

Usage Instructions for Automated ELK Stack Deployment

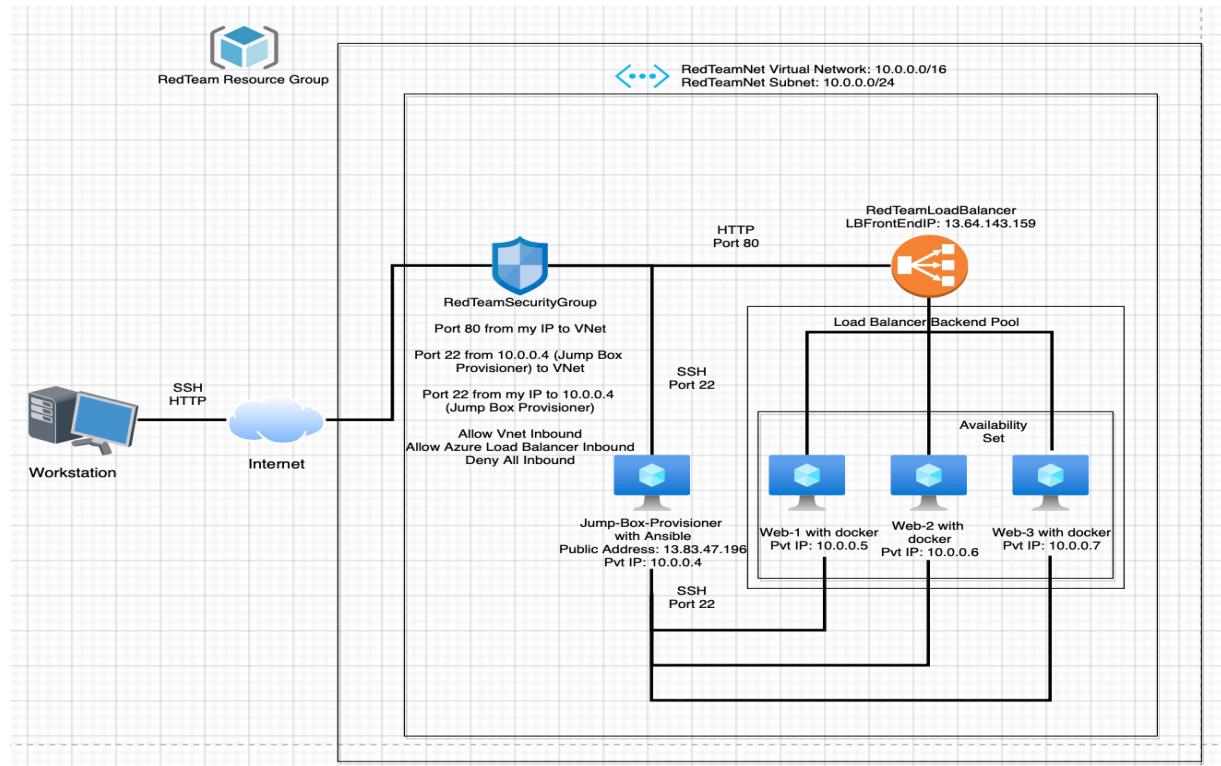
Pre-requisites

- Azure Portal account
- Resource Group: RedTeam
- Virtual Network: RedTeamNet (10.0.0.0/16; Subnet – 10.0.0.0/24)
- Network Security Group: RedTeamSecurityGroup

Rules:

- Port 80 from workstation IP to VNet
 - Port 22 from 10.0.0.4 (Jump Box Provisioner) to VNet
 - Port 22 from workstation IP to 10.0.0.4 (Jump Box Provisioner)
 - Allow Vnet Inbound
 - Allow Azure Load Balancer Inbound
 - Deny All Inbound
-
- Jumpbox: Jump-Box-Provisioner with Ansible (Public IP: 13.83.47.196 Private IP: 10.0.0.4)
 - Web Servers: Web-1 (Private IP: 10.0.0.5), Web-2 (Private IP: 10.0.0.6) and Web-3 (Private IP: 10.0.0.7)
 - Load Balancer: RedTeamLoadBalancer (Front End IP: 13.64.143.159)

The diagram below shows the network diagram representing the pre-requisites.



Instructions:

Chapter 1: Create a new Virtual Network

1. On the Azure portal, create a new virtual network located in the same resource group where the pre-requisite VMs (web servers) are located and in a new region that is different from that of the other VMs.

1.1 In my example, I had created **RedTeamNet** in US West zone and created **ELKNet** in US East zone.

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The title bar includes 'Microsoft Azure', 'Upgrade', 'Search resources, services, and docs (G+)', and a user profile. The main navigation bar has 'Home > Virtual networks >' followed by 'Create virtual network'. Below this, there are tabs for 'Basics', 'IP Addresses', 'Security', 'Tags', and 'Review + create'. The 'Basics' tab is selected. A descriptive text explains that VNet is the fundamental building block for private networks in Azure, enabling communication between VMs, the internet, and on-premises networks. It links to 'Learn more about virtual network'. The 'Project details' section contains fields for 'Subscription' (set to 'Azure subscription 1') and 'Resource group' (set to 'RedTeam'). The 'Instance details' section contains fields for 'Name' (set to 'ELKNet') and 'Region' (set to 'East US'). At the bottom, there are buttons for 'Review + create', '< Previous' (disabled), 'Next : IP Addresses >', and 'Download a template for automation'.

1.2 Click Next.

The IP addresses space will be automatically created.
Select the default subnet.

The screenshot shows the 'Create virtual network' wizard on the 'IP Addresses' tab. It displays the IPv4 address space configuration. A table lists one subnet named 'default' with the address range 10.1.0.0/24. There is an option to add an IPv6 address space, which is currently unchecked. A note indicates that the subnet's address range must be contained within the virtual network's address space. Below the table, there is a note about using a NAT gateway for outbound internet access, with a 'Learn more' link. At the bottom, there are navigation buttons for 'Review + create', '< Previous', 'Next : Security >', and 'Download a template for automation'.

1.3 Click Next.
Leave the settings at default.

The screenshot shows the 'Create virtual network' wizard on the 'Security' tab. It displays security settings for BastionHost, DDoS Protection Standard, and Firewall. For each, there are two radio button options: 'Disable' (selected) and 'Enable'. At the bottom, there are navigation buttons for 'Review + create', '< Previous', 'Next : Tags >', and 'Download a template for automation'.

1.4 Click Next.
Leave the settings at default.

The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The top navigation bar includes 'Microsoft Azure', 'Upgrade', a search bar, and user account information. Below the navigation is a breadcrumb trail: 'Home > Virtual networks > Create virtual network'. The main content area is titled 'Create virtual network' with a 'Tags' tab selected. A note states: 'Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups.' It also notes that tags will be automatically updated if changes are made on other tabs. Below this is a table for adding tags, with columns for 'Name' and 'Value'. At the bottom of the page are buttons for 'Review + create', '< Previous' (disabled), 'Next : Review + create >', and 'Download a template for automation'.

1.5 Click Next.
Review the settings and click on Create.

The screenshot shows the Microsoft Azure portal interface for creating a virtual network, now on the 'Review + create' tab. A green validation message 'Validation passed' is displayed. The page lists the configuration settings: Basics (Subscription: Azure subscription 1, Resource group: RedTeam, Name: ELKNet, Region: East US); IP addresses (Address space: 10.1.0.0/16, Subnet: default (10.1.0.0/24)); Tags (None); and Security (BastionHost: Disabled). At the bottom are buttons for 'Create' (highlighted in blue), '< Previous' (disabled), 'Next >', and 'Download a template for automation'.

