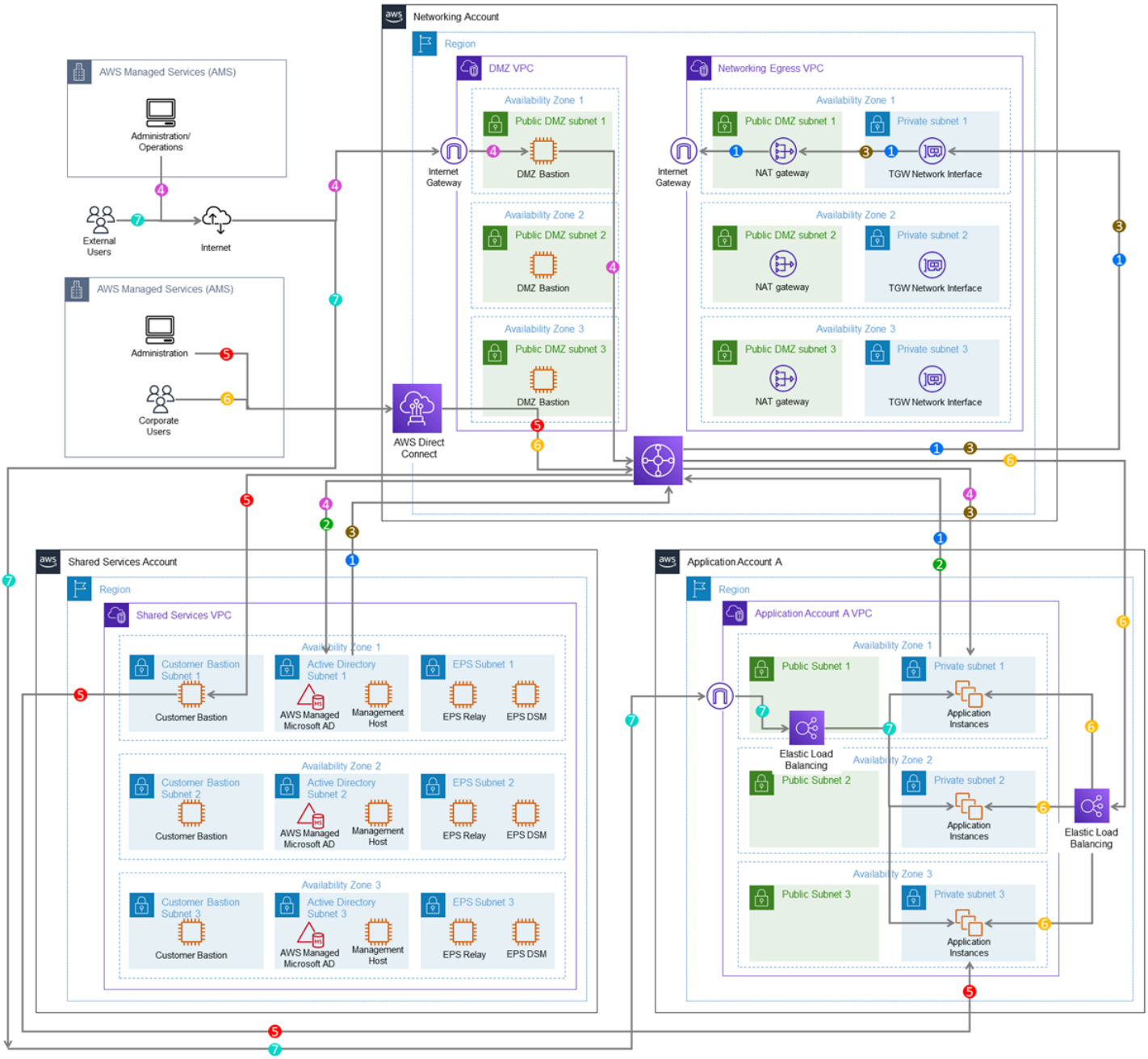
## Networking account

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.



| | |
|---|---|
| 1 | Egress Internet Traffic from Application Account VPC and Shared Services VPC through Egress VPC (Networking Account) and Transit Gateway |
| 2 | Egress Traffic from an Application Account VPC to Shared Services VPC via Transit gateway (Networking Account) |
| 3 | Egress Internal Traffic from Shared Services VPC to Application and Networking Account VPCs via Transit Gateway (Networking Account). |
| 4 | 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) |
| 5 | Ingress through DirectConnect (internal customer network administrators) and Customer Bastions to Application Account's VPC instances via Transit Gateway (Networking Account) |
| 6 | Ingress through DirectConnect (internal customer network users) for Corporate Users to Application Instances in Application Account VPCs via Transit Gateway (Networking Account). |
| 7 | 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**

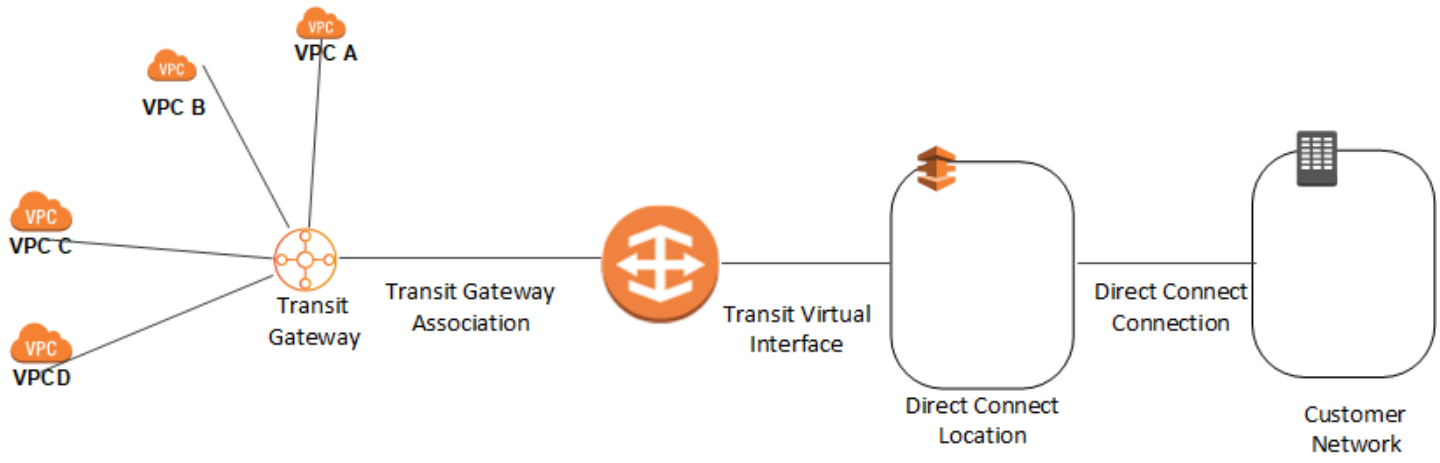
AWS Transit Gateway is a service that enables you to connect your VPCs and your on-premises networks to a single gateway. Transit gateway (TGW) can be used to consolidate your existing edge connectivity and route it through a single ingress/egress point. Transit gateway is created in the networking account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

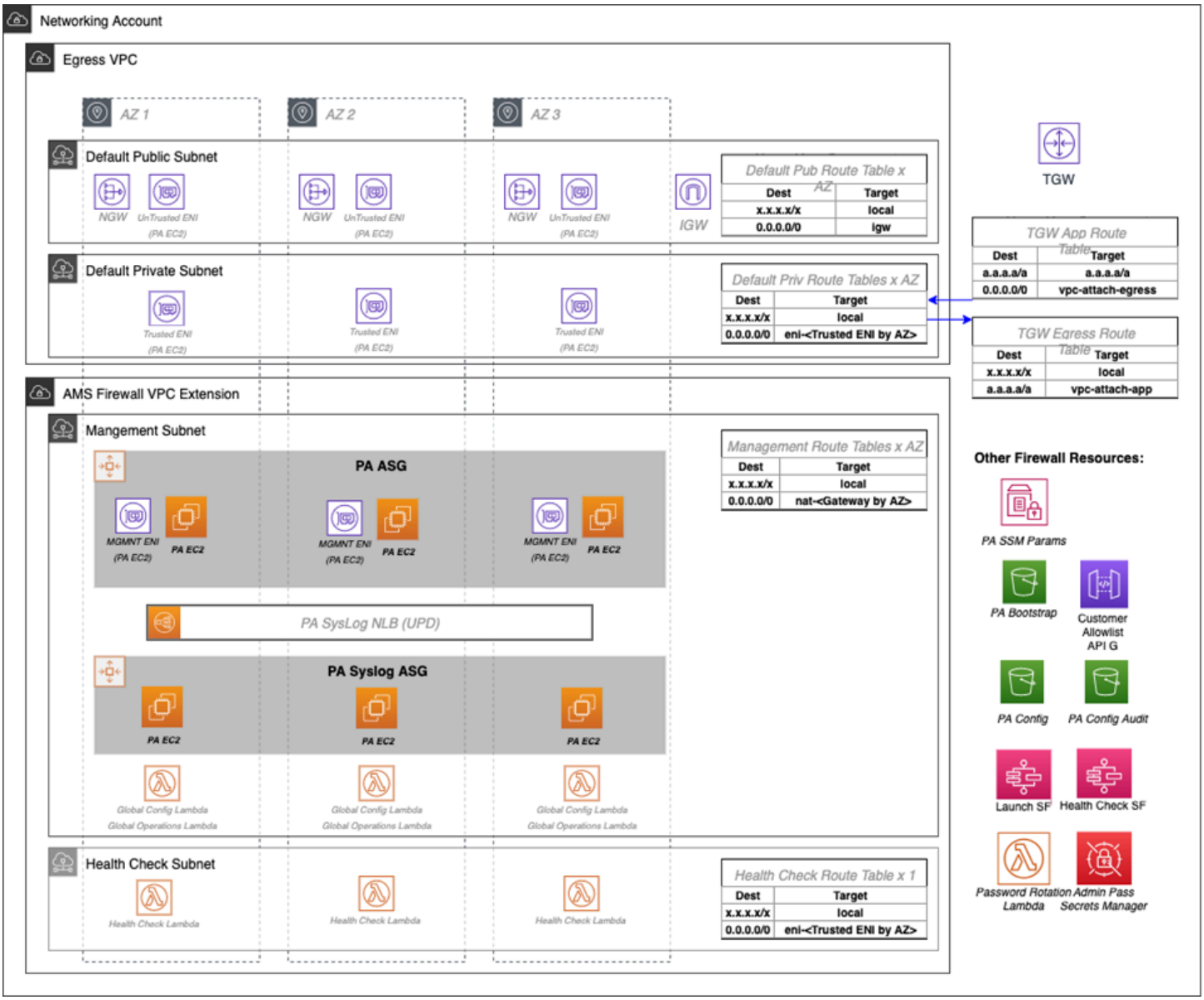
### Traffic control

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

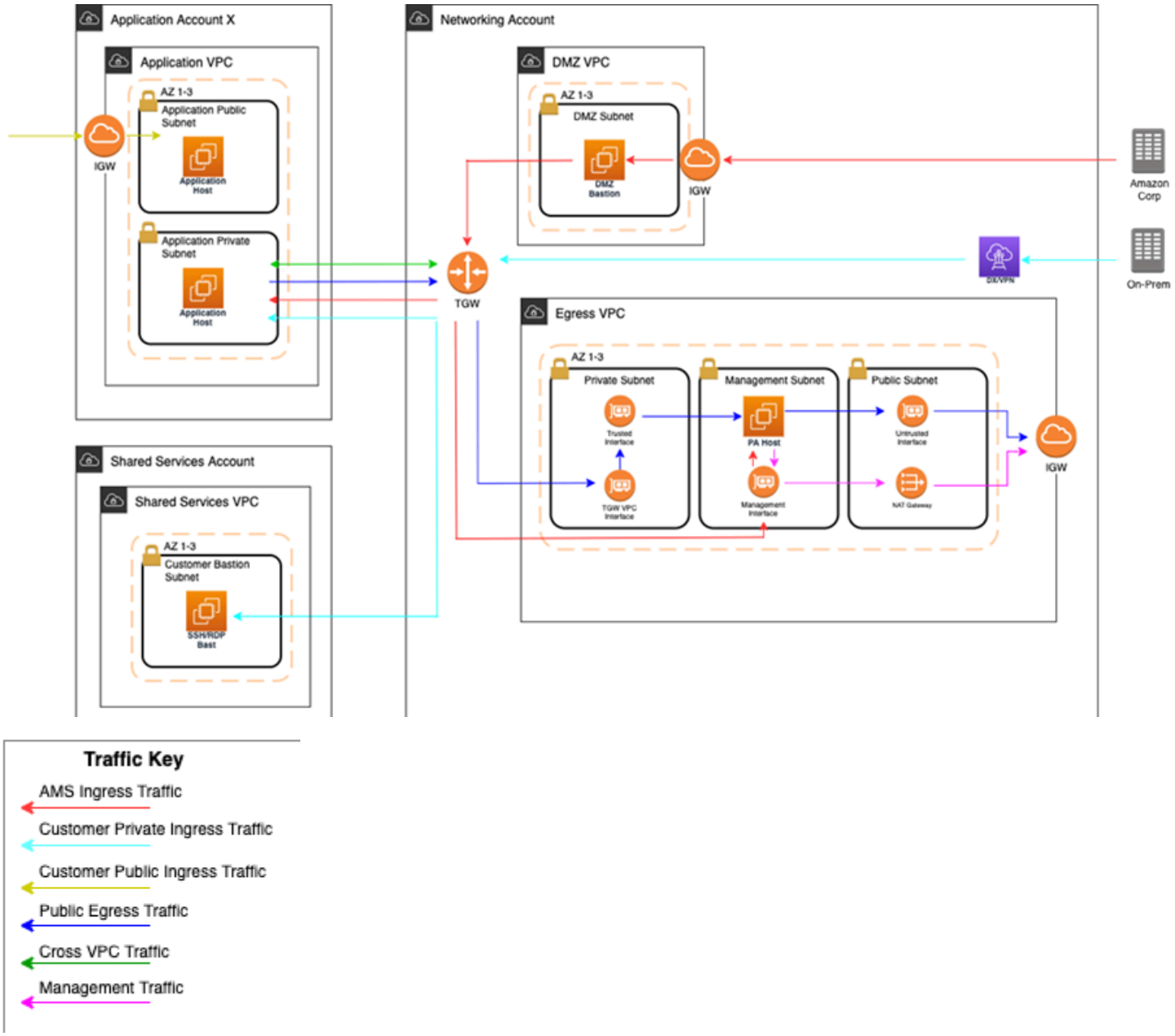
internet traffic is routed to the firewall, a session is opened, traffic is evaluated, and if it matches an allowed domain, the traffic is forwarded to the destination.

## 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. 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.

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.

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.<br><br>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.<br><br>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.<br><br>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. |

| Log Type | Description |
| --- | --- |
| 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.<br><br>Optionally, users can configure Authentication rules to Log Authentic ation 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. |

| Log Type | Description |
| --- | --- |
| Unified | Displays the latest Traffic, Threat, URL Filtering, WildFire Submissio ns, 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

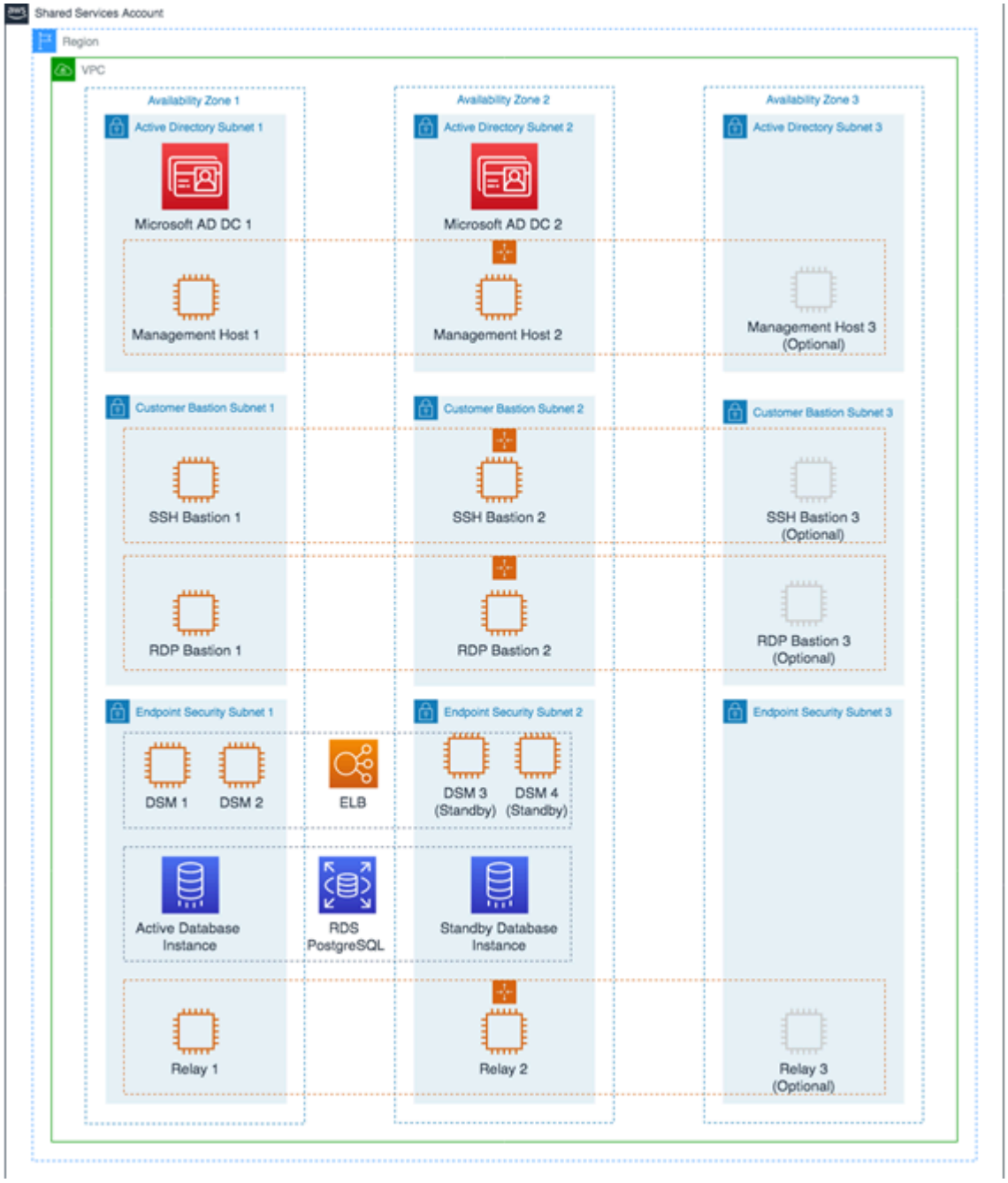
AWS Transit Gateway (TGW) is a service that enables you to connect your Amazon Virtual Private Clouds (VPCs) and your on-premises networks to a single gateway. Transit gateway is the networking backbone that handles the routing between AMS account networks and external networks. For information about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

**Updates to shared services: Multi-Account Landing Zone**

AMS applies data plane releases to managed accounts on a monthly basis, without prior notice.

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.

## 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 account types

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:

- AMS-managed application accounts
- AMS Accelerate accounts
- Customer Managed application accounts

Application accounts are grouped in different OUs in AWS Organizations depending on the Application account type:

- Root OU:
  1. Applications OU
     - Managed OU: AMS-managed accounts
     - Development OU: AMS-managed accounts with Developer mode enabled
  2. Accelerate OU: AMS Accelerate Application accounts
  3. Customer-managed OU: Customer-managed Application accounts

Application accounts are provisioned through an RFC submitted from the Management account:

- Create Application Account With VPC ct-1zdasmc2ewzrs
- Create Accelerate Account ct-2p93tyd5angmi
- Create Customer-Managed Application Account ct-3pwbixz27n3tn

**AMS-managed application accounts**

Application accounts that are fully managed by AMS are referred to as AMS-managed application accounts, where some or all operational tasks, 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.

The amount of tasks performed by AMS depends on the Change Management mode that you select. AMS-managed accounts support different modes for change management:

- RFC mode
- Direct Change mode in AMS
- AMS and AWS Service Catalog
- AMS Advanced Developer mode
- Self-Service Provisioning mode in AMS

For more information about change management and different modes, see Change management modes.

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

**AMS Accelerate accounts**

AMS Accelerate is the AMS operations plan that can operate AWS infrastructure supporting workloads. You can benefit from AMS Accelerate operational services such as monitoring and alerting, incident management, security management, and backup management, without going through a new migration, experiencing downtime, or changing how you use AWS. AMS Accelerate also offers an optional patch add-on for EC2 based workloads that require regular patching.

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

> **Note**
>
> AMS Accelerate accounts in AMS Advanced do not have AMS change management (RFCs) or the AMS Advanced console. Instead, they have the AMS Accelerate console and functionality.

Accelerate accounts can only be provisioned from your AMS multi-account landing zone Management account. Accelerate offers different operational capabilities. To learn more see the Accelerate service description.

- You will continue to enjoy some of the features from the multi-account landing zone (MALZ) core accounts such as centralized logging, single billing, Config Aggregator in the security account and SCPs.
- AMS Accelerate does not provide some AMS Advanced services like EPS, Access management, Change management and provisioning. We recommend you follow the next steps to gain access and configure the transit gateway (TGW).

For more details about Accelerate, see What is Accelerate.

**Creating your Accelerate account**

To create an Accelerate account, follow the steps outlined here Create an Accelerate account.

**Accessing your Accelerate account**

After you provision an Accelerate account in your multi-account landing zone (MALZ) account, a role with Administrative access permissions, `AccelerateDefaultAdminRole`, is in the account for you to assume.

To access the new Accelerate account:

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 Accelerate account ID and the name of the role to assume: `AccelerateDefaultAdminRole`.

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 Accelerate account, see Enabling SAML 2.0 federated users to access the AWS Management Console.

**Connecting your Accelerate account with Transit Gateway**

AMS does not manage the network setup of an Accelerate account. You have the option of managing your own network using AWS APIs (see Networking Solutions) or connecting to the MALZ 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 Accelerate account is in the same AWS Region. For more information see Transit gateways.

To add your Accelerate account to Transit Gateway, request a new route using the Deployment | Managed landing zone | Networking account | Add static route (ct-3r2ckznmt0a59) change type, include this information:

- **Blackhole**: True to indicate that the route's target isn't available. Do this when the traffic for the static route is to be dropped by the Transit Gateway. False to route the traffic to the specified TGW attachment ID. Default value is false.
- **DestinationCidrBlock**: The IPV4 CIDR range used for destination matches. Routing decisions are based on the most specific match. Example: 10.0.2.0/24.
- **TransitGatewayAttachmentId**: The TGW Attachment ID that will serve as the route table target. If **Blackhole** is false, this parameter is required, otherwise leave this parameter blank. Example: tgw-attach-04eb40d1e14ec7272.
- **TransitGatewayRouteTableId**: The ID of the TGW route table. Example: tgw-rtb-06ddc751c0c0c881c.

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 Accelerate VPC to communicate with.
3. Submit a Deployment | Managed landing zone | Networking account | Add static route (ct-3r2ckznmt0a59) change type, include this information:
   - **Blackhole**: True to indicate that the route's target isn't available. Do this when the traffic for the static route is to be dropped by the Transit Gateway. False to route the traffic to the specified TGW attachment ID. Default value is false.
   - **DestinationCidrBlock**: The IPV4 CIDR range used for destination matches. Routing decisions are based on the most specific match. Example: 10.0.2.0/24.
   - **TransitGatewayAttachmentId**: The TGW Attachment ID that will serve as the route table target. If **Blackhole** is false, this parameter is required, otherwise leave this parameter blank. Example: tgw-attach-04eb40d1e14ec7272.
   - **TransitGatewayRouteTableId**: The ID of the TGW route table. Example: tgw-rtb-06ddc751c0c0c881c.

**Connecting a new Accelerate account 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. In your Accelerate account, open the Amazon VPC console.
4. In the navigation pane, choose **Transit Gateway Attachments** > **Create Transit Gateway Attachment**. Make these choices:
   - For the **Transit Gateway ID**, choose the transit gateway ID you recorded in Step 2.
   - For **Attachment type**, choose **VPC**.
   - Under **VPC Attachment**, optionally type a name for **Attachment name tag**.
   - Choose whether to enable **DNS Support** and **IPv6 Support**.
   - For **VPC ID**, choose the VPC to attach to the transit gateway. This VPC must have at least one subnet associated with it.

- 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**:

1. Decide which TGW route table you want to associate the VPC with. We recommend creating a new application route table for Accelerate account VPCs using Deployment | Managed landing zone | Networking account | Create transit gateway route table (ct-3dscwaeyi6cup) change type.
2. Submit a Management | Managed landing zone | Networking account | Associate TGW attachment (ct-3nmhh0qr338q6) 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 Accelerate account VPC to communicate with.
3. Submit a Deployment | Managed landing zone | Networking account | Add static route (ct-3r2ckznmt0a59) 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**:

1. Decide with your solutions architect what traffic you want to send to the AMS Multi-Account Landing Zone transit gateway.
2. Submit a Deployment | Managed landing zone | Networking account | Add static route (ct-3r2ckznmt0a59) RFC against the networking account to create the TGW routes you need.

### 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 application account, see Management account | Create Customer-Managed Application Account.

To delete a Customer Managed application account, use Management account | Offboard Application Account. (The Confirm Offboarding CT does not apply to Customer Managed application accounts.)

### 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 with the Networking account | Add static route (ct-3r2ckznmt0a59) change type and include this information:

- **Blackhole**: True to indicate that the route's target isn't available. Do this when the traffic for the static route is to be dropped by the Transit Gateway. False to route the traffic to the specified TGW attachment ID. Default value is false.
- **DestinationCidrBlock**: The IPV4 CIDR range used for destination matches. Routing decisions are based on the most specific match. Example: `10.0.2.0/24`.
- **TransitGatewayAttachmentId**: The TGW Attachment ID that will serve as route table target. If **Blackhole** is false, this parameter is required, otherwise leave this parameter blank. Example: `tgw-attach-04eb40d1e14ec7272`.
- **TransitGatewayRouteTableId**: The ID of the TGW route table. Example: `tgw-rtb-06ddc751c0c0c881c`.

**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. In the navigation pane, choose **Transit Gateways**. Record the TGW ID of the transit gateway you see.

3. In your Customer Managed account, 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 by submitting a Deployment | Managed landing zone | Networking account | Create transit gateway route table (ct-3dscwaeyi6cup) RFC. To associate the VPC or TGW attachment to the route table you select, submit a Deployment | Managed landing zone | Networking account | Associate TGW attachment (ct-3nmhh0qr338q6) RFC on the Networking account.

**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 Deployment | Managed landing zone | Networking account | Add static route (ct-3r2ckznmt0a59) RFC against the networking account to create the TGW routes you need.

> **Note**
>
> This CT (ct-3r2ckznmt0a59) does not allow adding static routes to core route table EgressRouteDomain; if your CMA needs to allow egress traffic, submit a Management | Other | Other (MOO) RFC with ct-0xdawir96cy7k.

**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. Update your VPC route tables to send traffic to TGW attachment created earlier

**Getting operational help with your Customer Managed accounts**

AMS can help you operate the workloads you deployed in your Customer Managed accounts by on-boarding the account into AMS Accelerate. With AMS Accelerate you can benefit from operational services such as monitoring and alerting, incident management, security management, and backup management, without going through a new migration, experiencing downtime, or changing how you use AWS. AMS Accelerate also offers an optional patch add-on for EC2-based workloads that require regular patching. With AMS Accelerate you continue using, configuring, and deploying all AWS services natively, or with your preferred tools; as you do with AMS Advanced Customer Managed accounts. You use your preferred access and change mechanisms while AMS applies proven practices that help scale your team, optimize costs, increase security and efficiency, and improve resiliency. To learn more see the Accelerate service description.

To onboard your Customer Managed account into Accelerate, contact your CSDM and follow the steps from Getting Started with AMS Accelerate.

> **Note**
>
> AMS Accelerate accounts in AMS Advanced do not have AMS change management (requests for change or RFCs) or the AMS Advanced console. Instead, they have the AMS Accelerate console and functionality.

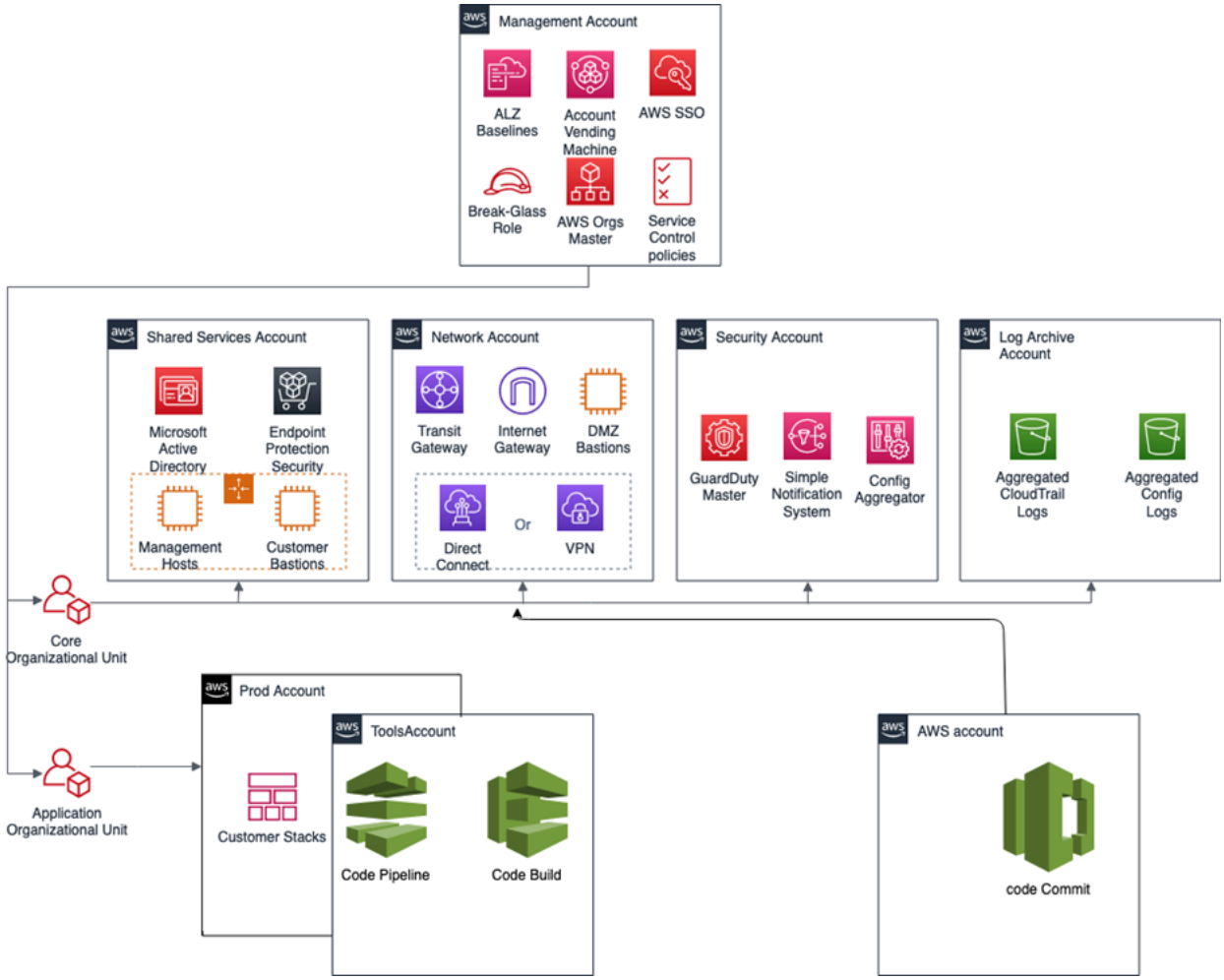
## AMS Tools account (migrating workloads)

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 `AWSManagedServicesMigrationRole` 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 `AWSManagedServicesMigrationRole` to edit the default template for your requirements.

Application Migration Service > Set up Application Migration Service

# Set up Application Migration Service

In order to use Application Migration Service in this region, the service must first be initialized by creating a Replication Settings template. After the template is created, Application Migration Service will automatically create the IAM roles required for the service to operate. The service can only be initialized by the Admin user of your AWS account.

## Create Replication Settings template Info

Every source server added to this console has Replication Settings that control how data is sent from the source server to AWS. These setting are created automatically based on this template, and can be modified at any time for any source server or group of source servers. The template itself can also be modified at any time (changes made will only affect newly added servers).

### Replication Servers Info

Staging area subnet Info

Replication Server instance type Info

EBS volume type (for replicating disks over 500GiB) Info

Faster, General Purpose SSD (gp2)

EBS encryption Info

Default

Security groups Info

☑ Always use Application Migration Service security group

Additional security groups

*Choose additional security groups*

### Data routing and throttling Info

☐ Use private IP for data replication (VPN, DirectConnect, VPC peering)

☑ Create public IP

☐ Throttle network bandwidth (per server - in Mbps)

### Replication resources tags Info

Add new tag

You can add up to 50 more tags

### Enable access to the new AMS 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 an additional IAM role and user available:

   - IAM role: `AWSManagedServicesMigrationRole`
   - IAM user: `customer_cloud_endure_user`

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:

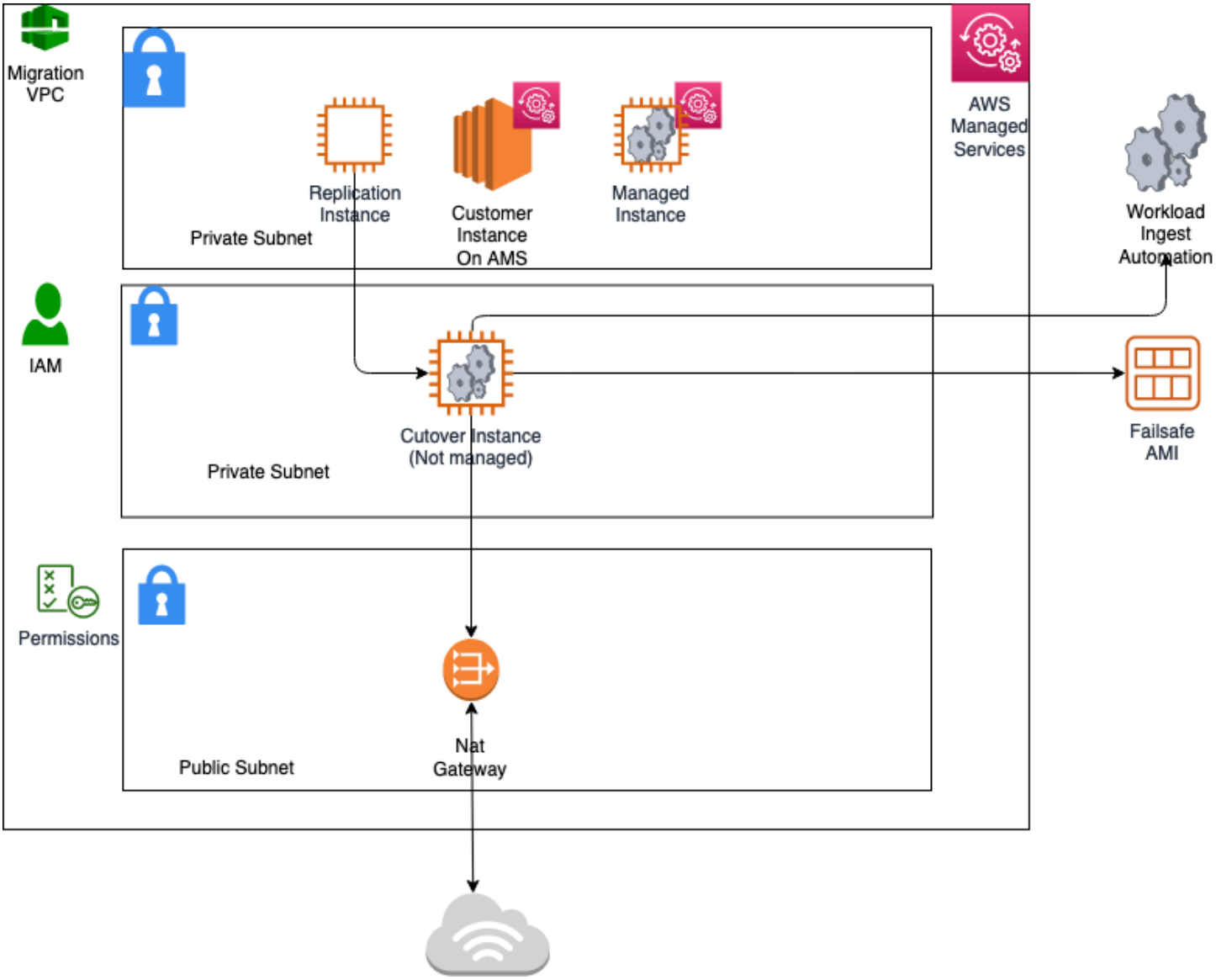
   a. Create KMS key. Use either Create KMS Key (auto) or Create KMS Key (review required).

