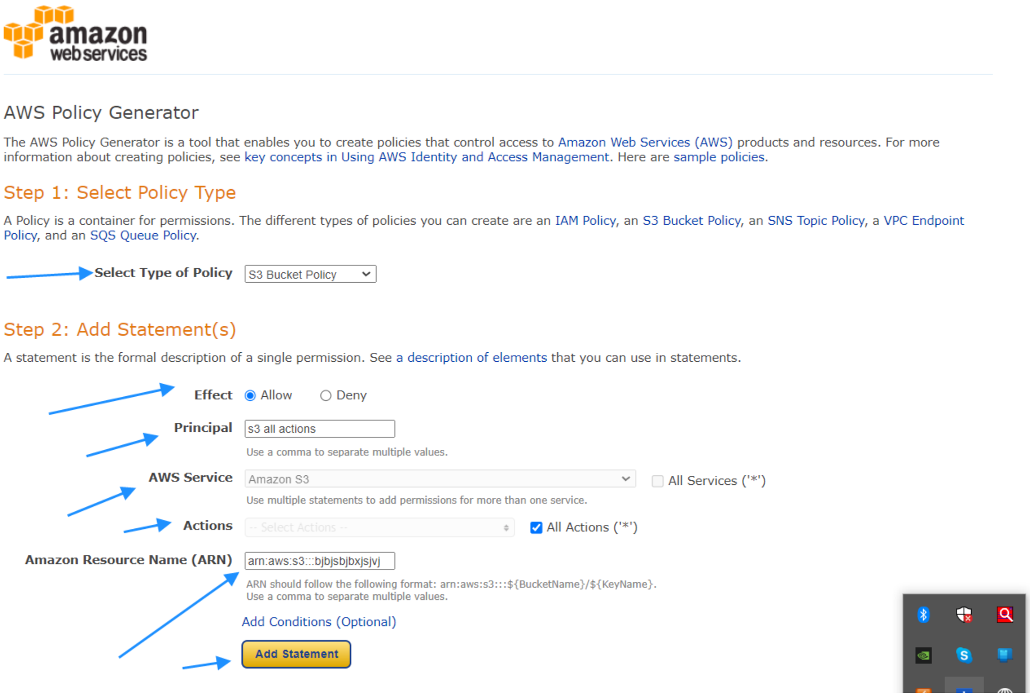
Creating Policy using Policy Generator

What is policy ?

IAM policy defines permissions for an action of the method that you use to perform operation.

Steps:-

1) Open chrome browser write **aws policy generator** in new tab
2) Open first link of aws policy generator
3) Select policy type
4) Give effect allow or deny
5) Add principle
6) Select actions which you want to give. I have given all actions
7) Add resource of amazon s3 bucket
8) Click on add statement



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy: S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect ● Allow ○ Deny

Principal: s3 all actions

Use a comma to separate multiple values.

AWS Service: Amazon S3 □ All Services ('*')

Use multiple statements to add permissions for more than one service.

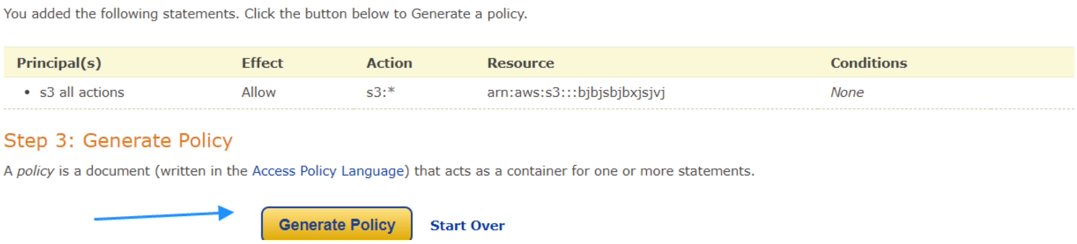
Actions: -- Select Actions -- ☑ All Actions ('*')

