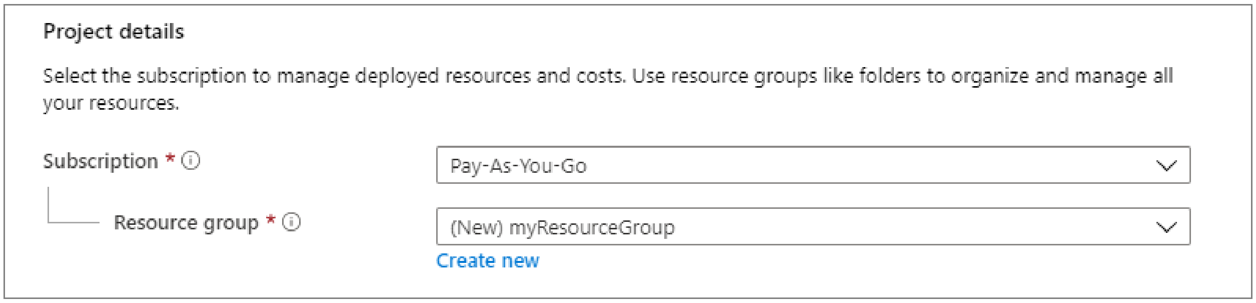
Create a Linux virtual machine in the Azure portal

1. Sign in to Azure
    a. Sign in to the Azure portal.
2. Create a virtual machine
    a. Enter virtual machines in the search.
    b. Under Services, select Virtual machines.
    c. On the Virtual Machines page, select "Create" and then "Virtual Machine." The "Create a Virtual Machine" page opens.
    d. In the Basics tab, under Project details, make sure the correct subscription is selected and then choose to Create new resource group. Enter [Name]-rg for the name.*.



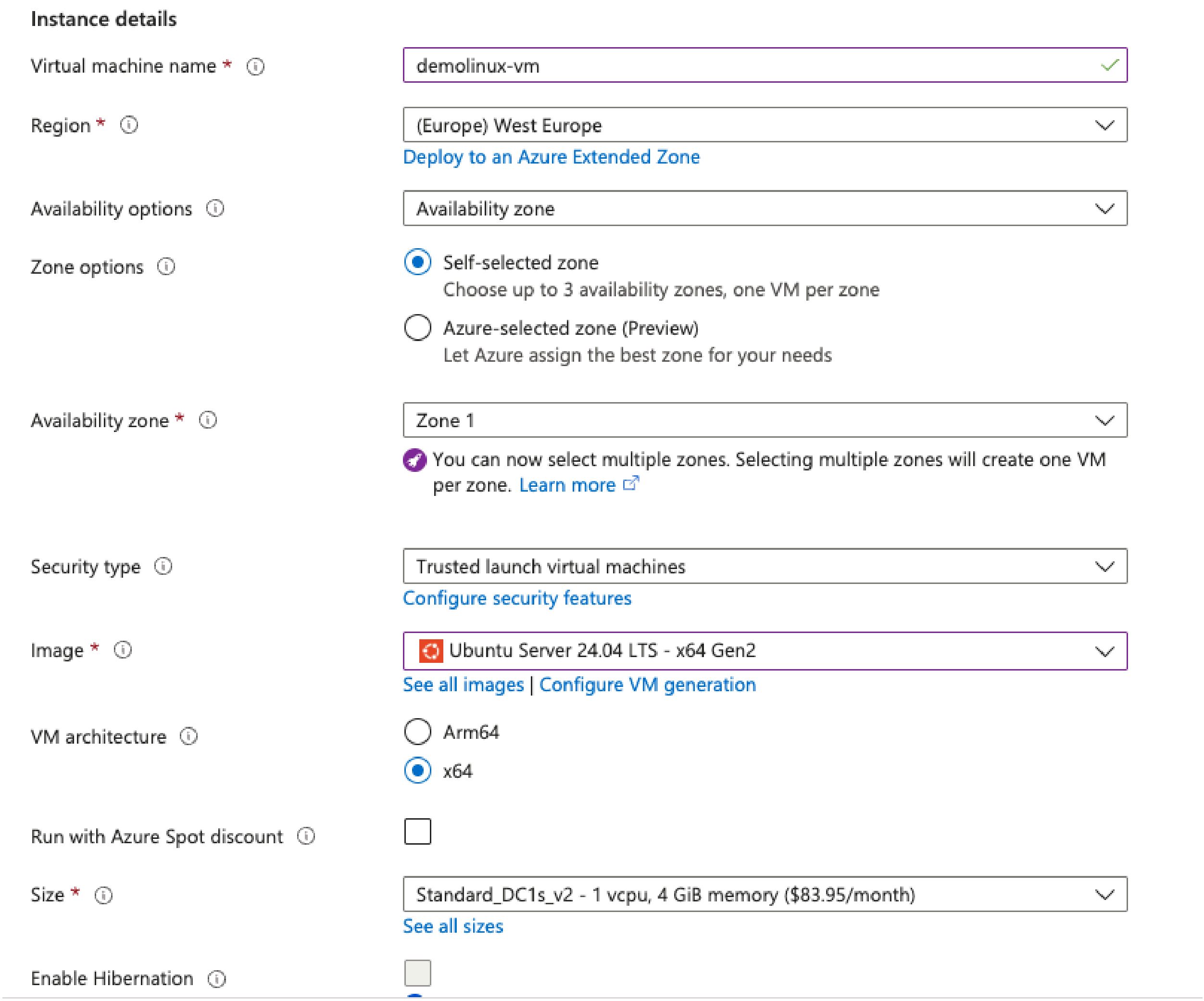
Project details

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

Subscription * : Pay-As-You-Go

Resource group * : (New) myResourceGroup

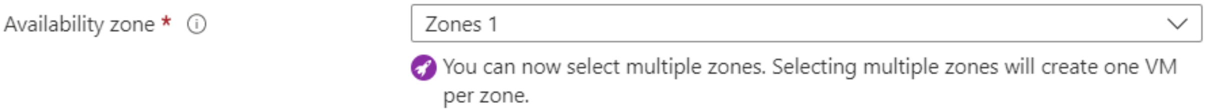
    e. Under Instance details, enter myVM for the Virtual machine name, and choose Ubuntu Server 22.04 LTS - Gen2 for your Image. Leave the other defaults. The default size and pricing is only shown as an example. Size availability and pricing are dependent on your region and subscription.



