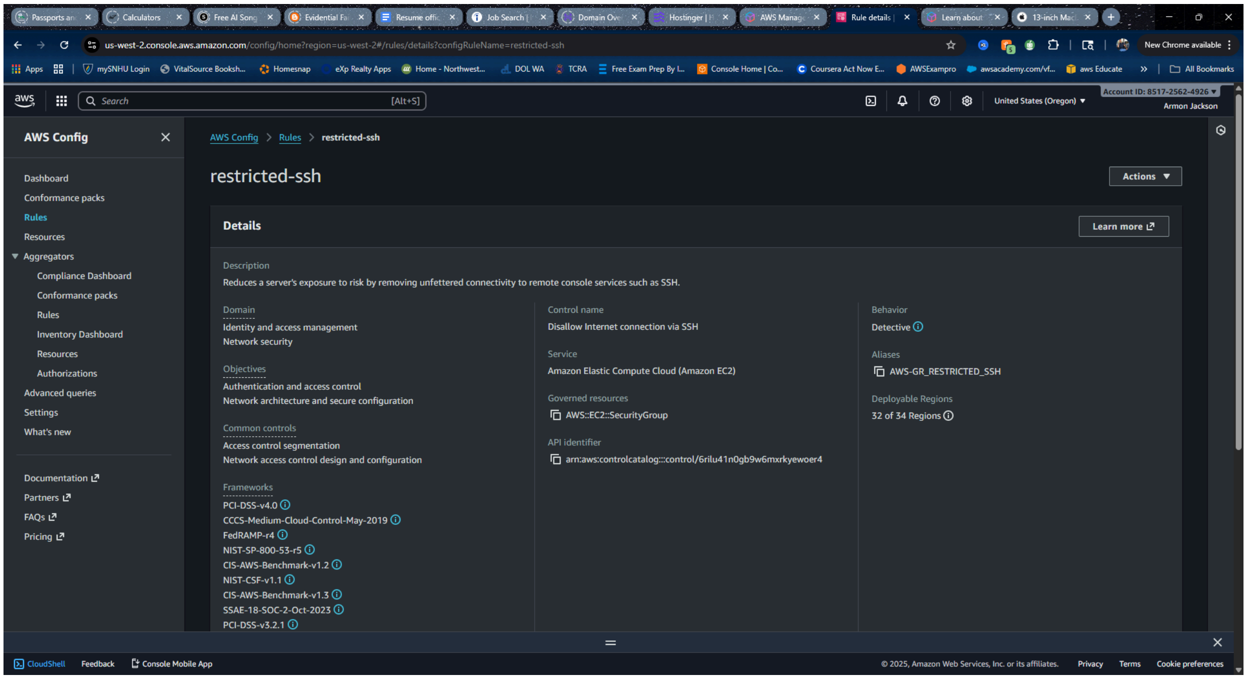


restricted-ssh

Details

Description
Reduces a server's exposure to risk by removing unfettered connectivity to remote console services such as SSH.

Domain
Identity and access management
Network security

Objectives
Authentication and access control
Network architecture and secure configuration

Common controls
Access control segmentation
Network access control design and configuration

Frameworks
PCI-DSS-v4.0
CCCS-Medium-Cloud-Control-May-2019
FedRAMP-r4
NIST-SP-800-53-r5
CIS-AWS-Benchmark-v1.2
NIST-CSF-v1.1
CIS-AWS-Benchmark-v1.3
SSAE-18-SOC-2-Oct-2023
PCI-DSS-v3.2.1

Control name
Disallow Internet connection via SSH

Service
Amazon Elastic Compute Cloud (Amazon EC2)

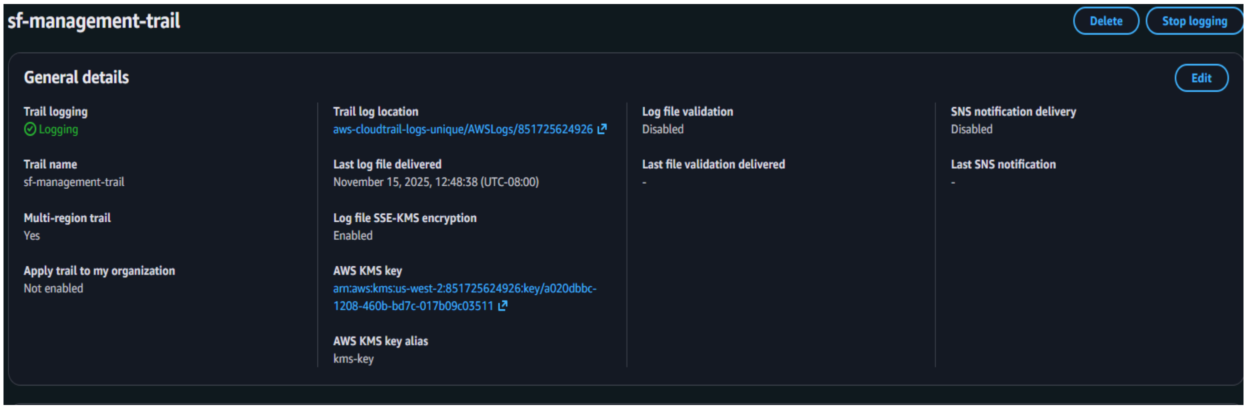
Governed resources
AWS::EC2::SecurityGroup

API identifier
arn:aws:controlcatalog:::control/6rilu41n0gb9w6mxrkyewoer4

Behavior
Detective

Aliases
AWS-GR_RESTRICTED_SSH

Deployable Regions
32 of 34 Regions



sf-management-trail

General details

Trail logging
✓ Logging

Trail name
sf-management-trail

Multi-region trail
Yes

Apply trail to my organization
Not enabled

Trail log location
aws-cloudtrail-logs-unique/AWSLogs/851725624926

Last log file delivered
November 15, 2025, 12:48:38 (UTC-08:00)

