AMITY UNIVERSITY

UTTAR PRADESH

AMITY SCHOOL OF ENGINEERING & TECHNOLOGY

Department of CSE

B. Tech (CSE) / (Sem-V)

Cloud Computing Practitioner Lab Test, Oct-2023

CSE314

Date: 03-10-23

Answer to any 2 Questions

Q1. Use AWS console to perform the following activity:

- **Launch a free tier EC2 instance in a specific availability zone.**
- **After launching EC2 instance add extra storage of 2GB to same instance.**
- **Add Load Balancing feature to it.**
- **To prevent over usage or to generate alerts add Cloud Watch and ensure that running instance should be stopped at a particular threshold value.**
- **Create a snapshot of the above one.**

Q2. Create a classical Load Balancer and manage the load on two different instances by demonstrating it.

Q3. Create a bucket and perform:

- **Transferring Object to the Bucket.**
- **Enabling retention period for the object transferred.**
- **Testing the object lock feature by removing the file**

	Marks Allotted	Marks Obtained
Aim of Program	5	
Source Code	20	
O/p and Result Verification	5	
Total	**30**	

Instructions:

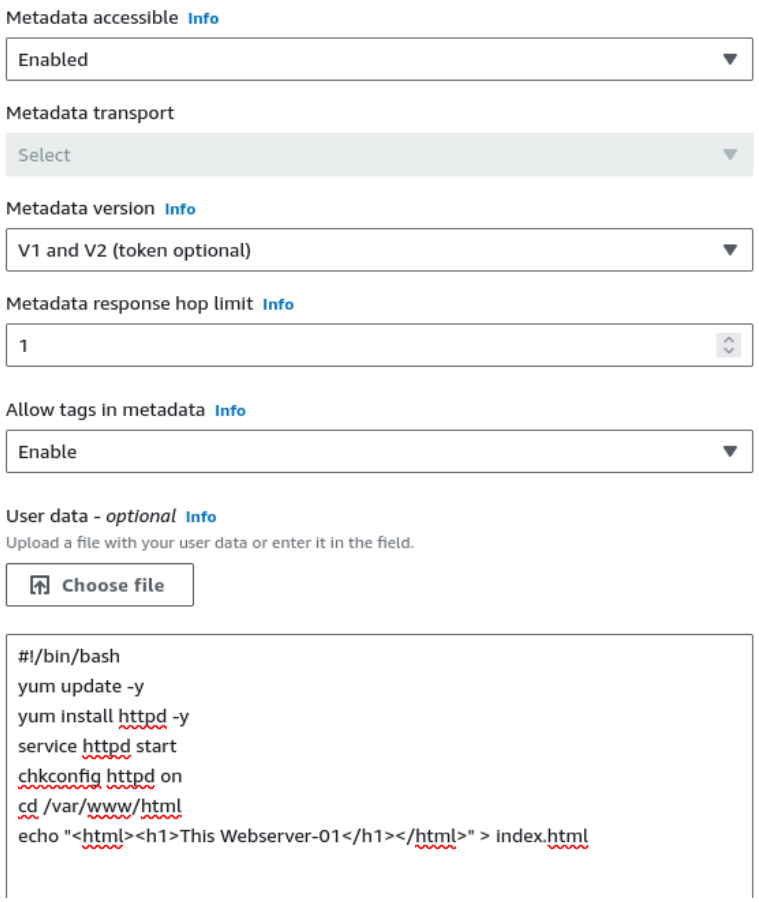
1. **Perform the Experiment on your machine and write down the steps along with the screenshots**
2. **The steps should be proper and written in your own words justifying your work.**
3. **Once Completed, convert the doc file to pdf and upload over the given link.**

Program : **B. Tech (CSE)**
Course Title / Code : **Cloud Computing Practitioner (CSE314)**
Semester / Section : **V / CSE6-X**
Academic Session : **2023-2024**
Name of Student : **Siddharth Johri**
Enroll. No. : **A2305221155**
Date : **03-Oct-2023**

Q2:

Pre configurations:

- Two EC2 instances were made and a web server was hosted on both of them using the following advanced settings:

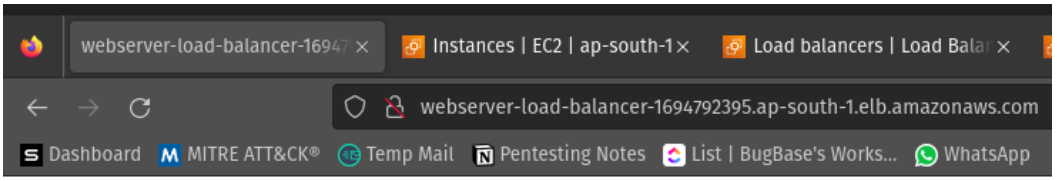


-
- For the instances, one of them will have Webserver-01 and the other will have Webserver-02 for demonstration purposes.
- Other than this, the configuration of the Instance will be having the usual settings for Name, Key-pair, Security group, AMI, architecture and instance type.

