Blue Team Azure and VPN Instructions

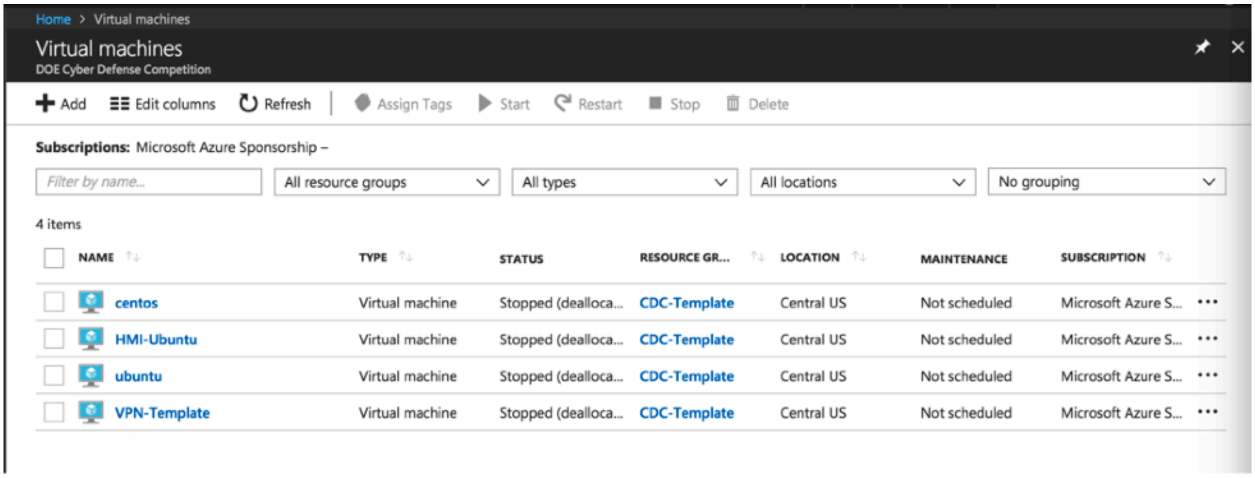
Introduction

Hello blue team member!

You have been provided with access to a resource pool in Microsoft Azure, which will be used to host all virtual machines for the Department of Energy's Spring 2018 Cyber Defense Competition. This document will provide you with instructions on the use of and details about the virtual machines in Azure.

Azure

Included with this email, you should have received credentials for your Azure environment. You may login to your competition environment at http://portal.azure.com. After logging in, there is a tour of the Microsoft Azure interface available if you are unfamiliar with this environment.

