U.S. DEPARTMENT OF ENERGY'S

CYBERFORCE COMPETITION®

DEFENDING U.S. ENERGY INFRASTRUCTURE

BLUE TEAM AWS AND VPN INSTRUCTIONS

2024

CYBERFORCE COMPETITION®

CONTENTS

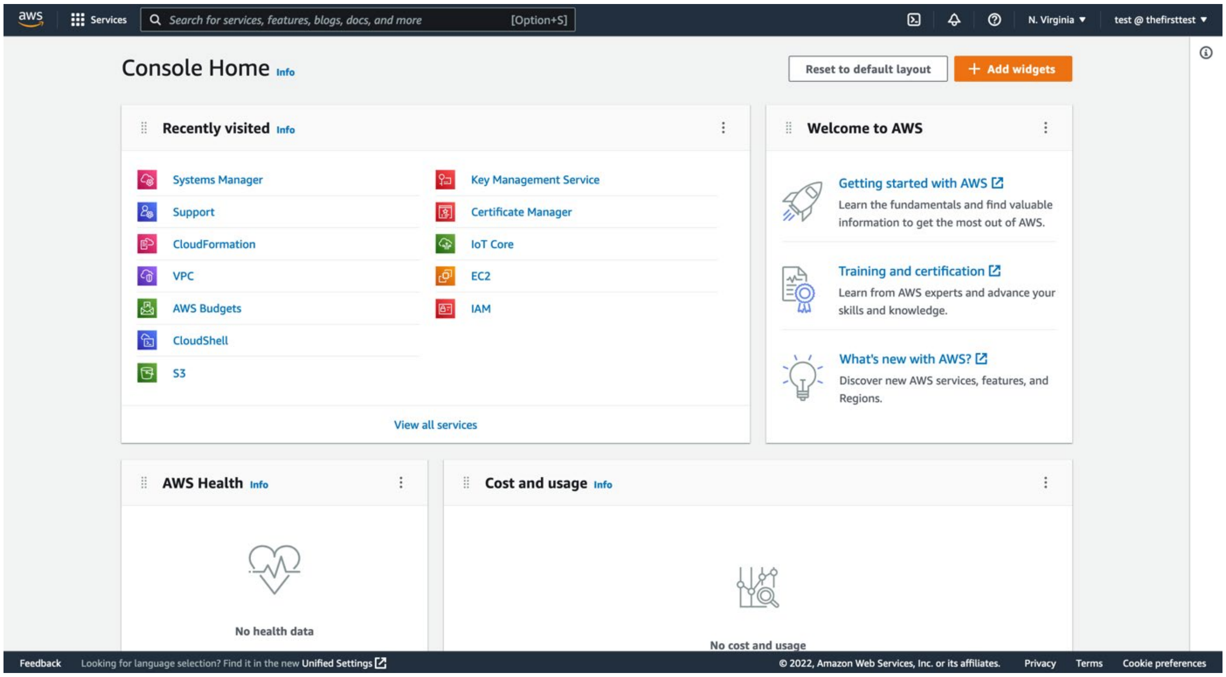
INTRODUCTION

You have been provided with access to a resource pool in Amazon Web Services (AWS), which will be used to host all virtual machines for the Department of Energy's 2024 CyberForce Competition®. This document will provide you with instructions on the use of and details about the virtual machines in AWS.

AWS

Included with this email, you should have received credentials for your AWS environment. You may login to your competition environment at [AWS Signin](). After logging in,