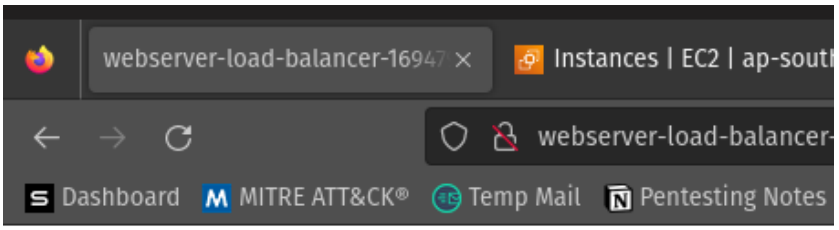
Creating a classic load balancer on the two instances.

1. Create two instances with a web page hosted on their port 80
2. Create a load balancer by visiting the load balancers tab from the EC2 menu
3. Choose Classical Load Balancer.
4. Set the Load balancer to be Internet Facing
5. Select the particular VPC and availability zones in which the instances are present.
6. Set the security groups. Preferably the same one used for the instances and setup the port forwarding. (eg. port 80 to port 80)
7. Add instances to the load balancer
8. Deploy/Create the Load balancer

Deployed Load Balancer works Properly and web traffic is divided between the two instances.

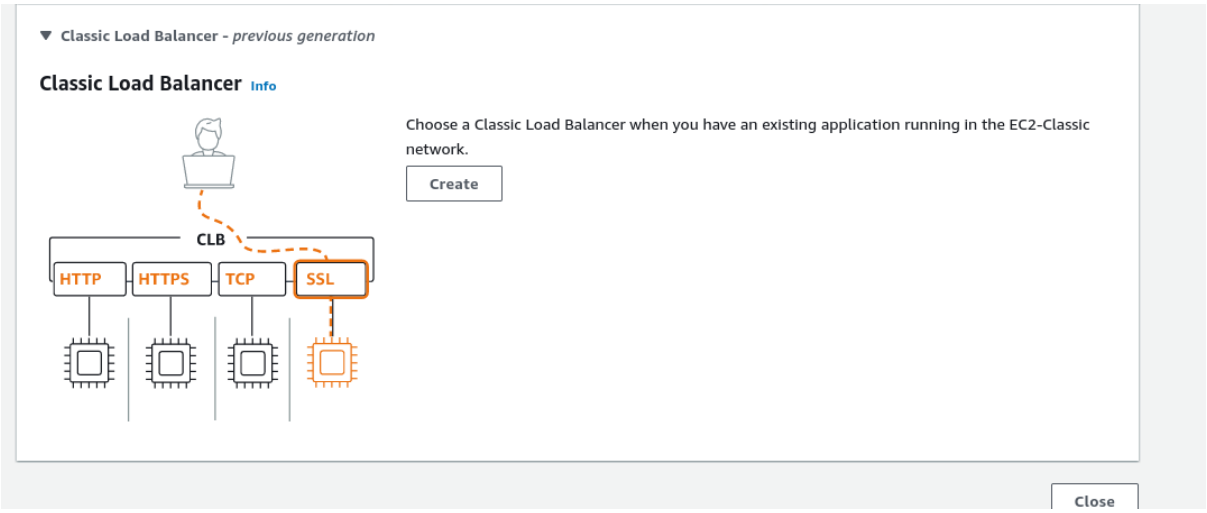


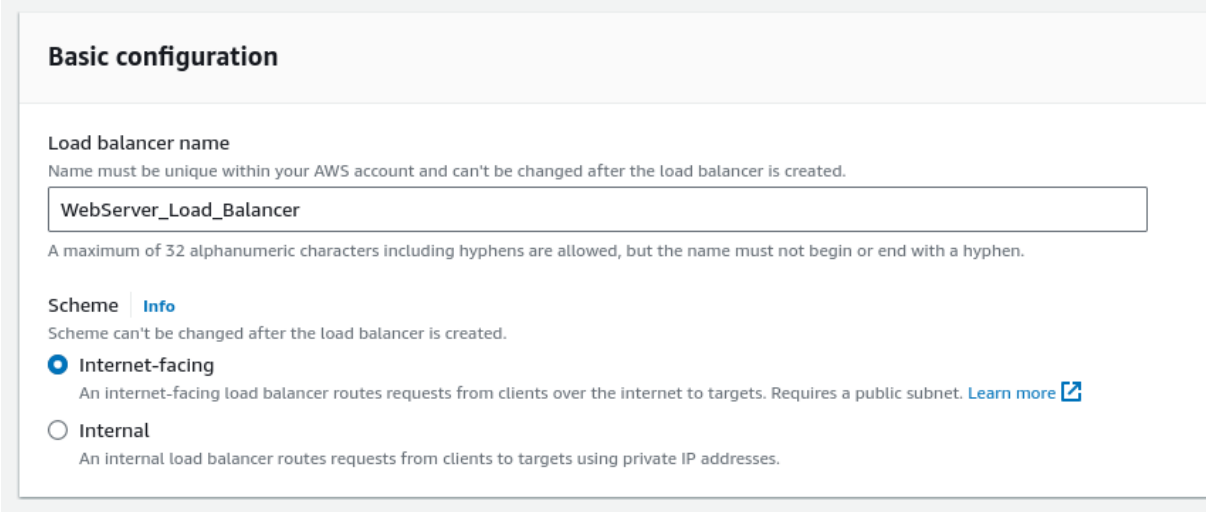
This Webserver-01



This Webserver-02

Screenshots for load balancer settings:





Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your network settings.

VPC Info

Select the virtual private cloud (VPC) for your targets or you can create a new VPC. Only VPCs with an internet gateway are available for selection. The selec
after the load balancer is created. When selecting a VPC for your load balancer, ensure each subnet has a CIDR block with at least a /27 bitmask and at least 8 fi

-
vpc-003b0eae18a021b44
IPv4: 172.31.0.0/16

Mappings

Select at least one Availability Zone and one subnet for each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic
Availability Zones. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

- [x] **ap-south-1a (aps1-az1)**

Subnet

subnet-0f8b4a41d89b1b7f9

IPv4 address

Assigned by AWS

- [ ] **ap-south-1b (aps1-az3)**
- [ ] **ap-south-1c (aps1-az2)**

Security groups Info

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups

Select up to 5 security groups

launch-wizard-5
sg-0dd56d600569fdc29 VPC: vpc-003b0eae18a021b44

Listeners and routing Info

A listener is a process that checks for connection requests using the protocol and port you configure. The settings you define for a listener determine how the load balancer r
its registered targets.

▼ Listener **HTTP:80** Instance **HTTP:80**

Listener protocol	Listener port	Instance protocol	Instance port
HTTP	80	HTTP	80
	1-65535		1-65535

Add listener

Add instances

Select EC2 instances to register to your load balancer. Requests will be routed to registered instances that meet the health check requirements. For maximum fault tolerance demand on your instances changes, you can register or deregister instances without disrupting the flow of requests to your application. Learn more

VPC

vpc-003b0eae18a021b44

Available instances (2/4)

Filter available instances by property or value

	Instance ID	Name	State	Security groups
☐	i-019e6eae001b47f2f	Test_EC2_1	Stopped	launch-wizard-1
☐	i-0a0348e924346d174	Test_EC2_Linux	Stopped	launch-wizard-2
☑	i-008ccc449d2403de2	EC2_WS1	Running	launch-wizard-3
☑	i-00b9e61ad96bf2e7b	EC2_WS2	Running	launch-wizard-4

Timeout (draining interval)

Load balancer: WebServer-Load-Balancer

Description | Instances | Health check | Listeners | Monitoring | Tags | Migration

Basic Configuration

Name	WebServer-Load-Balancer	**Creation time**	October 3, 2023 at 2:00:35 PM UTC+5:30
*** DNS name**	WebServer-Load-Balancer-1694792395.ap-south-1.elb.amazonaws.com (A Record)	**Hosted zone**	ZP97RAFLXTNZK
Type	Classic (Migrate Now)	**Status**	2 of 2 instances in service
Scheme	internet-facing	**VPC**	vpc-003b0eae18a021b44
Availability Zones	subnet-0f8b4a41d89b1b7f9 - ap-south-1a		