Log file SSE-KMS encryption
Enabled

AWS KMS key
arn:aws:kms:us-west-2:851725624926:key/a020dbbc-1208-460b-bd7c-017b09c03511

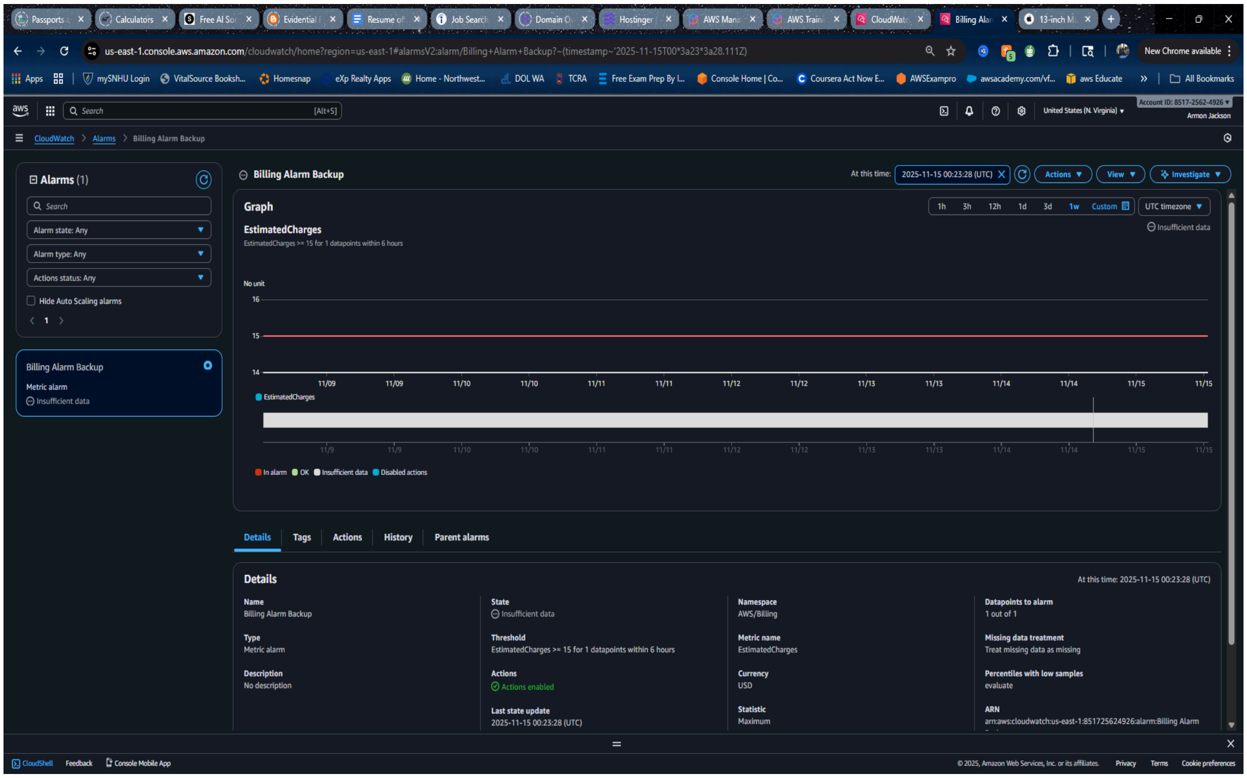
AWS KMS key alias
kms-key

Log file validation
Disabled

Last file validation delivered
-

SNS notification delivery
Disabled

Last SNS notification
-



Billing Alarm Backup

Graph

EstimatedCharges

EstimatedCharges >= 15 for 1 datapoints within 6 hours

Insufficient data

Details

At this time: 2025-11-15 00:23:28 (UTC)

Name
Billing Alarm Backup

Type
Metric alarm

Description
No description

State
Insufficient data

Threshold
EstimatedCharges >= 15 for 1 datapoints within 6 hours

Actions
Actions enabled

Last state update
2025-11-15 00:23:28 (UTC)

