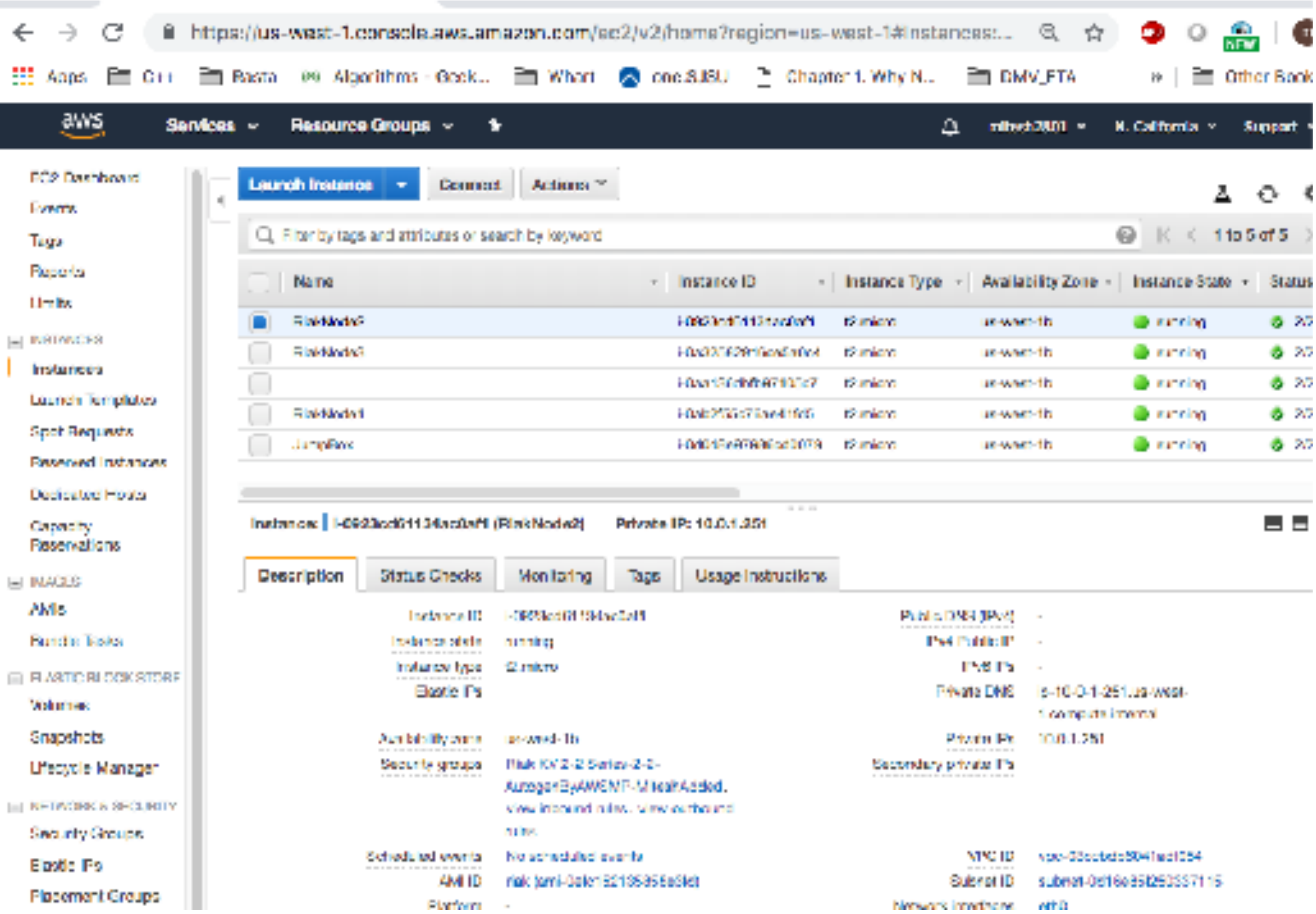
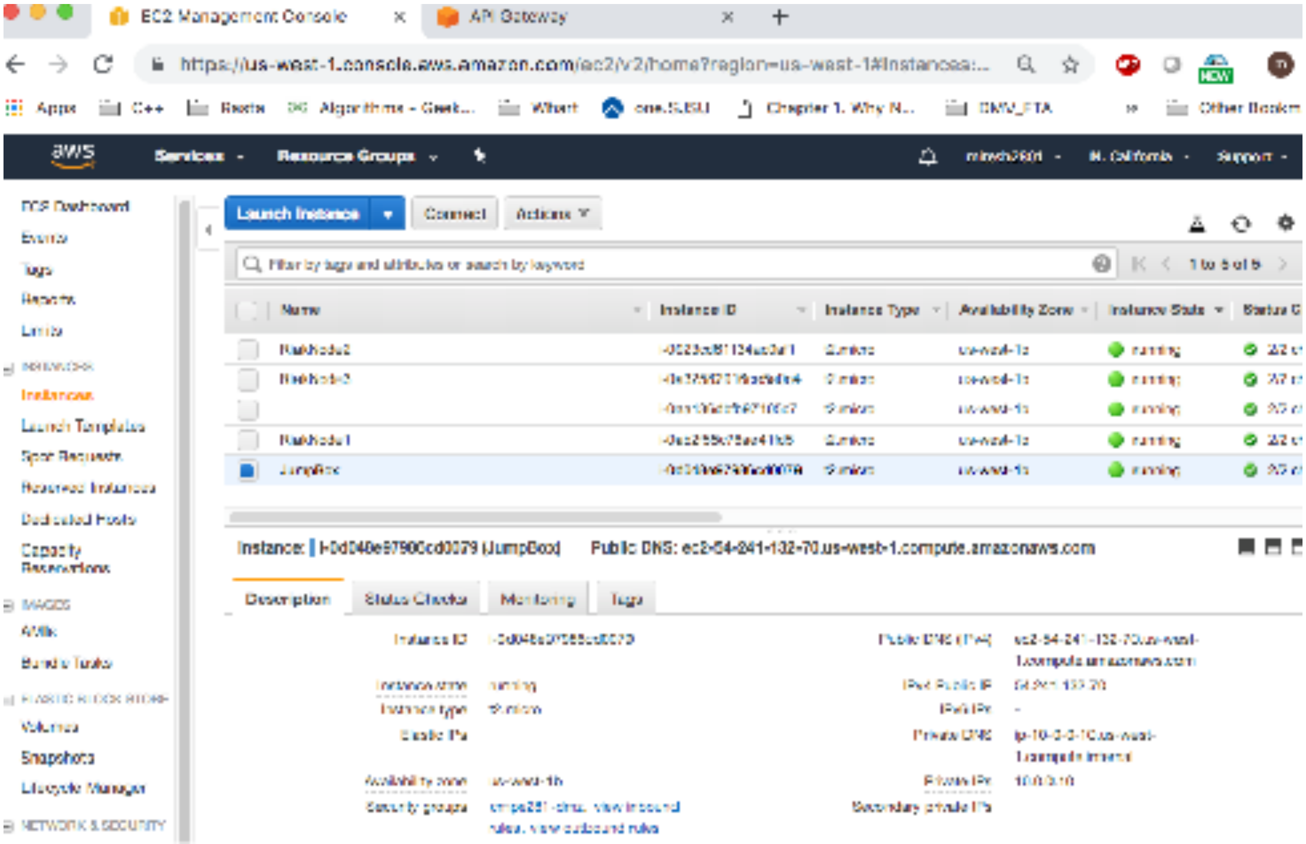
A. Risk Cluster on EC2



