include::attributes.txt[]

// Attributes [.topic] [#security-iam] = Identity and access management for the {aws} Cloud Development Kit ({aws} CDK) :info\_titleabbrev: Identity and access management

== [abstract]

## Provides information about identity and access management for the {aws} CDK.

// Content start

{aws} Identity and Access Management (IAM) is an {aws} service that helps an administrator securely control access to {aws} resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use {aws} resources. IAM is an {aws} service that you can use with no additional charge.

[#security-iam-audience] == Audience

How you use {aws} Identity and Access Management (IAM) differs, depending on the work that you do in {aws}.

*Service user* – If you use {aws} services to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more {aws} features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator.

*Service administrator* – If you’re in charge of {aws} resources at your company, you probably have full access to {aws} resources. It’s your job to determine which {aws} services and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM.

*IAM administrator* – If you’re an IAM administrator, you might want to learn details about how you can write policies to manage access to {aws} services.

[#security-iam-authentication] == Authenticating with identities

Authentication is how you sign in to {aws} using your identity credentials. You must be *authenticated* (signed in to {aws}) as the {aws} account root user, as an IAM user, or by assuming an IAM role.

You can sign in to {aws} as a federated identity by using credentials provided through an identity source. {aws} IAM Identity Center (IAM Identity Center) users, your company’s single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access {aws} by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the {aws} Management Console or the {aws} access portal. For more information about signing in to {aws}, see link:https://docs.aws.amazon.com/signin/latest/userguide/how-to-sign-in.html[How to sign in to your {aws} account] in the *{aws} Sign-In User Guide*.

To access {aws} programmatically, {aws} provides the {aws} CDK, software development kits (SDKs), and a command line interface (CLI) to cryptographically sign your requests using your credentials. If you don’t use {aws} tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see link:https://docs.aws.amazon.com/general/latest/gr/signature-version-4.html[Signature Version 4 signing process] in the *{aws} General Reference*.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, {aws} recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see https://docs.aws.amazon.com/singlesignon/latest/userguide/enable-mfa.html[Multi-factor authentication] in the *{aws} IAM Identity Center User Guide* and link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_credentials\_mfa.html[Using multi-factor authentication (MFA) in {aws}] in the *IAM User Guide*.

[#security-iam-authentication-rootuser] === {aws} account root user

When you create an {aws} account, you begin with one sign-in identity that has complete access to all {aws} services and resources in the account. This identity is called the {aws} account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don’t use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_root-user.html#root-user-tasks[Tasks that require root user credentials] in the *IAM User Guide*.

[#security-iam-authentication-federated] === Federated identity

As a best practice, require human users, including users that require administrator access, to use federation with an identity provider to access {aws} services by using temporary credentials.

A *federated identity* is a user from your enterprise user directory, a web identity provider, the {aws} Directory Service, the Identity Center directory, or any user that accesses {aws} services by using credentials provided through an identity source. When federated identities access {aws} accounts, they assume roles, and the roles provide temporary credentials.

For centralized access management, we recommend that you use {aws} IAM Identity Center. You can create users and groups in IAM Identity Center, or you can connect and synchronize to a set of users and groups in your own identity source for use across all your {aws} accounts and applications. For information about IAM Identity Center, see link:https://docs.aws.amazon.com/singlesignon/latest/userguide/what-is.html[What is IAM Identity Center?] in the *{aws} IAM Identity Center User Guide*.

[#security-iam-authentication-iamuser] === IAM users and groups

An *link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_users.html[IAM user]* is an identity within your {aws} account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see link:https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#rotate-credentials[Rotate access keys regularly for use cases that require long-term credentials] in the *IAM User Guide*.

An link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_groups.html[IAM group] is an identity that specifies a collection of IAM users. You can’t sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see link:https://docs.aws.amazon.com/IAM/latest/UserGuide/gs-identities-iam-users.html[Use cases for IAM users] in the *IAM User Guide*.

[#security-iam-authentication-iamrole] === IAM roles

An *link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles.html[IAM role]* is an identity within your {aws} account that has specific permissions. It’s similar to an IAM user, but isn’t associated with a specific person. You can temporarily assume an IAM role in the {aws} Management Console by link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles\_use\_switch-role-console.html[switching roles]. You can assume a role by calling an {aws} CLI or {aws} API operation or by using a custom URL. For more information about methods for using roles, see link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles\_use.html[Using IAM roles] in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

* *Federated user access* – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles\_create\_for-idp.html[Create a role for a third-party identity provider (federation)] in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see https://docs.aws.amazon.com/singlesignon/latest/userguide/permissionsetsconcept.html[Permission sets] in the *{aws} IAM Identity Center User Guide*.
* *Temporary IAM user permissions* – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
* *Cross-account access* – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some {aws} services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles\_compare-resource-policies.html[How IAM roles differ from resource-based policies] in the *IAM User Guide*.
* *Cross-service access* – Some {aws} services use features in other {aws} services. For example, when you make a call in a service, it’s common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal’s permissions, using a service role, or using a service-linked role.

|  |
| --- |
| \*\* *Service role* – A service role is an link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles.html[IAM role] that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles\_create\_for-service.html[Create a role to delegate permissions to an {aws} service] in the *IAM User Guide*. |
| \*\* *Service-linked role* – A service-linked role is a type of service role that is linked to an {aws} service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your {aws} account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles. |

* *Applications running on Amazon EC2* – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making {aws} CLI or {aws} API requests. This is preferable to storing access keys within the EC2 instance. To assign an {aws} role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles\_use\_switch-role-ec2.html[Use an IAM role to grant permissions to applications running on Amazon EC2 instances] in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see link:https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html#id\_which-to-choose\_role[When to create an IAM role (instead of a user)] in the *IAM User Guide*.