Namespace
AWS/Billing

Metric name
EstimatedCharges

Currency
USD

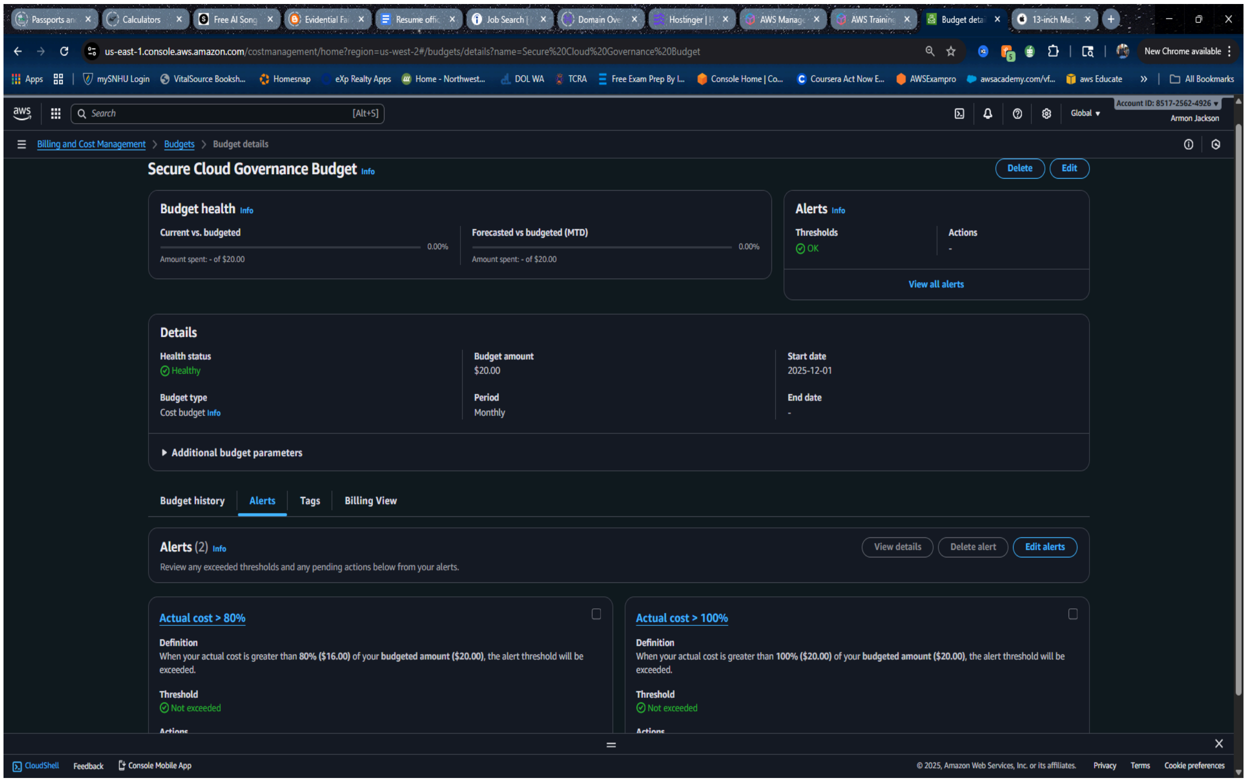
Statistic
Maximum

Datapoints to alarm
1 out of 1

Missing data treatment
Treat missing data as missing

Percentiles with low samples
evaluate

ARN
arn:aws:cloudwatch:us-east-1:851725624926:alarm:Billing Alarm



Secure Cloud Governance Budget

Budget health

Current vs. budgeted 0.00%
Amount spent: - of $20.00

Forecasted vs budgeted (MTD) 0.00%
Amount spent: - of $20.00

Alerts

Thresholds
✓ OK

Actions
-

Details

Health status
✓ Healthy

Budget type
Cost budget

Budget amount
$20.00

Period
Monthly

Start date
2025-12-01

End date
-

▸ Additional budget parameters

Alerts (2)

Review any exceeded thresholds and any pending actions below from your alerts.

Actual cost > 80% □

Definition
When your actual cost is greater than **80% ($16.00)** of your **budgeted amount ($20.00)**, the alert threshold will be exceeded.

Threshold
✓ Not exceeded

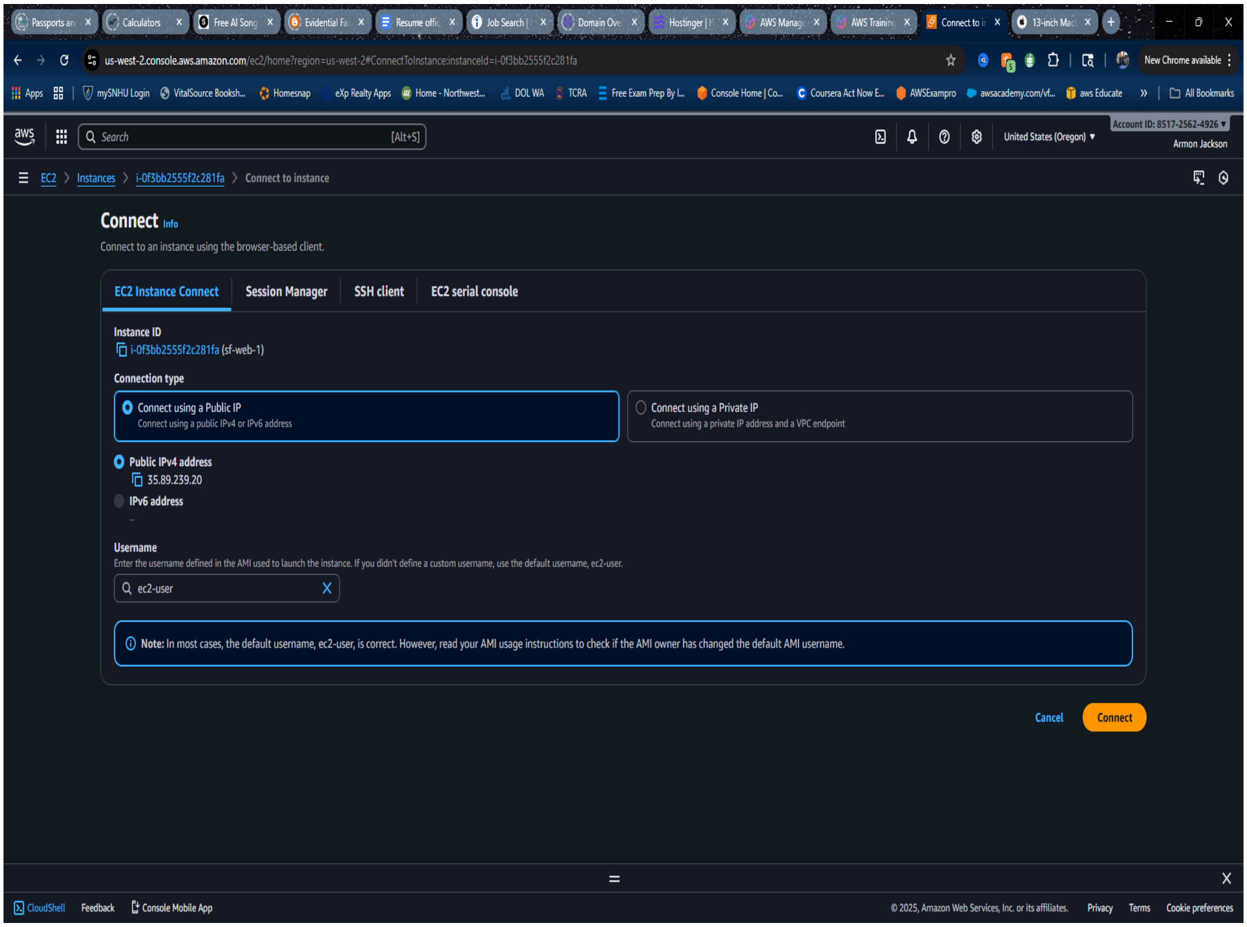
Actions

Actual cost > 100% □

Definition
When your actual cost is greater than **100% ($20.00)** of your **budgeted amount ($20.00)**, the alert threshold will be exceeded.

