

Check list:

- ☒ Github repo — <https://github.com/dustman7g/tech-challenge-2025>
- ☒ Terraform modules — ~~coalfires modules encouraged~~
 - ☒ Ec2 module = <https://github.com/Coalfire-CF/terraform-aws-ec2/tree/main>
- ☒ Diagram of solution
- ☒ [Readme.md](#)
- ☒ Deployment steps
- ☒ Commentary
 - ☒ Breaking up the subnets to use ALB
 - ☒ Using Management subnet for ALB since it public
 - ☒ Adding keys to talk to MGMT server to App servers for testing
 - ☒ t3.micro instead of t2.micro since t3 is on free tier
 - ☒ Added VPC endpoint for S3 to download httpd
- ☒ Network
 - ☒ 1 VPC — 10.1.0.0/16
 - ☒ 3 Subnets
 - ☒ Application /24 (no internet)
 - ☒ Management /24 (internet facing)
 - ☒ Application /24 (no internet)
- ☒ Compute
 - ☒ Ec2 in ASG to run linux in the application subnet
 - ☒ SG Allows from management ec2, allows web traffic from the Application Load balancer and no external traffic
 - ☒ Script installation of apache
 - ☒ 2 min and 6 max host in ASG
 - ☒ t2.micro
 - ☒ 1 EC2 running linux in MGMT Subnet
 - ☒ SG Allows SSH from a single specific IP or network space only
 - ☒ Can SSH from this instance to ASG
 - ☒ T2.micro
- ☒ Supporting Infrastructure
 - ☒ One ALB that sends web traffic to the ec2's in the ASG
- ☒ Document in README
 - ☒ Analysis of your own deployed infra
 - ☒ What security gaps exist?
 - ☒ What availability issues?
 - ☒ Cost Optimization opportunities?
 - ☒ Operational shortcomings (no backups and no monitoring)?
 - ☒ Improvement Plan

- ☒ List specific changes you 'd make to improve security, resilience, cost, maintainability
- ☒ Prioritize them(why would you first and why?)
- ☒ Include at least 2 implemented improvements in code or scripts(tightening SG rules, adding cloud watch alarms, setting bucket polices)
- ☒ Runbook style notes
 - ☒ How would someone else deploy and operate your environment?
 - ☒ How would you respond to an outage for the EC2 instance?
- ☒ Overall Deliverables
 - ☒ All terraform configurations
 - ☒ Architecture diagram
 - ☒ README including
 - ☒ Solution overview
 - ☒ Deployment instructions
 - ☒ Design decision and assumptions
 - ☒ Reference to resources used
 - ☒ Terraform registry
 - ☒ Goalfire git
 - ☒ Assumptions made
 - ☒ Internet gateway for internet access
 - ☒ VPC s3 endpoint to download httpd
 - ☒ Improvement plan with priorities
 - ☒ Analysis of operational gaps

To run terraform plan apply need to add to test in AWS

\$env:AWS_ACCESS_KEY_ID = "your access key id"

\$env:AWS_SECRET_ACCESS_KEY = "your access key"

\$env:AWS_DEFAULT_REGION = "us-east-1"

####Add open SSH

Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0

####Service might not be running and in a disabled state - enable openSSH service and start it

```
Set-Service "ssh-agent" -StartupType Automatic
```

```
Start-Service "ssh-agent"
```

Generate a key pair on your local machine (if you don't have one yet)

On **Windows (PowerShell with OpenSSH installed)**:

```
ssh-keygen -t rsa -b 4096 -f $env:USERPROFILE\.ssh\management-key
```

- `-f $env:USERPROFILE\.ssh\management-key` → saves the files as:
 - `management-key` → private key (keep this safe!)
 - `management-key.pub` → public key (AWS needs this)