Amazon Resource Name (ARN): arn:aws:s3:::bjbjsbjbxjsjvj

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

9) Now statement is added now click on generate policy



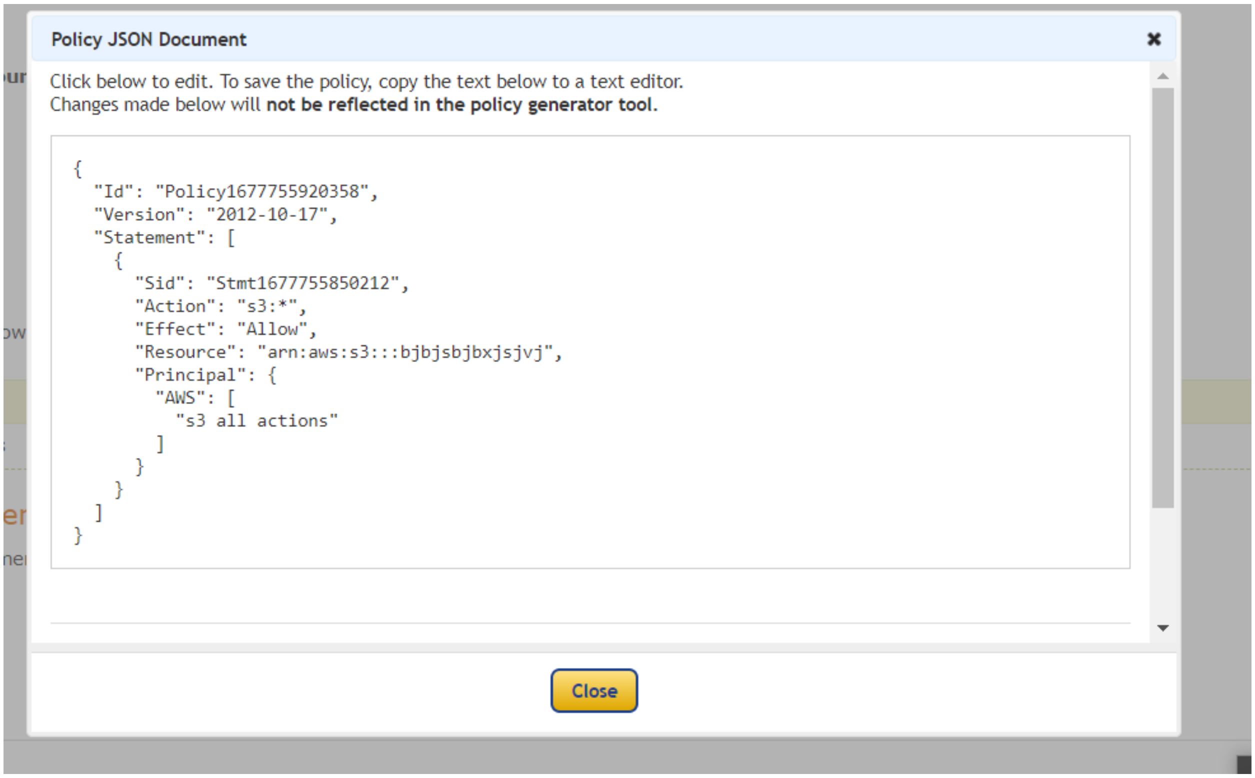
You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• s3 all actions	Allow	s3:*	arn:aws:s3:::bjbjsbjbxjsjvj	*None*

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

10) Now copy policy JSON document



Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

```
{
  "Id": "Policy1677755920358",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1677755850212",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bjbjsbjbxjsjvj",
      "Principal": {
        "AWS": [
          "s3 all actions"
        ]
      }
    }
  ]
}
```