	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status
■	RiskNode2	i-0923[illegible]	t2.micro	us-west-1b	● running	2/2
□	RiskNode3	i-0a3[illegible]	t2.micro	us-west-1b	● running	2/2
□		i-0aa1[illegible]	t2.micro	us-west-1b	● running	2/2
□	RiskNode1	i-0ab2[illegible]	t2.micro	us-west-1b	● running	2/2
□	JumpBox	i-0d04[illegible]	t2.micro	us-west-1b	● running	2/2

Instance: i-0923bcd61134ac0af1 (RiskNode2) Private IP: 10.0.1.251

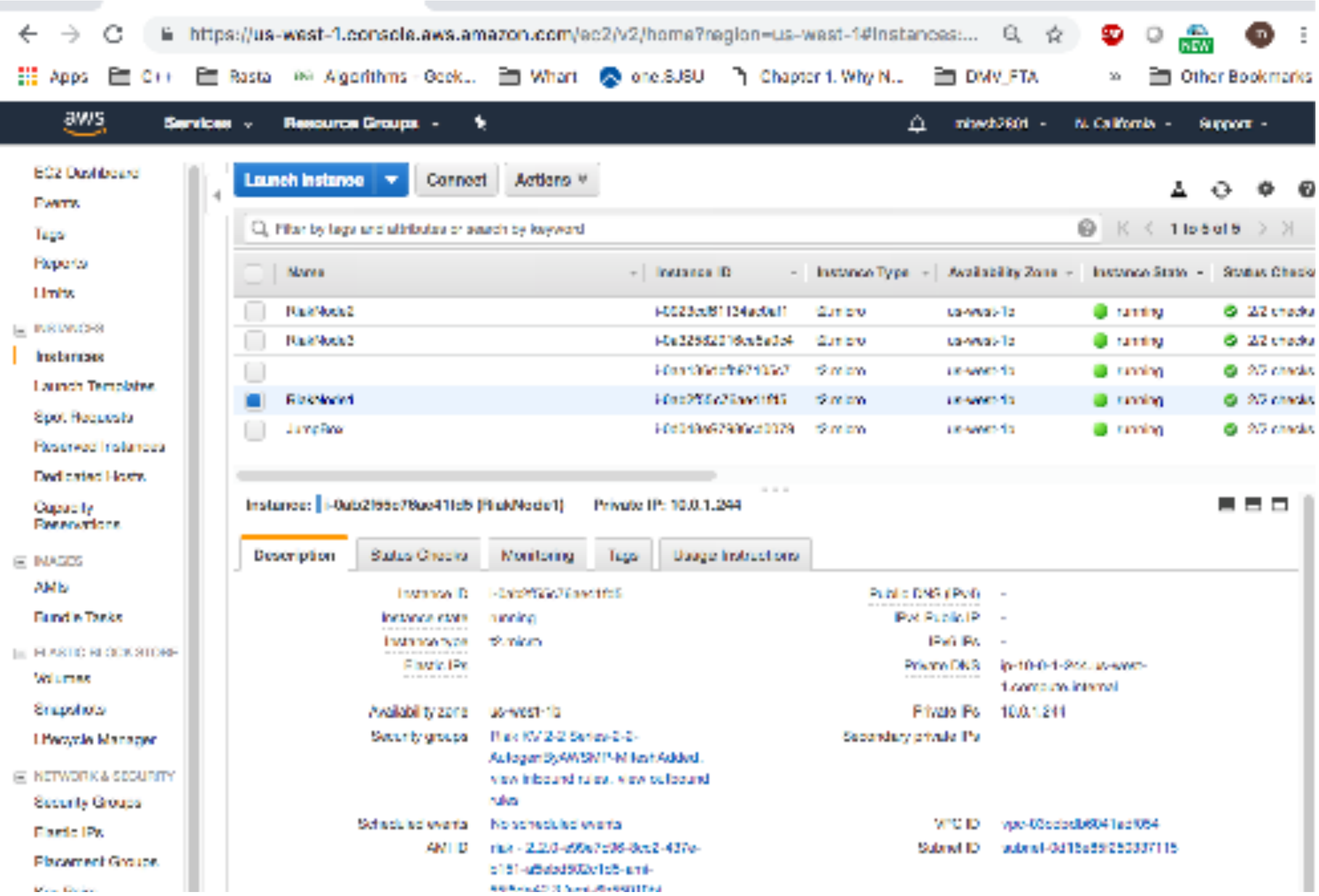
Instance ID	i-[illegible]	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	-
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-0-1-251.us-west-1.compute.internal
Availability zone	us-west-1b	Private IPs	10.0.1.251
Security groups	Risk [illegible]-AutogenByAWSMP-[illegible]. view inbound rules. view outbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-[illegible]
AMI ID	risk (ami-[illegible])	Subnet ID	subnet-[illegible]
Platform	-	Network interfaces	eth0



	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status C
□	RiskNode2	i-0923[illegible]	t2.micro	us-west-1b	● running	2/2 c
□	RiskNode3	i-0a3[illegible]	t2.micro	us-west-1b	● running	2/2 c
□		i-0aa1[illegible]	t2.micro	us-west-1b	● running	2/2 c
□	RiskNode1	i-0ab2[illegible]	t2.micro	us-west-1b	● running	2/2 c
■	JumpBox	i-0d040e[illegible]	t2.micro	us-west-1b	● running	2/2 c

Instance: i-0d040e97900cd0079 (JumpBox) Public DNS: ec2-54-241-132-70.us-west-1.compute.amazonaws.com

Instance ID	i-0d040e[illegible]	Public DNS (IPv4)	ec2-54-241-132-70.us-west-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	54.241.132.70
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-0-0-10.us-west-1.compute.internal
Availability zone	us-west-1b	Private IPs	10.0.0.10
Security groups	cmpe281-[illegible]. view inbound rules. view outbound rules	Secondary private IPs	



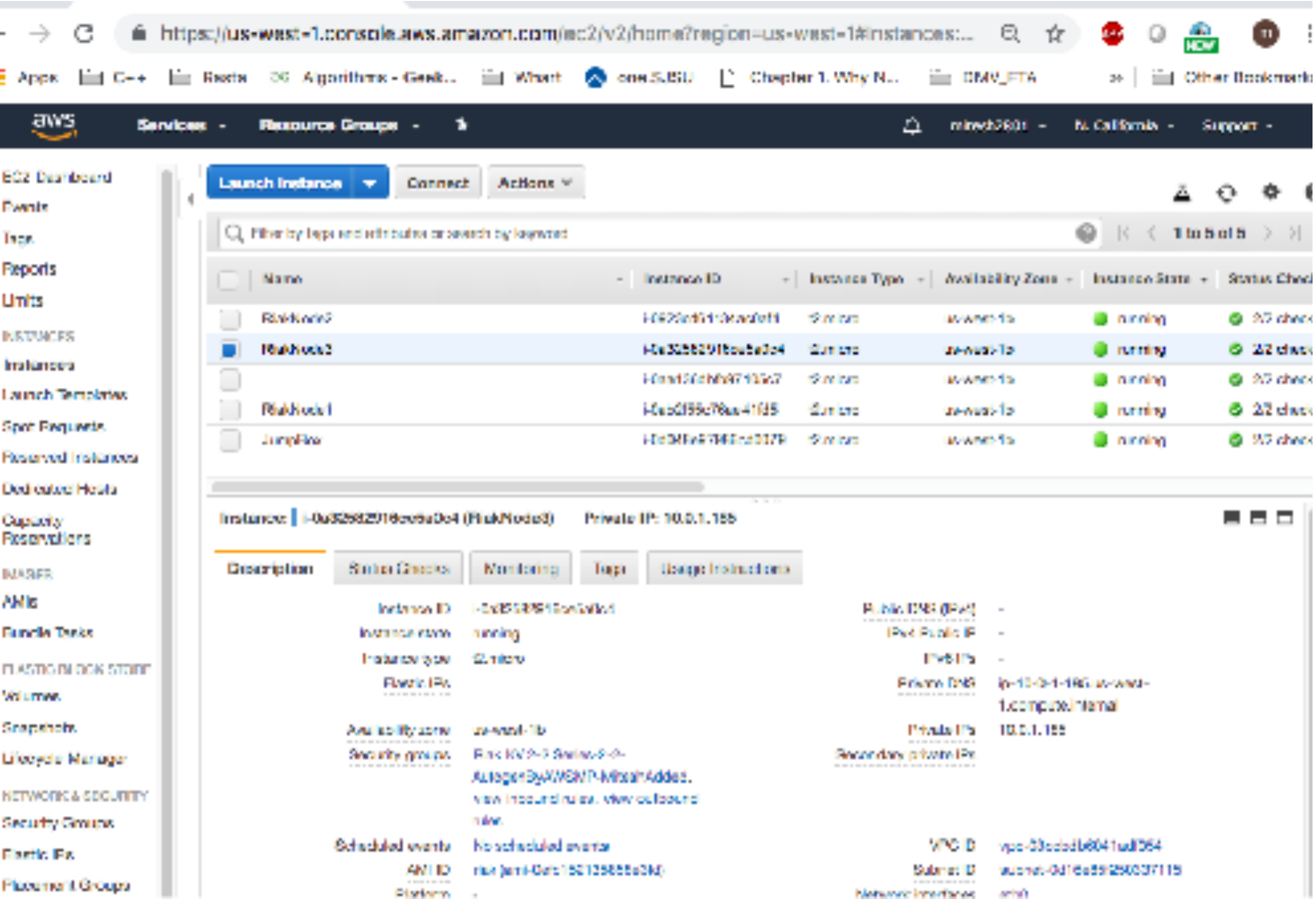
https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#Instances:...