      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 | Advanced stack components | KMS key | Share (review required) change type (ct-05yb337abq3x5) 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 AMS pre-approved IAM CloudEndure 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`.

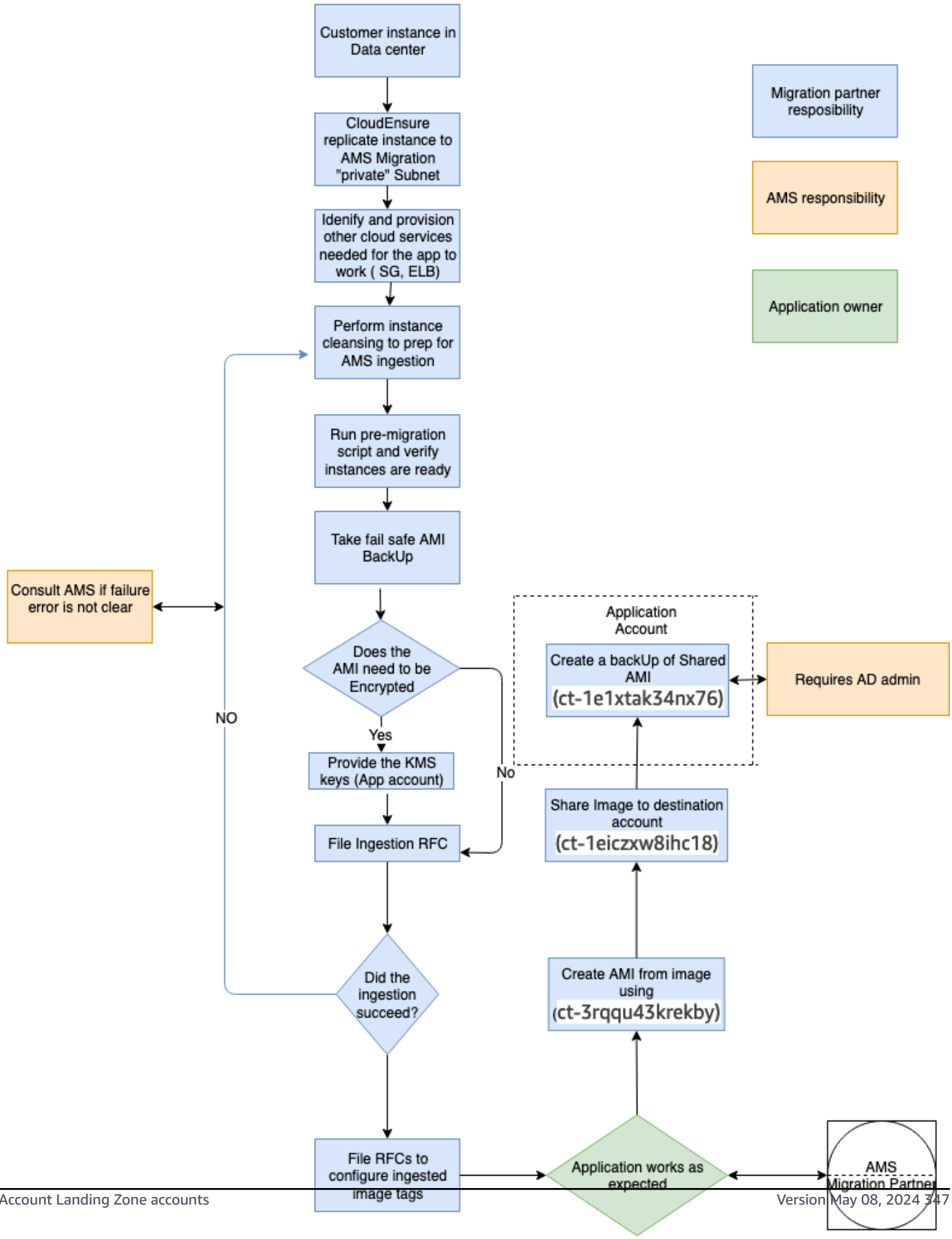
### Testing AMS Tools account connectivity and end-to-end setup

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:

# AMS Ingestion Process



### AMS 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 through Developer mode to ensure clean-up happens on regular basis, for example:
  - Security groups
  - Resources created via Cloud-formation
  - Network ACK
  - Subnet
  - VPC
  - Route Table
  - Roles
  - Users and accounts

### Migration at scale - Migration Factory

See Introducing AWS CloudEndure Migration Factory Solution.

# MALZ: Core account onboarding

The key tasks you'll need to accomplish when onboarding to an AWS multi-account landing zone core account are as follows:.

### Topics

- Create an AWS multi-account landing zone core account in AMS
- Create an IAM role for AMS to access your account

- Secure the new account with multi-factor authentication (MFA) for the root user in AMS
- Subscribe to AWS Marketplace for Trend Micro Endpoint Protection (EPS)
- Set up networking
- Set up access management

For onboarding questions, contact your Cloud Architect.

## Create an AWS multi-account landing zone core account in AMS

AMS multi-account landing zone requires the provisioning of a new Amazon Web Services (AWS) account to act as the management account in the AMS multi-account landing zone environment. To create an AWS account, follow these step-by-step instructions: How do I create and activate a new Amazon Web Services account?

The simple steps are: Go to Create Account, and click **Sign Up Now** and, on the page that opens, click **Create a new AWS account**. Follow the on-screen instructions, which include receiving a phone call and entering a PIN using your phone keypad. You'll also need to enter a credit card. AMS uses this account as the management account, or payer account, for your new multi-account landing zone.

> **Note**
>
> Once you are onboarded, talk to your cloud service delivery manager (CSDM) about moving billing off of your credit card and onto an invoice system. The following information will be required:
>
> - Billing Company Name
> - Billing Contact Name
> - Billing Contact Phone Number
> - Billing Contact Email
> - Billing Address
>
> Your CSDM will help you with this update. Once completed, and to change the payment method, see Managing your AWS payment methods.

> **Note**
>
> Do not link your new account to an existing management account, or payer account. Ensure that your account is not part of an existing AWS Organizations; for information, see What Is AWS Organizations?

> **Important**
>
> It is very important that you ensure that an **email address** (a distribution list, not an individual's email address) and **phone number** are associated with the account so that you receive responses to potential security incidents. The phone number and email address for the account cannot be changed without resetting the account password, which is a significant undertaking for an AMS root account. To ensure that these values are stable, *it is critical to select contact information not associated with individuals*, which can change. Choose an email alias that can point to a group. Follow this same practice in selecting a phone number: choose a number that can point to a group or to a number owned by the company and not an individual.

For details on the questions you will be asked to onboard your Core account to AMS multi-account landing zone, see Appendix: multi-account landing zone (MALZ) onboarding consideration list.

## Create an IAM role for AMS to access your account

Now that you've successfully created your new AWS account, the next step in the process is to allow AMS access to the new account to create and configure your AMS environment, and for ongoing change and provisioning requests to be fulfilled. For details, see Delegate Access Across AWS Accounts Using IAM Roles.

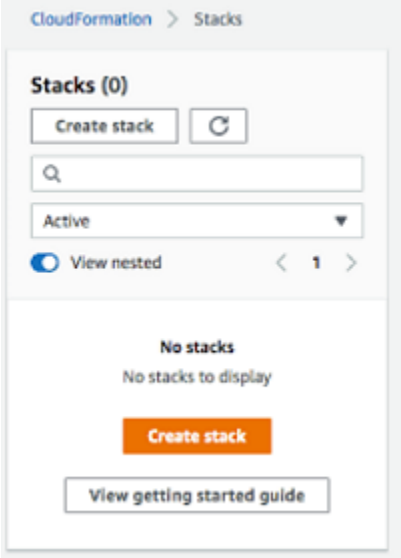
AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources for your users. You use IAM to control who can use your AWS resources (authentication) and what resources they can use and in what ways (authorization).

## Activate IAM access to the AWS console

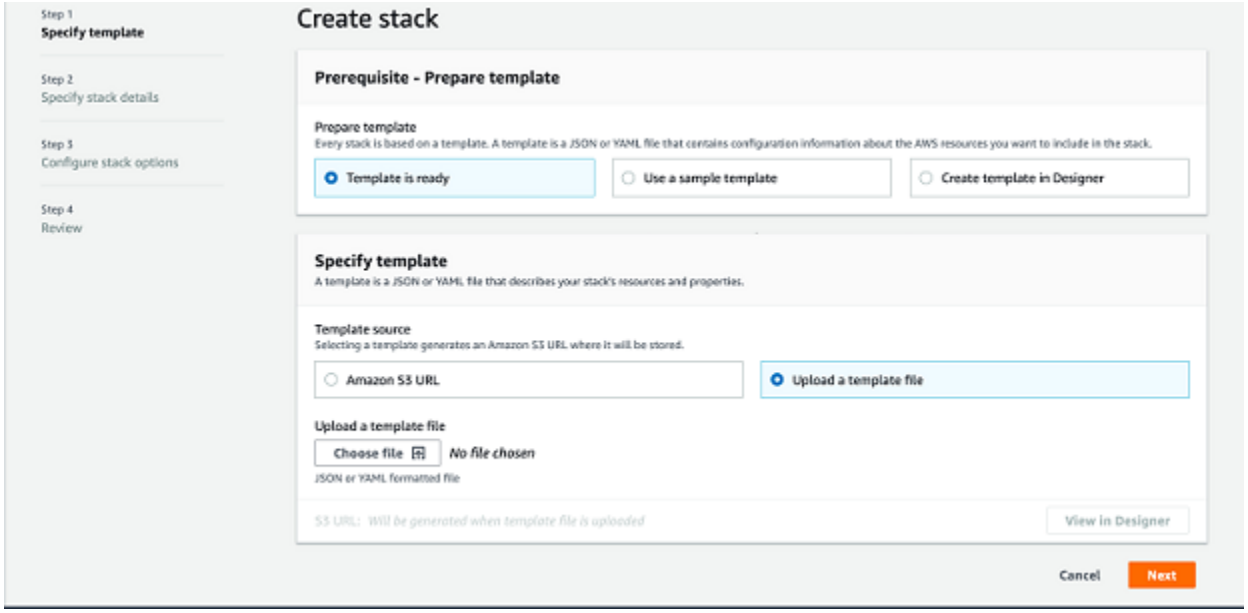
1. Sign in to the AWS Management console with your root account credentials (the email and password that you used to create your AWS account). Do not sign in with other IAM credentials. The AWS Management console home page opens.
2. In the top navigation bar, open the drop-down menu for your account name, and then choose **Account**. The Billing home page opens.
3. Scroll down to **IAM user and role access to Billing information**, and choose **Edit**. An **Activate IAM access** area opens.
4. Select the check box and then choose **Update**. You can now use IAM policies to control which pages a user can access.

## Create an IAM Role for AMS to use

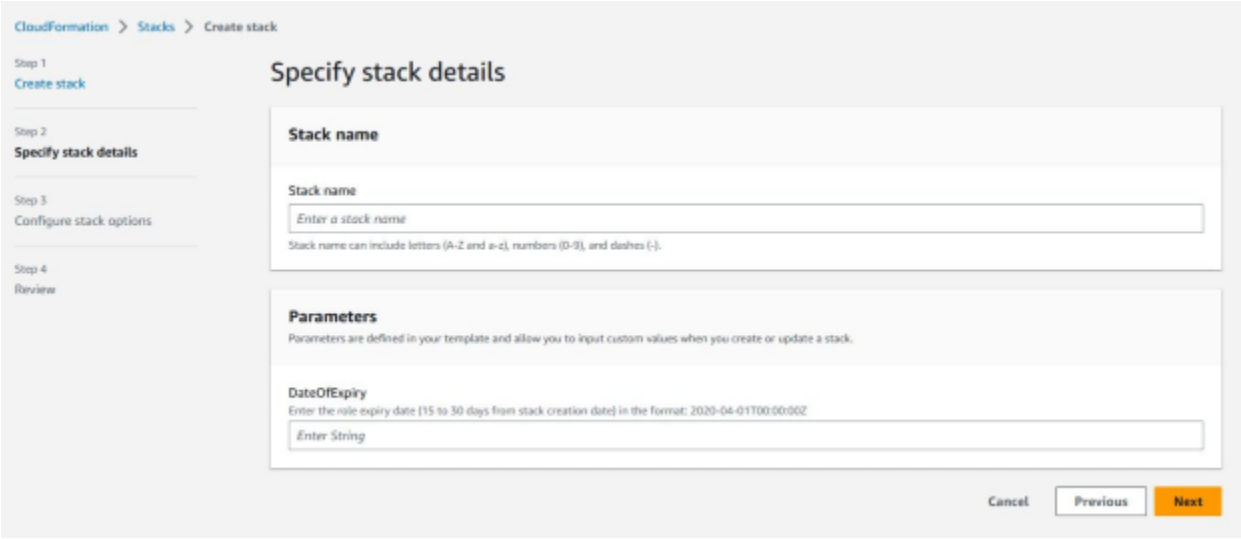
1. Obtain a JSON or YAML file that defines an IAM role for AMS to use to create your infrastructure. Either:
   - Your AMS cloud architect (CA) provides you with a JSON or YAML file.
   - You can download onboarding_iam_roles.zip and choose one of the following:
     - **onboarding_role_admin.json** (shorter, grants full admin access)
     - **onboarding_role_minimal.json** (longer, grants least privilege)
2. Sign in to the AWS Management Console and open the AWS CloudFormation console at https://console.aws.amazon.com/cloudformation.



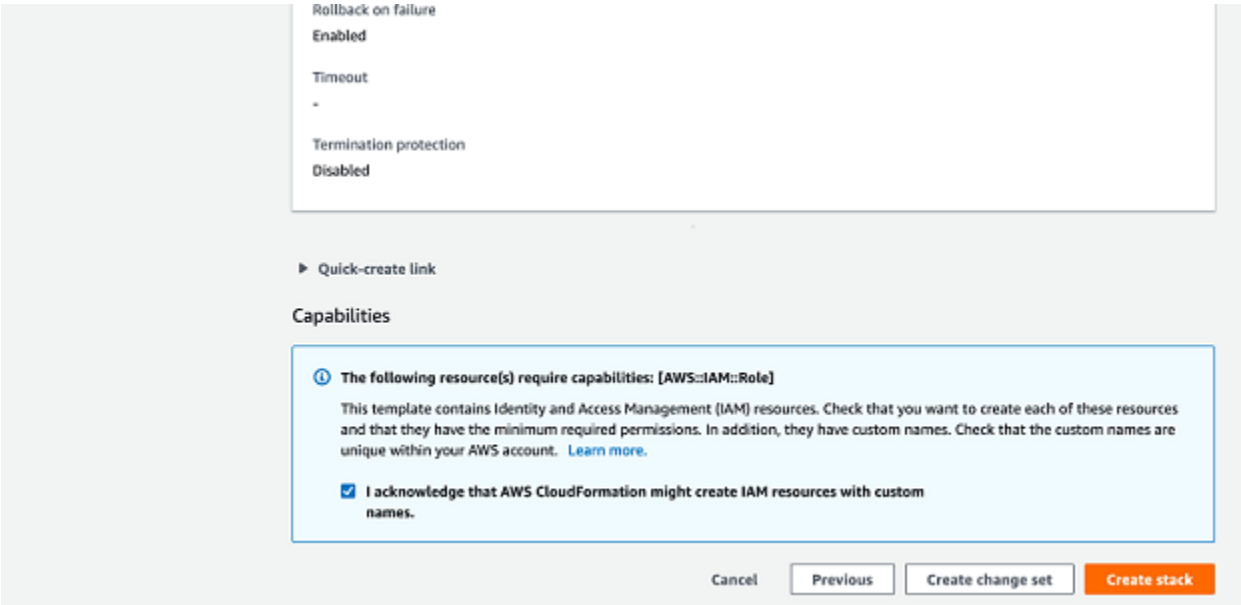
3. Choose **Create Stack**. You see the following page.




4. Choose **Upload a template file**, upload the JSON or YAML file of the IAM role, and then choose **Next**. You see the following page.




5. Enter **`ams-onboarding-role`** into the **Stack name** section and continue scrolling down and selecting next until you reach this page.




6. Make sure the check box is selected and then select **Create Stack**.
7. Make sure the stack was created successfully.

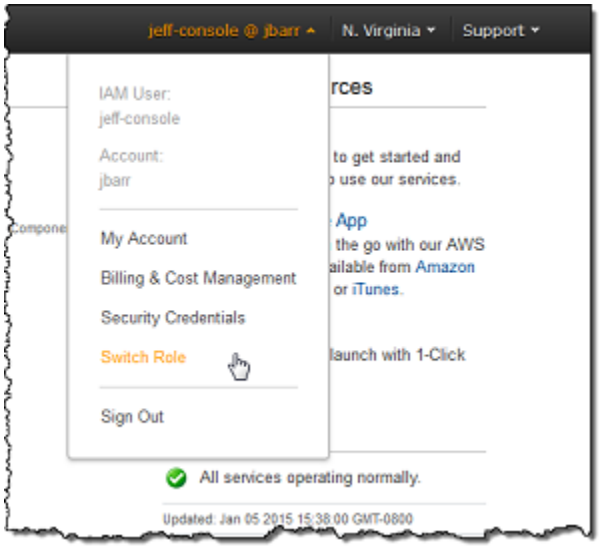
## Secure the new account with multi-factor authentication (MFA) for the root user in AMS

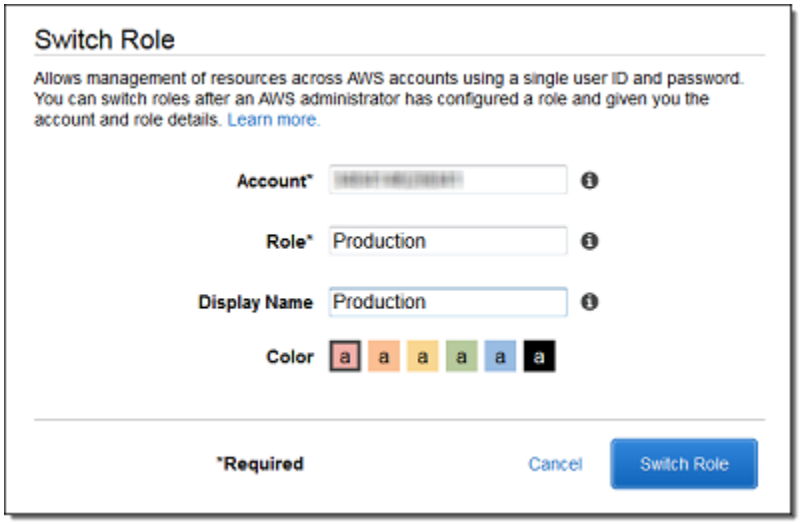
This section has been redacted because it contains sensitive AMS security-related information. This information is available through the AMS console **Documentation**. To access AWS Artifact, you can contact your CSDM for instructions or go to Getting Started with AWS Artifact.

## Subscribe to AWS Marketplace for Trend Micro Endpoint Protection (EPS)

Trend Micro Endpoint Protection (EPS) is the primary component within AMS for operating system security. In order to set up EPS once AMS landing zone creation is started, you need to log in to the shared services core account and subscribe to the Trend Micro Deep Security AMI on AWS Marketplace. Your CSDM or CA will advise you.

1. Log in to the AWS console using the role or user that you specified in the Onboarding Questionnaire for `CustomerEPSSubscriptionIAMRoleOrUser`
2. Navigate to the **Switch Role** screen.




- Account: Provided by AMS
- Role: `EPSMarketplaceSubscriptionRole`
- Display Name: EPS Subscription Session

To subscribe to Trend Micro Deep Security in the AWS Marketplace, follow these steps after you have switched the role in the console:

1. Navigate to the AWS Marketplace.
2. Under **Find AWS Marketplace products that meet your needs**, select the following options:
   a. **Vendors**: Trend Micro

   b. **Pricing Plan**: Bring Your Own License if you have a license or By Hosts Billing
   c. **Delivery Methods**: Amazon Machine Image
3. Click **Continue to Subscribe** in the right panel.
4. Review the **Terms and Conditions**, and click **Accept Terms** in the upper right corner.
5. Sign out of the account and confirm with your Cloud Architect that the procedure has been completed.

At this point AMS deploys infrastructure into your AMS environment and the environment is ready for you to use once you have connected your network and set up your access.

## Set up networking

Networking in the AMS environment is primarily handled in the networking core account.

There are several processes that need to be completed to set up networking for AWS Managed Services (AMS):

- Allocating IP space for your AMS environment
- Establishing private network connectivity to AWS
- Setting up your firewall to allow AMS operations

### Allocating IP space for your AMS environment

You should have already worked with your Cloud Architect in defining the IP space for your AMS environment while filling out the onboarding questionnaire.

### Establishing private network connectivity to AWS in AMS

AWS offers private connectivity by using VPN connectivity and dedicated lines through AWS Direct Connect. Private Connectivity can be setup in two ways:

- Centralized Edge connectivity using Transit Gateway
- Connecting Direct Connect and/or VPN to account VPCs

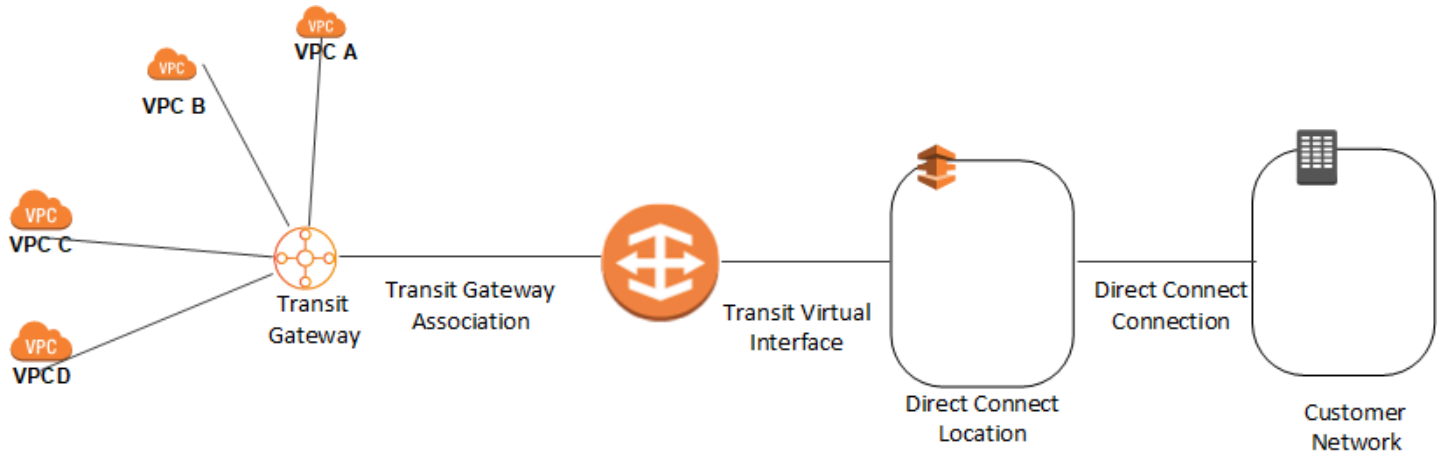
### Centralized edge connectivity using Transit Gateway

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. Transit Gateway can be used to consolidate your existing edge connectivity and route it through a single ingress/egress point. For more details, see AWS Transit Gateway.

### Connecting Direct Connect to Transit Gateway

You can use your existing Direct Connect connection or create a new Direct Connect connection in one of your existing AWS accounts. The Direct Connect connection should be a dedicated or hosted connection running at 1 Gbps or more.

> **Note**
>
> For information about using Direct Connect with AWS services, see Getting Started at an AWS Direct Connect Location.




To use an existing Direct Connect dedicated connection, the connection must not have more than 3 transit virtual interfaces created on it. This is because AWS Direct Connect dedicated connections have a limit of 4 transit virtual interfaces per connection.

For additional information on Direct Connect Limits, see AWS Direct Connect Limits.

After the Direct Connect connection is available, the following occurs:

1. AMS creates a Direct Connect Gateway in the networking account. You must provide an Autonomous System Number (ASN) number for the Direct Connect Gateway and the prefixes

that have to be advertised from the Direct Connect Gateway. This ASN is used as the Amazon ASN.

2. You create a new Transit VIF and set the virtual interface owner as the networking account.
3. AMS logs in to the networking account and accepts the connection proposal.
4. AMS associates the transit gateway with the Direct Connect gateway.
5. AMS associates the attachment with the on-prem Transit Gateway routing table.

> **Note**
>
> The ASN provided for the Direct Connect gateway and the Transit Gateway must be different.

To increase the resiliency of your connectivity, it's a best practice to attach at least 2 transit virtual interfaces, from different AWS Direct Connect locations, to the Direct Connect gateway. For more information, see AWS Direct Connect resiliency recommendation.

**Connecting VPN to Transit Gateway**

To attach a VPN connection to your transit gateway, you must specify the customer gateway. For more information about the requirements for a customer gateway, see Requirements for Your Customer Gateway in the Amazon VPC Network Administrator Guide.

You would need to provide the BGP ASN number, static public IP address and routing Option (Static or Dynamic). Once these details are provided, AMS would create the VPN attachment and associate the attachment with the on-prem Transit Gateway routing table.

For more details on Transit Gateway attachments, see Transit Gateway VPN Attachments.

**Connecting Direct Connect and/or VPN to account VPCs**

You can also directly connect your VPCs to Direct Connect or VPN. The traffic flows directly from the VPCs to Direct Connect or VPN without traversing through the transit gateway.

> **Note**
>
> The shared services VPC and application account VPCs have to be connected to a Direct Connect or VPN connection to establish private connectivity.

### AWS Direct Connect setup in AMS

Set up a AWS Direct Connect to communicate between your AMS-managed VPC and your internal network.

> **Note**
>
> For information about using Direct Connect with AWS services, see Getting Started at an AWS Direct Connect Location.

To set up a Direct Connect connection, complete the following steps:

1. Sign up for Amazon Web Services (AWS)
2. Submit an AWS Direct Connect connection request.
3. Complete the Cross Connect.
4. (Optional) Configure redundant connections with AWS Direct Connect.
5. Performed by AMS: Create a virtual interface.
6. Performed by AMS: Download router configuration.
7. Verify your virtual interface.

### VPN setup

The basic steps that AMS follows for setting up a VPN to communicate between your AMS-managed VPC and your internal network.

> **Note**
>
> To gain overall understanding about using a VPN with AWS services, see What is AWS Site-to-Site VPN and Your Customer Gateway (your VPN appliance).

We follow the AWS VPN User Guide Getting Started and Testing the Site-to-Site VPN Connection sections to complete the following steps:

1. In your AWS VPC, Create a Customer Gateway.
2. In your AWS VPC, Create a Virtual Private Gateway.

3. In your AWS VPC, Enable Route Propagation in Your Route Table.
4. In your AWS VPC, Update Your Security Group to Enable Inbound SSH, RDP, and ICMP Access.
5. In your internal Network, Create a VPN Connection and Configure the Customer Gateway.
6. Test VPN connectivity between the VPC and your internal network.

## Set up access management

Using a network managed by AWS Managed Services (AMS) means giving AMS access to manage your cloud infrastructure. You'll need to configure a means of securely connecting between your private network and AMS. This starts with some decisions:

- *AMS API/CLI and Console access*: You will want to install the AMS CLI (instructions are provided in this document). You use the AMS change management API to make change requests to AMS and the AMS SKMS API to learn about your AMS-managed resources. Using Active Directory Federation Services (AD FS), you can access the AMS Console.
- *User access*: Connectivity needs to be established between AD on the AMS side (via Directory Services) and the directory you use to manage users.
- *Instance access*: Instance-level access is accomplished via a one-way trust configuration. Directory Services trusts credentials in your CORP AD, allowing stacks within the AMS side to allow login with CORP credentials.

> **Note**
>
> Your Active Directory (AD) that AMS sets up the trust to, must be the directory that has the accounts of users authorized by you to gain access to your AWS resources.

### Establish an Active Directory Trust

To set up a trust, AMS requires your domain controller **Local Policies -> Security Options -> Network Access: Named Pipes that can be accessed anonymously**, have the **Netlogon** and **lsarpc** pipes listed. These pipes are listed by default, but are sometimes removed for security concerns. Once the trust is established, they can be removed from the list again.

### Configure the Conditional Forwarder

1. In the AD **DNS Manager -> Create a New Conditional Forwarder**, under **DNS Domain:** Use the domain name AMS supplied to you; for example, *A523434123.amazonaws.com* (change this to the domain name selected in the onboarding questionnaire.
2. Under **IP addresses of the master servers:** Add the AMS-supplied IP addresses. Make sure there isn't a connection problem by validating both addresses.
3. Select **Store this conditional forwarder in Active Directory and replicate as follows: All DNS servers in this domain** and press **OK**.

### Configure the AD trust

Follow this Microsoft AD article Create a one-way, incoming, forest trust for one side of the trust, using the settings and choices described in this section.

1. Open the **Start -> Administrative Tools -> Active Directory Domains and Trusts** dialog. Right-click the domain node for the domain that you want to establish a trust with, and then click **Properties -> Trusts -> New Trust** to open the New Trust Wizard. Enter the domain name provided to you by AMS for the **Trust Name** and press **Next**.
2. Under **Trust Type**, select appropriate trust level (e.g. Forest Trust). Press**Next**.
3. Under **Direction of Trust**, select **One-way: incoming**. Press **Next**.
4. Under **Sides of Trust**, select **This domain only**. Press **Next**.
5. Under **Trust Password**, type a password of your choosing. Press **Next**.
6. For **Trust Selections Completed** and **Trust Creation Complete**, just press **Next**.
7. Under **Confirm Incoming Trust**, select **No**, do not confirm the incoming trust. Press **Next**.
8. Under **Completed the New Trust Wizard**, select **Finish**, and then **OK** to close.
9. Provide the trust password (contact us via your CSDM's phone number for security reasons). AMS will complete the trust configuration.

### Active Directory sites and services

To reduce login latency, add the VPC CIDR range to your Active Directory sites and services (**Start -> Administrative Tools -> Active Directory Sites and Services**). Add the VPC CIDR range to an Active Directory Site that contains Domain Controllers that are closest to AWS.

Provide the AD site name of the site that you dedicated for AMS to your CSDM. AMS will rename the default site on the AMS side of AD to match the provided name.

### Active Directory name suffix routing

After the one-way forest trust has been established, complete the following steps to validate suffix routing:

1. Under **Start > All Programs > Administrative Tools**, click **Active Directory Domains and Trusts**.

   The Active Directory Domains and Trusts console opens.
2. Right-click your corporate domain and click **Properties**

   The Properties dialog for that domain opens.
3. Click the **Trusts** tab.

   The Trusts page opens.
4. Click the Amazon domain name and click **Properties**.

   The Properties page for the Amazon domain trust opens.
5. Click **Name Suffix Routing** and click **Refresh**.

   Make sure there are no conflicts to ensure that the Service Principal Names (SPNs) can resolve over the trust.

## Federate your Active Directory with the AMS IAM roles

The purpose of federating your directory with the AMS IAM roles is to enable corporate users to use their corporate credentials to interact with the AWS Console and the AWS APIs, and, therefore, the AMS console and APIs.

### Federation process example

This example uses Active Directory Federation Services (AD FS); however, any technology that supports AWS IAM Federation is supported. For more information on AWS-supported IAM federation, see IAM Partners and Identity Providers and Federation. Your CSDM will help you through this process, which involves a joint effort with your AD team and AMS.

For detailed information on integrating SAML for API access, refer to this AWS blog, How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS.

For an example that installs the AMS CLI and SAML, see Appendix: AD FS claim rule and SAML settings.

**Configuring federation to the AMS console (MALZ)**

The IAM roles and SAML identity provider (Trusted Entity) detailed in the following table have been provisioned as part of the AMS infrastructure. These roles allow you to audit and view the AMS core accounts.

| Role | Permissions |
| --- | --- |
| AWSManagedServicesReadOnlyRole | Allows you to view the AMS infrastructure in the core accounts. |
| AWSManagedServicesCaseRole | Allows you to view the resources in your new application account and file AMS incidents and service requests. |
| AWSManagedServicesChangeManagementRole | Allows you to view the AMS infrastructure in the core accounts, file AWS Support tickets, and request some RFCs. |

For the full list of the roles available under different accounts see IAM user role in AMS .

## Verify console access

Once you are set up with ADFS, and have the AMS URL to use for authentication, follow these steps.

With an Active Directory Federated Service (ADFS) configuration, you can follow these steps:

1. Open a browser window and go to the sign in page provided to you for your account. The ADFS **IdpInitiatedSignOn** page for your account opens.
2. Select the radio button next to **Sign in to one of the following sites**. The **Sign in** site picklist becomes active.

3. Choose the **signin.aws.amazon.com** site and click **Sign in**. Options for entering your credentials open.
4. Enter your CORP credentials and click **Sign in**. The AWS Management Console opens.
5. Paste into the location bar the URL of the AMS console and press **Enter**. The AMS console opens.

## Verify API access

AMS uses the AWS API, with some AMS-specific operations that you can read about in the AMS API Reference.

AWS provides several SDKs that you can access at Tools for Amazon Web Services. If you don't want to use an SDK, you can make direct API calls. For information on authentication, see Signing AWS API Requests. If you are not using an SDK, or making direct HTTP API requests, you can use the AMS CLIs for Change Management (CM) and SKMS.

Install the AMS CLIs

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).
2. After the installation, run aws help to verify the installation.
3. Once the AWS CLI is installed, to install or upgrade the AMS CLI, download the AMS 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.
4. Open either the **Managed Cloud Distributables -> CLI -> Windows** or the **Managed Cloud Distributables -> CLI -> Linux / MacOS** directory, depending on your operating system, and:
5. 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

6. For **Mac/Linux**, execute 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.
7. 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.
8. After the installation, run `aws amscm help` and `aws amsskms help` to see commands and options.

# MALZ: Application account onboarding

You must have a multi-account AWS Managed Services (AMS) environment set up with core accounts, before requesting a new application account. Here are the steps you'll need to take after setting up your environment.

**Topics**


- Requesting a new application account
- Setting up Active Directory to federate access to AMS IAM roles
- Setting up networking with the new Application account
- Setting up additional VPCs in the Application account


For onboarding questions, contact your cloud service delivery manager (CSDM). See also Application accounts: AMS-managed, Dev-mode, Customer-managed. For general information about modes, see AMS modes Service management in AWS Managed Services.

For information on the different modes of application accounts, see Application accounts: AMS-managed, Dev-mode, Customer-managed. For general information about modes, see AMS modes.

## Requesting a new application account

You must have a multi-account AWS Managed Services (AMS) environment set up with core accounts, before requesting a new application account. For information about setting up a multi-account environment with core accounts, see MALZ: Core account onboarding.

You can choose one of the following Amazon VPC types for the initial VPC in the application account:

- Private: This VPC has no Internet gateway attached. This is suitable for private applications that require no access to/from the Internet.
- Public: This VPC has an Internet gateway attached and has public and private subnets. This is suitable for public applications that require access to/from the Internet.

You can request a new application account by submitting a Deployment | Managed landing zone | Management account | Create application account (with VPC) (ct-1zdasmc2ewzrs) RFC and providing the following values in the RFC:

- Account Name: A custom name for the account. Note that the Account Name has a maximum length of 50 characters.
- Account Email: The distribution list email for the account. This email ID is used for creating the AWS account.
- Support level: The AWS Support level, Premium or Plus.
- VPC Name: A name for the VPC.
- Number of Availability Zones (AZs): 2 or 3.
- VPC CIDR: The CIDR block for the VPC.
- Route Type: This can be either `routable` or `isolated`. `Routable` means that application VPCs associated with the Transit Gateway (TGW) application route table can connect to this VPC. `Isolated` means that application VPCs associated with the TGW application route table cannot connect to this VPC. The default is `routable`.
- Transit Gateway Application Route Table: The Transit Gateway route table to which the application account VPC has to be associated with. If no value is provided, the default `defaultAppRouteDomain` is used, which means that this account will be able to communicate with all other accounts under the same route table.
- PublicSubnetAZ*<1-3>*CIDRCIDR for public subnet in AZ 1: The CIDR for public subnet in Availability Zone 1.
- PrivateSubnet*<1-10>*AZ*<I-3>*CIDRCIDR for public subnet in AZ 1: The CIDR for public subnet in Availability Zone 1.