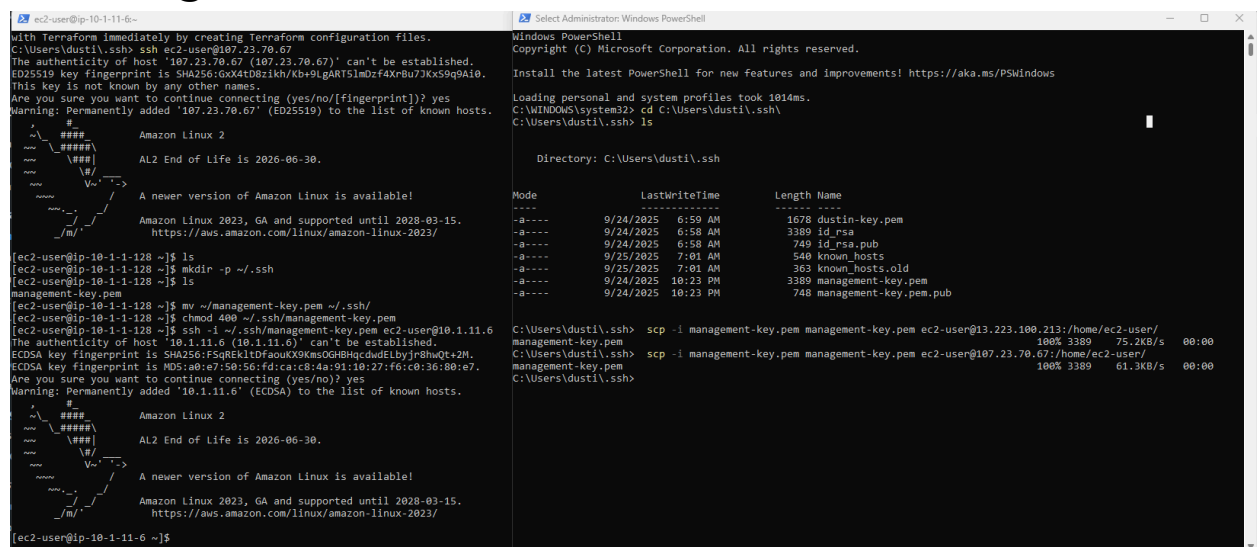
Find my public IP

(Invoke-WebRequest -Uri "https://ifconfig.me/ip").Content.Trim()

Update security group for management with your IP

ssh-add C:\users\username\.ssh\management-key.pem

ssh ec2-user@13.223.100.213



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

Loading personal and system profiles took 1014ms.
C:\WINDOWS\system32> cd C:\Users\dustil\.ssh\
C:\Users\dustil\.ssh> ls

Directory: C:\Users\dustil\.ssh

Mode                LastWriteTime         Length Name
----                -
-a----          9/24/2025   6:59 AM             1678 dustin-key.pem
-a----          9/24/2025   6:58 AM             3389 id_rsa
-a----          9/24/2025   6:58 AM              749 id_rsa.pub
-a----          9/25/2025   7:01 AM             540 known_hosts
-a----          9/25/2025   7:01 AM             363 known_hosts.old
-a----          9/24/2025  10:23 PM             3389 management-key.pem
-a----          9/24/2025  10:23 PM              748 management-key.pub

C:\Users\dustil\.ssh> scp -i management-key.pem management-key.pem ec2-user@13.223.100.213:/home/ec2-user/
management-key.pem
C:\Users\dustil\.ssh> scp -i management-key.pem management-key.pem ec2-user@107.23.70.67:/home/ec2-user/
management-key.pem
C:\Users\dustil\.ssh>
```

Copy key over to management server from local path

```
scp -i management-key.pem management-key.pem ec2-user@13.223.100.213:/home/ec2-user/
```

Make .ssh directory on management server, move mgmt pem key to folder and update permissions