- Update your password
- You'll be brought to the screen pictured below

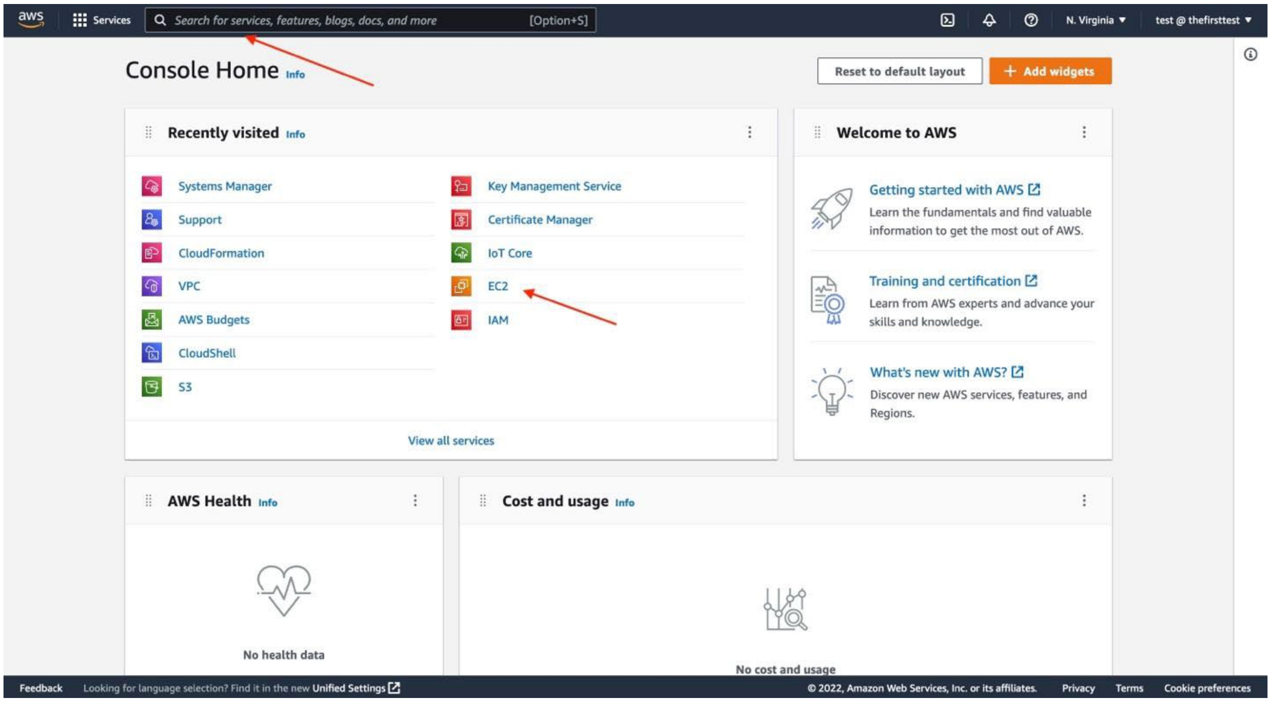


Learn the fundamentals and find valuable information to get the most out of AWS.

Learn from AWS experts and advance your skills and knowledge.

Discover new AWS services, features, and Regions.

To view your team's virtual machines, use the search bar and search for "EC2" or click on "EC2" on the middle of the page.



Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.

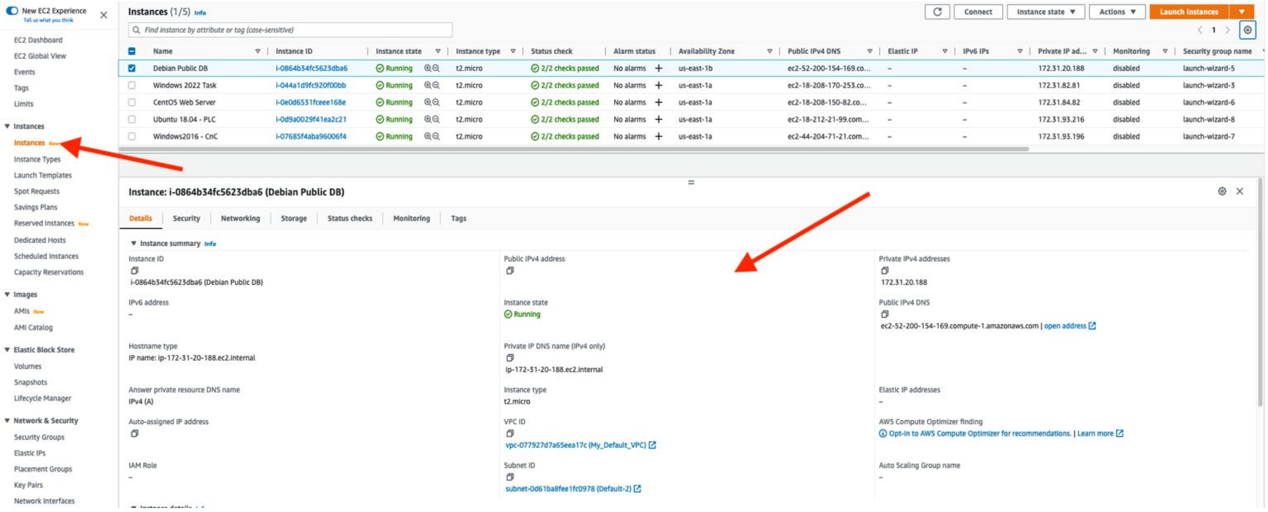
Training and certification
Learn from AWS experts and advance your skills and knowledge.

What's new with AWS?
Discover new AWS services, features, and Regions.

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates.