At this point, AMS deploys a new application account into your AMS management account, with the specified VPC configuration.

## Setting up Active Directory to federate access to AMS IAM roles

Federate your directory with the AMS IAM roles to enable corporate users to use their corporate credentials to interact with the AWS Console and the AWS APIs, and the AMS console and AMS APIs.

### Federation process example

This example uses Active Directory Federation Services (ADFS). However, any technology that supports AWS IAM Federation is supported. For more information about AWS-supported IAM federation, see IAM Partners and Identity Providers and Federation. Your CSDM will help you through this process, which involves a joint effort with your AD team and AMS.

For detailed information about integrating SAML for API access, refer to this AWS blog, How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS.

For an example that installs the AMS CLI and SAML, see Appendix: AD FS claim rule and SAML settings in the AMS User Guide.

### Configuring federation to the AMS console

The IAM roles and SAML identity provider (Trusted Entity) detailed in the following table are provisioned in your new application account. These roles allow you to gain access to the new application account and file RFCs, write to S3 buckets, and perform other actions.

| Role | Permissions |
| --- | --- |
| AWSManagedServicesReadOnlyRole | Allows you to view the resources in your new application account. |
| AWSManagedServicesCaseRole | Allows you to view the resources in your new application account and file AWS Support tickets. |
| AWSManagedServicesChangeManagementRole | Allows you to view the AMS infrastructure in the application accounts, file RFCs, file |

| Role | Permissions |
| --- | --- |
| | AWS Support tickets, write to S3 buckets, manage Secrets Manager secrets, and manage Reserved Amazon Elastic Compute Cloud (Amazon EC2) instances. |
| AWSManagedServicesSecurityOpsRole | Allows you to view the AMS infrastructure in the application accounts, manage Secrets Manager secrets, manage Web Application Firewall rules, manage certificates, and file AWS Support tickets. |
| AWSManagedServicesAdminRole | Allows you to view the AMS infrastructure in the application accounts, manage Marketpla ce subscriptions, manage Secrets Manager secrets, manage Web Application Firewall rules, manage certificates, create RFCs, manage Reserved Amazon EC2 instances, write to S3 buckets, file AWS Support tickets, and manage AWS Artifacts agreements. |

### Submitting the federation request to AMS

If this is your first account, work with your CSDM(s) and/or Cloud Architect(s) to provide the metadata XML file for your identity provider.

If you are onboarding an additional account or Identity Provider and have access to either the management account or the desired application account, follow these steps.

1. Create a service request from the AMS console.

> **Note**
>
> - If creating an identity provider for an application account, submit this request from either the application account itself or the management account.
> - If creating an identity provider for an AMS core account, submit this request from the management account.

- If creating an identity provider for the management account, submit this request from the management account, or contact your CSDM for assistance.

In the service request, provide the details necessary to add the identity provider:

- AccountId of the account where the new identity provider will be created.
- Desired identity provider name, if not provided, the default will be **customer-saml**; typically, this must match the settings configured in your federation provider.
- For existing accounts, include whether the new identity provider should be propagated to all existing console roles or provide a list of roles that should trust the new identity provider.
- Attach the metadata XML file exported from your federation agent to the service request as a file attachment.

2. From the same account where you created the service request, create a new RFC using CT-ID ct-1e1xtak34nx76 (Management | Other | Other | Create) with the following information.

- Title: "Onboard SAML IDP <Name> for Account <AccountId>".
- AccountId of the account where the identity provider will be created.
- Identity provider name.
- For Existing Accounts: Whether the identity provider should be propagated to all existing console roles, or the list of roles which should trust the new identity provider.
- Case ID of service request created in Step 1, where the metadata XML file is attached.

## Verify Console Access

After you are set up with AD FS, and have the AMS URL to use for authentication, you can perform the following procedure.

**With an Active Directory Federated Service (AD FS) configuration, you can follow these steps:**

1. Open a browser window and go to the sign in page provided to you for your account. The **AD FS IdpInitiatedSignOn** page for your account opens.
2. Select the radio button next to Sign in to one of the following sites. The Sign in site list becomes active.
3. Choose the signin.aws.amazon.com site and choose Sign in. Options for entering your credentials open.

4. Enter your CORP credentials and choose Sign in. The AWS Management Console opens.
5. Paste into the location bar the URL of the AMS console and press **Enter**. The AMS console opens.

### Verify API Access

AMS uses the AWS API, with some AMS-specific operations that you can read about in the AMS API Reference.

AWS provides several SDKs that you can access at Tools for Amazon Web Services. If you don't want to use an SDK, you can make direct API calls. For information on authentication, see Signing AWS API Requests.. If you are not using an SDK, or making direct HTTP API requests, you can use the AMS CLIs for Change Management (CM) and SKMS.

## Setting up networking with the new Application account

Setting up networking for the application account includes configuring firewall rules and potentially setting up additional Transit Gateway (TGW) route tables.

### Setting up your firewall

To use the applications deployed in your AMS environment, you must create some firewall rules. You do not need these rules to access your instances, you can hop through the bastions into your instances.

#### Firewall Rules for Application Access

You must open the following ports for traffic through your firewall:

- From your on-premise network to your new application VPC CIDRs in both the ingress and egress directions.
- From your new application VPC CIDRs to your on-premise network in both the ingress and egress directions (if your cloud applications need to reach out to your on-premise applications).

| Port | Protocol | Service | From/To | To/From |
|---|---|---|---|---|
| 80 | TCP | HTTP Web Access | On Premise Network | AMS Application VPC |

| Port | Protocol | Service | From/To | To/From |
|---|---|---|---|---|
| 443 | TCP | HTTPS Web Access | On Premise Network | AMS Application VPC |

### Setting up additional transit gateway application route tables

AWS Managed Services (AMS) networking is flexible and supports a variety of networking use cases.

- Communication between application VPCs in the same account.
- Communication between application VPCs in different accounts.
- Isolation between application VPCs in different accounts.
- Isolation between application VPCs in same accounts.

If you have unique/special requirements for networking, contact your AMS Cloud Architect and they will develop a plan for your requirements to be met by AMS network architecture.

Based on the networking decision taken for application account VPCs, you can create multiple Transit Gateway (TGW) application route tables by submitting a Deployment | Managed landing zone | Networking account | Create transit gateway route table (ct-3dscwaeyi6cup) RFC.

The change type requires you to specify `TransitGatewayRouteTableName` (a meaningful name for the TGW route table), `TransitGatewayId`, and `TGWRouteTableType`.

> **Note**
>
> If createCustomRouteDomain is selected for TGWRouteTableType, the route table created is empty. You must file an RFC with the Deployment | Managed landing zone | Networking account | Add static route (ct-3r2ckznmt0a59) change type.

## Setting up additional VPCs in the Application account

You can request an additional application account VPC by submitting a Deployment | Managed landing zone | Application account | Create VPC (ct-1j3503fres5a5) RFC.

This works in the same way as configuring a VPC for a new application account. For details, see Requesting a new application account.

# Appendix: multi-account landing zone (MALZ) onboarding consideration list

There are a number of key considerations you'll need to think about in planning your AMS multi-account landing zone deployment. Your choices will provide AMS with the information it requires to determine the infrastructure components you will need. Your Cloud Architect (CA) will provide you with a questionnaire to assist in this work.

**Topics**


- AMS multi-account landing zone account configuration
- AMS multi-account landing zone monitoring alerts
- Network configuration
- Active Directory configuration
- Trend Micro Endpoint Protection (EPS)
- Access: Bastions, SSH and RDP
- Federation


> **Note**
>
> For more information on instance types, see Amazon EC2 Instance Types.
> For more information on database instance types, see Amazon RDS Instance Types.
> If you require Direct connect, see the AMS single-account landing zone Onboarding Guide to create a Direct Connect connection.

You will receive an onboarding questionnaire from your Cloud Service Delivery Manager (CSDM) containing questions about your desired configuration settings for your account. Work with your CSDM to complete the questionnaire before proceeding.

## AMS multi-account landing zone account configuration

- New Account ID

The AWS account ID that you created for AMS multi-account landing zone. Should not be part of an AWS organization.

- Service Region

  The primary Region in which the AMS multi-account landing zone environment will be deployed.

- The core account emails for notifications. (these should all be in the same domain). Provide an email address for each:
  - Shared Services account
  - Networking account
  - Logging account
  - Security account
- Your service type, Premium or Plus

  This determines the service level agreements (SLAs) for resolving issues in your environment

## AMS multi-account landing zone monitoring alerts

AMS provides a way for you to be directly alerted (versus getting AMS service notifications) for certain monitoring alerts. To sign up for this, make sure that your Cloud Architect (CA) or Cloud Service Delivery Manager (CSDM) receive this information:

**Direct Alerts Email**: These are the email addresses that you want AMS to send certain resource-based alerts to. For details of which alerts are sent directly to email, see Alerts from baseline monitoring in AMS in the *AMS Advanced User Guide*. For more information on AMS monitoring, see Monitoring Management in the AMS User Guide for Single-Account Landing Zone.

## Network configuration

- Transit Gateway ASN Number

  This is the Autonomous System Number (ASN) for the AWS side of a Border Gateway Protocol (BGP) session, it must be unique and cannot be the same one used for your Direct Connect or VPN.  The range is 64512 to 65534 (inclusive) for 16-bit ASNs.

- Your AMS multi-account landing zone infrastructure VPC CIDR ranges.

  These CIDR ranges cannot overlap with your on-premise network

You can either include a /22 CIDR range, or provide each VPC CIDR individually. Note that only these CIDR ranges are allowed:

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Note that IP range 198.18.0.0/15 may not be used (it is reserved by AWS Directory Service).

- Core Infrastructure VPC CIDR range (/22 range recommended)
- Networking VPC CIDR range (/24 range recommended)
- Shared Services VPC CIDR range (/23 range recommended)
- DMZ VPC CIDR range (/25 range recommended)

- VPN ECMP (enable or disable)

  For VPN ECMP support, choose enable if you need Equal Cost Multipath (ECMP) routing support between VPN connections. If connections advertise the same CIDRs, the traffic is distributed equally between them.

## Network access control list (NACL)

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 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: Management, 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. Additionally, they must have "Allow All" configured 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.

## Active Directory configuration

Domain FQDN for AMS managed Active Directory

## Trend Micro Endpoint Protection (EPS)

- Instance sizes for your EC2 instances and Auto Scaling groups

  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 of AMS data plane and your EC2 instances.

  - Relay instance type (minimum supported by AMS is m5.large)
  - DB instance size (200 GB recommended)
  - RDS instance type (only db.m5.large or db.m5.xlarge allowed)
- DSM License type (Marketplace or BYOL)

  If you already have a license, choose BYOL (bring your own license). AMS will contact you to obtain the necessary information about the license.
- AWS IAM user or role Amazon resource name (ARN) for Trend Micro Deep Security Subscription (Role ARN: arn:aws:iam::*ACCOUNT_ID*:role/*ROLE_NAME*)

  Provide us an IAM role; ARN, or an IAM user ARN from one of your existing AWS accounts to which you have access. AMS creates an IAM role; in your AMS multi-account landing zone Shared Services account and adds the role or user provided in the trust of an IAM role in Shared Services so that the role can be assumed by you to subscribe to the Trend Micro Deep Security in AWS Marketplace.

## Access: Bastions, SSH and RDP

- SSH Bastion settings

  AMS provides SSH bastions in your Shared Services account to access hosts in the AMS environment. In order to access the AMS network as an SSH user, you must use SSH Bastions as the entry point. The network path originates from the On-Prem 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 your AMS environment, provided that the proper access request has been granted.

- Desired instance count (2 recommended)
- Maximum instances (4 recommended)
- Minimum instances (2 recommended)
- Instance type (m5.large recommended)
- Ingress CIDRs: IP address ranges from which users in your network will access SSH Bastions (ip range 1, ip range 2, ip range 3, ... etc)

- RDP Bastion settings

  AMS optionally provides RDP bastions in your Shared Services account to access hosts in the AMS environment. In order to access the AMS network as an RDP user, you must use RDP Bastions as the entry point. The network path originates from the On-Prem network, goes through DX/VPN to the TGW, and then is routed to Shared Services VPC. Once you are able to access the bastion, you can jump to other hosts in the AMS environment, provided that the proper access request has been granted.

  - Instance type (t3.medium recommended)
  - Desired minimum sessions (2 recommended)
  - Desired maximum sessions (10 recommended)

- RDP Bastion Configuration Type, Shared Standard or Shared HA (default is Shared Standard)

  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.

## Federation

Identity Provider (IDP) Name

Defaults to `customer-saml`

# AMS Single-account landing zone (SALZ) onboarding

## AMS SALZ onboarding process

To onboard AMS single-account landing zone (SALZ) accounts, you'll need to take the following steps:

1. Create a new AWS account that AMS configures as the networking account to host the firewall. Create the new account within your AWS organization, if you have one. AMS will follow the procedure of creating a normal AMS account, so all the information required must be gathered (for example CIDR, EPS licenses, and users). Note: A CIDR allocation of /24 is good.
2. Specify whether or not you want to remove the Internet gateways (IGWs) from the egress traffic accounts.
3. Determine your approved domains. AMS enables destination filtering by maintaining an approved domain list; the list can be modified later.
4. Confirm the instance size you want to use based on your expected throughput. By default, the instance is created in a m4.xlarge instance where we have found that the firewall throughput is 350Mbps. AMS can increase the size to a c4.8xLarge instance where the expected throughput is 1.25 Gbps.
5. Set up networking between AMS and your private network. This involves several tasks:
    a. Allocate IP space
    b. Establish private network connectivity to AWS
    c. Set up your firewall
    d. Set up access management
    e. Schedule backups
6. Provide access to the created account to AMS.
7. Validate that the AMS service is operating properly.

AMS will be able to perform the account build-out (onboarding) of your account within 2 weeks (10 business days) from the initial request date. Any follow-up activity can be performed by using AMS Planned Event Management (PEM).

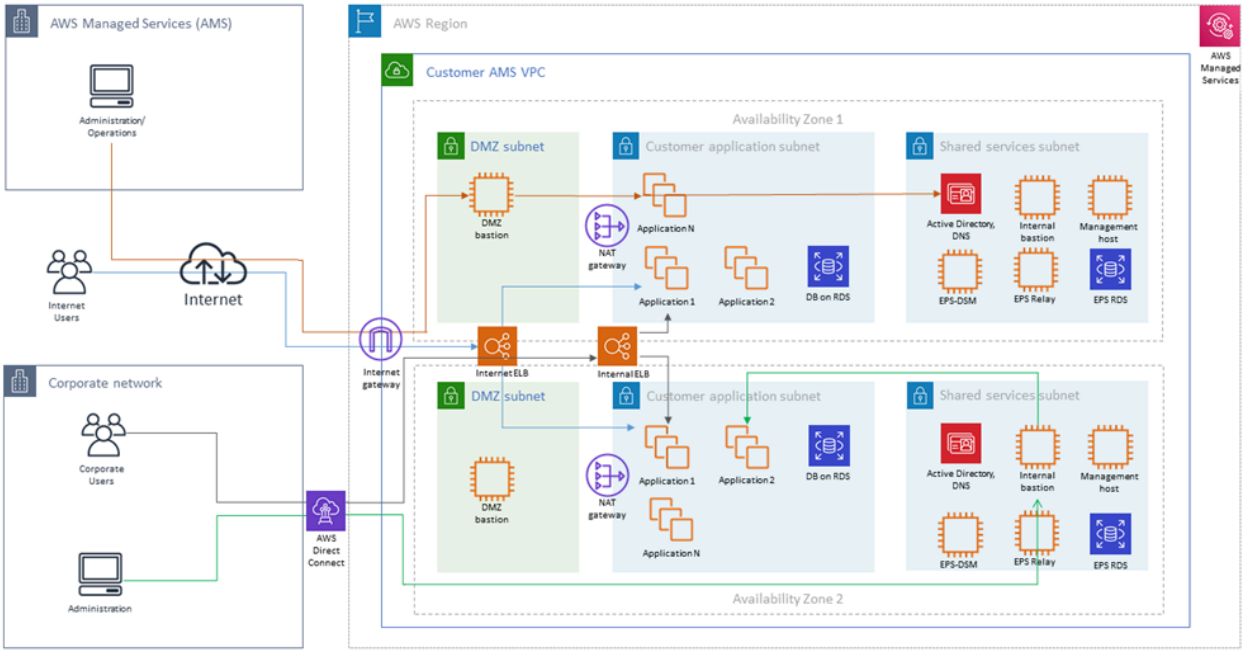
**Note**

- 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. For the most current list, see AWS regions and availability zones.

# SALZ network architecture

The following diagram depicts the AWS Managed Services (AMS) single-account landing zone (SALZ) VPC network layout and is an example of the highly available setup.




| | |
|---|---|
| — 1 → | Ingress through DirectConnect (internal customer network users) and Internet with managed Internet Gateway (external users), through AWS load balancers to customers subnet applications. **Note** that traffic for external users goes through load balancers in DMZ (Public) Subnet, while traffic for internal users goes through load balancers in Application (Private) Subnet |
| — 2 → | Ingress through Internet with managed Internet Gateway for AMS administrators and operators through DMZ bastions to customer and shared services subnets |
| — 3 → | Ingress through DirectConnect (internal customer network administrators) and internal bastions to customer subnets |

Each AMS account has a VPC in one region with resource subnets located in two availability zones. Each availability zone has three subnets: DMZ, Customer, and Shared Services. Your ("customer") corporate network is connected through a DirectConnect (VPN) tunnel, and AMS Operations connects to your managed VPC over the Internet.

Shared services subnets contain AMS Directory Services with one AD Domain Controller per shared services subnet, and AMS Management Hosts that automate provisioning and common tasks, Antivirus (TrendMicro) management servers that include EPS DSM and EPS relay (for scalability), and internal (customer) bastion hosts.

DMZ subnets contain Internet load balancers, your DMZ instances, and DMZ bastion hosts that serve as SSH jump boxes for the AMS Operations team. DMZ bastions, as well as other AMS infrastructure in the Shared services subnet, have two nodes for high availability.

Your "customer" subnets 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 DMZ.

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 gateways, 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)

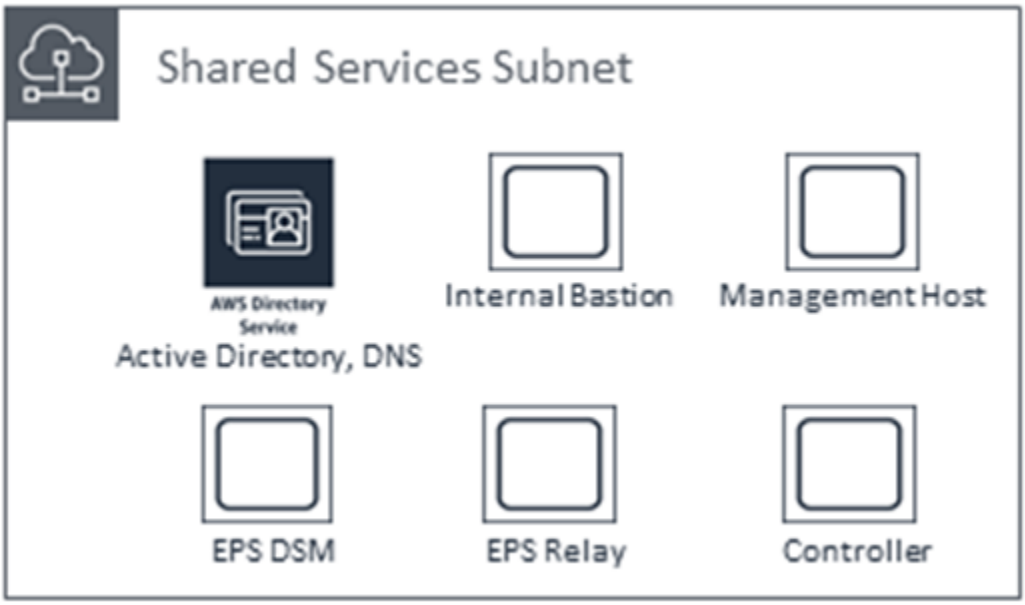
Act as an API endpoint to modify AWS Directory Service, interact with AWS Directory Service domain controllers.

- 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.




## SALZ: Create a new AWS account for AMS

The five steps to creating a new AWS account for AWS Managed Services (AMS) are:

1. Create an AWS account
2. Set up consolidated billing–link new account to Payer account
3. Configure your AWS account for AMS access
4. Secure the new account with multi-factor authentication (MFA) for the root user in AMS
5. Subscribe to AWS Marketplace for EPS

Please contact your customer service delivery manager (CSDM) if you have any questions.

# Create an AWS account

The AMS program requires the provisioning of a new Amazon Web Services (AWS) account. Step by step instructions are available in the following video: How do I create and activate a new Amazon Web Services account? The simple steps are:

## Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

**To sign up for an AWS account**

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call or text message and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform tasks that require root user access.

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ and choosing **My Account**.

## Create a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

**Secure your AWS account root user**

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

For help signing in by using root user, see Signing in as the root user in the *AWS Sign-In User Guide*.

2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) in the *IAM User Guide*.

**Create a user with administrative access**

1. Enable IAM Identity Center.

   For instructions, see Enabling AWS IAM Identity Center in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to a user.

   For a tutorial about using the IAM Identity Center directory as your identity source, see Configure user access with the default IAM Identity Center directory in the *AWS IAM Identity Center User Guide*.

**Sign in as the user with administrative access**

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

  For help signing in using an IAM Identity Center user, see Signing in to the AWS access portal in the *AWS Sign-In User Guide*.

**Assign access to additional users**

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

   For instructions, see Create a permission set in the *AWS IAM Identity Center User Guide*.

2. Assign users to a group, and then assign single sign-on access to the group.

   For instructions, see Add groups in the *AWS IAM Identity Center User Guide*.

> **Note**
>
> If you already have an account, you can go to the AWS Pricing page and click **Create a Free Account**. *Be sure to sign up* for the **EC2 Service**, at least. Signing up for one service allows you access to all services in AWS. You are charged only for the services that you use.
> If you plan to link your new account to a payer account for the purposes of consolidated billing, you do not need to enter payment method information when prompted. Instead, once you reach the screen to enter credit card information, simply navigate away. You will need the email address associated with the payer account to send a consolidated billing/linked account request which is detailed in the next section.

> **Important**
>
> It is critical that you ensure that an email address and phone number are associated with the account so you receive responses to potential security incidents. The phone number and email address for the account cannot be changed without resetting the account password, which is a significant undertaking for an AMS root account. To ensure that these values are stable, it is critical to select contact information not associated with individuals, which can change. Choose an email alias that can point to a group. Follow this same best practice in selecting a phone number: choose a number that can point to a group or to a number owned by the company and not an individual.

## Set up consolidated billing–link new account to Payer account

If you'd like your new AMS-managed AWS account bill to be rolled into a payment for an existing AWS Organizations management account, you need to set up consolidated billing and link the accounts. For details on doing this, see

- Consolidated billing for AWS Organizations and AWS Multi-Account Billing Strategy.
- Inviting an AWS account to join your organization

> **Note**
>
> You can perform these steps before doing the account handover to AMS. After the handover, the steps for joining your organization (provided above) can be done through the

change management process. Consult with your cloud service deliver manager (CSDM) or cloud architect (CA) if you need assistance.

For general billing information including managing consolidated billing, see What is AWS Billing. For general AWS Organizations information about how accounts can work together, see What is AWS Organizations. For prescriptive guidance on AWS Organizations management accounts, see The management account, trusted access, and delegated administrators

## Configure your AWS account for AMS access

With the above steps completed, you've successfully secured your new AWS account and ensured associated costs are billed appropriately. The final step in the process is to allow AMS access to the new account for initial stack configuration and for ongoing change and provisioning requests to be fulfilled. For details, read Delegate Access Across AWS Accounts Using IAM Roles. The basic steps are described in this section.

### Activate access to the AWS website

In order to grant your IAM users access to your account's billing information and tools, you must activate the functionality.

Follow these steps:

1. Sign in to the AWS Management Console with your *root account* credentials (the email and password that you used to create your AWS account). Don't sign in with your IAM user credentials.

   The AWS Management Console home page opens.
2. In the top navigation bar, open the drop-down menu for your account name, and then choose **My Account**.

   The Billing home page opens.
3. Scroll down to the **IAM User Access to Billing Information** area, and click **Edit** on the right side. *The area does not appear unless you are logged in with root credentials*.

   An **Activate IAM access** area opens.

4. Select the check box and click **Update**.

   You can now use IAM policies to control which pages a user can access.

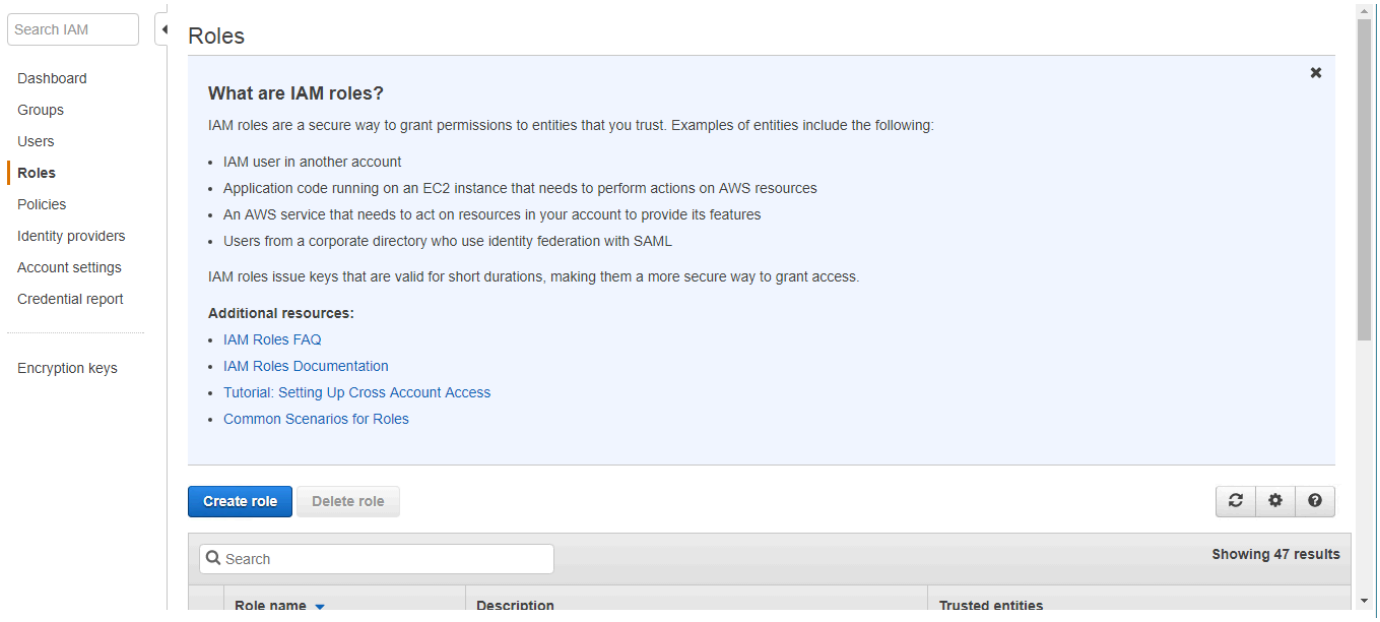
For more details on this process in AWS, see Overview of managing access permissions.

## Create an IAM role with access to the AWS website

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources for your users. You use IAM to control who can use your AWS resources (authentication) and what resources they can use and in what ways (authorization).

1. Go to the IAM Management Console, click **Roles** in the left nav pane.

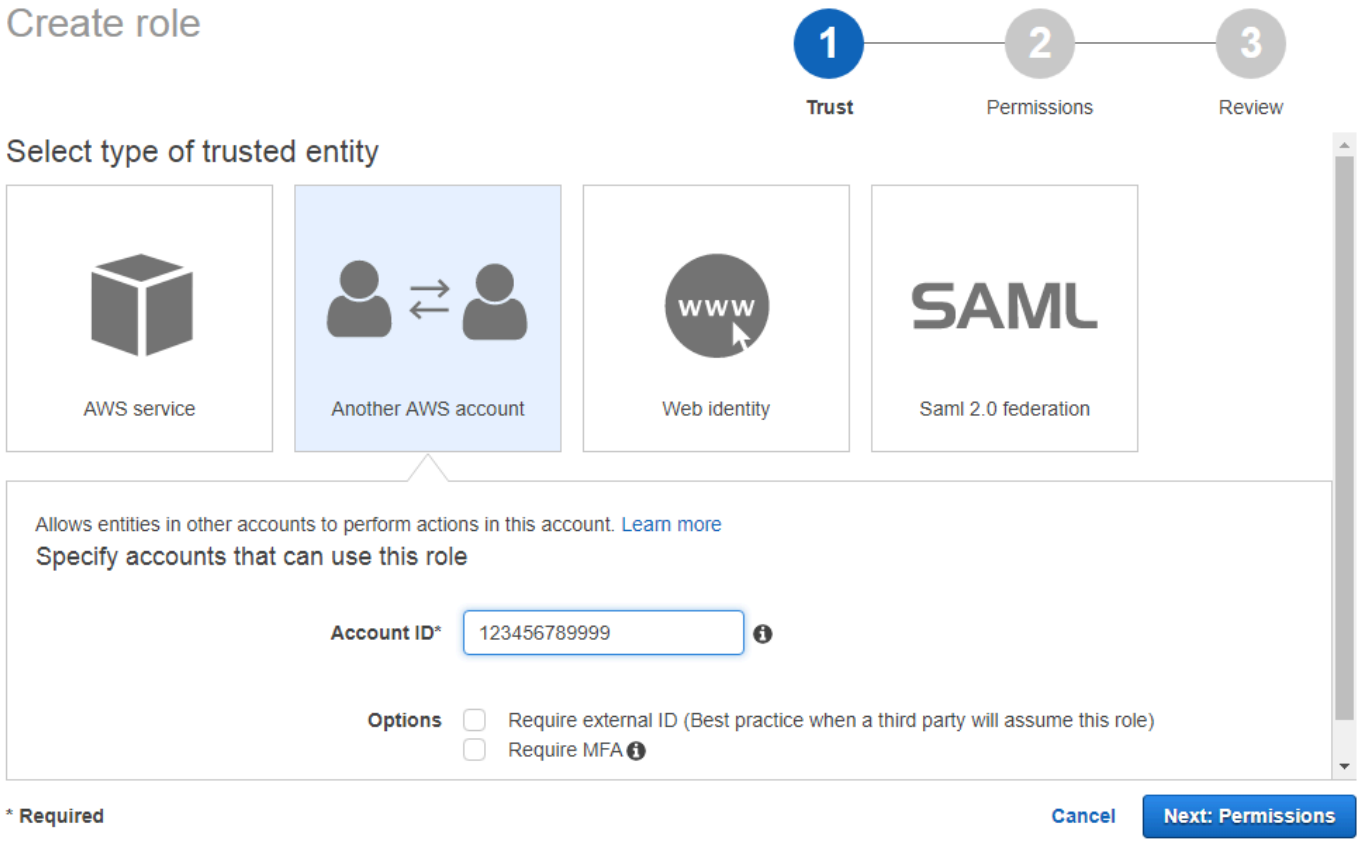
   The Roles management page opens with information about IAM roles, a **Create role** option, and a list of existing roles.




2. Click **Create role**.

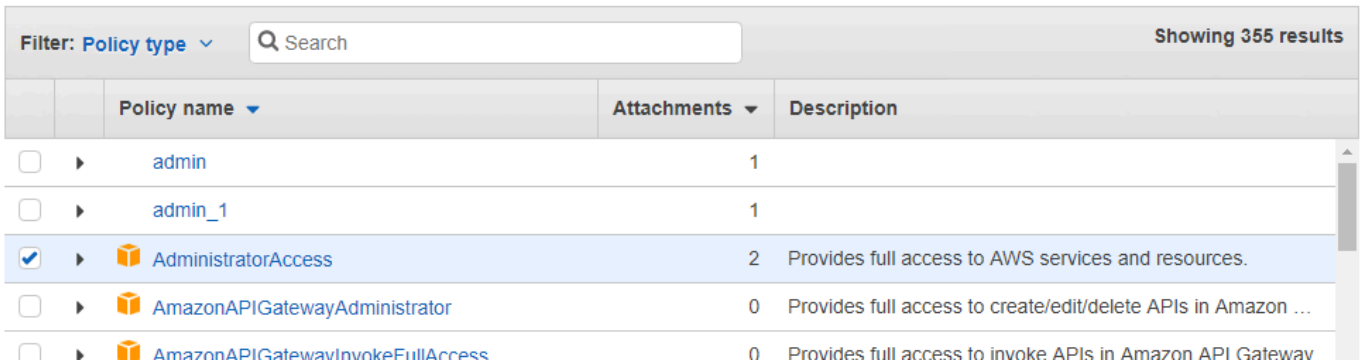
   The Create role **Select type of trusted entity** page opens. Click **Another AWS account** and a settings area opens up below.

Enter the AMS trusted **Account ID** provided to you by AMS. Leave the **Require external ID** and **Require MFA** options de-selected.



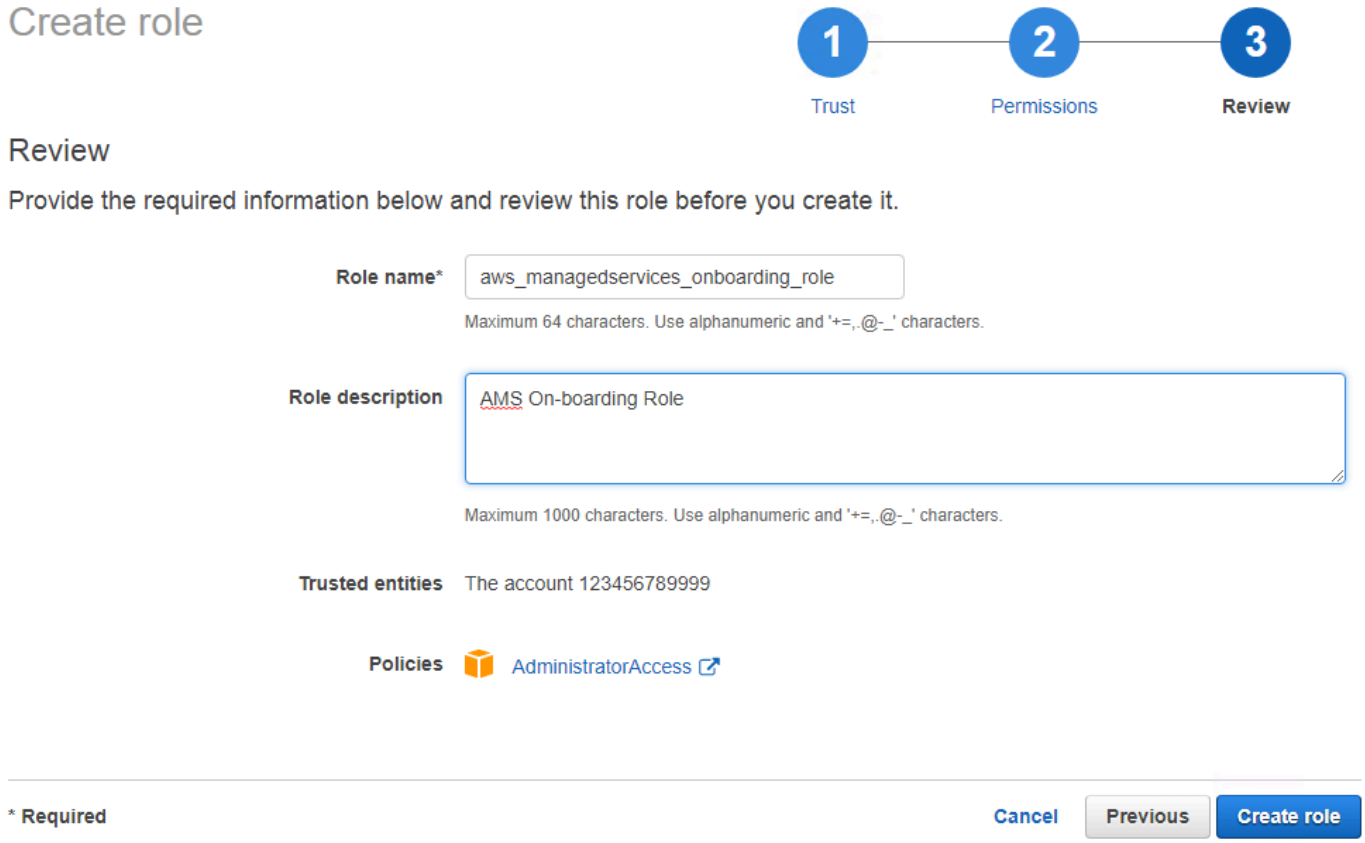

3. Click **Next: Permissions**.

   The Create role **Attach permissions policies** page opens with options for creating a new policy, refreshing the page, and searching existing policies. A list of existing policies is provided.