The screenshot shows the Microsoft Azure Deployment Overview page for a completed deployment named "Microsoft.VirtualNetwork-20220316191612". The deployment was successful, indicated by a green checkmark icon and the message "Your deployment is complete". Key details include:

- Deployment name: Microsoft.VirtualNetwork-20220316191612
- Subscription: Azure subscription 1
- Resource group: RedTeam
- Start time: 3/16/2022, 7:19:00 PM
- Correlation ID: bb929320-8a43-44ec-b2c4-7826c9aef1b8

Below the main summary, there are sections for "Deployment details" (with a download link) and "Next steps" (with a "Go to resource" button). To the right, there are promotional cards for "Cost Management", "Microsoft Defender for Cloud", "Free Microsoft tutorials", and "Work with an expert".

2. Create a peer connection between your virtual networks.

2.1 Navigate to 'Virtual Network' in the Azure Portal. Select your new virtual network.

The screenshot shows the Microsoft Azure Virtual Networks list page. It displays two existing virtual networks: "ELKNet" and "RedTeamNet". The table includes columns for Name, Resource group, Location, and Subscription. Both networks are associated with the "RedTeam" resource group, "East US" location, and "Azure subscription 1".

Name	Resource group	Location	Subscription
ELKNet	RedTeam	East US	Azure subscription 1
RedTeamNet	RedTeam	West US	Azure subscription 1

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and user information. Below it, the 'Virtual networks' section for 'ELKNet' is displayed. On the left, a sidebar lists various settings like 'Activity log', 'Access control (IAM)', 'Tags', and 'Subnets'. The main pane shows 'Essentials' details: Resource group (move) to 'RedTeam', Location to 'East US', Subscription ID to '14a85dd0-8465-40ad-8a3d-b2f56d3514e5', and Virtual network ID to '376a4814-95b2-47b5-a778-a53e73084e2f'. A 'Capabilities' tab is selected, showing sections for 'DDoS protection' (Not configured) and 'Azure Firewall' (Not configured). At the bottom, there's a 'Peerings' section with a 'Peering status == all' filter and a table header: Name, Peering status, Peer, and Gateway transit.

2.2 Under 'Settings' on the left side, select 'Peerings'.
Click on 'Add' to create a new peering.

This screenshot shows the 'Peerings' section within the 'ELKNet' virtual network configuration. The 'Peerings' option is highlighted in the sidebar. The main area displays a table with one row: 'Add a peering to get started'. The table has columns for 'Name', 'Peering status', 'Peer', and 'Gateway transit'. At the top of the table, there are filters: 'Filter by name...' and 'Peering status == all'. Below the table, there are buttons for '+ Add', 'Refresh', and 'Sync'.

2.3 Add peering link names for the ELK virtual network and remote virtual network (RedTeamNet).
Select remote virtual network (RedTeamNet) from the 'Virtual Network' dropdown.
Leave the remaining settings as default.

Microsoft Azure Search resources, services, and docs (G+/-) nandhinibootcamp22@... DEFAULT DIRECTORY

Home > Virtual networks > ELKNet > Add peering ...

For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.

This virtual network

Peering link name * Elk-to-Red

Traffic to remote virtual network Allow (default) Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network Allow (default) Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server None (default) Use this virtual network's gateway or Route Server Use the remote virtual network's gateway or Route Server

Remote virtual network

Peering link name * Red-to-Elk

Add

Microsoft Azure Search resources, services, and docs (G+/-) nandhinibootcamp22@... DEFAULT DIRECTORY

Home > Virtual networks > ELKNet > Add peering ...

ELKNet

Virtual network deployment model Resource manager Classic

I know my resource ID

Subscription * Azure subscription 1

Virtual network * RedTeamNet

Traffic to remote virtual network Allow (default) Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network Allow (default) Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server None (default) Use this virtual network's gateway or Route Server Use the remote virtual network's gateway or Route Server

Add

2.4 Click Next

Microsoft Azure Search resources, services, and docs (G+/)

nandhinibootcamp22@... DEFAULT DIRECTORY

Home > Virtual networks > ELKNet

ELKNet | Peering

Virtual network

Add Refresh Sync

Search (Cmd +/)

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Filter by name... Peering status = all

Name	Peering status	Peer	Gateway transit
Elk-to-Red	Updating	RedTeamNet	Disabled

Address space Connected devices Subnets DDoS protection Firewall Security Network manager DNS servers Peerings Service endpoints Private endpoints

Elk-to-Red

Chapter 2: Create a new Virtual Machine

1. Create a new Ubuntu VM (ELKServer) in the virtual network with the following configurations:

- a. **RAM:** 4 GB+

You can use either of these machines:

- Standard D2s v3 (2 vcpus, 8GiB memory)
- Standard B2s (2vcpus, 4GiB memory)

In case you are unable to get the required VM, try deploying the VM in a different region.

- b. **Operating System:** Ubuntu Server 18.04 LTS – Gen2 (free services eligible)

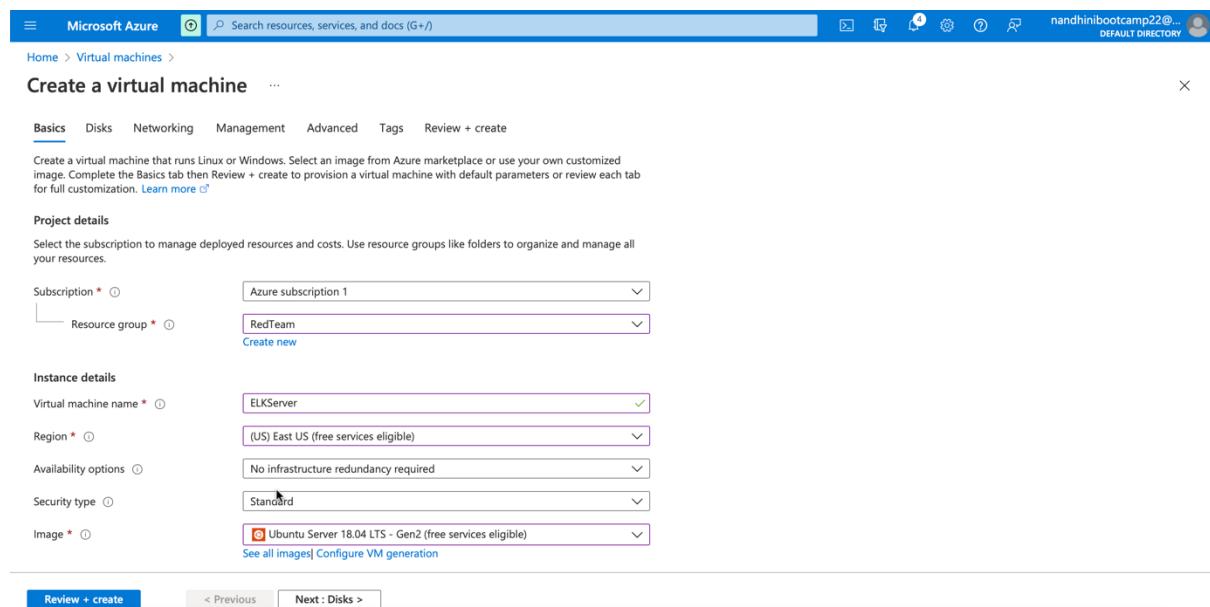
To get the SSH key created on the Ansible container running on your jump box, follow the steps below:

1. SSH into the jump box through the terminal on your workstation.
2. Run the docker commands to start and attach to your Ansible container.

```
sudo docker start (container_name)  
sudo docker attach (container_name)
```

3. Retrieve your public ssh key.

```
cat ~/.ssh/id_rsa.pub
```



The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal, specifically the 'Basics' step. The page title is 'Create a virtual machine ...'. At the top, there are tabs for Basics, Disks, Networking, Management, Advanced, Tags, and Review + create. The Basics tab is selected. Below the tabs, a brief description says: 'Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.' A 'Learn more' link is provided. The 'Project details' section includes fields for 'Subscription *' (set to 'Azure subscription 1') and 'Resource group *' (set to 'RedTeam'). The 'Instance details' section includes fields for 'Virtual machine name *' (set to 'ELKServer'), 'Region *' (set to '(US) East US (free services eligible)'), 'Availability options' (set to 'No infrastructure redundancy required'), 'Security type' (set to 'Standard'), and 'Image *' (set to 'Ubuntu Server 18.04 LTS - Gen2 (free services eligible)'). At the bottom of the form are buttons for 'Review + create' (highlighted in blue), '< Previous', and 'Next : Disks >'.