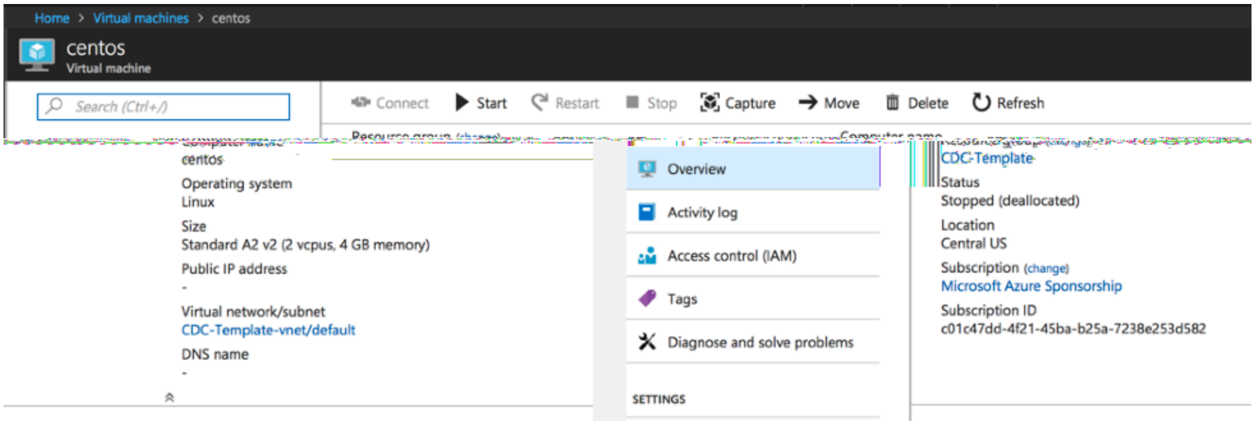


Subscriptions: Microsoft Azure Sponsorship –

4 items

NAME	TYPE	STATUS	RESOURCE GR...	LOCATION	MAINTENANCE	SUBSCRIPTION
centos	Virtual machine	Stopped (dealloca...	CDC-Template	Central US	Not scheduled	Microsoft Azure S...
HMI-Ubuntu	Virtual machine	Stopped (dealloca...	CDC-Template	Central US	Not scheduled	Microsoft Azure S...
ubuntu	Virtual machine	Stopped (dealloca...	CDC-Template	Central US	Not scheduled	Microsoft Azure S...
VPN-Template	Virtual machine	Stopped (dealloca...	CDC-Template	Central US	Not scheduled	Microsoft Azure S...

To view your team's virtual machines, select "Virtual Machines" from the sidebar and it will present you with the list of your virtual machines. You can edit the summary page's columns to view more information (i.e. private IP address) by clicking "Edit columns".



Resource group (change)
CDC-Template

Status
Stopped (deallocated)

Location
Central US

Subscription (change)
Microsoft Azure Sponsorship

Subscription ID
c01c47dd-4f21-45ba-b25a-7238e253d582

Computer name
centos

Operating system
Linux

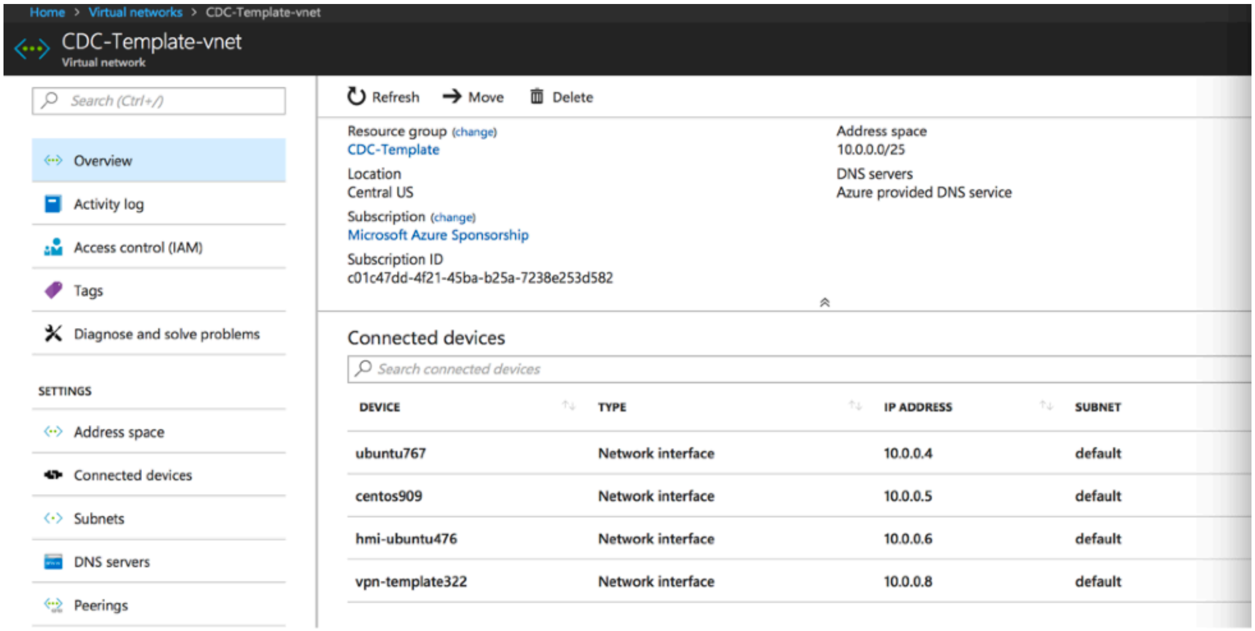
Size
Standard A2 v2 (2 vcpus, 4 GB memory)

Public IP address
-

Virtual network/subnet
CDC-Template-vnet/default

DNS name
-

From the Virtual Machines page, click a virtual machine to view details and configure settings.