4. Select the **AdministratorAccess** policy and then click **Next: Review**.

The Create role **Review** page opens.




5. Name the new role **aws_managedservices_onboarding_role** and type "AMS Onboarding Role" for the **Role description**. Review the settings for the new role and, if satisfied, click **Create role**.

   The role management page opens with your new role listed.

## Subscribe to AWS Marketplace for EPS

Recent changes to AMS endpoint security (EPS) require you to subscribe to TrendMicro Deep Security through the AWS Marketplace and accept the software terms.

TrendMicro offers two license models: Per Protected Instance Hour and Bring your own License (BYOL).

- **BYOL**:
  1. You use your own license that you have purchased through external channels.

2. You must provide all the license keys to AMS to build the EPS infrastructure. You can provide an activation code that licenses all modules, or individual activation codes that license a certain set of modules. AMS creates only the license files that correspond with the activation codes you provide. Since the license activation occurs during onboarding, in the presence of an AMS lead engineer and CSDM, you can share that information then.
3. Additionally, you must subscribe to BYOL TrendMicro Market Place AMI Subscription. See Trend Micro Deep Security (BYOL).

- **Per Protected Instance Hour**:
  1. In this subscription, you are not required to have any previously-procured Trend license.
  2. However, you must subscribe to the Marketplace subscription.
  3. No license key sharing with AMS is required in this model, as the Trend usage is metered automatically including the software license + EC2 infrastructure usage. See Trend Micro Deep Security.

To subscribe to Trend Micro, follow these steps:

1. Login into your AWS account.
2. Navigate to Trend Micro Deep Security (BYOL or Per Protected Instance Hour) product page.
3. Click **Continue to Subscribe** in the right panel.
4. Click **Accept Terms** in the upper right corner.

## 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.

Next step: Secure the new account with multi-factor authentication (MFA) for the root user in AMS

## Subscribe to AWS Marketplace for CentOS 7.6

AMS now provides the CentOS 7 (x86_64) - with Updates HVM sold by Centos.org, as an AMS AMI. In order to utilize this AMI, you must opt in to the FREE Cent OS license, and accept the license on all your AMS accounts.

To subscribe, go to AWS Marketplace and follow the instructions for opting-in.

You will not incur software charges for using this product, but you are still responsible for other AWS charges, including EC2 usage. If this is a "Bring Your Own License" product you must have a valid software license in order to use it.

You can review information for this software at CentOS 7 (x86_64) - with Updates HVM.

## Secure the new account with multi-factor authentication (MFA) for the root user in AMS

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.

# SALZ: Set up networking

There are several processes that need to be completed to set up networking for AWS Managed Services (AMS):

1. Allocating IP space for your AMS environment
2. Establishing private network connectivity to AWS
3. Setting up your firewall to allow AMS operations

## Allocate IP Space for your AMS Environment

AMS was designed and tested using a /16 CIDR block as the recommended network allocation. It is important that the trusted network connected to AMS use a CIDR block that does not overlap with the CIDR block assigned to AMS. These addresses are required to set up your virtual private cloud

(VPC) and subnets. For more information about AWS VPCs, see Amazon VPC Limits and Amazon VPC FAQs.

While a /16 CIDR block may seem like a lot of IP addresses, a VPC, once created, cannot be expanded. So this allocation ensures that your AMS-managed VPC can function for a considerable period. Within the CIDR block, you must allocate IP address ranges for, at least, two private subnets and two public subnets.

AWS accepts connectivity to the AMS environment via native AWS virtual private network (VPN) functionality. On your side, this can be achieved via AWS Direct Connect (DX), hardware VPN, or software VPN. On the AMS side, we use the Virtual Gateway functionality of VPCs.

**Basic Environment Components**

| User Network-to-Amazon VPC Connectivity Options | |
|---|---|
| **Hardware VPN** | Establishes a hardware VPN connection from your network equipment on a remote network to AMS-managed network equipment attached to your VPC. |
| **AWS Direct Connect (DX)** | Establishes a private, logical (or encrypted if used with a VPN) connection from your remote network to the Amazon VPC, leveragin g AWS Direct Connect. |
| **Software VPN** | Establishes a VPN connection from your equipment on a remote network to a user-managed software VPN appliance running inside an Amazon VPC. |

> **Note**
>
> AMS recommends redundant private VPN to DX connections. Your customer service delivery manager (CSDM) will assist in setting this up at the time of onboarding your account.

# Establish Private Network Connectivity to AWS

Add AMS to your corporate Active Directory to establish connectivity. You may want to perform administrative actions or user access over a private networking connection. AWS offers both VPN connectivity and dedicated lines via AWS Direct Connect. The following steps explain how to work with AMS to establish either (or both) means of connectivity.

## VPN Setup

This section describes the basic steps for setting up a VPN to communicate between your AMS-managed VPC and your internal network.

> **Note**
>
> To gain overall understanding about using a VPN with AWS services refer to What is AWS Site-to-Site VPN and all about Your Customer Gateway (your VPN appliance).

Follow the AWS VPN User Guide Getting Started and Testing the Site-to-Site VPN Connection sections to complete the following steps.

- Step 1: In your AWS VPC, Create a Customer Gateway
- Step 2: In your AWS VPC, Create a Virtual Private Gateway
- Step 3: In your AWS VPC, Enable Route Propagation in Your Route Table
- Step 4: In your AWS VPC, Update Your Security Group to Enable Inbound SSH, RDP, and ICMP Access
- Step 5: In your internal Network, Create a VPN Connection and Configure the Customer Gateway
- Step 6: Test VPN connectivity between the VPC and your internal network

## AWS Direct Connect Setup

This section describes the basic steps for setting up a AWS Direct Connect (DX) to communicate between your AMS-managed VPC and your internal network.

> **Note**
>
> For information about using a DX with AWS services, see Getting Started at an AWS Direct Connect Location.

To set up a DX connection, you need to complete the following steps:

1. Sign Up for Amazon Web Services
2. Submit AWS Direct Connect Connection Request
3. Complete the Cross Connect
4. (Optional) Configure Redundant Connections with AWS Direct Connect
5. Performed by AMS: Create a Virtual Interface
6. Performed by AMS: Download Router Configuration
7. Verify Your Virtual Interface

## Set up your Firewall

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 Bastion Options during Application Migrations/Onboarding

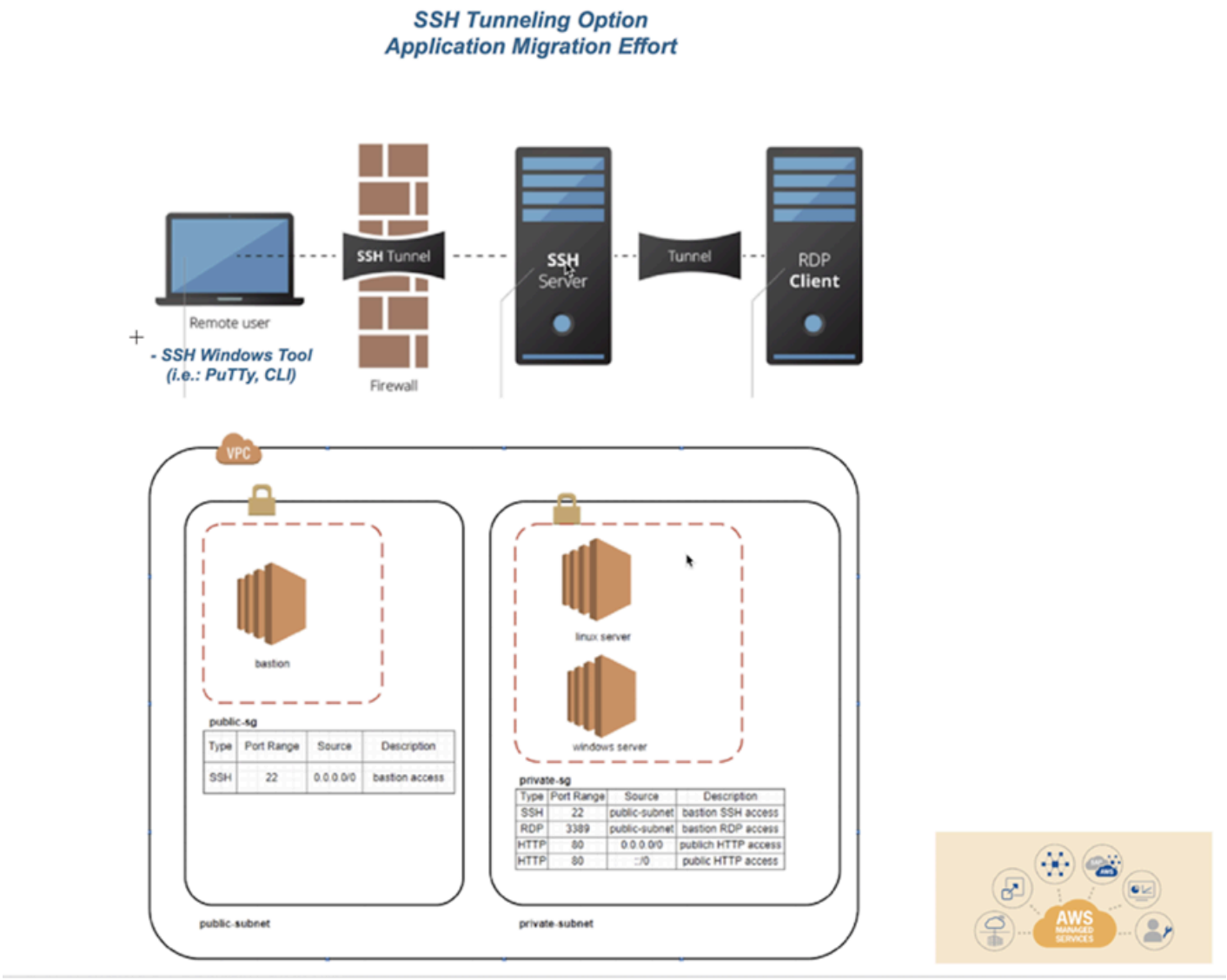
In order to provide you with the best experience during migration efforts, below are the potential options AMS could currently leverage:

- *Option 1*: Bypass Bastions for migration efforts only (you must sign off on this for security purposes as a temporary measure).

  Note: Auditing capabilities will still be in place to ensure AMS has visibility into each request.
- *Option 2*: SSH Tunneling with a tool of choice; for example, PuTTy, as illustrated.

  The environment components described would already need to be in place for this option.

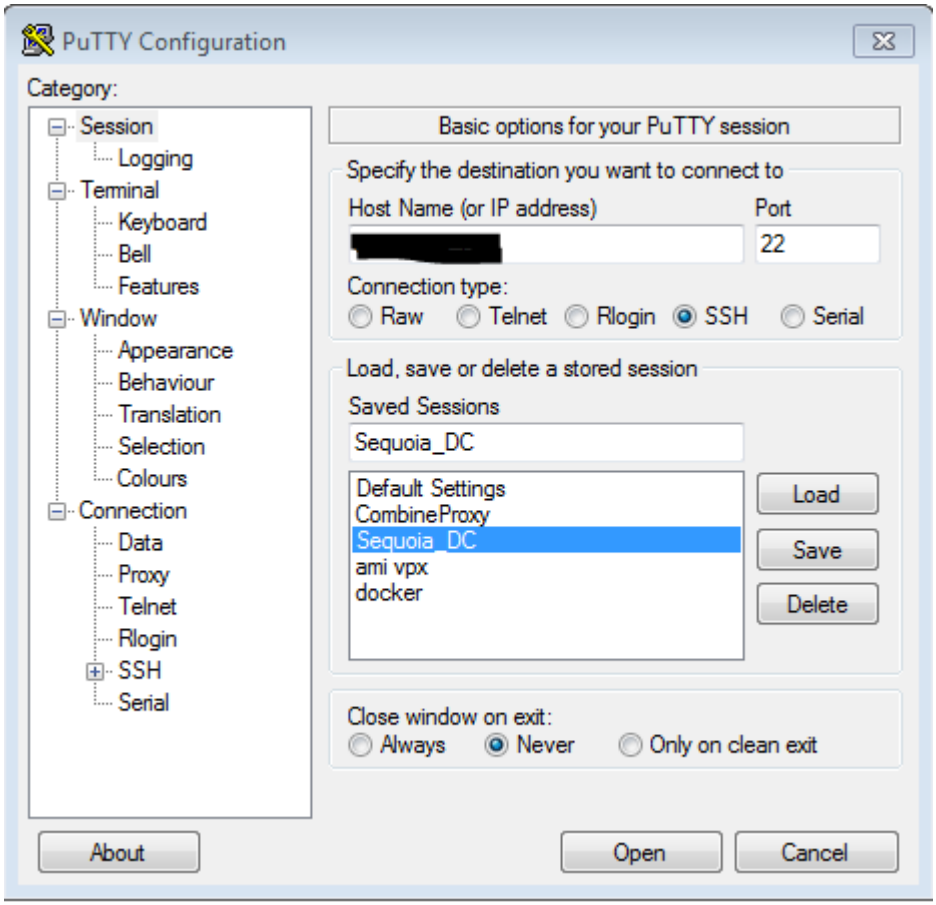
  AMS would provide additional notes and instructions.



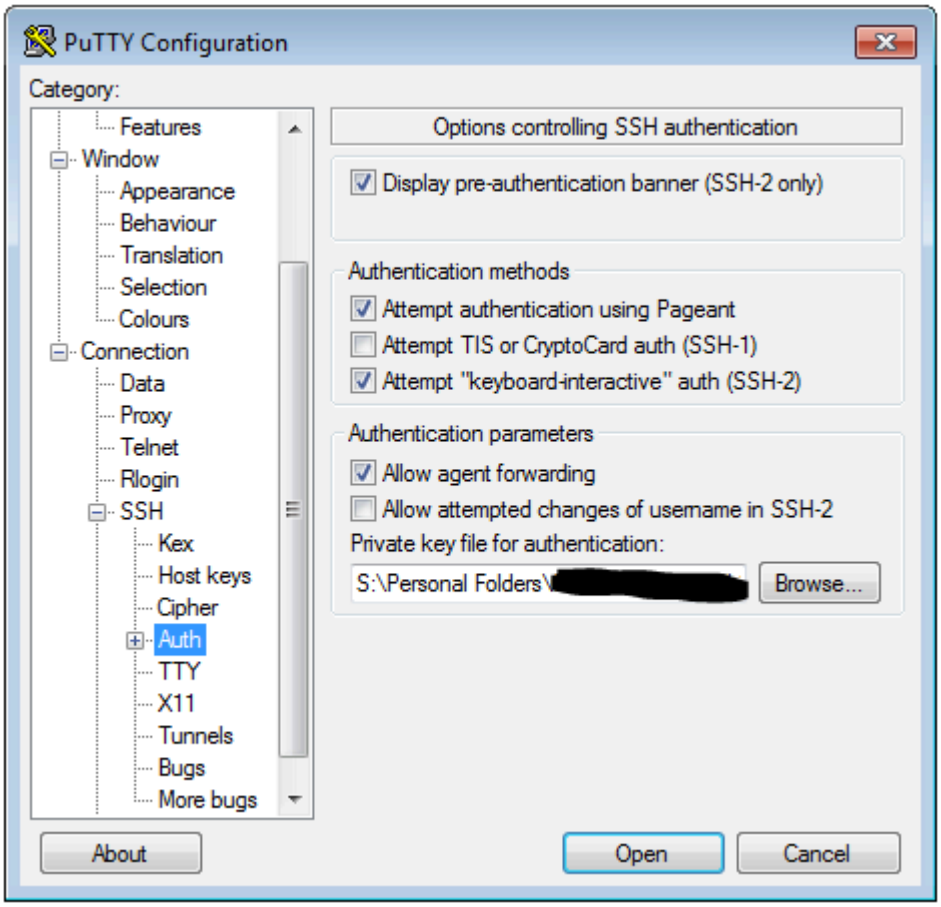

SSH tunneling steps with PuTTy:

Within PuTTY, you would create an SSH session, with the public IP of the bastion host, provide the PEM key in the AUTH section, and then create a Tunnel. The tunnel's source port should be an unused local port (e.g. 5000) and the IP would be the IP of the destination host (the Windows box you are trying to reach) with the RDP port appended (3389). Be sure to save your configuration, as you don't want to have to do it each time you log into the box. Connect to the bastion host, and log in. Then, start an RDP session for localhost:5000 (or whichever port you choose).

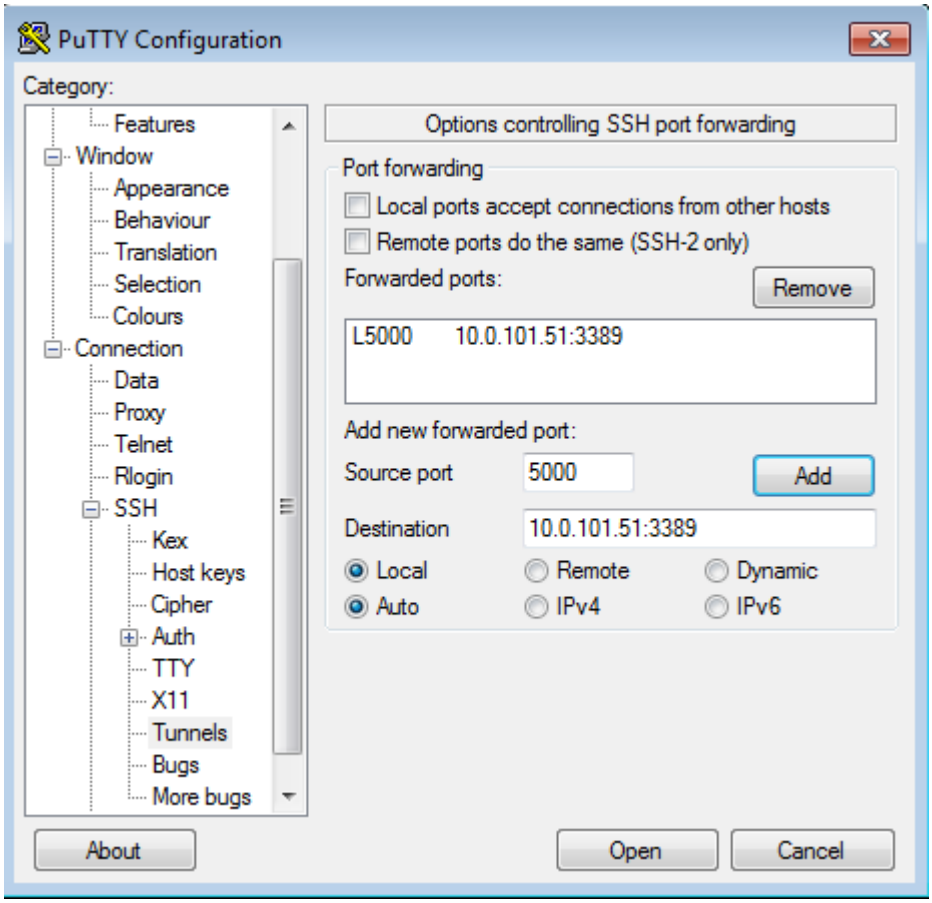
1. Set Host Name or public IP of the bastion host



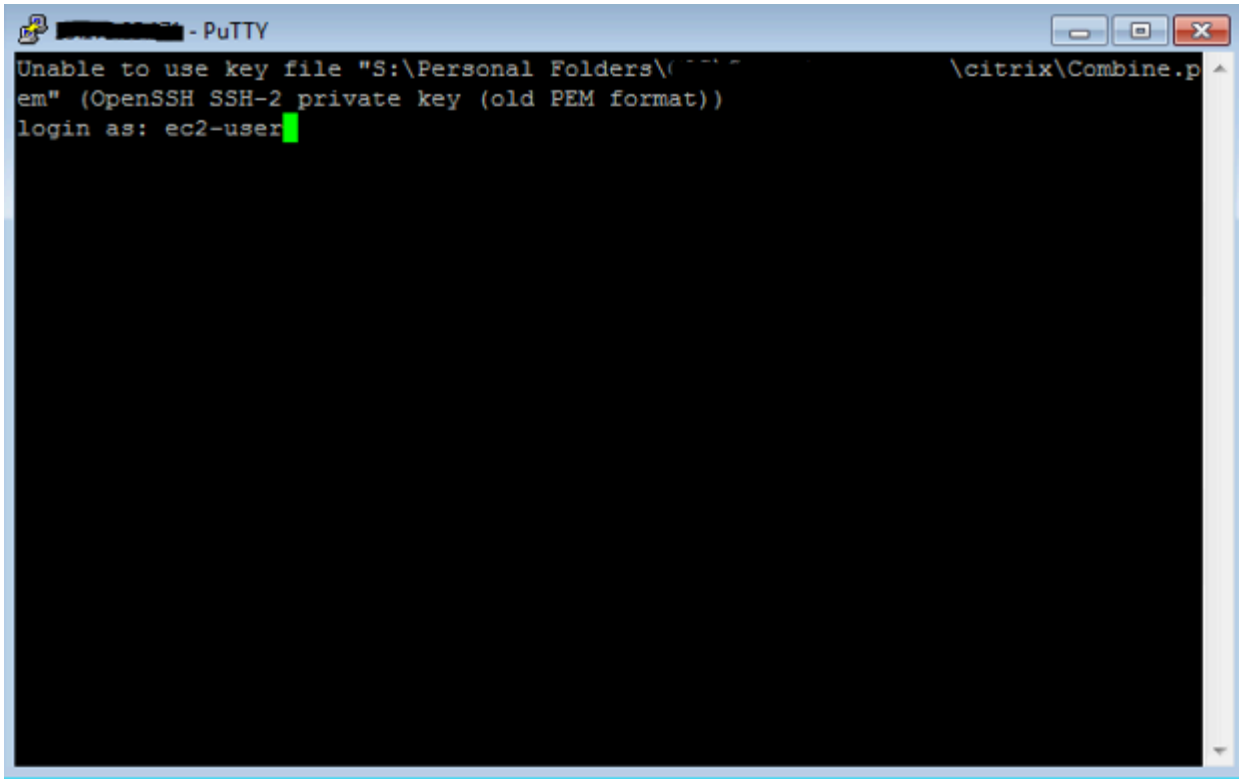

2. In SSH ->Auth, set the private key file in .ppk format



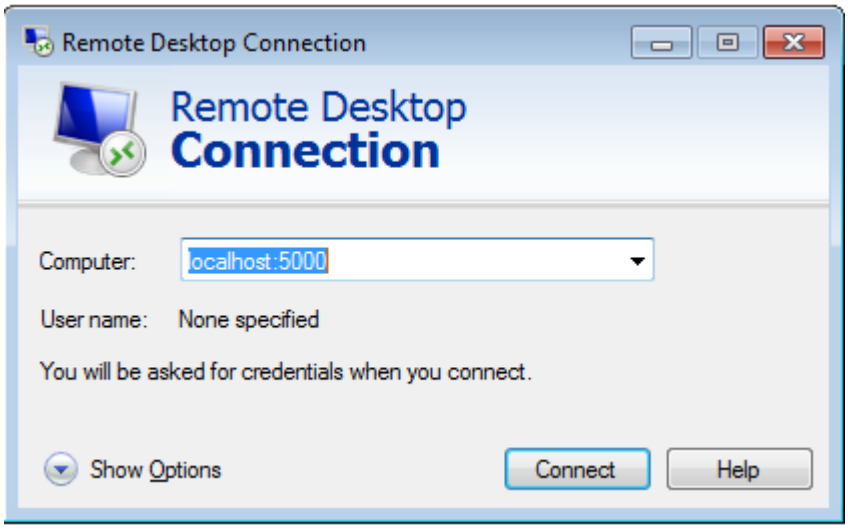

3. In SSH ->Tunnels, add the new forwarded port. The Source Port should be the arbitrary unused port, and the Destination should be the IP of the destination server behind the bastion host, with the RDP port appended.




4. Connect to the bastion host via PuTTY and log in.




5. Start an RDP session to localhost:5000 to reach the destination server.




# SALZ: Set up access management

Using a network managed by AWS Managed Services (AMS) means giving AMS access to manage your cloud infrastructure. You'll need to configure a means of securely connecting between your private network and AMS. This starts with some decisions about the kinds of access you want to provide:

- *For AMS API/CLI and Console access*: You will want to install the AMS CLI (instructions are provided in this document). You use the AMS change management API to make change requests to AMS and the AMS SKMS API to learn about your AMS-managed resources. Using Active Directory Federation Services (AD FS), you can access the AMS Console.

> **Note**
>
> If you are setting up your own ITSM, you will need to use the AWS Support API (SAPI) for service requests and incident reports. SAPI is documented in the AWS Support API Reference.

- *For user access*: Whether you manage users with Windows Active Directory (AD), or a Linux/LDAP solution, connectivity needs to be established between AD on the AMS side (via Directory Services) and your directory.
- *For instance access*: Instance-level access is accomplished via a one-way Forest trust configuration. Directory Services trusts credentials in their CORP AD, allowing stacks within the AMS side to allow login with CORP credentials.

  Note that your Active Directory (AD) that AMS sets up the trust to must be the directory that has the accounts of users authorized by you to gain access to your AWS resources.

> **Important**
>
> To set up a Forest trust, AMS requires your domain controller **Local Policies -> Security Options -> Network Access: Named Pipes that can be accessed anonymously**, have the **Netlogon** and **lsarpc** pipes listed. These pipes are listed by default, but are sometimes removed for security concerns. Once the trust is established, they can be removed from the list again.

## Establish an Active Directory (AD) trust

Before you begin to establish an Active Directory (AD) trust for your AWS Managed Services (AMS) account, make sure that the appropriate firewall ports are open.

The trust from the AMS-managed Active Directory and your corporate directory service allows you to use your corporate-managed credentials to access AMS-managed instances to perform development, test, or administrative functions.

Creating a trust connection is a two-part exercise:

First, configure a conditional forward, a DNS configuration so DNS queries know which DNS server to go to.

Second, configure a trust, an Active Directory (AD) construct to allow access from users in one domain to use resources in another domain.

## Configure the conditional forwarder

Follow this Microsoft AD article Assign a Conditional Forwarder for a Domain Name, and use these settings and choices:

1. In the AD **DNS Manager -> Create a New Conditional Forwarder**, under **DNS Domain:** Use the domain name AMS supplied to you; for example, *`A523434123.amazonaws.com`*.
2. Under **IP addresses of the master servers:** Add the AMS-supplied IP addresses. Make sure there isn't a connection problem by validating both addresses.
3. Select **Store this conditional forwarder in Active Directory and replicate as follows: All DNS servers in this domain** and press **OK**.

## Configure the trust

To configure the trust for your AWS Managed Services (AMS) account, follow this MicroSoft AD article Create a one-way, incoming, forest trust for one side of the trust, using the settings and choices described in this section.

1. Open the **Start -> Administrative Tools -> Active Directory Domains and Trusts** dialog. Right-click the domain node for the domain that you want to establish a trust with, and then click **Properties -> Trusts -> New Trust** to open the New Trust Wizard. Enter the domain name provided to you by AMS for the **Trust Name** and press **Next**.
2. Under **Trust Type**, select **Forest Trust**. Press **Next**.
3. Under **Direction of Trust**, select **One-way: incoming**. Press **Next**.
4. Under **Sides of Trust**, select **This domain only**. Press **Next**.

5. Under **Trust Password**, type a password of your choosing. Press **Next**.
6. For **Trust Selections Completed** and **Trust Creation Complete**, just press **Next**.
7. Under **Confirm Incoming Trust**, select **No**, do not confirm the incoming trust. Press **Next**.
8. Under **Completed the New Trust Wizard**, select **Finish**, and then **OK** to close.
9. Provide the trust password (contact us via your CSDM's phone number for security reasons). AMS will complete the trust configuration.

## Active Directory sites and services

To reduce login latency, add the VPC CIDR range to your Active Directory Sites and Services (**Start -> Administrative Tools -> Active Directory Sites and Services**). Add the VPC CIDR range to an Active Directory Site that contains Domain Controllers that are closest to AWS.

## Active Directory name suffix routing

After the one-way forest trust has been established, please complete the additional steps.

1. Under **Start > All Programs > Administrative Tools**, click **Active Directory Domains and Trusts**.

   The Active Directory Domains and Trusts console opens.
2. Right-click your corporate domain and click **Properties**

   The Properties dialog for that domain opens.
3. Click the **Trusts** tab.

   The Trusts page opens.
4. Click the Amazon domain name and click **Properties**.

   The Properties page for the Amazon domain trust opens.
5. Click **Name Suffix Routing** and click **Refresh**.

   These steps ensure that the Service Principal Names (SPNs) can resolve over the trust.

## Troubleshooting

Some things to try if you run into trouble:

- The AMS-managed Active Directory outbound security group needs to be allowed connection through your CIDR block (e.g. 10.27.0.0/16) to your domain controller.
- Trace the route in the AWS Console from domain controller to domain controller checking all security groups along the way.
- Make sure you can ping the AMS-managed Active Directory Domain Controllers if Internet Control Message Protocol (ICMP) is allowed.
- Make sure your Domain Controller can communicate with AWS Directory Services.
- Make sure the conditional forwarders resolve and are validated.
- If you do not see **Forest Trust** in the New Trust wizard, then your conditional forwarders may not be working correctly:
  - Use nslookup to test resolution
  - Try rebooting the Domain Controller

## 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 Amazon Relational Database Service (Amazon 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 through 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 Service description.

## Federate your Active Directory with the AMS AWS Identity and Access Management roles

The purpose of federating your directory with the AMS IAM roles is to enable corporate users to use their corporate credentials to interact with the AWS Management Console and the AWS APIs, and therefore the AMS console and APIs.

### Federation process example

This example uses Active Directory Federation Services (AD FS); however, any technology that supports AWS Identity and Access Management Federation is supported. For more information on AWS supported IAM federation, see IAM Partners and Identity Providers and Federation. Your CSDM will help you through this process, which involves a joint effort with your AD team and AMS.

For detailed information on integrating SAML for API access, refer to this AWS blog, How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS.

> **Note**
>
> For an example that installs the AMS CLI and SAML, see Appendix: ActiveDirectory Federation Services (ADFS) claim rule and SAML settings.

### Configuring federation to the AMS console (SALZ)

The IAM roles and SAML identity provider (Trusted Entity) detailed in the following table have been provisioned as part of your account onboarding. These roles allow you to submit and monitor RFCs, service requests, and incident reports, as well as get information on your VPCs and stacks.

| Role | Identity Provider | Permissions |
| --- | --- | --- |
| Customer_ReadOnly_Role | SAML | For standard AMS accounts. Allows you to submit RFCs to make changes to |

| Role | Identity Provider | Permissions |
| --- | --- | --- |
| | | AMS-managed infrastructure, as well as create service requests and incidents. |
| customer_managed_ad_user_role | SAML | For AMS Managed Active Directory accounts. Allows you to login to the AMS Console to create service requests and incidents (no RFCs). |

For the full list of the roles available under different accounts see IAM user role in AMS .

A member of the onboarding team uploads the metadata file from your federation solution to the pre-configured identity provider. You use a SAML identity provider when you want to establish trust between a SAML-compatible IdP (identity provider) such as Shibboleth or Active Directory Federation Services, so that users in your organization can access AWS resources. SAML identity providers in IAM are used as principals in an IAM trust policy with the above roles.

While other federation solutions provide integration instructions for AWS, AMS has separate instructions. Using the following blog post, Enabling Federation to AWS Using Windows Active Directory, AD FS, and SAML 2.0, along with the amendments given below, will enable your corporate users to access multiple AWS accounts from a single browser.

After creating the relying party trust as per the blog post, configure the claims rules in the following way:

- **NameId**: Follow the blog post.
- **RoleSessionName**: Use the following values:
  - **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: Follow the blog post.
- Role claim: Follow the blog post, but for the Custom rule, use this:

```
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/"));
```

When using AD FS, you must create Active Directory security groups for each role in the format shown in the following table (customer_managed_ad_user_role is for AMS Managed AD accounts only):

| Group | Role |
| --- | --- |
| AWS-[AccountNo]-Customer_ReadOnly_Role | Customer_ReadOnly_Role |
| AWS-[AccountNo]-customer_managed_ad_user_role | customer_managed_ad_user_role |

For further information, see Configuring SAML Assertions for the Authentication Response.

> **Tip**
> To help with troubleshooting, download the SAML tracer plugin for your browser.

**Submitting the federation request to AMS**

If this is your first account, work with your CSDM(s) and/or Cloud Architect(s) to provide the metadata XML file for your identity provider.

If you are onboarding an additional account or Identity Provider and have access to either the management account or the desired application account, follow these steps.

1. Create a service request from the AMS console, provide the details necessary to add the identity provider:
   - AccountId of the account where the new identity provider will be created.
   - Desired identity provider name, if not provided, the default will be **customer-saml**; typically, this must match the settings configured in your federation provider.
   - For existing accounts, include whether the new identity provider should be propagated to all existing console roles or provide a list of roles that should trust the new identity provider.

- Attach the metadata XML file exported from your federation agent to the service request as a file attachment.

2. From the same account where you created the service request, create a new RFC using CT-ID ct-1e1xtak34nx76 (Management | Other | Other | Create) with the following information.

   - Title: "Onboard SAML IDP <Name> for Account <AccountId>".
   - AccountId of the account where the identity provider will be created.
   - Identity provider name.
   - For Existing Accounts: Whether the identity provider should be propagated to all existing console roles, or the list of roles which should trust the new identity provider.
   - Case ID of service request created in Step 1, where the metadata XML file is attached.

## Verify console access

Once you are set up with ADFS, and have the AMS URL to use for authentication, follow these steps.

With an Active Directory Federated Service (ADFS) configuration, you can follow these steps:

1. Open a browser window and go to the sign in page provided to you for your account. The ADFS **IdpInitiatedSignOn** page for your account opens.
2. Select the radio button next to **Sign in to one of the following sites**. The **Sign in** site picklist becomes active.
3. Choose the **signin.aws.amazon.com** site and click **Sign in**. Options for entering your credentials open.
4. Enter your CORP credentials and click **Sign in**. The AWS Management Console opens.
5. Paste into the location bar the URL of the AMS console and press **Enter**. The AMS console opens.

## Verify API access

AMS uses the AWS API, with some AMS-specific operations that you can read about in the AMS API Reference.

AWS provides several SDKs that you can access at Tools for Amazon Web Services. If you don't want to use an SDK, you can make direct API calls. For information on authentication, see Signing

AWS API Requests. If you are not using an SDK, or making direct HTTP API requests, you can use the AMS CLIs for Change Management (CM) and SKMS.

**Install the AMS CLIs**

For an example of installing the AWS Managed Services (AMS) CLI to use with SAML, see Appendix: ActiveDirectory Federation Services (ADFS) claim rule and SAML settings.

If you need temporary access, in order to get and install the AWS Managed Services (AMS) SDKs, see Temporary AMS console access.

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

The AWS CLI is a prerequisite for using the AWS Managed Services (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 **Developer's Resources** link in the left nav of the AMS console.
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: **AWSManagedServices_InstallCLI.sh** by running this command: `sh AWSManagedServices_InstallCLI.sh`. Note that the **amscm** and **amsskms** directories and their contents must be in the same directory as the **AWSManagedServices_InstallCLI.sh** file.

4. If your corporate credentials are used through 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.

> **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. You may need to add a `--profile` option for authentication; for example, `aws amsskms` *`ams-cli-command`* `--profile SAML`. You may also need to add the `--region` option as all AMS commands run out of us-east-1; for example `aws amscm` *`ams-cli-command`* `--region=us-east-1`.

## Scheduling AMS backups at the VPC level

AWS Managed Services (AMS) backup scheduling in the VPC, where the target instances are allocated, is created during account onboarding with a default tag in the VPC creation schema. The backup system schedules the execution of the snapshots depending on that VPC Tag. Modification of the schedule can be made by creating a service request. For more information, see VPC Tag and Defaults.

For backup defaults, see Understanding AMS Defaults

# SALZ: Default settings

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 security, access, monitoring, logging, continuity, and patching, management.

For an example of infrastructure costs, see Basic components.

