include::attributes.txt[]

// Attributes [.topic] [#customize-permissions-boundaries] = Create and apply permissions boundaries for the {aws} CDK :info\_titleabbrev: Create and apply permissions boundaries :keywords: {aws} CDK, IAM, security, permissions, Permissions boundaries

== [abstract]

## A *permissions boundary* is an {aws} Identity and Access Management (IAM) advanced feature that you can use to set the maximum permissions that an IAM entity, such as a user or role, can have. You can use permissions boundaries to restrict the actions that IAM entities can perform when using the {aws} Cloud Development Kit ({aws} CDK).

// Content start A *permissions boundary* is an {aws} Identity and Access Management (IAM) advanced feature that you can use to set the maximum permissions that an IAM entity, such as a user or role, can have. You can use permissions boundaries to restrict the actions that IAM entities can perform when using the {aws} Cloud Development Kit ({aws} CDK).

To learn more about permissions boundaries, see link:https://docs.aws.amazon.com/IAM/latest/UserGuide/access\_policies\_boundaries.html[Permissions boundaries for IAM entities] in the *IAM User Guide*.

[#customize-permissions-boundaries-when] == When to use permissions boundaries with the {aws} CDK

Consider applying permissions boundaries when you need to restrict developers in your organization from performing certain actions with the {aws} CDK. For example, if there are specific resources in your {aws} environment that you don’t want developers to modify, you can create and apply a permissions boundary.

[#customize-permissions-boundaries-how] == How to apply permissions boundaries with the {aws} CDK

[#customize-permissions-boundaries-how-create] === Create the permissions boundary

First, you create the permissions boundary, using an {aws} managed policy or a customer managed policy to set the boundary for an IAM entity (user or role). This policy limits the maximum permissions for the user or role. For instructions on creating permissions boundaries, see link:https://docs.aws.amazon.com/IAM/latest/UserGuide/access\_policies\_boundaries.html[Permissions boundaries for IAM entities] in the *IAM User Guide*.

Permissions boundaries set the maximum permissions that an IAM entity can have, but don’t grant permissions on their own. You must use permissions boundaries with IAM policies to effectively limit and grant the proper permissions for your organization. You must also prevent IAM entities from being able to escape the boundaries that you set. For an example, see link:https://docs.aws.amazon.com/IAM/latest/UserGuide/access\_policies\_boundaries.html#access\_policies\_boundaries-delegate[Delegating responsibility to others using permissions boundaries] in the *IAM User Guide*.

[#customize-permissions-boundaries-how-apply] === Apply the permissions boundary during bootstrapping

After creating the permissions boundary, you can enforce it for the {aws} CDK by applying it during bootstrapping.

Use the xref:ref-cli-cmd-bootstrap-options-custom-permissions-boundary[--custom-permissions-boundary] option and specify the name of the permissions boundary to apply. The following is an example that applies a permissions boundary named cdk-permissions-boundary:

== [source,none,subs=“verbatim,attributes”]

$ cdk bootstrap –custom-permissions-boundary ++++++—-++++++

By default, the CDK uses the CloudFormationExecutionRole IAM role, defined in the bootstrap template, to receive permissions for performing deployments. By applying the custom permissions boundary during bootstrapping, the permissions boundary gets attached to this role. The permissions boundary will then set the maximum permissions that can be performed by developers in your organization when using the {aws} CDK. To learn more about this role, see xref:bootstrapping-env-roles[IAM roles created during bootstrapping].

When you apply permissions boundaries in this way, they are applied to the specific environment that you bootstrap. To use the same permissions boundary across multiple environments, you must apply the permissions boundary for each environment during bootstrapping. You can also apply different permissions boundaries for different environments.

[#customize-permissions-boundaries-learn] == Learn more

For more information on permissions boundaries, see https://aws.amazon.com/blogs/security/when-and-where-to-use-iam-permissions-boundaries/[When and where to use IAM permissions boundaries] in the *{aws} Security Blog*.