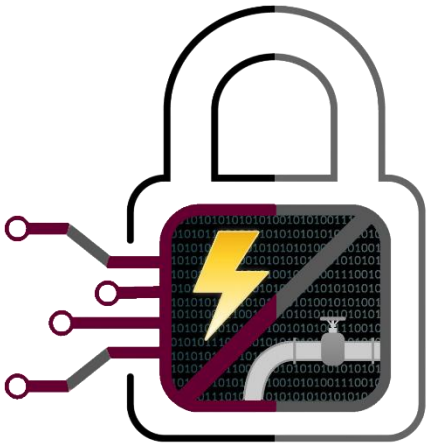


U.S. DEPARTMENT OF ENERGY'S

CYBERFORCE COMPETITION®

DEFENDING U.S. ENERGY INFRASTRUCTURE

AWS and VPN Instructions

2025

CYBERFORCE COMPETITION®

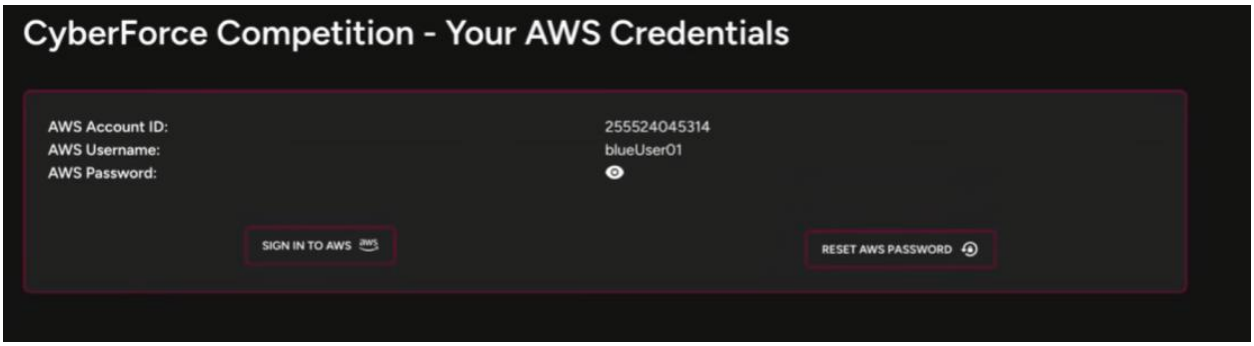
CONTENTS