Firewall rules are provided in Set up your Firewall

## 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) |

| Setting | Default |
| --- | --- |
| Activation of multiple computers with the same host name | Is allowed |
| Alerts for pending updates are raised | After seven days |
| Update schedule | AMS targets a monthly release cycle for Trend Micro Deep Security Manager (DSM) / Deep Security Agent (DSA) software updates. However, AMS doesn't maintain an SLA for updates. Updates are performed fleet-wide by AMS developer teams during a deployment.<br><br>DSA/DSA updates are logged in Trend Micro DSM system events that AMS retains locally by default for 13 weeks. For vendor documenta tion, see System events in the Trend Micro Deep Security Help Center. Logs are also exported to log group /aws/ams/eps/var/log/DSM.log in Amazon CloudWatch. |
| 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 | Quarantine all suspected viruses. Enable IntelliTrap and spyware/grayware protection.<br><br>Spyware and Grayware trigger Anti-Malware and result in a quarantine of the item. |
| | Every Day/All Day (24 hours) | |

| Setting | Default | Notes |
| --- | --- | --- |
| 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 |

## 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 (restrict s outbound traffic to members of the same security group) |
| All traffic | All | All | SentinelDefaultSecurityGroupPrivateOnlyEgress All (does not restrict outbound traffic) |
| HTTP, HTTPS, SSH, RDP | TCP | 80 / 443 (Source 0.0.0.0/0)<br><br>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)<br><br>SSH and RDP access is allowed from bastions | SentinelDefaultSecurityGroupPublic (does not restrict outbound traffic) |
| **MALZ bastions**: | | | |

| Type | Protocol | Port range | Source |
|---|---|---|---|
| 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 `Deployment | Advanced stack components | Security group | Create (review required)` change type (ct-1oxx2g2d7hc90).

For Active Directory (AD) security group modifications, use the following change types:

- To add a user: Submit an RFC using Management | Directory Service | Users and groups | Add user to group [ct-24pi85mjtza8k]
- To remove a user: Submit an RFC using Management | Directory Service | Users and groups | Remove user from group [ct-2019s9y3nfml4]

> **Note**
>
> When using "review required" CTs, AMS recommends that you use the ASAP **Scheduling** 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`.

## 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

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` | `AmazonSSMManagedInstanceCore` : Allows Ec2 instances to use the SSM agent. |
| | `AMSInstanceProfileLoggingPolicy` : Allows Ec2 instances to push logs to S3 and CloudWatch. |

| Profile | Policies |
| --- | --- |
| | `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` | `AMSInstanceProfileBYOEPSPolicy` : Allows Ec2 instances to use AMS bring your own EPS. |
| | `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

There is one AMS default instance profile, `customer-mc-ec2-instance-profile`, that grants permissions from the IAM instance policy `customer_ec2_instance_profile_policy`. 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).** | | | |
|---|---|---|---|
| **Policy statement** | **Effect** | **Actions** | **Description and resource (ARN)** |
| **Amazon Elastic Compute Cloud (Amazon EC2)** | | | |
| EC2 Message Actions | Allow | AcknowledgeMessage,<br>DeleteMessage,<br>FailMessage,<br>GetEndpoint,<br>GetMessages,<br>SendReply | Allows EC2 Systems Manager messaging actions in your account. |
| 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-*` |

| CW = CloudWatch. ARN = Amazon Resource Name. * = wildcard (any). | | | |
|---|---|---|---|
| **Policy statement** | **Effect** | **Actions** | **Description and resource (ARN)** |
| | | Create Log Stream | Allows logs to be streamed to: `aws:logs:*:*:log-group:i-*` |
| CW For MMS | Allow | DescribeAlarms,<br>PutMetricAlarm,<br>PutMetricData | Allows CloudWatch to retrieve alarms in your account.<br>Allows CW to create or update an alarm and associate it with the specified metric.<br>Allows CW to publish metric data points to your account. |
| Ec2 Tags | Allow | CreateTags,<br>DescribeTags, | Allows tags to be added, overwritten, and described on the specified instances in your account. |
| Explicitly Deny CW Logs | Deny | DescribeLogStreams,<br>FilterLogEvents,<br>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,<br>GetDocument,<br>ListAssociations,<br>UpdateAssociationStatus,<br>UpdateInstanceInformation | Allows a variety of SSM functions in your account. |

| CW = CloudWatch. ARN = Amazon Resource Name. * = wildcard (any). | | | |
|---|---|---|---|
| **Policy statement** | **Effect** | **Actions** | **Description and resource (ARN)** |
| SSM Access In S3 | Allow | GetObject,<br>PutObject,<br>AbortMultipartUpload,<br>ListMultipartUploadPorts,<br>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*` . |
| **Amazon EC2 Simple Storage Service (S3)** | | | |
| Get Object In S3 | Allow | Get<br>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}/*` |

| CW = CloudWatch. ARN = Amazon Resource Name. * = wildcard (any). | | | |
|---|---|---|---|
| **Policy statement** | **Effect** | **Actions** | **Description and resource (ARN)** |
| Explicitly Deny MC Namespace S3 Logs | Deny | GetObject*<br><br>Put* | Disallows EC2 applications getting or putting any objects from or to:<br><br>`aws:s3:::mc-*-logs-*/encrypted/mc*` ,<br><br>`aws:s3:::mc-*-logs-*/mc/*`,<br><br>`aws:s3:::mc-a*-logs-*-audit/*` |
| Explicitly Deny S3 Delete | Deny | * (all) | Disallows EC2 applications taking any action on objects in:<br><br>`aws:s3:::mc-a*-logs-*/*` ,<br><br>`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-*` |
| **AWS Secrets Manager in Amazon EC2** | | | |

| CW = CloudWatch. ARN = Amazon Resource Name. * = wildcard (any). | | | |
|---|---|---|---|
| **Policy statement** | **Effect** | **Actions** | **Description and resource (ARN)** |
| Trend Cloud One Secrets Access | Allow | GetSecretValue | Allows Amazon EC2 to access secrets for Trend Cloud One migration:<br>`aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id* ,`<br>`arn:aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-activation-token* ,`<br>`aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id* ,`<br>`aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-guid*` |
| **AWS Key Management Service in Amazon EC2** | | | |
| Trend Cloud One Decryption Key | Allow | Decrypt | Allow Amazon EC2 to decrypt the AWS KMS key with alias name /ams/eps/cloudone-migration<br>`arn:aws:kms:*:*:alias/ams/eps/cloudone-migration` |

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.

## Monitored metrics defaults

The following table shows what is monitored and the default alerting thresholds. You can change the defaults with a change management request for change (RFC).

> **Note**
>
> CloudWatch launched extended retention of metrics in November 1, 2016. For more information, see CloudWatch Limits.

### Alerts from baseline monitoring

| Service | 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 correct 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<br><br>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 | No | TargetConnectionErrorCount | CloudWatch alarm if number of connections were unsuccess |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| Balancer (ALB) target | | sum > 0 for 1 min, 5 consecutive times. | fully established between the load balancer and the registered instances. |
| Amazon EC2 instance – Windows | No | SecureChannelFailure<br><br>> 0.0 for 10 out of the last 15 data points. | CloudWatch alarm on Windows instances to alert when Secure a Channel connection has failed. |
| Aurora instance | No | CPUUtilization<br><br>> 85% for 5 mins, 2 consecutive times. | CloudWatch alarm. |
| AWS Backup | Yes | DeleteRecoveryPoint<br><br>An unexpected IAM role principal or IAM user principal has deleted an AWS Backup recovery point. | CloudWatch event. Emitted when a backup recovery point is deleted. |
| AWS Outposts | Yes | AMSOutpostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability<br><br>= 80% for 5 minutes, 12 consecutive times. | CloudWatch alarm on instance family capacity availability of the AWS Outposts resource. |
| | | AMSOutpostsInstanceTypeCapacityAvailability TypeCapacityAvailability<br><br>= 80% for 5 minutes, 12 consecutive times. | CloudWatch alarm on instance type capacity availability of the AWS Outposts resource. |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| | | AMSOutpostsConnectedStatusConnectedStatus<br><br>< 1 for 5 minutes, 1 consecutive time. | CloudWatch alarm on AWS Outposts service link connection, less than 1 count is impaired. |
| | | AMSOutpostsCapacityExceptionCapacityExceptions<br><br>0 for 5 minutes, 1 consecutive time. | CloudWatch alarm on insufficient capacity errors for instance launches for AWS Outpostss resource<br>. |
| EC2 instance - all OSs | No | CPUUtilization*<br><br>>= 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<br><br>> 0 for 5 minutes, 3 consecutive times. | CloudWatch alarm. |
| | | Root Volume Usage<br><br>>= 95% for 5 mins, 6 consecutive times. | |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| | | Non-root Volume Usage<br><br>> 85% for 5 mins, 2 consecutive times.<br><br>**Disabled by default; for additional information, see https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info**. | |
| | | Memory Free*<br><br>MemoryFree < 5% for 5 minutes, 6 consecutive times. | |
| | Yes | EPS Malware<br><br>Malware found on instance. | CloudWatch event. |
| Amazon EC2 instance - Linux | No | Root Volume Inode Usage<br><br>Average >= 95% for 5 mins, 6 consecutive times. | CloudWatch alarm. Applied to Linux instances only. |
| | | Swap Free*<br><br>Memory Swap < 5% for 5 minutes, 6 consecutive times. | |

| Service | Security alert | Alert name and trigger condition | Notes |
| --- | --- | --- | --- |
| ElastiCache Cluster | No | CurrConnections = 65000 | This alarm notifies AMS of the maximum connection limit of an ElastiCache Host.<br><br>CloudWatch Alarm. If you would like to update this threshold, contact AMS support. |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| ElastiCache Node | No | CPUUtilization<br><br>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:<br><br>• cache.t1.micro: 90%<br>• cache.m1.small: 90%<br>• cache.m1.medium: 90%<br>• cache.m1.large: 45%<br>• cache.m1.xlarge: 22.5%<br>• cache.m2.xlarge: 45%<br>• cache.m2.4xlarge: 11.25%<br>• cache.c1.xlarge: 11.25%<br>• cache.t2.micro: 90%<br>• cache.t2.small: 90%<br>• cache.t2.medium: 45%<br>• cache.m3.medium: 90%<br>• cache.m3.large: 45%<br>• cache.m3.xlarge: 22.5%<br>• cache.m3.2xlarge: 11.25%<br>• cache.r3.large: 45%<br>• cache.r3.xlarge: 22.5%<br>• cache.r3.2xlarge: 11.25%<br>• cache.r3.4xlarge: 5.625%<br>• cache.r3.8xlarge: 2.8125% |
| ElastiCache Node - memcached | No | SwapUsage<br><br>maximum > 50,000,000 bytes for 5 mins, 5 consecutive times. | CloudWatch alarm. Applied to memcached only. |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| OpenSearch cluster | No | ClusterStatus.red<br><br>maximum is >= 1 for 1 minute, 1 consecutive time.<br><br>*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<br><br>>= 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. |
| | | ClusterStatus.yellow<br><br>maximum is >= 1 for 1 minute, 1 consecutive time<br><br>*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<br><br>minimum is <= 20480 for 1 minute, 1 consecutive time<br><br>*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. |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| | | ClusterIndexWritesBlocked<br><br>>= 1 for 5 minutes, 1 consecutive time<br><br>*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<br><br>minimum is < x for 1 day, 1 consecutive time<br><br>*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<br><br>average is >= 80% for 15 minutes, 3 consecutive times<br><br>*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. |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| | | JVMMemoryPressure<br><br>maximum is >= 80% for 5 minutes, 3 consecutive times<br><br>*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 . |
| | | MasterCPUUtilization<br><br>average is >= 50% for 15 minutes, 3 consecutive times<br><br>*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<br><br>maximum is >= 80% for 15 minutes, 1 consecutive time<br><br>*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. |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| OpenSearch instance | No | AutomatedSnapshotFailure<br><br>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<br><br>> 100 for 1 minute, 15 consecutive times. | CloudWatch alarm if an excess number of requests are pending routing. |
| | | HTTPCode_ELB_5XX_Count<br><br>sum > 0 for 5 min, 3 consecutive times. | CloudWatch alarm on excess number of HTTP 5XX response codes that originate from the load balancer. |
| | | SpilloverCount<br><br>> 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.<br><br>Changes in the GuardDuty findings. These changes include newly generated findings or subsequent occurrences of existing findings. | List of supported GuardDuty finding types are on GuardDuty Active Finding Types. |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| Health | Varies | AWS Health Dashboard | Notifications are sent when there are changes in the status of AWS Health Dashboard (AWS Health) events in relation to baseline services supported by AMS. For more information, see Supported services. |
| AWS Managed Microsoft AD | No | Active Directory Status<br><br>AWS Managed Microsoft AD instance sends an active status event. | Service event. Emitted when the directory is operating normally after an event. |
| | | Impaired Directory Status<br><br>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<br><br>AWS Managed Microsoft AD instance sends an inoperable status event. | Service event. Emitted when the directory is not functiona l. All directory endpoints have reported issues. |
| | | Deleting Directory Status<br><br>AWS Managed Microsoft AD instance sends a deleting directory status event. | Service event. Emitted when the directory is currently being deleted. |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| | | Failed Directory Status<br><br>AWS Managed Microsoft AD instance sends a failed status event. | Service event. Emitted when the directory could not be created. |
| | | RestoreFailed Directory Status<br><br>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 | 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. |
| | | DB instance fail<br><br>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. |
| | | Failover not attempted<br><br>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. |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| | | DB instance invalid parameters<br><br>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. |
| | | Invalid subnet IDs DB instance<br><br>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. |
| | | DB instance read replica error<br><br>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. |
| | | DB instance read replication ended<br><br>Replication on the Read Replica was ended. | Service event. RDS-EVENT-0057, Amazon RDS Event Categories and Event Messages. |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| | | Error create statspack user account<br><br>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 recovery start<br><br>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. |
| | | A failover for the DB cluster has failed. | RDS-EVENT-0069, see details at Amazon RDS Event Categories and Event Messages. |
| | | Invalid permissions recovery S3 bucket<br><br>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. |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| | | Aurora was unable to copy backup data from an Amazon S3 bucket. | RDS-EVENT-0082, see details at Amazon RDS Event Categories and Event Messages. |
| | | 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. |
| | | The DB instance is in an invalid state. No actions are necessary. Autoscaling will retry later. | RDS-EVENT-0219, see details at Amazon RDS Event Categories and Event Messages. |
| | | The DB instance has reached the storage-full threshold, and the database has been shut down. | RDS-EVENT-0221, see details at Amazon RDS Event Categories and Event Messages. |
| | | This event indicates the RDS instance storage autoscaling is unable to scale, there could be multiple reasons for why the autoscaling failed. | RDS-EVENT-0223, see details at Amazon RDS Event Categories and Event Messages. |
| | | Storage autoscaling has triggered a pending scale storage task that would reach the maximum storage threshold. | RDS-EVENT-0224, see details at Amazon RDS Event Categories and Event Messages. |
| | | The DB instance has a storage type that's currently unavailable in the Availability Zone. Autoscaling will retry later. | RDS-EVENT-0237, see details at Amazon RDS Event Categories and Event Messages. |

| Service | Security alert | Alert name and trigger condition | Notes |
|---|---|---|---|
| | | RDS couldn't provision capacity for the proxy because there aren't enough IP addresses available in your subnets. | RDS-EVENT-0243, see details at Amazon RDS Event Categories and Event Messages. |
| | | The storage for your AWS account has exceeded the allowed storage quota. | RDS-EVENT-0254, see details at Amazon RDS Event Categories and Event Messages. |
| | | CPUUtilization<br><br>Average CPU utilization > 90% for 15 mins, 2 consecutive times. | CloudWatch alarm. |
| | | DiskQueueDepth<br><br>Sum is > 75 for 1 mins, 15 consecutive times. | |
| | | FreeStorageSpace<br><br>Average < 1,073,741,824 bytes for 5 mins, 2 consecutive times. | |
| | | SwapUsage<br><br>Average >= 104,857,600 bytes for 5 mins, 2 consecutive times. | |
| Amazon Redshift cluster | No | RedshiftClusterStatus<br><br>The health of the cluster when not in maintenance mode < 1 for 5 min. | 1 represents a healthy cluster. |

| Service | Security alert | Alert name and trigger condition | Notes |
| --- | --- | --- | --- |
| Amazon Macie | Yes | Newly generated alerts and updates to existing alerts.<br><br>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 Analyzing Amazon Macie Findings. Note that Macie is not enabled for all accounts. |

## 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.

# Continuity management defaults

This section describes AMS continuity management defaults; for more information on AMS backups, see the AMS User Guide Continuity Management chapter.

Backup configuration is done at the time of onboarding. These are the default (recommended) backup settings.

## VPC tag and defaults

For the most current information on AMS backup, see Continuity management.

> **Important**
>
> By default, EC2 stack backups are disabled (Backup = False). You can enable EC2 instance backups at the time of creation by adding a tag `Key: Backup, Value: True` when requesting an EC2 stack through an RFC (CT ct-14027q0sjyt1h). If you want to add the tag after the instance has been created, submit an RFC with the Management | Advanced stack components | EC2 instance stack | Update CT (ct-38s4s4tm4ic4u).

## EC2 instance tag and defaults

The **EC2 stack backup tag** specifies whether the stack requires a snapshot of the attached EBS volumes or not.

Tag `Key: Backup`

Tag `Value: True, False`

By default, the value is `False` the backup tag is not present, and the stack does not have scheduled backups.

Change the tag `Key: Backup` to `Value: True` to enable backups, which are then done on the schedule set with the VPC backup tag.

> **Note**
>
> The casing for the tag value (Value only) is insensitive, so True/true or False/false are all acceptable.

### RDS instance backup and defaults

The Amazon Relational Database Service (RDS) default values are defined in the stack templates:

```
Backup: Yes

Backup Window: 22:00-23:00 (RDS local time zone)

Retention Period: 7 (7 snapshots stored)
```

## Patching defaults

This section describes AMS patching defaults; for more information on AMS patching, see the AMS User Guide Patch Management chapter.

AMS releases patched AMIs on a monthly basis; all new stack requests should be configured with the latest AMS AMI.

> **Important**
>
> AMS Patch Orchestrator, tag-based patching, uses AWS Systems Manager (SSM) functionality to allow you to tag, or have AMS tag for you, instances and have those instances patched using a baseline and a window that you configure. To learn more, see Patch Orchestrator: a tag-based patching model.

AMS-standard, account-based, patching: For each account with stacks that receive in-place patching, a notification of upcoming applicable patches is sent out shortly after “patch Tuesday”. The notification contains a list of all stacks and the applicable patches as well as the suggested patch window. For critical patches, the window is set no longer than 10 days in advance, and for standard patching no more than 14 days in advance. If you do not reply to the notification, patching does not occur. If you would like to exclude certain patches, reply to the notification, or submit a service request. If you reply with consent to patching, but don’t specifically request a different schedule, patches are applied as described in the notification that you receive.

> **Note**
>
> The patch service notification is an email sent to the account contacts and contains a link to the AWS Support console. You can reply through the AWS Support console or through the AMS service request page, where the notification appears as a service notification.

At the time of the AMS-standard patching process, AMS performs the following:

1. You are sent a patching service notification fourteen days before the proposed patch window. The patching service notification is sent via email to the contact email address that you have on file for your account.
2. Identifies all reachable EC2 instances in the stack based on the list of stacks provided in the patching notification. In this case, "Reachable" means instances that are in the "Running" EC2 state, and have the EC2 Run Command agent fully operational.
3. AMS performs patching in a manner that ensures that a sufficient number of EC2 instances are running concurrently (configured through the `healthy-host-threshold` setting) so that the stack remains healthy.
4. After the patching operation is complete for all EC2 instances, AMS updates the RFC with the patching status: Success, Partial Success or Failure. In the case of any status other than Success, a ticket is created for an operator to follow up on the patching results and take any corrective actions.

# Validate the AMS service (SALZ)

To validate that the AWS Managed Services (AMS) service is working as expected, some exercise that you can do are described in this chapter.

## Find AMS account settings

Account settings that are used to create AMS RFCs, set schedules, and determine who receives notifications.

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 **Developer's resources** page, 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 after you have installed the AMS SKMS CLI (this command uses a SAML profile, remove if your authentication method is different):

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

**Important**

**Note**

The AMS API/CLI (amscm and amsskms) endpoints are in the AWS N. Virginia Region, `us-east-1`. Depending on how your authentication is set, and what AWS Region your account and resources are in, you may need to add `--region us-east-1` when issuing commands. You may also need to add `--profile saml`, if that is your authentication method.

## Find FQDNs in AMS

AWS Managed Services (AMS) access change types (CTs) require the fully qualified domain name, or FQDN, of your AMS-trusted domain, in the form of `C844273800838.amazonaws.com`. To discover your AWS FQDN, do one of the following:

- AWS Console: Look in the AWS Directory Service console in the **Directory name** column.
- 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
  ```

**Note**

The AMS API/CLI (amscm and amsskms) endpoints are in the AWS N. Virginia Region, `us-east-1`. Depending on how your authentication is set, and what AWS Region your

account and resources are in, you may need to add `--region us-east-1` when issuing commands. You may also need to add `--profile saml`, if that is your authentication method.

## Find availability zones (AZs) in AMS

**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.

- AMS Console: In the navigation pane click **VPCs**, and then click the relevant VPC, if necessary. On the VPCs details page, select the relevant subnet in the table of subnets to open the subnet details page with the name of the associated availability zone.
- AMS SKMS API/CLI:

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

> **Note**
>
> The AMS API/CLI (amscm and amsskms) endpoints are in the AWS N. Virginia Region, `us-east-1`. Depending on how your authentication is set, and what AWS Region your account and resources are in, you may need to add `--region us-east-1` when issuing commands. You may also need to add `--profile saml`, if that is your authentication method.

## Find SNS topics in AMS

Your SNS topics determine who is notified under various circumstances. AMS provides SNS topics for AMI notifications (see AMS AMI notifications with SNS), CloudWatch alarms and EC2 resources (see Receiving alerts generated by AMS) and more. To discover your existing SNS topics:

- AWS 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, requires the AWS CLI):

List your SNS topics:

```
aws sns list-topics
```

List your SNS subscriptions:

```
aws sns list-subscriptions
```

> **Note**
>
> The AMS API/CLI (amscm and amsskms) endpoints are in the AWS N. Virginia Region, `us-east-1`. Depending on how your authentication is set, and what AWS Region your account and resources are in, you may need to add `--region us-east-1` when issuing commands. You may also need to add `--profile saml`, if that is your authentication method.

### Find backup settings in AMS

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. To find your AMS account AWS Backup settings, use the https://console.aws.amazon.com/backup console, or the *AWS CLI Command Reference* for backup commands.

For more information about AMS and AWS Backup, see Continuity Management.

## Finding an instance ID or IP address

You need an instance IP address to log into the instance.

- 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. You may need to add a `--profile` option for authentication; for example, `aws amsskms` *`ams-cli-command`* `--profile SAML`. You may also need to add the `--region` option as all AMS commands run out of us-east-1; for example `aws amscm` *`ams-cli-command`* `--region=us-east-1`.

> **Note**
>
> The AMS API/CLI (amscm and amsskms) endpoints are in the AWS N. Virginia Region, `us-east-1`. Depending on how your authentication is set, and what AWS Region your account and resources are in, you may need to add `--region us-east-1` when issuing commands. You may also need to add `--profile saml`, if that is your authentication method.

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"
    }
}
```

## 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`

## Finding bastion IP addresses

AMS customers can use SSH and RDP bastions, either the DNS friendly bastion names 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.

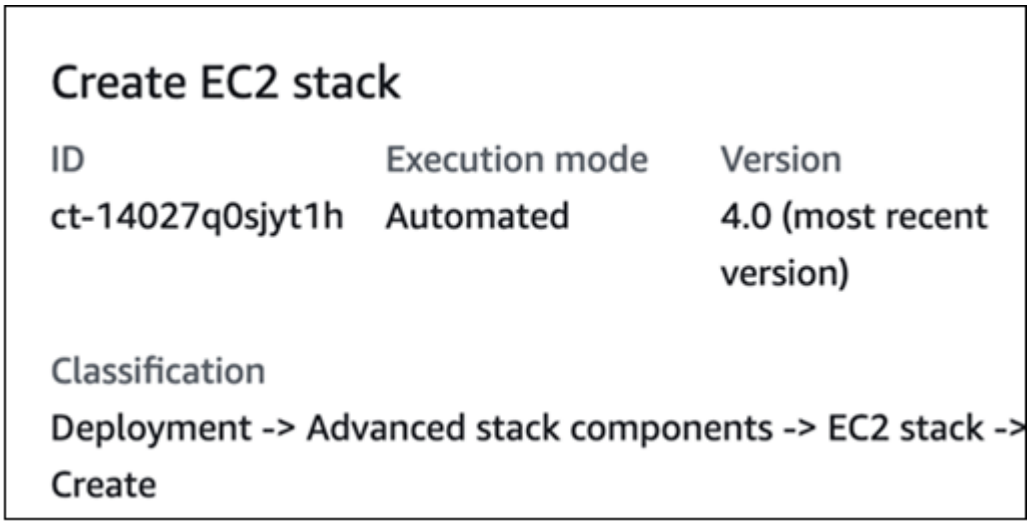
# EC2 instances: Creating

You can use the AMS console or API/CLI to create an Amazon EC2 and an Amazon EC2 with additional volumes.

## Create stack

### Creating an EC2 instance with the console

The following shows this change type in the AMS console.




How it works:

1. Navigate to the **Create RFC** page: In the left navigation pane of the AMS console click **RFCs** to open the RFCs list page, and then click **Create RFC**.

2. Choose a popular change type (CT) in the default **Browse change types** view, or select a CT in the **Choose by category** view.
   - **Browse by change type**: You can click on a popular CT in the **Quick create** area to immediately open the **Run RFC** page. Note that you cannot choose an older CT version with quick create.

     To sort CTs, use the **All change types** area in either the **Card** or **Table** view. In either view, select a CT and then click **Create RFC** to open the **Run RFC** page. If applicable, a **Create with older version** option appears next to the **Create RFC** button.
   - **Choose by category**: Select a category, subcategory, item, and operation and the CT details box opens with an option to **Create with older version** if applicable. Click **Create RFC** to open the **Run RFC** page.
3. On the **Run RFC** page, open the CT name area to see the CT details box. A **Subject** is required (this is filled in for you if you choose your CT in the **Browse change types** view). Open the **Additional configuration** area to add information about the RFC.

   In the **Execution configuration** area, use available drop-down lists or enter values for the required parameters. To configure optional execution parameters, open the **Additional configuration** area.
4. When finished, click **Run**. If there are no errors, the **RFC successfully created** page displays with the submitted RFC details, and the initial **Run output**.
5. Open the **Run parameters** area to see the configurations you submitted. Refresh the page to update the RFC execution status. Optionally, cancel the RFC or create a copy of it with the options at the top of the page.

**Creating an EC2 instance with the CLI**

How it works:

1. Use either the Inline Create (you issue a `create-rfc` command with all RFC and execution parameters included), or Template Create (you create two JSON files, one for the RFC parameters and one for the execution parameters) and issue the `create-rfc` command with the two files as input. Both methods are described here.
2. Submit the RFC: `aws amscm submit-rfc --rfc-id` *`ID`* command with the returned RFC ID.

   Monitor the RFC: `aws amscm get-rfc --rfc-id` *`ID`* command.

To check the change type version, use this command:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> You can use any `CreateRfc` parameters with any RFC whether or not they are part of the schema for the change type. For example, to get notifications when the RFC status changes, add this line, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` to the RFC parameters part of the request (not the execution parameters). For a list of all CreateRfc parameters, see the AMS Change Management API Reference.

*INLINE CREATE*:

Issue the create RFC command with execution parameters provided inline (escape quotation marks when providing execution parameters inline), and then submit the returned RFC ID. For example, you can replace the contents with something like this:

```
aws amscm create-rfc --change-type-id "ct-14027q0sjyt1h" --change-type-version "4.0"
 --title "EC2-Create-RFC" --execution-parameters "{\"Description\": \"Create a new
 EC2 Instance stack\",\"VpcId\": \"vpc-0a60eb65b4EXAMPLE\",\"Name\": \"My-EC2\",
\"TimeoutInMinutes\": 60,\"Parameters\": {\"InstanceAmiId\": \"ami-1234567890EXAMPLE\",
\"InstanceDetailedMonitoring\": false,\"InstanceEBSOptimized\": false,\"InstanceProfile
\": \"customer-mc-ec2-instance-profile\",\"InstanceRootVolumeIops\": 3000,
\"InstanceRootVolumeType\": \"gp3\",\"InstanceType\": \"t2.large\",\"InstanceUserData
\": \"\",\"InstanceSubnetId\": \"subnet-0bb1c79de3EXAMPLE\",\"EnforceIMDSV2\":
 \"false\"}}"
```

*TEMPLATE CREATE*:

1. Output the execution parameters for this change type to a JSON file; this example names it CreateEC2Params.json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-14027q0sjyt1h" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2Params.json
   ```

2. Modify and save the CreateEC2Params file. For example, you can replace the contents with something like this:

```
{
  "Description": "Create a new EC2 Instance stack",
  "VpcId": "vpc-0a60eb65b4EXAMPLE",
  "Name": "My-EC2",
  "TimeoutInMinutes": 60,
  "Parameters": {
    "InstanceAmiId": "ami-1234567890EXAMPLE",
    "InstanceDetailedMonitoring": false,
    "InstanceEBSOptimized": false,
    "InstanceProfile": "customer-mc-ec2-instance-profile",
    "InstanceRootVolumeIops": 3000,
    "InstanceRootVolumeType": "gp3",
    "InstanceType": "t2.large",
    "InstanceUserData": "",
    "InstanceSubnetId": "subnet-0bb1c79de3EXAMPLE",
    "EnforceIMDSV2": "false"
  }
}
```

3. Output the RFC template to a file in your current folder; this example names it CreateEC2Rfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2Rfc.json
```

4. Modify and save the CreateEC2Rfc.json file. For example, you can replace the contents with something like this:.

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-14027q0sjyt1h",
"Title":                "EC2-Create-RFC"
}
```

5. Create the RFC, specifying the CreateEC2Rfc file and the CreateEC2Params file:

```
aws amscm create-rfc --cli-input-json file://CreateEC2Rfc.json  --execution-
parameters file://CreateEC2Params.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.

**Tips**

> **Security Groups**
>
> Starting with version 3.0 of this change type, AMS does not attach the default AMS security groups if you specify your own security groups. If you do not specify your own security groups in the request, AMS attaches the AMS default security groups. In previous versions, AMS attached the default security groups whether or not you provided your own security groups.
> Currently, if you specify custom security groups, you must also specify the IDs of the default AMS security groups for your account, `mc-initial-garden-SG-name` and `mc-initial-garden-SG-name`.

> **Instance Types**
>
> AMS does not recommend the **t2.micro/t3.micro** and **t2.nano/t3.nano** types. These are smaller instance types, and can degrade the performance of your application and AMS tools. EC2 instances need enough capacity to support AMS tools such as EPS, SSM, and Cloudwatch in addition to the application workload. For more information, see Choosing the Right EC2 Instance Type for Your Application.

To create an EC2 stack with additional volumes, see EC2 Stack | Create (with Additional Volumes).

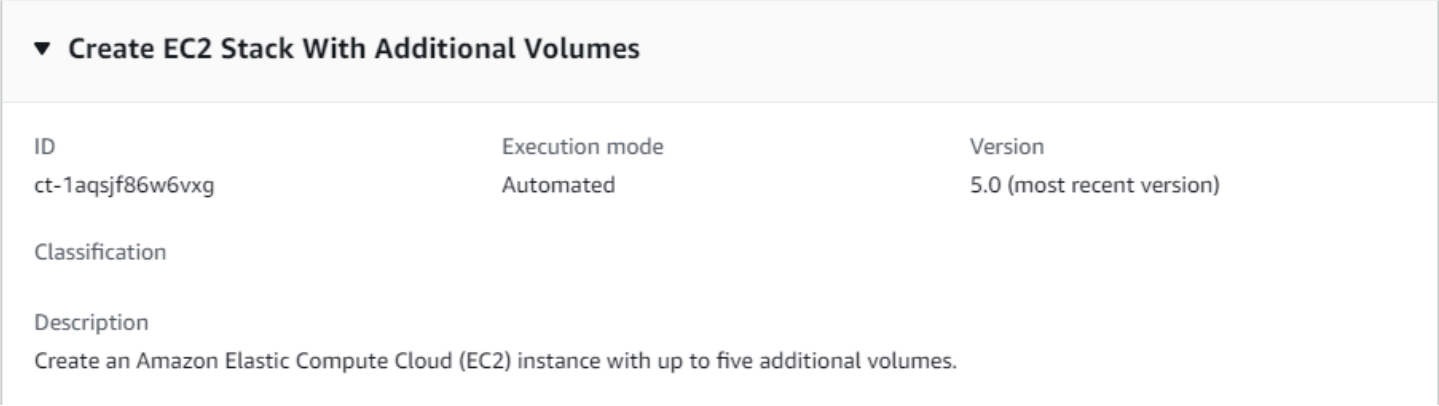
You can add up to 50 tags, but to do so you must enable the **Additional configuration** view.

If needed, see EC2 instance stack create fail.

## Create stack (with additional volumes)

### Creating an EC2 instance and additional volumes with the console

The following shows this change type in the AMS console.




How it works:

1. Navigate to the **Create RFC** page: In the left navigation pane of the AMS console click **RFCs** to open the RFCs list page, and then click **Create RFC**.
2. Choose a popular change type (CT) in the default **Browse change types** view, or select a CT in the **Choose by category** view.
   - **Browse by change type**: You can click on a popular CT in the **Quick create** area to immediately open the **Run RFC** page. Note that you cannot choose an older CT version with quick create.

     To sort CTs, use the **All change types** area in either the **Card** or **Table** view. In either view, select a CT and then click **Create RFC** to open the **Run RFC** page. If applicable, a **Create with older version** option appears next to the **Create RFC** button.
   - **Choose by category**: Select a category, subcategory, item, and operation and the CT details box opens with an option to **Create with older version** if applicable. Click **Create RFC** to open the **Run RFC** page.
3. On the **Run RFC** page, open the CT name area to see the CT details box. A **Subject** is required (this is filled in for you if you choose your CT in the **Browse change types** view). Open the **Additional configuration** area to add information about the RFC.

   In the **Execution configuration** area, use available drop-down lists or enter values for the required parameters. To configure optional execution parameters, open the **Additional configuration** area.
4. When finished, click **Run**. If there are no errors, the **RFC successfully created** page displays with the submitted RFC details, and the initial **Run output**.

5. Open the **Run parameters** area to see the configurations you submitted. Refresh the page to update the RFC execution status. Optionally, cancel the RFC or create a copy of it with the options at the top of the page.

### Creating an EC2 instance and additional volumes with the CLI

How it works:

1. Use either the Inline Create (you issue a `create-rfc` command with all RFC and execution parameters included), or Template Create (you create two JSON files, one for the RFC parameters and one for the execution parameters) and issue the `create-rfc` command with the two files as input. Both methods are described here.
2. Submit the RFC: `aws amscm submit-rfc --rfc-id` *`ID`* command with the returned RFC ID.

   Monitor the RFC: `aws amscm get-rfc --rfc-id` *`ID`* command.

To check the change type version, use this command:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> You can use any `CreateRfc` parameters with any RFC whether or not they are part of the schema for the change type. For example, to get notifications when the RFC status changes, add this line, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` to the RFC parameters part of the request (not the execution parameters). For a list of all CreateRfc parameters, see the AMS Change Management API Reference.