Port Configuration

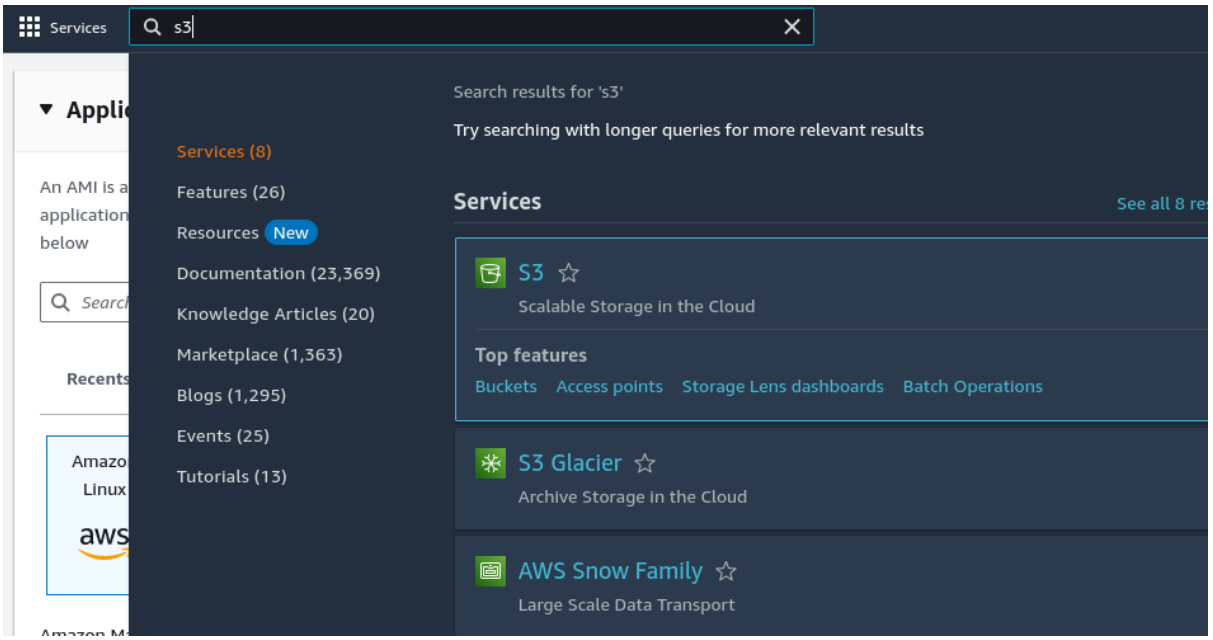
Port Configuration	**80 (HTTP) forwarding to 80 (HTTP)** Stickiness: Disabled Edit stickiness

Security

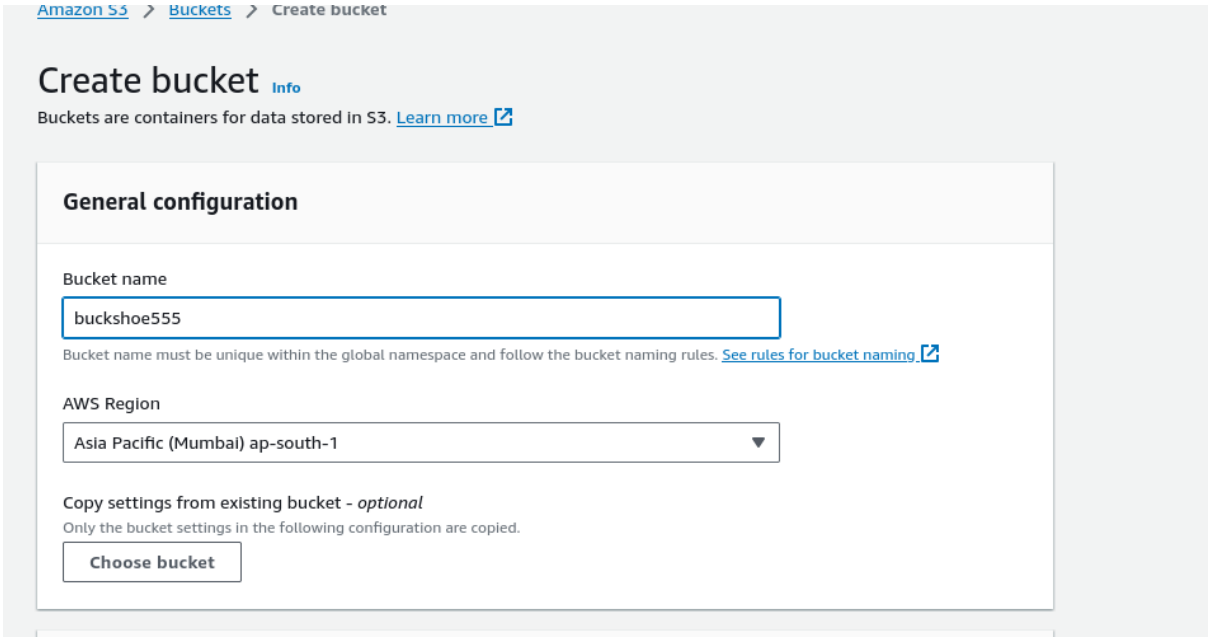
Source Security Group	sg-0dd56d600569fdc29 , **launch-wizard-5** • launch-wizard-5 created 2023-09-02T04:45:56.041Z

