



Building an Enterprise Blueprint Factory by using AWS Service Catalog

AWS Prescriptive Guidance



AWS Prescriptive Guidance: Building an Enterprise Blueprint Factory by using AWS Service Catalog

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

Introduction	1
Business overview	1
Solution overview	2
Intended audience	2
Objectives	3
Architecture	4
Components	6
Product repo	6
Config repo	6
Config file	7
Config pipeline	9
Release pipeline	11
Blueprint life cycle	14
Blueprint creation	14
Blueprint update	14
Blueprint deletion	15
Setting up	17
Prerequisites	17
Best practices	18
Create repos	18
Set up the factory	19
Delete the factory	27
Using the factory	29
Prerequisites	29
Create blueprint	29
Update blueprint	32
Delete blueprint	33
Troubleshooting	34
Related resources	36
AWS documentation	36
AWS blog posts	36
Contributors	37
Authoring	37
Reviewing	37

Technical writing	37
Document history	38
Glossary	39
#	39
A	40
B	43
C	45
D	48
E	52
F	54
G	56
H	57
I	58
L	61
M	62
O	66
P	69
Q	71
R	72
S	75
T	79
U	80
V	81
W	81
Z	82

Building an Enterprise Blueprint Factory by using AWS Service Catalog

Amazon Web Services ([contributors](#))

October 2024 ([document history](#))

Business overview

Many enterprises face challenges when scaling their workloads in the cloud. These organizational challenges include the following:

- Creating infrastructure as code (IaC) templates that can be reused at scale for multiple AWS services
- Validating that IaC templates follow security best practices
- Reducing [undifferentiated](#) or repetitive tasks that can significantly reduce developer productivity and extend the time to market
- Establishing consistency for IaC templates
- Reducing resource utilization, particularly for the security team, to avoid repeatable manual reviews

Creating an IaC template that follows security best practices requires that you establish guardrails and security controls. Traditionally, the cloud platform team or security team would manually review the code in each IaC template. Alternatively, developers would deploy the IaC template in non-production environment and rely on [detective controls](#) to find any security issues. Both of these approaches require iterative feedback cycles, slow down the development process, and increase the manual engineering effort.

As a result, many enterprises want to streamline the creation, validation, and release of IaC templates. They also want a means of managing and governing those templates after release. Proper management and governance mechanisms help you update templates and make sure that developers have access to the latest versions. These mechanisms also help you oversee and audit the use of templates across the organization.

Solution overview

This guide explains the Enterprise Blueprint Factory solution, which helps you streamline the creation, validation, publishing, distribution, and consumption of infrastructure as code (IaC) templates across your organization. These IaC templates are also called *blueprints*. This solution supports blueprint files that are AWS CloudFormation [templates](#) or AWS Cloud Development Kit (AWS CDK) [constructs](#).

The Enterprise Blueprint Factory uses a config-driven approach to automate the sharing, publishing, and distribution of blueprints. A developer adds a blueprint to a product repository and then adds the blueprint information to a config file. This automatically initiates a continuous integration and continuous delivery (CI/CD) release pipeline. This pipeline validates that the blueprint follows AWS security best practices. This helps make sure that your organization's blueprints are secure by design. *Security by design* is a system engineering approach that takes security into account through the whole development process.

The Enterprise Blueprint Factory releases blueprints as *products* in [AWS Service Catalog](#). By using Service Catalog, end users can quickly deploy the approved blueprints that you provide. Service Catalog is also designed to provide management and governance features so that administrators can define [fine-grained access controls](#) and oversee blueprint usage.

Intended audience

The [Enterprise Blueprint Factory architecture](#) section helps architects, managers, and technical leads evaluate this solution and determine whether it is a good fit for their organization. This section describes what blueprints are, how you can use Service Catalog to manage them, and the architecture of the Enterprise Blueprint Factory.

The [Setting up the Enterprise Blueprint Factory](#) section helps DevOps engineers deploy the Enterprise Blueprint Factory in your AWS environment. It includes detailed instructions for setting up the required repositories and the configuration pipeline.

The [Using the Enterprise Blueprint Factory](#) section helps blueprint developers create, update, or delete blueprints in your environment. It provides detailed instructions for managing a blueprint throughout its life cycle. To create blueprints, developers must understand how to create IaC templates, such as CloudFormation templates. This guide does not include information or instructions about how to define these blueprints.

Objectives

The Enterprise Blueprint Factory helps your organization achieve the following benefits:

- Validate that blueprints follow AWS security best practices
- Automate and standardize the release and validation process for blueprints
- Improve developer productivity by reducing the number of manual tasks they must perform
- Use fine-grained access controls to determine which blueprints end users can access
- Use version control to manage blueprint updates and share them with end users
- Help end users self-serve the discovery and launch of blueprints
- Oversee and audit the use of blueprints across the organization

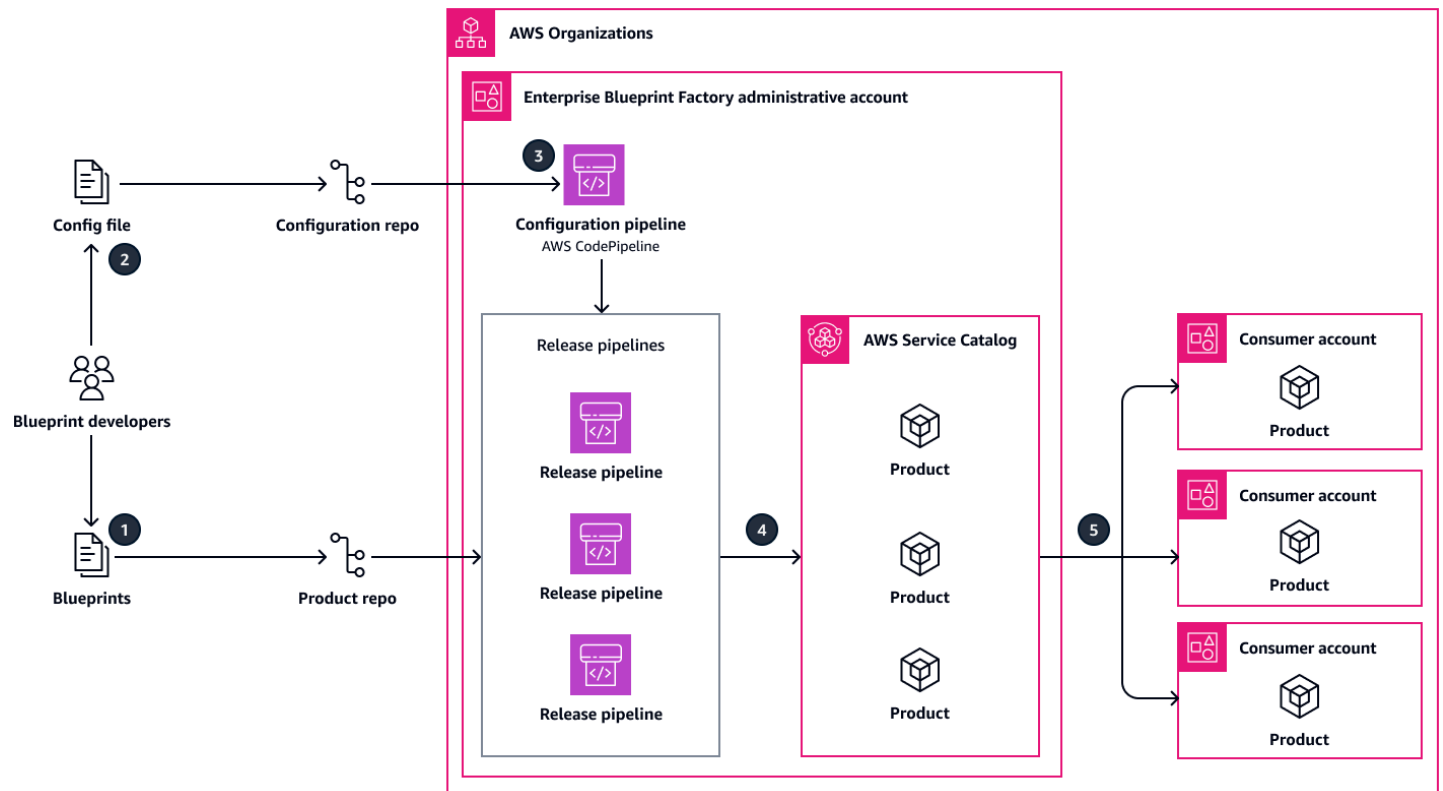
Enterprise Blueprint Factory architecture

An infrastructure as code (IaC) template, also called a *blueprint*, is a configuration file that helps you provision and manage cloud resources. A blueprint might provision a single resource, or it might provision the architecture for a complex, multi-tier application. IaC is designed to help you centralize infrastructure management, standardize resources, and scale quickly.

The Enterprise Blueprint Factory helps you streamline the creation, validation, publishing, distribution, and consumption of blueprints across your organization. In addition to providing an architectural overview, this section reviews the [architectural components](#) of the solution and the [blueprint life cycle](#).

When you release a blueprint through the Enterprise Blueprint Factory, the blueprint becomes a [product](#) in [AWS Service Catalog](#). You collect products into one or more [portfolios](#) and then grant permissions that allow end users to access the products in that portfolio. You can use a [portfolio share](#) to allow a Service Catalog administrator for another AWS account to distribute your products to end users.

The following diagram shows a high-level overview of the Enterprise Blueprint Factory architecture. This workflow releases the blueprint as a product in Service Catalog. It also creates or updates the portfolios and portfolio shares in order to make the blueprint available to the target end users.



This diagram shows the following workflow:

1. A developer builds the blueprint. They create a feature branch in the product repository, push the blueprint to the branch, and then create a pull request. A blueprint administrative team and security team review the pull request to make sure that the blueprint meets organizational and security requirements. These teams approve the pull request. The developer merges the feature branch into the main branch. For more information, see [Product repository](#) in this guide.
2. The developer adds or updates the blueprint information in the config file that is located in the configuration repository. For more information, see [Configuration repository](#) and [Configuration file](#) in this guide.
3. The update to the config file invokes the configuration pipeline. This pipeline uses [AWS CodePipeline](#) and [AWS CodeBuild](#) projects to create or update the Service Catalog portfolios and portfolio shares. It also creates a release pipeline for the blueprint. For more information, see [Configuration pipeline](#) in this guide.
4. The release pipeline performs various security checks on the blueprint. If the blueprint passes, the release pipeline deploys the blueprint as a product in Service Catalog. For more information, see [Release pipeline](#) in this guide.

5. By accessing the product through portfolios and portfolio shares, end users deploy the blueprint in their target consumer accounts.

Enterprise Blueprint Factory components

The Enterprise Blueprint Factory consists of the following components:

- [Product repository](#) – A repository where you store the blueprints.
- [Configuration repository](#) – A repository where you store the config file that defines your AWS Service Catalog portfolios and products.
- [Configuration file](#) – The config file that defines what blueprints are available, who can use them, and how they can use them.
- [Configuration pipeline](#) – A DevOps CI/CD pipeline that sets up the Service Catalog portfolio and portfolio shares and creates a release pipeline for each product.
- [Release pipeline](#) – A DevOps CI/CD pipeline that releases blueprints as Service Catalog products.

The cloud infrastructure team typically manages the overall Enterprise Blueprint Factory because they must approve each blueprint. However, the DevOps code team is typically responsible for the configuration pipeline and release pipeline. In order to release new blueprints, developers interact only with the product repository, configuration repository, and configuration file.

Product repository

The product repository is a centralized location where you store the blueprints that your organization approves. A blueprint administrative team and security team review the pull requests to this repository to make sure that each blueprint meets organizational and security requirements. In this guide, we use GitHub for the repository, but you could use an alternative.

Configuration repository

The configuration repository (config repo) is the location where your organization stores the configuration file for your Service Catalog portfolios and products that are released through the Enterprise Blueprint Factory. In this guide, we use GitHub for the repository, but you could use an alternative.

Configuration file

The Enterprise Blueprint Factory configuration file (config file) is stored in the configuration repository, which is owned by the blueprint administrative team. The name of this file is **bp_config.yml**. When a developer updates this file, the blueprint administrative team reviews the changes. Merging the changes into the main branch initiates the configuration pipeline. The config file orchestrates the publishing, sharing, and distribution of all blueprints that are managed through the Enterprise Blueprint Factory.

The config file is a YAML file that consists of two main objects: `portfolios` and `products`. The following is an example of a sample config file:

```
portfolios:
  - portfolio_name: blueprint-portfolio
    owner: Blueprint-team
    provider_name: AWS
    description: "Blueprint portfolio"
    portfolio_access_role:
      - arn:aws:iam::123456789012:role/examplerole
      - arn:aws:iam::123456789012:user/exampleuser
    share_to_ou:
      - org_id: "o-exampleOrgID"
    stack_tags:
      DataClassification: Confidential
      Organization: AWS
products:
  - name: BP-S3-Product
    description: "Blueprint for BP-S3 product"
    product_config_file: 'BP-S3/product_config.json'
    owner: Blueprint-team
    stack_tags:
      DataClassification: Confidential
      Organization: AWS
    portfolio_associations:
      - blueprint-portfolio
    launch_constraint_role: arn:aws:iam::123456789012:role/examplelaunchrole
```

In the `portfolios` object, you define your target Service Catalog portfolios. For each portfolio, you provide the following attributes:

- `portfolio_name` is the name of the portfolio. This attribute is required.

- `owner` is the name of the team who owns the portfolio. This attribute is optional.
- `provider_name` is the name of the team or organization that manages the portfolio. The default value is `AWS`. This attribute is required.
- `description` is a brief description of the portfolio. This attribute is optional.
- `portfolio_access_roles` are the AWS Identity and Access Management (IAM) [identities](#) (users, roles, or groups) that are allowed to access the portfolio and its associated products. This attribute is optional.
- `share_to_ou` is the [organizational unit](#) (OU) in AWS Organizations that the portfolio is shared with. End users can deploy this portfolio's products in AWS accounts that are members of the target OU. This attribute is optional.
- `stack_tags` are the [tags](#) applied to the portfolio. This attribute is optional.

In the `products` object, you define each blueprint that you want to release as a product in Service Catalog. For each product, you provide the following attributes:

- `name` is the name of the product in Service Catalog. This attribute is required.
- `description` is a brief description of the product. This attribute is required.
- `product_config_file` is the name of the blueprint product configuration file that is stored in the product repository. This attribute is required.
- `owner` is the name of the team who owns the product. This attribute is required.
- `stack_tags` are the tags applied to the product. This attribute is optional.
- `portfolio_associations` are the target portfolios that contain the product. This attribute is optional.