Home > Virtual machines >

Create a virtual machine

Azure Spot instance

Size * Standard_D2s_v3 - 2 vcpus, 8 GiB memory (US\$70.08/month) See all sizes

Administrator account

Authentication type SSH public key Password

Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username *

SSH public key source Use existing public key

SSH public key * Learn more about creating and using SSH keys in Azure

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Review + create < Previous Next : Disks >

Microsoft Azure Search resources, services, and docs (G+/-)

Home > Virtual machines >

Create a virtual machine

Username *

SSH public key source Use existing public key

SSH public key * Learn more about creating and using SSH keys in Azure

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * None Allow selected ports

Select inbound ports *

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Review + create < Previous Next : Disks >

Click Next.

c. **Disks:** Standard SSD for OS Disk Type. Leave the remaining settings as default.

Microsoft Azure Search resources, services, and docs (G+) nandhinibootcamp22@... DEFAULT DIRECTORY

Home > Virtual machines > Create a virtual machine ...

Basics Disks Networking Management Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type * Standard SSD (locally-redundant storage) Premium SSD (Ultra low latency, higher IOPS and bandwidth, and bursting) [Learn more](#)

Delete with VM

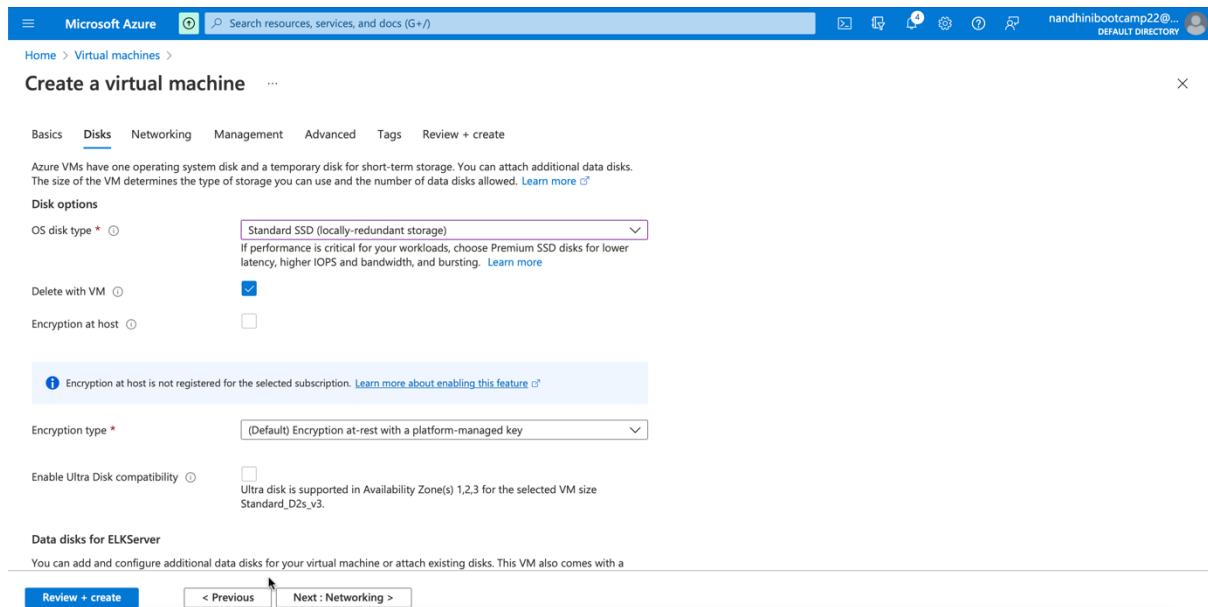
Encryption at host

Encryption type * (Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard_D2s_v3.

Data disks for ELKServer
You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

Review + create < Previous Next : Networking >



Microsoft Azure Search resources, services, and docs (G+) nandhinibootcamp22@... DEFAULT DIRECTORY

Home > Virtual machines > Create a virtual machine ...

Encryption type * (Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard_D2s_v3.

Data disks for ELKServer
You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

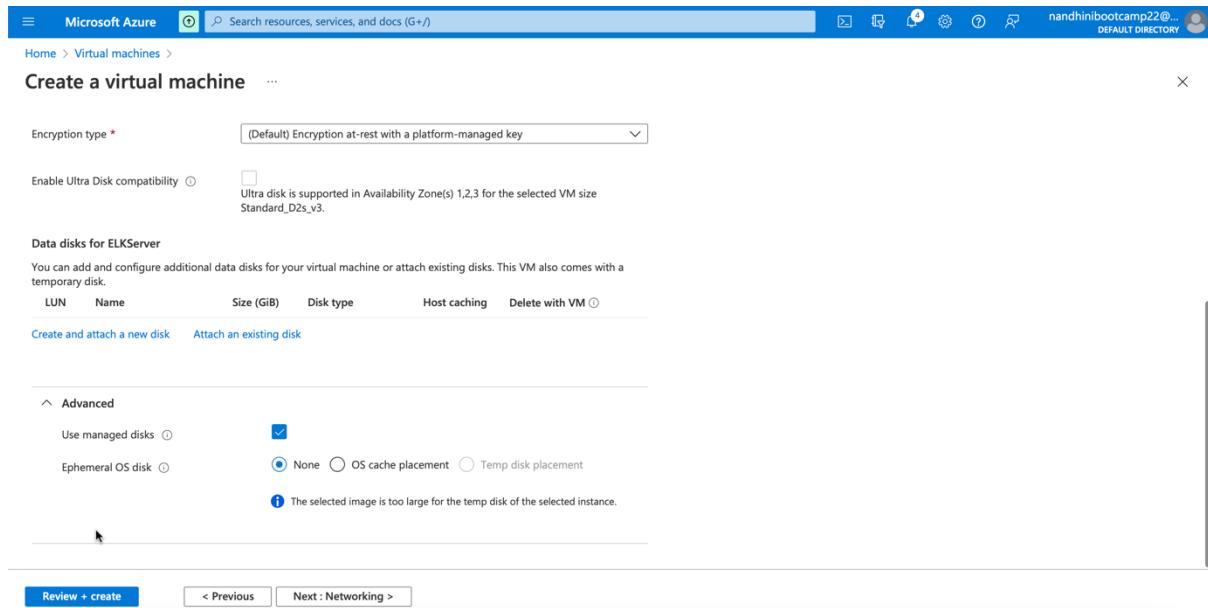
LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM
					<input type="checkbox"/>

Create and attach a new disk Attach an existing disk

Advanced

Use managed disks
Ephemeral OS disk None OS cache placement Temp disk placement
The selected image is too large for the temp disk of the selected instance.

Review + create < Previous Next : Networking >



d. **IP Address:** Create a new static public IP Address.

The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The top navigation bar includes 'Microsoft Azure', a search bar, and user account information. The main page title is 'Create a virtual machine'. The 'Networking' tab is selected, indicated by a blue underline. Below the tabs, a descriptive text explains network connectivity settings. A 'Network interface' section contains fields for 'Virtual network' (set to 'ELKNet'), 'Subnet' (set to 'default (10.1.0.0/24)'), 'Public IP' (set to '(new) ELKServer-ip'), 'NIC network security group' (set to 'Basic'), and 'Public inbound ports' (set to 'Allow selected ports'). On the right side, a separate 'Create public IP address' panel is open, showing a 'Name' field with 'ELKServer-ip', 'SKU' set to 'Basic', and 'Assignment' set to 'Static'. Navigation buttons at the bottom include 'Review + create', '< Previous', and 'Next : Management >'.

e. **Networking:** The VM should be added to the new region where you have created the virtual network. A new basic Security Group to be created for this VM.