Q3.

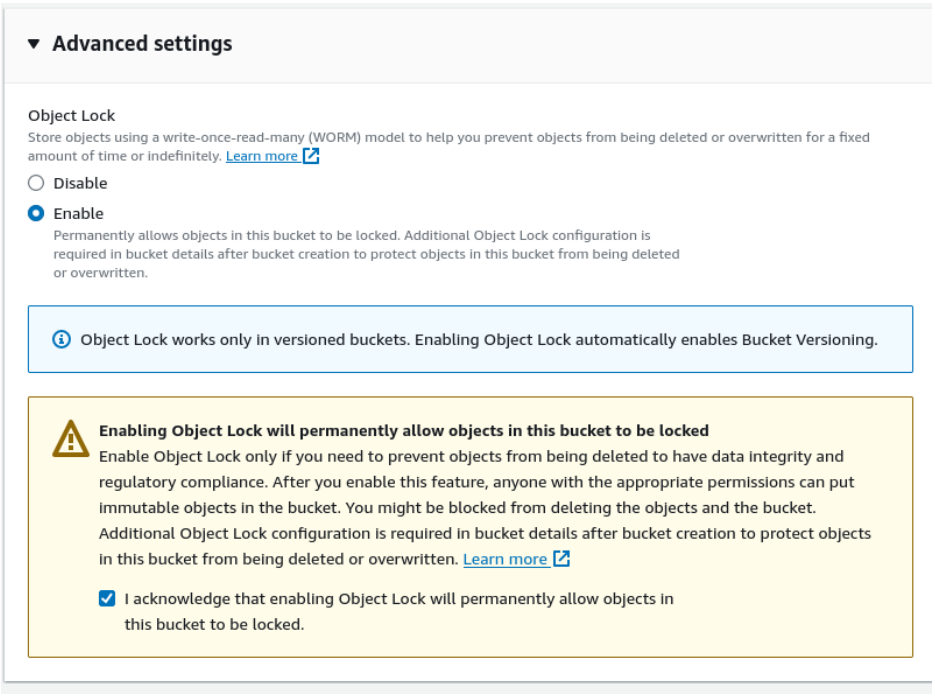
Traverse to the S3 dashboard



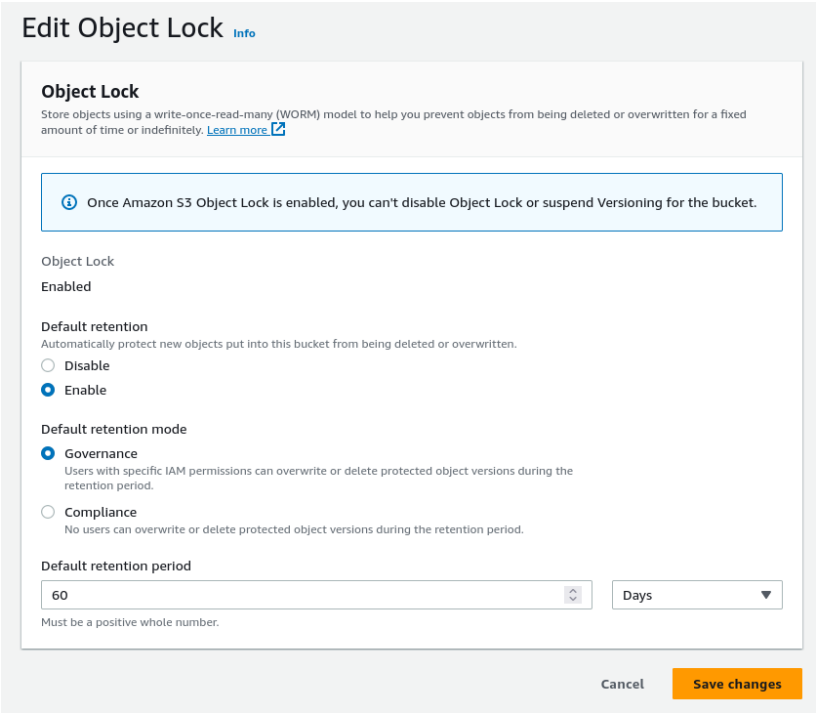