Apps | C++ | Rasta | Algorithms - Geek... | Whart | one.SJSU | Chapter 1. Why N... | DMV_FTA | » | Other Bookmarks

	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
□	RiakNode2	i-0023a81124ada11	t2.micro	us-west-1c	running	2/2 checks
□	RiakNode3	i-0a3268291 6ce5a0e4	t2.micro	us-west-1c	running	2/2 checks
□		i-0ad10fdcf6f7 1357	t2.micro	us-west-1b	running	2/2 checks
☑	RiakNode1	i-0ab2f55c78ae41fd5	t2.micro	us-west-1b	running	2/2 checks
□	JumpBox	i-0d149a6790fed3379	t2.micro	us-west-1b	running	2/2 checks

Instance: i-0ab2f55c78ae41fd5 (RiakNode1) Private IP: 10.0.1.244

Instance ID	i-0ab2f55c78ae41fd5	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	-
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-0-1-244.us-west-1.compute.internal
Availability zone	us-west-1b	Private IPs	10.0.1.244
Security groups	Riak KV 2-2 Series-2-2-AutogenByAWSMP-N last Added. view inbound rules. view outbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-00cdcdb6041ad064
AMI ID	riak - 2.2.3-d9fa7c96-8ce2-437e-a151-a8bdd902c1d5-ami-...	Subnet ID	subnet-0d15a5925a337115



https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#Instances:...

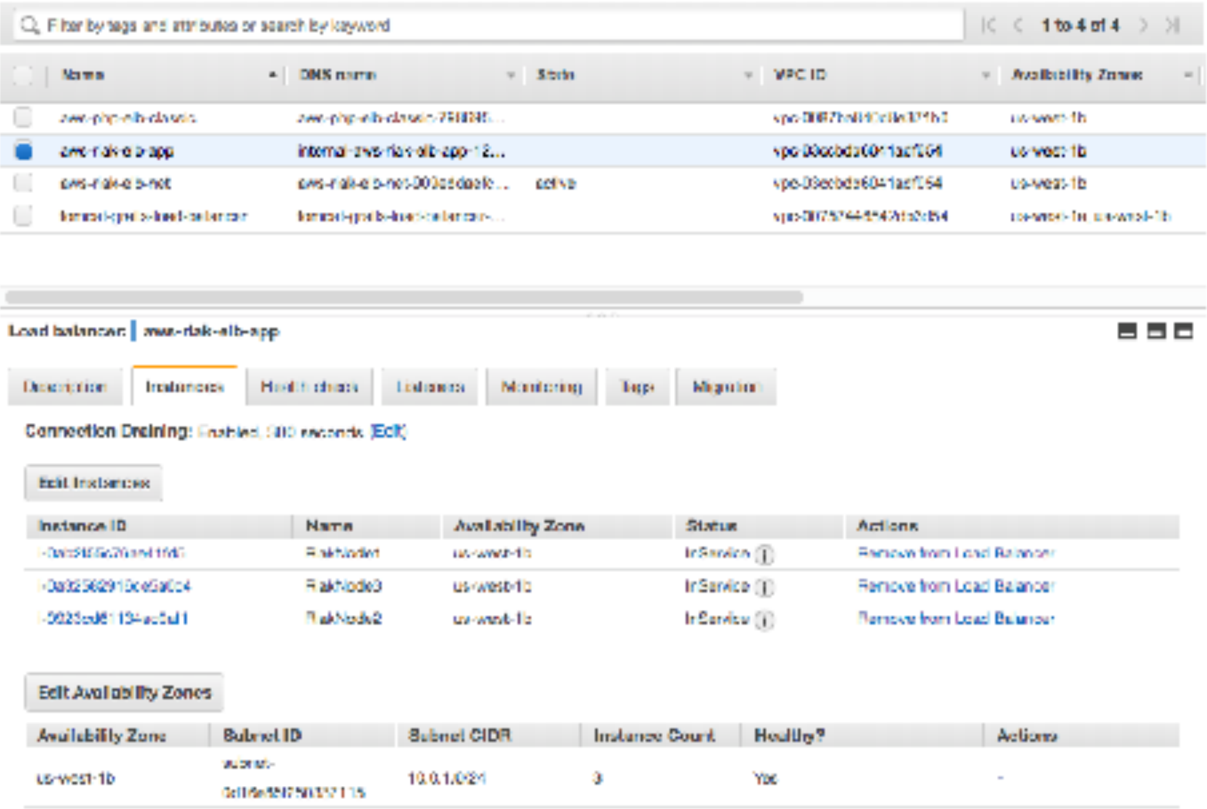
Apps | C++ | Rasta | Algorithms - Geek... | Whart | one.SJSU | Chapter 1. Why N... | DMV_FTA | » | Other Bookmarks

	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
□	RiakNode2	i-0623a81124ada011	t2.micro	us-west-1b	running	2/2 checks
☑	RiakNode3	i-0a3268291 6ce5a0e4	t2.micro	us-west-1c	running	2/2 checks
□		i-0ad10fdcf6f7 1357	t2.micro	us-west-1b	running	2/2 checks
□	RiakNode1	i-0ab2f55c78ae41fd5	t2.micro	us-west-1c	running	2/2 checks
□	JumpBox	i-0d149a6790fed3379	t2.micro	us-west-1b	running	2/2 checks

Instance: i-0a3268291 6ce5a0e4 (RiakNode3) Private IP: 10.0.1.165

Instance ID	i-0a3268291 6ce5a0e4	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	-
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-0-1-165.us-west-1.compute.internal
Availability zone	us-west-1c	Private IPs	10.0.1.165
Security groups	Riak KV 2-2 Series-2-2-AutogenByAWSMP-Mitesh Added. view inbound rules. view outbound rules.	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-00cdcdb6041ad064
AMI ID	riak (ami-0a51529858e3d)	Subnet ID	subnet-0d15a5925a337115
Platform	-	Network interfaces	eth0