Note

We recommend that you add products only to portfolios that are managed through the Enterprise Blueprint Factory. If you want to add products to portfolios that are not managed through the Enterprise Blueprint Factory, the user's IAM policy must allow the [AssociateProductWithPortfolio](#) action. However, as a security best practice, we recommend that you allow this action only for the Enterprise Blueprint Factory configuration pipeline.

- `launch_constraint_role` is the [launch role](#) that Service Catalog assumes when an end user launches the product. This attribute is required.

Configuration pipeline

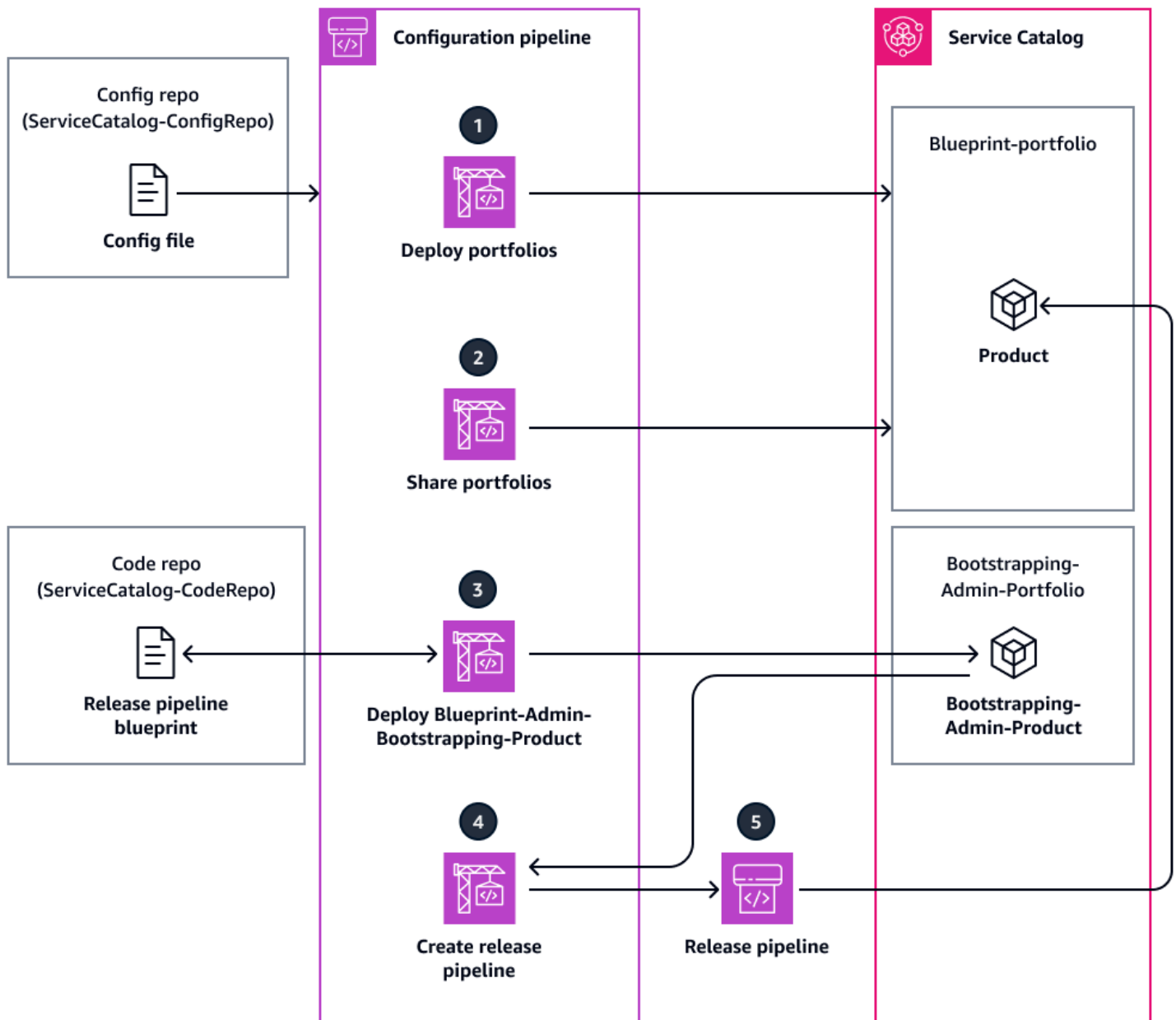
The configuration pipeline (config pipeline) automates the configuration of the Service Catalog portfolio and portfolio shares. It also creates the release pipeline for each product. This pipeline is an [AWS CodePipeline](#) resource. An update to the config file invokes the configuration pipeline.

The first time that you invoke the config pipeline, it creates two additional portfolios that are not defined in your config file:

- `Blueprint-portfolio` – Every product that you deploy through the Enterprise Blueprint Factory is added to this portfolio. This portfolio is available to the IAM principals and organizational units that you specify in the config file.
- `Bootstrapping-Admin-Portfolio` – The `Bootstrapping-Admin-Product` product is associated with this portfolio. This product is a CloudFormation template for the release pipeline. Allow only the blueprint administrative team to access this portfolio so that they can manage administrative products.

Configuration pipeline stages

The following image shows the stages in the config pipeline and the resources that the pipeline interacts with. Each stage in the pipeline is an [AWS CodeBuild](#) project.



The following are the stages of the configuration pipeline:

- 1. Deploy portfolios** – The config pipeline deploys any portfolios that have been added to the config file or deletes any portfolios that have been removed from the config file. If there are no changes to the portfolios, then the pipeline skips this stage.
- 2. Share portfolios** – The config pipeline shares the portfolios with the target organizational units (OUs). If there are no changes to the portfolio shares, then the pipeline skips this stage.
- 3. Deploy Blueprint-Admin-Bootstrapping-Product** – The config pipeline fetches the bp-pipeline blueprint from the ServiceCatalog-CodeRepo repo and deploys it to Service

Catalog as `Bootstrapping-Admin-Product`. This product is the CloudFormation template that is used to create a release pipeline. Deploying this template as a Service Catalog product helps maintain version control. If there are no changes to the `bp-pipeline` blueprint, then the pipeline skips this stage.

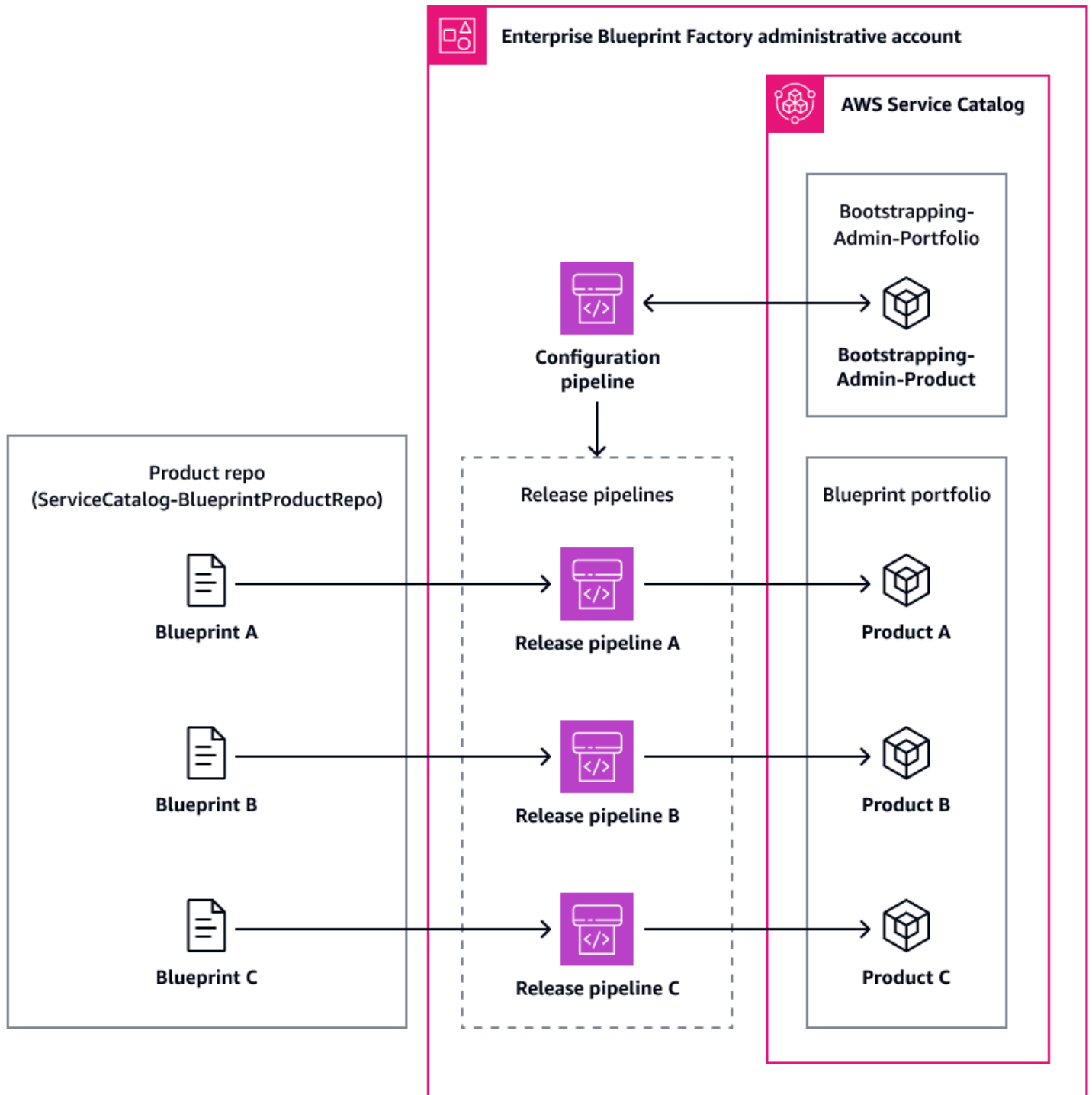
4. **Create release pipelines** – Based on the product attributes in the config file, the config pipeline prepares the stack parameters and launches a CloudFormation stack that creates a release pipeline for the product. For more information, see [Release pipeline](#) in this guide.
5. **Deploy products** – The release pipeline deploys the blueprint as a Service Catalog product and associates it with the target portfolio. End users can now deploy the product in AWS accounts that are members of the target OU.

Release pipeline

The release pipeline automates the release of blueprints as Service Catalog products. This pipeline is an [AWS CodePipeline](#) resource. When your organization wants to release a new blueprint, a developer uploads the IaC template and its product config file to the product repo. Adding the product details to the config file triggers the config pipeline. The config pipeline creates a release pipeline for this blueprint. Any subsequent updates to the blueprint triggers this release pipeline to update the product in Service Catalog with a new version.

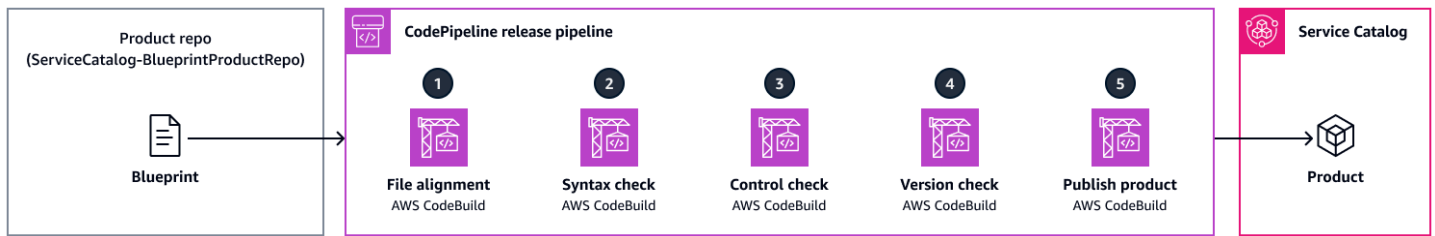
The release pipeline includes [proactive controls](#) that automate security and compliance checks for your blueprints. *Proactive controls* are designed to prevent the creation of noncompliant resources. These controls can reduce the number of security events handled by other types of [security controls](#), such as responsive and detective controls. Because proactive controls make sure that deployed resources are compliant before they are deployed, there is no detection event that requires response or remediation.

The first time that you invoke the configuration pipeline, it creates a Service Catalog product that is named `Bootstrapping-Admin-Product`. This product is the CloudFormation template for the release pipeline. As shown in the following figure, the configuration pipeline uses the `Bootstrapping-Admin-Product` product to create a dedicated release pipeline for each new blueprint. There is a one-to-one relationship between blueprints and release pipelines.



Release pipeline stages

The following image shows the default stages in the release pipeline and the resources that the pipeline interacts with. Each stage in the pipeline is a CodeBuild project.



The following are the stages of the release pipeline:

- 1. File alignment** – This stage verifies that the blueprint is an CloudFormation [template](#) or an AWS Cloud Development Kit (AWS CDK) [construct](#). If the blueprint is an AWS CDK construct, this stage synthesizes the AWS CDK construct into a CloudFormation template. This process automates and standardizes deployments through CloudFormation. If any errors are found, the pipeline fails.
- 2. Syntax check** – Syntax error is a common cause of CloudFormation deployment errors. In this stage, [AWS CloudFormation Linter \(cfn-lint\)](#) checks for syntax errors by comparing the template to the [AWS CloudFormation resource specification](#). It also performs other checks, such as checking for valid values for resource properties and adherence to best practices. If any errors are found, the pipeline fails, and cfn-lint returns suggestions.
- 3. Control check** – In this stage, [cfn_nag](#) checks for potential security issues by searching for patterns. For example, it checks for overly permissive security groups and AWS Identity and Access Management (IAM) policies, missing encryption, and password literals. If any errors are found, the pipeline fails, and cfn_nag returns suggestions.
- 4. Version check** – The release pipeline performs version control based on the version strategy that is defined in the product config file. If the product version is defined as [immutable](#), Service Catalog inactivates the previous product version.
- 5. Publish product** – The release pipeline releases the product in Service Catalog.