```
mkdir -p ~/.ssh
```

```
mv ~/.management-key.pem ~/.ssh/
```

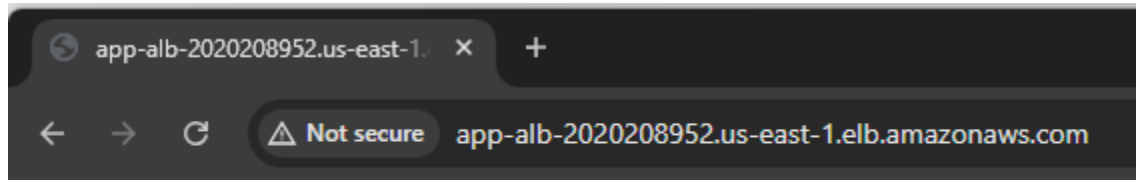
```
chmod 400 ~/.ssh/management-key.pem
```

SSH from MGMT server to ASG/App instance

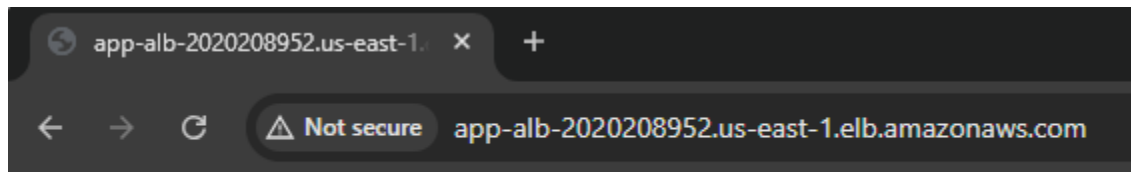
```
ssh -i ~/.ssh/management-key.pem ec2-user@10.1.11.6 or 10.1.10.71
```

Evidence of Success

<http://app-alb-2020208952.us-east-1.elb.amazonaws.com> - Success



Hello from ip-10-1-10-71.ec2.internal (instance-id: i-03a8b9d820c3374c8)



Hello from ip-10-1-10-71.ec2.internal (instance-id: i-03a8b9d820c3374c8)

MGMT instance

Instances (1/4) Info

Find Instance by attribute or tag (case-sensitive) All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elas
app-asg	i-0a0beb505649e1cae	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1b	-	-	-
app-asg	i-03a8b9d820c3374c8	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	-	-	-
management-instance	i-07db8cd0daa40ffc3	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	ec2-107-23-70-67.com...	107.23.70.67	-
management-instance	i-0466f2ac3400bbe62	Terminated	t3.micro	-	View alarms +	us-east-1a	-	-	-

i-07db8cd0daa40ffc3 (management-instance)

Details Status and alarms Monitoring Security Networking Storage Tags

▼ Instance summary Info

Instance ID
i-07db8cd0daa40ffc3

IPv6 address
-

Hostname type
IP name: ip-10-1-1-128.ec2.internal

Answer private resource DNS name
-

Auto-assigned IP address
107.23.70.67 [Public IP]

IAM Role
-

IMDSv2
Required

Public IPv4 address
107.23.70.67 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-10-1-1-128.ec2.internal

Instance type
t3.micro

VPC ID
vpc-0f152a15d66a8b3cb (coalfire-vpc)

Subnet ID
subnet-0372982cd211fc966 (management-subnet-0)

Instance ARN
arn:aws:ec2:us-east-1:980833626314:instance/i-07db8cd0daa40ffc3

Private IPv4 addresses
10.1.1.128

Public DNS
ec2-107-23-70-67.compute-1.amazonaws.com | open address

Elastic IP addresses
-

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
-

Managed
false

ASG

Instances (1/4) Info

Last updated 20 minutes ago

Connect

Instance state

Actions

Launch instances

Find instance by attribute or tag (case-sensitive)

All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input checked="" type="checkbox"/> app-asg	i-0a0beb505649e1cae	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1b	-	-	-
<input type="checkbox"/> app-asg	i-03a8b9d820c3374c8	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	-	-	-
<input type="checkbox"/> management-instance	i-07db8cd0daa40ffc3	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	ec2-107-23-70-67.com...	107.23.70.67	-
