

U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE
COMPETITION[®]

DEFENDING U.S. ENERGY INFRASTRUCTURE

AWS and VPN Instructions

2025

CYBERFORCE COMPETITION®

CONTENTS

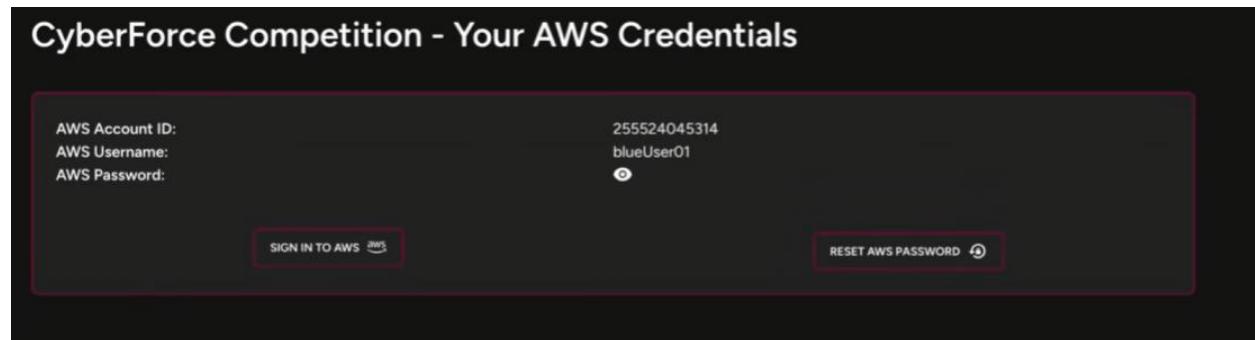
<u>INTRODUCTION.....</u>	<u>2</u>
<u>AWS.....</u>	<u>2</u>
<u>VPN CONNECTIONS.....</u>	<u>4</u>
<u>PROVIDED MACHINES.....</u>	<u>5</u>
TRADITIONAL INFRASTRUCTURE.....	5
TASK Box – UBUNTU 22.04 (10.0.x.144).....	5
PUBLIC DB – WINDOWS SERVER 2022 (10.0.X.140).....	6
AD/DNS – WINDOWS SERVER 2019 (10.0.x.141).....	6
WEB SERVER – OPENSUSE LEAP 15 (10.0.X.145)	6
ASSUME BREACH INFRASTRUCTURE	6
HMI – WINDOW SERVER 2019 (10.0.X.142)	6
PLC – UBUNTU 22.04 (10.0.X.143).....	6
<u>HOW TO MAKE & RESTORE FROM SNAPSHOTS.....</u>	<u>7</u>

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 2025 CyberForce Competition®. This document will provide you with instructions on the use of and details about the virtual machines in AWS.

AWS

Within the Controller, you should have received credentials for your Team AWS environment. Here you can also reset your AWS password.



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

A screenshot of the AWS Console Home page. The top navigation bar shows "Services", a search bar, and "N. Virginia". The main area features three sections: "Recently visited" (listing Systems Manager, Support, CloudFormation, VPC, AWS Budgets, CloudShell, and S3), "Welcome to AWS" (with links to Getting started with AWS, Training and certification, and What's new with AWS?), and "AWS Health" and "Cost and usage" sections. The bottom footer includes links for Feedback, Unified Settings, Copyright notice, Privacy, Terms, and Cookie preferences.

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.

The screenshot shows the AWS Console Home dashboard. At the top, there is a search bar with the placeholder "Search for services, features, blogs, docs, and more" and a "Reset to default layout" button. On the right, it shows "N. Virginia" and "test @ thefirsttest". Below the search bar, there are two main sections: "Recently visited" and "Welcome to AWS". The "Recently visited" section lists various services with icons: Systems Manager, Key Management Service; Support, Certificate Manager; CloudFormation, IoT Core; VPC, EC2 (highlighted with a red arrow); AWS Budgets, IAM; CloudShell; and S3. The "Welcome to AWS" section includes links for "Getting started with AWS", "Training and certification", and "What's new with AWS?". At the bottom, there are links for "Feedback", "Looking for language selection?", "Privacy", "Terms", and "Cookie preferences".

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 virtual machines provided have been connected to your virtual network which provides an address space of 10.0.#.0/27. This IP does not have a correlation to your team number so make sure you memorize it!