This screenshot shows the same networking configuration as the previous one, but with a prominent warning message at the bottom of the 'Public inbound ports' section: '⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to...' The rest of the configuration remains identical to the first screenshot.

Microsoft Azure Search resources, services, and docs (G+)

Home > Virtual machines >

Create a virtual machine

Basic Advanced

Public inbound ports * None Allow selected ports

Select inbound ports * SSH (22)

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete public IP and NIC when VM is deleted

Accelerated networking

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution?

Review + create [< Previous](#) [Next : Management >](#)

Click Next.

f. **Management:** Leave the settings as default.

Microsoft Azure Search resources, services, and docs (G+)

Home > Virtual machines >

Create a virtual machine

Basics Disks Networking **Management** Advanced Tags Review + create

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics Enable with managed storage account (recommended) Enable with custom storage account Disable

Enable OS guest diagnostics

Identity

System assigned managed identity

Azure AD

Login with Azure AD

Review + create [< Previous](#) [Next : Advanced >](#)

Identity

System assigned managed identity

Azure AD

Login with Azure AD

RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Azure AD login. [Learn more](#)

Azure AD login now uses SSH certificate-based authentication. You will need to use an SSH client that supports OpenSSH certificates. You can use Azure CLI or Cloud Shell from the Azure Portal. [Learn more](#)

Auto-shutdown

Enable auto-shutdown

Backup

Enable backup

Guest OS updates

Patch orchestration options Image default

Some patch orchestration options are not available for this image. [Learn more](#)

Review + create < Previous Next : Advanced >

Click Next.

g. Advanced: Leave the settings as default.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Virtual machines > Create a virtual machine ...

Create a virtual machine ...

Basics Disks Networking Management **Advanced** Tags Review + create

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions Select an extension to install

VM applications (preview)

VM applications contain application files that are securely and reliably downloaded on your VM after deployment. In addition to the application files, an install and uninstall script are included in the application. You can easily add or remove applications on your VM after create. [Learn more](#)

Select a VM application to install

Custom data and cloud init

Pass a cloud-init script, configuration file, or other data into the virtual machine **while it is being provisioned**. The data will be saved on the VM in a known location. [Learn more about custom data for VMs](#)

Custom data

Review + create < Previous Next : Tags >

Custom data

Custom data on the selected image will be processed by cloud-init. [Learn more about custom data for VMs](#)

User data

Pass a script, configuration file, or other data that will be accessible to your applications **throughout the lifetime of the virtual machine**. Don't use user data for storing your secrets or passwords. [Learn more about user data for VMs](#)

Enable user data

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#)

Host group

Pass a script, configuration file, or other data that will be accessible to your applications **throughout the lifetime of the virtual machine**. Don't use user data for storing your secrets or passwords. [Learn more about user data for VMs](#)

Enable user data

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#)

Host group

Capacity reservations

Capacity reservations allow you to reserve capacity for your virtual machine needs. You get the same SLA as normal virtual machines with the security of reserving the capacity ahead of time. [Learn more](#)

Capacity reservation group

Proximity placement group

Proximity placement groups allow you to group Azure resources physically closer together in the same region. [Learn more](#)

Proximity placement group

Click Next.

1. **Tags:** Leave the settings as default.

Microsoft Azure Search resources, services, and docs (G+ /) nandhinibootcamp22@... DEFAULT DIRECTORY

Home > Virtual machines > Create a virtual machine ...

Basics Disks Networking Management Advanced Tags Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value	Resource
		12 selected

[Review + create](#) < Previous Next : Review > create >

Click Review + create.

Microsoft Azure Search resources, services, and docs (G+ /) nandhinibootcamp22@... DEFAULT DIRECTORY

Home > Virtual machines > Create a virtual machine ...

Validation passed

Basics Disks Networking Management Advanced Tags Review + create

PRODUCT DETAILS

1 X Standard D2s v3 by Microsoft

Subscription credits apply 0.0960 USD/hr

[Terms of use](#) | [Privacy policy](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

WARNING You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

[Create](#) < Previous Next > [Download a template for automation](#)

Click Create.

The screenshot shows the Microsoft Azure Deployment Overview page for a deployment named 'CreateVm-Canonical.UbuntuServer-18_04-Its-gen2-20220316194410'. The status is 'Deployment succeeded'. The deployment details include a start time of 3/16/2022, 7:57:33 PM, a correlation ID of c08f9ea4-bff6-412a-aa03-e4e3bb78cfec, and a resource group of 'RedTeam'. There are sections for 'Deployment details' (Download), 'Next steps' (Setup auto-shutdown, Monitor VM health, Run a script inside the virtual machine), and buttons for 'Go to resource' and 'Create another VM'. On the right, there are links for Cost Management, Microsoft Defender for Cloud, Free Microsoft tutorials, and Work with an expert.

Click Go to resource to view the ELKServer VM.

The screenshot shows the Microsoft Azure Virtual Machine Properties page for 'ELKServer'. The 'Essentials' section displays basic information: Resource group (RedTeam), Status (Running), Location (East US), Subscription (Azure subscription 1), Subscription ID (14a85dd0-8465-40ad-8a3d-b2f56d3514e5), and Tags (None). The 'Properties' tab is selected, showing detailed settings for the virtual machine, networking, size, and other configurations. The 'Networking' section includes Public IP address (20.228.134.92), Private IP address (10.1.0.4), Virtual network/subnet (ELKNet/default), and DNS name (Not configured). The 'Size' section shows Standard D2s v3 and 2 vCPUs.

2. To verify if the VM was created correctly, SSH into the VM using the private IP address from the Ansible container on jump box.

Chapter 3: Downloading and Configuring the Container

Using Ansible, we can configure the new VM to function as an ELK Server.

1. From the Ansible VM, change to /etc/ansible/ directory.

```
cd /etc/ansible/
```

2. Add the new VM to Ansible's **hosts** file for Ansible to understand the list of machines it can discover and connect to.

```
nano hosts
```

3. Add **[elk]** group and IP address of the ELKServer VM.

We can specify the groups on which the playbooks should be run.

```
GNU nano 4.8                               hosts                                         Modified
# This is the default ansible 'hosts' file.
#
# It should live in /etc/ansible/hosts
#
#   - Comments begin with the '#' character
#   - Blank lines are ignored
#   - Groups of hosts are delimited by [header] elements
#   - You can enter hostnames or ip addresses
#   - A hostname/ip can be a member of multiple groups
#
# Ex 1: Ungrouped hosts, specify before any group headers.

#green.example.com
#blue.example.com
#192.168.100.1
#192.168.100.10

# Ex 2: A collection of hosts belonging to the 'webservers' group

[webservers]
#alpha.example.org
#beta.example.org
#192.168.1.100
#192.168.1.110
10.0.0.5 ansible_python_interpreter=/usr/bin/python3
10.0.0.6 ansible_python_interpreter=/usr/bin/python3
10.0.0.7 ansible_python_interpreter=/usr/bin/python3

[elk]
10.1.0.4 ansible_python_interpreter=/usr/bin/python3

^G Get Help      ^O Write Out     ^W Where Is     ^K Cut Text      ^J Justify      ^C Cur Pos      M-U Undo
^X Exit         ^R Read File     ^\ Replace       ^U Paste Text    ^T To Spell     ^I Go To Line   M-E Redo
                                         M-A Mark Text  M-6 Copy Text
```

4. Create the playbook to configure the ELK Server. The playbook should run on the **[elk]** group.

The playbook should:

- Install docker.io (Docker engine) and python3-pip (Python software installer) packages.
- Install docker, the Python client for Docker which required by Ansible to control the state of Docker containers.
- Download the Docker container called sebp/elk:761.
- Configure the container to start with the following port mappings:
 - 5601:5601
 - 9200:9200
 - 5044:5044
- Start the container

- Enables the docker service on boot

nano install-elk.yml

```
GNU nano 4.8                               install-elk.yml
-- 
- name: Configure Elk VM with Docker
  hosts: elk
  remote_user: RedAdmin
  become: true
  tasks:
    # Using apt module to download docker.io
    - name: Install docker.io
      apt:
        update_cache: yes
        force_apt_get: yes
        name: docker.io
        state: present

    # Using apt module to download python3-pip
    - name: Install python3-pip
      apt:
        force_apt_get: yes
        name: python3-pip
        state: present

    # Using pip module to install docker module
    - name: Install Docker module
      pip:
        name: docker
        state: present

    # Using command module to increase virtual memory
    - name: Increase virtual memory
      [ Read 57 lines ]
      ^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify
      ^X Exit       ^R Read File    ^A Replace     ^U Paste Text  ^T To Spell
      ^C Cur Pos    ^M-U Undo    ^A Go To Line  ^M-E Redo
      ^M-A Mark Text ^M-6 Copy Text
```

```
nandhinisreekumar - root@d1a2179a6c78: /etc/ansible/roles - ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 - 132x34
GNU nano 4.8                                         install-elk.yml                                         Modified
# Using command module to increase virtual memory
- name: Increase virtual memory
  command: sysctl -w vm.max_map_count=262144

# Using sysctl module to use more memory
- name: Use more memory
  sysctl:
    name: vm.max_map_count
    value: 262144
    state: present
    reload: yes

# Using docker_container module to download the docker elk container
- name: Download and launch a docker elk container
  docker_container:
    name: elk
    image: sebp/elk:7.6
    state: started
    restart_policy: always
    published_ports:
      - 5601:5601
      - 9200:9200
      - 5044:5044

# Using systemd module to enable docker service on boot
- name: Enable service docker on boot
  systemd:
    name: docker
    enabled: yes
```

Chapter 4: Launching and Exposing the Container

1. Run the playbook

```
ansible-playbook -m install-elk.yml
```

```
nandhinisreekumar — root@d1a2179a6c78: /etc/ansible/roles — ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 — 132x34

PLAY [Configure Elk VM with Docker] ****
TASK [Gathering Facts] ****
ok: [10.1.0.4]

TASK [Install docker.io] ****
ok: [10.1.0.4]

TASK [Install python3-pip] ****
ok: [10.1.0.4]

TASK [Install Docker module] ****
ok: [10.1.0.4]

TASK [Increase virtual memory] ****
changed: [10.1.0.4]

TASK [Use more memory] ****
ok: [10.1.0.4]

TASK [Download and launch a docker elk container] ****
[DEPRECATION WARNING]: The container_default_behavior option will change its default value from "compatibility" to "no_defaults" in community.docker 2.0.0. To remove this warning, please specify an explicit value for it now. This feature will be removed from community.docker in version 2.0.0. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
ok: [10.1.0.4]

TASK [Enable service docker on boot] ****
ok: [10.1.0.4]

PLAY RECAP ****
10.1.0.4 : ok=8    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

root@d1a2179a6c78:/etc/ansible/roles#
```

2. SSH into the ELK Server VM and ensure `sebp/elk:761` container is running.

```
docker ps
```

```
nandhinisreekumar — RedAdmin@ELKServer: ~ — ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 — 145x34

root@d1a2179a6c78:/etc/ansible/roles# ssh RedAdmin@10.1.0.4
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1072-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 System information as of Thu Mar 17 04:22:05 UTC 2022

 System load:  0.03      Processes:           128
 Usage of `/': 16.7% of 28.90GB  Users logged in:     0
 Memory usage: 33%
 Swap usage:   0%          IP address for eth0:   10.1.0.4
                           IP address for docker0: 172.17.0.1

6 updates can be applied immediately.
5 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

New release '20.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Mar 17 04:15:41 2022 from 10.0.0.4
RedAdmin@ELKServer:~$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS
NAMES
c318e5fb4e0e        sebp/elk:761      "/usr/local/bin/star..."   18 minutes ago   Up 9 minutes   0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp
elk
RedAdmin@ELKServer:~$
```

Chapter 5: Identity and Access Management

1. On the Azure portal, navigate to network security groups.

Microsoft Azure Search resources, services, and docs (G+)

Home > Network security groups > ELKServer-nsg

Overview

Resource group (move) : RedTeam

Location : East US

Subscription (move) : Azure subscription 1

Subscription ID : 14a85dd0-8465-40ad-8a3d-b2f56d3514e5

Tags (edit) : Click here to add tags

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Logs

Custom security rules : 1 inbound, 0 outbound

Associated with : 0 subnets, 1 network interfaces

Priority ↑	Name ↑	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
300	⚠️ SSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow

2. Create an inbound security rule in the network security group to allow traffic over TCP 5601 from the workstation public IP to the ELK Server and to restrict other access to the ELK Server.

Microsoft Azure Search resources, services, and docs (G+)

Home > Network security groups > ELKServer-nsg

ELKServer-nsg | Inbound security rules

Add inbound security rule

Source ⓘ IP Addresses

Source IP addresses/CIDR ranges * ⓘ

98.207.9.229

Source port ranges * ⓘ

*

Destination ⓘ IP Addresses

Destination IP addresses/CIDR ranges * ⓘ

10.1.0.4

Service ⓘ Custom

Destination port ranges * ⓘ

5601

Protocol

Any

TCP

UDP

Add Cancel

The screenshot shows the Azure portal interface for managing a Network Security Group (NSG). The left sidebar navigation includes Home, Network security groups, ELKServer-nsg, Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (selected), Inbound security rules (selected), Outbound security rules, Network interfaces, Subnets, Properties, Locks, Monitoring, Alerts, Diagnostic settings, and Logs.

The main content area displays the 'ELKServer-nsg | Inbound security rules' page. It shows a table of existing rules:

Priority	Name	Port	Protocol
300	SSH	22	TCP
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalanc...	Any	Any
65500	DenyAllInBound	Any	Any

A modal dialog titled 'Add inbound security rule' is open on the right side. It contains fields for Destination port ranges (5601), Protocol (TCP selected), Action (Allow selected), Priority (100), Name (AllowAccessToPort5601), and Description (Allow Access to Port 5601). Buttons for 'Add' and 'Cancel' are at the bottom.

3. Click Add.

The screenshot shows the same Azure portal interface and NSG settings as the previous screenshot, but the 'Inbound security rules' table now includes the newly added rule:

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowAccessToPort5601	5601	TCP	98.207.9.229	10.1.0.4	Allow
300	SSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

4. Navigate to [http://\[ELK-VM.External.IP\]:5601/app/kibana](http://[ELK-VM.External.IP]:5601/app/kibana) to verify access to ELK Server.

The screenshot shows the Elastic Home page with a sidebar on the left containing icons for different services: APM, Logstash, Beats, Metrics, X-Pack, Elasticsearch, Machine Learning, and Security. The main content area is divided into several sections:

- Observability**:
 - APM**: APM automatically collects in-depth performance metrics and errors from inside your applications. [Add APM](#)
 - Logs**: Ingest logs from popular data sources and easily visualize in preconfigured dashboards. [Add log data](#)
 - Metrics**: Collect metrics from the operating system and services running on your servers. [Add metric data](#)
- Security**: Centralize security events for interactive investigation in ready-to-go visualizations. [Add events](#)
- Data Sources**:
 - Add sample data**: Load a data set and a Kibana dashboard.
 - Upload data from log file**: Import a CSV, NDJSON, or log file.
 - Use Elasticsearch data**: Connect to your Elasticsearch index.
- Visualize and Explore Data**:
 - APM**: Automatically collect in-depth performance metrics. [Safari](#)
 - Canvas**: Showcase your data in a pixel-perfect way.
- Manage and Administer the Elastic Stack**:
 - Console**: Skip cURL and use this JSON interface to work.
 - Index Patterns**: Manage the index patterns that help retrieve your data.