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

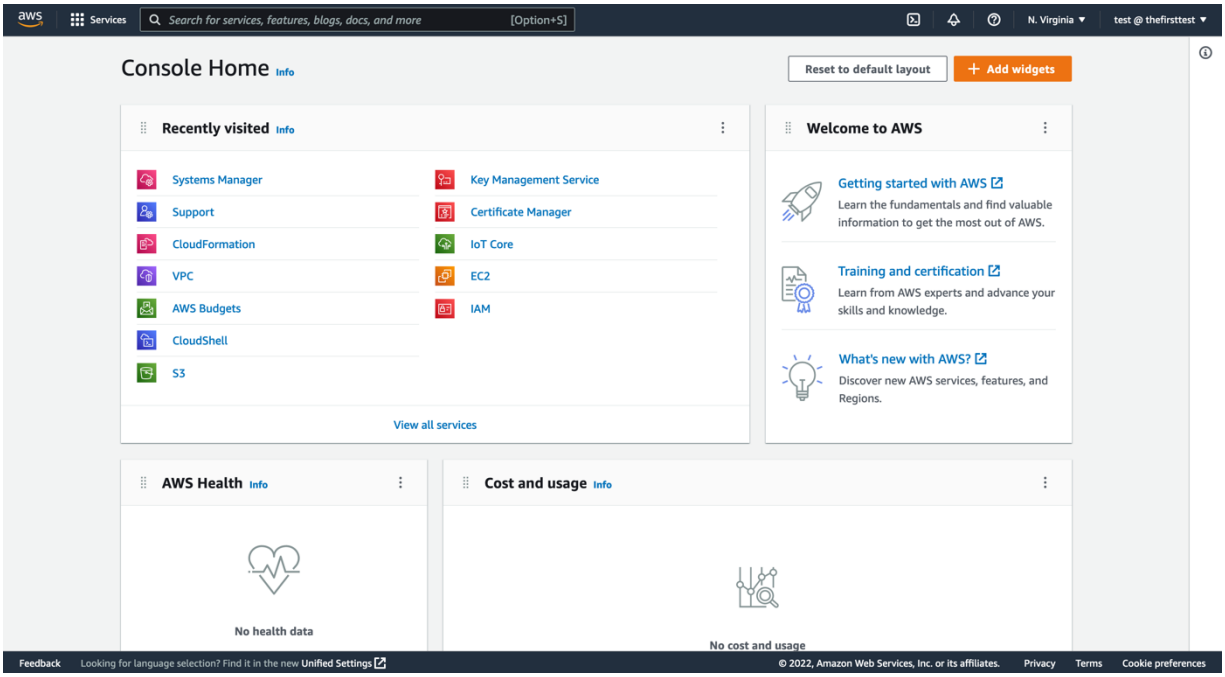
AWS

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

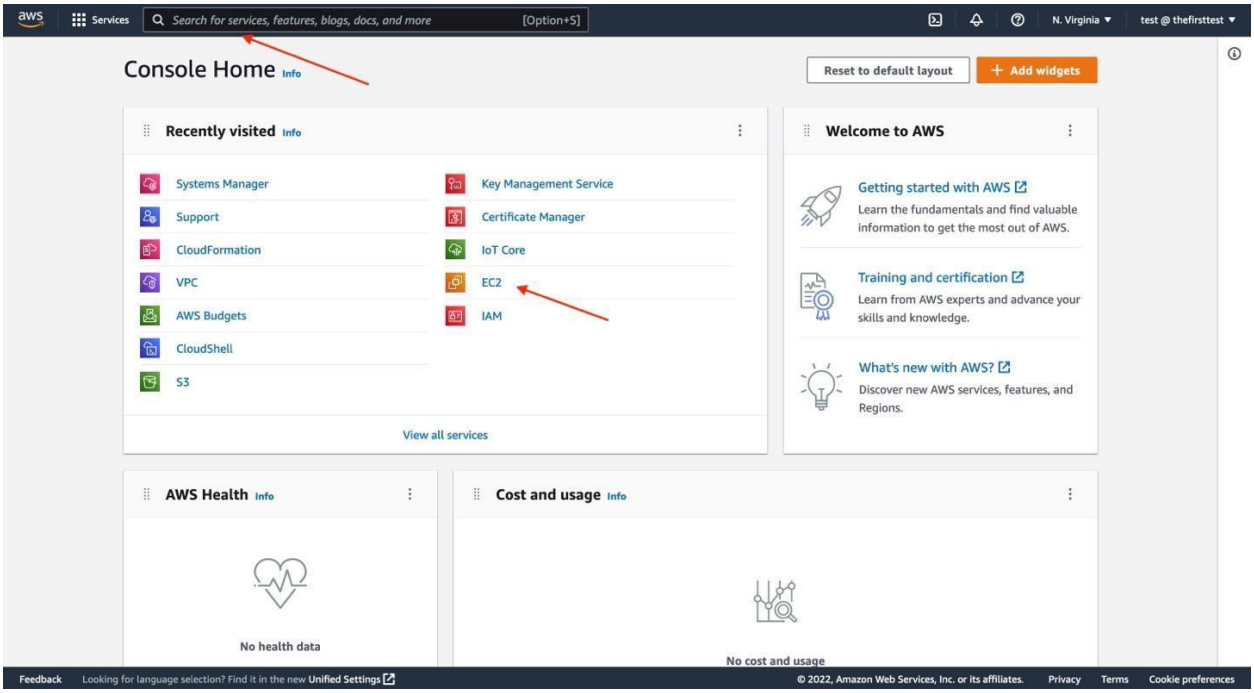


You may login to your competition environment at AWS_Signin. After logging in,