*INLINE CREATE*:

Issue the create RFC command with execution parameters provided inline (escape quotation marks when providing execution parameters inline), and then submit the returned RFC ID (example shows required parameters only). For example, you can replace the contents with something like this:

```
aws amscm create-rfc --change-type-id "ct-1aqsjf86w6vxg" --change-type-version "4.0"
 --title "EC2-Create-A-V-QC" --execution-parameters "{\"Description\":\"My EC2 stack
 with addl vol\",\"VpcId\":\"VPC_ID\",\"Name\":\"My Stack\",\"StackTemplateId\":
\"stm-nn8v8ffhcal611bmo\",\"TimeoutInMinutes\":60,\"Parameters\":{\"InstanceAmiId\":
\"AMI_ID\",\"InstanceSubnetId\":\"SUBNET_ID\"}}
```

*TEMPLATE CREATE*:

1. Output the execution parameters for this change type to a JSON file named CreateEC2AVParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-1aqsjf86w6vxg" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2AVParams.json
```

2. Modify and save the CreateEC2AVParams file (example shows most parameters). For example, you can replace the contents with something like this:

```
{
"Description":      "EC2-Create-1-Addl-Volumes",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-nn8v8ffhcal611bmo",
"Name":             "My-EC2-1-Addl-Volume",
"TimeoutInMinutes": 60,
"Parameters":   {
    "InstanceAmiId":    "AMI_ID",
    "InstanceSecurityGroupIds": "SECURITY_GROUP_ID",
    "InstanceCoreCount": 1,
    "InstanceThreadsPerCore": 2,
    "InstanceDetailedMonitoring": "true",
    "InstanceEBSOptimized": "false",
    "InstanceProfile": "customer-mc-ec2-instance-profile",
    "InstanceRootVolumeIops": 100,
    "InstanceRootVolumeName": "/dev/xvda",
    "InstanceRootVolumeSize": 50,
    "InstanceRootVolumeType": "io1",
    "RootVolumeKmsKeyId": "default",
    "InstancePrivateStaticIp": "10.27.0.100",
    "InstanceSecondaryPrivateIpAddressCount": 0,
    "InstanceTerminationProtection": "false",
    "InstanceType": "t3.large",
    "CreditSpecification": "unlimited",
    "InstanceUserData": "echo $",
```

```
    "Volume1Encrypted": "true",
    "Volume1Iops":      "IOPS"
    "Volume1KmsKeyId":  "KMS_MASTER_KEY_ID",
    "Volume1Name":      "xvdh"
    "Volume1Size":      "2 GiB",
    "Volume1Snapshot":  "SNAPSHOT_ID",
    "Volume1Type":      "iol",
    "InstanceSubnetId": "SUBNET_ID"
    }
}
```

3. Output the RFC template to a file in your current folder; this example names it CreateEC2AVRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2AVRfc.json
```

4. Modify and save the CreateEC2AVRfc.json file. For example, you can replace the contents with something like this:

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-1aqsjf86w6vxg",
"Title":                "EC2-Create-1-Addl-Volume-RFC"
}
```

5. Create the RFC, specifying the CreateEC2AVRfc file and the CreateEC2AVParams file:

```
aws amscm create-rfc --cli-input-json file://CreateEC2AVRfc.json  --execution-
parameters file://CreateEC2AVParams.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.

### Tips

> **Important**
>
> There is a new version of this change type, v 4.0, that uses a different StackTemplateId (stm-nn8v8ffhcal611bmo). This is important if you're submitting the RFC with this change type at the command line. The new version introduces two new parameters

(**RootVolumeKmsKeyId** and **CreditSpecification**) and changes the default for one existing parameter (**InstanceType**).

**Instance Types**

- If you choose to specify the number of cores or threads, you must specify values for both. Use the parameters `InstanceCoreCount` and `InstanceThreadsPerCore`. To find valid combinations of cores/threads, see CPU cores and threads per CPU core per instance type .
- AMS does not recommend the **t2.micro/t3.micro** or **t2.nano/t3.nano** instance types. These are too small to support AMS tools such as EPS, SSM, and Cloudwatch in addition to your business workload. For more information, see Choosing the Right EC2 Instance Type for Your Application.
- In version 4.0, the default type was raised from **t2.large** to **t3.large**. T3 instances launch with 'unlimited credits' by default. You won't experience CPU throttling even if the instance consumes all CPU credits. You can, instead, choose T2 instances and use the CreditSpecification unlimited option.
- For more information about Amazon EC2, including size recommendations, see Amazon Elastic Compute Cloud Documentation.

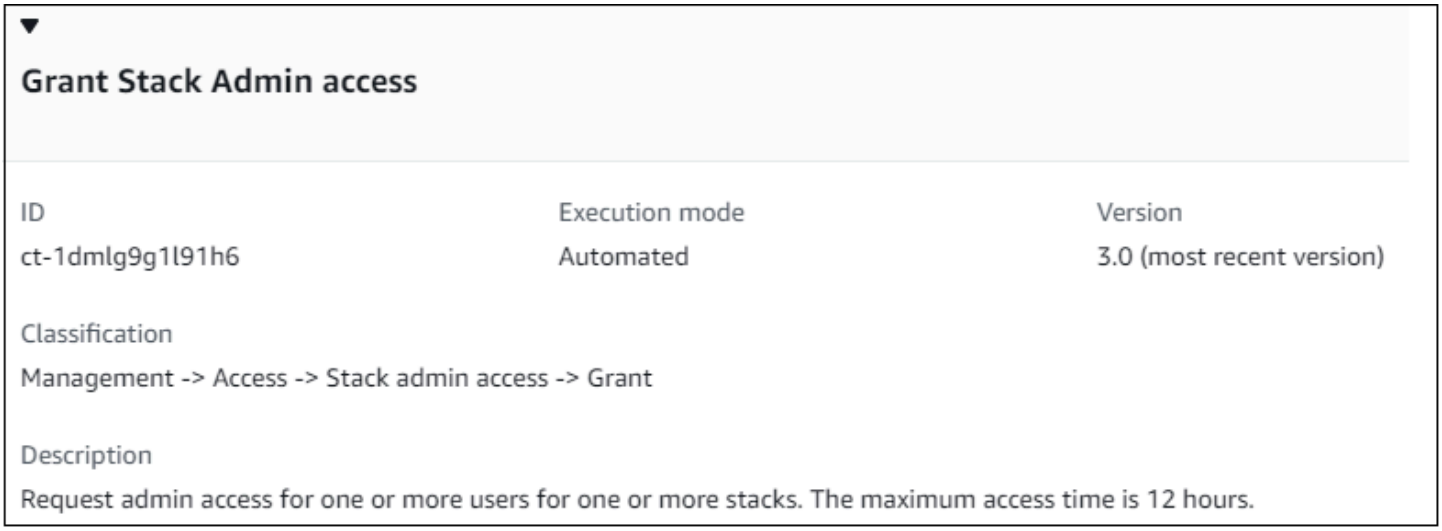
To update your EC2 stack with additional volumes after they're created, see EC2 Instance stack: Updating (With Additional Volumes)

# Access, requesting

## Request administrative access

### Requesting administrator access with the console

The following shows this change type in the AMS console.




How it works:

1. Navigate to the **Create RFC** page: In the left navigation pane of the AMS console click **RFCs** to open the RFCs list page, and then click **Create RFC**.
2. Choose a popular change type (CT) in the default **Browse change types** view, or select a CT in the **Choose by category** view.
   - **Browse by change type**: You can click on a popular CT in the **Quick create** area to immediately open the **Run RFC** page. Note that you cannot choose an older CT version with quick create.

     To sort CTs, use the **All change types** area in either the **Card** or **Table** view. In either view, select a CT and then click **Create RFC** to open the **Run RFC** page. If applicable, a **Create with older version** option appears next to the **Create RFC** button.
   - **Choose by category**: Select a category, subcategory, item, and operation and the CT details box opens with an option to **Create with older version** if applicable. Click **Create RFC** to open the **Run RFC** page.
3. On the **Run RFC** page, open the CT name area to see the CT details box. A **Subject** is required (this is filled in for you if you choose your CT in the **Browse change types** view). Open the **Additional configuration** area to add information about the RFC.

   In the **Execution configuration** area, use available drop-down lists or enter values for the required parameters. To configure optional execution parameters, open the **Additional configuration** area.

4. When finished, click **Run**. If there are no errors, the **RFC successfully created** page displays with the submitted RFC details, and the initial **Run output**.
5. Open the **Run parameters** area to see the configurations you submitted. Refresh the page to update the RFC execution status. Optionally, cancel the RFC or create a copy of it with the options at the top of the page.

### Requesting administrator access with the CLI

How it works:

1. Use either the Inline Create (you issue a `create-rfc` command with all RFC and execution parameters included), or Template Create (you create two JSON files, one for the RFC parameters and one for the execution parameters) and issue the `create-rfc` command with the two files as input. Both methods are described here.
2. Submit the RFC: `aws amscm submit-rfc --rfc-id` *`ID`* command with the returned RFC ID.

   Monitor the RFC: `aws amscm get-rfc --rfc-id` *`ID`* command.

To check the change type version, use this command:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> You can use any `CreateRfc` parameters with any RFC whether or not they are part of the schema for the change type. For example, to get notifications when the RFC status changes, add this line, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` to the RFC parameters part of the request (not the execution parameters). For a list of all CreateRfc parameters, see the AMS Change Management API Reference.

*INLINE CREATE*:

Issue the create RFC command with execution parameters provided inline (escape quotation marks when providing execution parameters inline), and then submit the returned RFC ID. For example, you can replace the contents with something like this:

```
aws --profile saml amscm create-rfc --change-type-id "ct-1dmlg9g1l91h6" --change-type-
version "3.0" --title "Stack-Admin-Access-QC" --execution-parameters "{\"DomainFQDN
\":\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

*TEMPLATE CREATE*:

1. Output the execution parameters JSON schema for this change type to a file; this example names it GrantAdminAccessParams.json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-1dmlg9g1l91h6"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantAdminAccessParams.json
   ```

   Modify and save the GrantAdminAccessParams file. For example, you can replace the contents with something like this:

   ```
   {
   "DomainFQDN":           "mycorpdomain.acme.com",
   "StackIds":              [STACK_ID, STACK_ID],
   "TimeRequestedInHours": 12,
   "Username":              ["USERNAME", "USERNAME"],
   "VpcId":                "VPC_ID"
   }
   ```

   Note that the `TimeRequestedInHours` option defaults to one hour. You can request up to twelve hours.

2. Output the RFC template to a file in your current folder; this example names it GrantAdminAccessRfc.json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > GrantAdminAccessRfc.json
   ```

3. Modify and save the GrantAdminAccessRfc.json file. For example, you can replace the contents with something like this:

```
{
"ChangeTypeId":         "ct-1dmlg9g1l91h6",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-Admin-Access-to-EC2-RFC"
}
```

4. Create the RFC, specifying the GrantAdminAccessRfc file and the GrantAdminAcessParams file:

```
aws amscm create-rfc --cli-input-json file://GrantAdminAccessRfc.json --execution-
parameters file://GrantAdminAccessParams.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.

To log in to the instance through a bastion, follow the next procedure, Instance access examples.

**Tips**

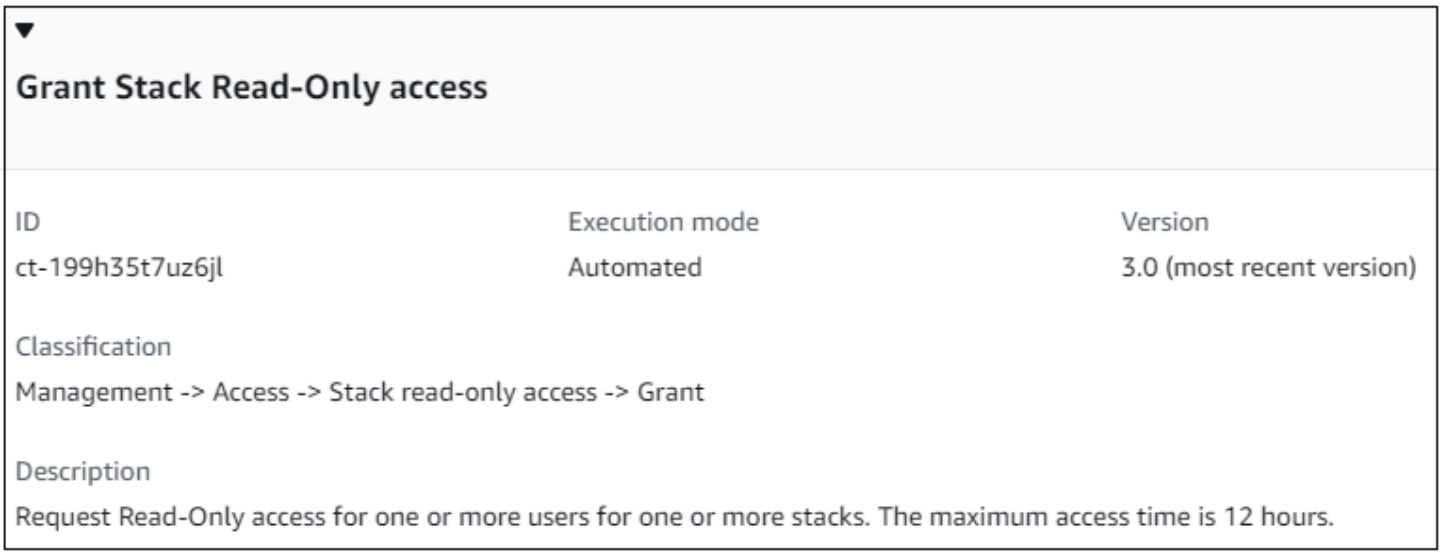
> **Note**
>
> You can submit an update to your access request before it expires. For information, see Stack Admin Access | Update.
> To log in to an instance that is part of an ASG, you request access to the ASG stack, which gives you access to all associated instances.

For an example about requesting ReadOnly access, see ReadOnly access: requesting.

## Request ReadOnly access

### Requesting ReadOnly access with the console

The following shows this change type in the AMS console.




How it works:

1. Navigate to the **Create RFC** page: In the left navigation pane of the AMS console click **RFCs** to open the RFCs list page, and then click **Create RFC**.
2. Choose a popular change type (CT) in the default **Browse change types** view, or select a CT in the **Choose by category** view.
   - **Browse by change type**: You can click on a popular CT in the **Quick create** area to immediately open the **Run RFC** page. Note that you cannot choose an older CT version with quick create.

     To sort CTs, use the **All change types** area in either the **Card** or **Table** view. In either view, select a CT and then click **Create RFC** to open the **Run RFC** page. If applicable, a **Create with older version** option appears next to the **Create RFC** button.
   - **Choose by category**: Select a category, subcategory, item, and operation and the CT details box opens with an option to **Create with older version** if applicable. Click **Create RFC** to open the **Run RFC** page.
3. On the **Run RFC** page, open the CT name area to see the CT details box. A **Subject** is required (this is filled in for you if you choose your CT in the **Browse change types** view). Open the **Additional configuration** area to add information about the RFC.

   In the **Execution configuration** area, use available drop-down lists or enter values for the required parameters. To configure optional execution parameters, open the **Additional configuration** area.

4. When finished, click **Run**. If there are no errors, the **RFC successfully created** page displays with the submitted RFC details, and the initial **Run output**.
5. Open the **Run parameters** area to see the configurations you submitted. Refresh the page to update the RFC execution status. Optionally, cancel the RFC or create a copy of it with the options at the top of the page.

### Requesting ReadOnly access with the CLI

How it works:

1. Use either the Inline Create (you issue a `create-rfc` command with all RFC and execution parameters included), or Template Create (you create two JSON files, one for the RFC parameters and one for the execution parameters) and issue the `create-rfc` command with the two files as input. Both methods are described here.
2. Submit the RFC: `aws amscm submit-rfc --rfc-id` *`ID`* command with the returned RFC ID.

   Monitor the RFC: `aws amscm get-rfc --rfc-id` *`ID`* command.

To check the change type version, use this command:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> You can use any `CreateRfc` parameters with any RFC whether or not they are part of the schema for the change type. For example, to get notifications when the RFC status changes, add this line, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` to the RFC parameters part of the request (not the execution parameters). For a list of all CreateRfc parameters, see the AMS Change Management API Reference.

*INLINE CREATE*:

Issue the create RFC command with execution parameters provided inline (escape quotes when providing execution parameters inline), and then submit the returned RFC ID. For example, you can replace the contents with something like this:

```
aws --profile saml amscm create-rfc --change-type-id "ct-199h35t7uz6jl" --change-type-
version "3.0" --title "Stack-RO-Access-QC" --execution-parameters "{\"DomainFQDN\":
\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

*TEMPLATE CREATE*:

1. Output the execution parameters JSON schema for this change type to a file; this example names it GrantReadOnlyAccessParams.json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-199h35t7uz6jl"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantReadOnlyAccessParams.json
   ```

   Modify and save the GrantReadOnlyAccessParams file. For example, you can replace the contents with something like this:

   ```
   {
   "DomainFQDN":           "mycorpdomain.acme.com",
   "StackIds":              [STACK_ID, STACK_ID],
   "TimeRequestedInHours": 12,
   "Usernames":              ["USERNAME", "USERNAME"],
   "VpcId":                "VPC_ID"
   }
   ```

   Note that the `TimeRequestedInHours` option defaults to one hour. You can request up to twelve hours.

2. Output the RFC template to a file in your current folder; this example names it GrantReadOnlyAccessRfc.json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > GrantReadOnlyAccessRfc.json
   ```

3. Modify and save the GrantReadOnlyAccessRfc.json file. For example, you can replace the contents with something like this:

```
{
"ChangeTypeId":         "ct-199h35t7uz6jl",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-ReadOnly-Access-to-EC2-RFC"
}
```

4. Create the RFC, specifying the GrantReadOnlyAccessRfc file and the GrantReadOnlyAcessParams file:

```
aws amscm create-rfc --cli-input-json file://GrantReadOnlyAccessRfc.json --
execution-parameters file://GrantReadOnlyAccessParams.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.

To log in to the instance through a bastion, follow the next procedure, Instance access examples.

**Tips**

> **Note**
>
> You can submit an update to your access request before it expires. For details, see Stack Read-Only Access | Update.
> To log into an instance that is part of an EC2 Auto Scaling group (ASG), you request access to the ASG stack, which gives you access to all associated instances.

For a walkthrough on requesting Admin access, see Admin Access: requesting.

## Other | Other RFC, creating (CLI)

This example shows how to request a change that none of the available CTs address, by using the Management | Other | Other | Create CT (ct-1e1xtak34nx76).

Use this CT when you can't find a change type for what you want; however, if you are unsure about specifying parameters in an existing CT, it is better to submit a service request for help. For information on submitting service requests, see Service Request Examples.

This type of RFC is Approval-required, meaning that it requires AMS approval before it can be implemented. After submitting the RFC, an AMS operator will contact you to discuss the stack that you want to deploy.

> **Note**
>
> When using "review required" CTs, AMS recommends that you use the ASAP **Scheduling** 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.

REQUIRED DATA:

- `Comment`: What the RFC is for.
- `ChangeTypeId` and `ChangeTypeVersion`: Use Other | Create (`ct-1e1xtak34nx76`) to request new resources, use Other | Update (`ct-0xdawir96cy7k`) to change existing resources; both are `v1`.

OPTIONAL DATA: `Priority`: Acceptable values are `High`, `Medium`, or `Low`.

*INLINE CREATE*:

- Issue the create RFC command with execution parameters provided inline (escape quotes when providing execution parameters inline). Example uses Other | Create.

```
aws amscm create-rfc --change-type-id "ct-1e1xtak34nx76" --change-type-version "1.0"
 --title "TITLE" --execution-parameters "{\"Comment\": \"What you want created\"}"
```

- Submit the RFC using the RFC ID returned in the create RFC operation. Until submitted, the RFC remains in the `Editing` state and is not acted on.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- Monitor the RFC status and view execution output:

```
aws amscm get-rfc --rfc-id RFC_ID
```

*TEMPLATE CREATE*:

1. Create and save a JSON file for the execution parameters; example names it OtherParams.json and includes the optional `Priority` parameter:

```
{
"Comment":          "What you want created",
"Priority":         "Medium"
}
```

2. Create and save a JSON file for the RFC parameters; example names it OtherRfc.json.

```
{
"ChangeTypeId":         "ct-1e1xtak34nx76",
"ChangeTypeVersion":    "1.0",
"Title":                "TITLE"
}
```

3. Create the RFC, specifying the OtherRfc file and the OtherParams file:

```
aws amscm create-rfc --cli-input-json file://OtherRfc.json  --execution-parameters
 file://OtherParams.json
```

   You receive the RfcId of the new RFC in the response. For example:

```
{
"RfcId": "RFC-ID"
}
```

4. Submit the RFC:

```
aws amscm submit-rfc --rfc-id RFC-ID
```

   If no errors are reported, the operation was successful.

5. To monitor the status of the request and to view Execution Output:

```
aws amscm get-rfc --rfc-id RFC-ID
```

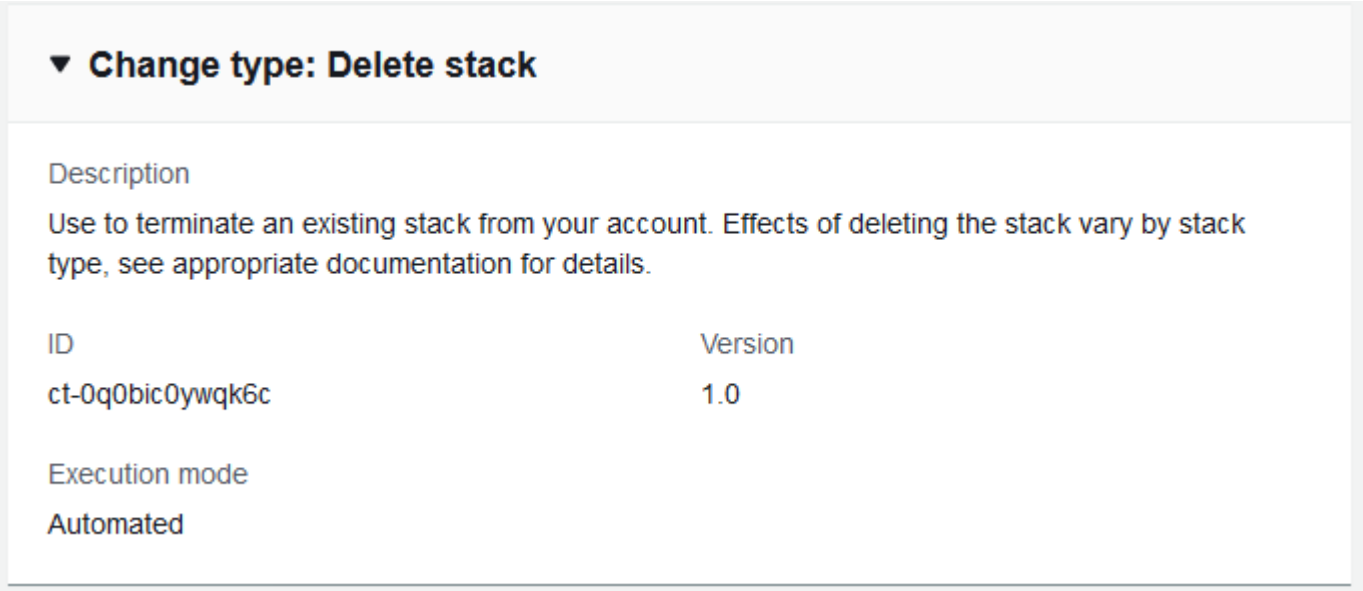
# Any stack: deleting, rebooting, starting, stopping

You can use the AMS console or API/CLI to delete, reboot, start, or stop, an AMS stack.

## Delete stack

### Deleting a Stack with the Console

Screenshot of this change type in the AMS console:




How it works:

1. Navigate to the **Create RFC** page: In the left navigation pane of the AMS console click **RFCs** to open the RFCs list page, and then click **Create RFC**.
2. Choose a popular change type (CT) in the default **Browse change types** view, or select a CT in the **Choose by category** view.
   - **Browse by change type**: You can click on a popular CT in the **Quick create** area to immediately open the **Run RFC** page. Note that you cannot choose an older CT version with quick create.

To sort CTs, use the **All change types** area in either the **Card** or **Table** view. In either view, select a CT and then click **Create RFC** to open the **Run RFC** page. If applicable, a **Create with older version** option appears next to the **Create RFC** button.

- **Choose by category**: Select a category, subcategory, item, and operation and the CT details box opens with an option to **Create with older version** if applicable. Click **Create RFC** to open the **Run RFC** page.

3. On the **Run RFC** page, open the CT name area to see the CT details box. A **Subject** is required (this is filled in for you if you choose your CT in the **Browse change types** view). Open the **Additional configuration** area to add information about the RFC.

   In the **Execution configuration** area, use available drop-down lists or enter values for the required parameters. To configure optional execution parameters, open the **Additional configuration** area.

4. When finished, click **Run**. If there are no errors, the **RFC successfully created** page displays with the submitted RFC details, and the initial **Run output**.
5. Open the **Run parameters** area to see the configurations you submitted. Refresh the page to update the RFC execution status. Optionally, cancel the RFC or create a copy of it with the options at the top of the page.

### Deleting a Stack with the CLI

How it works:

1. Use either the Inline Create (you issue a `create-rfc` command with all RFC and execution parameters included), or Template Create (you create two JSON files, one for the RFC parameters and one for the execution parameters) and issue the `create-rfc` command with the two files as input. Both methods are described here.
2. Submit the RFC: `aws amscm submit-rfc --rfc-id` *`ID`* command with the returned RFC ID.

   Monitor the RFC: `aws amscm get-rfc --rfc-id` *`ID`* command.

To check the change type version, use this command:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> You can use any `CreateRfc` parameters with any RFC whether or not they are part of the schema for the change type. For example, to get notifications when the RFC status changes, add this line, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` to the RFC parameters part of the request (not the execution parameters). For a list of all CreateRfc parameters, see the AMS Change Management API Reference.

*INLINE CREATE*:

Issue the create RFC command with execution parameters provided inline (escape quotation marks when providing execution parameters inline), and then submit the returned RFC ID. For example, you can replace the contents with something like this:

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0" --
title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

*TEMPLATE CREATE*:

1. Output the RFC template to a file in your current folder; this example names it DeleteStackRfc.json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. Modify and save the DeleteStackRfc.json file.

   The internal quotation marks in the ExecutionParameters JSON extension must be escaped with a backslash (\). Example without start and end time:

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. Create the RFC:

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.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.

### Tips

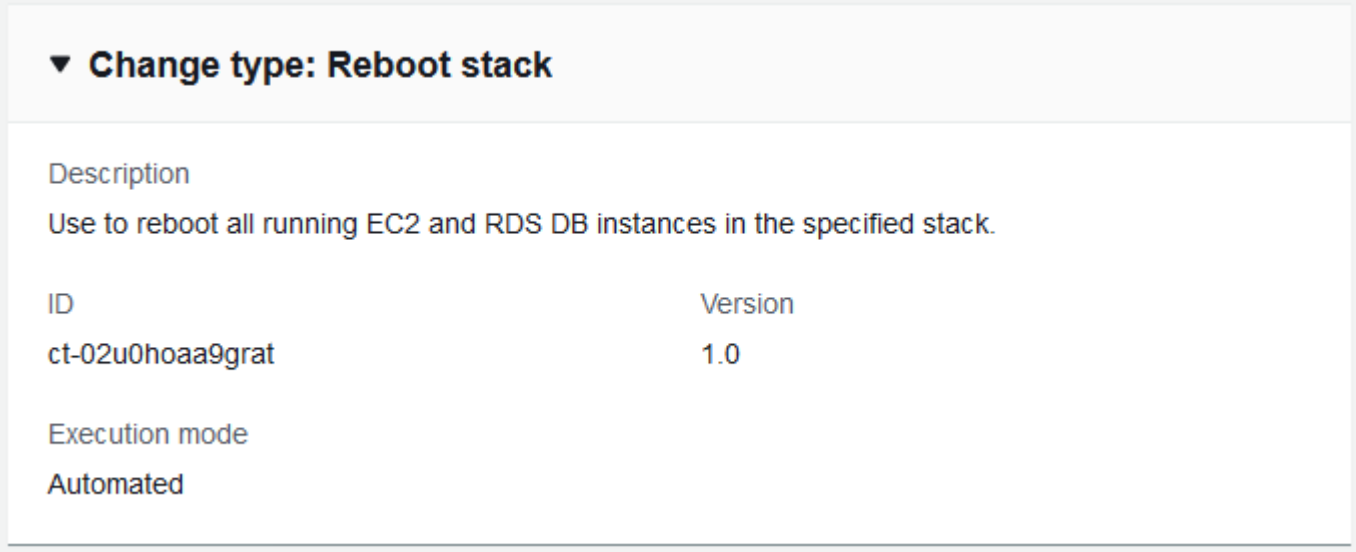
> **Note**
>
> If deleting an S3 bucket, it must be emptied of objects first.

> **Important**
>
> Deleting stacks can have unwanted and unanticipated consequences. For important caveats, see RFC Troubleshooting section RFCs for Delete Stack.

## Reboot stack

### Rebooting a Stack with the Console

Screenshot of this change type in the AMS console:




How it works:

1. Navigate to the **Create RFC** page: In the left navigation pane of the AMS console click **RFCs** to open the RFCs list page, and then click **Create RFC**.
2. Choose a popular change type (CT) in the default **Browse change types** view, or select a CT in the **Choose by category** view.
   - **Browse by change type**: You can click on a popular CT in the **Quick create** area to immediately open the **Run RFC** page. Note that you cannot choose an older CT version with quick create.

     To sort CTs, use the **All change types** area in either the **Card** or **Table** view. In either view, select a CT and then click **Create RFC** to open the **Run RFC** page. If applicable, a **Create with older version** option appears next to the **Create RFC** button.
   - **Choose by category**: Select a category, subcategory, item, and operation and the CT details box opens with an option to **Create with older version** if applicable. Click **Create RFC** to open the **Run RFC** page.
3. On the **Run RFC** page, open the CT name area to see the CT details box. A **Subject** is required (this is filled in for you if you choose your CT in the **Browse change types** view). Open the **Additional configuration** area to add information about the RFC.

   In the **Execution configuration** area, use available drop-down lists or enter values for the required parameters. To configure optional execution parameters, open the **Additional configuration** area.
4. When finished, click **Run**. If there are no errors, the **RFC successfully created** page displays with the submitted RFC details, and the initial **Run output**.
5. Open the **Run parameters** area to see the configurations you submitted. Refresh the page to update the RFC execution status. Optionally, cancel the RFC or create a copy of it with the options at the top of the page.

### Rebooting a Stack with the CLI

How it works:

1. Use either the Inline Create (you issue a `create-rfc` command with all RFC and execution parameters included), or Template Create (you create two JSON files, one for the RFC parameters and one for the execution parameters) and issue the `create-rfc` command with the two files as input. Both methods are described here.
2. Submit the RFC: `aws amscm submit-rfc --rfc-id` *`ID`* command with the returned RFC ID.

Monitor the RFC: `aws amscm get-rfc --rfc-id ID` command.

To check the change type version, use this command:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> You can use any `CreateRfc` parameters with any RFC whether or not they are part of the schema for the change type. For example, to get notifications when the RFC status changes, add this line, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` to the RFC parameters part of the request (not the execution parameters). For a list of all CreateRfc parameters, see the AMS Change Management API Reference.

*INLINE CREATE*:

Issue the create RFC command with execution parameters provided inline (escape quotation marks when providing execution parameters inline), and then submit the returned RFC ID. For example, you can replace the contents with something like this:

```
aws amscm create-rfc --change-type-id "ct-02u0hoaa9grat" --change-type-version "1.0" --
title "Reboot My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

*TEMPLATE CREATE*:

1. Output the RFC template to a file in your current folder. This example names it RebootStackRfc.json. Note that since there is only one execution parameter for stopping (rebooting, or starting) an instance, the execution parameter can be in the schema JSON file itself and there is no need to create a separate execution parameters JSON file.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopInstanceRfc.json
   ```

2. Modify and save the RebootStackRfc.json file.

The internal quotation marks in the `ExecutionParameters` JSON extension must be escaped with a backslash (\). Example:

```
{
"ChangeTypeId":         "ct-02u0hoaa9grat",
"Title":                "Reboot-My-EC2-RFC",
"TimeoutInMinutes":     60,
"ExecutionParameters":  "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. Create the RFC:

```
aws amscm create-rfc --cli-input-json file://RebootStackRfc.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.

### Tips

For information about Application Load Balancers, see Application Load Balancers.

## Start stack

### Starting a Stack with the Console

Screenshot of this change type in the AMS console:

How it works:

1. Navigate to the **Create RFC** page: In the left navigation pane of the AMS console click **RFCs** to open the RFCs list page, and then click **Create RFC**.
2. Choose a popular change type (CT) in the default **Browse change types** view, or select a CT in the **Choose by category** view.
   - **Browse by change type**: You can click on a popular CT in the **Quick create** area to immediately open the **Run RFC** page. Note that you cannot choose an older CT version with quick create.

     To sort CTs, use the **All change types** area in either the **Card** or **Table** view. In either view, select a CT and then click **Create RFC** to open the **Run RFC** page. If applicable, a **Create with older version** option appears next to the **Create RFC** button.
   - **Choose by category**: Select a category, subcategory, item, and operation and the CT details box opens with an option to **Create with older version** if applicable. Click **Create RFC** to open the **Run RFC** page.
3. On the **Run RFC** page, open the CT name area to see the CT details box. A **Subject** is required (this is filled in for you if you choose your CT in the **Browse change types** view). Open the **Additional configuration** area to add information about the RFC.

   In the **Execution configuration** area, use available drop-down lists or enter values for the required parameters. To configure optional execution parameters, open the **Additional configuration** area.

4. When finished, click **Run**. If there are no errors, the **RFC successfully created** page displays with the submitted RFC details, and the initial **Run output**.
5. Open the **Run parameters** area to see the configurations you submitted. Refresh the page to update the RFC execution status. Optionally, cancel the RFC or create a copy of it with the options at the top of the page.

### Starting a Stack with the CLI

How it works:

1. Use either the Inline Create (you issue a `create-rfc` command with all RFC and execution parameters included), or Template Create (you create two JSON files, one for the RFC parameters and one for the execution parameters) and issue the `create-rfc` command with the two files as input. Both methods are described here.
2. Submit the RFC: `aws amscm submit-rfc --rfc-id` *`ID`* command with the returned RFC ID.

   Monitor the RFC: `aws amscm get-rfc --rfc-id` *`ID`* command.

To check the change type version, use this command:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> You can use any `CreateRfc` parameters with any RFC whether or not they are part of the schema for the change type. For example, to get notifications when the RFC status changes, add this line, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` to the RFC parameters part of the request (not the execution parameters). For a list of all CreateRfc parameters, see the AMS Change Management API Reference.

*INLINE CREATE*:

Issue the create RFC command with execution parameters provided inline (escape quotation marks when providing execution parameters inline), and then submit the returned RFC ID. For example, you can replace the contents with something like this:

```
aws amscm create-rfc --change-type-id "ct-1h5xgl9cr4bzy" --change-type-version "1.0" --
title "Start My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

*TEMPLATE CREATE*:

1. Output the RFC template to a file in your current folder. This example names it StartInstanceRfc.json. Note that since there is only one execution parameter for starting a stack, the execution parameter can be in the schema JSON file itself and there is no need to create a separate execution parameters JSON file.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StartStackRfc.json
   ```

2. Modify and save the StartStackRfc.json file. For example, you can replace the contents with something like this:

   ```
   {
   "ChangeTypeId":         "ct-1h5xgl9cr4bzy",
   "Title":                "Start-My-EC2-RFC",
   "TimeoutInMinutes":     60,
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. Create the RFC:

   ```
   aws amscm create-rfc --cli-input-json file://StartStackRfc.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.

### Tips

For information about Application Load Balancers, see Application Load Balancers.

## Stop stack

### Stopping a Stack with the Console

Screenshot of this change type in the AMS console:

How it works:

1. Navigate to the **Create RFC** page: In the left navigation pane of the AMS console click **RFCs** to open the RFCs list page, and then click **Create RFC**.
2. Choose a popular change type (CT) in the default **Browse change types** view, or select a CT in the **Choose by category** view.
   - **Browse by change type**: You can click on a popular CT in the **Quick create** area to immediately open the **Run RFC** page. Note that you cannot choose an older CT version with quick create.

     To sort CTs, use the **All change types** area in either the **Card** or **Table** view. In either view, select a CT and then click **Create RFC** to open the **Run RFC** page. If applicable, a **Create with older version** option appears next to the **Create RFC** button.
   - **Choose by category**: Select a category, subcategory, item, and operation and the CT details box opens with an option to **Create with older version** if applicable. Click **Create RFC** to open the **Run RFC** page.
3. On the **Run RFC** page, open the CT name area to see the CT details box. A **Subject** is required (this is filled in for you if you choose your CT in the **Browse change types** view). Open the **Additional configuration** area to add information about the RFC.

In the **Execution configuration** area, use available drop-down lists or enter values for the required parameters. To configure optional execution parameters, open the **Additional configuration** area.

4. When finished, click **Run**. If there are no errors, the **RFC successfully created** page displays with the submitted RFC details, and the initial **Run output**.
5. Open the **Run parameters** area to see the configurations you submitted. Refresh the page to update the RFC execution status. Optionally, cancel the RFC or create a copy of it with the options at the top of the page.

### Stopping a Stack with the CLI

How it works:

1. Use either the Inline Create (you issue a `create-rfc` command with all RFC and execution parameters included), or Template Create (you create two JSON files, one for the RFC parameters and one for the execution parameters) and issue the `create-rfc` command with the two files as input. Both methods are described here.
2. Submit the RFC: `aws amscm submit-rfc --rfc-id` *`ID`* command with the returned RFC ID.

   Monitor the RFC: `aws amscm get-rfc --rfc-id` *`ID`* command.