Instance details

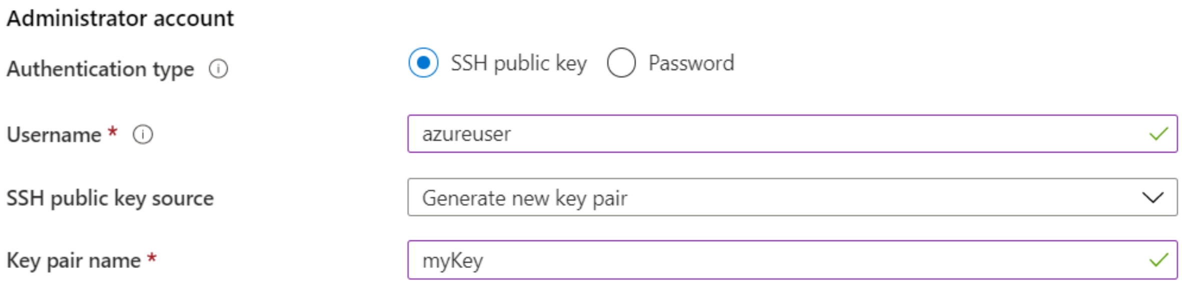
Virtual machine name * ⓘ	demolinux-vm ✓
Region * ⓘ	(Europe) West Europe Deploy to an Azure Extended Zone
Availability options ⓘ	Availability zone
Zone options ⓘ	● Self-selected zone Choose up to 3 availability zones, one VM per zone ○ Azure-selected zone (Preview) Let Azure assign the best zone for your needs
Availability zone * ⓘ	Zone 1 You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more
Security type ⓘ	Trusted launch virtual machines Configure security features
Image * ⓘ	Ubuntu Server 24.04 LTS - x64 Gen2 See all images | Configure VM generation
VM architecture ⓘ	○ Arm64 ● x64
Run with Azure Spot discount ⓘ	□
Size * ⓘ	Standard_DC1s_v2 - 1 vcpu, 4 GiB memory ($83.95/month) See all sizes
Enable Hibernation ⓘ	□

Note: Some users will now see the option to create VMs in multiple zones.



Availability zone * ⓘ	Zones 1 You can now select multiple zones. Selecting multiple zones will create one VM per zone.

3. Under the Administrator account, select SSH public key.
4. In Username, enter azureuser.
5. For the SSH public key source, leave the default of Generate new key pair, and then enter myKey for the Key pair name.



Administrator account

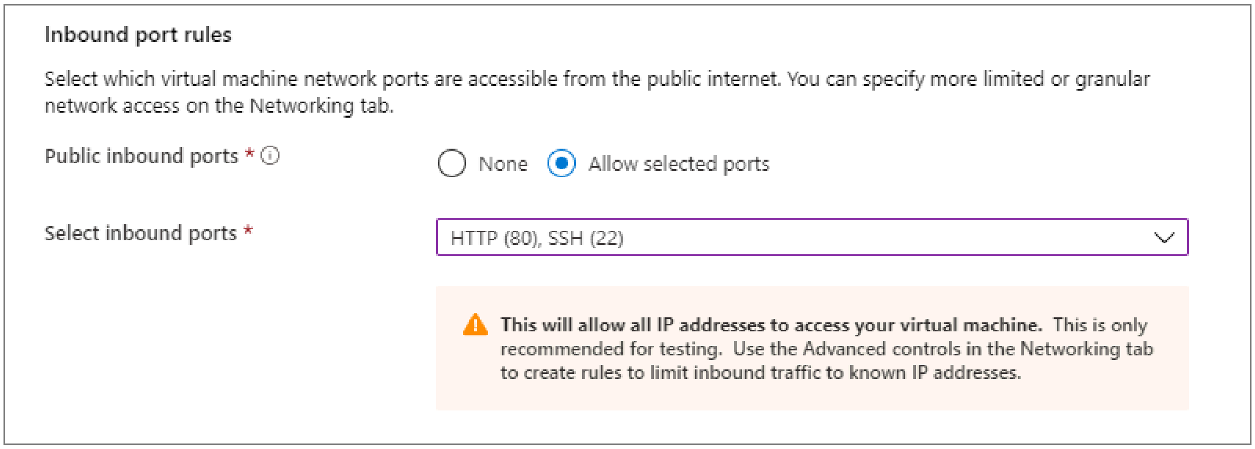
Authentication type ⓘ ● SSH public key ○ Password

Username * ⓘ azureuser ✓

SSH public key source Generate new key pair

Key pair name * myKey ✓

6. Under Inbound port rules > Public inbound ports, choose Allow selected ports and then select SSH (22) and HTTP (80) from the drop-down.



Inbound port rules

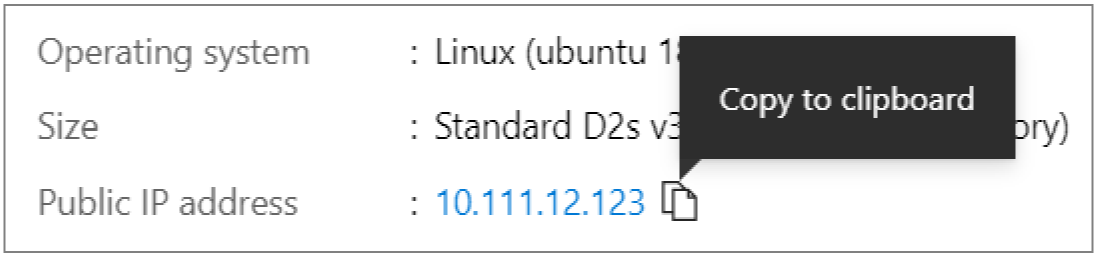
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ ○ None ● Allow selected ports

Select inbound ports * HTTP (80), 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.

7. Leave the remaining defaults and then select the Review + create button at the bottom of the page.
8. On the Create a virtual machine page, you can see the details about the VM you are about to create. When you are ready, select Create.
9. When the Generate new key pair window opens, select Download Private Key and create a resource. Your key file will be downloaded as myKey.pem. Make sure you know where the .pem file was downloaded; you will need the path to it in the next step.
10. When the deployment is finished, select Go to resource.
11. On the page for your new VM, select the public IP address and copy it to your clipboard.



