

1, Create a vm with Ds1-V2 standard?

In basics, we have to select vm with ds1-v2 standard. The diagrams are as follows.

Basics

Disks

Networking

Management

Advanced

Tags

Review + create

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. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Free Trial

Resource group * ⓘ

(New) VM2_group

Create new

Instance details

Virtual machine name * ⓘ

VM2

Region * ⓘ

(US) East US

Availability options ⓘ

No infrastructure redundancy required

Image * ⓘ

Windows Server 2016 Datacenter

Browse all public and private images

Review + create

< Previous

Next : Disks >

Create a virtual machine

Azure Spot instance ⓘ

☐ Yes ☒ No

Size * ⓘ

Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (₹6,079.53/month) ✓

[Select size](#)

Administrator account

Username * ⓘ

Charitha1999 ✓

Password * ⓘ

..... ✓

Confirm password * ⓘ

..... ✓

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 *

RDP (3389) ✓



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 >](#)

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 HDD

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Encryption type *

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





Enable Ultra Disk compatibility

☐ Yes ☒ No

Ultra disk is available only for Availability Zones in eastus.

Data disks

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	
0	VM2_DataDisk_0	1024	Premium SSD	None	 
1	No existing disks i... 			Read-only	

Review + create

< Previous

Next : Networking >

Create a virtual machine

Basics Disks Networking Management 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) VM2_group-vnet

Create new

Subnet * ⓘ

(new) default (10.0.1.0/24)

Public IP ⓘ

(new) VM2-ip

Create new

NIC network security group ⓘ

☐ None ☒ Basic ☐ Advanced

Public inbound ports * ⓘ

☐ None ☒ Allow selected ports

Select inbound ports *

RDP (3389)

 **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 restrict access to only selected IP addresses.

Review + create

< Previous

Next : Management >


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 ⓘ ☒ On ☐ Off

OS guest diagnostics ⓘ ☐ On ☒ Off

Diagnostics storage account * ⓘ 
[Create new](#)

Identity

System assigned managed identity ⓘ ☐ On ☒ Off

Azure Active Directory

[Review + create](#)

[< Previous](#)

[Next : Advanced >](#)

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 ⓘ



Microsoft Antimalware
Microsoft Corp.



[Select an extension to install](#)

Custom data

Pass a 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



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

[Review + create](#)

[< Previous](#)

[Next : Tags >](#)

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
<input type="text" value="cs2"/>	<input type="text" value="12345"/>	12 selected   ...
<input type="text"/>	<input type="text"/>	12 selected 

Review + create

< Previous

Next : Review + create >

2, Attach one data disk of size 50gb and split into 3 inside the vm

Create a managed disk

storage type, and number of transactions.

Disk name * ⓘ

Zdrive



Resource group *

VM2_group



[Create new](#)