Chapter 6: Installing Filebeat on the DVWA Container

1. Click 'Explore on my Own' on the Kibana server landing page.

The screenshot shows the Kibana home page with a sidebar on the left containing various icons. The main area is divided into two main sections: 'Observability' and 'Security'. The 'Observability' section contains four cards: 'APM', 'Logs', 'Metrics', and 'SIEM'. Each card has a brief description and a button labeled 'Add [Category]'. Below these are three links: 'Add sample data', 'Upload data from log file', and 'Use Elasticsearch data'. The 'Security' section is partially visible on the right. At the bottom, there are two more sections: 'Visualize and Explore Data' and 'Manage and Administer the Elastic Stack', each with their own cards and descriptions.

2. Click Add Log Data.

The screenshot shows the 'Add data' page in Kibana. The sidebar on the left is identical to the home page. The main area displays a grid of 14 cards, each representing a different type of log collection. The cards are arranged in four rows of four. From top-left to bottom-right, the cards are: ActiveMQ logs, Apache logs, AWS Cloudwatch logs, AWS S3 based logs; Elasticsearch logs, IBM MQ logs, IIS logs, Kafka logs; Logstash logs, MySQL logs, Nats logs, Nginx logs; PostgreSQL logs, Redis logs, System logs, Traefik logs. Each card includes a small icon, a title, and a brief description.

3. Choose System Logs.
Click on the DEB tab under Getting Started.

The Filebeat installation instructions can be found here which is used for installing Filebeat using ansible playbook.

4. Install Filebeat using the commands displayed on the Kibana server landing page.

```

nandhinisreekumar - root@d1a2179a6c78: ~ - ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 - 148x28
root@d1a2179a6c78:~# curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb
% Total    % Received % Xferd  Average Speed   Time   Time Current
          Dload  Upload Total Spent   Left Speed
100 23.9M  100 23.9M    0     0  117M      0 --:--:-- --:--:-- 117M
root@d1a2179a6c78:~# sudo dpkg -i filebeat-7.6.1-amd64.deb
bash: sudo: command not found
root@d1a2179a6c78:~# dpkg -i filebeat-7.6.1-amd64.deb
Selecting previously unselected package filebeat.
(Reading database ... 18241 files and directories currently installed.)
Preparing to unpack filebeat-7.6.1-amd64.deb ...
Unpacking filebeat (7.6.1) ...
Setting up filebeat (7.6.1) ...
root@d1a2179a6c78:~#

```

5. Install Elasticsearch using the following commands:

```

curl -L -O https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.6.2-
amd64.deb
sudo dpkg -i elasticsearch-7.6.2-amd64.deb
sudo /etc/init.d/elasticsearch start

```

```

nandhinisreekumar - root@d1a2179a6c78: ~ -- ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 - 148x28
root@d1a2179a6c78:~# curl -L -O https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.6.2-amd64.deb
  % Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload Total Spent   Left Speed
100 282M  100 282M    0     0 18.2M      0:00:15 0:00:15 --:-- 21.0M
root@d1a2179a6c78:~# dpkg -i elasticsearch-7.6.2-amd64.deb
Selecting previously unselected package elasticsearch.
(Reading database ... 19044 files and directories currently installed.)
Preparing to unpack elasticsearch-7.6.2-amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (7.6.2) ...
Setting up elasticsearch (7.6.2) ...
Created elasticsearch keystore in /etc/elasticsearch
root@d1a2179a6c78:~# sudo /etc/init.d/elasticsearch start
bash: sudo: command not found
root@d1a2179a6c78:~# /etc/init.d/elasticsearch start
 * Starting Elasticsearch Server
sysctl: setting key "vm.max_map_count": Read-only file system
Exception in thread "main" java.lang.RuntimeException: starting java failed with [1]
output:
#
# There is insufficient memory for the Java Runtime Environment to continue.
# Native memory allocation (mmap) failed to map 986513408 bytes for committing reserved memory.
# An error report file with more information is saved as:
# /var/log/elasticsearch/hs_err_pid177.log
error:
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
OpenJDK 64-Bit Server VM warning: INFO: os::commit_memory(0x0000000c533000, 986513408, 0) failed; error='Not enough space' (errno=12)

```

6. SSH into your Jumpbox.

7. Start and attach to the docker container.

8. Run the following curl command to get the filebeat configuration file:

curl

<https://gist.githubusercontent.com/slapo/5cc350109583af6cbe577bcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat>

```

nandhinisreekumar - root@d1a2179a6c78: /etc/ansible -- ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 - 148x28
root@d1a2179a6c78:~# cd /etc/ansible/
root@d1a2179a6c78:~/etc/ansible# curl https://gist.githubusercontent.com/slapo/5cc350109583af6cbe577bcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat
#####
# Filebeat Configuration #####
# This file is a full configuration example documenting all non-deprecated
# options in comments. For a shorter configuration example, that contains only
# the most common options, please see filebeat.yml in the same directory.
#
# You can find the full configuration reference here:
# https://www.elastic.co/guide/en/beats/filebeat/index.html
filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml

=====
filebeat.modules:

-----
System Module -----
#-- module: system
 #- Syslog
 #syslog:
 #enabled: true

 # Set custom paths for the log files. If left empty,
 # Filebeat will choose the paths depending on your OS.
 #var.paths:

 # Input configuration (advanced). Any input configuration option
 # can be added under this section.

```

We can also use the Filebeat configuration file template provided.

9. Copy the content to a new file (**filebeat-config.yml**)

```
nandhinisreekumar - root@d1a2179a6c78:/etc/ansible/files - ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 - 148x28
root@d1a2179a6c78:/etc/ansible# mkdir files
root@d1a2179a6c78:/etc/ansible# cd files
root@d1a2179a6c78:/etc/ansible/files# nano filebeat-config.yml
root@d1a2179a6c78:/etc/ansible/files#
```

9.1 Edit the username and password to **elastic** and **changeme** respectively in the configuration file. Also, replace the IP address with the IP address of your ELK Server VM.

```
nandhinisreekumar - root@d1a2179a6c78:/etc/ansible - ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 - 148x28
GNU nano 4.8                                         filebeat-config.yml

# Configure what output to use when sending the data collected by the beat.

----- Elasticsearch output -----
output.elasticsearch:
  # Boolean flag to enable or disable the output module.
  #enabled: true

  # Array of hosts to connect to.
  # Scheme and port can be left out and will be set to the default (http and 9200)
  # In case you specify and additional path, the scheme is required: http://localhost:9200/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:9200
  hosts: ["10.1.0.4:9200"]
  username: "elastic"
  password: "changeme"

  # Set gzip compression level.
  #compression_level: 0

  # Configure escaping HTML symbols in strings.
  #escape_html: false

  # Optional protocol and basic auth credentials.
  #protocol: "https"

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo   M-A Mark Text   M-] To Bracket
^X Exit      ^R Read File    ^\ Replace    ^U Paste Text  ^T To Spell   ^_ Go To Line  M-E Redo   M-6 Copy Text  ^Q Where Was
```