Threshold
✓ Not exceeded

Actions



us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#ConnectToInstance:instanceId=i-0f3bb2555f2c281fa

Connect Info

Connect to an instance using the browser-based client.

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID
i-0f3bb2555f2c281fa (sf-web-1)

Connection type

● Connect using a Public IP
Connect using a public IPv4 or IPv6 address

○ Connect using a Private IP
Connect using a private IP address and a VPC endpoint

● Public IPv4 address
35.89.239.20

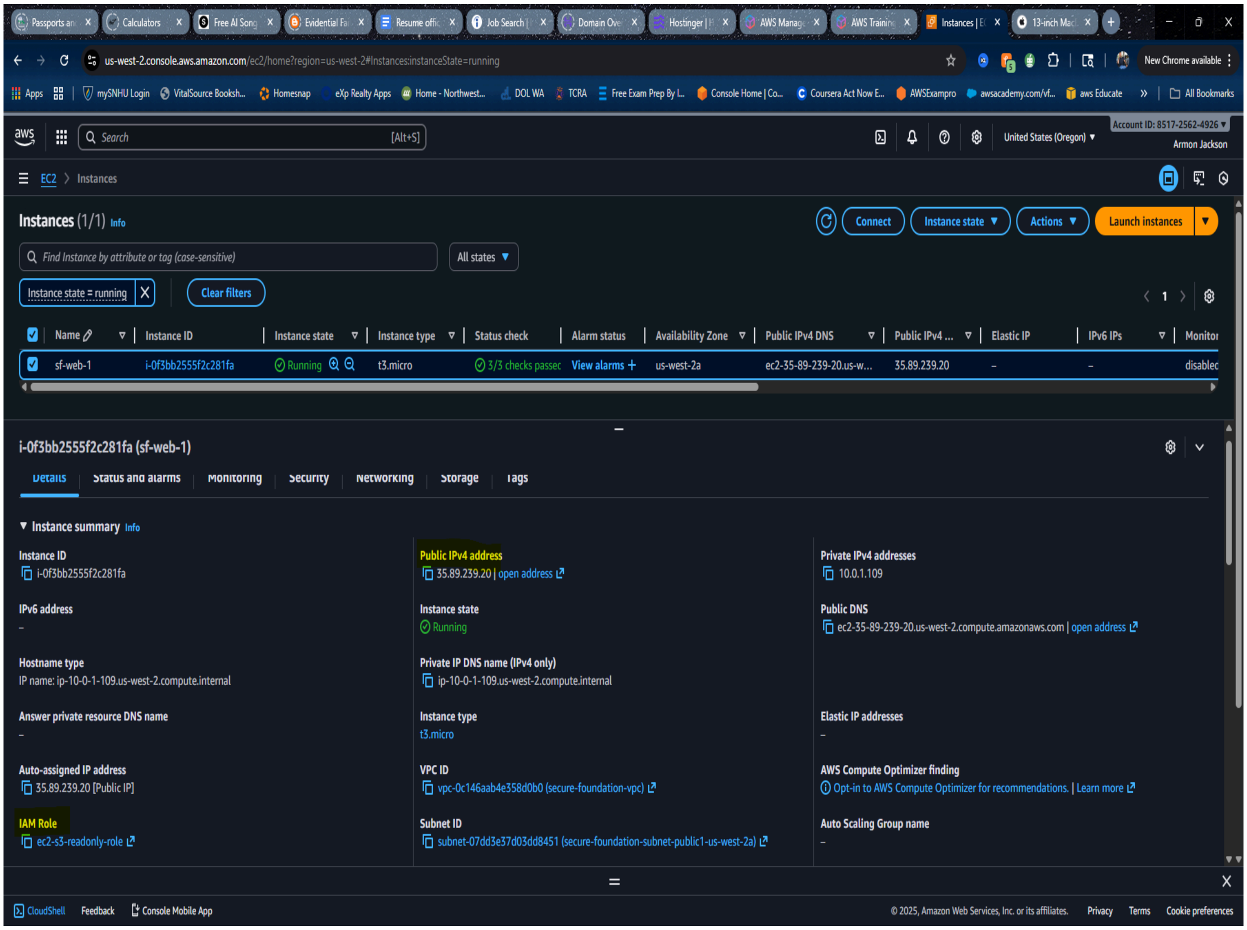
○ IPv6 address
–

Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.

