```
# Project-1 GitHub-Fundamentals - Cloud Security
 Cloud Security - VMs setup including ELK
```

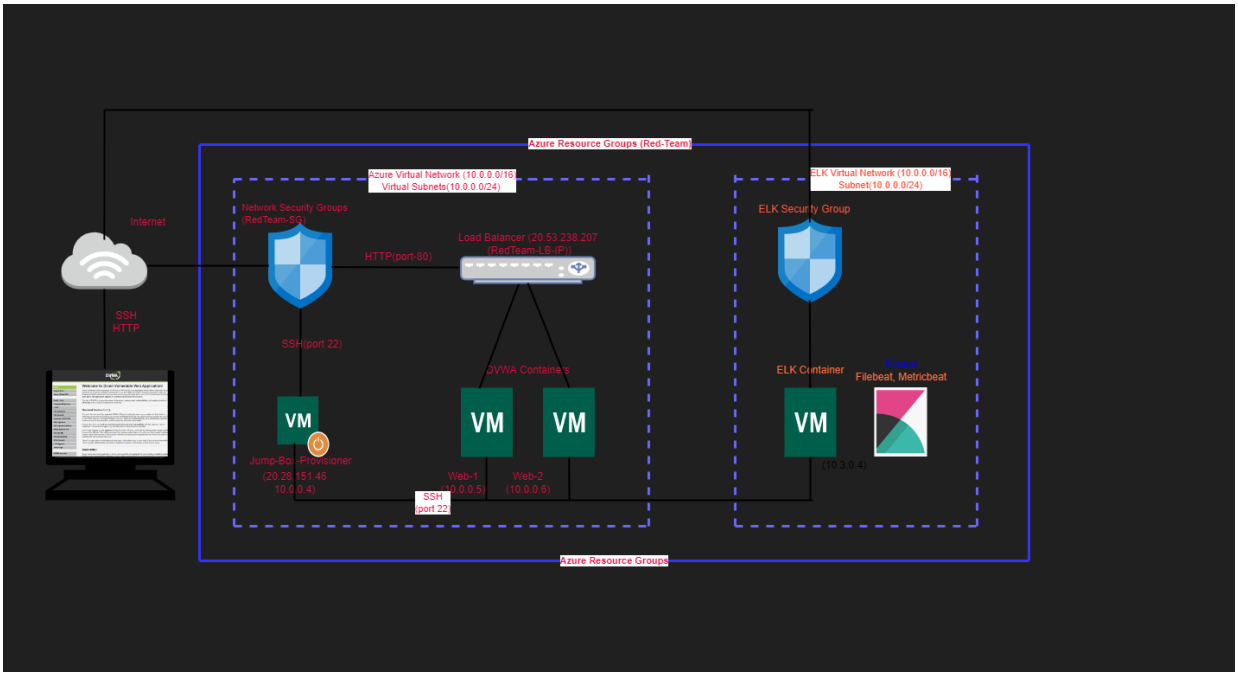
Configuring an ELK Server

Lectures cover the following:

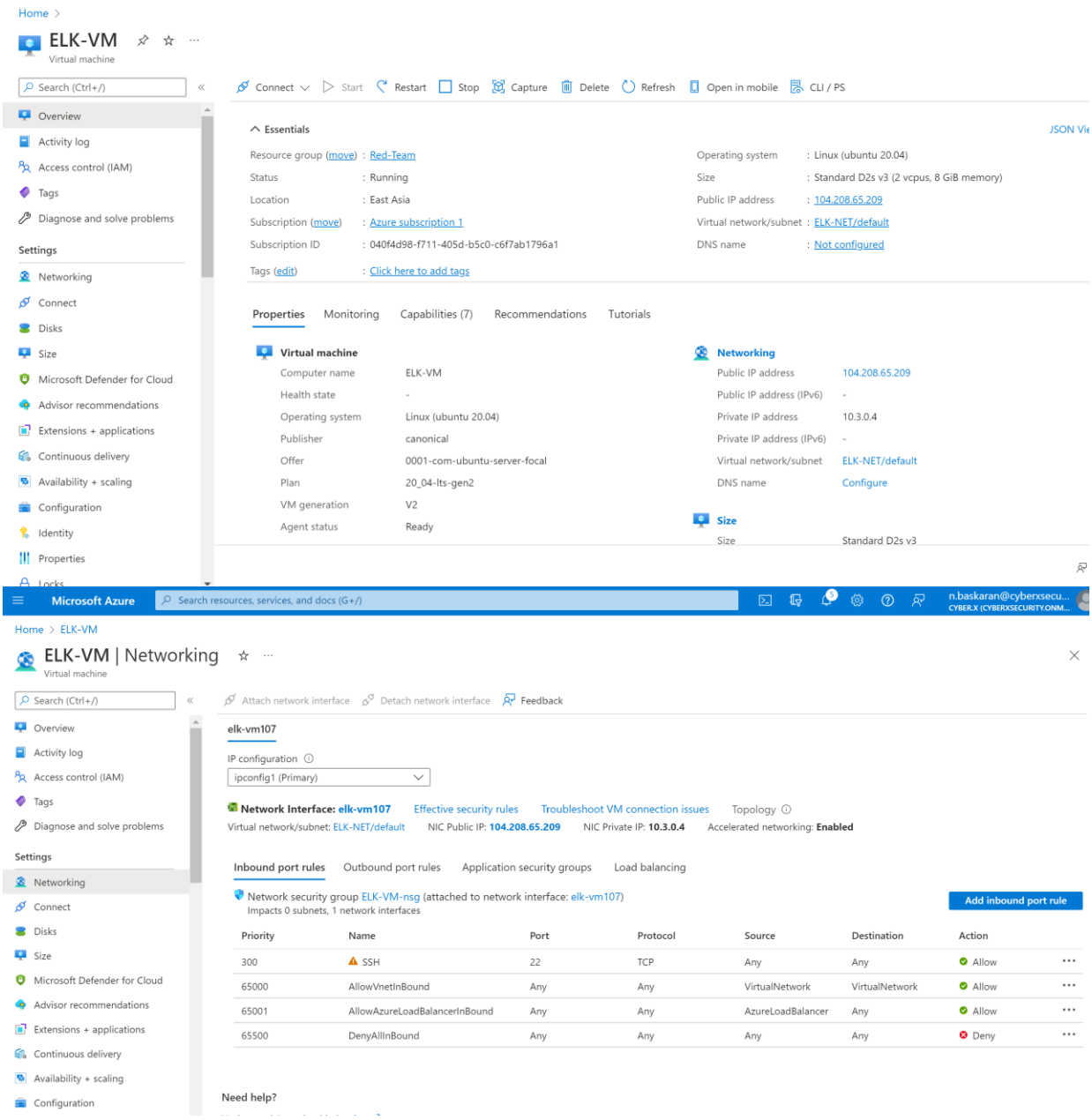
- Give an overview of the ELK stack and how it performs network security monitoring. This overview will also give you valuable context for why you're configuring and deploying these tools during the week.
- Provide the project overview as well as suggested milestones for each day.
- Due to Azure Free account limitations, you can only utilize 4vCPUs per region in Azure. Therefore, we will need to create a new vNet in another region for our ELK server.
- By the end of the project, we will have an ELK server deployed and receiving logs from all three web VMs created in the previous cloud weeks.

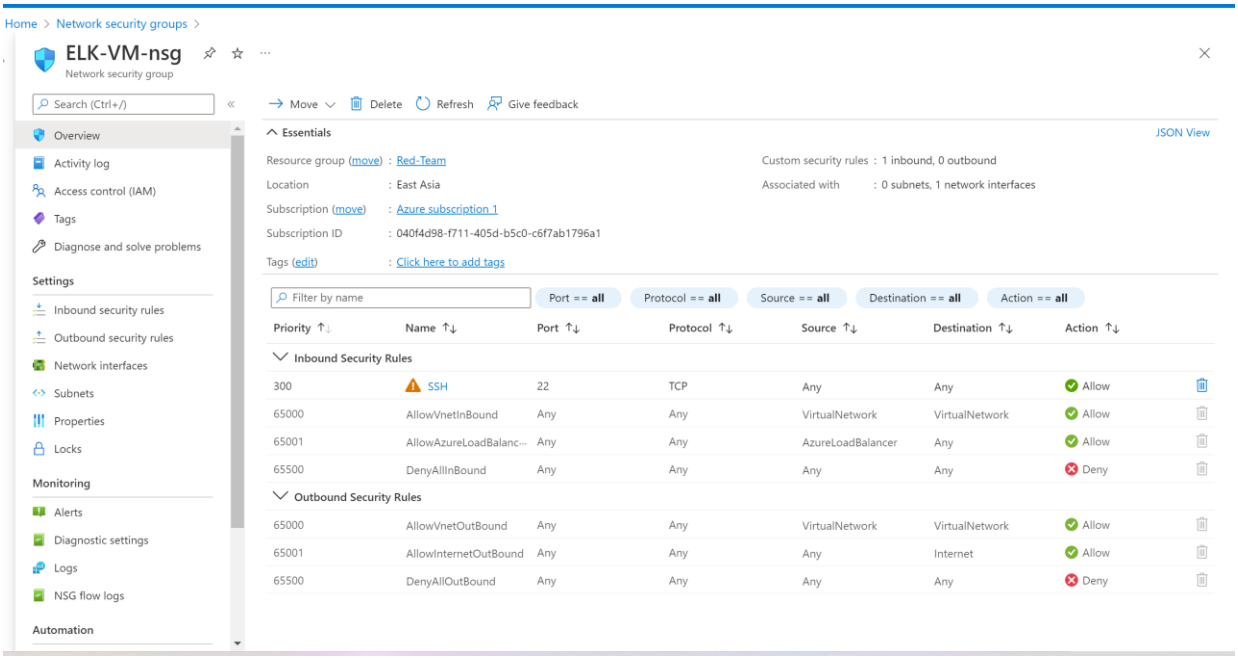
Activities involve the following:

- Create a new vNet in Azure in a different region, within the same resource group.
- Create a peer-to-peer network connection between your vNets.
- Create a new VM in the new vNet that has 2vCPUs and a minimum of 4GiB of memory.
- Add the new VM to Ansible's `hosts` file in your provisioner VM.
- Create an Ansible playbook that installs Docker and configures an ELK container.
- Run the playbook to launch the container.
- Restrict access to the ELK VM.



ELK VM


Home
ELK-VM
Virtual machine
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Microsoft Defender for Cloud
Advisor recommendations
Extensions + applications
Continuous delivery
Availability + scaling
Configuration
Identity
Properties
Locks
Connect
Start
Restart
Stop
Capture
Delete
Refresh
Open in mobile
CLI / PS
Essentials
JSON Vie
Resource group (move) : Red-Team
Status : Running
Location : East Asia
Subscription (move) : Azure subscription 1
Subscription ID : 040f4d98-f711-405d-b5c0-c6f7ab1796a1
Tags (edit) : Click here to add tags
Operating system : Linux (ubuntu 20.04)
Size : Standard D2s v3 (2 vcpus, 8 GiB memory)
Public IP address : 104.208.65.209
Virtual network/subnet : ELK-NET/default
DNS name : Not configured
Properties
Monitoring
Capabilities (7)
Recommendations
Tutorials
Virtual machine
Computer name ELK-VM
Health state -
Operating system Linux (ubuntu 20.04)
Publisher canonical
Offer 0001-com-ubuntu-server-focal
Plan 20_04-lts-gen2
VM generation V2
Agent status Ready
Networking
Public IP address 104.208.65.209
Public IP address (IPv6) -
Private IP address 10.3.0.4
Private IP address (IPv6) -
Virtual network/subnet ELK-NET/default
DNS name Configure
Size
Size Standard D2s v3
Microsoft Azure
Search resources, services, and docs (G+/)
n.baskaran@cyberxsecu...
CYBER.X (CYBERXSECURITY.ONM...
Home > ELK-VM
ELK-VM | Networking
Virtual machine
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Microsoft Defender for Cloud
Advisor recommendations
Extensions + applications
Continuous delivery
Availability + scaling
Configuration
Attach network interface
Detach network interface
Feedback
elk-vm107
IP configuration
ipconfig1 (Primary)
Network Interface: elk-vm107
Effective security rules
Troubleshoot VM connection issues
Topology
Virtual network/subnet: ELK-NET/default
NIC Public IP: 104.208.65.209
NIC Private IP: 10.3.0.4
Accelerated networking: Enabled
Inbound port rules
Outbound port rules
Application security groups
Load balancing
Network security group ELK-VM-nsg (attached to network interface: elk-vm107)
Impacts 0 subnets, 1 network interfaces
Add inbound port rule
Priority Name Port Protocol Source Destination Action
300 SSH 22 TCP Any Any Allow
65000 AllowVnetInBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowAzureLoadBalancerInBound Any Any AzureLoadBalancer Any Allow
65500 DenyAllInBound Any Any Any Any Deny
Need help?



Filebeat

Lectures cover the following

- Provide a brief overview of Filebeat.

Activities involve the following:

- Navigate to the ELK server's GUI to view Filebeat installation instructions.
- Create a Filebeat configuration file.
- Create an Ansible playbook that copies this configuration file to the DVWA VMs and then installs Filebeat.
- Run the playbook to install Filebeat.
- Confirm that the ELK Stack is receiving logs.
- Use the same method to install Metricbeat.

Installing Filebeat on the DVWA Container

1. First, make sure that the ELK server container is up and running:
    - Navigate to *http: 20.53.238.207:5601/app/kibana*. Use the public IP address of the ELK server that you created.
    - Click 'Explore on my Own'

- If you do not see the Kibana server landing page, open a terminal on your computer and SSH into the ELK server.
  - Run `docker container list -a` to verify that the container is on.
  - If it isn't, run `sudo docker start elk`.

2. Use the ELK server's GUI to begin installing Filebeat on your DVWA VM.
   - Navigate to your ELK server's IP address:
     - Click **Add Log Data**.
     - Choose **System Logs**.
     - Click on the **DEB** tab under **Getting Started**.
   -