B. Network Load Balancer



Filter by tags and attributes or search by keyword — 1 to 4 of 4

☐	Name	DNS name	State	VPC ID	Availability Zones
☐	aws-php-elb-classic	aws-php-elb-classic-798895...		vpc-0087ba840d8e371b0	us-west-1b
●	aws-riak-elb-app	internal-aws-riak-elb-app-12...		vpc-03ccbdb6041adf264	us-west-1b
☐	aws-riak-elb-net	aws-riak-elb-net-903eddaefe...	active	vpc-03ccbdb6041adf264	us-west-1b
☐	tomcat-grails-load-balancer	tomcat-grails-load-balancer-...		vpc-00757446542db3d54	us-west-1a, us-west-1b

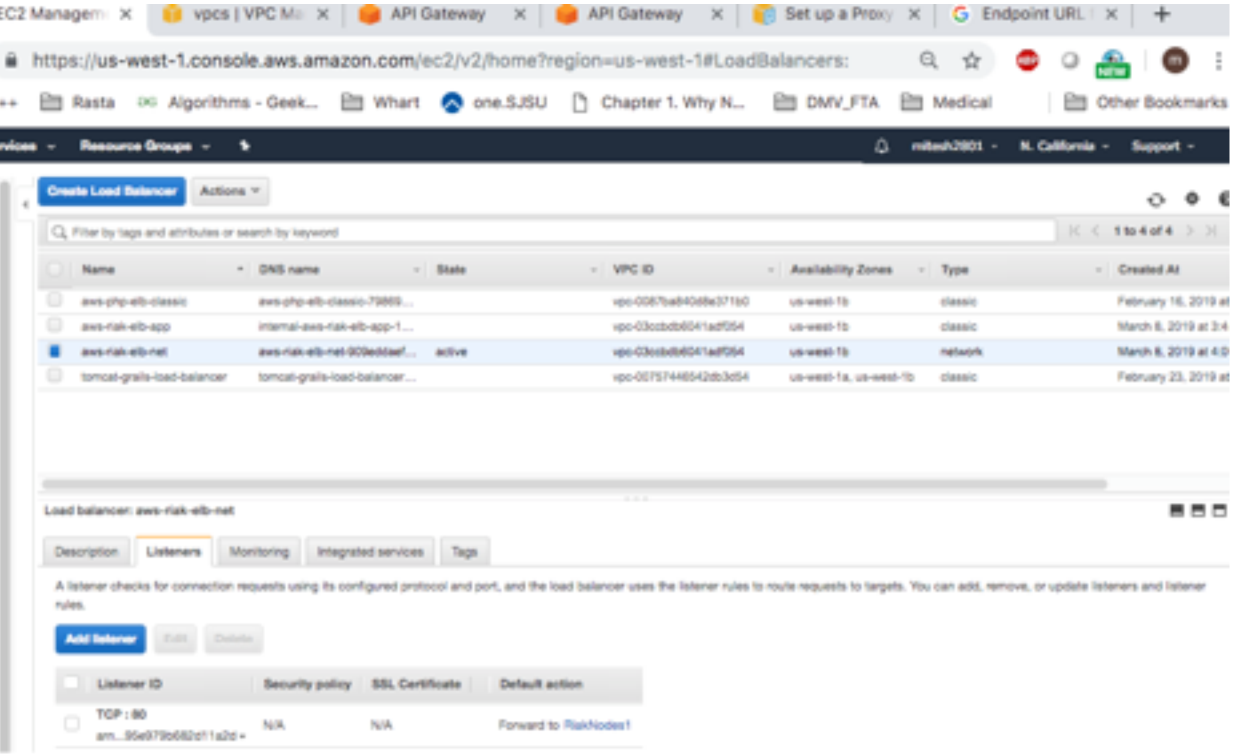
Load balancer: aws-riak-elb-app

Connection Draining: Enabled, 300 seconds (Edit)

Instance ID	Name	Availability Zone	Status	Actions
i-0a0815a70aed1f45	RiakNode1	us-west-1b	InService ⓘ	Remove from Load Balancer
i-0a02569915ce6a0c4	RiakNode3	us-west-1b	InService ⓘ	Remove from Load Balancer
i-0925cd8113-ac5a11	RiakNode2	us-west-1b	InService ⓘ	Remove from Load Balancer

Availability Zone	Subnet ID	Subnet CIDR	Instance Count	Healthy?	Actions
us-west-1b	subnet- 0e116e5675037115	10.0.1.0/24	3	Yes	-

B.2 Network Load Balancer connection to Risk Cluster



Filter by tags and attributes or search by keyword — 1 to 4 of 4

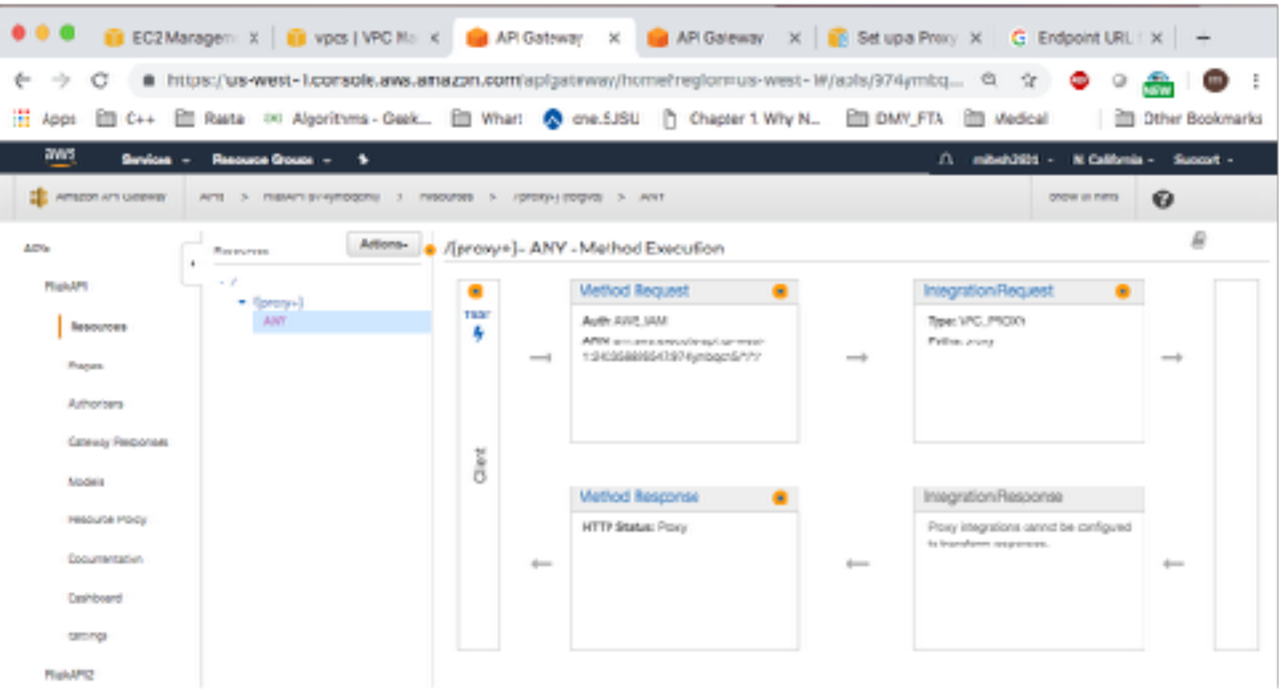
☐	Name	DNS name	State	VPC ID	Availability Zones	Type	Created At
☐	aws-php-elb-classic	aws-php-elb-classic-79869...		vpc-0087ba840d8e371b0	us-west-1b	classic	February 16, 2019 at
☐	aws-riak-elb-app	internal-aws-riak-elb-app-1...		vpc-03ccbdb6041adf264	us-west-1b	classic	March 6, 2019 at 3:4
■	aws-riak-elb-net	aws-riak-elb-net-903eddaef...	active	vpc-03ccbdb6041adf264	us-west-1b	network	March 6, 2019 at 4:0
☐	tomcat-grails-load-balancer	tomcat-grails-load-balancer...		vpc-00757446542db3d54	us-west-1a, us-west-1b	classic	February 23, 2019 at

Load balancer: aws-riak-elb-net

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and listener rules.