Note

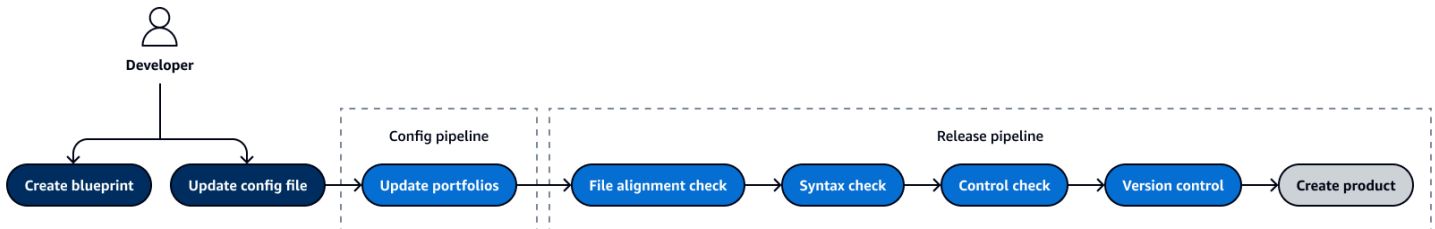
The release pipeline is customizable. For example, you can remove any stages that are not applicable for your use case. You could also add more stages if you want to add other control checks, additional validations, or a manual approval step. This guide does not include instructions for modifying the release pipeline. For more information, see the [CodePipeline](#) and [CodeBuild](#) documentation.

Blueprint life cycle in the Enterprise Blueprint Factory

The life cycle of an Enterprise Blueprint Factory blueprint consists of three typical stages: creation, update, and deletion. The life cycle stage affects which actions that the config pipeline and release pipeline perform.

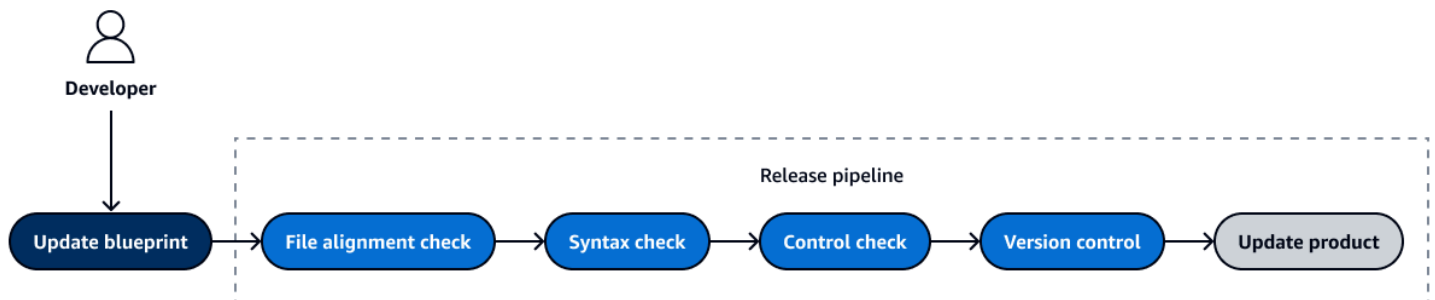
Blueprint creation

To release a new blueprint as a product in AWS Service Catalog, a developer merges the blueprint into the product repository, updates the portfolios in the config file, and adds the new product to the config file. This invokes the configuration pipeline. The config pipeline creates a release pipeline for the product. In the release pipeline, the blueprint undergoes multiple security checks. The release pipeline then deploys the blueprint as a Service Catalog product.



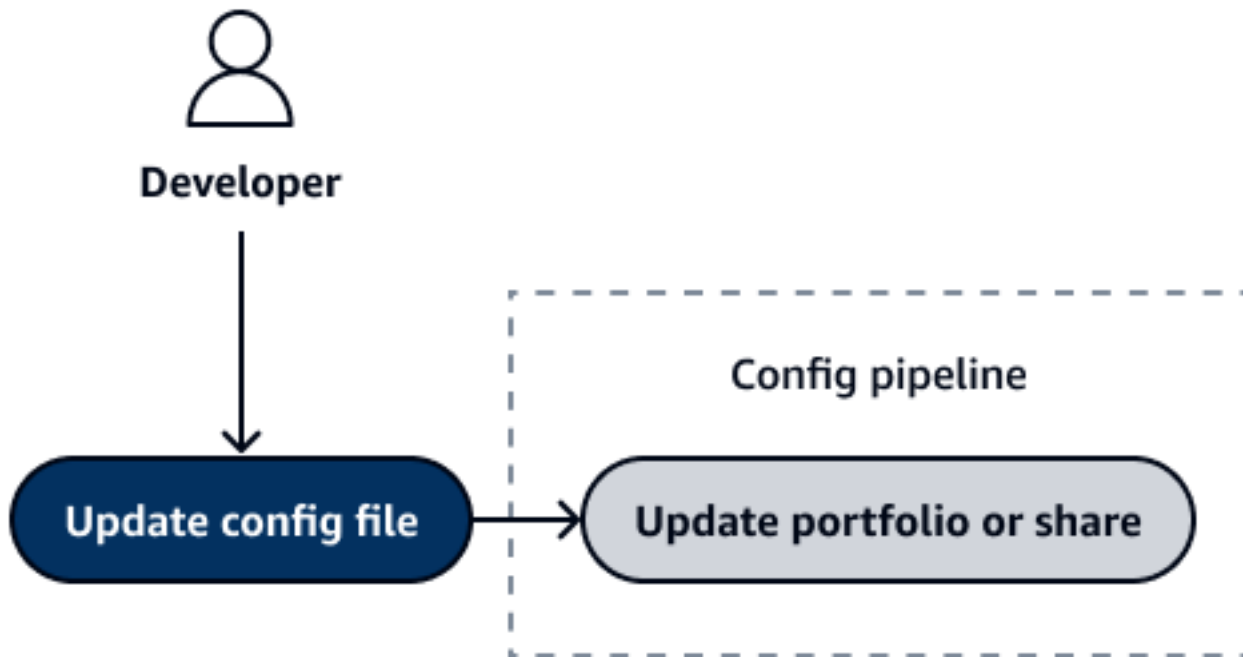
Blueprint update

A developer can update the product in Service Catalog by merging an updated version of the blueprint into the product repository. This update invokes the release pipeline for the product. The updated template undergoes the security checks in the release pipeline. The release pipeline deploys a new version of the Service Catalog product. For more information about how Service Catalog updates the product version, see [Managing versions](#) in the Service Catalog documentation.



Alternatively, you can update which Service Catalog portfolio the blueprint is associated with or you can change the sharing configurations for those portfolios. In this case, the developer updates

the config file in the configuration repo. The configuration pipeline updates the portfolios or portfolio shares. In this case, the product in Service Catalog is unchanged, although it may now be included in different portfolios.



Blueprint deletion

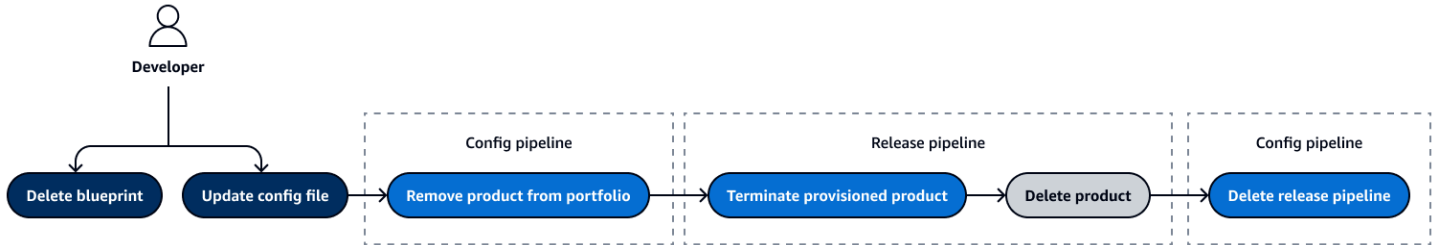
⚠ Important

You cannot recover a Service Catalog product after it is deleted. However, you can redeploy the blueprint as a new product.

When you delete a product, Service Catalog removes all of product versions from every portfolio that contains the product. For more information, see [Deleting products](#) in the Service Catalog documentation.

To delete a blueprint after it has been deployed in Service Catalog, a developer deletes the blueprint in the product repo. Then they remove the product from the config file. The config pipeline disassociates the product from the portfolios that contain it and deletes all product associates. The release pipeline terminates the Service Catalog product and the [provisioned products](#). Then, the config pipeline deletes the product's release pipeline.

If the config pipeline is unable to disassociate all of the product's resources, then the product is not deleted and the pipeline fails. You must resolve the failed resource disassociation and then restart the pipeline. For more information, see [Resolving failed resource disassociations when deleting a product](#).



Setting up the Enterprise Blueprint Factory

This section helps you set up the Enterprise Blueprint Factory in your AWS environment. It includes detailed instructions for setting up the required repositories and the AWS resources for the Enterprise Blueprint Factory.

Prerequisites

The following are the prerequisites for setting up the Enterprise Blueprint Factory in your AWS environment:

- The following AWS accounts:
 - An account that is used to administrate the Enterprise Blueprint Factory and to release products
 - One or more accounts that consume the released product
- All accounts are:
 - Managed as an organization in [AWS Organizations](#)
 - Located in the same [organizational unit \(OU\)](#)
 - The organization follows the [account-per-tenant model](#)
- AWS Command Line Interface (AWS CLI), [installed](#) and [configured](#)
- Permissions to deploy an AWS CloudFormation stack that creates the following AWS resources:
 - Amazon CloudWatch Logs log group
 - AWS CodePipeline pipelines
 - AWS CodeBuild projects
 - Amazon EventBridge event bus policy and rule
 - AWS Identity and Access Management (IAM) role and policy
 - AWS Key Management Service (AWS KMS) key and key policy
 - AWS Service Catalog portfolios, products, and provisioned products
 - Amazon Simple Notification Service (Amazon SNS) topic, topic policy, and subscription
 - Amazon Simple Storage Service (Amazon S3) buckets
 - AWS Systems Manager Parameter Store parameters

For more information about setting up these permissions, see the [CloudFormation documentation](#) and [Implementing policies for least-privilege permissions for AWS CloudFormation](#).

- A GitHub account

Best practices

We recommend that you follow these best practices when setting up the Enterprise Blueprint Factory in your AWS environment:

- When configuring the permissions necessary to deploy the Enterprise Blueprint Factory, follow the principle of least privilege and grant the minimum permissions required. For more information, see [Grant least privilege](#) and [Security best practices](#) in the IAM documentation.
- When configuring access to Service Catalog portfolios, follow the principle of least privilege and grant access only to specific roles, users, or administrators. Follow the [security best practices](#) for Service Catalog.

Creating the repositories

This section helps you set up the [configuration repository](#) and the [product repository](#) for the Enterprise Blueprint Factory. To set up your repositories, you [fork](#) the provided repositories in GitHub. Then, you use AWS CodeConnections to create a [connection](#) to your GitHub repository. Then, you clone the GitHub repositories to your local machine.

To fork the GitHub repositories

1. Log in to [GitHub](#).
2. Navigate to the [Configuration repo](#) GitHub repository.
3. Choose **Fork**.
4. On the **Create a new fork** page, in the **Repository name** box, enter ServiceCatalog-ConfigRepo.
5. (Optional) Enter a description.
6. Select **Copy the main branch only**.
7. Choose **Create fork**.

- Repeat these steps to fork the [Code repo](#) GitHub repository. Enter the name `ServiceCatalog-CodeRepo` for this repository.
- Repeat these steps to fork the [Product repo](#) GitHub repository. Enter the name `ServiceCatalog-BlueprintProductRepo` for this repository.

To create the CodeConnections connection

- In the AWS CLI, enter the following command to create an CodeConnections connection to GitHub:

```
aws codeconnections create-connection --provider-type GitHub --connection-name  
<MyConnection>
```

- Use the AWS Developer Tools console to complete the connection. For more information, see [Update a pending connection](#).

To clone the forked repositories

- Enter the following commands to clone the GitHub repositories to your local workstation:

```
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-config-repo  
ServiceCatalog-ConfigRepo  
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-blueprint-repo  
ServiceCatalog-BlueprintProductRepo  
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-code-repo  
ServiceCatalog-CodeRepo
```

Setting up the Enterprise Blueprint Factory

The instructions in this section describe how to set up the Enterprise Blueprint Factory in your target account. The product repo that you cloned from GitHub contains two sample CloudFormation templates, `BP-S3` and `BP-SNS`. By following these instructions, you deploy these two sample blueprints as products in Service Catalog.

To set up the roles

1. In the Blueprint Developer's account, create the following trust policy, and then save it as `sc-enduserrole-trust-policy.json`:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::account-id:role"
    },
    "Action": "sts:AssumeRole"
  }
}
```

2. Enter the following command to create the `ServiceCatalogEndUserRole` IAM role:

```
aws iam create-role \
--role-name ServiceCatalogEndUserRole \
--assume-role-policy-document file://sc-enduserrole-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess \
-- role-name ServiceCatalogEndUserRole
```

Note

Developers use the `ServiceCatalogEndUserRole` role to provision the Service Catalog product. This role does not need permissions to create the resources defined in the blueprint. This follows the best practices of least privileged permissions and segregation of duties.

3. Create the following trust policy and then save it as `sc-launchconstraintrole-trust-policy.json`:

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



```
    "Service": "servicecatalog.amazonaws.com"
  },
  "Action": "sts:AssumeRole"
}
}
```

4. Enter the following command to create the ServiceCataloglogLaunchConstraintRole IAM role:

```
aws iam create-role \
--role-name ServiceCataloglogLaunchConstraintRole \
--assume-role-policy-document file://sc-launchconstraintrole-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonSNSFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSCloudFormationFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
```

5. Add the following policy to the ServiceCataloglogLaunchConstraintRole IAM role. Include any other permissions that are required for the product resources, as described in [Configuring a Launch Role](#) in the Service Catalog documentation:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
        }
      }
    }
  ]
}
```

Note

Service Catalog uses this role to deploy the CloudFormation stack as a product in Service Catalog. The trust policy for this role makes sure that only Service Catalog can assume it. Other users or services cannot assume this role. This follows the best practice of segregation of duties.

6. Create the following trust policy, and then save it as `sc-codebuild-trust-policy.json`:

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

7. Enter the following command to create the `codebuild-servicecatalog-admin-role` IAM role:

```
aws iam create-role \
--role-name codebuild-servicecatalog-admin-role \
--assume-role-policy-document file://sc-codebuild-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess \
--role-name codebuild-servicecatalog-admin-role
```

Note

The CodeBuild jobs in the config pipeline use this role.