Resource group (change)
CDC-Template

Location
Central US

Subscription (change)
Microsoft Azure Sponsorship

Subscription ID
c01c47dd-4f21-45ba-b25a-7238e253d582

Address space
10.0.0.0/25

DNS servers
Azure provided DNS service

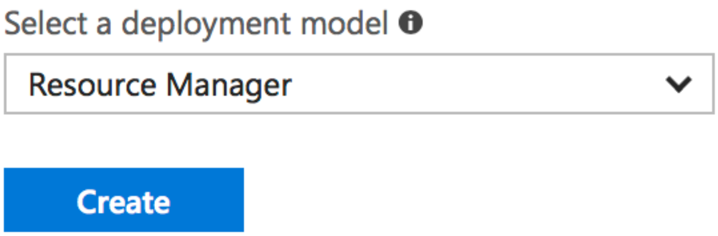
Connected devices

Search connected devices

DEVICE	TYPE	IP ADDRESS	SUBNET
ubuntu767	Network interface	10.0.0.4	default
centos909	Network interface	10.0.0.5	default
hmi-ubuntu476	Network interface	10.0.0.6	default
vpn-template322	Network interface	10.0.0.8	default

All of these machines have been connected to a virtual network that contains an address space of 10.0.TEAM_NUMBER.0/25. This network can be viewed by clicking “Virtual Networks” in the sidebar and clicking on your network.

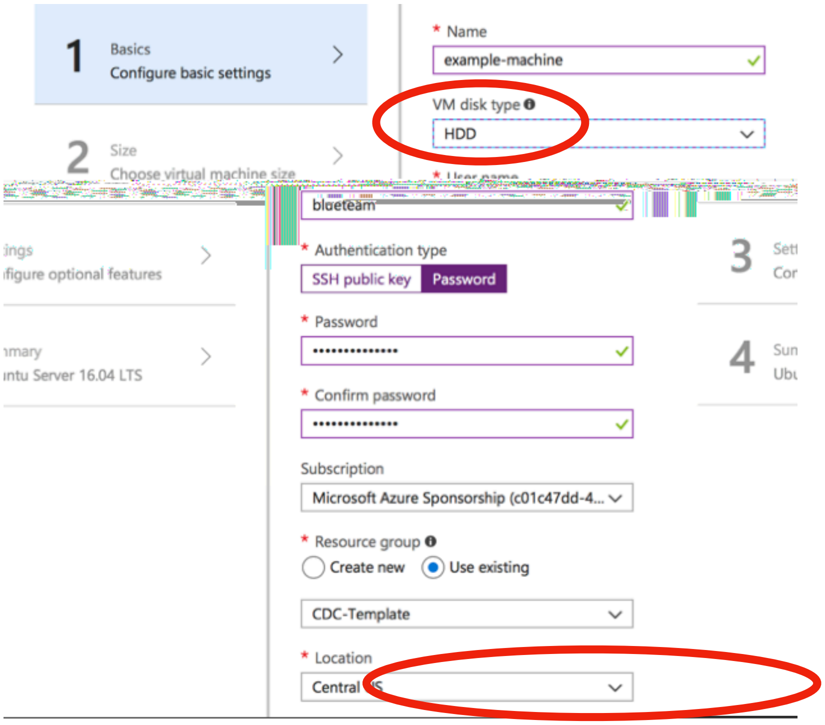
The only subnet that exists under your network will have a route table assigned to it. **Do not change this.** This route table contains routes that tells your virtual network’s router where to route packets that are destined for your VPN subnet. Your VPN subnet is address space



Select a deployment model

Resource Manager

Once you have selected an image, make sure the deployment model is set to “Resource Manager” and click create.