☐	Listener ID	Security policy	SSL Certificate	Default action
☐	TCP : 80 arn...95e979b682d11a2d ▸	N/A	N/A	Forward to RiakNodes1

C. API Gateway Configs



/{proxy+} - ANY - Method Execution

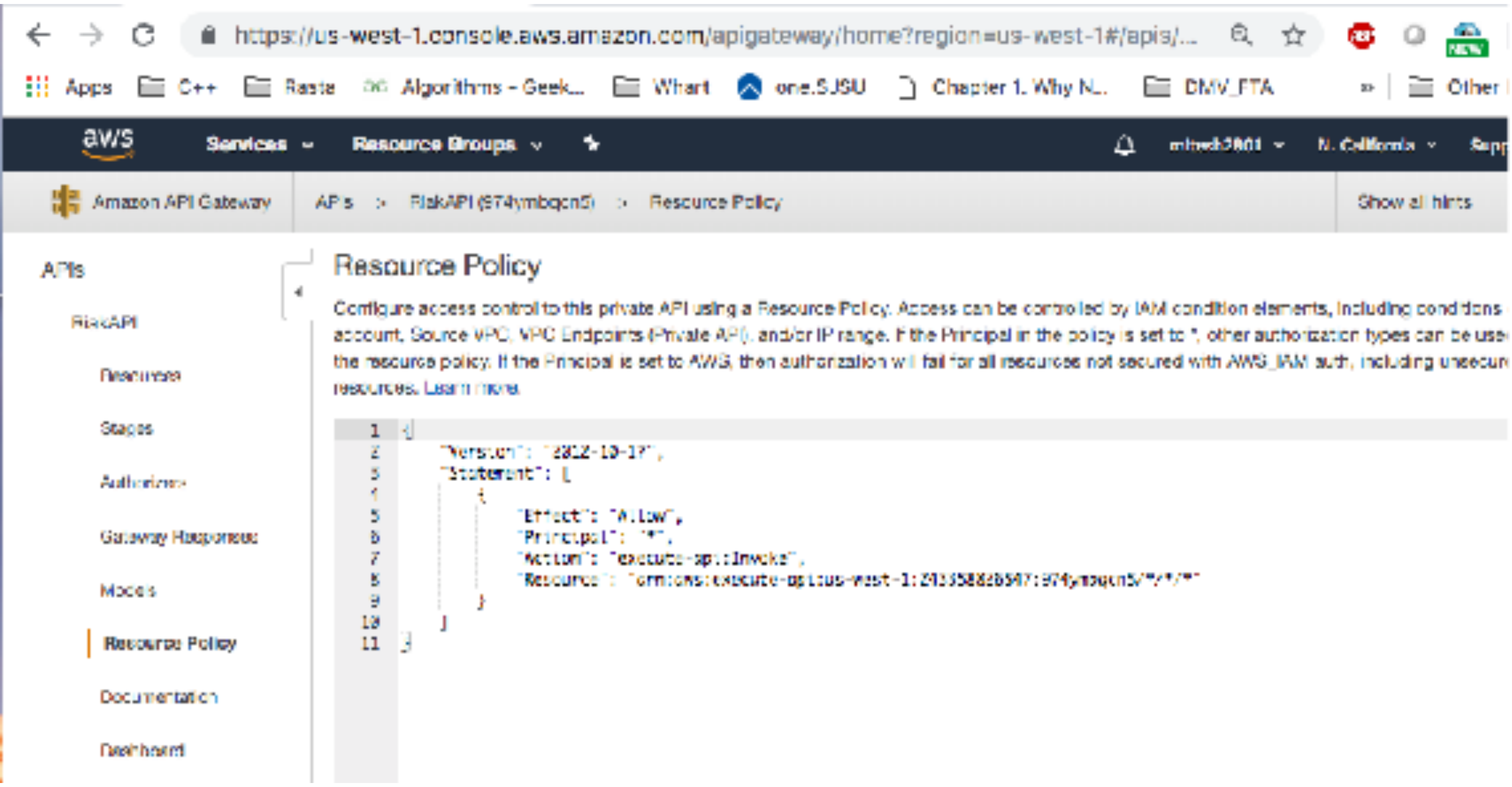
Method Request
Auth: AWS_IAM

Integration Request
Type: VPC_PROXY

Method Response
HTTP Status: Proxy

Integration Response
Proxy integrations cannot be configured to transform responses.