To set up the Amazon S3 bucket

- To create an Amazon Simple Storage Service (Amazon S3) bucket that is used to store the CodePipeline artifacts, follow the instructions in [Creating a bucket](#) in the Amazon S3 documentation. Follow the [Security best practices for Amazon S3](#).

To set up the AWS Systems Manager parameters

- Follow the instructions in [Creating Parameter Store parameters in Systems Manager](#) in order to create the Systems Manager parameters in the following table. These parameters are used in the CloudFormation template that deploys the configuration pipeline.

Parameter name	Type	Description
/blueprints/resources/vpc_id	String	Parameter that stores the ID of the target virtual private cloud (VPC).
/blueprints/resources/subnets	StringList	Parameter that stores the IDs of the target subnets.
/blueprints/resources/securitygroups	StringList	Parameter that stores the IDs of the target security groups.
/blueprints/resources/artifacts-bucket-name	String	Parameter that stores the Amazon S3 bucket name that is used for CodePipeline artifacts.

Parameter name	Type	Description
/blueprints/resources/BlueprintRepo	String	Parameter that stores the GitHub repo where the Enterprise Blueprint Factory blueprints are stored. The default value is <user>/aws-enterprise-blueprint-factory-blueprint-repo .
/blueprints/resources/CodeRepo	String	Parameter that stores the GitHub repo where the Enterprise Blueprint Factory configuration pipeline code and the Bootstrapping-Admin-Product code are stored. The default value is <user>/aws-enterprise-blueprint-factory-code-repo .
/blueprints/resources/ConfigRepo	String	Parameter that stores the GitHub repo where the Enterprise Blueprint Factory configuration files are stored. The default value is <user>/aws-enterprise-blueprint-factory-config-repo .

To update the CloudFormation templates

1. In the code repository (ServiceCatalog-CodeRepo), open the **ServiceCatalog-Pipeline.yml** file.
2. Edit the default values for the following parameters in this file:

- `ConfigRepositoryName` is the Systems Manager parameter that stores the GitHub repo where the Enterprise Blueprint Factory configuration files are stored. The default value is `/blueprints/resources/ConfigRepo`.
 - `CodeRepositoryName` is the Systems Manager parameter that stores the GitHub repo where the Enterprise Blueprint Factory configuration pipeline code and the `Bootstrapping-Admin-Product` code are stored. The default value is `/blueprints/resources/CodeRepo`.
 - `BlueprintRepositoryName` is the Systems Manager parameter that stores the GitHub repo where the Enterprise Blueprint Factory blueprints are stored. The default value is `/blueprints/resources/BlueprintRepo`.
 - `BranchName` is the branch of the config repository where the config file is stored. The default value is `main`.
 - `VPCID` is the Systems Manager parameter that stores the ID of the target VPC. The default value is `/blueprints/resources/vpc_id`.
 - `Subnets` is the Systems Manager parameter that stores the IDs of the target subnets. The default value is `/blueprints/resources/subnets`.
 - `SecurityGroupIds` is the Systems Manager parameter that stores the IDs of the target security groups. The default value is `/blueprints/resources/securitygroups`.
 - `IamRoleName` is the name of the IAM role that the CodeBuild jobs use. The default value is `codebuild-servicecatalog-admin-role`.
 - `EnvironmentType` is the environment where you are deploying the Enterprise Blueprint Factory. The default value is `DEV`.
 - `ArtifactBucket` is the Systems Manager parameter that stores the Amazon S3 bucket where CodePipeline stores artifacts. The default value is `/blueprints/resources/artifacts-bucket-name`.
 - `CodeConnectionArn` is the Amazon Resource Name (ARN) of the CodeConnections connection to GitHub.
3. Save and close the **ServiceCatalog-Pipeline.yml** file.
 4. Enter the following commands to merge the changes into the code repository:

```
cd ServiceCatalog-CodeRepo
git add ServiceCatalog-Pipeline.yml
git commit -m "<description of change>"
```

```
git push origin main
```

5. In the configuration repository (ServiceCatalog-ConfigRepo), open the **bp_config.yml** file.
6. Update the values in the portfolio section as needed for your organization. For example, update the `portfolio_access_roles` and `share_to_ou` attributes. For more information, see [Configuration file](#) in this guide.
7. Save and close the **bp_config.yml** file.
8. Enter the following commands to merge the changes into the code repository:

```
cd ServiceCatalog-ConfigRepo
git add bp_config.yml
git commit -m "<description of change>"
git push origin main
```

To deploy the CloudFormation stack

1. Sign in to the Enterprise Blueprint Factory administrative account.
2. Switch to an IAM role that has [administrative permissions](#).
3. Open the [CloudFormation console](#).
4. On the navigation bar at the top of the screen, choose the target AWS Region.
5. On the **Stacks** page, choose **Create stack** at top right, and then choose **With new resources (standard)**.
6. For **Prepare template**, choose **Template is ready**.
7. Under **Specify template**, choose **Upload a template file**.
8. Choose **Choose File**, navigate to the ServiceCatalog-CodeRepo folder, and then choose **ServiceCatalog-Pipeline.yml**.
9. Choose **Next** to continue and to validate the template.
10. For **Stack name**, enter a name for the stack.
11. In the **Parameters** section, do not change the default values.
12. Choose **Next**.
13. On the **Configure stack options** page, do not change the default values, and then choose **Next**.

14. On the **Review and create** page, verify the template and stack details, and then choose **Submit**.
15. Monitor the progress of the stack deployment. For more information, see the [CloudFormation documentation](#).
16. Wait for the status to change to CREATE_COMPLETE.

To validate the deployment

1. Open the [AWS Service Catalog console](#).
2. In the navigation pane, choose **Products**.
3. Confirm that **ServiceCatalog-Pipeline** is available in the list of products.
4. Open the [AWS CodePipeline console](#).
5. In **Name**, choose the configuration pipeline. By default, the pipeline name is ServiceCatalog-Pipeline.
6. Choose **View history**.
7. View the status of the pipeline and stage execution. For more information about the status, see [View execution status](#) in the CodePipeline documentation.
8. Wait until the configuration pipeline status is Succeeded.
9. Open the [Service Catalog console](#).
10. In the navigation pane, choose **Products**.
11. Confirm that the **BP-S3-Product** and **BP-SNS-Product** products are available. This indicates that the product release pipelines for the sample blueprints completed successfully.
12. If you want to delete the sample blueprints that you deployed when setting up the Enterprise Blueprint Factory, follow the instructions in [Deleting a blueprint](#).

Delete the Enterprise Blueprint Factory

If you are not using the Enterprise Blueprint Factory, you can delete it to stop incurring the costs associated with its AWS resources.

To delete the resources

1. Enter the following commands to delete the IAM roles that were deployed in the Enterprise Blueprint Factory administrative account:

```
aws iam detach-role-policy \  
--policy-arn arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess \  
--role-name ServiceCatalogEndUserRole  
aws iam delete-role --role-name ServiceCatalogEndUserRole  
aws iam detach-role-policy \  
--policy-arn arn:aws:iam::aws:policy/AmazonSNSFullAccess \  
--role-name ServiceCataloglogLaunchConstraintRole  
aws iam delete-role --role-name ServiceCataloglogLaunchConstraintRole
```

2. Delete the CloudFormation stack for the Enterprise Blueprint Factory. For instructions, see [Delete a stack from the CloudFormation console](#) or [Delete a stack from the AWS CLI](#).
3. Delete the Amazon S3 bucket that is used to store the CodePipeline artifacts. For instructions, see [Deleting a bucket](#) in the Amazon S3 documentation.
4. Delete the following Systems Manager parameters from Parameter Store:
 - /blueprints/resources/vpc_id
 - /blueprints/resources/subnets
 - /blueprints/resources/securitygroups
 - /blueprints/resources/artifacts-bucket-name
 - /blueprints/resources/BlueprintRepo
 - /blueprints/resources/CodeRepo
 - /blueprints/resources/ConfigRepo

For instructions, see [Deleting parameters from Parameter Store](#) in the Systems Manager documentation.

Using the Enterprise Blueprint Factory

This section helps you create, update, or delete blueprints in your environment. It provides detailed instructions for managing a blueprint throughout its [life cycle](#).

To create or update custom blueprints, you must have an understanding of how to create IaC templates, such as AWS CloudFormation [templates](#) or AWS Cloud Development Kit (AWS CDK) [constructs](#). This guide does not include information or instructions about how to define the blueprints that you release through the Enterprise Blueprint Factory.

Prerequisites

The following are the prerequisites for using the Enterprise Blueprint Factory in your AWS environment:

- AWS Command Line Interface (AWS CLI), [installed](#) and [configured](#)
- Permissions to assume the `ServiceCatalogEndUserRole` AWS Identity and Access Management (IAM) role
- An CloudFormation template or AWS CDK construct

Creating a blueprint

The Enterprise Blueprint Factory pipelines deploy the blueprints that you define in the configuration file. The developer initiates the configuration pipeline by merging the configuration file into the configuration repository. Then, the Enterprise Blueprint Factory uses the `ServiceCatalogLaunchConstraintRole` to deploy the blueprint as a product in Service Catalog. For more information about the actions that the configuration pipeline and release pipeline perform when you create a blueprint, see [Blueprint creation](#) in this guide.

To add the blueprint to the product repository

1. Make sure that you have set up your Enterprise Blueprint Factory according to the instructions in [Setting up the Enterprise Blueprint Factory](#) in this guide.
2. Confirm that the policy for the `ServiceCatalogLogLaunchConstraintRole` role allows you to provision the resources defined in the blueprint.

3. In the product repository (ServiceCatalog-BlueprintProductRepo), create a folder for the new blueprint.
4. Paste the IaC template (CloudFormation template or AWS CDK construct) into the folder that you created.
5. Create a file named **product_config.json** in the folder that you created.
6. Open the **product_config.json** file, and paste the following into the file:

```
{
  "SchemaVersion": "1.0",
  "ProductVersionName": "1.0.1",
  "Deprecated_Versions" : [],
  "ProductVersionDescription": "<description>",
  "ProductType": "CLOUD_FORMATION_TEMPLATE",
  "Properties": {
    "TemplateFilePath": "./<folder name>/<file name>"
  }
}
```

Where:

- <description> is a brief description of the blueprint version
- <folder name> is the name of the folder you created in the product repository
- <file name> is the name of the IaC template

 **Note**

You can update the schema version or product version names to match your organization's policies.

7. Save and close the **product_config.json** file.
8. Enter the following commands to merge the changes into the product repository:

```
cd ServiceCatalog-BlueprintProductRepo
git add <folder name>/<file name> <folder name>\product_config.json
git commit -m "The first version of <file name> blueprint"
git push origin main
```

To update the configuration file

1. In the configuration repository (ServiceCatalog-ConfigRepo), open the **config.yml** file.
2. Edit the **portfolios** section and **products** section as needed for the new blueprint. For more information, see [Configuration file](#) in this guide.
3. Save and close the **config.yml** file.
4. Enter the following commands to merge the changes into the configuration repository:

```
cd ServiceCatalog-ConfigRepo
git add config.yml
git commit -m "<description of change>"
git push origin main
```

Approval of this pull request initiates the configuration pipeline. The configuration pipeline creates a release pipeline for the product.

To review the deployment logs

1. Sign in to the Enterprise Blueprint Factory administrative account.
2. Open the [AWS CodePipeline console](#).
3. In **Name**, choose the release pipeline for the product. By default, the pipeline name is `Blueprint_<Product-Name>-<CloudFormation-Stack-Name>`.
4. Choose **View history**.
5. View the status of the pipeline and stage execution. For more information about the status, see [View execution status](#) in the CodePipeline documentation.
6. If the pipeline fails, review the cause of the failure. For instructions about how to configure monitoring for your pipelines, see [Monitoring pipelines](#) in the CodePipeline documentation. If the release pipeline failed due to a `cfn-lint` or `cfn_nag` check, correct the error in the template. Submit another pull request to the product repo. This restarts the release pipeline. For more information about correcting template errors, see the [Troubleshooting](#) section in this guide.
7. Wait until the release pipeline status is Succeeded.

To validate the deployment

1. Sign in to a consumer account in the organization.

2. Assume the `ServiceCatalogEndUserRole` IAM role.
3. Open the [Service Catalog console](#).
4. In the navigation pane, choose **Products**.
5. Confirm that the new product is available in the list of products.

Updating a blueprint

For more information about the actions that the configuration pipeline and release pipeline perform when you create a blueprint, see [Blueprint update](#) in this guide.

To update a blueprint

1. In the product repository, navigate into the folder for the product.
2. Paste the updated IaC template. Make sure that the file name is the same as the previous version.
3. Open the **product_config.json** file.
4. For `ProductVersionName`, update the version number.
5. If you want to prevent the previous product version from being deployed in future, for `Deprecated_Versions`, enter the previous version numbers in a comma-separated list.
6. Enter the following commands to merge the changes into the product repository:

```
cd ServiceCatalog-BlueprintProductRepo
git add <folder name>/<file name> <folder name>\product_config.json
git commit -m "Version <number> of <file name> blueprint"
git push origin main
```

Approval of this pull request initiates the release pipeline for the product.

To review the deployment logs

1. Sign in to the Enterprise Blueprint Factory administrative account.
2. Open the [AWS CodePipeline console](#).
3. In **Name**, choose the release pipeline. By default, the pipeline name is `Blueprint_<Product-Name>-<CloudFormation-Stack-Name>`.
4. Choose **View history**.

5. View the status of the pipeline and stage execution. For more information about the status, see [View execution status](#) in the CodePipeline documentation.
6. If the pipeline fails, review the cause of the failure. For instructions about how to configure monitoring for your pipelines, see [Monitoring pipelines](#) in the CodePipeline documentation. If the release pipeline failed due to a cfn-lint or cfn_nag check, correct the error in the template. Submit another pull request to the product repo. This restarts the release pipeline. For more information about correcting template errors, see the [Troubleshooting](#) section in this guide.
7. Wait until the release pipeline status is Succeeded.

To validate the update

1. Sign in to a consumer account in the organization.
2. Assume the `ServiceCatalogEndUserRole` IAM role.
3. Open the [Service Catalog console](#).
4. In the navigation pane, choose **Products**.
5. Confirm that the new product version is available in the list of products.

Deleting a blueprint

When you delete a product, Service Catalog removes all of product versions from every portfolio that contains the product. For more information, see [Deleting products](#) in the Service Catalog documentation. For more information about the actions that the configuration pipeline and release pipeline perform when you create a blueprint, see [Blueprint deletion](#) in this guide.