1 Basics
Configure basic settings

2 Size
Choose virtual machine size

3 Sett
Cor

ings
figure optional features

4 Sun
Ubu

mary
ntu Server 16.04 LTS

* Name: example-machine

VM disk type: HDD

* User name: blueteam

* Authentication type: SSH public key | Password

* Password: ••••••••••••••

* Confirm password: ••••••••••••••

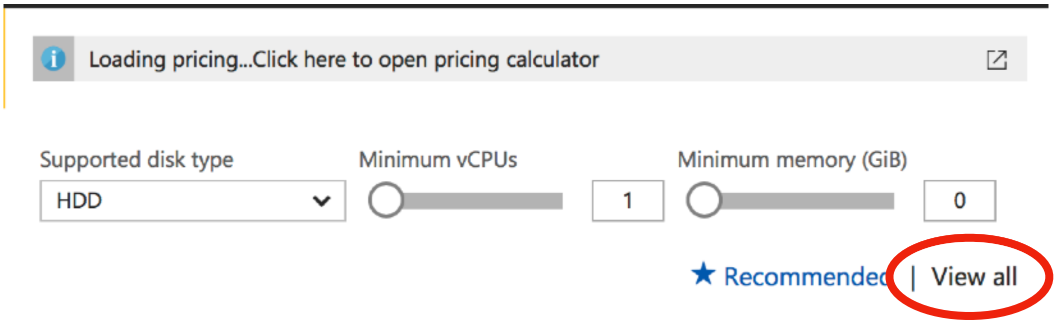
Subscription: Microsoft Azure Sponsorship (c01c47dd-4...

* Resource group: ○ Create new ● Use existing

CDC-Template

* Location: Central US

On the first page, select “VM disk type” as HDD, select your existing resource group that you were assigned, and make sure the location is Central US.



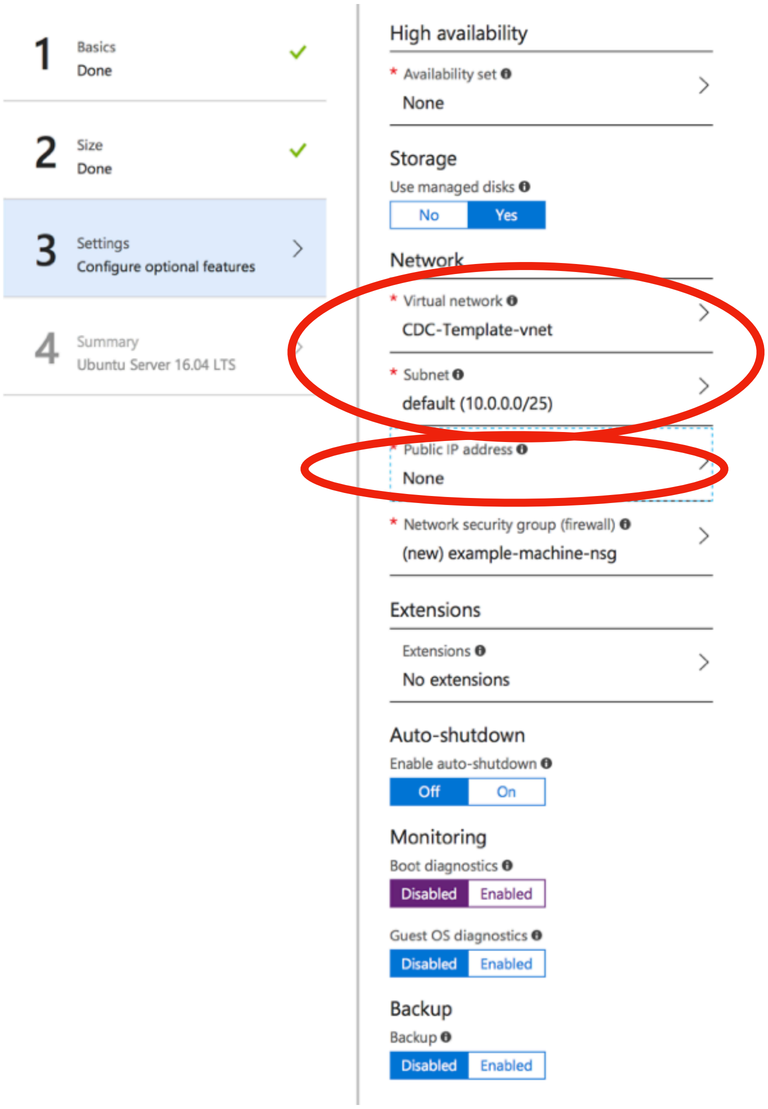
Loading pricing...Click here to open pricing calculator

