

Phase 1 – Azure Virtual Machine Installation

Intro (What & Why)

In this phase, **we are creating a Linux virtual machine in Azure**.

During this process, **Azure automatically creates the required resource group** for us.

This approach is common for beginners and labs, and it is **perfectly acceptable** as long as we understand what Azure is doing in the background.

The VM will later be used to:

- Generate security-relevant logs
- Act as a monitored endpoint
- Integrate with Microsoft Sentinel

Steps

1. Virtual Machine Creation

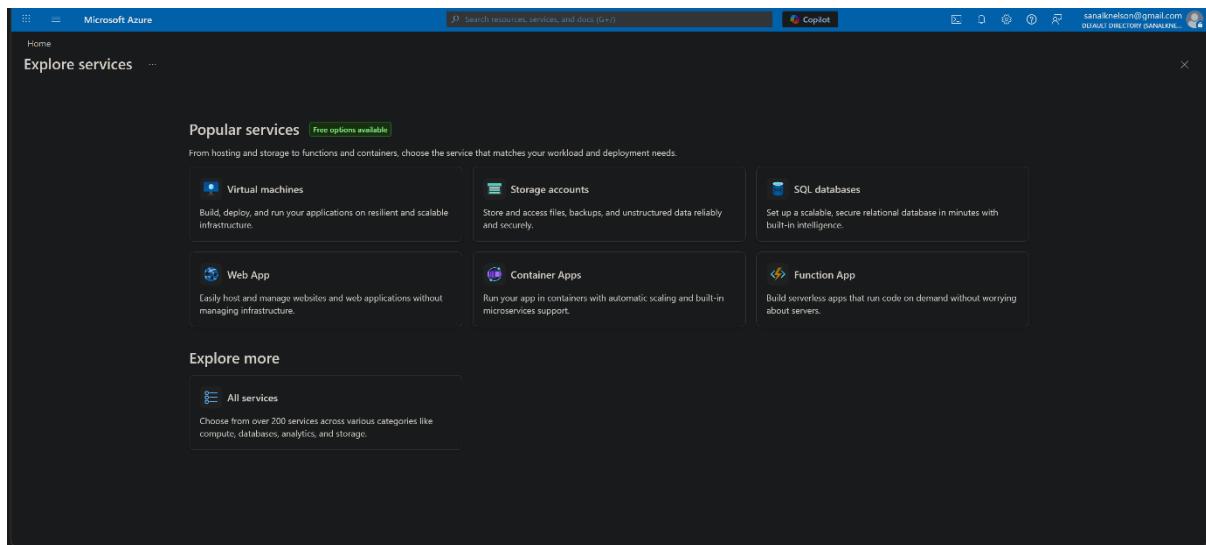
We start by **creating a new virtual machine directly**.

During the VM creation:

- We select **Create new** for the resource group
- Azure automatically creates the resource group along with the VM

I did not create the resource group separately.

Azure created it as part of the VM deployment, which is a valid and commonly used approach.



2. Virtual Machine Basics

We now **configure the core VM settings**.

We need to:

- Choose **Ubuntu Server 24.04 LTS**
- Select a cost-effective VM size (B2as v2)
- Use **SSH public key authentication**
- Enable Secure Boot and vTPM

I used Azure-generated SSH keys for simplicity.

A better practice would be managing keys locally, which we can improve later.

Microsoft Azure

Home

Choose recommended defaults that match your workload

configurations at any time.

Select a workload environment

Dev/Test	Production default
✓ Boot diagnostics	✓ Boot diagnostics
High availability	✓ High availability
Azure backup (where available)	✓ Azure backup (where available)

Select a workload type

General purpose (D-Series) default	Memory optimized (E-Series)	Compute optimized (F-Series)
Example sizes DS2_v2: 2 CPU, 7 GB DS3_v2: 4 CPU, 14 GB	Example sizes E2s_v3: 2 CPU, 16 GB E4s_v3: 4 CPU, 32 GB	Example sizes F2s_v2: 2 CPU, 4 GB F4s_v2: 4 CPU, 8 GB
Fast CPUs with optimal CPU-to-memory configuration	High memory-to-core ratio optimized for heavy in-memory applications	High CPU-to-memory ratio optimized for compute intensive workloads
Workload types Enterprise applications, relational databases, analytics	Workload types SAP HANA, SQL Hekaton, other large in-memory workloads	Workload types Batch processing, web servers, gaming

[Continue to create a VM](#) [Skip this step](#)

Microsoft Azure

Home

Select a VM size

Search by VM size... Display cost : Monthly vCPUs : All RAM (GiB) : All Add filter