Operating system : Linux (ubuntu 1

Size : Standard D2s v3 ory)

Public IP address : 10.111.12.123

Connect to the virtual machine

1. Create an SSH connection with the VM.
    a. If you are on a Mac or Linux machine, open a Bash prompt and set read-only permission on the .pem file using

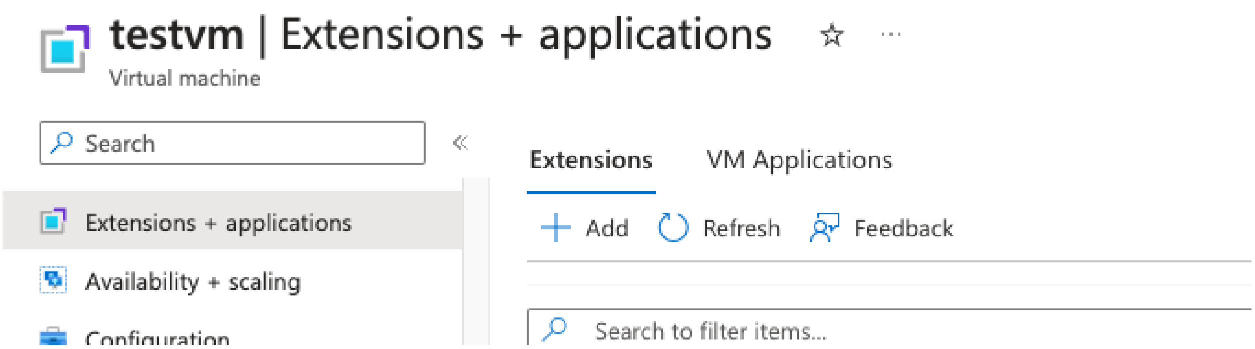
```
chmod 400 ~/Downloads/myKey.pem.
```

    b. If you are on a Windows machine, open a PowerShell prompt.
2. At your prompt, open an SSH connection to your virtual machine. Replace the IP address with the one from your VM, and replace the path to the .pem with the path to where the key file was downloaded.

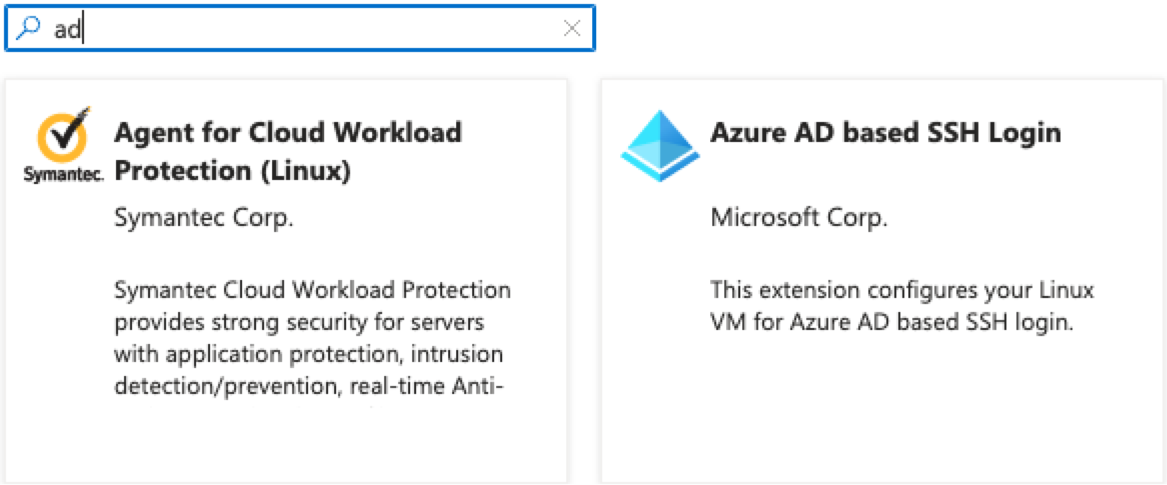
```
ssh -i ~/Downloads/myKey.pem azureuser@10.111.12.123
```

Install AADLoginForLinux Extension

1. Navigate to Your VM:
    a. In the left sidebar, click on "Virtual Machines".
    b. Find and click on the name of the virtual machine where you want to install the extension.
2. Add the AADLoginForLinux Extension:
    a. In the VM's pane, under the "Settings" section, click on "Extensions".



    b. Click on "+ Add" at the top of the page to add a new extension.
    c. In the search box, type **Azure AD based SSH Login** to filter the list.
    d. From the results, select **Azure AD based SSH Login** by Microsoft and click "Create".



ad

Agent for Cloud Workload Protection (Linux)

Symantec Corp.

Symantec Cloud Workload Protection provides strong security for servers with application protection, intrusion detection/prevention, real-time Anti-

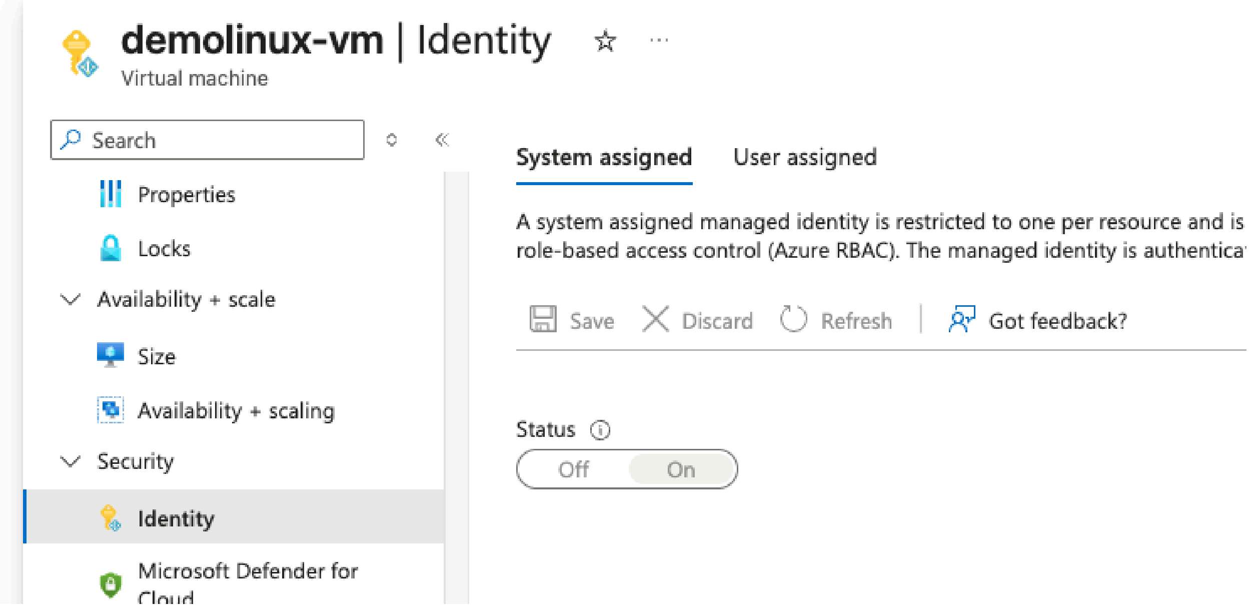
Azure AD based SSH Login

Microsoft Corp.