ec2-user

Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel | Connect



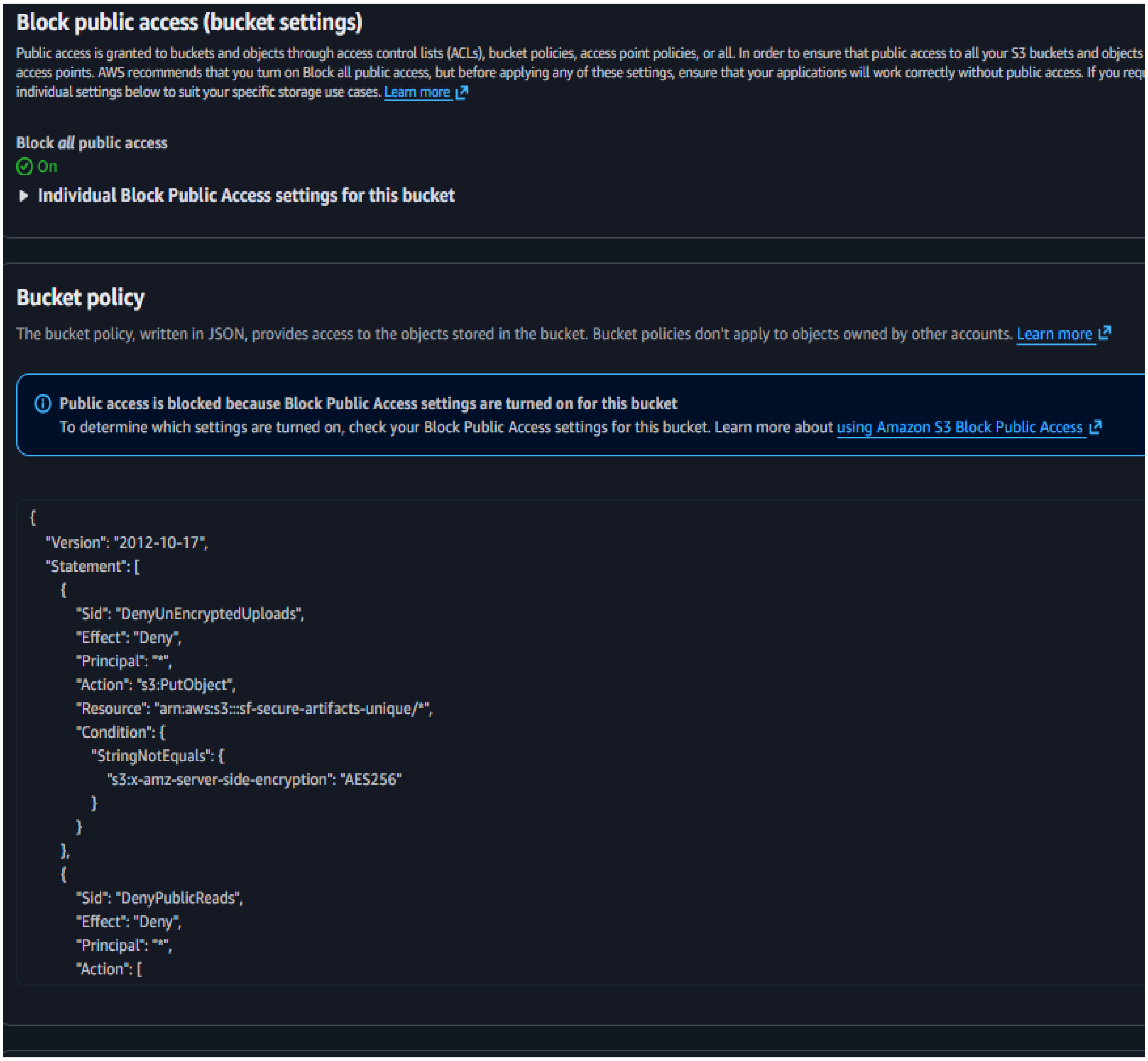
Instances (1/1) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitor
☑	sf-web-1	i-0f3bb2555f2c281fa	✓ Running	t3.micro	✓ 3/3 checks passec	View alarms +	us-west-2a	ec2-35-89-239-20.us-w...	35.89.239.20	–	–	disablec

i-0f3bb2555f2c281fa (sf-web-1)

▼ Instance summary Info

Instance ID i-0f3bb2555f2c281fa	Public IPv4 address 35.89.239.20 | open address	Private IPv4 addresses 10.0.1.109
IPv6 address –	Instance state ✓ Running	Public DNS ec2-35-89-239-20.us-west-2.compute.amazonaws.com | open address
Hostname type IP name: ip-10-0-1-109.us-west-2.compute.internal	Private IP DNS name (IPv4 only) ip-10-0-1-109.us-west-2.compute.internal	
Answer private resource DNS name –	Instance type t3.micro	Elastic IP addresses –
Auto-assigned IP address 35.89.239.20 [Public IP]	VPC ID vpc-0c146aab4e358d0b0 (secure-foundation-vpc)	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role ec2-s3-readonly-role	Subnet ID subnet-07dd3e37d03dd8451 (secure-foundation-subnet-public1-us-west-2a)	Auto Scaling Group name –



Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects
access points. 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 req
individual settings below to suit your specific storage use cases. Learn more