Showing 1044 VM sizes. | Subscription: Azure subscription 1 | Region: Central India | Current size: Standard_B2as_v2 | Image: Ubuntu Server 24.04 LTS | Learn more about VM sizes Group by series

VM Size ↑↓	Type ↑↓	vCPUs ↑↓	RAM (GiB) ↑↓	Data disks ↑↓	Max IOPS ↑↓	Local storage (GiB) ↑↓	Premium disk ↑↓	Cost/month ↑↓
The most used sizes by users in Azure								
B2as_v2 ↗	General purpose	2	8	4	3750	N/A	Supported	\$35.92
D2as_v5 ↗	General purpose	2	8	4	3750	N/A	Supported	\$40.59
D2ads_v5 ↗	General purpose	2	8	4	3750	75 (SCSI)	Supported	\$48.98
D2ls_v5 ↗	General purpose	2	4	4	3750	N/A	Supported	\$62.05
B4as_v2 ↗	General purpose	4	16	8	6400	N/A	Supported	\$71.83
D2s_v5 ↗	General purpose	2	8	4	3750	N/A	Supported	\$73.73
D4as_v5 ↗	General purpose	4	16	8	6400	N/A	Supported	\$81.03
D8as_v5 ↗	General purpose	8	32	16	12800	N/A	Supported	\$162.06

> B-Series v2 Ideal for workloads that do not need continuous full CPU performance

Select Prices presented are estimates in USD that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Final charges will appear in your local currency in cost analysis and billing views. [View Azure pricing calculator.](#) Give feedback

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The user is on the 'Choose recommended defaults that match your workload' step.

SSH public key source: Generate new key pair

SSH Key Type: RSA SSH Format (selected)

Key pair name *: azure-secure-web-vm_key

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 *: Allow selected ports (selected)

Select inbound ports *:

- SSH (22) (selected)
- HTTP (80)
- HTTPS (443)
- SSH (22) (selected)

Buttons: < Previous, Next : Disks >, Review + create

3. Disk Configuration

We continue by **configuring VM storage**.

We keep:

- Default OS disk size
- Managed disks
- Platform-managed encryption
- Delete disk on VM delete

For a learning lab, default disk settings are sufficient and reduce complexity.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The current step is 'Choose recommended defaults that match your workload'. The configuration shown includes:

- VM disk encryption:** A note states "Encryption at host is not registered for the selected subscription." with a link to learn more.
- OS disk:**
 - OS disk size: Image default (30 GiB)
 - OS disk type: Premium SSD (locally-redundant storage)
 - Delete with VM: Checked
 - Key management: Platform-managed key
- Data disks for azure-secure-web-vm:** A table with columns LUN, Name, Size (GiB), Disk type, Host caching, and Delete with VM. It contains two rows:
 - Create and attach a new disk
 - Attach an existing disk

At the bottom are navigation buttons: < Previous, Next : Networking >, and Review + create.

4. Networking Configuration

Now we **set up networking for the VM**.

We need to:

- Create a new virtual network and subnet
- Assign a public IP address
- Attach a Network Security Group
- Allow inbound SSH (22)

SSH is open to the internet only for lab access.

In real environments, this should be restricted to known IPs or private access.

Microsoft Azure

Search resources, services, and more

Home > Explore services > Choose recommended defaults that match your workload

Create a virtual machine

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network [\(New\) vnet-centralindia \(rg-azure-secure-vm\)](#) [Edit virtual network](#)

Subnet * [\(New\) snet-centralindia-1](#) [Edit subnet](#) 172.16.0.0 - 172.16.0.255 (256 addresses)

Public IP [Create new](#) [Public IP addresses have a nominal charge. Estimate price](#)

NIC network security group [None](#) [Basic](#) [Advanced](#)

Public inbound ports * [None](#) [Allow selected ports](#)

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

The screenshot shows the Microsoft Azure 'Create a virtual machine' configuration page. At the top, the navigation bar includes 'Home > Explore services > Choose recommended defaults that match your workload'. The main title is 'Create a virtual machine'. Below the title, there's a section for 'Inbound ports' where 'Allow selected ports' is selected, and 'SSH (22)' is chosen from a dropdown. A warning message states: '⚠️ 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.' Under 'Advanced networking', 'Delete public IP and NIC when VM is deleted' is checked. In the 'Load balancing' section, 'None' is selected. At the bottom, there are navigation buttons: '< Previous', 'Next : Management >', and a blue 'Review + create' button.

5. Management & Auto-Shutdown

Next, we **configure management options**.