This extension configures your Linux VM for Azure AD based SSH login.

   e. The default settings should be sufficient for most installations. Review the settings, and if everything looks good, click "OK".

3. The virtual machine needs a managed identity to communicate with Entra ID
   a. On the virtual machine menu
   b. Go to **Security->Identity**
   c. On the **System Assigned** set status to On
   d. **Save**



demolinux-vm | Identity

Virtual machine

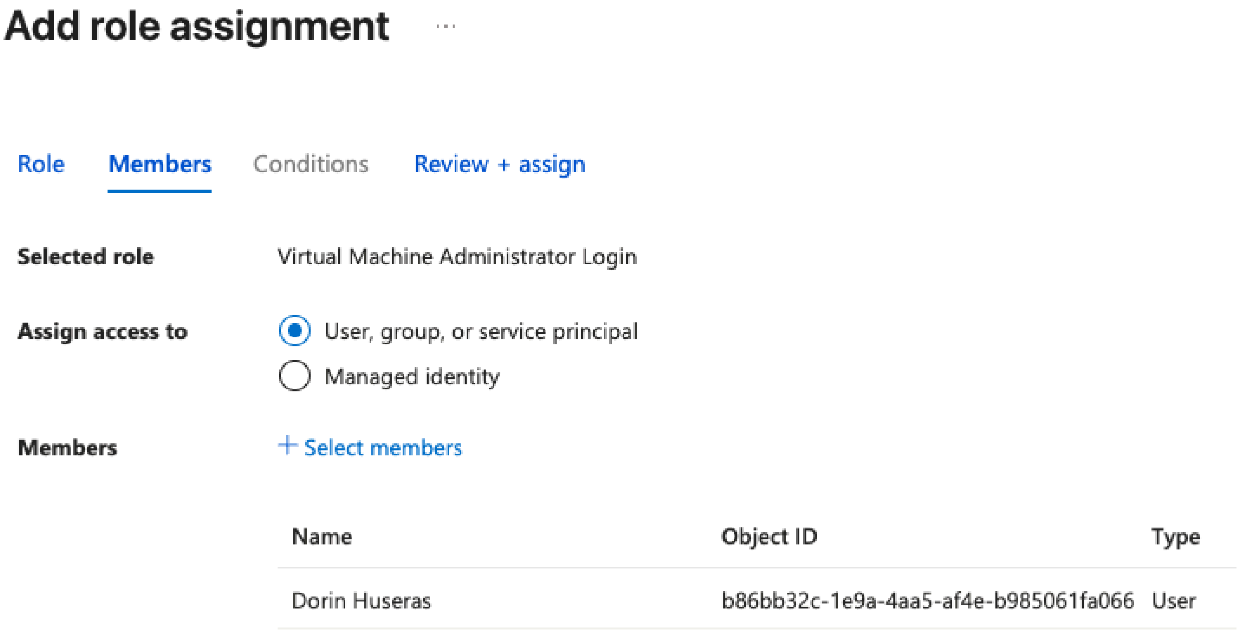
System assigned | User assigned

A system assigned managed identity is restricted to one per resource and is role-based access control (Azure RBAC). The managed identity is authentica

Status: Off / On

4. Grant VM Access to Azure AD (AAD) Users/Groups:
   a. This step is important as installing the extension alone doesn't grant any AAD user access to the VM. You need to explicitly provide access:
   b. While still in the VM's settings, click on "Access Control(IAM)" from the sidebar.
   c. Click on Role assignments
      i. For individual users:

            1. Click "Add user", and then search for and select the Azure AD user. Assign a role (like "**Virtual Machine Administrator Login**") and set the type as "Azure AD user". Click "Save".
        ii. For groups:
            1. Click "Add group", and then search for and select the Azure AD group. Assign a role (like "**Virtual Machine Administrator Login**") and set the type as "Azure AD group". Click "Save".



Add role assignment ...

Selected role Virtual Machine Administrator Login

Assign access to
● User, group, or service principal
○ Managed identity

Members + Select members

Name	Object ID	Type
Dorin Huseras	b86bb32c-1e9a-4aa5-af4e-b985061fa066	User

5. Restart the VM
6. SSH Using AAD Credentials:
    a. With the extension installed and access granted:
    b. AAD users or members of the AAD groups you've granted access to can SSH into the VM using:

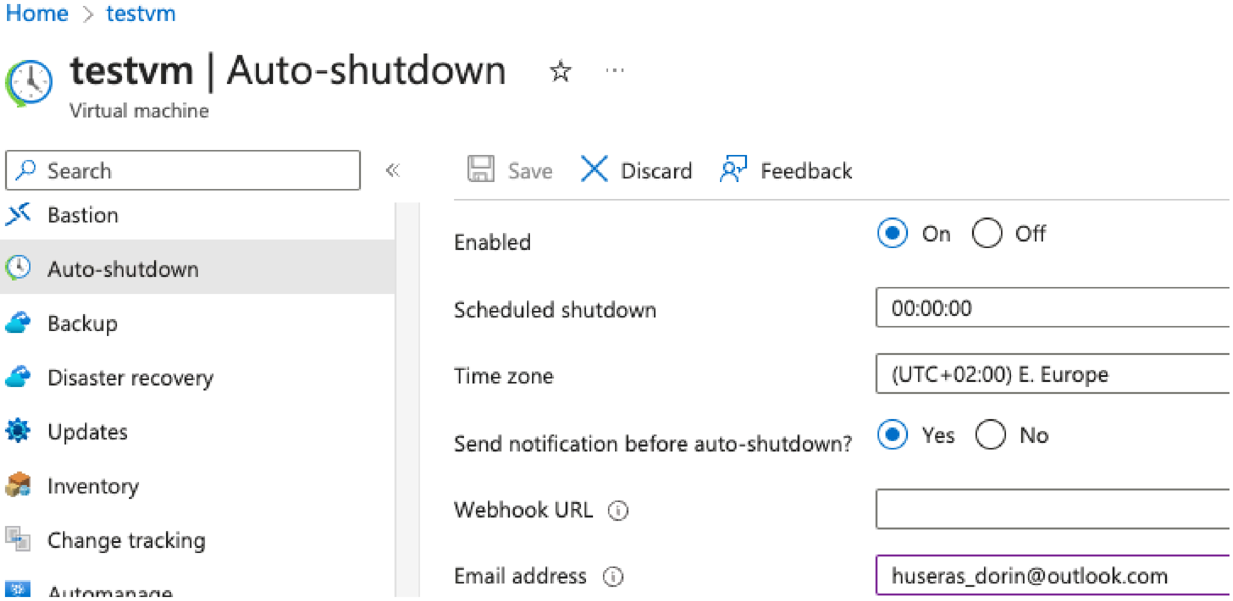
```
az login -t TENANT_ID
sudo az ssh vm --ip IP.ADR.FROM.PORTAL
```

Auto-shutdown

If the VM is still needed, Azure provides an Auto-shutdown feature for virtual machines to help manage costs and ensure you are not billed for unused resources.

1. On the Operations section for the VM, select the Auto-shutdown option.
    a. A page will open where you can configure the auto-shutdown time. Select the On option to enable and then set a time that works for you.

2. Once you have set the time, select Save at the top to enable your Auto-shutdown configuration.



Enabled ● On ○ Off

Scheduled shutdown 00:00:00

Time zone (UTC+02:00) E. Europe

Send notification before auto-shutdown? ● Yes ○ No

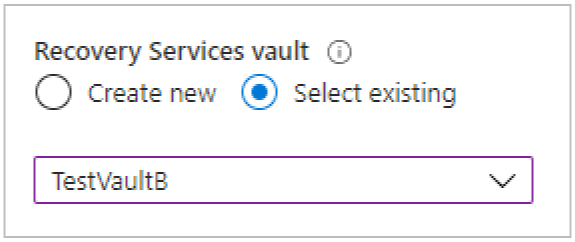
Webhook URL

Email address huseras_dorin@outlook.com

Backup an Azure VM from the VM settings

Azure Backup provides independent and isolated backups to guard against unintended destruction of the data on your VMs. Backups are stored in a Recovery Services vault with built-in management of recovery points. Configuration and scaling are simple, backups are optimized, and you can easily restore as needed. You can back up Azure VMs using a couple of methods:

1. Sign in to the Azure portal.
    a. Select all services and in the Filter, type Virtual machines, and then select Virtual machines.
    b. From the list of VMs, select the VM you want to back up.
2. On the VM menu, select Backup.
3. In Recovery Services vault, do the following:
    a. If you already have a vault, select Select existing, and select a vault.
    b. If you don't have a vault, select Create new. Specify a name for the vault. It's created in the same region and resource group as the VM. You can't modify these settings when you enable backup directly from the VM settings.

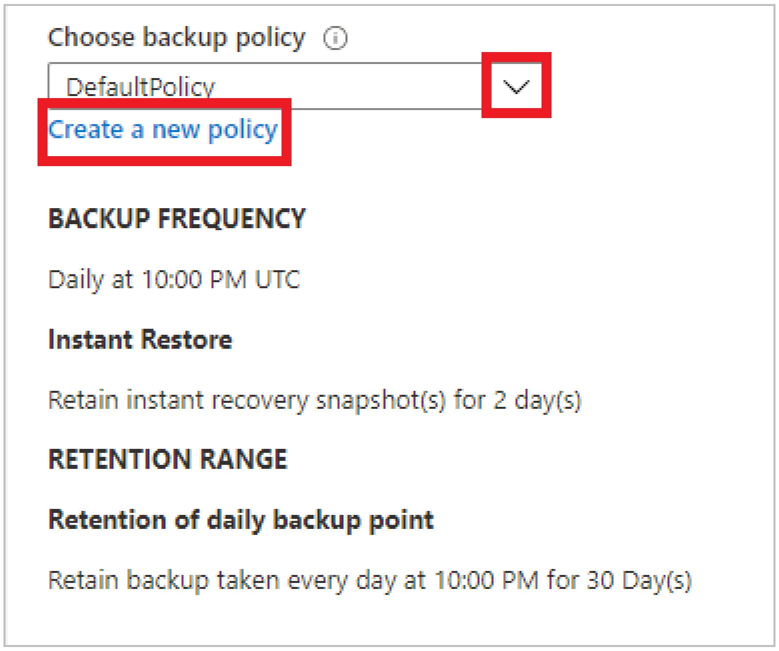


Recovery Services vault ⓘ

○ Create new ● Select existing

TestVaultB

4. In Choose backup policy, do one of the following:
   a. Leave the default policy. This backs up the VM once a day at the time specified, and retains backups in the vault for 30 days.
   b. Select an existing backup policy if you have one.
   c. Create a new policy, and define the policy settings.