Click on Create Bucket and give the bucket a name.



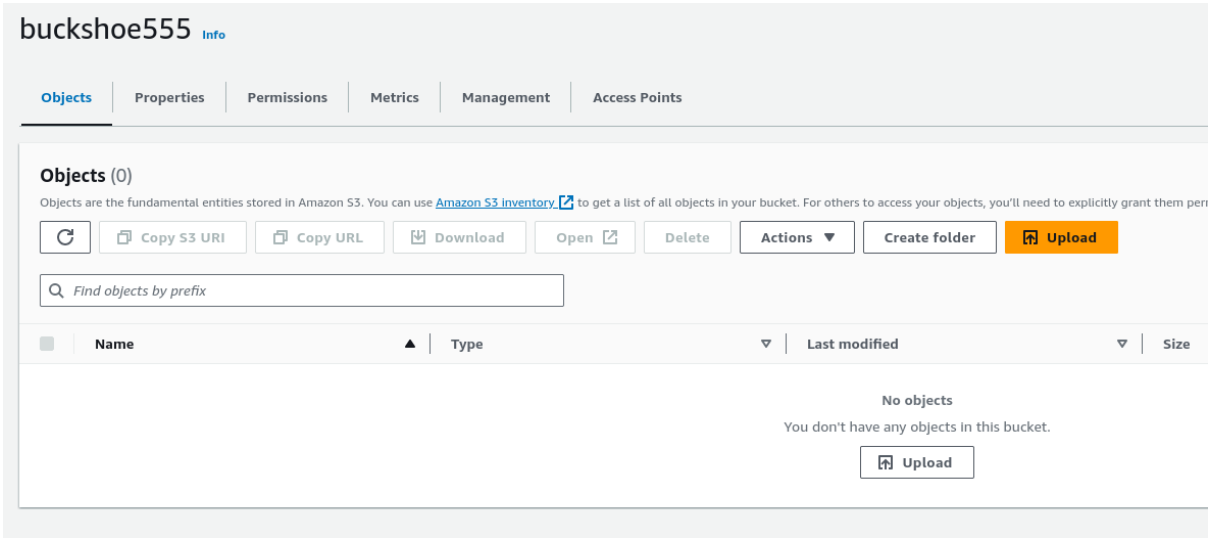
Object Lock can be enabled from the Advanced Settings