To delete a blueprint

1. In the configuration repository, open the **config.yml** file.
2. Edit the products section, remove or comment out the product you want to delete.
3. Save and close the **config.yml** file.
4. Enter the following commands to merge the changes into the configuration repository:

```
cd ServiceCatalog-ConfigRepo
git add config.yml
git commit -m "<description of change>"
git push origin main
```

Approval of this pull request initiates the configuration pipeline. The configuration pipeline deletes the product and its release pipeline.

5. In the product repository, delete the folder for the product, including its contents.
6. Enter the following commands to merge the changes into the product repository:

```
cd ServiceCatalog-BlueprintProductRepo
git add .
git commit -m "Delete <file name> blueprint"
git push origin main
```

To validate the deletion

1. Sign in to a consumer account in the organization.
2. Assume the `ServiceCatalogEndUserRole` IAM role.
3. Open the [Service Catalog console](#).
4. In the navigation pane, choose **Products**.
5. Confirm that the deleted product is no longer available.

Troubleshooting

When you create or update a blueprint, the `cfn-lint` and `cfn-nag` tools validate the blueprint. For more information about validation in the release pipeline, see [Release pipeline](#) in this guide. Any reported syntax or security errors cause the pipeline to fail. To successfully deploy the blueprint through the release pipeline, you must correct the errors in the blueprint.

The following is an example output that shows two security-related errors, a failure and a warning.

```
BP-SNS.yml
-----
BP-SNS.yml
-----
| WARN W47
|
| Resource: ["ExampleTopic"]
| Line numbers: [5]
|
```

```
| SNS Topic should specify KmsMasterKeyId property
-----
| FAIL F18
|
| Resource: ["ExampleTopicPolicy"]
| Line numbers: [10]
|
| SNS topic policy should not allow * principal

Failures count: 1
Warnings count: 1
```

To correct these errors, in the blueprint file, you would replace the `*` principal in the Amazon Simple Notification Service (Amazon SNS) topic policy and associate an AWS Key Management Service (AWS KMS) key with the topic. The following code example demonstrates these updates.

```
ExampleTopic:
  Type: AWS::SNS::Topic
  Properties:
    TopicName: ExampleTopic
ExampleTopicPolicy:
  Type: AWS::SNS::TopicPolicy
  Properties:
    KmsMasterKeyId: alias/aws/sns # Added KMS key
    PolicyDocument:
      Id: Id1
      Version: '2012-10-17'
      Statement:
        - Sid: Sid2
          Effect: Allow
          Principal:
            "Service" : "s3.amazonaws.com" # Replaced "AWS": '*'
          Action: 'sns:Publish'
          Resource: !Ref ExampleTopic
  Topics:
    - !Ref ExampleTopic
```

Related resources

AWS documentation

- [Tutorial: Create a pipeline that deploys to Service Catalog](#) (AWS CodePipeline documentation)
- [AWS CodePipeline documentation](#)
- [AWS CodeBuild documentation](#)
- [AWS Service Catalog Administrator Guide](#)
- [AWS Service Catalog User Guide](#)

AWS blog posts

- [Report and Visualize your AWS Service Catalog Estate](#) (AWS blog post)
- [Implementing an alarm to automatically detect drift in AWS CloudFormation stacks](#) (AWS blog post)

Contributors

The following individuals contributed to this guide.

Authoring

- Haofei Feng, Senior Cloud Architect, AWS
- Cam Maxwell, Principal Security Advisor, AWS
- Joe Guo, Cloud Support Engineer, AWS
- Shreejesh MV, Senior Cloud Architect, AWS

Reviewing

- Joseph Dominic, Cloud Architect, AWS
- Naresh Rajaram, Consulting Partner Solutions Architect, AWS

Technical writing

- Lilly AbouHarb, Senior Technical Writer, AWS

Document history

The following table describes significant changes to this guide. If you want to be notified about future updates, you can subscribe to an [RSS feed](#).

Change	Description	Date
Initial publication	—	October 10, 2024

AWS Prescriptive Guidance glossary

The following are commonly used terms in strategies, guides, and patterns provided by AWS Prescriptive Guidance. To suggest entries, please use the **Provide feedback** link at the end of the glossary.

Numbers

7 Rs

Seven common migration strategies for moving applications to the cloud. These strategies build upon the 5 Rs that Gartner identified in 2011 and consist of the following:

- **Refactor/re-architect** – Move an application and modify its architecture by taking full advantage of cloud-native features to improve agility, performance, and scalability. This typically involves porting the operating system and database. Example: Migrate your on-premises Oracle database to the Amazon Aurora PostgreSQL-Compatible Edition.
- **Replatform (lift and reshape)** – Move an application to the cloud, and introduce some level of optimization to take advantage of cloud capabilities. Example: Migrate your on-premises Oracle database to Amazon Relational Database Service (Amazon RDS) for Oracle in the AWS Cloud.
- **Repurchase (drop and shop)** – Switch to a different product, typically by moving from a traditional license to a SaaS model. Example: Migrate your customer relationship management (CRM) system to Salesforce.com.
- **Rehost (lift and shift)** – Move an application to the cloud without making any changes to take advantage of cloud capabilities. Example: Migrate your on-premises Oracle database to Oracle on an EC2 instance in the AWS Cloud.
- **Relocate (hypervisor-level lift and shift)** – Move infrastructure to the cloud without purchasing new hardware, rewriting applications, or modifying your existing operations. You migrate servers from an on-premises platform to a cloud service for the same platform. Example: Migrate a Microsoft Hyper-V application to AWS.
- **Retain (revisit)** – Keep applications in your source environment. These might include applications that require major refactoring, and you want to postpone that work until a later time, and legacy applications that you want to retain, because there's no business justification for migrating them.

- **Retire** – Decommission or remove applications that are no longer needed in your source environment.

A

ABAC

See [attribute-based access control](#).

abstracted services

See [managed services](#).

ACID

See [atomicity, consistency, isolation, durability](#).

active-active migration

A database migration method in which the source and target databases are kept in sync (by using a bidirectional replication tool or dual write operations), and both databases handle transactions from connecting applications during migration. This method supports migration in small, controlled batches instead of requiring a one-time cutover. It's more flexible but requires more work than [active-passive migration](#).

active-passive migration

A database migration method in which the source and target databases are kept in sync, but only the source database handles transactions from connecting applications while data is replicated to the target database. The target database doesn't accept any transactions during migration.

aggregate function

A SQL function that operates on a group of rows and calculates a single return value for the group. Examples of aggregate functions include SUM and MAX.

AI

See [artificial intelligence](#).

AIOps

See [artificial intelligence operations](#).

anonymization

The process of permanently deleting personal information in a dataset. Anonymization can help protect personal privacy. Anonymized data is no longer considered to be personal data.

anti-pattern

A frequently used solution for a recurring issue where the solution is counter-productive, ineffective, or less effective than an alternative.

application control

A security approach that allows the use of only approved applications in order to help protect a system from malware.

application portfolio

A collection of detailed information about each application used by an organization, including the cost to build and maintain the application, and its business value. This information is key to [the portfolio discovery and analysis process](#) and helps identify and prioritize the applications to be migrated, modernized, and optimized.

artificial intelligence (AI)

The field of computer science that is dedicated to using computing technologies to perform cognitive functions that are typically associated with humans, such as learning, solving problems, and recognizing patterns. For more information, see [What is Artificial Intelligence?](#)

artificial intelligence operations (AIOps)

The process of using machine learning techniques to solve operational problems, reduce operational incidents and human intervention, and increase service quality. For more information about how AIOps is used in the AWS migration strategy, see the [operations integration guide](#).

asymmetric encryption

An encryption algorithm that uses a pair of keys, a public key for encryption and a private key for decryption. You can share the public key because it isn't used for decryption, but access to the private key should be highly restricted.

atomicity, consistency, isolation, durability (ACID)

A set of software properties that guarantee the data validity and operational reliability of a database, even in the case of errors, power failures, or other problems.

attribute-based access control (ABAC)

The practice of creating fine-grained permissions based on user attributes, such as department, job role, and team name. For more information, see [ABAC for AWS](#) in the AWS Identity and Access Management (IAM) documentation.

authoritative data source

A location where you store the primary version of data, which is considered to be the most reliable source of information. You can copy data from the authoritative data source to other locations for the purposes of processing or modifying the data, such as anonymizing, redacting, or pseudonymizing it.

Availability Zone

A distinct location within an AWS Region that is insulated from failures in other Availability Zones and provides inexpensive, low-latency network connectivity to other Availability Zones in the same Region.

AWS Cloud Adoption Framework (AWS CAF)

A framework of guidelines and best practices from AWS to help organizations develop an efficient and effective plan to move successfully to the cloud. AWS CAF organizes guidance into six focus areas called perspectives: business, people, governance, platform, security, and operations. The business, people, and governance perspectives focus on business skills and processes; the platform, security, and operations perspectives focus on technical skills and processes. For example, the people perspective targets stakeholders who handle human resources (HR), staffing functions, and people management. For this perspective, AWS CAF provides guidance for people development, training, and communications to help ready the organization for successful cloud adoption. For more information, see the [AWS CAF website](#) and the [AWS CAF whitepaper](#).

AWS Workload Qualification Framework (AWS WQF)

A tool that evaluates database migration workloads, recommends migration strategies, and provides work estimates. AWS WQF is included with AWS Schema Conversion Tool (AWS SCT). It analyzes database schemas and code objects, application code, dependencies, and performance characteristics, and provides assessment reports.

B

bad bot

A [bot](#) that is intended to disrupt or cause harm to individuals or organizations.

BCP

See [business continuity planning](#).

behavior graph

A unified, interactive view of resource behavior and interactions over time. You can use a behavior graph with Amazon Detective to examine failed logon attempts, suspicious API calls, and similar actions. For more information, see [Data in a behavior graph](#) in the Detective documentation.

big-endian system

A system that stores the most significant byte first. See also [endianness](#).

binary classification

A process that predicts a binary outcome (one of two possible classes). For example, your ML model might need to predict problems such as "Is this email spam or not spam?" or "Is this product a book or a car?"

bloom filter

A probabilistic, memory-efficient data structure that is used to test whether an element is a member of a set.

blue/green deployment

A deployment strategy where you create two separate but identical environments. You run the current application version in one environment (blue) and the new application version in the other environment (green). This strategy helps you quickly roll back with minimal impact.

bot

A software application that runs automated tasks over the internet and simulates human activity or interaction. Some bots are useful or beneficial, such as web crawlers that index information on the internet. Some other bots, known as *bad bots*, are intended to disrupt or cause harm to individuals or organizations.

botnet

Networks of [bots](#) that are infected by [malware](#) and are under the control of a single party, known as a *bot herder* or *bot operator*. Botnets are the best-known mechanism to scale bots and their impact.

branch

A contained area of a code repository. The first branch created in a repository is the *main branch*. You can create a new branch from an existing branch, and you can then develop features or fix bugs in the new branch. A branch you create to build a feature is commonly referred to as a *feature branch*. When the feature is ready for release, you merge the feature branch back into the main branch. For more information, see [About branches](#) (GitHub documentation).

break-glass access

In exceptional circumstances and through an approved process, a quick means for a user to gain access to an AWS account that they don't typically have permissions to access. For more information, see the [Implement break-glass procedures](#) indicator in the AWS Well-Architected guidance.

brownfield strategy

The existing infrastructure in your environment. When adopting a brownfield strategy for a system architecture, you design the architecture around the constraints of the current systems and infrastructure. If you are expanding the existing infrastructure, you might blend brownfield and [greenfield](#) strategies.

buffer cache

The memory area where the most frequently accessed data is stored.

business capability

What a business does to generate value (for example, sales, customer service, or marketing). Microservices architectures and development decisions can be driven by business capabilities. For more information, see the [Organized around business capabilities](#) section of the [Running containerized microservices on AWS](#) whitepaper.

business continuity planning (BCP)

A plan that addresses the potential impact of a disruptive event, such as a large-scale migration, on operations and enables a business to resume operations quickly.

C

CAF

See [AWS Cloud Adoption Framework](#).

canary deployment

The slow and incremental release of a version to end users. When you are confident, you deploy the new version and replace the current version in its entirety.

CCoE

See [Cloud Center of Excellence](#).

CDC

See [change data capture](#).

change data capture (CDC)

The process of tracking changes to a data source, such as a database table, and recording metadata about the change. You can use CDC for various purposes, such as auditing or replicating changes in a target system to maintain synchronization.

chaos engineering

Intentionally introducing failures or disruptive events to test a system's resilience. You can use [AWS Fault Injection Service \(AWS FIS\)](#) to perform experiments that stress your AWS workloads and evaluate their response.

CI/CD

See [continuous integration and continuous delivery](#).

classification

A categorization process that helps generate predictions. ML models for classification problems predict a discrete value. Discrete values are always distinct from one another. For example, a model might need to evaluate whether or not there is a car in an image.

client-side encryption

Encryption of data locally, before the target AWS service receives it.

Cloud Center of Excellence (CCoE)

A multi-disciplinary team that drives cloud adoption efforts across an organization, including developing cloud best practices, mobilizing resources, establishing migration timelines, and leading the organization through large-scale transformations. For more information, see the [CCoE posts](#) on the AWS Cloud Enterprise Strategy Blog.

cloud computing

The cloud technology that is typically used for remote data storage and IoT device management. Cloud computing is commonly connected to [edge computing](#) technology.

cloud operating model

In an IT organization, the operating model that is used to build, mature, and optimize one or more cloud environments. For more information, see [Building your Cloud Operating Model](#).

cloud stages of adoption

The four phases that organizations typically go through when they migrate to the AWS Cloud:

- Project – Running a few cloud-related projects for proof of concept and learning purposes
- Foundation – Making foundational investments to scale your cloud adoption (e.g., creating a landing zone, defining a CCoE, establishing an operations model)
- Migration – Migrating individual applications
- Re-invention – Optimizing products and services, and innovating in the cloud

These stages were defined by Stephen Orban in the blog post [The Journey Toward Cloud-First & the Stages of Adoption](#) on the AWS Cloud Enterprise Strategy blog. For information about how they relate to the AWS migration strategy, see the [migration readiness guide](#).