We:

- Enable auto-shutdown
- Set the correct time zone
- Configure email notification

Auto-shutdown helps control cost and shows good cloud hygiene.

Microsoft Azure ≡ Search resources, services

Home > Explore services > Choose recommended defaults that match your workload

Create a virtual machine ...

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Configure management options for your VM.

Microsoft Defender for Cloud

Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more ↗](#)

Your subscription is protected by Foundational Cloud Security Posture Management Free Plan.

Identity

Enable system assigned managed identity

Microsoft Entra ID

Login with Microsoft Entra ID
 RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Microsoft Entra ID login. [Learn more ↗](#)

Microsoft Entra ID 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

< Previous Next : Monitoring > **Review + create**

User Login is required when using Microsoft Entra ID login. [Learn more](#)

Auto-shutdown

Enable auto-shutdown

Shutdown time

Time zone

Notification before shutdown

Email * ✓

Backup

Enable backup

Guest OS updates

Enable periodic assessment

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

< Previous Next : Monitoring > Review + create

6. Monitoring & Diagnostics

We then **enable monitoring and diagnostics**.

We need to:

- Enable boot diagnostics
- Enable OS guest diagnostics
- Allow Azure to create a diagnostics storage account
- Enable recommended alert rules

These settings are important later when we analyze logs in Sentinel.

Microsoft Azure

Home > Explore services > Choose recommended defaults that match your workload

Create a virtual machine ...

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

Configure monitoring options for your VM.

Alerts

Enable recommended alert rules

Alert rules **Alert rules not configured** Configure

Diagnostics

Boot diagnostics Enable with managed storage account (recommended) Enable with custom storage account Disable There is a nominal charge for the managed storage account.

Enable OS guest diagnostics

Health

Enable application health monitoring

Set up recommended alert rules

Select alert rules

- > Percentage CPU is greater than 80
- > Available Memory Bytes is less than 1
- > Data Disk IOPS Consumed Percentage is greater than 95
- > OS Disk IOPS Consumed Percentage is greater than 95
- > Network In Total is greater than 500
- > Network Out Total is greater than 200
- > VmAvailabilityMetric is less than 1

Notify me by

Email Email Azure Resource Manager Role Azure mobile app notification

Estimated monthly total: 0.00 USD

< Previous | Next : Advanced > | Review + create | Save | Cancel

Microsoft Azure

Home > Explore services > Choose recommended defaults that match your workload

Create a virtual machine ...

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

Configure monitoring options for your VM.

Alerts

Enable recommended alert rules

Alert rules

Alert me if

- Percentage CPU is greater than 80%
- Available Memory Bytes is less than 1GB
- Data Disk IOPS Consumed Percentage is greater than 95%
- OS Disk IOPS Consumed Percentage is greater than 95%
- Network In Total is greater than 500GB
- Network Out Total is greater than 200GB
- VmAvailabilityMetric is less than 1

Notify me by

- Email: sanalknelson@gmail.com

Edit

Diagnostics

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

< Previous | Next : Advanced > | Review + create

The screenshot shows the Microsoft Azure 'Create a virtual machine' configuration page. At the top, there are navigation links: Home > Explore services > Choose recommended defaults that match your workload. Below this, the title 'Create a virtual machine' is displayed. A vertical sidebar on the left contains sections for 'Diagnostics' (Boot diagnostics, Enable OS guest diagnostics), 'Health' (Enable application health monitoring), and 'Advanced settings' (VM extensions, Cloud-init, Capacity reservations). The main content area includes a 'Metrics alert' section with a list of triggers:

- Available Memory Bytes is less than 1GB
- Data Disk IOPS Consumed Percentage is greater than 95%
- OS Disk IOPS Consumed Percentage is greater than 95%
- Network In Total is greater than 500GB
- Network Out Total is greater than 200GB
- VmAvailabilityMetric is less than 1

Below this, there is a 'Notify me by' section with an email address listed: sanalknelson@gmail.com. There is also an 'Edit' button.

In the 'Diagnostics' section, 'Boot diagnostics' is set to 'Enable with managed storage account (recommended)' (radio button selected). 'Enable OS guest diagnostics' is checked. 'Diagnostics storage account' is set to '(new) rgazuresecurevmdiag' (dropdown menu selected).

In the 'Health' section, 'Enable application health monitoring' is unchecked.

At the bottom, there are navigation buttons: '< Previous', 'Next : Advanced >', and a blue 'Review + create' button.

7. Advanced Settings

At this stage, we **do not add advanced features**.

We leave:

- VM extensions disabled
- Cloud-init empty
- Capacity reservations unused

Keeping this minimal avoids deployment failures during learning.



