



WCE ACM
STUDENT CHAPTER

Walchand College of
Engineering, Sangli.
(An Autonomous Institute)



WORKSHOP ON CLOUD COMPUTING

DOCUMENTATION



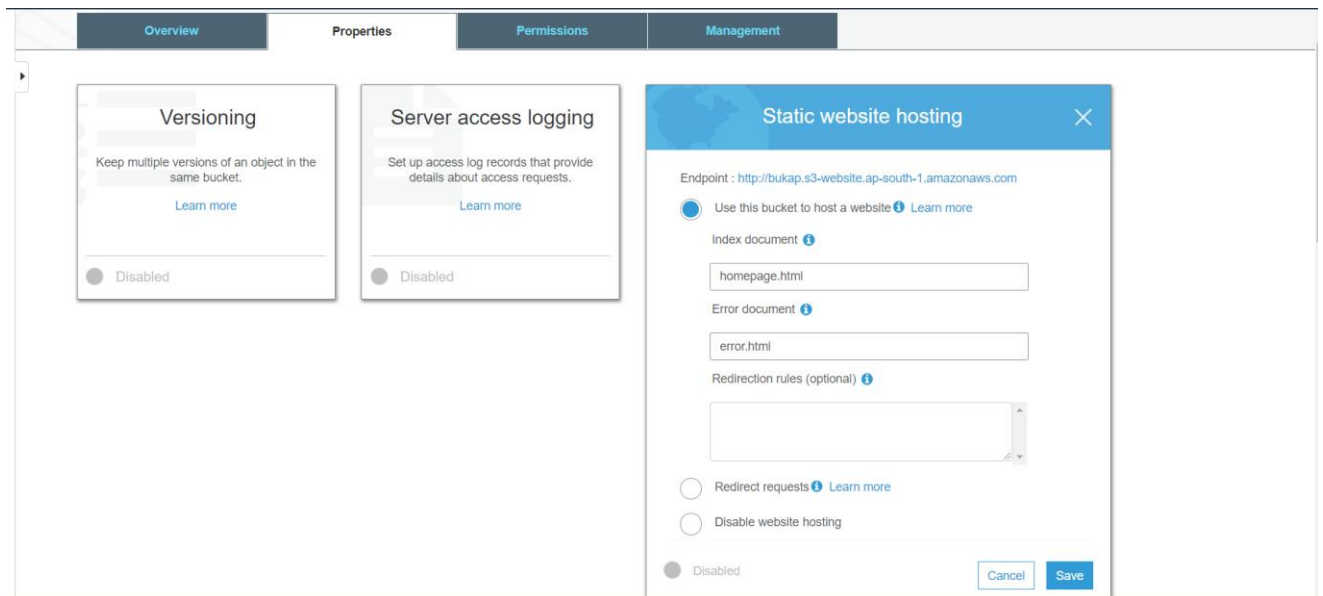
19th & 20th OCTOBER

Hosting a Static Website on Amazon S3

You can host a static website on Amazon S3. On a static website, individual webpages include static content. They might also contain client-side scripts.

A] Configure an Amazon S3 bucket for website hosting.

1. Go to Properties of Bucket and select static web hosting.
2. Enter Index (Homepage of Website) and error file (File that has to be shown when the website not works).



The screenshot shows the Amazon S3 console interface. At the top, there are four tabs: Overview, Properties, Permissions, and Management. The 'Properties' tab is selected. On the left, there are two cards: 'Versioning' and 'Server access logging', both with a 'Disabled' toggle. The main area displays the 'Static website hosting' configuration window. It shows the endpoint: `http://bukap.s3-website.ap-south-1.amazonaws.com`. There are two radio buttons: 'Use this bucket to host a website' (selected) and 'Disable website hosting'. Below the radio buttons, there are input fields for 'Index document' (containing 'homepage.html') and 'Error document' (containing 'error.html'). There is also a text area for 'Redirection rules (optional)'. At the bottom, there are two radio buttons: 'Redirect requests' (selected) and 'Disable website hosting'. There are 'Cancel' and 'Save' buttons at the bottom right.

Then upload your website content to the bucket. This bucket must have public read access. It is intentional that everyone in the world will have read access to this bucket.

B] Permissions Required for Website Access

While configuring a bucket as a website, public read access must be granted to the bucket so that people can access the website. To make bucket publicly readable, one has to disable block public access settings and write a bucket policy. If bucket contains objects that not owned by the bucket owner, then there is also need to add an object access control list (ACL) that grants everyone read access.

Edit Block Public Access Settings

By default Amazon S3 does not allow public access to account or buckets.

- **To disable block public access for a bucket configured as a static website**
 1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
 2. Select the bucket that you have configured as a static website, and choose **Edit public access setting**.
 3. 3. Clear **Block *all* public access**, and choose **Save**.

Dialog title: Edit block public access settings for selected buckets

Total buckets: 1 (Public: 0)

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block *all* public access. These settings apply only to selected buckets. AWS recommends that you turn on Block *all* public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

The Block public access settings turned on at the account level affect public access to all buckets in the account. To determine which settings are on, check your Block public access (account settings).

☐ **Block *all* public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.

Buttons: Cancel, Save

4. In the confirmation box, enter **confirm**, and then choose **Confirm**.

Edit block public access settings for selected buckets

Updating the Amazon S3 block public access settings affects all selected buckets. This may result in some buckets and objects becoming public.

To confirm the settings, type *confirm* in the field.

CancelConfirm

- **To add a bucket policy**

To make the objects in your bucket publicly readable, you must write a bucket policy that grants everyone `s3:GetObject` permission.

1. Choose the bucket that you have configured as a static website.
2. Choose **Permissions**.
3. Choose **Bucket Policy**.
4. In the **Bucket policy editor**, add a bucket policy, and choose **Save**. (By using policy generator create bucket policy.)



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 *

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 1 Action(s) Selected ☐ All Actions ("*")

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

ARN should follow the following format: arn:aws:s3:::<bucket_name>/<key_name>.
Use a comma to separate multiple values.

[Add Conditions \(Optional\)](#)

[Add Statement](#)

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": "Policy1571907721798",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1571907716489",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bukap",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services.

[Close](#)

5. Add /* at end of Resource in policy if Principle is for all(*).
6. Add this bucket policy and hit save.

Website URL is present in Static Website Hosting Section.

Website is Hosted Successfully.