From the EC2 dashboard menu, click on "Instances" to view the list of your team's virtual machines. Clicking on a virtual machine will reveal additional details and settings below. All the provided virtual machines have been connected to your virtual network which provides an address space of 10.0.#.0/27. <u>This IP does not have a correlation to your team number so make sure you memorize it!</u>



Instances (1/5) Info

Find instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Elastic IP	IPv6 IPs	Private IP ad...	Monitoring	Security group name
☑	Debian Public DB	i-0864b34fc5623dba6	Running	t2.micro	2/2 checks passed	No alarms +	us-east-1b	ec2-52-200-154-169.co...	–	–	172.31.20.188	disabled	launch-wizard-5
□	Windows 2022 Task	i-044a1d9fc920f00bb	Running	t2.micro	2/2 checks passed	No alarms +	us-east-1a	ec2-18-208-170-253.co...	–	–	172.31.82.81	disabled	launch-wizard-3
□	CentOS Web Server	i-0e0d6531fceee168e	Running	t2.micro	2/2 checks passed	No alarms +	us-east-1a	ec2-18-208-150-82.co...	–	–	172.31.84.82	disabled	launch-wizard-6
□	Ubuntu 18.04 - PLC	i-0d9a0029f41ea2c21	Running	t2.micro	2/2 checks passed	No alarms +	us-east-1a	ec2-18-212-21-99.com...	–	–	172.31.93.216	disabled	launch-wizard-8
□	Windows2016 - CnC	i-07685f4aba96006f4	Running	t2.micro	2/2 checks passed	No alarms +	us-east-1a	ec2-44-204-71-21.com...	–	–	172.31.93.196	disabled	launch-wizard-7

Instance: i-0864b34fc5623dba6 (Debian Public DB)

▼ Instance summary Info

Instance ID
i-0864b34fc5623dba6 (Debian Public DB)

IPv6 address
–

Hostname type
IP name: ip-172-31-20-188.ec2.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address

IAM Role
–

Public IPv4 address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-20-188.ec2.internal

Instance type
t2.micro

VPC ID
vpc-077927d7a65eea17c (My_Default_VPC)

Subnet ID
subnet-0d61ba8fee1fc0978 (Default-2)

Private IPv4 addresses
172.31.20.188

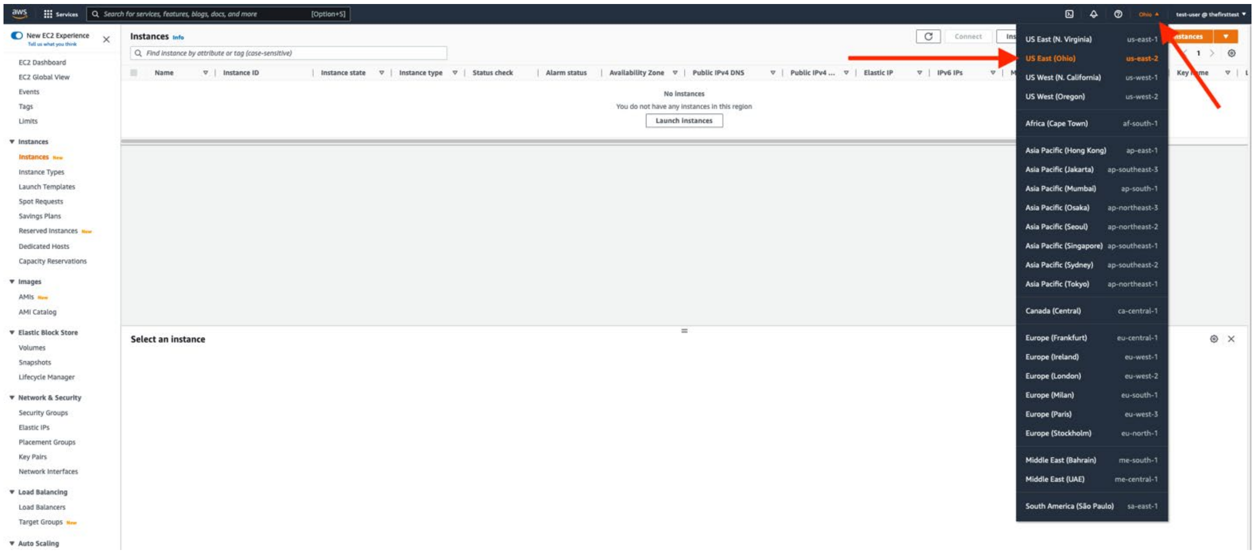
Public IPv4 DNS
ec2-52-200-154-169.compute-1.amazonaws.com | open address

Elastic IP addresses
–

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

Auto Scaling Group name
–

If you are unable to see your machines, make sure you are in the correct region on the top right of the page. You should be in the "US East (Ohio)" region.