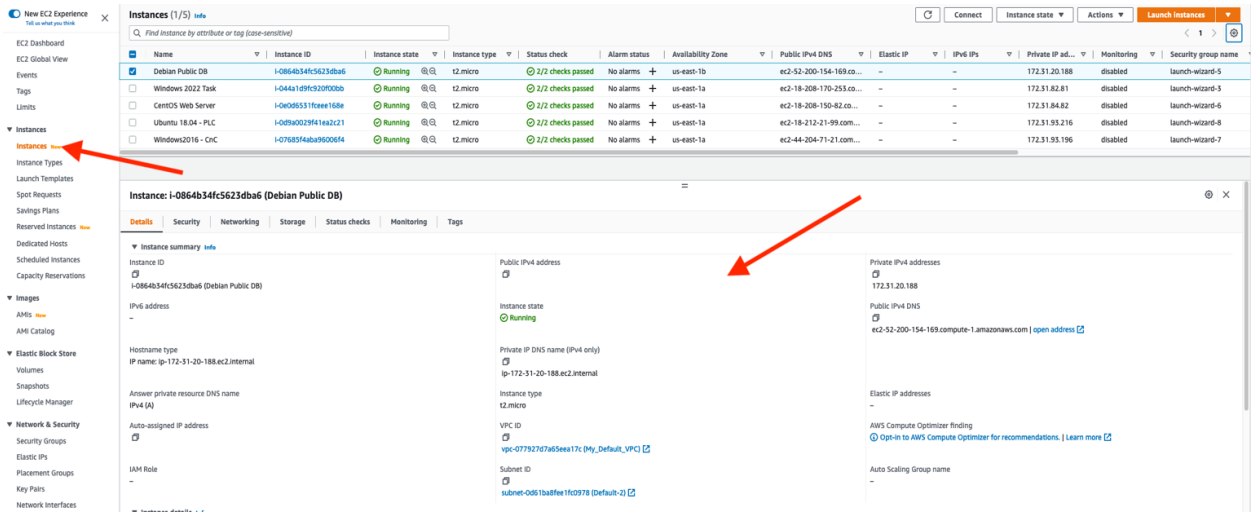
- Update your password
- You'll be brought to the screen pictured below



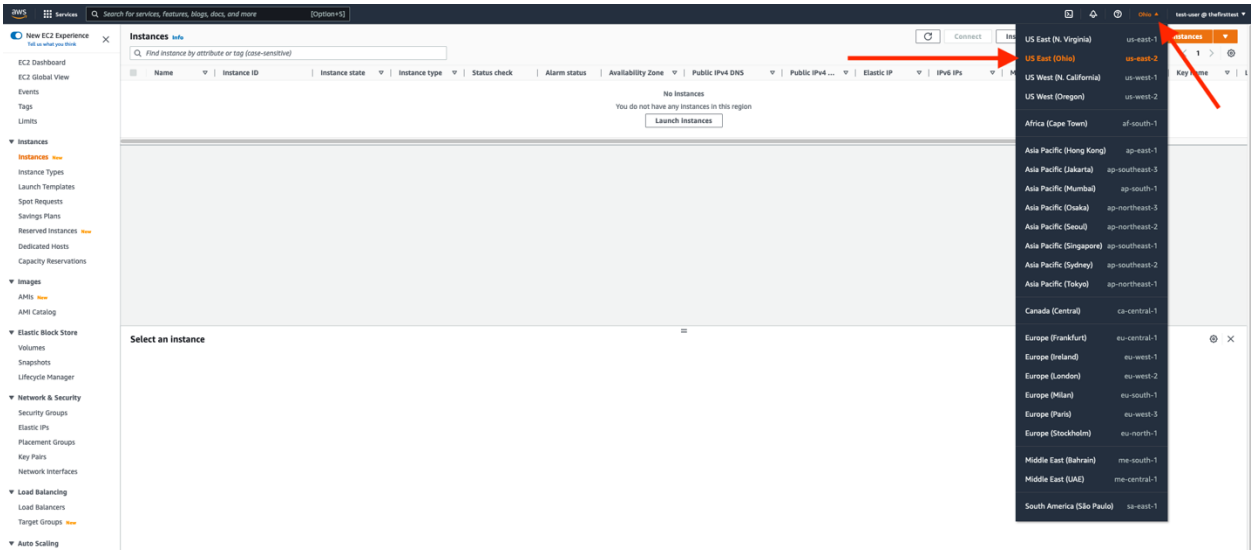
To view your team's virtual machines, use the search bar and search for "EC2" or click on "EC2" on the middle of the page.



