This document is a truncated version of the information published in the IAM User Guide: <https://docs.aws.amazon.com/IAM/latest/UserGuide/using-service-linked-roles.html>

# Using Service-Linked Roles

A service-linked role is a unique type of IAM role that is linked directly to an AWS service. Service-linked roles are predefined by the service and include all the permissions that the service requires to call other AWS services on your behalf. The linked service also defines how you create, modify, and delete a service-linked role. A service might automatically create or delete the role. It might allow you to create, modify, or delete the role as part of a wizard or process in the service. Or it might require that you use IAM to create or delete the role. Regardless of the method, service-linked roles make setting up a service easier because you don’t have to manually add the necessary permissions for the service to complete actions on your behalf.

The linked service defines the permissions of its service-linked roles, and unless defined otherwise, only that service can assume the roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete the roles only after first deleting their related resources. This protects your resources because you can't inadvertently remove permission to access the resources.

**Tip**

For information about which services support using service-linked roles, see [AWS Services That Work with IAM](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html) and look for the services that have **Yes**in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

## Service-Linked Role Permissions

You must configure permissions for an IAM entity (user, group, or role) to allow the user or role to create or edit the service-linked role.

**Note**

The ARN for a service-linked role includes a service principal, which is indicated in the policies below as *SERVICE-NAME*.amazonaws.com. Do not try to guess the service principal, because it is case sensitive and the format can vary across AWS services. To view the service principal for a service, see its service-linked role documentation.

**To allow an IAM entity to create a specific service-linked role**

Add the following policy to the IAM entity that needs to create the service-linked role.

{

 "Version": "2012-10-17",

 "Statement": [

 {

 "Effect": "Allow",

 "Action": "iam:CreateServiceLinkedRole",

 "Resource": "arn:aws:iam::\*:role/aws-service-role/*SERVICE-NAME*.amazonaws.com/*SERVICE-LINKED-ROLE-NAME-PREFIX*\*",

 "Condition": {"StringLike": {"iam:AWSServiceName": "*SERVICE-NAME*.amazonaws.com"}}

 },

 {

 "Effect": "Allow",

 "Action": [

 "iam:AttachRolePolicy",

 "iam:PutRolePolicy"

 ],

 "Resource": "arn:aws:iam::\*:role/aws-service-role/*SERVICE-NAME*.amazonaws.com/*SERVICE-LINKED-ROLE-NAME-PREFIX*\*"

 }

 ]

}

**To allow an IAM entity to create any service-linked role**

Add the following statement to the permissions policy for the IAM entity that needs to create a service-linked role, or any service role that includes the needed policies. This policy statement does not allow the IAM entity to attach a policy to the role.

{

 "Effect": "Allow",

 "Action": "iam:CreateServiceLinkedRole",

 "Resource": "arn:aws:iam::\*:role/aws-service-role/\*"

}

**To allow an IAM entity to edit the description of any service roles**

Add the following statement to the permissions policy for the IAM entity that needs to edit the description of a service-linked role, or any service role.

{

 "Effect": "Allow",

 "Action": "iam:UpdateRoleDescription",

 "Resource": "arn:aws:iam::\*:role/aws-service-role/\*"

}

**To allow an IAM entity to delete a specific service-linked role**

Add the following statement to the permissions policy for the IAM entity that needs to delete the service-linked role.

{

 "Effect": "Allow",

 "Action": [

 "iam:DeleteServiceLinkedRole",

 "iam:GetServiceLinkedRoleDeletionStatus"

 ],

 "Resource": "arn:aws:iam::\*:role/aws-service-role/*SERVICE-NAME*.amazonaws.com/*SERVICE-LINKED-ROLE-NAME-PREFIX*\*"

}

**To allow an IAM entity to delete any service-linked role**

Add the following statement to the permissions policy for the IAM entity that needs to delete a service-linked role, but not service role.