9.2 Scroll to line #1806 (setup.kibana) and replace the IP address with the IP address of your ELK machine.

```
nandhinisreekumar - root@d1a2179a6c78:/etc/ansible - ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 - 148x28
GNU nano 4.8                                         filebeat-config.yml                                         Modified
# 'filebeat-%{[agent.version]}'.
#setup.ilm.policy_name: "mypolicy"

# The path to a JSON file that contains a lifecycle policy configuration. Used
# to load your own lifecycle policy.
#setup.ilm.policy_file:

# Disable the check for an existing lifecycle policy. The default is false. If
# you disable this check, set setup.ilm.overwrite: true so the lifecycle policy
# can be installed.
#setup.ilm.check_exists: false

# Overwrite the lifecycle policy at startup. The default is false.
#setup.ilm.overwrite: false

===== Kibana =====

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:
  host: "10.1.0.4:5601"
  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo   M-A Mark Text   M-] To Bracket
^X Exit      ^R Read File    ^\ Replace    ^U Paste Text  ^T To Spell   ^_ Go To Line  M-E Redo   M-6 Copy Text  ^Q Where Was
```

Chapter 7: Creating the Filebeat Installation Play

1. Create a playbook to install Filebeat in /etc/ansible/roles/ directory. (**filebeat-playbook.yml**) with the following tasks:

- Download the .deb file from artifacts.elastic.co.
- Install the .deb file.
- Copy the Filebeat configuration file from the Ansible container to the WebVM(s) Filebeat was installed.
- Enable and configure the system modules
- Setup Filebeat
- Start Filebeat service
- Enable the Filebeat service on boot.



The screenshot shows a terminal window with a light gray background and a dark gray header bar. In the header bar, there are three small colored circles (red, yellow, green) on the left, followed by the text "nandhinisreekumar — root@d1a2179a6c78: /etc/ansible — ssh -i .ssh/id_rsa RedAdmin@13.83.47.196". Below the header, the terminal prompt is "[root@d1a2179a6c78:~#". The user then enters the following commands:
cd /etc/ansible
cd roles
nano filebeat-playbook.yml

```
nandhinisreekumar — root@d1a2179a6c78:/etc/ansible/roles — ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 — 148x28
GNU nano 4.8                                     filebeat-playbook.yml

- name: Installing and launching Filebeat
  hosts: webservers
  become: yes
  tasks:
    - name: download filebeat deb
      command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb

    - name: install filebeat deb
      command: dpkg -i filebeat-7.4.0-amd64.deb

    - name: drop in filebeat.yml
      copy:
        src: /etc/ansible/files/filebeat-config.yml
        dest: /etc/filebeat/filebeat.yml

    - name: enable and configure system module
      command: filebeat modules enable system

    - name: setup filebeat
      command: filebeat setup

    - name: start filebeat service
      command: service filebeat start

- name: enable service filebeat on boot
  systemd:
    name: filebeat
    enabled: yes

[ Read 30 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo  M-A Mark Text  M-J To Bracket
^X Exit     ^R Read File   ^M Replace   ^U Paste Text  ^T To Spell   ^_ Go To Line  M-E Redo   M-G Copy Text  ^Q Where Was
```

```
nandhinisreekumar — root@d1a2179a6c78:/etc/ansible/roles — ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 — 148x28
GNU nano 4.8                                     filebeat-playbook.yml

  command: curl -L -O filebeat-7.4.0-amd64.deb

- name: install filebeat deb
  command: dpkg -i filebeat-7.4.0-amd64.deb

- name: drop in filebeat.yml
  copy:
    src: /etc/ansible/files/filebeat-config.yml
    dest: /etc/filebeat/filebeat.yml

- name: enable and configure system module
  command: filebeat modules enable system

- name: setup filebeat
  command: filebeat setup

- name: start filebeat service
  command: service filebeat start

- name: enable service filebeat on boot
  systemd:
    name: filebeat
    enabled: yes

[ Read 30 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo  M-A Mark Text  M-J To Bracket
^X Exit     ^R Read File   ^M Replace   ^U Paste Text  ^T To Spell   ^_ Go To Line  M-E Redo   M-G Copy Text  ^Q Where Was
```

2. Save the file.
3. Run the playbook.

```
root@d1a2179a6c78:/etc/ansible# cd roles
root@d1a2179a6c78:/etc/ansible/roles# nano filebeat-playbook.yml
root@d1a2179a6c78:/etc/ansible/roles# ansible-playbook filebeat-playbook.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may result in incorrectly calculated text widths that can cause
Display to print incorrect line lengths

PLAY [Installing and launching Filebeat] ****
TASK [Gathering Facts] ****
ok: [10.0.0.6]
ok: [10.0.0.5]
ok: [10.0.0.7]

TASK [download filebeat deb] ****
changed: [10.0.0.5]
changed: [10.0.0.7]
changed: [10.0.0.6]

TASK [install filebeat deb] ****
changed: [10.0.0.5]
changed: [10.0.0.7]
changed: [10.0.0.6]

TASK [drop in filebeat.yml] ****
changed: [10.0.0.6]
changed: [10.0.0.5]
changed: [10.0.0.7]
```

```
ok: [10.0.0.5]

TASK [enable and configure system module] ****
changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.7]

TASK [setup filebeat] ****
changed: [10.0.0.5]
changed: [10.0.0.7]
changed: [10.0.0.6]

TASK [start filebeat service] ****
changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.7]

TASK [enable service filebeat on boot] ****
ok: [10.0.0.7]
ok: [10.0.0.5]
ok: [10.0.0.6]

PLAY RECAP ****
10.0.0.5      : ok=8    changed=5    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.6      : ok=8    changed=5    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.7      : ok=8    changed=5    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Chapter 8: Verifying Installation and Playbook

1. Navigate to the Filebeat installation page on Kibana.
2. On the same page, scroll to **Step 5: Module Status** and click **Check Data**.
3. Scroll to the bottom of the page and click **Verify Incoming Data**.

The screenshot shows the Kibana interface with the title "System logs". The left sidebar has various icons for different data sources. The main area displays a step-by-step guide:

- Step 1: `./filebeat modules enable system`
Modify the settings in the `modules.d/system.yml` file.
- Step 2: **Start Filebeat**
The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.
`./filebeat setup
./filebeat -e`
[Copy snippet](#)
- Step 3: **Module status**
Check that data is received from the Filebeat `system` module
[Check data](#)
Data successfully received from this module

Chapter 9: Creating a Play to Install Metricbeat

1. Click 'Explore on my Own' on the Kibana server landing page.

The Kibana Home page displays several sections:

- Observability**: Includes APM, Logs, Metrics, and SIEM sections. Buttons for "Add APM", "Add log data", "Add metric data", and "Add events" are present.
- Add sample data**: Options to "Load a data set and a Kibana dashboard", "Upload data from log file" (import CSV, NDJSON, or log file), and "Use Elasticsearch data" (connect to Elasticsearch index).
- Visualize and Explore Data**: Includes APM and Canvas sections.
- Manage and Administer the Elastic Stack**: Includes Console and Index Patterns sections.

2. Click Add Metric Data.

The Kibana Add data page lists various metrics:

- ActiveMQ metrics
- Aerospike metrics
- Apache metrics
- AWS metrics
- Ceph metrics
- CockroachDB metrics
- Consul metrics
- CoreDNS metrics
- Couchbase metrics
- CouchDB metrics
- Docker metrics
- Dropwizard metrics
- Elasticsearch metrics
- Envoy Proxy metrics
- Etc metrics
- Golang metrics
- HAProxy metrics
- Kafka metrics
- Kibana metrics
- Kubernetes metrics

3. Click **Docker Metrics**.

Click the **DEB** tab under Getting Started.

The screenshot shows the Metricbeat Getting Started page. It has a sidebar with various icons. The main content area is titled "Getting Started" and has tabs for "macOS", "DEB" (which is selected), "RPM", and "Windows". Step 1, "Download and install Metricbeat", provides a command to download the DEB package from artifactory.elastic.co and install it using dpkg. Step 2, "Edit the configuration", shows a snippet of the metricbeat.yml configuration file for Elasticsearch output.

The Metricbeat installation instructions can be found here which is used for installing Metricbeat using ansible playbook.

4. Install Metricbeat using the commands displayed on the Kibana server landing page.