Block *all* public access

✓ On

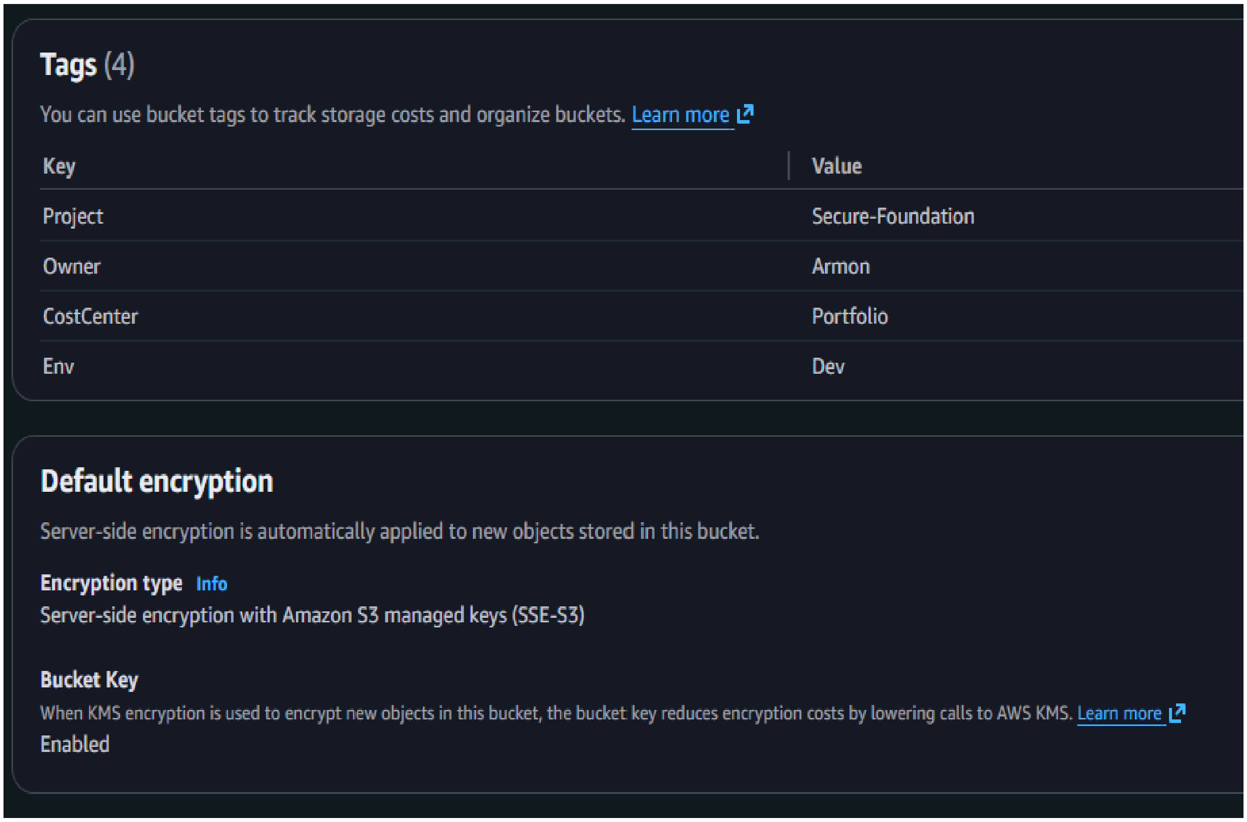
▸ Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