{

 "Effect": "Allow",

 "Action": [

 "iam:DeleteServiceLinkedRole",

 "iam:GetServiceLinkedRoleDeletionStatus"

 ],

 "Resource": "arn:aws:iam::\*:role/aws-service-role/\*"

}

## Creating a Service-Linked Role

The method that you use to create a service-linked role depends on the service. In some cases, you don't need to manually create a service-linked role. For example, when you complete a specific action (such as creating a resource) in the service, the service might create the service-linked role for you. Or if you were using a service before it began supporting service-linked roles, then the service might have automatically created the role in your account. To learn more, see [A New Role Appeared in My AWS Account](https://docs.aws.amazon.com/IAM/latest/UserGuide/troubleshoot_roles.html#troubleshoot_roles_new-role-appeared).

In other cases, the service might support creating a service-linked role manually using the service console, API, or CLI. For information about which services support using service-linked roles, see [AWS Services That Work with IAM](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html) and look for the services that have **Yes**in the **Service-Linked Role** column. To learn whether the service supports creating the service-linked role, choose the **Yes** link to view the service-linked role documentation for that service.

If the service does not support creating the role, then you can use IAM to create the service-linked role.

**Important**

Service-linked roles count toward your [IAM roles in an AWS account](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_iam-limits.html#reference_iam-limits-entities) limit, but if you have reached your limit, you can still create service-linked roles in your account. Only service-linked roles can exceed the limit.

### Creating a Service-Linked Role (Console)

Before you create a service-linked role in IAM, find out whether the linked service automatically creates service-linked roles, In addition, learn whether you can create the role from the service's console, API, or CLI.

**To create a service-linked role (console)**

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the navigation pane of the IAM console, choose **Roles**. Then choose **Create role**.
3. Choose the **AWS Service** role type, and then choose the service that you want to allow to assume this role.
4. Choose the use case for your service. If the specified service has only one use case, it is selected for you. Use cases are defined by the service to include the trust policy required by the service. Then choose **Next: Permissions**.
5. Choose one or more permissions policies to attach to the role. Depending on the use case that you selected, the service might do any of the following:
	* Define the permissions used by the role
	* Allow you to choose from a limited set of permissions
	* Allow you to choose from any permissions
	* Allow you to select no policies at this time, create the policies later, and then attach them to the role.

Select the box next to the policy that assigns the permissions that you want the role to have, and then choose **Next: Review**.

**Note**

The permissions that you specify are available to any entity that uses the role. By default, a role has no permissions.

1. For **Role name**, the degree of role name customization is defined by the service. If the service defines the role's name, then this option is not editable. In other cases, the service might define a prefix for the role and allow you to type an optional suffix.

If possible, type a role name suffix to add to the default name. This suffix helps you identify the purpose of this role. Role names must be unique within your AWS account. They are not distinguished by case. For example, you cannot create roles named both **<service-linked-role-name>\_SAMPLE** and **<service-linked-role-name>\_sample**. Because various entities might reference the role, you cannot edit the name of the role after it has been created.

1. (Optional) For **Role description**, edit the description for the new service-linked role.
2. Review the role and then choose **Create role**.

### Creating a Service-Linked Role (AWS CLI)

Before creating a service-linked role in IAM, find out whether the linked service automatically creates service-linked roles and whether you can create the role from the service's CLI. If the service CLI is not supported, you can use IAM commands to create a service-linked role with the trust policy and inline policies that the service needs to assume the role.

**To create a service-linked role (AWS CLI)**

Run the following command:

$ **aws iam** [**create-service-linked-role**](https://docs.aws.amazon.com/cli/latest/reference/iam/create-service-linked-role.html) **--aws-service-name *SERVICE-NAME*.amazonaws.com**

### Creating a Service-Linked Role (AWS API)

Before creating a service-linked role in IAM, find out whether the linked service automatically creates service-linked roles and whether you can create the role from the service's API. If the service API is not supported, you can use the AWS API to create a service-linked role with the trust policy and inline policies that the service needs to assume the role.

**To create a service-linked role (AWS API)**

Use the [CreateServiceLinkedRole](https://docs.aws.amazon.com/IAM/latest/APIReference/API_CreateServiceLinkedRole.html) API call. In the request, specify a service name of *SERVICE\_NAME\_URL*.amazonaws.com.

For example, to create the **Lex Bots** service-linked role, use lex.amazonaws.com.