<input type="checkbox"/> management-instance	i-0466f2ac3400bbe62	Terminated	t3.micro	-	View alarms +	us-east-1a	-	-	-

i-0a0beb505649e1cae (app-asg)

DetailsStatus and alarmsMonitoringSecurityNetworkingStorageTags

Instance summary Info

Instance ID

i-0a0beb505649e1cae

IPv6 address

-

Hostname type

IP name: ip-10-11-11-6.ec2.internal

Answer private resource DNS name

-

Auto-assigned IP address

-

IAM Role

-

IMDSv2

Optional

Public IPv4 address

-

Instance state

Running

Private IP DNS name (IPv4 only)

ip-10-11-11-6.ec2.internal

Instance type

t3.micro

VPC ID

vpc-0f152a15d66a8b3cb (coalfire-vpc)

Subnet ID

subnet-001500d0d37118071 (app-subnet-1)

Instance ARN

arn:aws:ec2:us-east-1:980833626314:instance/i-0a0beb505649e1cae

Private IPv4 addresses

10.1.11.6

Public DNS

-

Elastic IP addresses

-

AWS Compute Optimizer finding

Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name

app-asg

Managed

false

Target groups

Target groups (1/1) Info

Actions

Create target group

Filter target groups

< 1 >

Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
<input checked="" type="checkbox"/> app-tg	arn:aws:elasticloadbalancing:us-east-1:980833626314:targetgroup/app-tg/69a3eb344cd06ed1	80	HTTP	Instance	app-alb	vpc-0f152a15d66a8b3cb

Target group: app-tg

DetailsTargetsMonitoringHealth checksAttributesTags

Details

Target type

Instance

IP address type

IPv4

Protocol : Port

HTTP: 80

Load balancer

app-alb

Protocol version

HTTP1

VPC

vpc-0f152a15d66a8b3cb

2

Total targets

2

Healthy

0

Unhealthy

0

Unused

0

Initial

0

Draining

Target group: app-tg

Registered targets (2) Info

Anomaly mitigation: Not applicable
Deregister
Register targets

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

2 matches

Health status = healthy
Clear filters

<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details	Admini...	Overrid...	Launch ...	Anomaly detectio...
<input type="checkbox"/>	i-03a8b9d820c3374c8	app-asg	80	us-east-1a (us...	Healthy	-	No override.	No overrid...	Septembe...	Normal
<input type="checkbox"/>	i-0a0beb505649e1cae	app-asg	80	us-east-1b (us...	Healthy	-	No override.	No overrid...	Septembe...	Normal

Load Balancer

Load balancers (1/1)

Actions
Create load balancer

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

<input checked="" type="checkbox"/>	Name	State	Type	Scheme	IP address type	VPC ID	Availability Zones	Security groups	DNS name