C.2 API Resource Policy

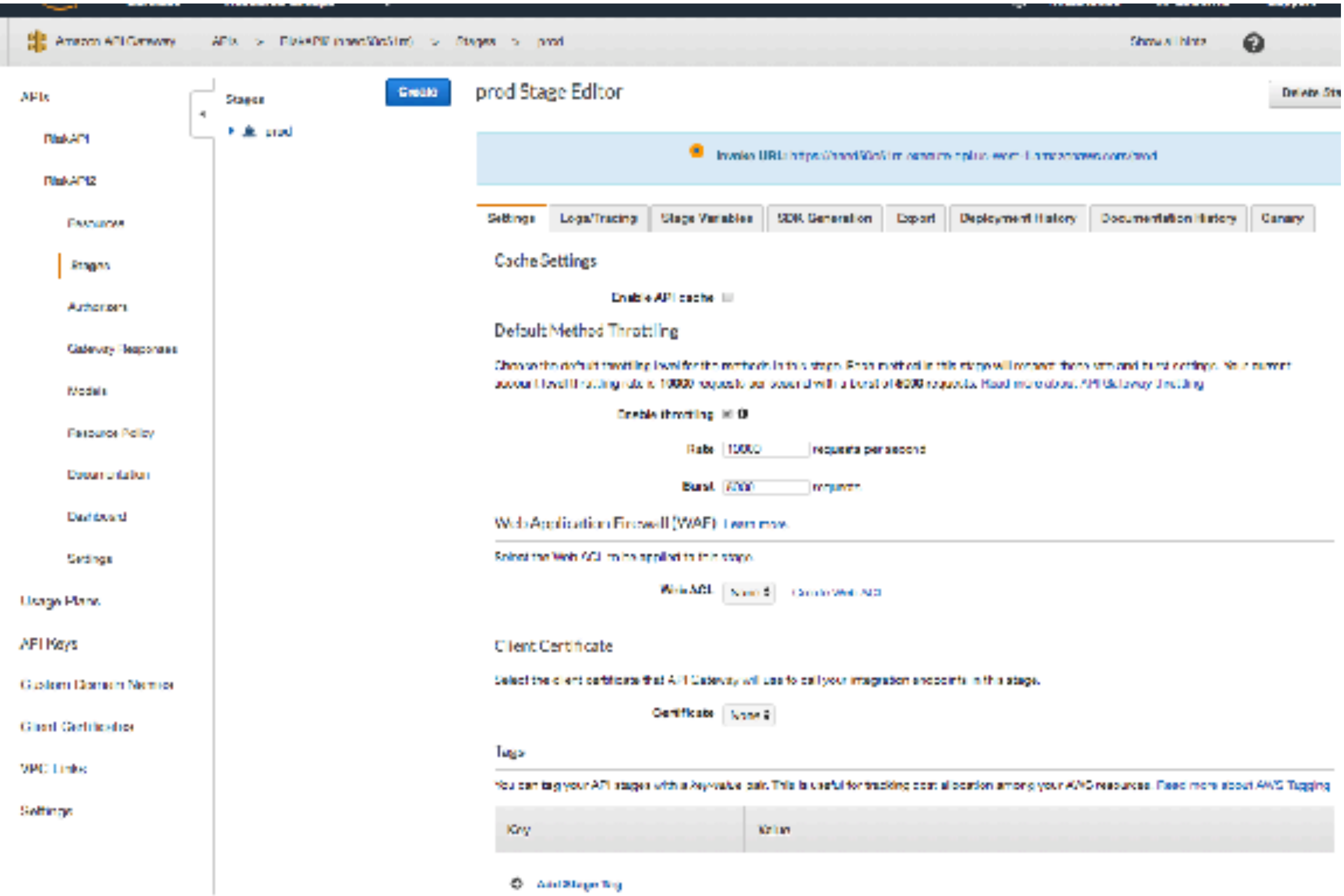


Resource Policy

Configure access control to this private API using a Resource Policy. Access can be controlled by IAM condition elements, including conditions account, Source VPC, VPC Endpoints (Private API), and/or IP range. If the Principal in the policy is set to *, other authorization types can be use the resource policy. If the Principal is set to AWS, then authorization will fail for all resources not secured with AWS_IAM auth, including unsecur resources. Learn more.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "execute-api:Invoke",
            "Resource": "arn:aws:execute-api:us-west-1:243358826547:974ymbqcn5/*/*/*"
        }
    ]
}
```

API Gateway Prod



prod Stage Editor

Invoke URL: [illegible]

Cache Settings

Enable API cache ☐

Default Method Throttling

Choose the default throttling level for the methods in this stage. Each method in this stage will respect these rate and burst settings. Your current account level throttling rate is 10000 requests per second with a burst of 5000 requests. Read more about API Gateway throttling

Enable throttling ☑

Rate 10000 requests per second

Burst 5000 requests

Web Application Firewall (WAF) Learn more.

Select the Web ACL to be applied to this stage.