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. <u>This IP **does not** have a correlation to your team number so make sure you memorize it!</u>

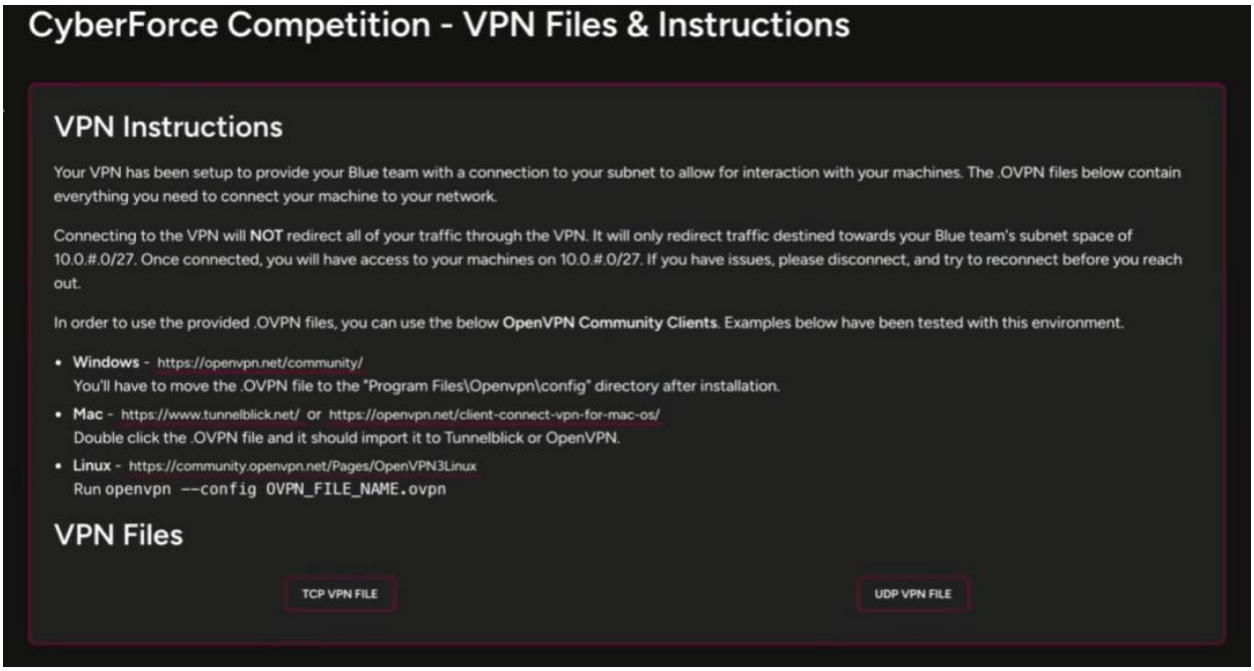


If you are unable to see your machines, make sure you are in the correct region on the top right of the page. You should be in the “US East (Ohio)” region.



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.



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.bluexxxx.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!

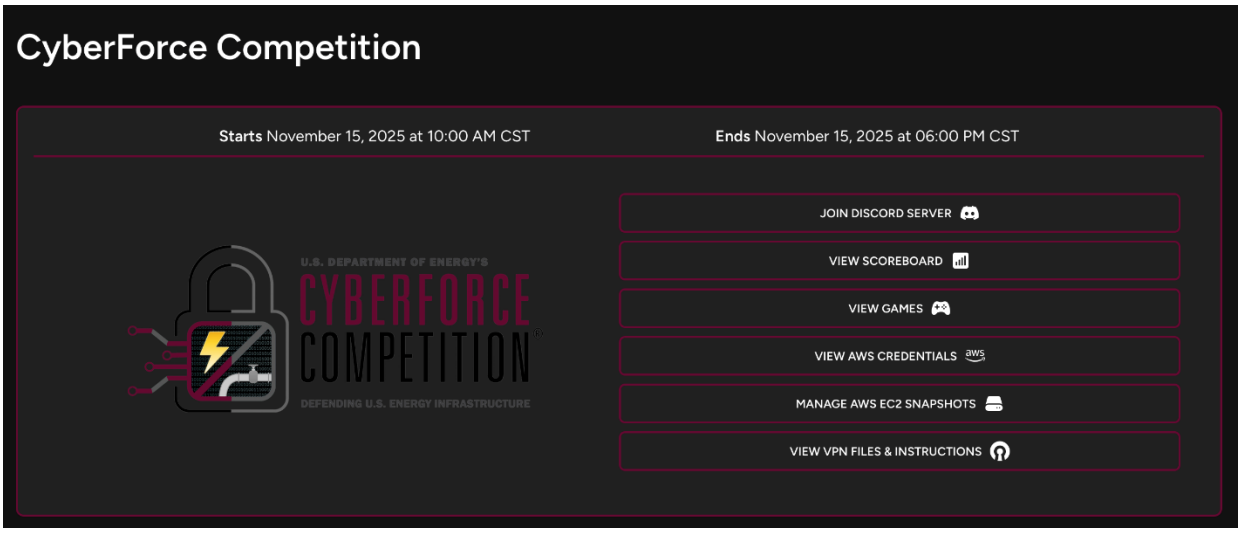
PLC – UBUNTU 22.04 (10.0.X.143)