<input checked="" type="checkbox"/>	app-alb	Active	application	Internet-facing	IPv4	vpc-0f152a15d66a8b3cb	2 Availability Zones	sg-05305213b02905a7...	app-alb-20202

Load balancer: app-alb

Details
Listeners and rules
Network mapping
Resource map
Security
Monitoring
Integrations
Attributes
Capacity
Tags

Details

Load balancer type
Application

Status
Active

VPC
vpc-0f152a15d66a8b3cb

Load balancer IP address type
IPv4

Scheme
Internet-facing

Hosted zone
Z35SXDOTRQ7X7K

Availability Zones
subnet-0372982cd211fc966 us-east-1a (use1-az1)
subnet-0430d910e7cecdac us-east-1b (use1-az2)

Date created
September 25, 2025, 15:01 (UTC-05:00)

Load balancer ARN
arn:aws:elasticloadbalancing:us-east-1:980833626314:loadbalancer/app/app-alb/698d514dff10a48e

DNS name Info
app-alb-2020208952.us-east-1.elb.amazonaws.com (A Record)

SGs

<input type="checkbox"/>	alb-sg	sg-05305213b02905a77	alb-sg	vpc-0f152a15d66a8b3cb	Allow HTTP from internet to ALB	980833626314
<input checked="" type="checkbox"/>	app-sg	sg-09560f70abfae0311	app-sg	vpc-0f152a15d66a8b3cb	Allow HTTP from ALB and SSH from ma...	980833626314
<input type="checkbox"/>	mgmt-sg	sg-09e7cf0c7b6b6eaa7	mgmt-sg	vpc-0f152a15d66a8b3cb	Allow SSH from allowed_mgmt_ip to m...	980833626314

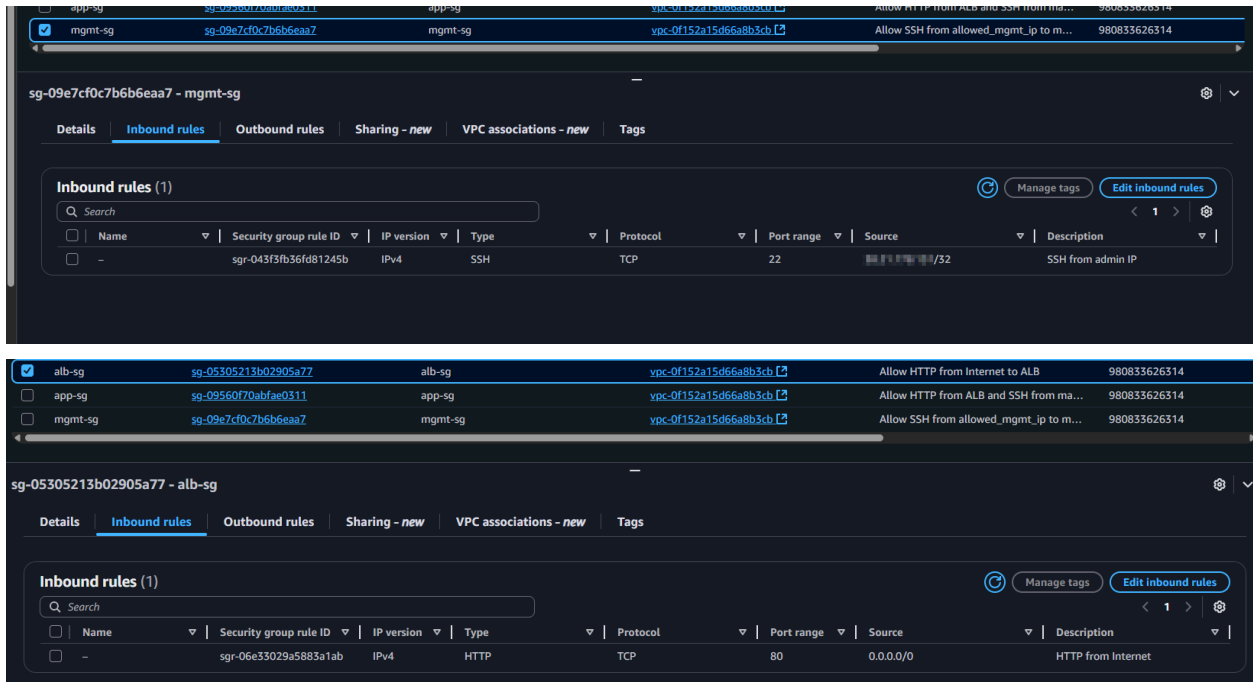
sg-09560f70abfae0311 - app-sg

Details
Inbound rules
Outbound rules
Sharing - new
VPC associations - new
Tags

Inbound rules (2)

Manage tags
Edit inbound rules

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-0f7dd582900807952	-	HTTP	TCP	80	sg-05305213b02905a77 / alb-sg	HTTP from ALB
<input type="checkbox"/>	-	sgr-00c65eb16e38f6b05	-	SSH	TCP	22	sg-09e7cf0c7b6b6eaa7 / mgm...	SSH from management instance



Measure-Command {terraform apply -auto-approve | Out-File -FilePath "apply.log" -Encoding utf8}

```
Days           : 0
Hours          : 0
Minutes        : 3
Seconds        : 35
Milliseconds   : 556
Ticks          : 2155563592
TotalDays      : 0.00249486526851852
TotalHours     : 0.0598767664444444
TotalMinutes   : 3.59260598666667
TotalSeconds   : 215.5563592
TotalMilliseconds : 215556.3592
```

Measure-Command {terraform destroy -auto-approve | Out-File -FilePath "destroy.log" -Encoding utf8}

```
Days           : 0
Hours          : 0
Minutes        : 6
Seconds        : 41
```

```
Milliseconds      : 438
Ticks             : 4014384869
TotalDays         : 0.00464627878356481
TotalHours        : 0.111510690805556
TotalMinutes      : 6.69064144833333
TotalSeconds      : 401.4384869
TotalMilliseconds : 401438.4869
```