ⓘ **Public access is blocked because Block Public Access settings are turned on for this bucket**
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyUnEncryptedUploads",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::sf-secure-artifacts-unique/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    },
    {
      "Sid": "DenyPublicReads",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
```



Tags (4)

You can use bucket tags to track storage costs and organize buckets. Learn more

Key	Value
Project	Secure-Foundation
Owner	Armon
CostCenter	Portfolio
Env	Dev

Default encryption

Server-side encryption is automatically applied to new objects stored in this bucket.

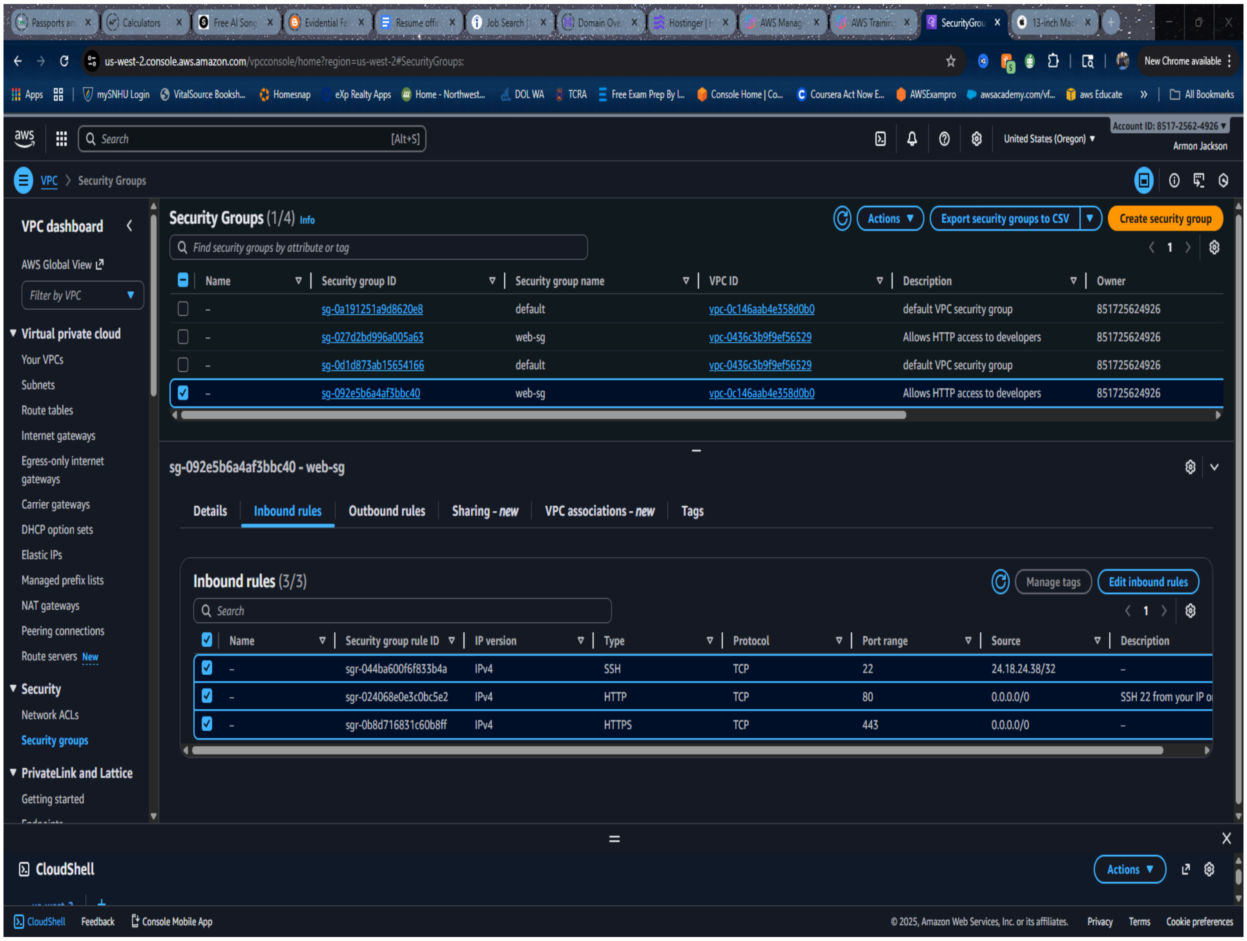
Encryption type Info

Server-side encryption with Amazon S3 managed keys (SSE-S3)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more

Enabled



Security Groups (1/4) Info

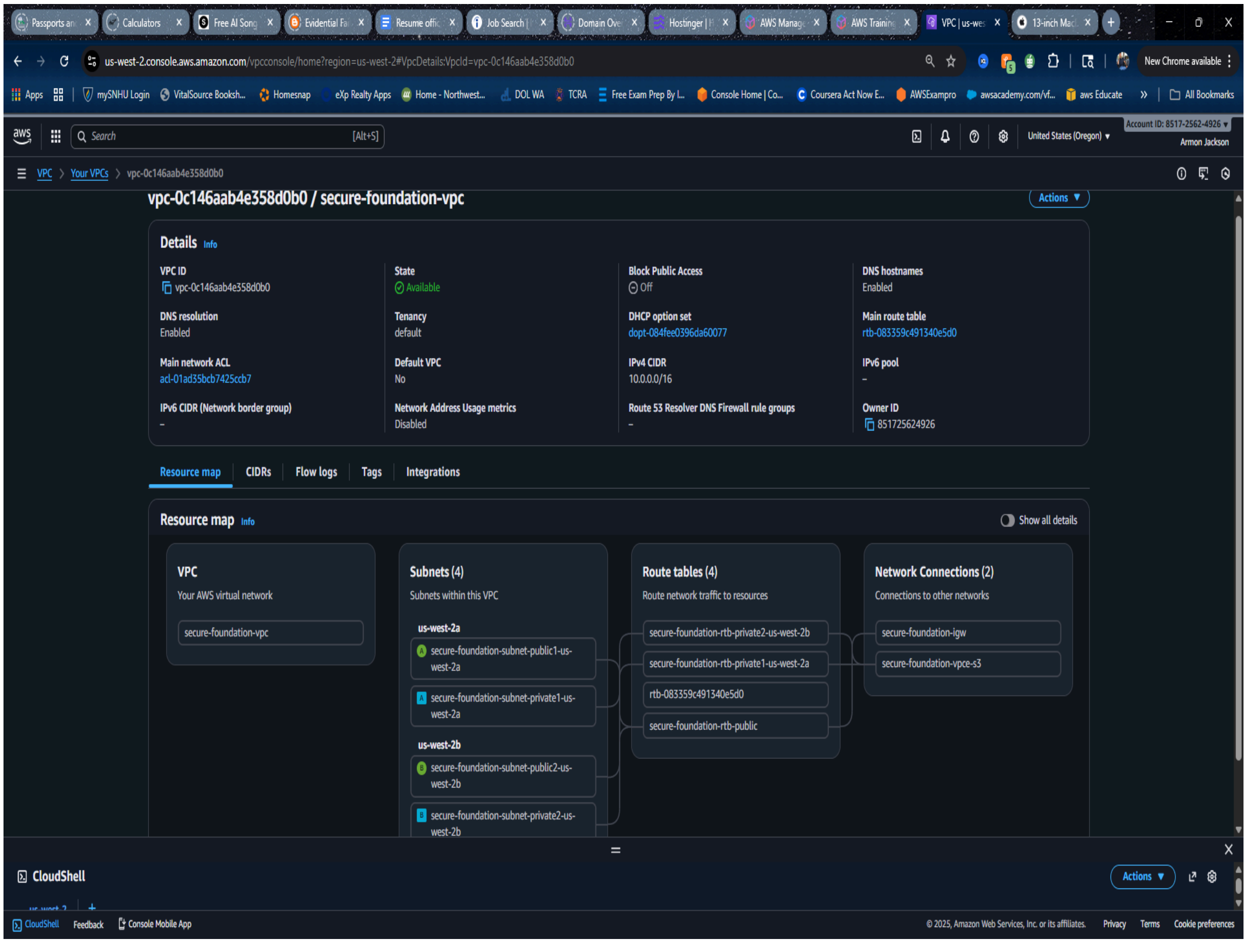
Find security groups by attribute or tag

	Name	Security group ID	Security group name	VPC ID	Description	Owner
□	–	sg-0a191251a9d8620e8	default	vpc-0c146aab4e358d0b0	default VPC security group	851725624926
□	–	sg-027d2bd996a005a63	web-sg	vpc-0436c3b9f9ef56529	Allows HTTP access to developers	851725624926
□	–	sg-0d1d873ab15654166	default	vpc-0436c3b9f9ef56529	default VPC security group	851725624926
☑	–	sg-092e5b6a4af3bbc40	web-sg	vpc-0c146aab4e358d0b0	Allows HTTP access to developers	851725624926

sg-092e5b6a4af3bbc40 - web-sg

Inbound rules (3/3)

☑	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
☑	–	sgr-044ba600f6f833b4a	IPv4	SSH	TCP	22	24.18.24.38/32	–