Web ACL None ⇕ Create Web ACL

Client Certificate

Select the client certificate that API Gateway will use to call your integration endpoints in this stage.

Certificate None ⇕

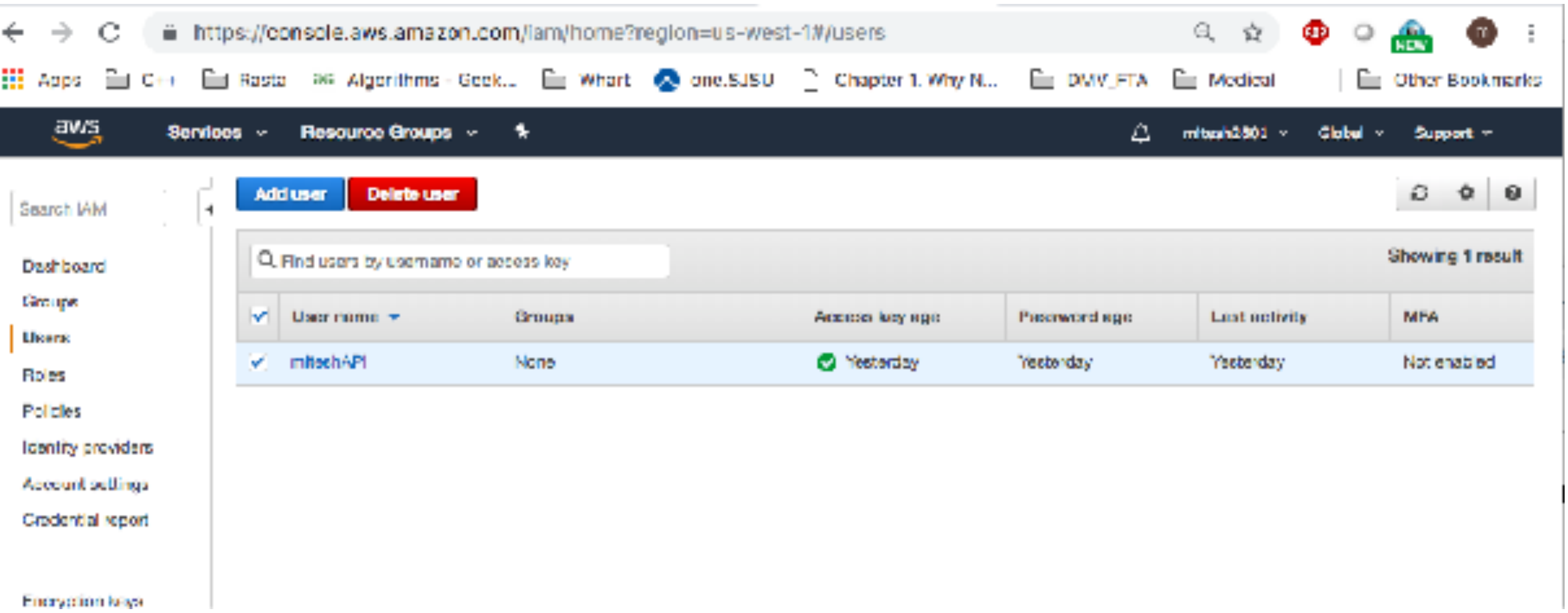
Tags

You can tag your API stages with a key-value pair. This is useful for tracking cost allocation among your AWS resources. Read more about AWS Tagging

Key	Value

⊕ Add Stage Tag

IAM User and Settings



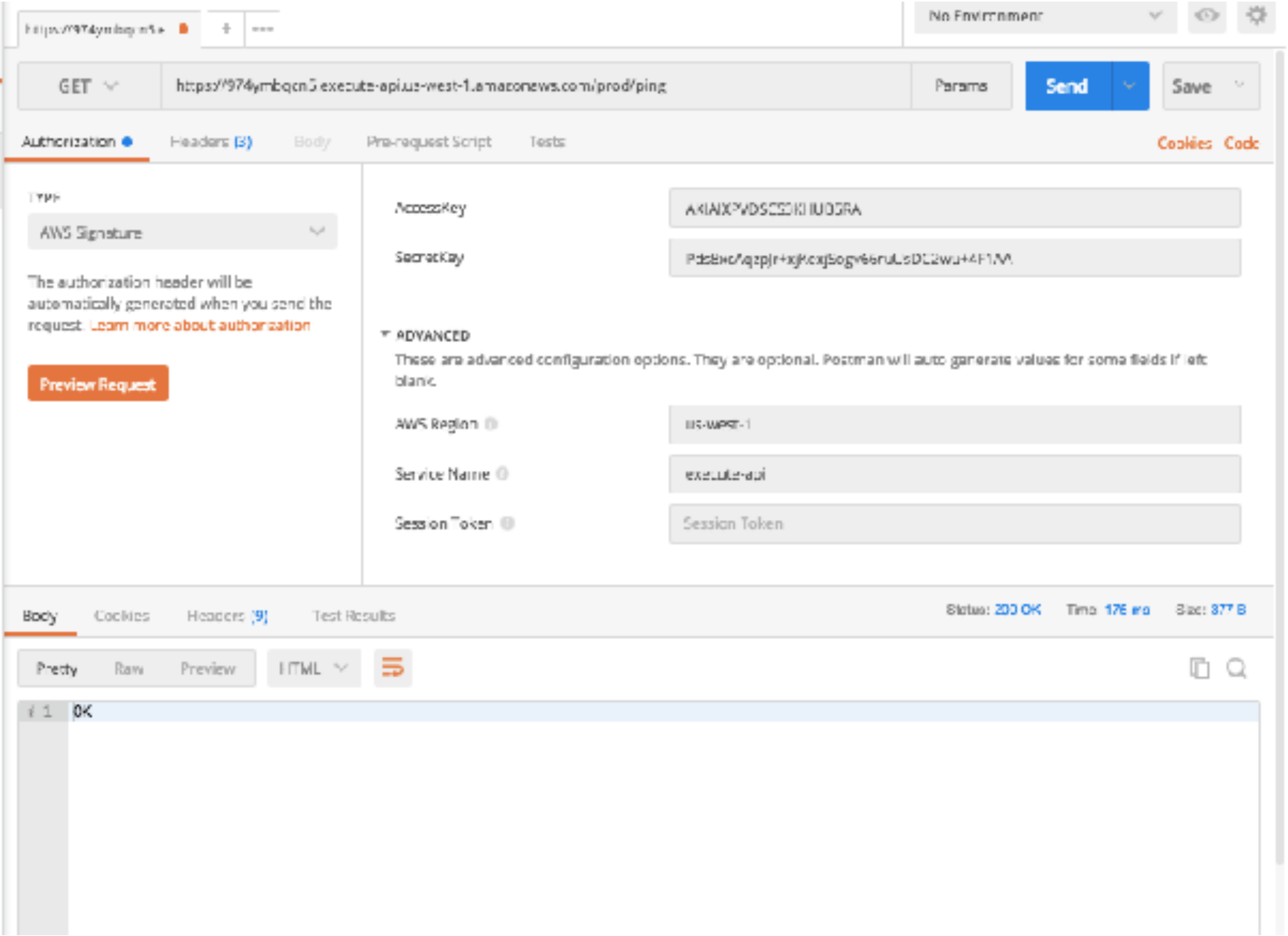
Find users by username or access key

Showing 1 result

☑	User name	Groups	Access key age	Password age	Last activity	MFA
☑	miteshAPI	None	✓ Yesterday	Yesterday	Yesterday	Not enabled

Postman Output

GET



https://974ymbqcn5.execute-api.us-west-1.amazonaws.com/prod/ping

TYPE

AWS Signature

The authorization header will be automatically generated when you send the request. Learn more about authorization

AccessKey: AKIAIXPVDSCSDKHUD3RA

SecretKey: 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

ADVANCED

These are advanced configuration options. They are optional. Postman will auto generate values for some fields if left blank.

AWS Region: us-west-1

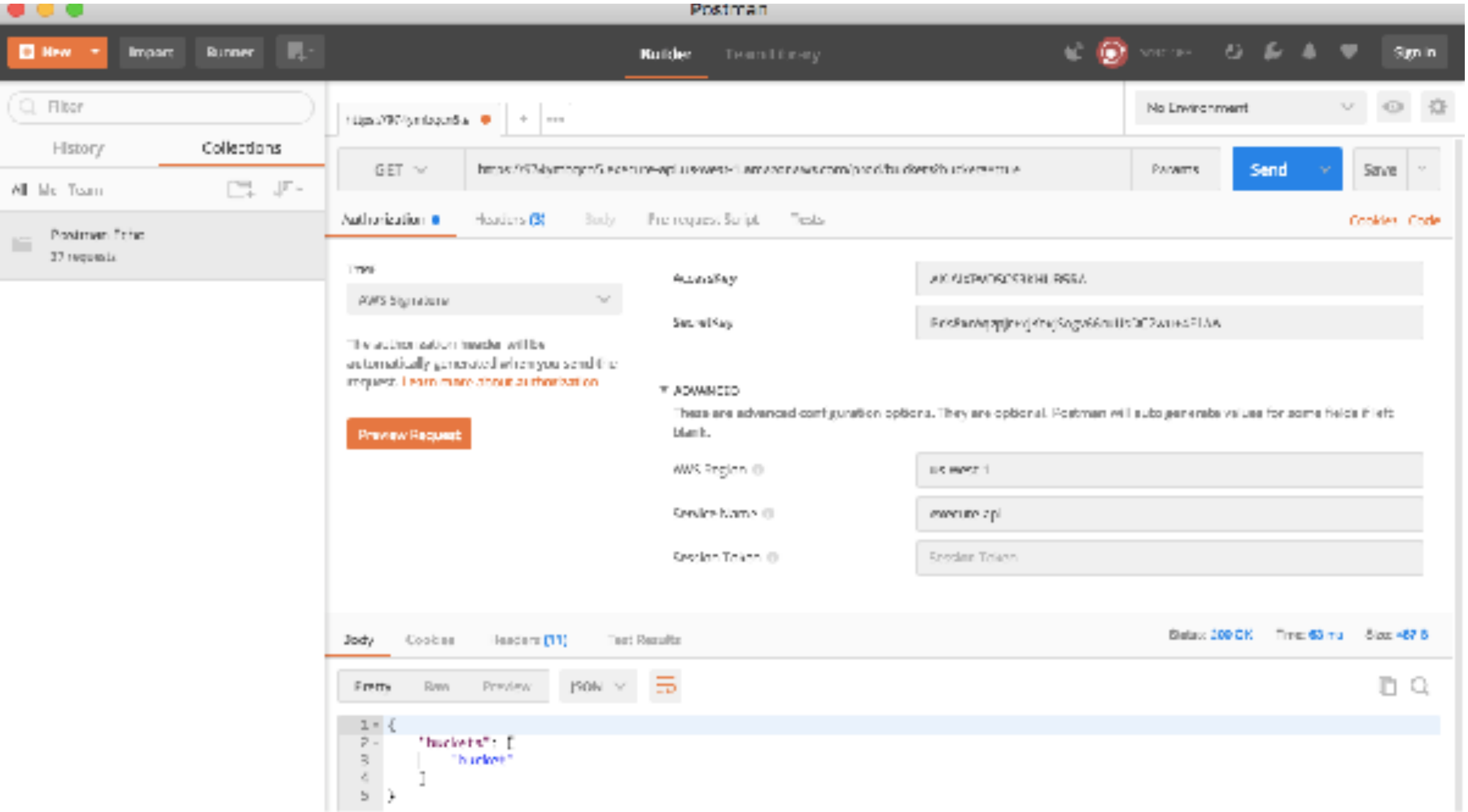
Service Name: execute-api

Session Token: Session Token

Status: 200 OK   Time: 176 ms   Size: 377 B

