Using tags to control access to your Amazon Lightsail resources

Last updated: November 28, 2018

You can use tags in Amazon Lightsail to control access to resources, control access to requests, and control access to tag keys. In this guide, you'll learn how to create an AWS Identity and Access Management (IAM) policy that specifies a key-value tag required to create or delete Lightsail resources, and attach the policy to users or groups who need to make those requests.

Note
To learn more about tags in Lightsail, what resources can be tagged, and the restrictions, see Tags in Amazon Lightsail.

Step 1: Create an IAM policy

First, create the following IAM policies in the IAM console. For more information about creating IAM policies, see Creating IAM Policies in the IAM documentation.

The following policy restricts users from creating new Lightsail resources unless a key tag of `allow` and a value of `true` is defined with the create request. This policy also restricts users from deleting resources unless they have the `allow/true` key-value tag.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:Create*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/allow": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:Delete*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allow": "true"
                }
            }
        }
    ]
}
```

The following policy restricts users from changing the tag for resources that have a key-value tag that is not
allow/false.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "lightsail:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:ResourceTag/allow": "false"
                }
            }
        }
    ]
}
```

Step 2: Attach the policy to users or groups

After you've created the IAM policies, attach them to the users or groups who need to create Lightsail
resources using the key-value pair. For more information about attaching IAM policies to users or groups, see
Adding and Removing IAM Policies in the IAM documentation.