Local Credentials (SSH) – blueteam : BlueTeam2025!

PLC - 502

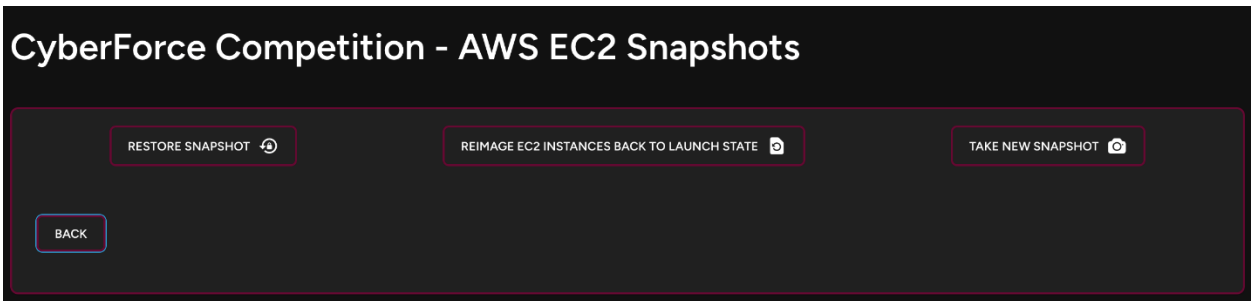
HOW TO MAKE & RESTORE FROM SNAPSHOTS OR RE-IMAGE

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



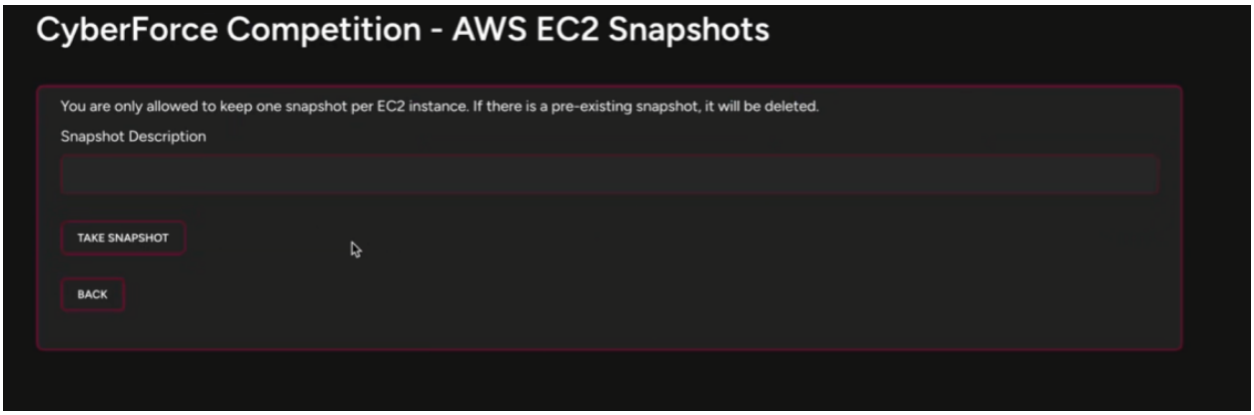
2. Click on which VM you would like to make or restore a snapshot with.

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



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**.