CMDB

See [configuration management database](#).

code repository

A location where source code and other assets, such as documentation, samples, and scripts, are stored and updated through version control processes. Common cloud repositories include GitHub or Bitbucket Cloud. Each version of the code is called a *branch*. In a microservice structure, each repository is devoted to a single piece of functionality. A single CI/CD pipeline can use multiple repositories.

cold cache

A buffer cache that is empty, not well populated, or contains stale or irrelevant data. This affects performance because the database instance must read from the main memory or disk, which is slower than reading from the buffer cache.

cold data

Data that is rarely accessed and is typically historical. When querying this kind of data, slow queries are typically acceptable. Moving this data to lower-performing and less expensive storage tiers or classes can reduce costs.

computer vision (CV)

A field of [AI](#) that uses machine learning to analyze and extract information from visual formats such as digital images and videos. For example, AWS Panorama offers devices that add CV to on-premises camera networks, and Amazon SageMaker AI provides image processing algorithms for CV.

configuration drift

For a workload, a configuration change from the expected state. It might cause the workload to become noncompliant, and it's typically gradual and unintentional.

configuration management database (CMDB)

A repository that stores and manages information about a database and its IT environment, including both hardware and software components and their configurations. You typically use data from a CMDB in the portfolio discovery and analysis stage of migration.

conformance pack

A collection of AWS Config rules and remediation actions that you can assemble to customize your compliance and security checks. You can deploy a conformance pack as a single entity in an AWS account and Region, or across an organization, by using a YAML template. For more information, see [Conformance packs](#) in the AWS Config documentation.

continuous integration and continuous delivery (CI/CD)

The process of automating the source, build, test, staging, and production stages of the software release process. CI/CD is commonly described as a pipeline. CI/CD can help you automate processes, improve productivity, improve code quality, and deliver faster. For more information, see [Benefits of continuous delivery](#). CD can also stand for *continuous deployment*. For more information, see [Continuous Delivery vs. Continuous Deployment](#).

CV

See [computer vision](#).

D

data at rest

Data that is stationary in your network, such as data that is in storage.

data classification

A process for identifying and categorizing the data in your network based on its criticality and sensitivity. It is a critical component of any cybersecurity risk management strategy because it helps you determine the appropriate protection and retention controls for the data. Data classification is a component of the security pillar in the AWS Well-Architected Framework. For more information, see [Data classification](#).

data drift

A meaningful variation between the production data and the data that was used to train an ML model, or a meaningful change in the input data over time. Data drift can reduce the overall quality, accuracy, and fairness in ML model predictions.

data in transit

Data that is actively moving through your network, such as between network resources.

data mesh

An architectural framework that provides distributed, decentralized data ownership with centralized management and governance.

data minimization

The principle of collecting and processing only the data that is strictly necessary. Practicing data minimization in the AWS Cloud can reduce privacy risks, costs, and your analytics carbon footprint.

data perimeter

A set of preventive guardrails in your AWS environment that help make sure that only trusted identities are accessing trusted resources from expected networks. For more information, see [Building a data perimeter on AWS](#).

data preprocessing

To transform raw data into a format that is easily parsed by your ML model. Preprocessing data can mean removing certain columns or rows and addressing missing, inconsistent, or duplicate values.

data provenance

The process of tracking the origin and history of data throughout its lifecycle, such as how the data was generated, transmitted, and stored.

data subject

An individual whose data is being collected and processed.

data warehouse

A data management system that supports business intelligence, such as analytics. Data warehouses commonly contain large amounts of historical data, and they are typically used for queries and analysis.

database definition language (DDL)

Statements or commands for creating or modifying the structure of tables and objects in a database.

database manipulation language (DML)

Statements or commands for modifying (inserting, updating, and deleting) information in a database.

DDL

See [database definition language](#).

deep ensemble

To combine multiple deep learning models for prediction. You can use deep ensembles to obtain a more accurate prediction or for estimating uncertainty in predictions.

deep learning

An ML subfield that uses multiple layers of artificial neural networks to identify mapping between input data and target variables of interest.

defense-in-depth

An information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout a computer network to protect the confidentiality, integrity, and availability of the network and the data within. When you adopt this strategy on AWS, you add multiple controls at different layers of the AWS Organizations structure to help secure resources. For example, a defense-in-depth approach might combine multi-factor authentication, network segmentation, and encryption.

delegated administrator

In AWS Organizations, a compatible service can register an AWS member account to administer the organization's accounts and manage permissions for that service. This account is called the *delegated administrator* for that service. For more information and a list of compatible services, see [Services that work with AWS Organizations](#) in the AWS Organizations documentation.

deployment

The process of making an application, new features, or code fixes available in the target environment. Deployment involves implementing changes in a code base and then building and running that code base in the application's environments.

development environment

See [environment](#).

detective control

A security control that is designed to detect, log, and alert after an event has occurred. These controls are a second line of defense, alerting you to security events that bypassed the preventative controls in place. For more information, see [Detective controls](#) in *Implementing security controls on AWS*.

development value stream mapping (DVSM)

A process used to identify and prioritize constraints that adversely affect speed and quality in a software development lifecycle. DVSM extends the value stream mapping process originally designed for lean manufacturing practices. It focuses on the steps and teams required to create and move value through the software development process.

digital twin

A virtual representation of a real-world system, such as a building, factory, industrial equipment, or production line. Digital twins support predictive maintenance, remote monitoring, and production optimization.

dimension table

In a [star schema](#), a smaller table that contains data attributes about quantitative data in a fact table. Dimension table attributes are typically text fields or discrete numbers that behave like text. These attributes are commonly used for query constraining, filtering, and result set labeling.

disaster

An event that prevents a workload or system from fulfilling its business objectives in its primary deployed location. These events can be natural disasters, technical failures, or the result of human actions, such as unintentional misconfiguration or a malware attack.

disaster recovery (DR)

The strategy and process you use to minimize downtime and data loss caused by a [disaster](#). For more information, see [Disaster Recovery of Workloads on AWS: Recovery in the Cloud](#) in the AWS Well-Architected Framework.

DML

See [database manipulation language](#).

domain-driven design

An approach to developing a complex software system by connecting its components to evolving domains, or core business goals, that each component serves. This concept was introduced by Eric Evans in his book, *Domain-Driven Design: Tackling Complexity in the Heart of Software* (Boston: Addison-Wesley Professional, 2003). For information about how you can use domain-driven design with the strangler fig pattern, see [Modernizing legacy Microsoft ASP.NET \(ASMX\) web services incrementally by using containers and Amazon API Gateway](#).

DR

See [disaster recovery](#).

drift detection

Tracking deviations from a baselined configuration. For example, you can use AWS CloudFormation to [detect drift in system resources](#), or you can use AWS Control Tower to [detect changes in your landing zone](#) that might affect compliance with governance requirements.

DVSM

See [development value stream mapping](#).

E

EDA

See [exploratory data analysis](#).

EDI

See [electronic data interchange](#).

edge computing

The technology that increases the computing power for smart devices at the edges of an IoT network. When compared with [cloud computing](#), edge computing can reduce communication latency and improve response time.

electronic data interchange (EDI)

The automated exchange of business documents between organizations. For more information, see [What is Electronic Data Interchange](#).

encryption

A computing process that transforms plaintext data, which is human-readable, into ciphertext.

encryption key

A cryptographic string of randomized bits that is generated by an encryption algorithm. Keys can vary in length, and each key is designed to be unpredictable and unique.

endianness

The order in which bytes are stored in computer memory. Big-endian systems store the most significant byte first. Little-endian systems store the least significant byte first.

endpoint

See [service endpoint](#).

endpoint service

A service that you can host in a virtual private cloud (VPC) to share with other users. You can create an endpoint service with AWS PrivateLink and grant permissions to other AWS accounts or to AWS Identity and Access Management (IAM) principals. These accounts or principals can connect to your endpoint service privately by creating interface VPC endpoints. For more information, see [Create an endpoint service](#) in the Amazon Virtual Private Cloud (Amazon VPC) documentation.

enterprise resource planning (ERP)

A system that automates and manages key business processes (such as accounting, [MES](#), and project management) for an enterprise.

envelope encryption

The process of encrypting an encryption key with another encryption key. For more information, see [Envelope encryption](#) in the AWS Key Management Service (AWS KMS) documentation.

environment

An instance of a running application. The following are common types of environments in cloud computing:

- development environment – An instance of a running application that is available only to the core team responsible for maintaining the application. Development environments are used to test changes before promoting them to upper environments. This type of environment is sometimes referred to as a *test environment*.
- lower environments – All development environments for an application, such as those used for initial builds and tests.
- production environment – An instance of a running application that end users can access. In a CI/CD pipeline, the production environment is the last deployment environment.
- upper environments – All environments that can be accessed by users other than the core development team. This can include a production environment, preproduction environments, and environments for user acceptance testing.

epic

In agile methodologies, functional categories that help organize and prioritize your work. Epics provide a high-level description of requirements and implementation tasks. For example, AWS CAF security epics include identity and access management, detective controls, infrastructure security, data protection, and incident response. For more information about epics in the AWS migration strategy, see the [program implementation guide](#).

ERP

See [enterprise resource planning](#).

exploratory data analysis (EDA)

The process of analyzing a dataset to understand its main characteristics. You collect or aggregate data and then perform initial investigations to find patterns, detect anomalies, and check assumptions. EDA is performed by calculating summary statistics and creating data visualizations.

F

fact table

The central table in a [star schema](#). It stores quantitative data about business operations. Typically, a fact table contains two types of columns: those that contain measures and those that contain a foreign key to a dimension table.

fail fast

A philosophy that uses frequent and incremental testing to reduce the development lifecycle. It is a critical part of an agile approach.

fault isolation boundary

In the AWS Cloud, a boundary such as an Availability Zone, AWS Region, control plane, or data plane that limits the effect of a failure and helps improve the resilience of workloads. For more information, see [AWS Fault Isolation Boundaries](#).

feature branch

See [branch](#).

features

The input data that you use to make a prediction. For example, in a manufacturing context, features could be images that are periodically captured from the manufacturing line.

feature importance

How significant a feature is for a model's predictions. This is usually expressed as a numerical score that can be calculated through various techniques, such as Shapley Additive Explanations (SHAP) and integrated gradients. For more information, see [Machine learning model interpretability with AWS](#).

feature transformation

To optimize data for the ML process, including enriching data with additional sources, scaling values, or extracting multiple sets of information from a single data field. This enables the ML model to benefit from the data. For example, if you break down the "2021-05-27 00:15:37" date into "2021", "May", "Thu", and "15", you can help the learning algorithm learn nuanced patterns associated with different data components.

few-shot prompting

Providing an [LLM](#) with a small number of examples that demonstrate the task and desired output before asking it to perform a similar task. This technique is an application of in-context learning, where models learn from examples (*shots*) that are embedded in prompts. Few-shot prompting can be effective for tasks that require specific formatting, reasoning, or domain knowledge. See also [zero-shot prompting](#).

FGAC

See [fine-grained access control](#).

fine-grained access control (FGAC)

The use of multiple conditions to allow or deny an access request.

flash-cut migration

A database migration method that uses continuous data replication through [change data capture](#) to migrate data in the shortest time possible, instead of using a phased approach. The objective is to keep downtime to a minimum.

FM

See [foundation model](#).

foundation model (FM)

A large deep-learning neural network that has been training on massive datasets of generalized and unlabeled data. FMs are capable of performing a wide variety of general tasks, such as understanding language, generating text and images, and conversing in natural language. For more information, see [What are Foundation Models](#).

G

generative AI

A subset of [AI](#) models that have been trained on large amounts of data and that can use a simple text prompt to create new content and artifacts, such as images, videos, text, and audio. For more information, see [What is Generative AI](#).

geo blocking

See [geographic restrictions](#).

geographic restrictions (geo blocking)

In Amazon CloudFront, an option to prevent users in specific countries from accessing content distributions. You can use an allow list or block list to specify approved and banned countries. For more information, see [Restricting the geographic distribution of your content](#) in the CloudFront documentation.

Gitflow workflow

An approach in which lower and upper environments use different branches in a source code repository. The Gitflow workflow is considered legacy, and the [trunk-based workflow](#) is the modern, preferred approach.

golden image

A snapshot of a system or software that is used as a template to deploy new instances of that system or software. For example, in manufacturing, a golden image can be used to provision software on multiple devices and helps improve speed, scalability, and productivity in device manufacturing operations.

greenfield strategy

The absence of existing infrastructure in a new environment. When adopting a greenfield strategy for a system architecture, you can select all new technologies without the restriction

of compatibility with existing infrastructure, also known as [brownfield](#). If you are expanding the existing infrastructure, you might blend brownfield and greenfield strategies.

guardrail

A high-level rule that helps govern resources, policies, and compliance across organizational units (OUs). *Preventive guardrails* enforce policies to ensure alignment to compliance standards. They are implemented by using service control policies and IAM permissions boundaries. *Detective guardrails* detect policy violations and compliance issues, and generate alerts for remediation. They are implemented by using AWS Config, AWS Security Hub, Amazon GuardDuty, AWS Trusted Advisor, Amazon Inspector, and custom AWS Lambda checks.

H

HA

See [high availability](#).

heterogeneous database migration

Migrating your source database to a target database that uses a different database engine (for example, Oracle to Amazon Aurora). Heterogeneous migration is typically part of a re-architecting effort, and converting the schema can be a complex task. [AWS provides AWS SCT](#) that helps with schema conversions.

high availability (HA)

The ability of a workload to operate continuously, without intervention, in the event of challenges or disasters. HA systems are designed to automatically fail over, consistently deliver high-quality performance, and handle different loads and failures with minimal performance impact.

historian modernization

An approach used to modernize and upgrade operational technology (OT) systems to better serve the needs of the manufacturing industry. A *historian* is a type of database that is used to collect and store data from various sources in a factory.

holdout data

A portion of historical, labeled data that is withheld from a dataset that is used to train a [machine learning](#) model. You can use holdout data to evaluate the model performance by comparing the model predictions against the holdout data.

homogeneous database migration

Migrating your source database to a target database that shares the same database engine (for example, Microsoft SQL Server to Amazon RDS for SQL Server). Homogeneous migration is typically part of a rehosting or replatforming effort. You can use native database utilities to migrate the schema.

hot data

Data that is frequently accessed, such as real-time data or recent translational data. This data typically requires a high-performance storage tier or class to provide fast query responses.

hotfix

An urgent fix for a critical issue in a production environment. Due to its urgency, a hotfix is usually made outside of the typical DevOps release workflow.

hypercure period

Immediately following cutover, the period of time when a migration team manages and monitors the migrated applications in the cloud in order to address any issues. Typically, this period is 1–4 days in length. At the end of the hypercure period, the migration team typically transfers responsibility for the applications to the cloud operations team.

I

laC

See [infrastructure as code](#).

identity-based policy

A policy attached to one or more IAM principals that defines their permissions within the AWS Cloud environment.

idle application

An application that has an average CPU and memory usage between 5 and 20 percent over a period of 90 days. In a migration project, it is common to retire these applications or retain them on premises.