Supported disk type: HDD

Minimum vCPUs: 1

Minimum memory (GiB): 0

On the next page, you will be asked select a VM size. **Click view all in the corner and scroll down to view A1_v2, A2_v2, and A4_v2. These are the VM sizes permitted in the competition.**



1 Basics
Done ✓

2 Size
Done ✓

3 Settings
Configure optional features

4 Summary
Ubuntu Server 16.04 LTS

High availability

* Availability set
None

Storage

Use managed disks
No [✓ Yes]

Network

* Virtual network
CDC-Template-vnet

* Subnet
default (10.0.0.0/25)

* Public IP address
None

* Network security group (firewall)
(new) example-machine-nsg

Extensions

Extensions
No extensions

Auto-shutdown

Enable auto-shutdown
[✓ Off] On

Monitoring

Boot diagnostics
[✓ Disabled] Enabled

Guest OS diagnostics
[✓ Disabled] Enabled

Backup

Backup
[✓ Disabled] Enabled

On the next page, ensure your VM is assigned to your team's virtual network and **change the public IP to none. There are a limited amount of public IP addresses available and any public IPs assigned to anything other than your VPN will be deleted.**

Finally, you will be provided a summary of the new machine you have created. Ensure everything is correct and click create. Azure will notify you when the creation is complete. You can then login to your new machine through your VPN connection after its creation is completed.

VPN Connection

Your VPN server has been setup to provide you with a connection to your subnet to allow for configuration and monitoring of your machines. Its other primary function is to provide your ICS with a connection to interact with the human machine interface (HMI) on your virtual network. Included in this email is a .OVPN file that contains everything you need to connect your machine to your network. Your ICS device has a similar .OVPN file that it will use to automatically connect to the VPN with an IP of 10.0.TEAM_NUMBER.250 30 seconds after it has been powered on.

In order to use this .OVPN file, you can use any OpenVPN client. Examples below have been tested with this environment.

Windows - https://openvpn.net/index.php/download/community-downloads.html
You'll have to move the .OVPN file to the "Program Files/Openvpn/config directory.

Mac - https://www.tunnelblick.net
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 of your traffic through the VPN. It will only give you access to your subnet. If your VPN client complains about having the same public IP address after connecting, this is intended behavior. Once connected, you will have access to your machines on 10.0.TEAM_NUMBER.0/25.

Provided Machines

Your team has been provided with 4 machines. Details on these machines' credentials and services are provided below. **These machines contain only a portion of the required services. Do not delete these machines. Secure them to the best of your ability.**

- Ubuntudb (10.0.TEAM_NUMBER.4)
  - Username: blueteam
  - Password: CDC2018BlueTeam
  - Mysql
    - This database contains the database used in the centoswebserver's WordPress instance
  - FTP File Share
    - This is a required service to host Green team documentation that can be uploaded for the Green team to be able to download at any time from the WordPress site.
- Centoswebserver (10.0.TEAM_NUMBER.5)
  - Username: blueteam
  - Password: CDC2018BlueTeam
  - WordPress Webserver
    - Username: admin
    - Password: password
    - Provides an interface for green team to interact with your client services. `
    - /var/www/html/wp-config.php
      - Change DB_HOST to your ubuntudb's IP
      - Change WP_HOME and WP_SITEURL to your centoswebserver's IP
    - Change HMI Wordpress iframe's address to your ubuntuhmi's IP
  - Dashboardd Systemd Service
    - Generates a webpage to display the status of the ICS device in WordPress
    - Change IP in /usr/local/bin/update_dashboard to your raspberry pi's IP
- Ubuntuhmi (10.0.TEAM_NUMBER.6)
  - Username: blueteam
  - Password: CDC2018BlueTeam
  - NoVNC graphical desktop on port 6080
    - Password: password
  - For more information on ICS HMI, please read attached Cybati User Manual
- Raspberry Pi PLC (10.0.TEAM_NUMBER.250)
  - Username: pi

  - Password: cybati
  - For more information on the Raspberry Pi PLC, please read attached Cybati User Manual
- VPN (10.0.TEAM_NUMBER.7)
  - This machine is provided solely to establish connectivity to your Azure environment
  - Credentials will NOT be provided as this machine.
  - This machine will be off-limits to the red team and should not be altered in any way.