Home > Explore services > Choose recommended defaults that match your workload

Create a virtual machine

Basics Disks Networking Management Monitoring 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

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

< Previous

Next : Tags >

[Review + create](#)

Microsoft Azure

Home > Explore services > Choose recommended defaults that match your workload

Create a virtual machine

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

Performance (NVMe)

Enable capabilities to enhance the performance of your resources.

Higher remote disk storage performance with NVMe ⓘ The selected size is not supported for NVMe. [See supported size families](#)

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 ⓘ No host groups found ▼

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](#)

< Previous Next : Tags > Review + create

The screenshot shows the Microsoft Azure 'Create a virtual machine' wizard. The top navigation bar includes 'Microsoft Azure', a search bar, and a 'Home > Explore services > Choose recommended defaults that match your workload' breadcrumb trail. The main title is 'Create a virtual machine'. The current step is 'Host', which describes Azure Dedicated Hosts. It includes a note about capacity reservations and proximity placement groups. The 'Capacity reservations' section shows three options: 'None' (selected), 'Capacity reservation group', and '(Preview) Shared capacity reservation group'. The 'Proximity placement group' section shows no results found. At the bottom, there are navigation buttons: '< Previous', 'Next : Tags >', and a prominent blue 'Review + create' button.

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 ⓘ No host groups found

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 reservations ⓘ

- None
Do not use reserved capacity
- Capacity reservation group
Use reserved capacity from this subscription
- (Preview) Shared capacity reservation group
Use reserved capacity from another subscription

Proximity placement group

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

Proximity placement group ⓘ No proximity placement groups found

< Previous Next : Tags > Review + create

8. Deployment & SSH Validation

Finally, we **review and create the VM**.

After deployment:

- Download the private SSH key
- Connect to the VM using SSH
- Confirm successful login

Successful SSH access confirms that networking and authentication are correctly configured.

Microsoft Azure

Search resources, services, and

Home > Explore services > Choose recommended defaults that match your workload

Create a virtual machine

Validation passed

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Price

1 X Standard B2as v2 by Microsoft Subscription credits apply ⓘ

0.0492 USD/hr Pricing for other VM sizes

[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.

Name SANAL NELSON

Preferred e-mail address sanalknelson@gmail.com

Preferred phone number

< Previous Next > **Create**

Microsoft Azure

Home > Explore services > Choose recommended defaults that match your workload

Create a virtual machine

Validation passed

User data: No
Disk controller type: SCSI
Proximity placement group: None
Capacity reservation group: None

Tags:

Project	azure-secure-vm (Auto-shutdown schedule)
Project	azure-secure-vm (Availability set)
Project	azure-secure-vm (Disk)
Project	azure-secure-vm (Network interface)
Project	azure-secure-vm (Network security group)
Project	azure-secure-vm (Public IP address)
Project	azure-secure-vm (Recovery Services vault)
Project	azure-secure-vm (undefined)
Project	azure-secure-vm (SQL Virtual Machine)
Project	azure-secure-vm (SSH key)
Project	azure-secure-vm (Storage account)
Project	azure-secure-vm (Virtual machine)
Project	azure-secure-vm (Virtual machine extension)
Project	azure-secure-vm (Virtual network)

Generate new key pair

An SSH key pair contains both a public key and a private key. **Azure doesn't store the private key.** After the SSH key resource is created, you won't be able to download the private key again. [Learn more](#)

[Download private key and create resource](#)

[Return to create a virtual machine](#)

< Previous | Next > | [Create](#)

```
PS C:\Users\lenovo\Downloads> ssh -i "azure-secure-web-vm_key.pem" azureuser@1.Your-VM-public-IP
The authenticity of host '1.Your-VM-public-IP (1.Your-VM-public-IP)' can't be established.
ED25519 key fingerprint is SHA256:NDC7ep5tVc4AVC7jBMOCIt3RzOABCbXRWu4+D3ohQeM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '1.Your-VM-public-IP' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1017-azure x86_64)

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

System information as of Sun Feb  1 12:08:40 UTC 2026

System load:  0.02           Processes:          119
Usage of /:   6.6% of 28.02GB  Users logged in:     0
Memory usage: 3%              IPv4 address for eth0: 172.16.0.4
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@azure-secure-web-vm:~$ |
```

Outcome

At the end of this phase:

- A Linux VM is successfully running in Azure
- Resource group was auto-created during VM deployment
- SSH access is verified
- Diagnostics and monitoring are enabled
- The VM is ready for Sentinel integration in the next phase