Choose backup policy ⓘ

DefaultPolicy

Create a new policy

BACKUP FREQUENCY

Daily at 10:00 PM UTC

Instant Restore

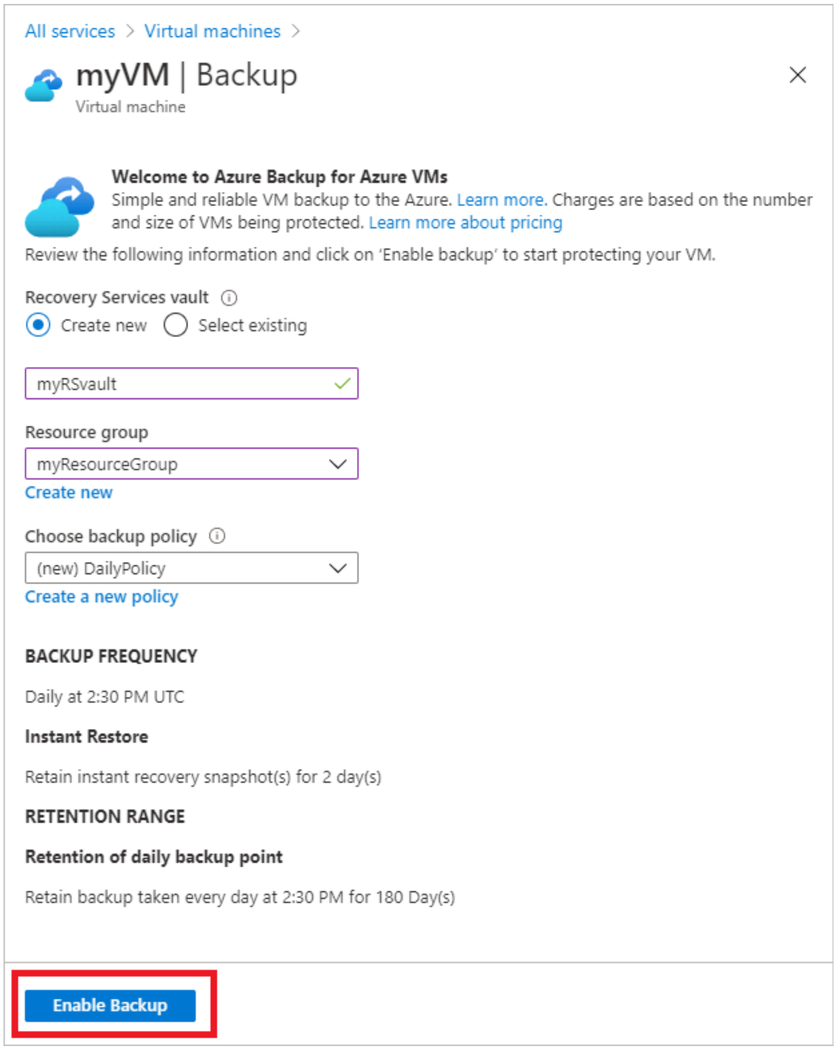
Retain instant recovery snapshot(s) for 2 day(s)

RETENTION RANGE

Retention of daily backup point

Retain backup taken every day at 10:00 PM for 30 Day(s)

5. Select Enable Backup. This associates the backup policy with the VM.



myVM | Backup

Virtual machine

Welcome to Azure Backup for Azure VMs

Simple and reliable VM backup to the Azure. Learn more. Charges are based on the number and size of VMs being protected. Learn more about pricing

Review the following information and click on 'Enable backup' to start protecting your VM.

Recovery Services vault

● Create new ○ Select existing

myRSvault ✓

Resource group

myResourceGroup

Choose backup policy

(new) DailyPolicy

BACKUP FREQUENCY

Daily at 2:30 PM UTC

Instant Restore

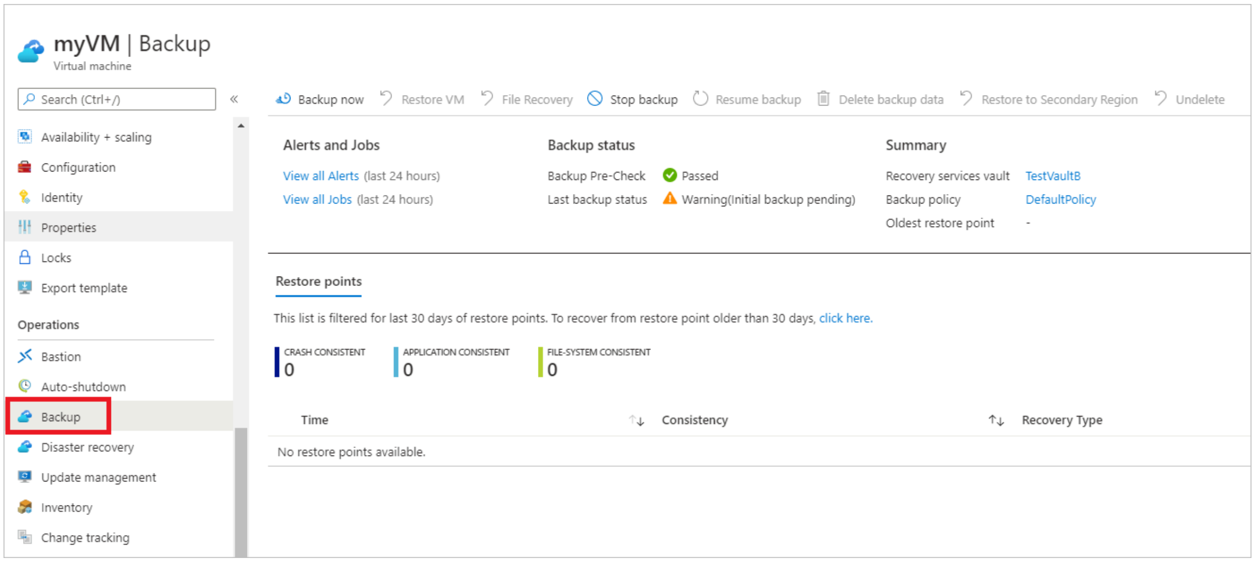
Retain instant recovery snapshot(s) for 2 day(s)

RETENTION RANGE

Retention of daily backup point

Retain backup taken every day at 2:30 PM for 180 Day(s)

6. You can track the configuration progress in the portal notifications.
7. After the job completes, in the VM menu, select Backup. The page shows backup status for the VM, information about recovery points, jobs running, and alerts issued.



Alerts and Jobs

View all Alerts (last 24 hours)
View all Jobs (last 24 hours)

Backup status

Backup Pre-Check ✓ Passed
Last backup status ⚠ Warning(Initial backup pending)

Summary

Recovery services vault TestVaultB
Backup policy DefaultPolicy
Oldest restore point -

Restore points

This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, click here.

CRASH CONSISTENT 0
APPLICATION CONSISTENT 0
FILE-SYSTEM CONSISTENT 0

Time	Consistency	Recovery Type
No restore points available.		