```

nandhinisreekumar — root@d1a2179a6c78:/ — ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 — 148x28
root@d1a2179a6c78:# curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.6.1-amd64.deb
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload  Upload Total   Spent    Left Speed
100 34.7M  100 34.7M    0      0  111M  0 --:--:-- --:--:-- --:--:-- 111M
root@d1a2179a6c78:# dpkg -i metricbeat-7.6.1-amd64.deb

Selecting previously unselected package metricbeat.
(Reading database ... 19998 files and directories currently installed.)
Preparing to unpack metricbeat-7.6.1-amd64.deb ...
Unpacking metricbeat (7.6.1) ...
Setting up metricbeat (7.6.1) ...
root@d1a2179a6c78:/#
root@d1a2179a6c78:/#

```

5. SSH into your Jumpbox.
6. Start and attach to the docker container.
7. Copy the content of the Metricbeat configuration file template to a new file (**metricbeat-config.yml**)

```

nandhinisreekumar — root@d1a2179a6c78:/etc/ansible/files — ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 — 148x28
root@d1a2179a6c78:/etc/ansible# cd files/
root@d1a2179a6c78:/etc/ansible/files# nano metricbeat-config.yml

```

7.1 Edit the username and password to **elastic** and **changeme** respectively in the configuration file. Also, replace the IP address with the IP address of your ELK Server VM.

```
● ○ ● nandhinisreekumar — root@d1a2179a6c78: /etc/ansible/files — ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 — 121x24
GNU nano 4.8                                     metricbeat-config.yml
# Configure what output to use when sending the data collected by the beat.

----- Elasticsearch output -----
output.elasticsearch:
  # TODO: Change the hosts IP address to the IP address of your ELK server
  # TODO: Change password from `changeme` to the password you created
  hosts: ["10.1.0.4:9200"]
  username: "elastic"
  password: "changeme"

----- Logstash output -----
#output.logstash:
  # The Logstash hosts
  #hosts: ["localhost:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificateAuthorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo
^X Exit       ^R Read File    ^\ Replace     ^U Paste Text  ^T To Spell   ^_ Go To Line M-B Redo
                                         M-A Mark Text
                                         M-6 Copy Text
```

7.2 Scroll to line #1806 (setup.kibana) and replace the IP address with the IP address of your ELK machine.

```
● ○ ● nandhinisreekumar — root@d1a2179a6c78: /etc/ansible/files — ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 — 121x24
GNU nano 4.8                                     metricbeat-config.yml
# website.
#setup.dashboards.url:

===== Kibana =====

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:
  host: "10.1.0.4:5601"

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  #host: "localhost:5601"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo
^X Exit       ^R Read File    ^\ Replace     ^U Paste Text  ^T To Spell   ^_ Go To Line M-B Redo
                                         M-A Mark Text
                                         M-6 Copy Text
```

8. Create a playbook to install Filebeat in /etc/ansible/roles/ directory. (**filebeat-playbook.yml**) with the following tasks:

- Download the .deb file from artifacts.elastic.co.
- Install the .deb file.

- Copy the Metribeat configuration file from the Ansible container to the WebVM(s) Metricbeat was installed.
- Enable and configure the docker module for metricbeat
- Setup Metricbeat
- Start Metricbeat service
- Enable the Metricbeat service on boot

```
nandhinisreekumar — root@d1a2179a6c78:/etc/ansible/roles — ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 — 148x28
root@d1a2179a6c78:# cd /etc/ansible/roles/
root@d1a2179a6c78:/etc/ansible/roles# nano metricbeat-playbook.yml
root@d1a2179a6c78:/etc/ansible/roles#
```

```
nandhinisreekumar — root@d1a2179a6c78:/etc/ansible/roles — ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 — 121x24
GNU nano 4.8                                     metricbeat-playbook.yml
[ Read 30 lines ]
- name: Install metric beat
  hosts: webservers
  become: true
  tasks:
    - name: Download metricbeat
      command: curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.4.0-amd64.deb
    - name: install metricbeat
      command: dpkg -i metricbeat-7.4.0-amd64.deb
    - name: drop in metricbeat config
      copy:
        src: /etc/ansible/files/metricbeat-config.yml
        dest: /etc/metricbeat/metricbeat.yml
    - name: enable and configure docker module for metric beat
      command: metricbeat modules enable docker
^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo   M-A Mark Text
^X Exit       ^R Read File   ^L Replace    ^U Paste Text  ^T To Spell   ^G Go To Line  M-E Redo   M-6 Copy Text  2
```

```
nandhinisreekumar — root@d1a2179a6c78:/etc/ansible/roles — ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 — 121x24
GNU nano 4.8                                     metricbeat-playbook.yml
[ Read 30 lines ]
- name: drop in metricbeat config
  copy:
    src: /etc/ansible/files/metricbeat-config.yml
    dest: /etc/metricbeat/metricbeat.yml
- name: enable and configure docker module for metric beat
  command: metricbeat modules enable docker
- name: setup metric beat
  command: metricbeat setup
- name: start metric beat
  command: service metricbeat start -e
- name: enable service metricbeat on boot
  systemd:
    name: metricbeat
    enabled: yes
^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo   M-A Mark Text
^X Exit       ^R Read File   ^L Replace    ^U Paste Text  ^T To Spell   ^G Go To Line  M-E Redo   M-6 Copy Text
```

9. Save the file.

10. Run the playbook.

```
root@d1a2179a6c78:/etc/ansible/roles# ansible-playbook metricbeat-playbook.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this
may result in incorrectly calculated text widths that can cause Display to
print incorrect line lengths

PLAY [Install metric beat] *****
TASK [Gathering Facts] *****
ok: [10.0.0.6]
ok: [10.0.0.7]
ok: [10.0.0.5]

TASK [Download metricbeat] *****
changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.7]

TASK [install metricbeat] *****
changed: [10.0.0.5]
changed: [10.0.0.7]
changed: [10.0.0.6]

TASK [drop in metricbeat config] *****
ok: [10.0.0.7]

root@d1a2179a6c78:/etc/ansible/roles# ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 - 121x24
nandhinisreekumar - root@d1a2179a6c78: /etc/ansible/roles - ssh -i .ssh/id_rsa RedAdmin@13.83.47.196 - 121x24

changed: [10.0.0.6]
changed: [10.0.0.7]

TASK [setup metric beat] *****
changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.7]

TASK [start metric beat] *****
changed: [10.0.0.6]
changed: [10.0.0.7]
changed: [10.0.0.5]

TASK [enable service metricbeat on boot] *****
ok: [10.0.0.7]
ok: [10.0.0.6]
ok: [10.0.0.5]

PLAY RECAP *****
10.0.0.5      : ok=8    changed=5    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.6      : ok=8    changed=5    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.7      : ok=8    changed=5    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

root@d1a2179a6c78:/etc/ansible/roles#
```

11. Navigate to the Filebeat installation page on Kibana.

12. On the same page, scroll to **Step 5: Module Status** and click **Check Data**.

13. Scroll to the bottom of the page and click **Verify Incoming Data**.

The screenshot shows a Kibana dashboard titled "Docker metrics". On the left, there's a sidebar with various icons. The main area has a light gray background with several sections:

- Step 1:** A terminal window with the command `./metricbeat modules enable docker`. Below it, a note says "Modify the settings in the `modules.d/docker.yml` file." There's also a "Copy snippet" button.
- Step 2:** A section titled "Start Metricbeat" with the command `./metricbeat setup` followed by `./metricbeat -e`.
- Step 3:** A section titled "Module status" with the note "Check that data is received from the Metricbeat `docker` module". It includes a "Check data" button and a message "Data successfully received from this module".
- Bottom:** A note "When all steps are complete, you're ready to explore your data." and a "Docker metrics dashboard" button.