☑	–	sgr-024068e0e3c0bc5e2	IPv4	HTTP	TCP	80	0.0.0.0/0	SSH 22 from your IP o
☑	–	sgr-0b8d716831c60b8ff	IPv4	HTTPS	TCP	443	0.0.0.0/0	–



us-west-2.console.aws.amazon.com/vpcconsole/home?region=us-west-2#VpcDetails:VpcId=vpc-0c146aab4e358d0b0

VPC > Your VPCs > vpc-0c146aab4e358d0b0

vpc-0c146aab4e358d0b0 / secure-foundation-vpc

Details

VPC ID
vpc-0c146aab4e358d0b0

State
Available

Block Public Access
Off

DNS hostnames
Enabled

DNS resolution
Enabled

Tenancy
default

DHCP option set
dopt-084fee0396da60077

Main route table
rtb-083359c491340e5d0

Main network ACL
acl-01ad35bcb7425ccb7

Default VPC
No

IPv4 CIDR
10.0.0.0/16

IPv6 pool
–

IPv6 CIDR (Network border group)
–

Network Address Usage metrics
Disabled

Route 53 Resolver DNS Firewall rule groups
–

Owner ID
851725624926

Resource map | CIDRs | Flow logs | Tags | Integrations

Resource map

Show all details

VPC
Your AWS virtual network
- secure-foundation-vpc

Subnets (4)
Subnets within this VPC

us-west-2a
- A secure-foundation-subnet-public1-us-west-2a
- A secure-foundation-subnet-private1-us-west-2a

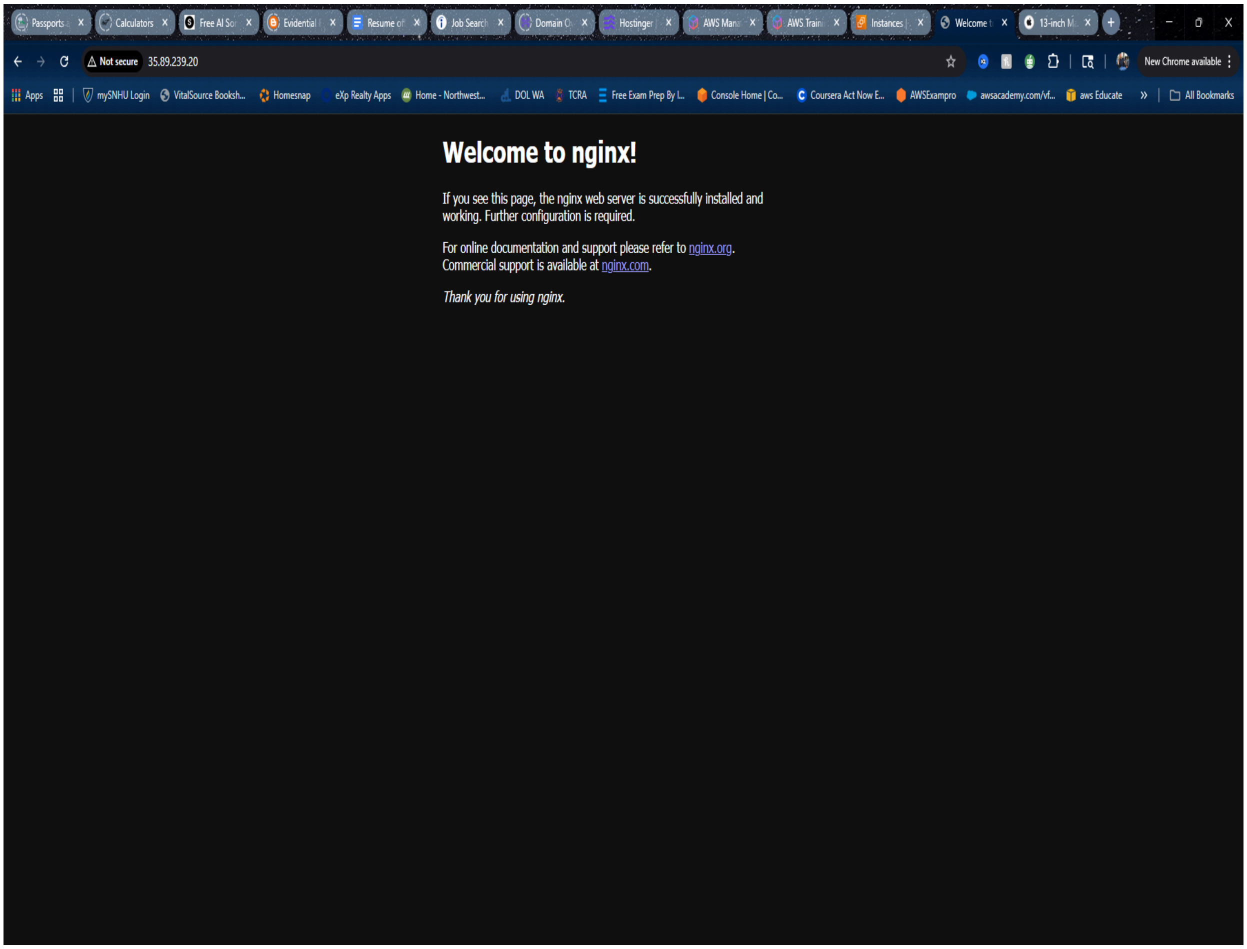
us-west-2b
- B secure-foundation-subnet-public2-us-west-2b
- B secure-foundation-subnet-private2-us-west-2b

Route tables (4)
Route network traffic to resources
- secure-foundation-rtb-private2-us-west-2b
- secure-foundation-rtb-private1-us-west-2a
- rtb-083359c491340e5d0
- secure-foundation-rtb-public

Network Connections (2)
Connections to other networks
- secure-foundation-igw
- secure-foundation-vpce-s3

CloudShell

© 2025, Amazon Web Services, Inc. or its affiliates.



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.