The screenshot shows the AWS EC2 Instances dashboard. On the left, there is a sidebar with links: New EC2 Experience, EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (highlighted with a red arrow), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances (new), Dedicated Hosts, Scheduled Instances, 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. The main area shows a table of instances. One instance, "Debian Public DB", is selected and shown in a detailed view. The detailed view includes tabs for Details, Security, Networking, Storage, Status checks, Monitoring, and Tags. Under the Details tab, there is an "Instance summary" section with fields for Instance ID (i-0864b34fc5623db6), Public IPv4 address (172.31.20.188), Instance state (Running), Private IPv4 address (172.31.82.81), and Public IPv4 DNS (ec2-52-200-154-169.compute-1.amazonaws.com). A red arrow points from the "Public IPv4 address" field to the right.

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.

The screenshot shows the AWS EC2 Instances page. On the left is a navigation sidebar with various services like EC2 Dashboard, Events, Tags, Limits, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The main area shows a table with columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4, Elastic IP, and IPv6 IPs. A search bar at the top says "Find instance by attribute or tag (case-sensitive)". Below the table, it says "No Instances" and "You do not have any instances in this region". At the bottom is a "Launch Instances" button. On the right, there's a "Regions" dropdown menu with a red arrow pointing to the "US East (Ohio)" option, which is highlighted. Other regions listed include US East (N. Virginia), US West (N. California), US West (Oregon), Africa (Cape Town), Asia Pacific (Hong Kong), Asia Pacific (Jakarta), Asia Pacific (Mumbai), Asia Pacific (Osaka), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), Canada (Central), Europe (Frankfurt), Europe (Ireland), Europe (London), Europe (Milan), Europe (Paris), Europe (Stockholm), Middle East (Bahrain), Middle East (UAE), and South America (São Paulo).

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. The .ovpn file that contains everything you need to connect your machine to your network will be obtained through the Controller.

CyberForce Competition - VPN Files & Instructions

VPN Instructions

Your VPN has been setup to provide your Blue team with a connection to your subnet to allow for interaction with your machines. The .ovpn files below contain everything you need to connect your machine to your network.

Connecting to the VPN will NOT redirect all of 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.

In order to use the provided .ovpn files, you can use the below OpenVPN Community Clients. Examples below have been tested with this environment.

- Windows - <https://openvpn.net/community/>
You'll have to move the .ovpn file to the "Program Files\Openvpn\config" directory after installation.
- 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 or OpenVPN.
- Linux - <https://community.openvpn.net/Pages/OpenVPN3Linux>
Run `openvpn --config OVPN_FILE_NAME.ovpn`

VPN Files

TCP VPN FILE

UDP VPN FILE

To use your provided .ovpn file, you can use the **OPENVPN COMMUNITY CLIENTS** below. Examples below have been tested with this environment.

- Windows – OpenVPN Community - <https://openvpn.net/community-downloads/>
 - Place the OVPN file into “C:\Program Files\Openvpn\config”.
- MacOS – Tunnelblick - <https://www.tunnelblick.net> or <https://openvpn.net/client-connect-vpn-for-mac-os/>
 - Double click the OVPN file to import it to Tunnelblick
- Linux – sudo apt (or yum) install openvpn
 - Run “openvpn --config YOUR_OVPN_FILE.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. Details on these machines’ services and credentials are provided below. You will need to implement and/or configure services on some machines in your environment. **DO NOT DELETE THE MACHINES PROVIDED.**

Within the Assume Breach Infrastructure, you can install and configure monitoring software, but at your team’s own risk. If Red team or the scoreboard is unable to interact with your VMs due to modification not instructed via Red/White Team, it may cost your team points. Users “**SCORE1**” and “**SCORE2**” SSH and RDP users must remain intact with **no configuration or permission changes**. The **REQUIRED SERVICES PROVIDED MUST** be the services used for scoring purposes on the scoreboard. 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.bluexxx.cfc.local domain.**
This is already configured at the AWS level and does not need to be modified.

TRADITIONAL INFRASTRUCTURE

TASK BOX – UBUNTU 22.04 (10.0.X.144)

Local Credentials (SSH,RDP) – **blueteam : BlueTeam2025!**

SMB - 139/445

IMAP - 143/993

SMTP - 25

SSH - 22

PUBLIC DB – WINDOWS SERVER 2022 (10.0.X.140)

Local Credentials (RDP) – blueteam : BlueTeam2025!

SMB - 139/445

phpmyadmin - 80

MariaDB - 3306

DB Credentials - root : BlueTeam2025!
- website_u : BlueTeam2025!

AD/DNS – WINDOWS SERVER 2019 (10.0.X.141)

Local Credentials (RDP) – blueteam : BlueTeam2025!

LDAP - 389

WinRM - 5985/5986

WEB SERVER – OPENSUSE LEAP 15 (10.0.X.145)

Local Credentials (SSH) – blueteam : BlueTeam2025!

HTTP - 80

NFS - 111/2049

ASSUME BREACH INFRASTRUCTURE

HMI – WINDOW SERVER 2019 (10.0.X.142)

Local Credentials (RDP) – blueteam : BlueTeam2025!