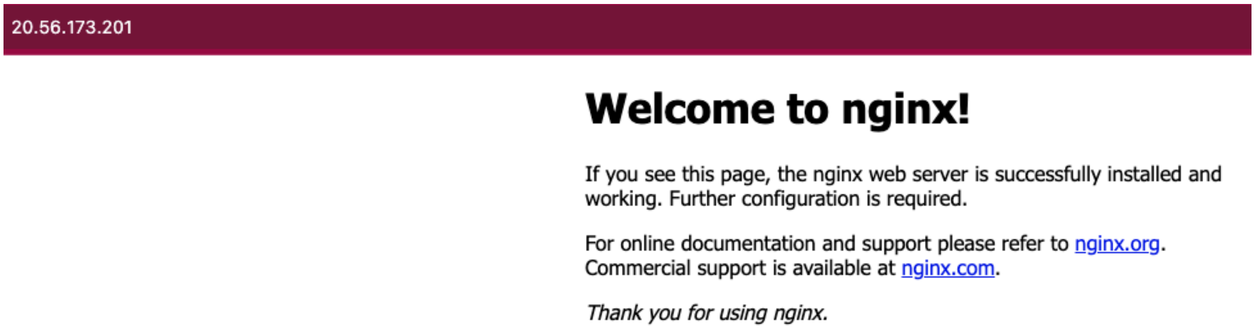
8. After enabling backup, an initial backup will run. You can start the initial backup immediately or wait until it starts in accordance with the backup schedule.
   a. Until the initial backup completes, the Last backup status shows as Warning (Initial backup pending).
   b. To see when the next scheduled backup will run, select the backup policy name.

Install a Web server

1. To see your VM in action, install the NGINX web server. From your SSH session, update your package sources and then install the latest NGINX package.

```
sudo apt-get -y update
sudo apt-get -y install nginx
```

2. When done, type exit to leave the SSH session.
3. View the web server in action
   a. Use a web browser of your choice to view the default NGINX welcome page. Type the public IP address of the VM as the web address. The public IP address can be found on the VM overview page or as part of the SSH connection string you used earlier.



20.56.173.201

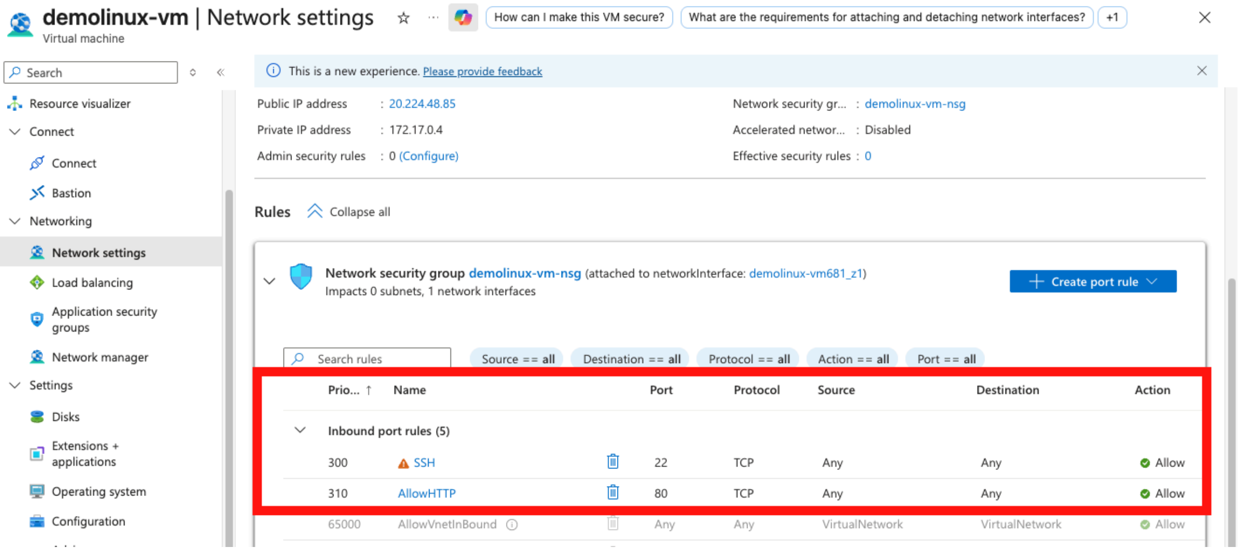
Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

9. Make sure you allow access to port 80 from the internet.



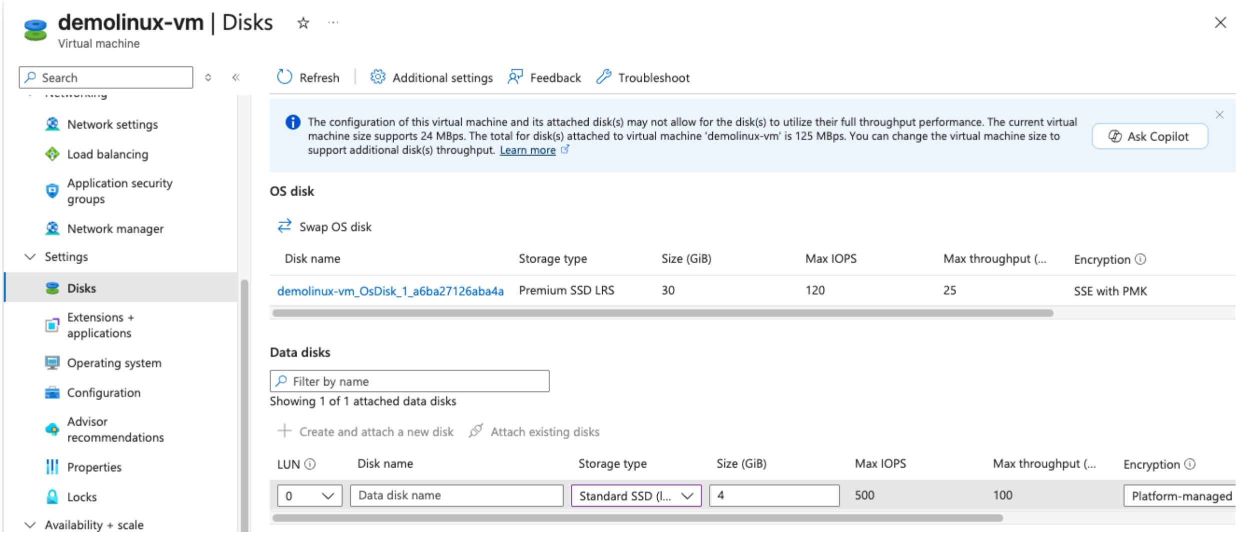
Public IP address : 20.224.48.85
Private IP address : 172.17.0.4
Admin security rules : 0 (Configure)
Network security gr... : demolinux-vm-nsg
Accelerated networ... : Disabled
Effective security rules : 0