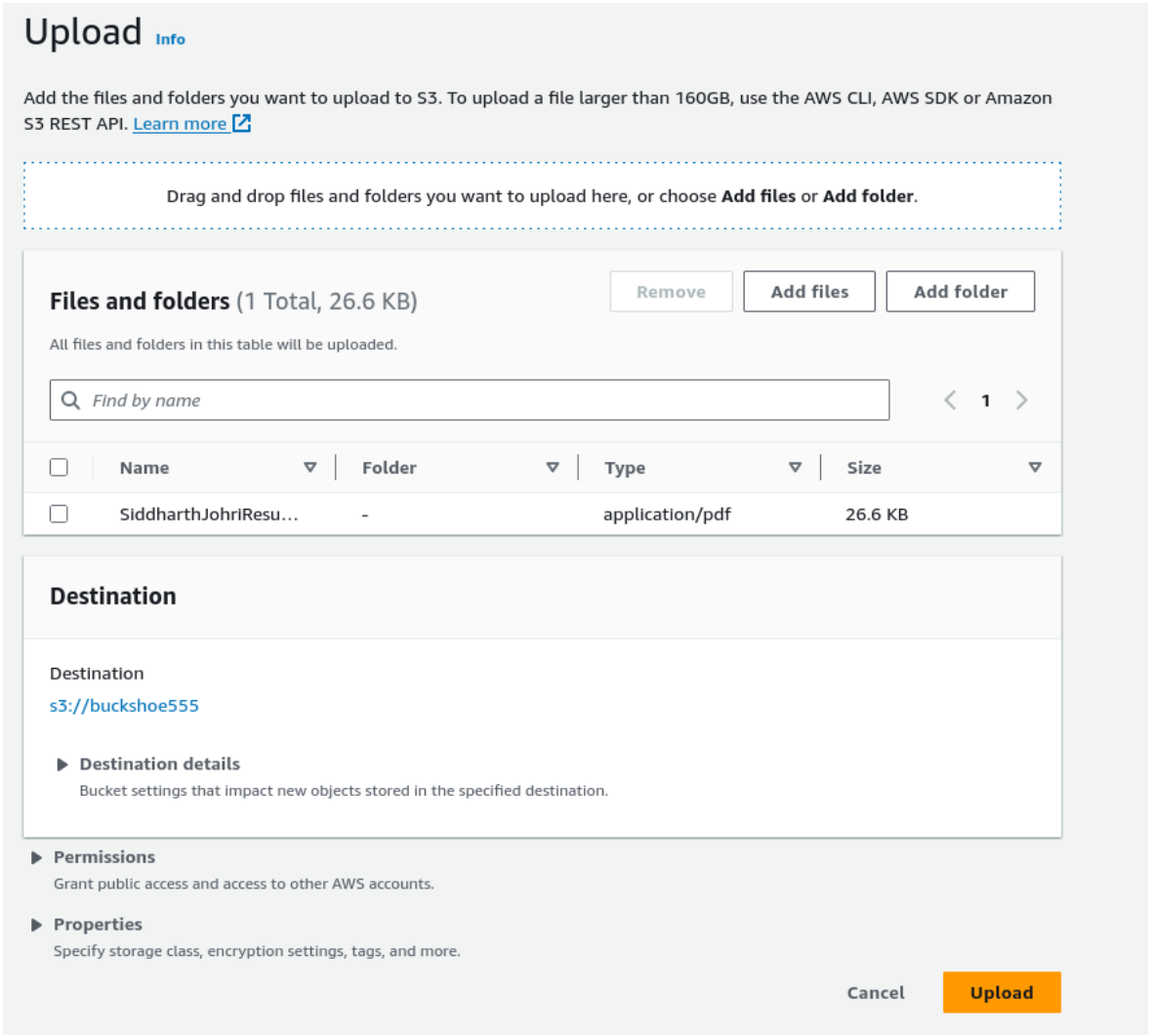


Retention Policy for the Object Lock can be set using the Bucket's Properties Tab

