

# Using Service-Linked Roles for Amazon Lightsail

---

*Last updated: November 28, 2018*

Amazon Lightsail uses AWS Identity and Access Management (IAM) [service-linked roles](#). A service-linked role is a unique type of IAM role that is linked directly to Lightsail. Service-linked roles are predefined by Lightsail and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Lightsail easier because you don't have to manually add the necessary permissions. Lightsail defines the permissions of its service-linked roles, and unless defined otherwise, only Lightsail can assume its 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 a service-linked role only after first deleting their related resources. This protects your Lightsail resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see [AWS Services That Work with IAM](#) 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 for Lightsail

Lightsail uses the service-linked role named **AWSServiceRoleForLightsail** – Role to export Lightsail instance and block storage disk snapshots to Amazon Elastic Compute Cloud (Amazon EC2).

The AWSServiceRoleForLightsail service-linked role trusts the following services to assume the role:

- [lightsail.amazonaws.com](#)

The role permissions policy allows Lightsail to complete the following actions on the specified resources:

- Action: [ec2:CopySnapshot](#) on all AWS resources.
- Action: [ec2:DescribeSnapshots](#) on all AWS resources.
- Action: [ec2:CopyImage](#) on all AWS resources.
- Action: [ec2:DescribeImages](#) on all AWS resources.
- Action: [kms:Decrypt](#) on Lightsail-managed keys.
- Action: [kms:DescribeKey](#) on Lightsail-managed keys.
- Action: [kms:CreateGrant](#) on Lightsail-managed keys.
- Action: [cloudformation:DescribeStacks](#) on all AWS CloudFormation stacks.

## Service-Linked Role Permissions

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create or edit the description of a service-linked role.

### 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/lightsail.amazonaws.com/AWSServiceRoleForLightsail*",
      "Condition": {"StringLike": {"iam:AWSServiceName":
"lightsail.amazonaws.com"}}
    },
    {
      "Effect": "Allow",
      "Action": "iam:PutRolePolicy",
      "Resource": "arn:aws:iam::*:role/aws-service-
role/lightsail.amazonaws.com/AWSServiceRoleForLightsail*"
    }
  ]
}
```

### 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 attaches 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/lightsail.amazonaws.com/AWSServiceRoleForLightsail*"
}
```

### To allow an IAM entity to delete any service role

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

```
{
  "Effect": "Allow",
  "Action": [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

Alternatively, you can use an AWS managed policy to provide full access to the service.

## Creating a Service-Linked Role for Lightsail

You don't need to manually create a service-linked role. When you export your Lightsail instance or block storage disk snapshot to Amazon EC2 in the AWS Management Console, the AWS CLI, or the AWS API, Lightsail creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you export your Lightsail instance or block storage disk snapshot to Amazon EC2, Lightsail creates the service-linked role for you again.

### Important

You must configure IAM permissions to allow Lightsail to create the service-linked role. To do this, complete the steps that are in the following *Service-Linked Role Permissions* section.

## Editing a Service-Linked Role for Lightsail

Lightsail does not allow you to edit the AWSServiceRoleForLightsail service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see [Editing a Service-Linked Role](#) in the *IAM User Guide*.

## Deleting a Service-Linked Role for Lightsail

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must confirm that there are no Lightsail instance or disk snapshots in a pending copy state before you can delete the `AWSServiceRoleForLightsail` service-linked role. For more information, see [Exporting Amazon Lightsail snapshots to Amazon EC2](#).

### **To manually delete the service-linked role using IAM**

Use the IAM console, the AWS CLI, or the AWS API to delete the `AWSServiceRoleForLightsail` service-linked role. For more information, see [Deleting a Service-Linked Role](#) in the *IAM User Guide*.

## Supported Regions for Lightsail Service-Linked Roles

Lightsail supports using service-linked roles in all of the regions where the service is available. For more information about the regions that Lightsail is available in, see [Amazon Lightsail Regions](#).