IIoT

See [Industrial Internet of Things](#).

immutable infrastructure

A model that deploys new infrastructure for production workloads instead of updating, patching, or modifying the existing infrastructure. Immutable infrastructures are inherently more consistent, reliable, and predictable than [mutable infrastructure](#). For more information, see the [Deploy using immutable infrastructure](#) best practice in the AWS Well-Architected Framework.

inbound (ingress) VPC

In an AWS multi-account architecture, a VPC that accepts, inspects, and routes network connections from outside an application. The [AWS Security Reference Architecture](#) recommends setting up your Network account with inbound, outbound, and inspection VPCs to protect the two-way interface between your application and the broader internet.

incremental migration

A cutover strategy in which you migrate your application in small parts instead of performing a single, full cutover. For example, you might move only a few microservices or users to the new system initially. After you verify that everything is working properly, you can incrementally move additional microservices or users until you can decommission your legacy system. This strategy reduces the risks associated with large migrations.

Industry 4.0

A term that was introduced by [Klaus Schwab](#) in 2016 to refer to the modernization of manufacturing processes through advances in connectivity, real-time data, automation, analytics, and AI/ML.

infrastructure

All of the resources and assets contained within an application's environment.

infrastructure as code (IaC)

The process of provisioning and managing an application's infrastructure through a set of configuration files. IaC is designed to help you centralize infrastructure management, standardize resources, and scale quickly so that new environments are repeatable, reliable, and consistent.

industrial Internet of Things (IIoT)

The use of internet-connected sensors and devices in the industrial sectors, such as manufacturing, energy, automotive, healthcare, life sciences, and agriculture. For more information, see [Building an industrial Internet of Things \(IIoT\) digital transformation strategy](#).

inspection VPC

In an AWS multi-account architecture, a centralized VPC that manages inspections of network traffic between VPCs (in the same or different AWS Regions), the internet, and on-premises networks. The [AWS Security Reference Architecture](#) recommends setting up your Network account with inbound, outbound, and inspection VPCs to protect the two-way interface between your application and the broader internet.

Internet of Things (IoT)

The network of connected physical objects with embedded sensors or processors that communicate with other devices and systems through the internet or over a local communication network. For more information, see [What is IoT?](#)

interpretability

A characteristic of a machine learning model that describes the degree to which a human can understand how the model's predictions depend on its inputs. For more information, see [Machine learning model interpretability with AWS](#).

IoT

See [Internet of Things](#).

IT information library (ITIL)

A set of best practices for delivering IT services and aligning these services with business requirements. ITIL provides the foundation for ITSM.

IT service management (ITSM)

Activities associated with designing, implementing, managing, and supporting IT services for an organization. For information about integrating cloud operations with ITSM tools, see the [operations integration guide](#).

ITIL

See [IT information library](#).

ITSM

See [IT service management](#).

L

label-based access control (LBAC)

An implementation of mandatory access control (MAC) where the users and the data itself are each explicitly assigned a security label value. The intersection between the user security label and data security label determines which rows and columns can be seen by the user.

landing zone

A landing zone is a well-architected, multi-account AWS environment that is scalable and secure. This is a starting point from which your organizations can quickly launch and deploy workloads and applications with confidence in their security and infrastructure environment. For more information about landing zones, see [Setting up a secure and scalable multi-account AWS environment](#).

large language model (LLM)

A deep learning [AI](#) model that is pretrained on a vast amount of data. An LLM can perform multiple tasks, such as answering questions, summarizing documents, translating text into other languages, and completing sentences. For more information, see [What are LLMs](#).

large migration

A migration of 300 or more servers.

LBAC

See [label-based access control](#).

least privilege

The security best practice of granting the minimum permissions required to perform a task. For more information, see [Apply least-privilege permissions](#) in the IAM documentation.

lift and shift

See [7 Rs](#).

little-endian system

A system that stores the least significant byte first. See also [endianness](#).

LLM

See [large language model](#).

lower environments

See [environment](#).

M

machine learning (ML)

A type of artificial intelligence that uses algorithms and techniques for pattern recognition and learning. ML analyzes and learns from recorded data, such as Internet of Things (IoT) data, to generate a statistical model based on patterns. For more information, see [Machine Learning](#).

main branch

See [branch](#).

malware

Software that is designed to compromise computer security or privacy. Malware might disrupt computer systems, leak sensitive information, or gain unauthorized access. Examples of malware include viruses, worms, ransomware, Trojan horses, spyware, and keyloggers.

managed services

AWS services for which AWS operates the infrastructure layer, the operating system, and platforms, and you access the endpoints to store and retrieve data. Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB are examples of managed services. These are also known as *abstracted services*.

manufacturing execution system (MES)

A software system for tracking, monitoring, documenting, and controlling production processes that convert raw materials to finished products on the shop floor.

MAP

See [Migration Acceleration Program](#).

mechanism

A complete process in which you create a tool, drive adoption of the tool, and then inspect the results in order to make adjustments. A mechanism is a cycle that reinforces and improves itself as it operates. For more information, see [Building mechanisms](#) in the AWS Well-Architected Framework.

member account

All AWS accounts other than the management account that are part of an organization in AWS Organizations. An account can be a member of only one organization at a time.

MES

See [manufacturing execution system](#).

Message Queuing Telemetry Transport (MQTT)

A lightweight, machine-to-machine (M2M) communication protocol, based on the [publish/subscribe](#) pattern, for resource-constrained [IoT](#) devices.

microservice

A small, independent service that communicates over well-defined APIs and is typically owned by small, self-contained teams. For example, an insurance system might include microservices that map to business capabilities, such as sales or marketing, or subdomains, such as purchasing, claims, or analytics. The benefits of microservices include agility, flexible scaling, easy deployment, reusable code, and resilience. For more information, see [Integrating microservices by using AWS serverless services](#).

microservices architecture

An approach to building an application with independent components that run each application process as a microservice. These microservices communicate through a well-defined interface by using lightweight APIs. Each microservice in this architecture can be updated, deployed,

and scaled to meet demand for specific functions of an application. For more information, see [Implementing microservices on AWS](#).

Migration Acceleration Program (MAP)

An AWS program that provides consulting support, training, and services to help organizations build a strong operational foundation for moving to the cloud, and to help offset the initial cost of migrations. MAP includes a migration methodology for executing legacy migrations in a methodical way and a set of tools to automate and accelerate common migration scenarios.

migration at scale

The process of moving the majority of the application portfolio to the cloud in waves, with more applications moved at a faster rate in each wave. This phase uses the best practices and lessons learned from the earlier phases to implement a *migration factory* of teams, tools, and processes to streamline the migration of workloads through automation and agile delivery. This is the third phase of the [AWS migration strategy](#).

migration factory

Cross-functional teams that streamline the migration of workloads through automated, agile approaches. Migration factory teams typically include operations, business analysts and owners, migration engineers, developers, and DevOps professionals working in sprints. Between 20 and 50 percent of an enterprise application portfolio consists of repeated patterns that can be optimized by a factory approach. For more information, see the [discussion of migration factories](#) and the [Cloud Migration Factory guide](#) in this content set.

migration metadata

The information about the application and server that is needed to complete the migration. Each migration pattern requires a different set of migration metadata. Examples of migration metadata include the target subnet, security group, and AWS account.

migration pattern

A repeatable migration task that details the migration strategy, the migration destination, and the migration application or service used. Example: Rehost migration to Amazon EC2 with AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

An online tool that provides information for validating the business case for migrating to the AWS Cloud. MPA provides detailed portfolio assessment (server right-sizing, pricing, TCO

comparisons, migration cost analysis) as well as migration planning (application data analysis and data collection, application grouping, migration prioritization, and wave planning). The [MPA tool](#) (requires login) is available free of charge to all AWS consultants and APN Partner consultants.

Migration Readiness Assessment (MRA)

The process of gaining insights about an organization's cloud readiness status, identifying strengths and weaknesses, and building an action plan to close identified gaps, using the AWS CAF. For more information, see the [migration readiness guide](#). MRA is the first phase of the [AWS migration strategy](#).

migration strategy

The approach used to migrate a workload to the AWS Cloud. For more information, see the [7 Rs](#) entry in this glossary and see [Mobilize your organization to accelerate large-scale migrations](#).

ML

See [machine learning](#).

modernization

Transforming an outdated (legacy or monolithic) application and its infrastructure into an agile, elastic, and highly available system in the cloud to reduce costs, gain efficiencies, and take advantage of innovations. For more information, see [Strategy for modernizing applications in the AWS Cloud](#).

modernization readiness assessment

An evaluation that helps determine the modernization readiness of an organization's applications; identifies benefits, risks, and dependencies; and determines how well the organization can support the future state of those applications. The outcome of the assessment is a blueprint of the target architecture, a roadmap that details development phases and milestones for the modernization process, and an action plan for addressing identified gaps. For more information, see [Evaluating modernization readiness for applications in the AWS Cloud](#).

monolithic applications (monoliths)

Applications that run as a single service with tightly coupled processes. Monolithic applications have several drawbacks. If one application feature experiences a spike in demand, the entire architecture must be scaled. Adding or improving a monolithic application's features also becomes more complex when the code base grows. To address these issues, you can

use a microservices architecture. For more information, see [Decomposing monoliths into microservices](#).

MPA

See [Migration Portfolio Assessment](#).

MQTT

See [Message Queuing Telemetry Transport](#).

multiclass classification

A process that helps generate predictions for multiple classes (predicting one of more than two outcomes). For example, an ML model might ask "Is this product a book, car, or phone?" or "Which product category is most interesting to this customer?"

mutable infrastructure

A model that updates and modifies the existing infrastructure for production workloads. For improved consistency, reliability, and predictability, the AWS Well-Architected Framework recommends the use of [immutable infrastructure](#) as a best practice.

O

OAC

See [origin access control](#).

OAI

See [origin access identity](#).

OCM

See [organizational change management](#).

offline migration

A migration method in which the source workload is taken down during the migration process. This method involves extended downtime and is typically used for small, non-critical workloads.

OI

See [operations integration](#).

OLA

See [operational-level agreement](#).

online migration

A migration method in which the source workload is copied to the target system without being taken offline. Applications that are connected to the workload can continue to function during the migration. This method involves zero to minimal downtime and is typically used for critical production workloads.

OPC-UA

See [Open Process Communications - Unified Architecture](#).

Open Process Communications - Unified Architecture (OPC-UA)

A machine-to-machine (M2M) communication protocol for industrial automation. OPC-UA provides an interoperability standard with data encryption, authentication, and authorization schemes.

operational-level agreement (OLA)

An agreement that clarifies what functional IT groups promise to deliver to each other, to support a service-level agreement (SLA).

operational readiness review (ORR)

A checklist of questions and associated best practices that help you understand, evaluate, prevent, or reduce the scope of incidents and possible failures. For more information, see [Operational Readiness Reviews \(ORR\)](#) in the AWS Well-Architected Framework.

operational technology (OT)

Hardware and software systems that work with the physical environment to control industrial operations, equipment, and infrastructure. In manufacturing, the integration of OT and information technology (IT) systems is a key focus for [Industry 4.0](#) transformations.

operations integration (OI)

The process of modernizing operations in the cloud, which involves readiness planning, automation, and integration. For more information, see the [operations integration guide](#).

organization trail

A trail that's created by AWS CloudTrail that logs all events for all AWS accounts in an organization in AWS Organizations. This trail is created in each AWS account that's part of the

organization and tracks the activity in each account. For more information, see [Creating a trail for an organization](#) in the CloudTrail documentation.

organizational change management (OCM)

A framework for managing major, disruptive business transformations from a people, culture, and leadership perspective. OCM helps organizations prepare for, and transition to, new systems and strategies by accelerating change adoption, addressing transitional issues, and driving cultural and organizational changes. In the AWS migration strategy, this framework is called *people acceleration*, because of the speed of change required in cloud adoption projects. For more information, see the [OCM guide](#).

origin access control (OAC)

In CloudFront, an enhanced option for restricting access to secure your Amazon Simple Storage Service (Amazon S3) content. OAC supports all S3 buckets in all AWS Regions, server-side encryption with AWS KMS (SSE-KMS), and dynamic PUT and DELETE requests to the S3 bucket.

origin access identity (OAI)

In CloudFront, an option for restricting access to secure your Amazon S3 content. When you use OAI, CloudFront creates a principal that Amazon S3 can authenticate with. Authenticated principals can access content in an S3 bucket only through a specific CloudFront distribution. See also [OAC](#), which provides more granular and enhanced access control.

ORR

See [operational readiness review](#).

OT

See [operational technology](#).

outbound (egress) VPC

In an AWS multi-account architecture, a VPC that handles network connections that are initiated from within an application. The [AWS Security Reference Architecture](#) recommends setting up your Network account with inbound, outbound, and inspection VPCs to protect the two-way interface between your application and the broader internet.

P

permissions boundary

An IAM management policy that is attached to IAM principals to set the maximum permissions that the user or role can have. For more information, see [Permissions boundaries](#) in the IAM documentation.

personally identifiable information (PII)

Information that, when viewed directly or paired with other related data, can be used to reasonably infer the identity of an individual. Examples of PII include names, addresses, and contact information.

PII

See [personally identifiable information](#).

playbook

A set of predefined steps that capture the work associated with migrations, such as delivering core operations functions in the cloud. A playbook can take the form of scripts, automated runbooks, or a summary of processes or steps required to operate your modernized environment.

PLC

See [programmable logic controller](#).