To check the change type version, use this command:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> You can use any `CreateRfc` parameters with any RFC whether or not they are part of the schema for the change type. For example, to get notifications when the RFC status changes, add this line, `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` to the RFC parameters part of the request (not the execution parameters). For a list of all CreateRfc parameters, see the AMS Change Management API Reference.

*INLINE CREATE*:

Issue the create RFC command with execution parameters provided inline (escape quotation marks when providing execution parameters inline), and then submit the returned RFC ID. For example, you can replace the contents with something like this:

```
aws amscm create-rfc --change-type-id "ct-3dgbnh6gpst4d" --change-type-version "1.0" --
title "Stop My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

*TEMPLATE CREATE*:

1. Output the RFC template to a file in your current folder. This example names it StopStackRfc.json. Note that since there is only one execution parameter for stopping (rebooting, or starting) an instance, the execution parameter can be in the schema JSON file itself and there is no need to create a separate execution parameters JSON file.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopStackRfc.json
   ```

2. Modify and save the StopStackRfc.json file. For example, you can replace the contents with something like this:

   ```
   {
   "ChangeTypeId":         "ct-3dgbnh6gpst4d",
   "Title":                "Stop-My-EC2-RFC",
   "TimeoutInMinutes":     60,
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. Create the RFC:

   ```
   aws amscm create-rfc --cli-input-json file://StopInstanceRfc.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.

**Tips**

Stopped instances remain stopped unless you have scheduled restarts using the AMS Resource Scheduler.

If needed, see EC2 instance stack stop fail.

## Access examples

These examples show how to log in to an instance via a bastion once you have been granted access through an RFC. For details on getting access granted, see Access requests.

> **Note**
>
> An EC2 instance created through an Auto Scaling group will have an IP address that cycles in and out and you will have to use your 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 or find bastion IP addresses as described in Finding bastion IP addresses.
- **Username** (for example username@customerdomain.com) and **Password**: Credentials for the account.
- **Stack IP address**: Get this by looking at the AMS console **Stacks** page for the stack you want to log into and then filtering on that stack ID in the EC2 console for your account. For a single EC2 instance, you can also use the AMS SKMS command For the AMS SKMS API reference, see the **Reports** tab in the AWS Artifact Console. to find the stack ID and then For the AMS SKMS API reference, see the **Reports** tab in the AWS Artifact Console. 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.

### 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.

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.

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
   > ```

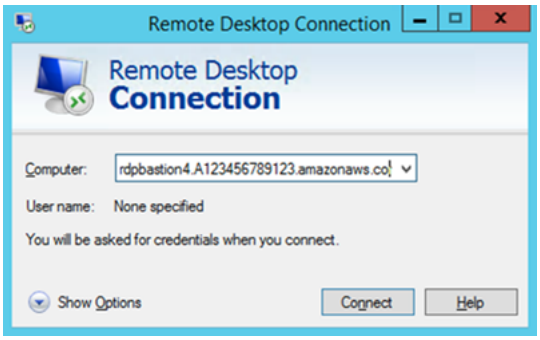
## Windows computer to Windows instance

Use Windows Remote Desktop Connection client to connect to a Windows instance from your Windows computer.

MALZ

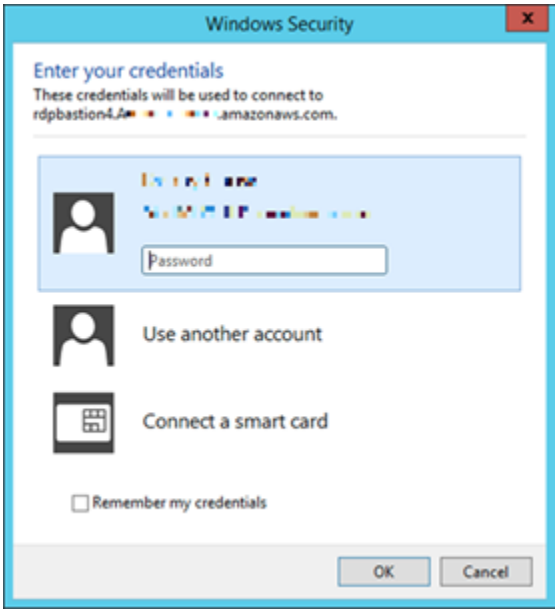
For more information about the friendly bastion names, see DNS friendly bastion names.

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.

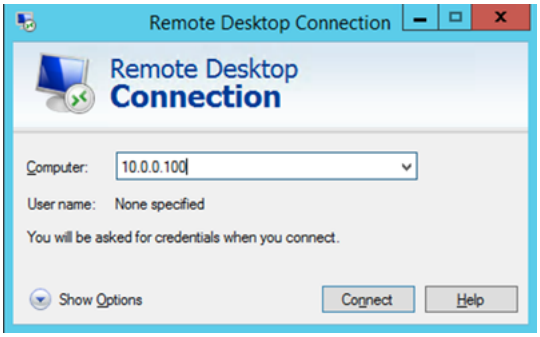



2. Choose **Connect**. The Remote Desktop Connection attempts an RDP connection to the bastion.

   If successful, a credentials dialog box opens. To gain access, use your corporate Active Directory credentials, as you would with the Windows instance.



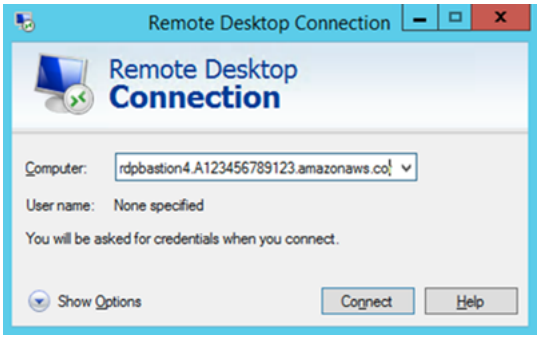

3. Open the Remote Desktop Connection program on the bastion and enter the IP address of the Windows instance you would like to connect to (for example, 10.0.0.100), and then choose **Connect**. Your corporate Active Directory credentials are again required before you connect to the Windows instance.




SALZ

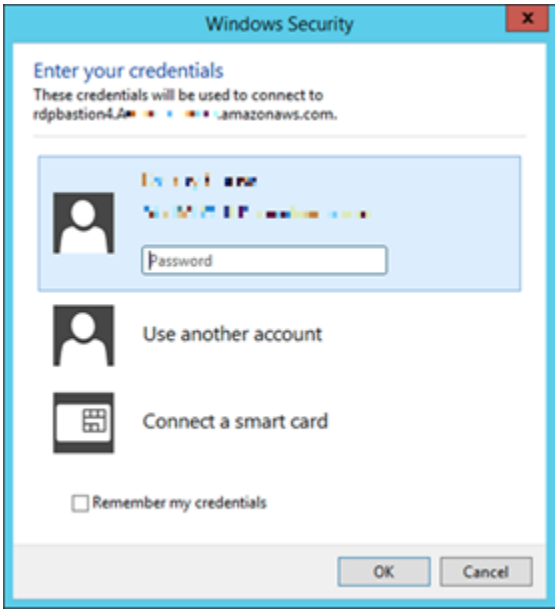
For more information about the friendly bastion names, see DNS friendly bastion names.

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`.

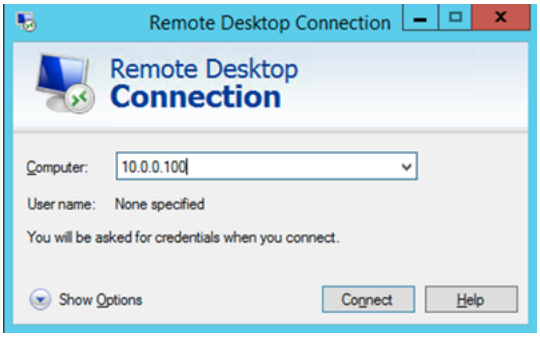



2. Choose **Connect**. The Remote Desktop Connection attempts an RDP connection to the bastion.

   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
```

## Reporting an incident

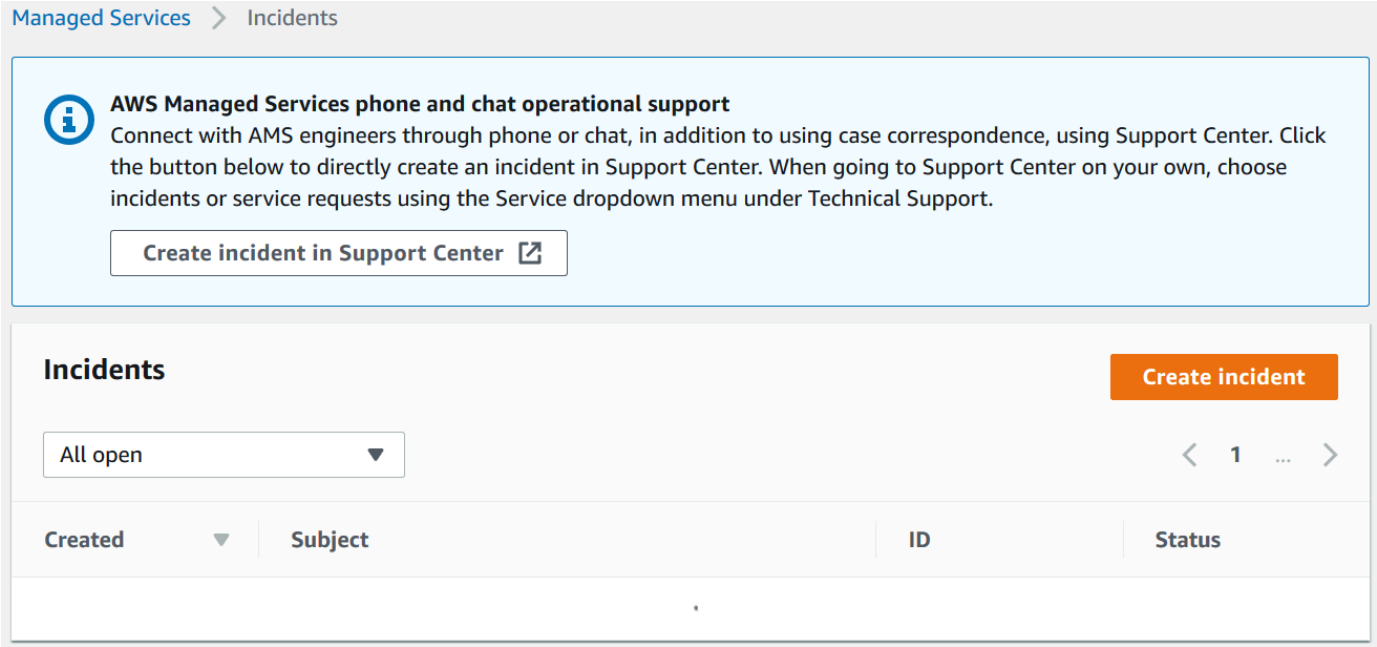
Use the AMS console to report an incident. It's important to create a new incident for each new issue or question. When opening cases related to old inquiries, it's helpful to include the related case number so we can refer to previous correspondence.

> **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:



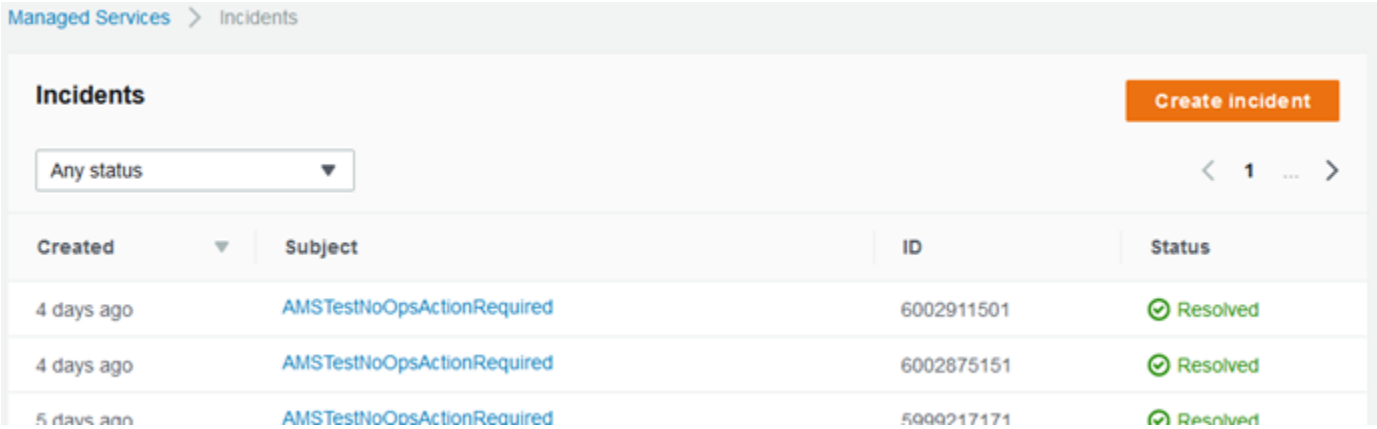

   If your incident list is empty, the **Clear filter** option resets the filter to **Any status**.

   If you know you want to use phone or chat, click **Create incident in Support Center** to open the incident **Create** page in the Support Center Console, auto-populated with the AMS service type.

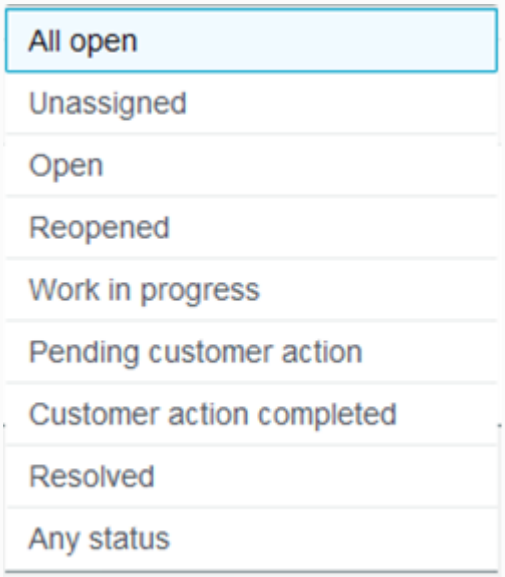
   **Important**

   - Phone calls initiated with Support 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.
   - Phone and chat support is designed to help with support cases, incidents. and service requests, not RFC or security issues.
   - For RFC issues, use the correspondence option on the relevant RFC details page, to reach an AMS engineer.

- For security issues, create a high-priority (P1 or P2) support case. The live chat feature is not for security events.



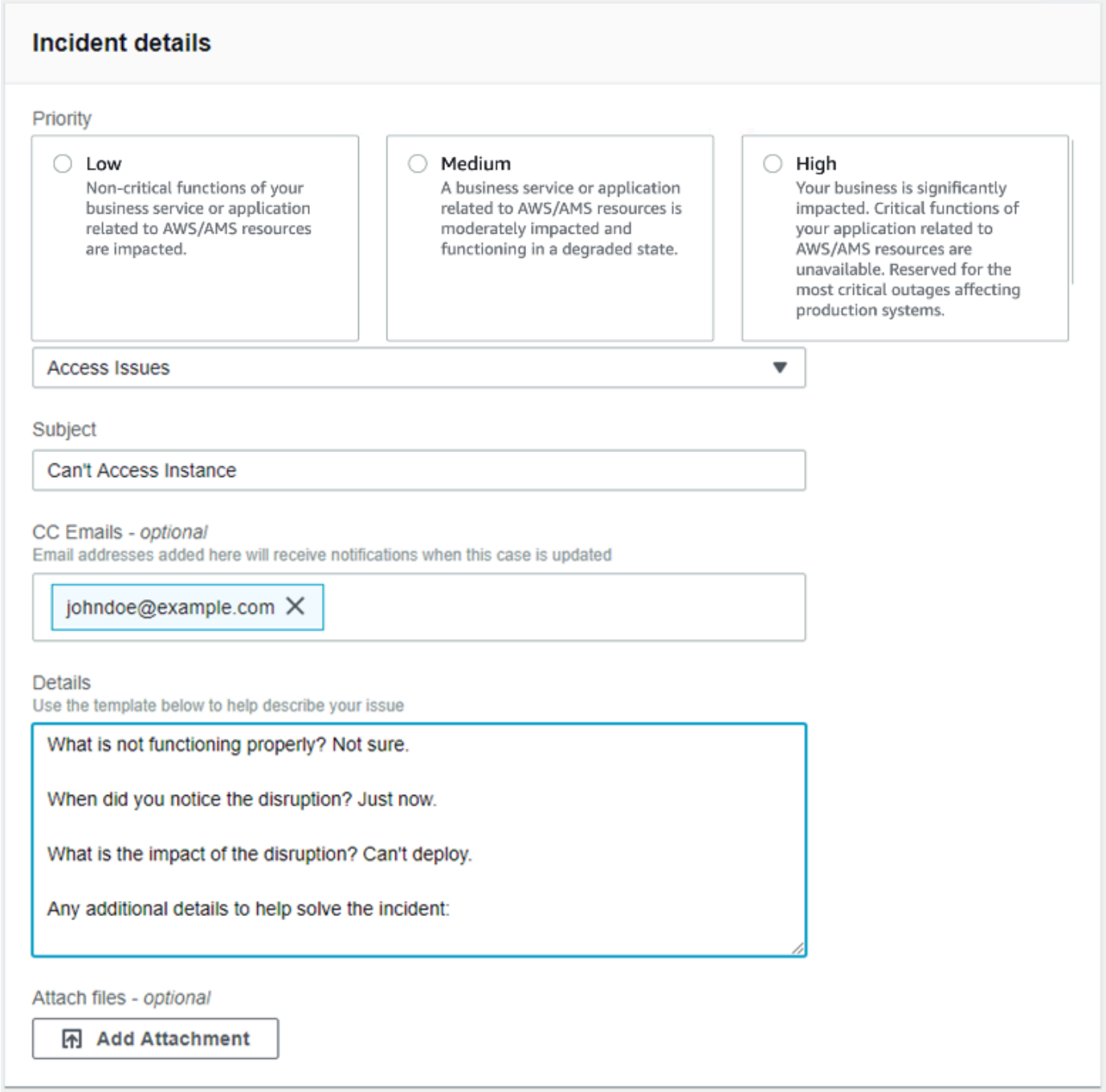

2. If you want to find an existing incident, select an incident status filter in the drop-down list.




- 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**.

> **Note**
>
> If you are going to test incident functionality, then 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**.

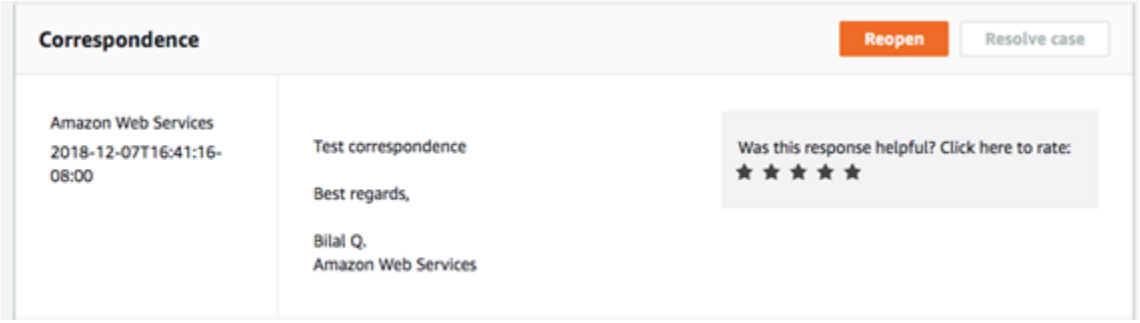
   A details page opens with information on the incident—such as **Type**, **Subject**, **Created**, **ID**, and **Status**—and a **Correspondence** area that includes the description of the request you created.

   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!



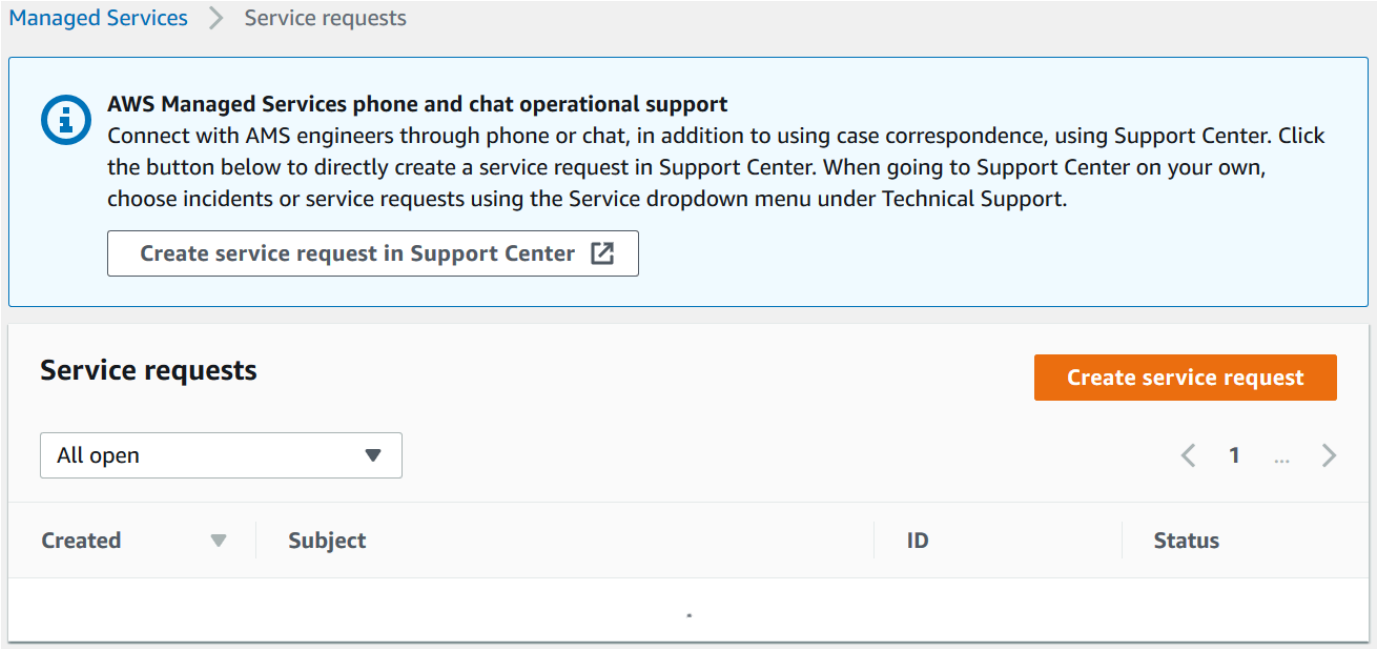

Your incident displays on the **Incidents** list page.

## Creating a service request

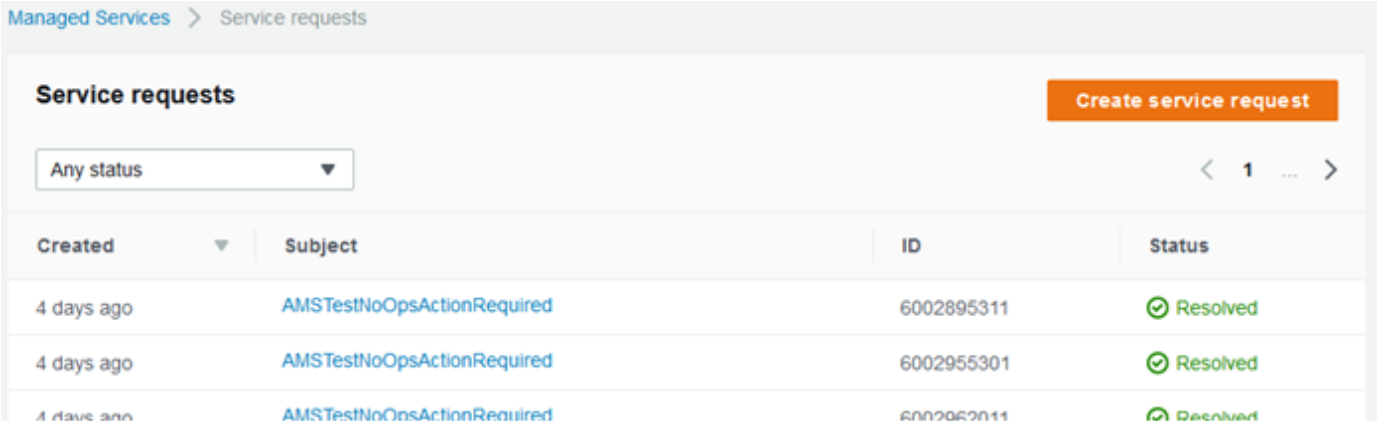
To create a service request using the AWS Managed Services (AMS) console:

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**.

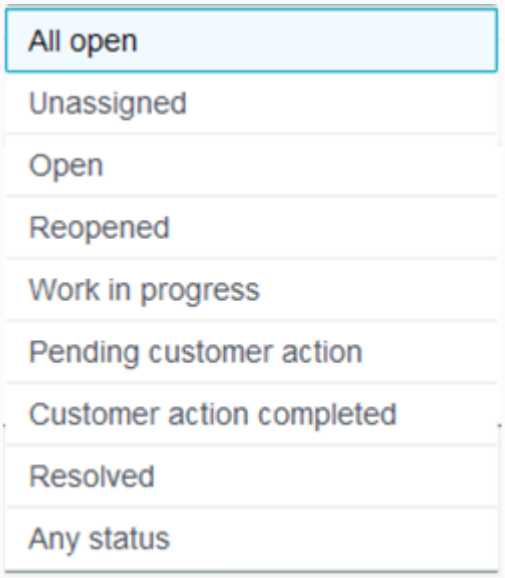



If you know you want to use phone or chat, click **Create service request in Support Center** to open the service request **Create** page in the Support Center Console, auto-populated with the AMS service type.

> **Note**
>
> Phone calls initiated with 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.

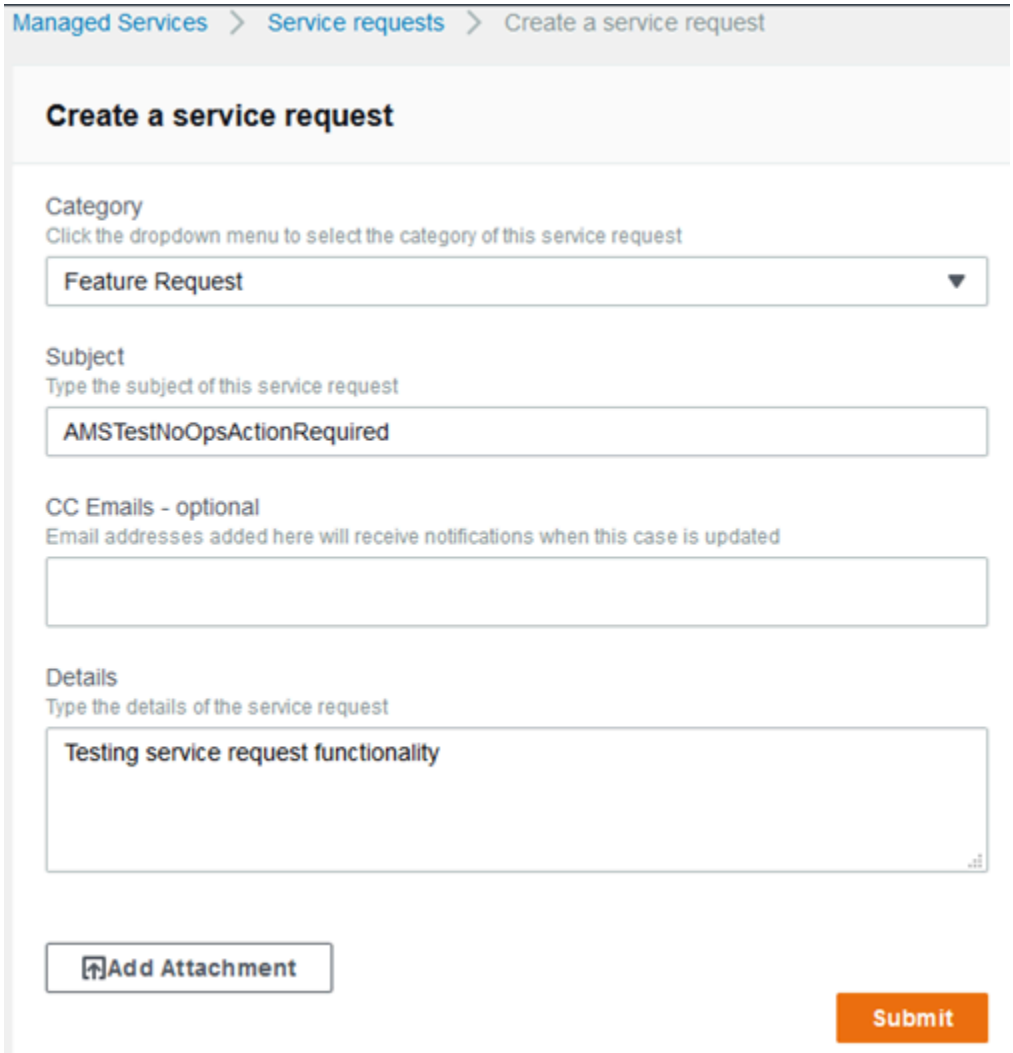
2. If you want to find an existing service request, select a service request status filter in the drop-down list.




- All 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**.

> **Note**
>
> If you are going to test service request functionality, 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.

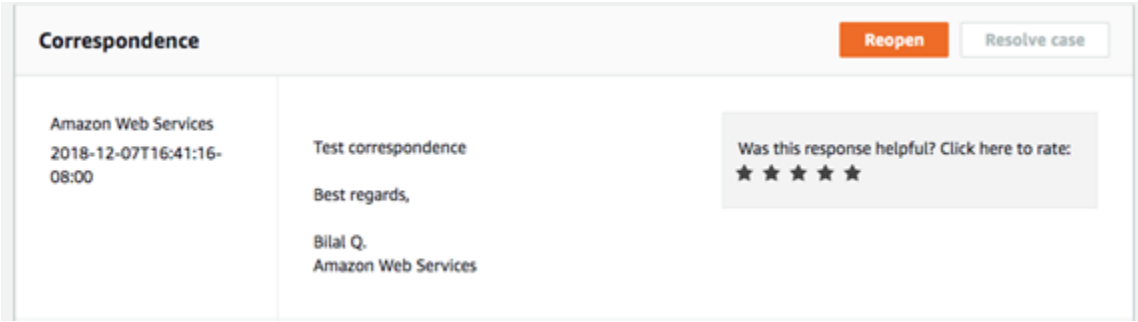
   Additionally, your service request displays on the **Service Request** list page. Use this when you have an alert but have not yet heard from AMS.

   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.

## Post-onboarding steps

Now that you've on boarded an AMS account, you'll want to read more AMS documentation. See these documents:

- The tutorials for using the HA Two-Tier stack CT to create a fully-functioning WordPress stack, next, provides a full AMS experience.
- AMS User Guide: The AMS User Guide describes AMS functionality, lists key terms, operations, interfaces and provides an overview of a typical AMS managed-infrastructure architecture. Additionally, access management details and AMS defaults are given. Also provided are detailed descriptions of how to use the AMS change management system and several walkthroughs are provided. Additional management concepts are described as well.
- AMS API Reference: This API reference provides descriptions of all API calls, including request, response, and examples.
- AMS Application Guide: The AMS Application Guide describes different options and methods for deploying and maintaining your applications in AMS.

## Tutorials

The following tutorials detail the steps to creating a two-tier stack with the High Availability (advanced) CT (ct-06mjngx5flwto), using the CLI and using the Console. A tutorial is given for deploying a Linux Auto Scaling group (ASG) and for deploying a Windows ASG.

Descriptions for all CT options, including ChangeTypeId can be found in the AMS Change Type Reference.

### CLI Tutorial: High Availability Two-Tier Stack (Linux/RHEL)

This section describes how to deploy a high availability (HA) two-tier stack into an AMS environment using the AMS CLI.

> **Note**
>
> This deployment walkthrough has been tested in AMZN Linux and RHEL environments.

Summary of tasks and required RFCs:

1. Create infrastructure (HA two-tier stack)
2. Create an S3 bucket for CodeDeploy applications
3. Create the WordPress application bundle and upload it to the S3 bucket
4. Deploy the application with CodeDeploy
5. Access the WordPress site and log in to validate the deployment

**Before You Begin**

The Deployment | Advanced Stack Components | High Availability Two Tier Stack Advanced | Create CT creates an Auto Scaling group, a load balancer, a database, and a CodeDeploy application name and deployment group (with the same name that you give the application). For information on CodeDeploy see What is CodeDeploy?

This walkthrough uses a High Availability Two-Tier Stack (Advanced) RFC that includes UserData and also describes how to create a WordPress bundle that CodeDeploy can deploy.

The `UserData` shown in the example gets instance metadata such as instance ID, region, etc, from within a running instance by querying the EC2 instance metadata service available at http://169.254.169.254/latest/meta-data/. This line in the user data script: `REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, retrieves the availability zone name from the meta-data service into the $REGION variable for our supported regions, and uses it to complete the URL for the S3 bucket where the CodeDeploy agent is downloaded. The 169.254.169.254 IP is routable only within the VPC (all VPCs can query the service). For information about the service, see Instance Metadata and User Data. Note also that scripts entered as UserData are executed as the "root" user and do not need to use the "sudo" command.

This walkthrough leaves the following parameters at the default value (shown):

- Auto Scaling group: `Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60,`

`ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`.

- Load Balancer: `HealthCheckInterval=30, HealthCheckTimeout=5`.
- Database: `BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.
- Application: `DeploymentConfigName=CodeDeployDefault.OneAtATime`.
- S3 bucket: `AccessControl=Private`.

ADDITIONAL SETTINGS:

`RequestedStartTime` and `RequestedEndTime` if you want to schedule your RFC: You can use Time.is to determine the correct UTC time. The examples provided must be adjusted appropriately. An RFC cannot proceed if the start time has passed. Alternatively, you can leave those values off to create an ASAP RFC that executes as soon as approvals are passed.

> **Note**
>
> There are many parameters that you might choose to set differently than as shown. The values for those parameters shown in the example have been tested but may not be right for you.

**Create the Infrastructure**

Gathering the following data before you begin will make the deployment go more quickly.

REQUIRED DATA HA STACK:

- AutoScalingGroup:
  - `UserData`: This value is provided in this tutorial. It includes commands to set up the resource for CodeDeploy and start the CodeDeploy agent.

- `AMI-ID`: This value determines what kind of EC2 instances your Auto Scaling group (ASG) will spin up. Be sure to select an AMI in your account that starts with "customer-" and is of the operating system that you want. Find AMI IDs with the For the AMS SKMS API reference, see the **Reports** tab in the AWS Artifact Console. operation (CLI: list-amis) or in the AMS Console VPCs -> VPCs details page. This walkthrough is for ASGs configured to use a Linux AMI.
- Database:
  - These parameters, `DBEngine`, `EngineVersion`, and `LicenseModel` should be set according to your situation though the values shown in the example have been tested.
  - These parameters, `RDSSubnetIds`, `DBName`, `MasterUsername`, and `MasterUserPassword` are required when deploying the application bundle. For RDSSubnetIds, use two Private subnets.
- LoadBalancer:
  - These parameters, `DBEngine`, `EngineVersion`, and `LicenseModel` should be set according to your situation though the values shown in the example have been tested.
  - `ELBSubnetIds`: Use two Public subnets.
- Application: The `ApplicationName` value sets the CodeDeploy application name and CodeDeploy deployment group name. You use it to deploy your application. It must be unique in the account. To check your account for CodeDeploy names, see the CodeDeploy Console. The example uses "WordPress" but, if you will use that value, make sure that it is not already in use.

This procedure utilizes the High availability two-tier stack (advanced) CT (ct-06mjngx5flwto) and the Create S3 storage CT (ct-1a68ck03fn98r). From your authenticated account, follow these steps at the command line.

1. Launch the infrastructure stack.

   a. Output the execution parameters JSON schema for the HA two tier stack CT to a file in your current folder named CreateStackParams.json.

   ```
   aws amscm get-change-type-version --change-type-id "ct-06mjngx5flwto"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    CreateStackParams.json
   ```

   b. Modify the schema. Replace the *`variables`* as appropriate. For example, use the OS that you want for the EC2 instances the ASG will create. Record the `ApplicationName` as you will use it later to deploy the application. Note that you can add up to 50 tags.