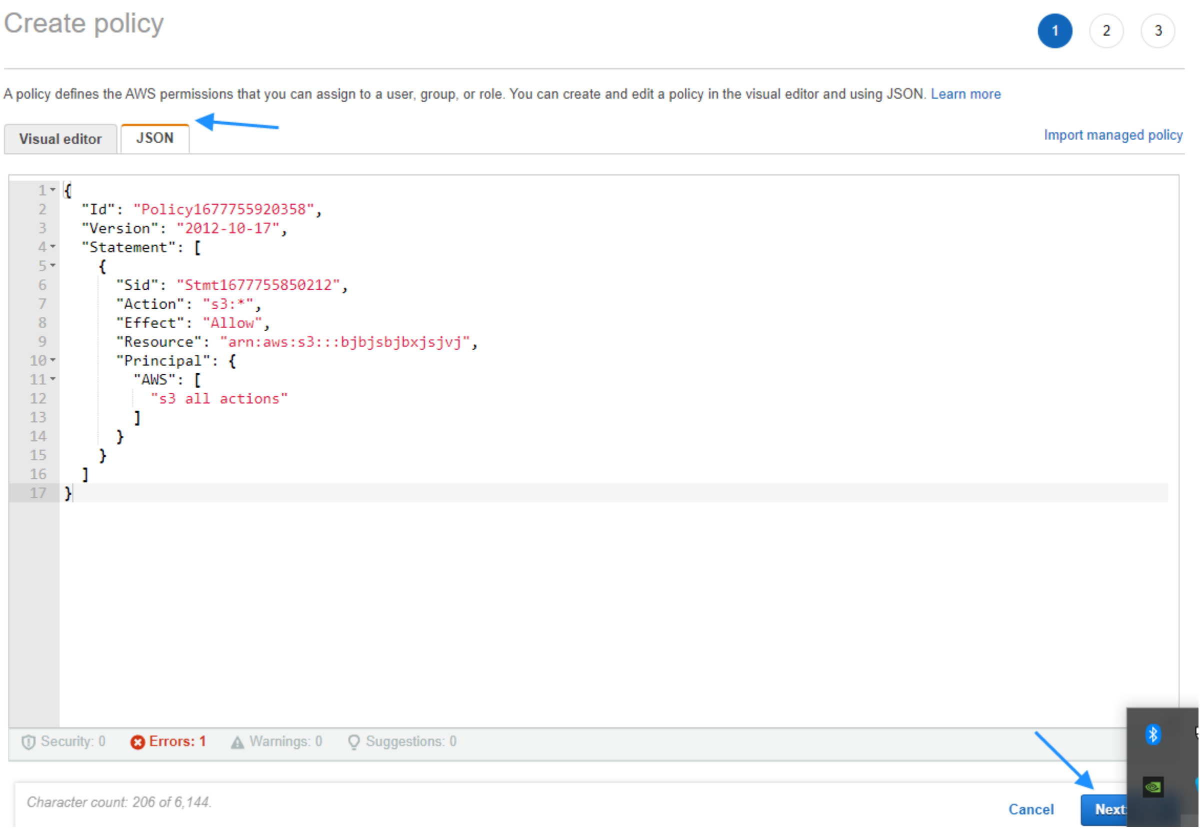
11) Now open IAM console

12) Go to policies

13) Click on create policy

14) Select JSON

15) Paste copied JSON format here



A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

```
{
  "Id": "Policy1677755920358",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1677755850212",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bjbjsbjbxjsjvj",
      "Principal": {
        "AWS": [
          "s3 all actions"
        ]
      }
    }
  ]
}
```

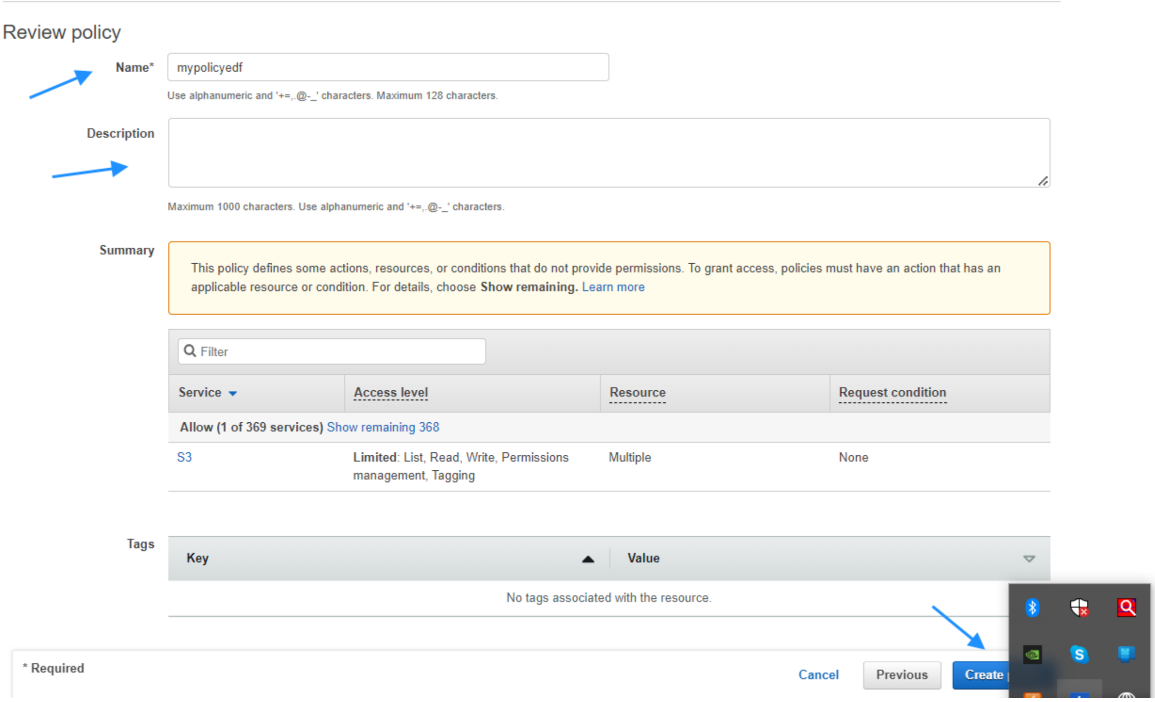
Security: 0 Errors: 1 Warnings: 0 Suggestions: 0

Character count: 206 of 6,144.

16) Give tags and click on next

17) Give name to the policy

18) And click on create policy



Name* mypolicyedf

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose **Show remaining.** Learn more

Filter

Service	Access level	Resource	Request condition
Allow (1 of 369 services) Show remaining 368			
S3	Limited: List, Read, Write, Permissions management, Tagging	Multiple	None

Tags

Key	Value
No tags associated with the resource.	

* Required