Location

East US

Availability zone ⓘ

None

Source type ⓘ

None



Size * ⓘ

50 GiB

Premium SSD

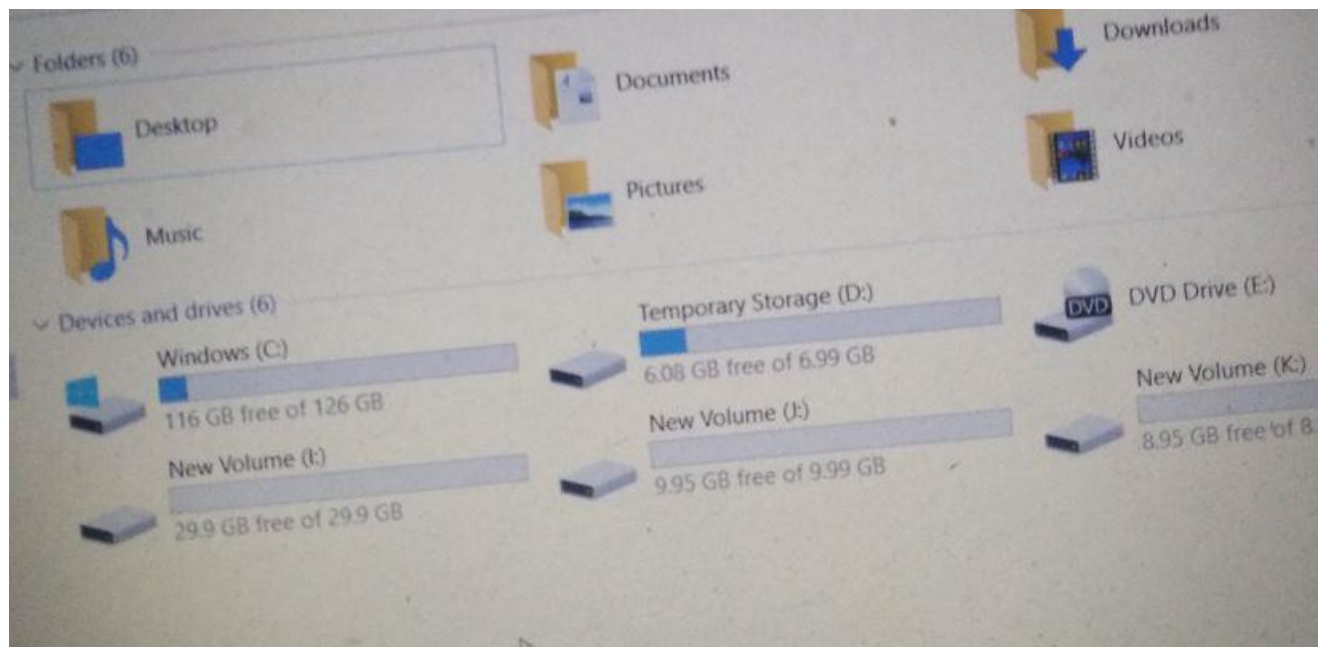
[Change size](#)

Encryption type *

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



Create



3, It should have enabled auto shutdown by 5:00 PM IST before that it has to trigger a notification to the email id?

Home >

VM2 | Auto-shutdown

Virtual machine

Search (Ctrl+/) << Save Discard Feedback

- Security
- Advisor recommendations
- Extensions
- Continuous delivery
- Availability + scaling
- Configuration
- Identity
- Properties
- Locks
- Export template

Operations

- Bastion
- Auto-shutdown**
- Backup
- Disaster recovery
- Update management
- Inventory

Enabled

On Off

Scheduled shutdown

5:00:00 PM

Time zone

(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Send notification before auto-shutdown?

Yes No

Webhook URL ⓘ

Email address ⓘ

nagacharitha985@gmail.com

4, You should be able to login to the servers with two usernames?

To login into the same server but with different user name the step to be followed is shown in the image.

Initially, I login with VM2 as a user name but later I login using dummy as a user name.

Mode ⓘ

- ☒ Reset password
☐ Reset configuration only

Username * ⓘ

dummy

Password *

.....

Confirm password *

.....

5, Install Microsoft antimalware extension in the vm?



Microsoft Antimalware

Microsoft Corp.

blade without inputting any configuration setting values.

To **enable** antimalware with a **custom configuration**, input the supported values for the configuration settings provided on the **Add Extension** blade and click **Create**. Please refer to the **tooltips** provided with each configuration setting on the Add Extension blade to see the supported configuration values.

To **enable antimalware event collection** for a virtual machine, click any part of the **Monitoring lens** in the virtual machine blade, click **Diagnostics** command on Metric blade, select **Status ON** and check **Windows Event system logs**. The antimalware events are collected from the Windows Event system logs to your storage account. You can configure the storage account for your virtual machine to collect the antimalware events by selecting the appropriate storage account.

Legal Terms

By clicking the Create button, I acknowledge that I am getting this software from Microsoft Corp. and that the [legal terms](#) of Microsoft Corp. apply to it. Microsoft does not provide rights for third-party software. Also see the [privacy statement](#) from Microsoft Corp.,

Publisher

Microsoft Corp.

Useful Links

[Documentation](#)

[Powershell Cmdlets](#)

Create

Install extension

Excluded files and locations ⓘ

sample

Excluded file extensions ⓘ

sample

Excluded processes ⓘ

sample

Real-time protection ⓘ

Enable

Disable

Run a scheduled scan ⓘ

Enable

Disable

Scan type ⓘ

Quick

Full

Scan day ⓘ

Saturday

▼

Scan time ⓘ

120

OK