HMI - 8088

MySQL - Data Historian - 3306

DB Credentials - blueteam : BlueTeam2025!

PLC – UBUNTU 22.04 (10.0.X.143)

Local Credentials (SSH) – blueteam : BlueTeam2025!

PLC - 502

HOW TO MAKE & RESTORE FROM SNAPSHOTS OR RE-IMAGE

1. Within the Controller, you should see the “Manage AWS EC2 Snapshots” button

The screenshot shows the CyberForce Competition homepage. At the top, it says "CyberForce Competition". Below that, it says "Starts November 15, 2025 at 10:00 AM CST" and "Ends November 15, 2025 at 06:00 PM CST". In the center, there is a logo for "U.S. DEPARTMENT OF ENERGY'S CYBERFORCE COMPETITION DEFENDING U.S. ENERGY INFRASTRUCTURE". To the right, there is a vertical list of buttons: "JOIN DISCORD SERVER" (with a discord icon), "VIEW SCOREBOARD" (with a chart icon), "VIEW GAMES" (with a game controller icon), "VIEW AWS CREDENTIALS" (with an AWS icon), "MANAGE AWS EC2 SNAPSHOTS" (with a folder icon), and "VIEW VPN FILES & INSTRUCTIONS" (with a gear icon).

2. Click on which VM you would like to make or restore a snapshot with.

The screenshot shows a list of VM instances under the heading "CyberForce Competition - AWS EC2 Snapshots". The instances are:

- PLC
i-0660c3e7dd3f21e48
- Task
i-069afe46406d5b545
- AD
i-0b1ab11ab3755a403
- Webservice
i-0a64d1a7630dcff18
- DB
i-0c2099acd32eaa23d
- HMI
i-029c21e7e181e76e9

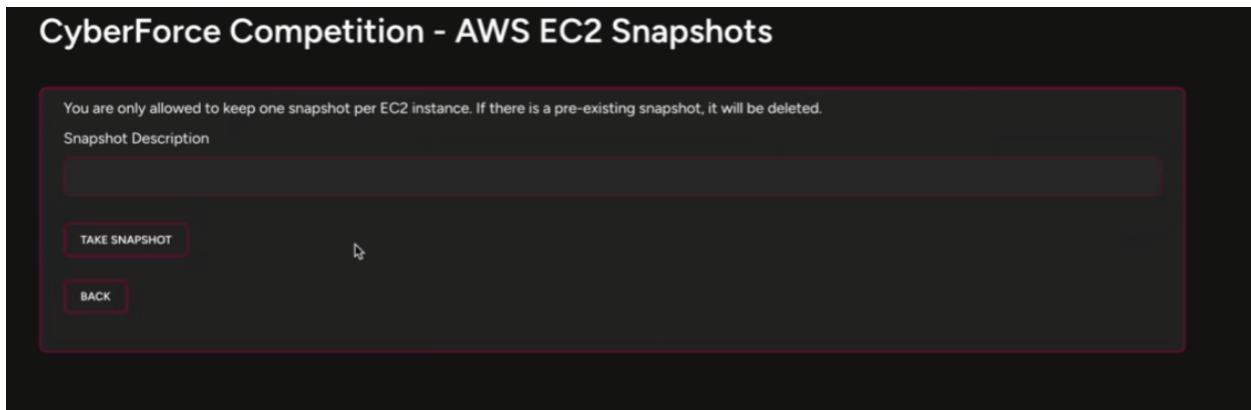
At the bottom right is a "NEXT" button.

3. Click if you would like to Restore Snapshot or Take New Snapshot.

The screenshot shows three buttons under the heading "CyberForce Competition - AWS EC2 Snapshots": "RESTORE SNAPSHOT" (with a circular arrow icon), "REIMAGE EC2 INSTANCES BACK TO LAUNCH STATE" (with a camera icon), and "TAKE NEW SNAPSHOT" (with a camera icon). At the bottom left is a "BACK" button.

4. If RESTORING from a snapshot, click “RESTORE SNAPSHOT”, the system will automatically use the most up to date snapshot you have created, and send an email with a success or failure message.

If CREATING a new snapshot, click “TAKE NEW SNAPSHOT”, you can provide a description of the snapshot for the AWS console. Once you “TAKE SNAPSHOT”, you will be sent an email with whether it was successful in taking a snapshot.



5. If your team damages any virtual machines beyond the point of recovery, you may restore to a fresh, default image of the system by clicking “REIMAGE EC2 INSTANCES BACK TO LAUNCH STATE”. However, your team will incur a scoring penalty of **150 points per VM restoration**.