Services
Search for services, features, blogs, docs, and more [Option+S]
Ohio
test-user @ thefirsttest
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances New
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances New
Dedicated Hosts
Capacity Reservations
Images
AMIs New
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Load Balancing
Load Balancers
Target Groups New
Auto Scaling
Instances Info
Find instance by attribute or tag (case-sensitive)
Connect
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
IPv6 IPs
Key Name
Launch instances
Select an instance
US East (N. Virginia) us-east-1
US East (Ohio) us-east-2
US West (N. California) us-west-1
US West (Oregon) us-west-2
Africa (Cape Town) af-south-1
Asia Pacific (Hong Kong) ap-east-1
Asia Pacific (Jakarta) ap-southeast-3
Asia Pacific (Mumbai) ap-south-1
Asia Pacific (Osaka) ap-northeast-3
Asia Pacific (Seoul) ap-northeast-2
Asia Pacific (Singapore) ap-southeast-1
Asia Pacific (Sydney) ap-southeast-2
Asia Pacific (Tokyo) ap-northeast-1
Canada (Central) ca-central-1
Europe (Frankfurt) eu-central-1
Europe (Ireland) eu-west-1
Europe (London) eu-west-2
Europe (Milan) eu-south-1
Europe (Paris) eu-west-3
Europe (Stockholm) eu-north-1
Middle East (Bahrain) me-south-1
Middle East (UAE) me-central-1
South America (São Paulo) sa-east-1

No instances

You do not have any instances in this region

VPN CONNECTIONS

Your VPN has been setup to provide your Blue team with a connection to your subnet to allow for interaction with your machines. A .OVPN file that contains everything you need to connect your machine to your network will be sent separately.

To use your provided .OVPN file, you can use the below OpenVPN COMMUNITY clients. Examples below have been tested with this environment.

- Windows - https://openvpn.net/community-downloads/
    - You'll have to move the .OVPN file to the "Program Files/Openvpn/config directory.
- Mac - https://www.tunnelblick.net or https://openvpn.net/client-connect-vpn-for-mac-os/
    - Double click the .OVPN file and it should import it to Tunnelblick.
- Linux - apt (or yum) install openvpn
    - Run 'openvpn –config OVPN_FILE_NAME.ovpn'

Connecting to the VPN will **not** redirect all your traffic through the VPN. It will only redirect traffic destined towards your Blue team's subnet space of 10.0.#.0/27. Once connected, you will have access to your machines on 10.0.#.0/27. If you have issues, please disconnect and try to reconnect before you reach out.

PROVIDED MACHINES

Your team has been provided with **6 machines, plus the MapBox VM**. You *will need* to implement and/or configure services on some machines in your environment.

- Do not delete the provided machines.

- Do not alter anything within the Assume Breach Infrastructure, unless instructed to by Red or White team personnel.
- You may move and alter services within the Traditional Infrastructure, except for scored services, but “green03” and “test04” SSH and RDP users must remain intact with no configuration, permission, or password changes.
- The required services provided MUST be the services used for scoring purposes in the scoreboard on the machines provided.
- If you restore these machines from a backup, name them identically to how they were provided.

YOU SHOULD NEVER NEED TO CONFIGURE ANY EXTERNAL AWS DNS ROUTING UTILIZING THE X.BLUEXXXX.CFC.LOCAL DOMAIN. THIS IS ALREADY CONFIGURED AT THE AWS LEVEL AND DOES NOT NEED TO BE MODIFIED.

TRADITIONAL INFRASTRUCTURE

TASK BOX – WINDOWS SERVER 2022 (10.0.X.144)

Local Credentials (RDP) – blueteam : BlueTeam2024!

PUBLIC DB – OPENSUSE 15 (10.0.X.143)

Local Credentials (SSH) – blueteam : BlueTeam2024!

AD/DNS – WINDOWS SERVER 2019 (10.0.X.145)

Local Credentials (SSH) – blueteam : BlueTeam2024!

ASSUME BREACH INFRASTRUCTURE

WEB SERVER - CENTOS7 (10.0.X.142)

Local Credentials (SSH) – blueteam : BlueTeam2024!

CNC – WINDOW SERVER 2016 (10.0.X.141)

Local Credentials (RDP) – blueteam : BlueTeam2024!

PLC – UBUNTU 22.04 (10.0.X.140)

Local Credentials (SSH) – blueteam : BlueTeam2024!