PLM

See [product lifecycle management](#).

policy

An object that can define permissions (see [identity-based policy](#)), specify access conditions (see [resource-based policy](#)), or define the maximum permissions for all accounts in an organization in AWS Organizations (see [service control policy](#)).

polyglot persistence

Independently choosing a microservice's data storage technology based on data access patterns and other requirements. If your microservices have the same data storage technology, they can encounter implementation challenges or experience poor performance. Microservices are more easily implemented and achieve better performance and scalability if they use the data store

best adapted to their requirements. For more information, see [Enabling data persistence in microservices](#).

portfolio assessment

A process of discovering, analyzing, and prioritizing the application portfolio in order to plan the migration. For more information, see [Evaluating migration readiness](#).

predicate

A query condition that returns `true` or `false`, commonly located in a `WHERE` clause.

predicate pushdown

A database query optimization technique that filters the data in the query before transfer. This reduces the amount of data that must be retrieved and processed from the relational database, and it improves query performance.

preventative control

A security control that is designed to prevent an event from occurring. These controls are a first line of defense to help prevent unauthorized access or unwanted changes to your network. For more information, see [Preventative controls](#) in *Implementing security controls on AWS*.

principal

An entity in AWS that can perform actions and access resources. This entity is typically a root user for an AWS account, an IAM role, or a user. For more information, see *Principal* in [Roles terms and concepts](#) in the IAM documentation.

privacy by design

A system engineering approach that takes privacy into account through the whole development process.

private hosted zones

A container that holds information about how you want Amazon Route 53 to respond to DNS queries for a domain and its subdomains within one or more VPCs. For more information, see [Working with private hosted zones](#) in the Route 53 documentation.

proactive control

A [security control](#) designed to prevent the deployment of noncompliant resources. These controls scan resources before they are provisioned. If the resource is not compliant with the control, then it isn't provisioned. For more information, see the [Controls reference guide](#) in the

AWS Control Tower documentation and see [Proactive controls](#) in *Implementing security controls on AWS*.

product lifecycle management (PLM)

The management of data and processes for a product throughout its entire lifecycle, from design, development, and launch, through growth and maturity, to decline and removal.

production environment

See [environment](#).

programmable logic controller (PLC)

In manufacturing, a highly reliable, adaptable computer that monitors machines and automates manufacturing processes.

prompt chaining

Using the output of one [LLM](#) prompt as the input for the next prompt to generate better responses. This technique is used to break down a complex task into subtasks, or to iteratively refine or expand a preliminary response. It helps improve the accuracy and relevance of a model's responses and allows for more granular, personalized results.

pseudonymization

The process of replacing personal identifiers in a dataset with placeholder values. Pseudonymization can help protect personal privacy. Pseudonymized data is still considered to be personal data.

publish/subscribe (pub/sub)

A pattern that enables asynchronous communications among microservices to improve scalability and responsiveness. For example, in a microservices-based [MES](#), a microservice can publish event messages to a channel that other microservices can subscribe to. The system can add new microservices without changing the publishing service.

Q

query plan

A series of steps, like instructions, that are used to access the data in a SQL relational database system.

query plan regression

When a database service optimizer chooses a less optimal plan than it did before a given change to the database environment. This can be caused by changes to statistics, constraints, environment settings, query parameter bindings, and updates to the database engine.

R

RACI matrix

See [responsible, accountable, consulted, informed \(RACI\)](#).

RAG

See [Retrieval Augmented Generation](#).

ransomware

A malicious software that is designed to block access to a computer system or data until a payment is made.

RASCI matrix

See [responsible, accountable, consulted, informed \(RACI\)](#).

RCAC

See [row and column access control](#).

read replica

A copy of a database that's used for read-only purposes. You can route queries to the read replica to reduce the load on your primary database.

re-architect

See [7 Rs](#).

recovery point objective (RPO)

The maximum acceptable amount of time since the last data recovery point. This determines what is considered an acceptable loss of data between the last recovery point and the interruption of service.

recovery time objective (RTO)

The maximum acceptable delay between the interruption of service and restoration of service.

refactor

See [7 Rs](#).

Region

A collection of AWS resources in a geographic area. Each AWS Region is isolated and independent of the others to provide fault tolerance, stability, and resilience. For more information, see [Specify which AWS Regions your account can use](#).

regression

An ML technique that predicts a numeric value. For example, to solve the problem of "What price will this house sell for?" an ML model could use a linear regression model to predict a house's sale price based on known facts about the house (for example, the square footage).

rehost

See [7 Rs](#).

release

In a deployment process, the act of promoting changes to a production environment.

relocate

See [7 Rs](#).

replatform

See [7 Rs](#).

repurchase

See [7 Rs](#).

resiliency

An application's ability to resist or recover from disruptions. [High availability](#) and [disaster recovery](#) are common considerations when planning for resiliency in the AWS Cloud. For more information, see [AWS Cloud Resilience](#).

resource-based policy

A policy attached to a resource, such as an Amazon S3 bucket, an endpoint, or an encryption key. This type of policy specifies which principals are allowed access, supported actions, and any other conditions that must be met.

responsible, accountable, consulted, informed (RACI) matrix

A matrix that defines the roles and responsibilities for all parties involved in migration activities and cloud operations. The matrix name is derived from the responsibility types defined in the matrix: responsible (R), accountable (A), consulted (C), and informed (I). The support (S) type is optional. If you include support, the matrix is called a *RASCI matrix*, and if you exclude it, it's called a *RACI matrix*.

responsive control

A security control that is designed to drive remediation of adverse events or deviations from your security baseline. For more information, see [Responsive controls](#) in *Implementing security controls on AWS*.

retain

See [7 Rs](#).

retire

See [7 Rs](#).

Retrieval Augmented Generation (RAG)

A [generative AI](#) technology in which an [LLM](#) references an authoritative data source that is outside of its training data sources before generating a response. For example, a RAG model might perform a semantic search of an organization's knowledge base or custom data. For more information, see [What is RAG](#).

rotation

The process of periodically updating a [secret](#) to make it more difficult for an attacker to access the credentials.

row and column access control (RCAC)

The use of basic, flexible SQL expressions that have defined access rules. RCAC consists of row permissions and column masks.

RPO

See [recovery point objective](#).

RTO

See [recovery time objective](#).

runbook

A set of manual or automated procedures required to perform a specific task. These are typically built to streamline repetitive operations or procedures with high error rates.

S

SAML 2.0

An open standard that many identity providers (IdPs) use. This feature enables federated single sign-on (SSO), so users can log into the AWS Management Console or call the AWS API operations without you having to create user in IAM for everyone in your organization. For more information about SAML 2.0-based federation, see [About SAML 2.0-based federation](#) in the IAM documentation.

SCADA

See [supervisory control and data acquisition](#).

SCP

See [service control policy](#).

secret

In AWS Secrets Manager, confidential or restricted information, such as a password or user credentials, that you store in encrypted form. It consists of the secret value and its metadata. The secret value can be binary, a single string, or multiple strings. For more information, see [What's in a Secrets Manager secret?](#) in the Secrets Manager documentation.

security by design

A system engineering approach that takes security into account through the whole development process.

security control

A technical or administrative guardrail that prevents, detects, or reduces the ability of a threat actor to exploit a security vulnerability. There are four primary types of security controls: [preventative](#), [detective](#), [responsive](#), and [proactive](#).

security hardening

The process of reducing the attack surface to make it more resistant to attacks. This can include actions such as removing resources that are no longer needed, implementing the security best practice of granting least privilege, or deactivating unnecessary features in configuration files.

security information and event management (SIEM) system

Tools and services that combine security information management (SIM) and security event management (SEM) systems. A SIEM system collects, monitors, and analyzes data from servers, networks, devices, and other sources to detect threats and security breaches, and to generate alerts.

security response automation

A predefined and programmed action that is designed to automatically respond to or remediate a security event. These automations serve as [detective](#) or [responsive](#) security controls that help you implement AWS security best practices. Examples of automated response actions include modifying a VPC security group, patching an Amazon EC2 instance, or rotating credentials.

server-side encryption

Encryption of data at its destination, by the AWS service that receives it.

service control policy (SCP)

A policy that provides centralized control over permissions for all accounts in an organization in AWS Organizations. SCPs define guardrails or set limits on actions that an administrator can delegate to users or roles. You can use SCPs as allow lists or deny lists, to specify which services or actions are permitted or prohibited. For more information, see [Service control policies](#) in the AWS Organizations documentation.

service endpoint

The URL of the entry point for an AWS service. You can use the endpoint to connect programmatically to the target service. For more information, see [AWS service endpoints](#) in *AWS General Reference*.

service-level agreement (SLA)

An agreement that clarifies what an IT team promises to deliver to their customers, such as service uptime and performance.

service-level indicator (SLI)

A measurement of a performance aspect of a service, such as its error rate, availability, or throughput.

service-level objective (SLO)

A target metric that represents the health of a service, as measured by a [service-level indicator](#).

shared responsibility model

A model describing the responsibility you share with AWS for cloud security and compliance. AWS is responsible for security *of* the cloud, whereas you are responsible for security *in* the cloud. For more information, see [Shared responsibility model](#).

SIEM

See [security information and event management system](#).

single point of failure (SPOF)

A failure in a single, critical component of an application that can disrupt the system.

SLA

See [service-level agreement](#).

SLI

See [service-level indicator](#).

SLO

See [service-level objective](#).

split-and-seed model

A pattern for scaling and accelerating modernization projects. As new features and product releases are defined, the core team splits up to create new product teams. This helps scale your organization's capabilities and services, improves developer productivity, and supports rapid

innovation. For more information, see [Phased approach to modernizing applications in the AWS Cloud](#).

SPOF

See [single point of failure](#).

star schema

A database organizational structure that uses one large fact table to store transactional or measured data and uses one or more smaller dimensional tables to store data attributes. This structure is designed for use in a [data warehouse](#) or for business intelligence purposes.

strangler fig pattern

An approach to modernizing monolithic systems by incrementally rewriting and replacing system functionality until the legacy system can be decommissioned. This pattern uses the analogy of a fig vine that grows into an established tree and eventually overcomes and replaces its host. The pattern was [introduced by Martin Fowler](#) as a way to manage risk when rewriting monolithic systems. For an example of how to apply this pattern, see [Modernizing legacy Microsoft ASP.NET \(ASMX\) web services incrementally by using containers and Amazon API Gateway](#).

subnet

A range of IP addresses in your VPC. A subnet must reside in a single Availability Zone.

supervisory control and data acquisition (SCADA)

In manufacturing, a system that uses hardware and software to monitor physical assets and production operations.

symmetric encryption

An encryption algorithm that uses the same key to encrypt and decrypt the data.

synthetic testing

Testing a system in a way that simulates user interactions to detect potential issues or to monitor performance. You can use [Amazon CloudWatch Synthetics](#) to create these tests.

system prompt

A technique for providing context, instructions, or guidelines to an [LLM](#) to direct its behavior. System prompts help set context and establish rules for interactions with users.

T

tags

Key-value pairs that act as metadata for organizing your AWS resources. Tags can help you manage, identify, organize, search for, and filter resources. For more information, see [Tagging your AWS resources](#).

target variable

The value that you are trying to predict in supervised ML. This is also referred to as an *outcome variable*. For example, in a manufacturing setting the target variable could be a product defect.

task list

A tool that is used to track progress through a runbook. A task list contains an overview of the runbook and a list of general tasks to be completed. For each general task, it includes the estimated amount of time required, the owner, and the progress.

test environment

See [environment](#).

training

To provide data for your ML model to learn from. The training data must contain the correct answer. The learning algorithm finds patterns in the training data that map the input data attributes to the target (the answer that you want to predict). It outputs an ML model that captures these patterns. You can then use the ML model to make predictions on new data for which you don't know the target.

transit gateway

A network transit hub that you can use to interconnect your VPCs and on-premises networks. For more information, see [What is a transit gateway](#) in the AWS Transit Gateway documentation.

trunk-based workflow

An approach in which developers build and test features locally in a feature branch and then merge those changes into the main branch. The main branch is then built to the development, preproduction, and production environments, sequentially.

trusted access

Granting permissions to a service that you specify to perform tasks in your organization in AWS Organizations and in its accounts on your behalf. The trusted service creates a service-linked role in each account, when that role is needed, to perform management tasks for you. For more information, see [Using AWS Organizations with other AWS services](#) in the AWS Organizations documentation.

tuning

To change aspects of your training process to improve the ML model's accuracy. For example, you can train the ML model by generating a labeling set, adding labels, and then repeating these steps several times under different settings to optimize the model.

two-pizza team

A small DevOps team that you can feed with two pizzas. A two-pizza team size ensures the best possible opportunity for collaboration in software development.

U

uncertainty

A concept that refers to imprecise, incomplete, or unknown information that can undermine the reliability of predictive ML models. There are two types of uncertainty: *Epistemic uncertainty* is caused by limited, incomplete data, whereas *aleatoric uncertainty* is caused by the noise and randomness inherent in the data. For more information, see the [Quantifying uncertainty in deep learning systems](#) guide.

undifferentiated tasks

Also known as *heavy lifting*, work that is necessary to create and operate an application but that doesn't provide direct value to the end user or provide competitive advantage. Examples of undifferentiated tasks include procurement, maintenance, and capacity planning.

upper environments

See [environment](#).

V

vacuuming

A database maintenance operation that involves cleaning up after incremental updates to reclaim storage and improve performance.

version control

Processes and tools that track changes, such as changes to source code in a repository.

VPC peering

A connection between two VPCs that allows you to route traffic by using private IP addresses. For more information, see [What is VPC peering](#) in the Amazon VPC documentation.

vulnerability

A software or hardware flaw that compromises the security of the system.

W

warm cache

A buffer cache that contains current, relevant data that is frequently accessed. The database instance can read from the buffer cache, which is faster than reading from the main memory or disk.

warm data

Data that is infrequently accessed. When querying this kind of data, moderately slow queries are typically acceptable.

window function

A SQL function that performs a calculation on a group of rows that relate in some way to the current record. Window functions are useful for processing tasks, such as calculating a moving average or accessing the value of rows based on the relative position of the current row.

workload

A collection of resources and code that delivers business value, such as a customer-facing application or backend process.

workstream

Functional groups in a migration project that are responsible for a specific set of tasks. Each workstream is independent but supports the other workstreams in the project. For example, the portfolio workstream is responsible for prioritizing applications, wave planning, and collecting migration metadata. The portfolio workstream delivers these assets to the migration workstream, which then migrates the servers and applications.

WORM

See [write once, read many](#).

WQF

See [AWS Workload Qualification Framework](#).

write once, read many (WORM)

A storage model that writes data a single time and prevents the data from being deleted or modified. Authorized users can read the data as many times as needed, but they cannot change it. This data storage infrastructure is considered [immutable](#).

Z

zero-day exploit

An attack, typically malware, that takes advantage of a [zero-day vulnerability](#).

zero-day vulnerability

An unmitigated flaw or vulnerability in a production system. Threat actors can use this type of vulnerability to attack the system. Developers frequently become aware of the vulnerability as a result of the attack.

zero-shot prompting

Providing an [LLM](#) with instructions for performing a task but no examples (*shots*) that can help guide it. The LLM must use its pre-trained knowledge to handle the task. The effectiveness of zero-shot prompting depends on the complexity of the task and the quality of the prompt. See also [few-shot prompting](#).

zombie application

An application that has an average CPU and memory usage below 5 percent. In a migration project, it is common to retire these applications.