```
{
"Description":      "HA two tier stack for WordPress",
"Name":             "WordPressStack",
"TimeoutInMinutes":  360,
"Tags": [
        {
            "Key": "ApplicationName",
            "Value": "WordPress"
        }
    ],
"AutoScalingGroup": {
            "AmiId":    "AMI-ID",
            "UserData": "#!/bin/bash \n
            REGION=$(curl 169.254.169.254/latest/meta-data/placement/
availability-zone/ | sed 's/[a-z]$//') \n
            yum -y install ruby httpd \n
            chkconfig httpd on \n
            service httpd start \n
            touch /var/www/html/status \n
            cd /tmp \n
            curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/
install \n
            chmod +x ./install \n
            ./install auto \n
            chkconfig codedeploy-agent on \n
            service codedeploy-agent start"
    },
    "LoadBalancer": {
        "Public":               true,
        "HealthCheckTarget":    "HTTP:80/status"
    },
    "Database":     {
        "DBEngine":             "MySQL",
        "DBName":               "wordpress",
        "EngineVersion":        "8.0.16 ",
        "LicenseModel":         "general-public-license",
        "MasterUsername":       "admin",
        "MasterUserPassword":   "p4ssw0rd"
    },
    "Application":  {
    "ApplicationName":  "WordPress"
        }
```

```
}
```

c. Output the CreateRfc JSON template to a file in your current folder named CreateStackRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateStackRfc.json
```

d. Modify the RFC template as follows and save it, you can delete and replace the contents. Note that `RequestedStartTime` and `RequestedEndTime` are now optional; excluding them creates an ASAP RFC that executes as soon as it is approved (which usually happens automatically). To submit a scheduled RFC, add those values.

```
{
"ChangeTypeVersion":    "3.0",
"ChangeTypeId":         "ct-06mjngx5flwto",
"Title":                "HA-Stack-For-WP-RFC"
}
```

e. Create the RFC, specifying the CreateStackRfc.json file and the CreateStackParams.json execution parameters file:

```
aws amscm create-rfc --cli-input-json file://CreateStackRfc.json --execution-
parameters file://CreateStackParams.json
```

You receive the RFC ID in the response. Save the ID for subsequent steps.

f. Submit the RFC:

```
aws amscm submit-rfc --rfc-id  RFC_ID
```

If the RFC succeeds, you receive no output.

g. To check RFC status, run

```
aws amscm get-rfc --rfc-id RFC_ID
```

Keep note of the RFC ID.

2. Launch an S3 bucket

Gathering the following data before you begin will make the deployment go more quickly.

REQUIRED DATA S3 BUCKET:

- `VPC-ID`: This value determines where your S3 Bucket will be. Use the same VPC ID that you used previously.
- `BucketName`: This value sets the S3 Bucket name, you use it to upload your application bundle. It must be unique across the region of the account and cannot include upper-case letters. Including your account ID as part of the BucketName is not a requirement but makes it easier to identify the bucket later. To see what S3 bucket names exist in the account, go to the Amazon S3 Console for your account.

a. Output the execution parameters JSON schema for the S3 storage create CT to a JSON file named CreateS3StoreParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3StoreParams.json
```

b. Modify the schema as follows, you can delete and replace the contents. Replace *`VPC_ID`* appropriately. The values in the example have been tested, but may not be right for you.

> **Tip**
>
> The `BucketName` must be unique across the region of the account and cannot include upper-case letters. Including your account ID as part of the BucketName is not a requirement but makes it easier to identify the bucket later. To see what S3 bucket names exist in the account, go to the Amazon S3 Console for your account.

```
{
"Description":      "S3BucketForWordPressBundle",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-s2b72beb000000000",
"Name":             "S3BucketForWP",
"TimeoutInMinutes":  60,
"Parameters":   {
    "AccessControl":    "Private",
    "BucketName":       "ACCOUNT_ID-BUCKET_NAME"
    }
```

```
}
```

c. Output the JSON template for CreateRfc to a file, in your current folder, named CreateS3StoreRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateS3StoreRfc.json
```

d. Modify and save the CreateS3StoreRfc.json file, you can delete and replace the contents. Note that `RequestedStartTime` and `RequestedEndTime` are now optional; excluding them creates an ASAP RFC that executes as soon as it is approved (which usually happens automatically). To submit a scheduled RFC, add those values.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-1a68ck03fn98r",
"Title":                "S3-Stack-For-WP-RFC"
}
```

e. Create the RFC, specifying the CreateS3StoreRfc.json file and the CreateS3StoreParams.json execution parameters file:

```
aws amscm create-rfc --cli-input-json file://CreateS3StoreRfc.json  --
execution-parameters file://CreateS3StoreParams.json
```

You receive the RfcId of the new RFC in the response. Save the ID for subsequent steps.

f. Submit the RFC:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

If the RFC succeeds, you receive no output.

g. To check RFC status, run

```
aws amscm get-rfc --rfc-id RFC_ID
```

### Create, Upload, and Deploy the Application

First, create a WordPress application bundle, and then use the CodeDeploy CTs to create and deploy the application.

1. Download WordPress, extract the files and create a ./scripts directory.

   Linux command:

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: Paste `https://github.com/WordPress/WordPress/archive/master.zip` into a browser window and download the zip file.

   Create a temporary directory in which to assemble the package.

   Linux:

   ```
   mkdir /tmp/WordPress
   ```

   Windows: Create a "WordPress" directory, you will use the directory path later.

2. Extract the WordPress source to the "WordPress" directory and create a ./scripts directory.

   Linux:

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

   Windows: Go to the "WordPress" directory that you created and create a "scripts" directory there.

   If you are in a Windows environment, be sure to set the break type for the script files to Unix (LF). In Notepad ++, this is an option at the bottom right of the window.

3. Create the CodeDeploy **appspec.yml** file, in the WordPress directory (if copying the example, check the indentation, each space counts). IMPORTANT: Ensure that the "source" path is correct for copying the WordPress files (in this case, in your WordPress directory) to the expected destination (/var/www/html/WordPress). In the example, the appspec.yml file is in the directory with the WordPress files, so only "/" is needed. Also, even if you used a RHEL AMI for your Auto Scaling group, leave the "os: linux" line as-is. Example appspec.yml file:

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. Create bash file scripts in the WordPress ./scripts directory.

   First, create `config_wordpress.sh` with the following content (if you prefer, you can edit the wp-config.php file directly).

> **Note**
>
> Replace *DBName* with the value given in the HA Stack RFC (for example, `wordpress`).
> Replace *DB_MasterUsername* with the `MasterUsername` value given in the HA Stack RFC (for example, `admin`).
> Replace *DB_MasterUserPassword* with the `MasterUserPassword` value given in the HA Stack RFC (for example, `p4ssw0rd`).
> Replace *DB_ENDPOINT* with the endpoint DNS name in the execution outputs of the HA Stack RFC (for example, `srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com`). You can find this with the GetRfc operation (CLI: get-

rfc --rfc-id RFC_ID) or in the AMS Console RFC details page for the HA Stack RFC that you previously submitted.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. In the same directory create `install_dependencies.sh` with the following content:

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS is installed as part of the user data at launch in order to allow health checks to work from the start.

6. In the same directory create `start_server.sh` with the following content:

   - For Amazon Linux instances, use this:

     ```
     #!/bin/bash
     service httpd start
     ```

   - For RHEL instances, use this (the extra commands are policies that allow SELINUX to accept WordPress):

     ```
     #!/bin/bash
     setsebool -P  httpd_can_network_connect_db 1
     setsebool -P  httpd_can_network_connect 1
     ```

```
chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
restorecon -Rv /var/www/html
service httpd start
```

7. In the same directory create `stop_server.sh` with the following content:

```
#!/bin/bash
service httpd stop
```

8. Create the zip bundle.

   Linux:

```
$ cd /tmp/WordPress
$ zip -r wordpress.zip .
```

   Windows: Go to your "WordPress" directory and select all of the files and create a zip file, be sure to name it wordpress.zip.

1. Upload the application bundle to the S3 bucket.

   The bundle needs to be in place in order to continue deploying the stack.

   You automatically have access to any S3 bucket instance that you create. You can access it through your bastions, or through the S3 console, and upload the WordPress bundle with drag-and-drop or browsing to and selecting the zip file.

   You can also use the following command in a shell window; be sure that you have the correct path to the zip file:

```
aws s3 cp wordpress.zip s3://BUCKET_NAME/
```

2. Deploy the WordPress application bundle.

   Gathering the following data before you begin will make the deployment go more quickly.

   REQUIRED DATA:

   - `VPC-ID`: This value determines where your S3 Bucket will be. Use the same VPC ID that you used previously.

- `CodeDeployApplicationName` and `CodeDeployApplicationName`: The `ApplicationName` value you used in the HA 2-Tier Stack RFC set the CodeDeployApplicationName and the CodeDeployDeploymentGroupName. The example uses "WordPress" but you may have used a different value.
- `S3Location`: For `S3Bucket`, use the `BucketName` that you previously created. The `S3BundleType` and `S3Key` are from the bundle that you put on your S3 store.

a. Output the execution parameters JSON schema for the CodeDeploy application deploy CT to a JSON file named DeployCDAppParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-2edc3sd1sqmrb"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 DeployCDAppParams.json
```

b. Modify the schema as follows and save it as, you can delete and replace the contents.

```
{
"Description":                        "DeployWPCDApp",
"VpcId":                              "VPC_ID",
"Name":                               "WordPressCDAppDeploy",
"TimeoutInMinutes":                   60,
"Parameters":   {
    "CodeDeployApplicationName":                "WordPress",
    "CodeDeployDeploymentGroupName":            "WordPress",
    "CodeDeployIgnoreApplicationStopFailures":   false,
    "CodeDeployRevision": {
      "RevisionType": "S3",
      "S3Location": {
        "S3Bucket":     "BUCKET_NAME",
        "S3BundleType": "zip",
        "S3Key":        "wordpress.zip" }
        }
    }
}
```

c. Output the JSON template for CreateRfc to a file, in your current folder, named DeployCDAppRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > DeployCDAppRfc.json
```

d. Modify and save the DeployCDAppRfc.json file, you can delete and replace the contents. Note that `RequestedStartTime` and `RequestedEndTime` are now optional; excluding them creates an ASAP RFC that executes as soon as it is approved (which usually happens automatically). To submit a scheduled RFC, add those values.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-2edc3sd1sqmrb",
"Title":                "CD-Deploy-For-WP-RFC"
}
```

e. Create the RFC, specifying the DeployCDAppRfc file and the DeployCDAppParams execution parameters file:

```
aws amscm create-rfc --cli-input-json file://DeployCDAppRfc.json  --execution-
parameters file://DeployCDAppParams.json
```

You receive the RfcId of the new RFC in the response. Save the ID for subsequent steps.

f. Submit the RFC:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

If the RFC succeeds, you receive no output.

g. To check RFC status, run

```
aws amscm get-rfc --rfc-id RFC_ID
```

### Validate the Application Deployment

Navigate to the endpoint (ELB CName) of the previously-created load balancer, with the WordPress deployed path: /WordPress. For example:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

### Tear Down the Application Deployment

Once you are finished with the tutorial, you will want to tear down the deployment so you are not charged for the resources.

The following is a generic stack delete operation. You'll want to submit it twice, once for the HA 2-Tier stack and once for the S3 bucket stack. As a final follow-through, submit a service request that all snapshots for the S3 bucket (include the S3 bucket stack ID in the service request) be deleted. They are automatically deleted after 10 days, but deleting them early saves a little bit of cost.

This walkthrough provides an example of using the AMS console to delete an S3 stack; this procedure applies to deleting any stack using the AMS console.

> **Note**
>
> If deleting an S3 bucket, it must be emptied of objects first.

REQUIRED DATA:

- `StackId`: The stack to use. You can find this by looking at the AMS Console **Stacks** page, available through a link in the left nav. Using the AMS SKMS API/CLI, run the For the AMS SKMS API reference, see the **Reports** tab in the AWS Artifact Console. operation (`list-stack-summaries` in the CLI).
- The change type ID for this walkthrough is `ct-0q0bic0ywqk6c`, the version is "1.0", to find out the latest version, run this command:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-0q0bic0ywqk6c
```

*INLINE CREATE*:

- Issue the create RFC command with execution parameters provided inline (escape quotes when providing execution parameters inline). E

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0"
 --title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

- Submit the RFC using the RFC ID returned in the create RFC operation. Until submitted, the RFC remains in the `Editing` state and is not acted on.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- Monitor the RFC status and view execution output:

```
aws amscm get-rfc --rfc-id RFC_ID
```

*TEMPLATE CREATE*:

1. Output the RFC template to a file in your current folder; example names it DeleteStackRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
```

2. Modify and save the DeleteStackRfc.json file. Since deleting a stack has only one execution parameter, the execution parameters can be in the DeleteStackRfc.json file itself (there is no need to create a separate JSON file with execution parameters).

   The internal quotation marks in the ExecutionParameters JSON extension must be escaped with a backslash (\). Example without start and end time:

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-0q0bic0ywqk6c",
"Title":                "Delete-My-Stack-RFC"
"ExecutionParameters":  "{
        \"StackId\":\"STACK_ID\"}"
}
```

3. Create the RFC:

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

   You receive the RfcId of the new RFC in the response. For example:

```
{
"RfcId": "daaa1867-ffc5-1473-192a-842f6b326102"
}
```

   Save the ID for subsequent steps.

4. Submit the RFC:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

If the RFC succeeds, you receive no confirmation at the command line.

5. To monitor the status of the request and to view Execution Output:

```
aws amscm get-rfc --rfc-id RFC_ID --query "Rfc.
{Status:Status.Name,Exec:ExecutionOutput}" --output table
```

## Console Tutorial: High Availability Two Tier Stack (Linux/RHEL)

This section describes how to deploy a high availability (HA) WordPress site into an AMS environment using the AMS console.

> **Note**
>
> This deployment walkthrough has been tested in AMZN Linux and RHEL environments.

Summary of tasks and required RFCs:

1. Create infrastructure (HA two-tier stack)
2. Create an S3 bucket for CodeDeploy applications
3. Create the WordPress application bundle and upload it to the S3 bucket
4. Deploy the application with CodeDeploy
5. Access the WordPress site and log in to validate the deployment
6. Tear down the deployment

Descriptions for all CT options, including ChangeTypeId, can be found in AMS Change Type Reference.

**Before You Begin**

The Deployment | Advanced Stack Components | High Availability Two Tier Stack | Create CT creates an Auto Scaling group, a load balancer, a database, and a CodeDeploy application name and deployment group (with the same name that you give the application). For information on CodeDeploy see What is CodeDeploy?

This walkthrough uses a High Availability Two-Tier Stack RFC that includes `UserData` and also describes how to create a WordPress bundle that CodeDeploy can deploy.

The `UserData` shown in the example gets instance metadata such as instance ID, region, etc, from within a running instance by querying the EC2 instance metadata service available at http://169.254.169.254/latest/meta-data/. This line in the user data script: `REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, retrieves the availability zone name from the meta-data service into the $REGION variable for our supported regions, and uses it to complete the URL for the S3 bucket where the CodeDeploy agent is downloaded. The 169.254.169.254 IP is routable only within the VPC (all VPCs can query the service). For information about the service, see Instance Metadata and User Data. Note also that scripts entered as UserData are executed as the "root" user and do not need to use the "sudo" command.

This walkthrough leaves the following parameters at the default value (shown):

- Auto Scaling group: `Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`.
- Load Balancer: `HealthCheckInterval=30, HealthCheckTimeout=5`.
- Database: `BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.
- Application: `DeploymentConfigName=CodeDeployDefault.OneAtATime`.

Variable Parameters:

The Console provides an **ASAP** option for the start time and this walkthrough recommends using it. **ASAP** causes the RFC to be executed as soon as approvals are passed.

> **Note**
>
> There are many parameters that you might choose to set differently than as shown. The values for those parameters shown in the example have been tested but may not be right for you. Only required values are shown in the examples. Values in *`replaceable`* font should be changed as they are particular to your account.

**Create the Infrastructure**

This procedure utilizes the High availability two-tier stack CT followed by the Create S3 storage CT.

Gathering the following data before you begin will make the deployment go more quickly.

REQUIRED DATA HA STACK:

- **AutoScalingGroup**:
  - **UserData**: This value is provided in this tutorial. It includes commands to set up the resource for CodeDeploy and start the CodeDeploy agent.
  - **AMI-ID**: This value determines the operating system of EC2 instances your Auto Scaling group (ASG) will spin up. Select an AMI in your account that starts with "customer-" and is of the operating system that you want. Find AMI IDs in the AMS Console VPCs -> VPCs details page. This walkthrough is for ASGs configured to use an Amazon Linux or RHEL AMI.
- **Database**:
  - These parameters, **DBEngine**, **EngineVersion**, and **LicenseModel** should be set according to your situation though the values shown in the example have been tested. The tutorial uses these values, respectively: *`MySQL`*, *`8.0.16`*, *`general-public-license`*.
  - These parameters, **DBName**, **MasterUserPassword**, and **MasterUsername** are required when deploying the application bundle. The tutorial uses these values, respectively: *`wordpressDB`*, *`p4ssw0rd`*, *`admin`*. Note that DBName can only contain alphanumeric characters.
  - When you enter the **MasterUsername** for the RDS DB, it will appear in cleartext, so log in to the database as soon as possible and change the password to ensure your security.
  - For **RDSSubnetIds**, use two Private subnets. Enter them one at a time pressing "Enter" after each. Find Subnet IDs with the For the AMS SKMS API reference, see the **Reports** tab in the

AWS Artifact Console. operation (CLI: list-subnet-summaries) or in the AMS Console VPCs -> VPC details page.

- **LoadBalancer**:
  - Set this parameter, **Public** to **true** because the tutorial uses Public ELB subnets.
  - **ELBSubnetIds**: Use two Public subnets. Enter them one at a time pressing "Enter" after each. Find Subnet IDs with the For the AMS SKMS API reference, see the **Reports** tab in the AWS Artifact Console. operation (CLI: list-subnet-summaries) or in the AMS Console VPCs -> VPC details page.
- **Application**: The **ApplicationName** value sets the CodeDeploy application name and CodeDeploy deployment group name. You use it to deploy your application. It must be unique in the account. To check your account for CodeDeploy names, see the CodeDeploy Console. The example uses `WordPress` but, if you will use that value, make sure that it is not already in use.

1. Launch the high availability stack.

   a. On the **Create RFC** page, select the category **Deployment**, subcategory **Standard Stacks**, item **High availability two-tier stack** and operation **Create**, from the list.

   b. IMPORTANT: Choose **Advanced** and set the values as shown.

      You only need to enter values for starred (*) options, tested values are shown in the example; you can leave not-required empty options blank.

   c. For the **RFC Description** section:

      ```
      Subject: WP-HA-2-Tier-RFC
      ```

   d. For the **Resource information** section, set parameters for **AutoScalingGroup**, **Database**, **LoadBalancer**, **Application**, and **Tags**.

      Also, the purpose of the "AppName" tag key is so you can easily search for the ASG instances in the EC2 console; you can call this tag key "Name" or any other key name that you want. Note that you can add up to 50 tags.

      ```
      UserData:
          #!/bin/bash
          REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/
       | sed 's/[a-z]$//')
          yum -y install ruby httpd
      ```

```
    chkconfig httpd on
    service httpd start
    touch /var/www/html/status
    cd /tmp
    curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/install
    chmod +x ./install
    ./install auto
    chkconfig codedeploy-agent on
    service codedeploy-agent start
AmiId:                AMI-ID
Description:          WP-HA-2-Tier-Stack

Database:
    LicenseModel:     general-public-license (USE RADIO BUTTON)
    EngineVersion:    8.0.16
    DBEngine:         MySQL
    RDSSubnetIds:     PRIVATE_AZ1 PRIVATE_AZ2 (ENTER ONE AT A TIME PRESSING
 "ENTER" AFTER EACH)
    MasterUserPassword:  p4ssw0rd
    MasterUsername:      admin
    DBName:              wordpressDB

LoadBalancer:
    Public:              true (USE RADIO BUTTON)
    ELBSubnetIds:        PUBLIC_AZ1 PUBLIC_AZ2

Application:
    ApplicationName:     WordPress

Tags:
    Name:                WP-Rhel-Stack
```

e. Click **Submit** when finished.

2. Log in to the database that you created and change the password.
3. Launch an S3 bucket Stack.

   Gathering the following data before you begin will make the deployment go more quickly.

   REQUIRED DATA S3 BUCKET:

   - **VPC-ID**: This value determines where your S3 Bucket will be. Find VPC IDs with the For the AMS SKMS API reference, see the **Reports** tab in the AWS Artifact Console. operation (CLI: list-vpc-summaries) or in the AMS Console VPCs page.

- **BucketName**: This value sets the S3 Bucket name, you use it to upload your application bundle. It must be unique across the region of the account and cannot include upper-case letters. Including your account ID as part of the BucketName is not a requirement but makes it easier to identify the bucket later. To see what S3 bucket names exist in the account, go to the Amazon S3 Console for your account.

a. On the **Create RFC** page, select the category **Deployment**, subcategory **Advanced Stack Components**, item **S3 storage**, and operation **Create** from the RFC CT pick list.

b. Keep the default **Basic** option and set the values as shown.

```
Subject:              S3-Bucket-WP-HA-RFC
Description:          S3BucketForWordPressBundles
BucketName:           ACCOUNT_ID-BUCKET_NAME
AccessControl:        Private
VpcId:                VPC_ID
Name:                 S3-Bucket-WP-HA-Stack
TimeoutInMinutes:     60
```

c. Click **Submit** when finished. The bucket deployed with this change type allows full read/write access to the whole account.

### Create, Upload, and Deploy the Application

First, create a WordPress application bundle, and then use the CodeDeploy CTs to create and deploy the application.

1. Download WordPress, extract the files and create a ./scripts directory.

   Linux command:

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: Paste `https://github.com/WordPress/WordPress/archive/master.zip` into a browser window and download the zip file.

   Create a temporary directory in which to assemble the package.

   Linux:

```
mkdir /tmp/WordPress
```

Windows: Create a "WordPress" directory, you will use the directory path later.

2. Extract the WordPress source to the "WordPress" directory and create a ./scripts directory.

   Linux:

```
unzip master.zip -d /tmp/WordPress_Temp
cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
rm -rf /tmp/WordPress_Temp
rm -f master
cd /tmp/WordPress
mkdir scripts
```

   Windows: Go to the "WordPress" directory that you created and create a "scripts" directory there.

   If you are in a Windows environment, be sure to set the break type for the script files to Unix (LF). In Notepad ++, this is an option at the bottom right of the window.

3. Create the CodeDeploy **appspec.yml** file, in the WordPress directory (if copying the example, check the indentation, each space counts). IMPORTANT: Ensure that the "source" path is correct for copying the WordPress files (in this case, in your WordPress directory) to the expected destination (/var/www/html/WordPress). In the example, the appspec.yml file is in the directory with the WordPress files, so only "/" is needed. Also, even if you used a RHEL AMI for your Auto Scaling group, leave the "os: linux" line as-is. Example appspec.yml file:

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
```

```
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. Create bash file scripts in the WordPress ./scripts directory.

   First, create `config_wordpress.sh` with the following content (if you prefer, you can edit the wp-config.php file directly).

   > **Note**
   >
   > Replace *DBName* with the value given in the HA Stack RFC (for example, `wordpress`).
   > Replace *DB_MasterUsername* with the `MasterUsername` value given in the HA Stack RFC (for example, `admin`).
   > Replace *DB_MasterUserPassword* with the `MasterUserPassword` value given in the HA Stack RFC (for example, `p4ssw0rd`).
   > Replace *DB_ENDPOINT* with the endpoint DNS name in the execution outputs of the HA Stack RFC (for example, `srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com`). You can find this with the GetRfc operation (CLI: get-rfc --rfc-id RFC_ID) or in the AMS Console RFC details page for the HA Stack RFC that you previously submitted.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. In the same directory create `install_dependencies.sh` with the following content:

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS is installed as part of the user data at launch in order to allow health checks to work from the start.

6. In the same directory create `start_server.sh` with the following content:

   - For Amazon Linux instances, use this:

     ```
     #!/bin/bash
     service httpd start
     ```

   - For RHEL instances, use this (the extra commands are policies that allow SELINUX to accept WordPress):

     ```
     #!/bin/bash
     setsebool -P  httpd_can_network_connect_db 1
     setsebool -P  httpd_can_network_connect 1
     chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
     restorecon -Rv /var/www/html
     service httpd start
     ```

7. In the same directory create `stop_server.sh` with the following content:

   ```
   #!/bin/bash
   service httpd stop
   ```

8. Create the zip bundle.

   Linux:

   ```
   $ cd /tmp/WordPress
   $ zip -r wordpress.zip .
   ```

Windows: Go to your "WordPress" directory and select all of the files and create a zip file, be sure to name it wordpress.zip.

1. Upload the application bundle to the S3 bucket

   The package needs to be in place in order to continue deploying the stack.

   You automatically have access to any S3 bucket instance that you create. You can access it through your Bastions (see Accessing Instances), or through the S3 console, and upload the CodeDeploy package with drag-and-drop, or by browsing to and selecting the file.

   You can also use the following command in a shell window; be sure that you have the correct path to the zip file:

   ```
   aws s3 cp wordpress/wordpress.zip s3://BUCKET_NAME/
   ```

2. Deploy the WordPress CodeDeploy Application Bundle

   REQUIRED DATA CODEDEPLOY APPLICATION DEPLOYMENT:

   - **CodeDeployApplicationName**: The name you gave the CodeDeploy application.
   - **CodeDeployGroupName**: Since the CodeDeploy application and group were both created from the name you gave the CodeDeploy application in the HA stack RFC, this is the same name as the **CodeDeployApplicationName**.
   - **S3Bucket**: The name you gave the S3 bucket.
   - **S3BundleType** and **S3Key**: These are part of the WordPress application bundle you deployed.
   - **VpcId**: The relevant VPC.

   a. On the **Create RFC** page, select the category **Deployment**, subcategory **Applications**, item **CodeDeploy application**, and operation **Deploy** from the RFC CT pick list.

   b. Keep the default **Basic** option, and set the values as shown.

> **Note**
>
> Reference the CodeDeploy application, CodeDeploy deployment group, S3 bucket and bundle previously created.

```
Subject:                                    WP-CD-Deploy-RFC
Description:                                DeployWordPress
S3Bucket:                                   BUCKET_NAME
S3Key:                                      wordpress.zip
S3BundleType:                               zip
CodeDeployApplicationName:                  WordPress
CodeDeployDeploymentGroupName:              WordPress
CodeDeployIgnoreApplicationStopFailures:    false
RevisionType:                               S3



VpcId:                                      VPC_ID
Name:                                       WP-CD-Deploy-Op
TimeoutInMinutes:                           60
```

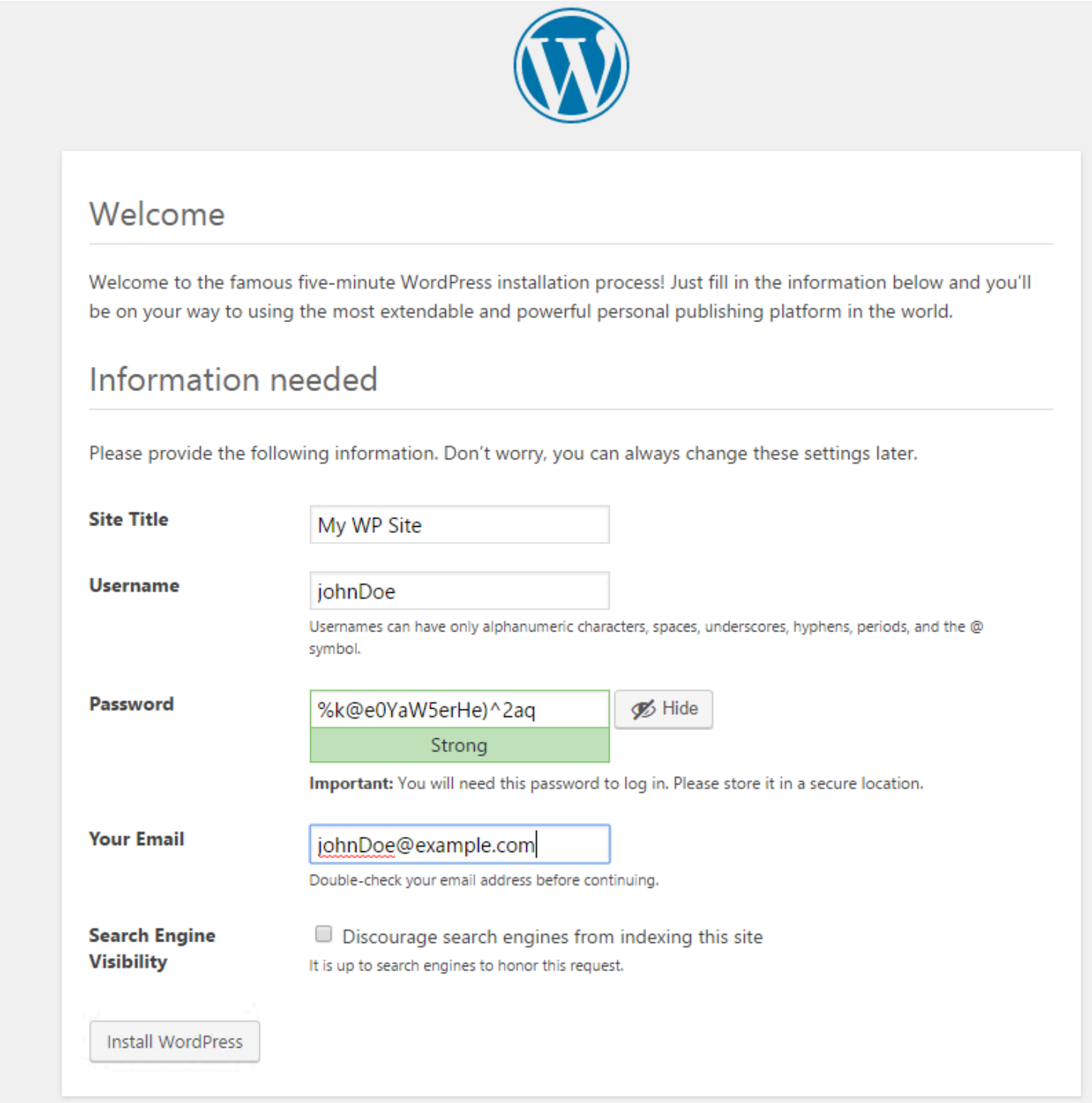
c. Click **Submit** when finished.

### Validate the Application Deployment

Navigate to the endpoint (LoadBalancerCName) of the previously-created load balancer, with the WordPress deployed path: /WordPress. For example:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

You should see a page like this:




### Tear Down the High Availability Deployment

To tear down the deployment, you submit the Delete Stack CT against the HA Two-Tier stack, and the S3 bucket, and you can request that RDS snapshots be deleted (they are deleted automatically after ten days, but they do cost a small amount while there). Gather the stack IDs for the HA stack and the S3 bucket and then follow these steps. See Stack | Delete.

# Appendix: SALZ onboarding questionnaire

**Topics**


- Deployment summary
- Environment architecture considerations
- Single-Account Landing Zone Monitoring Alerts
- Maintenance Window
- Next Steps


This is some of the information that you will need to think about before onboarding an account.

## Deployment summary

A description of the deployment. For example:

- This account is for a Line-of-Business application deployment (as opposed to a Product application deployment).
- The deployment involves an auto-scaled ARP (authenticated reverse proxy) within the account's public or DMZ subnet.
- Web and application servers will be deployed within the account's private subnet.
- An RDS (Amazon Relational Database Service) instance will also be deployed within the account's private Subnet.
- The servers (ARP, web, application, database, load balancer, etc.) are separated into distinct security groups.
- The account requires an HA (high availability) design spread across availability zones (AZs) i.e. "Multi-AZ".

## Environment architecture considerations

Consider the following criteria in deciding how to configure your environment and architecture.

- Will your virtual data center connect back to your corporate network?
  - Do you have an existing AWS DirectConnect service or do you require a new DirectConnect service?

  - Do you have an existing VPN connection or do you require a new VPN service?
- What is the available CIDR block range of internal addresses that you could allocate? (/16 recommended, must not overlap corporate network ranges)
- Will your virtual data center require internet access?
- Which Region(s) do you intend to use? (Sydney/N. Virginia/Dublin)
- Will you require a Shared Services subnet to host applications that have connectivity to all other subnets?
- What are your organizational divisions that you would like to be hosted as separate subnets. For each:
  - What connectivity to other subnets do you need?
  - Does the subnet require Internet access?
  - Are there any application deployment restrictions to that subnet?
  - Are there any particular network requirements for that subnet?
- Would you like separate development and/or test environments? (Will include shared services duplicate for anytime access)
- What are your snapshot backup requirements?
- Do you have an existing maintenance process or patch window(s) that you would like to keep?
- What are your domain registration requirements?
- Do you have any single sign-on requirements? (e.g., AD, LDAP)
- What are your overall expected operating system and anticipated capacity requirements?

## Single-Account Landing Zone Monitoring Alerts

AMS provides a way for you to be directly alerted (versus getting AMS service notifications) for certain monitoring alerts. To sign up for this, make sure that your Cloud Architect (CA or Cloud Service Delivery Manager (CSDM) receive this information:

**Direct Alerts Email**: These are the email addresses that you want AMS to send certain resource-based alerts to. For details of which alerts are sent directly to email, see Alerts from Baseline Monitoring in AMS in the AMS User Guide for Single-Account Landing Zone. For more information on AMS monitoring, see Monitoring Management in the AMS User Guide for Single-Account Landing Zone.

## Maintenance Window

You will want to create a maintenance window that considers different application needs, different AWS Regions, and different stress periods. Your maintenance window is when AMS will apply patching. Here are some guidelines:

- To limit the impact on users, plan your maintenance window according to the AWS Region where your environments are deployed.
- Schedule a window outside of regular business hours and when the least traffic is expected on production servers.
- Typically, infrastructure stacks require monthly updates.
- Schedule a maintenance window for at least 300 minutes. Operating system patching takes 60-90 minutes, infrastructure stack patching takes 180-300 minutes.

## Next Steps

The AMS onboarding team will assist you in every step of onboarding your account to AMS. These are onboarding requirements:

- Provision a new AWS account to use for AMS and provide an AWS account ID.
- Sign up for the desired level of Support.
- Create a cross-account IAM role to grant the AMS provisioning account access and provide the role name to AMS.
- Add the account 753102745277 as a Trusted Entity.

# 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:** March 21, 2024

| Change | Description | Date |
| --- | --- | --- |
| Precise change type reference s | Create, Change, or Delete Security Groups.<br><br>To add a user: Submit an RFC using Management \| Directory Service \| Users and groups \| Add user to group [ct-24pi85mjtza8k] and To remove a user: Submit an RFC using Management \| Directory Service \| Users and groups \| Remove user from group [ct-2019s 9y3nfml4] | August 08, 2025 |
| TOC link removed | TOC AWS Glossary link removed. | August 08, 2025 |
| Added link for prescription guidance | Set up consolidated billing–link new account to Payer account. | May 08, 2025 |
| Updated instructions to activate IAM access to the AWS Management Console | Clarified the instructions for activating IAM access to the AWS Management Console. | Activate IAM access to the AWS console |
| Updated number of allowed transit virtual interfaces on Direct Connect dedicated connections | Direct Connect dedicated connections now have a limit of 4 transit virtual interfaces per connection | Connectin g Direct Connect to Transit Gateway |

| Change | Description | Date |
| --- | --- | --- |
| Improve wording. | Specified that "only used as a "Deny" list " must include "Allow All" to ensure AMS monitoring and management operations. | Network configuration |
| Additional information on using the AMS CLI. | "Added note that the `--region` option may be needed for some CLI commands" | Install the AMS CLIs |
| Updated: Chapter headings for consistency and readabili y, moved some topic sub-secti ons into more appropriate sections | "Modes for change management" is the new heading for "Change management" | Change management modes |
| Updated content | The AMS mode previously known as "Change Management mode" or "Standard CM mode" is now known as "RFC mode." The modes section has been expanded. | RFC mode. |
| Updated content | The AMS mode previously known as "Change Management mode" or "Standard CM mode" is now known as "RFC mode." The modes section has been shortened and links to the *AMS Advanced User Guide* sections on modes added. | AMS modes. |
| MALZ: Updated network architecture diagram | Networking account architecturem | June 16, 2022 |
| Moved topic list to below opening paragraphs | AWS Managed Services Onboarding Introduct ion | June 16, 2022 |
| Updated content, inclusive language initiative | "Management account" not "Master account. | IAM user role in AMS , "Policy examples" section |

| Change | Description | Date |
| --- | --- | --- |
| Updated content, Tools account role names | Updated role name CustomerMigrationAccessRole to AWSManagedServicesMigrationRole. | AWS Application Migration Service (AWS MGN) |
| SALZ: Continuity management defaults | Updated link and removed obsolete information from VPC tag and defaults | February 28, 2022 |