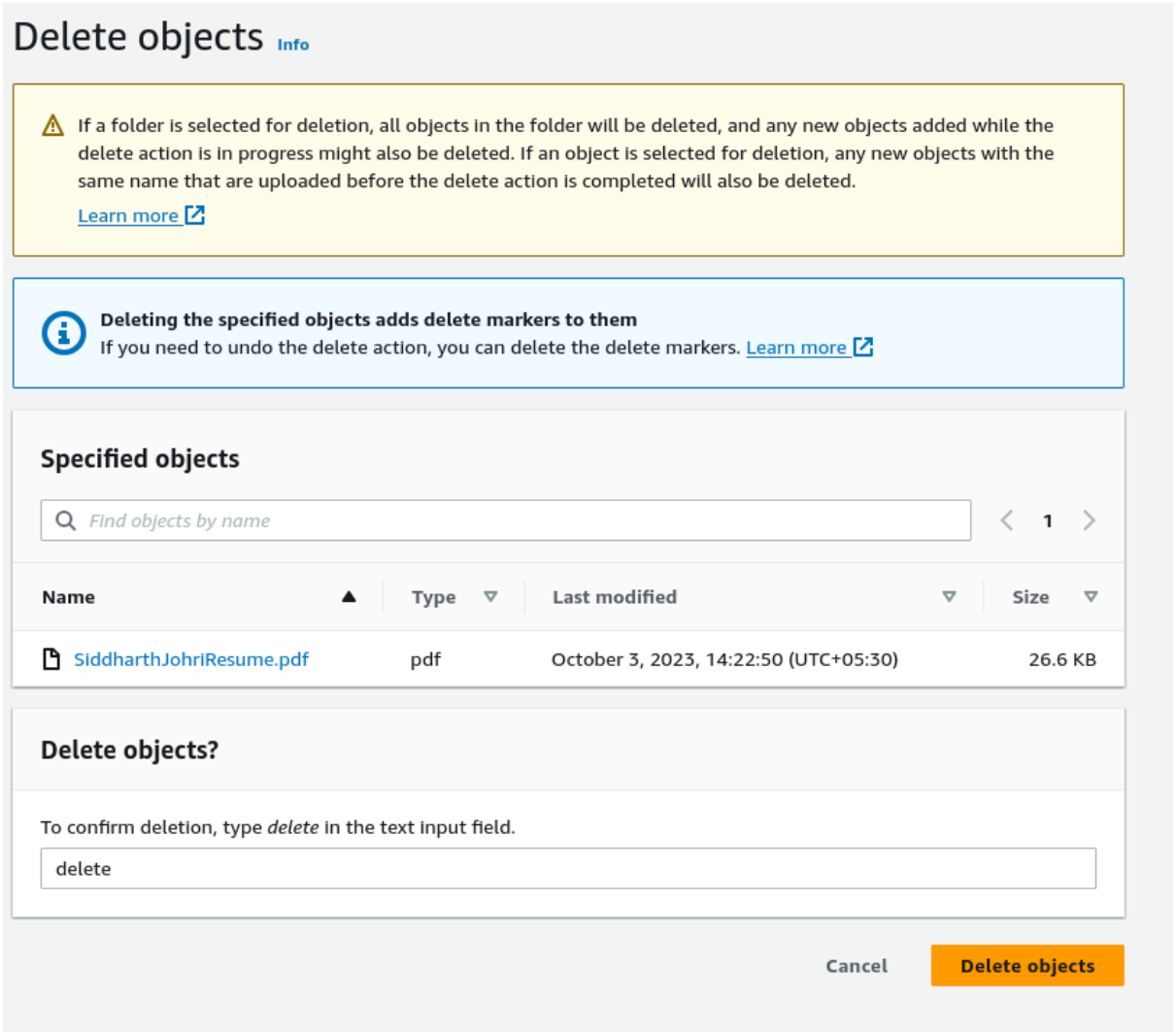


Visit the bucket and upload an item

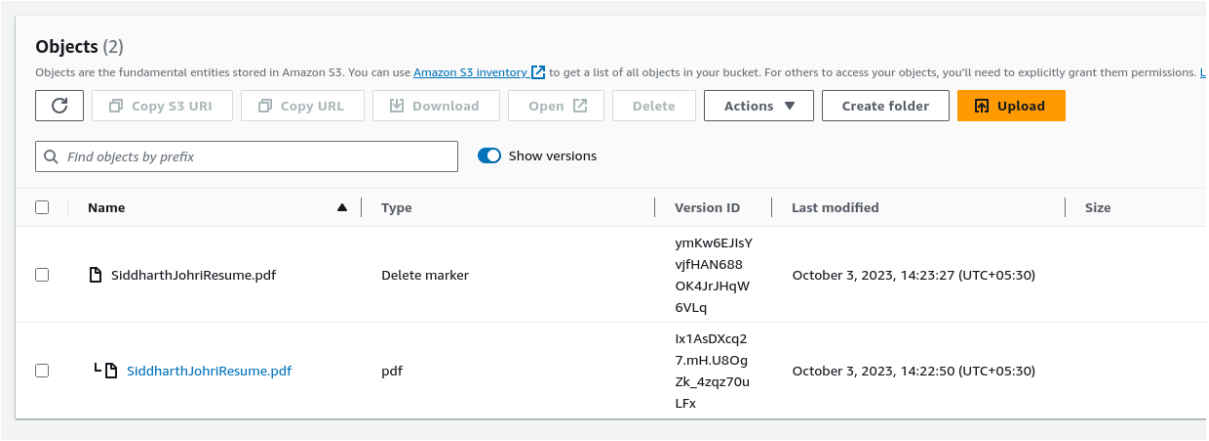




Deleting the added object.



Enable the show versions option on the bucket and see the file there.



Can still be successfully accessed since object lock was enabled.