```
OK
```

GET buckets



GET [illegible]

Type: AWS Signature

The authorization header will be automatically generated when you send the request. Learn more about authorization

AccessKey: [illegible]

SecretKey: [illegible]

▼ ADVANCED

These are advanced configuration options. They are optional. Postman will auto generate values for some fields if left blank.

AWS Region: us-west-1

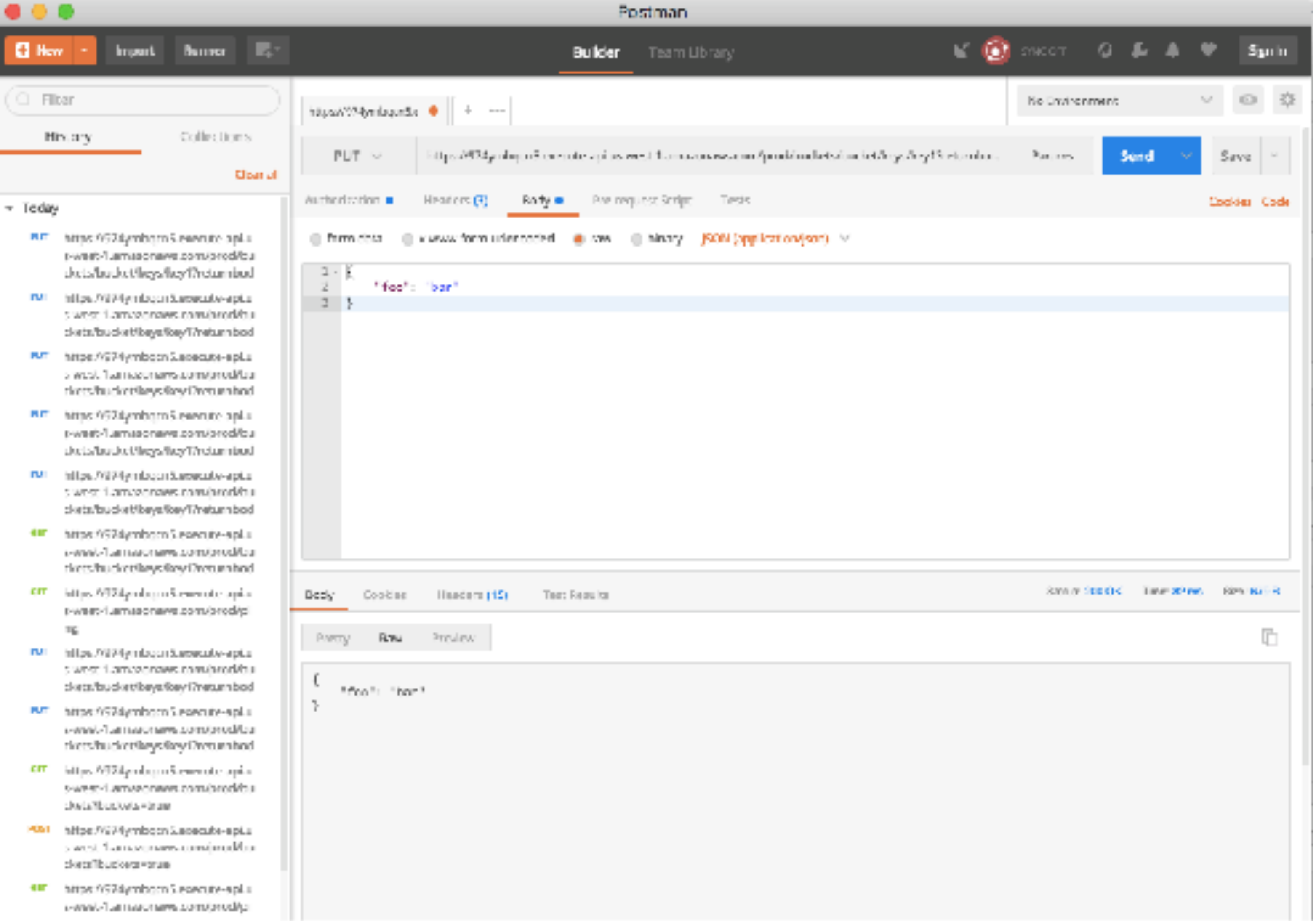
Service Name: execute-api

Session Token: Session Token

Status: 200 OK Time: 63 ms Size: 487 B

```
{
    "buckets": [
        "bucket"
    ]
}
```

PUT request



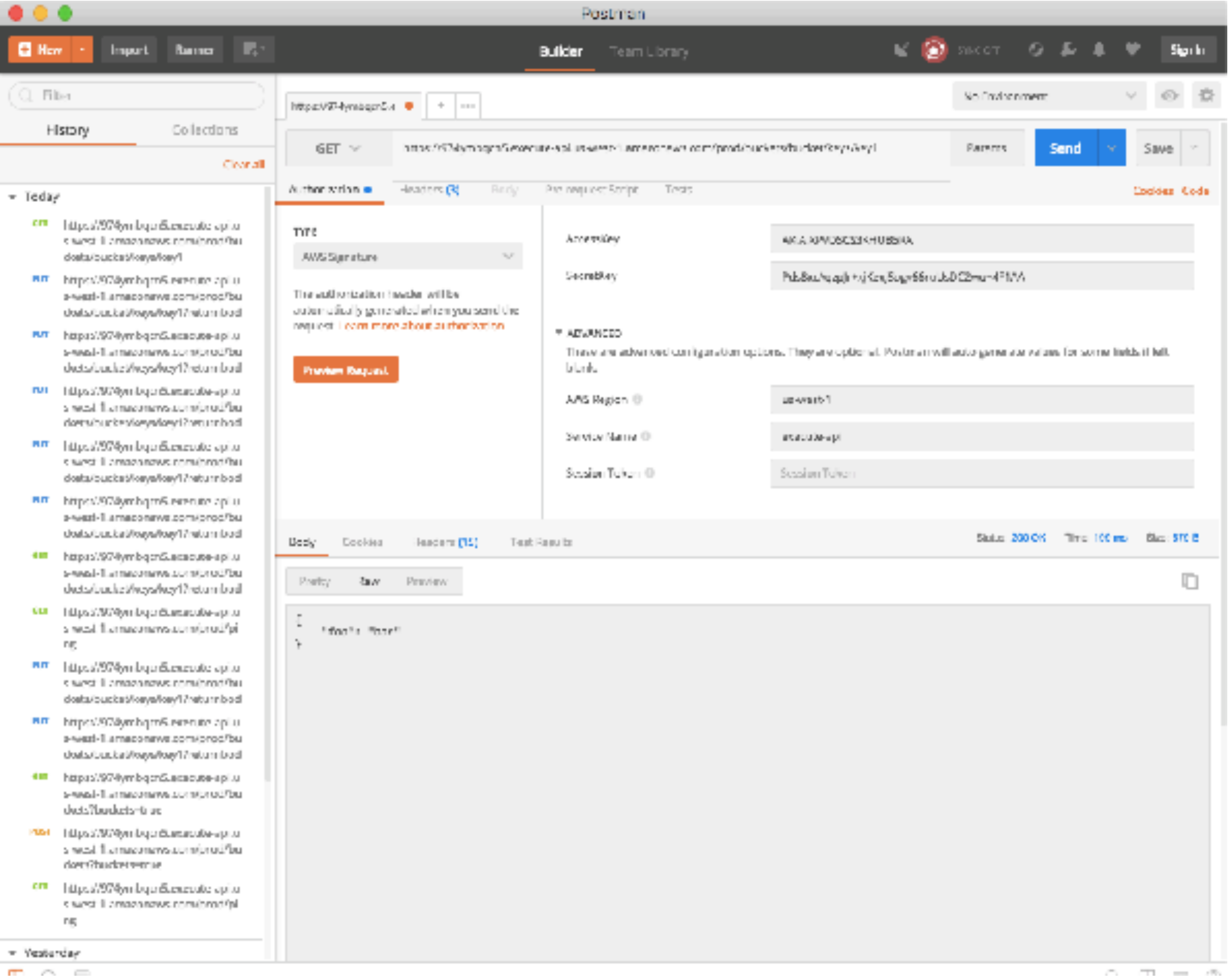
Request body (raw, JSON (application/json)):

```
{
    "foo": "bar"
}
```

Response body (Raw):

```
{
  "foo": "bar"
}
```

GET Request



GET [illegible]

TYPE: AWS Signature

The authorization header will be automatically generated when you send the request. Learn more about authorization

AccessKey: [illegible]

SecretKey: [illegible]

ADVANCED

These are advanced configuration options. They are optional. Postman will auto generate values for some fields if left blank.

AWS Region: us-west-1

Service Name: execute-api

Session Token: Session Token

Status: 200 OK Time: 100 ms Size: 370 B

```
{
  "foo": "bar"
}
```