Network security group demolinux-vm-nsg (attached to networkInterface: demolinux-vm681_z1)
Impacts 0 subnets, 1 network interfaces

Prio... ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (5)						
300	⚠ SSH	22	TCP	Any	Any	✓ Allow
310	AllowHTTP	80	TCP	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow

Create and attach a data disk

1. Go to your VM
    a. In the Azure Portal, open Virtual Machines.
    b. Select the Linux VM where you want to attach the disk.
2. Open the Disks blade
    a. In the VM’s menu (left-hand side), click Disks.
3. Add a data disk
    a. Click + Add data disk.
    b. You now have two options:
    c. Create disk → Azure will let you create a new managed disk (you choose size, performance tier, etc.).
    d. Attach existing disk → pick one of your already-created managed disks.
4. Save changes
    a. After choosing/creating the disk, click Save at the top.
    b. Azure will hot-attach the disk to your VM.



demolinux-vm | Disks

Virtual machine

The configuration of this virtual machine and its attached disk(s) may not allow for the disk(s) to utilize their full throughput performance. The current virtual machine size supports 24 MBps. The total for disk(s) attached to virtual machine 'demolinux-vm' is 125 MBps. You can change the virtual machine size to support additional disk(s) throughput. Learn more

OS disk

Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption ⓘ
demolinux-vm_OsDisk_1_a6ba27126aba4a	Premium SSD LRS	30	120	25	SSE with PMK

Data disks

Filter by name

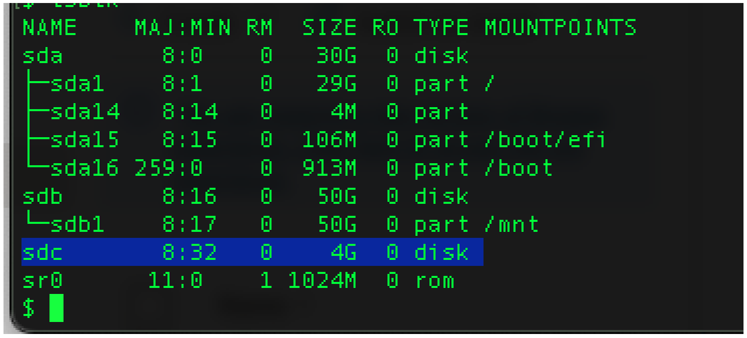
Showing 1 of 1 attached data disks

LUN ⓘ	Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption ⓘ
0	Data disk name	Standard SSD (l...	4	500	100	Platform-managed

Mount the disk

1. SSH into your VM.
2. Run:

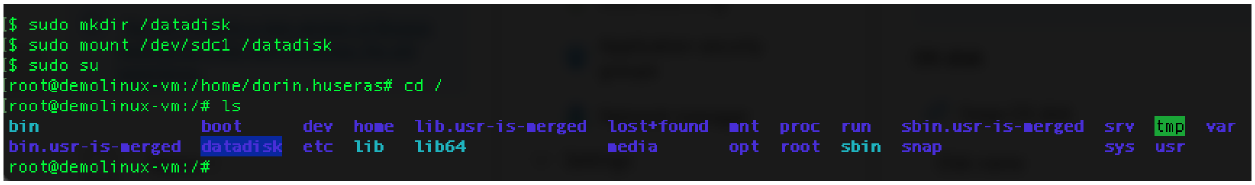
```
lsblk
```



```
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda       8:0    0   30G  0 disk
├─sda1    8:1    0   29G  0 part /
├─sda14   8:14   0    4M  0 part
├─sda15   8:15   0  106M  0 part /boot/efi
└─sda16 259:0    0  913M  0 part /boot
sdb       8:16   0   50G  0 disk
└─sdb1    8:17   0   50G  0 part /mnt
sdc       8:32   0    4G  0 disk
sr0      11:0    1 1024M  0 rom
$ 
```

   a. → You'll see the new disk (likely /dev/sdc).
3. Partition & format:

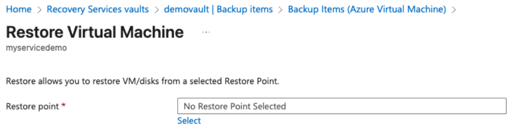
```
sudo fdisk /dev/sdc
    - When inside fdisk /dev/sdc:
    - Press n → new partition
    - Choose p (primary).
    - Partition number: 1.
    - First sector: press Enter (default).
    - Last sector: press Enter (use entire disk).
    - Press w → write changes and exit.
sudo mkfs -t ext4 /dev/sdc1

sudo mkdir /datadisk
sudo mount /dev/sdc1 /datadisk

#check it out
df -h | grep datadisk
```



```
$ sudo mkdir /datadisk
$ sudo mount /dev/sdc1 /datadisk
$ sudo su
root@demolinux-vm:/home/dorin.huseras# cd /
root@demolinux-vm:/# ls
bin                boot      dev  home  lib.usr-is-merged  lost+found  mnt  proc  run   sbin.usr-is-merged  srv  tmp  var
bin.usr-is-merged  datadisk  etc  lib   lib64              media       opt  root  sbin  snap                sys  usr
root@demolinux-vm:/#
```

Restore from backup

1. Go to Recovery Services vaults → select the vault where your VM is backed up.
2. In the left menu, click Backup items → Azure Virtual Machine.
3. Find and click your VM.
4. Click Restore VM.
5. Choose a restore point (date/time snapshot).
6. Choose a restore type:
    a. Create new VM → Azure deploys a brand-new VM from the backup.
    b. Replace existing → overwrites the current VM (careful, this will stop the existing VM).
7. Pick the resource group, network, and storage settings for the restore.
8. Click **Restore**.



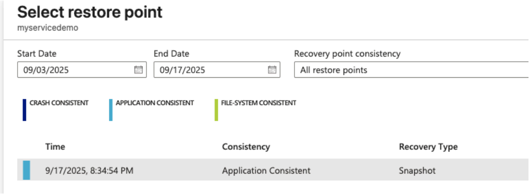
Home > Recovery Services vaults > demovault | Backup items > Backup Items (Azure Virtual Machine) >

Restore Virtual Machine ...

myservicedemo

Restore allows you to restore VM/disks from a selected Restore Point.

Restore point * No Restore Point Selected



Select restore point

myservicedemo

Start Date 09/03/2025

End Date 09/17/2025

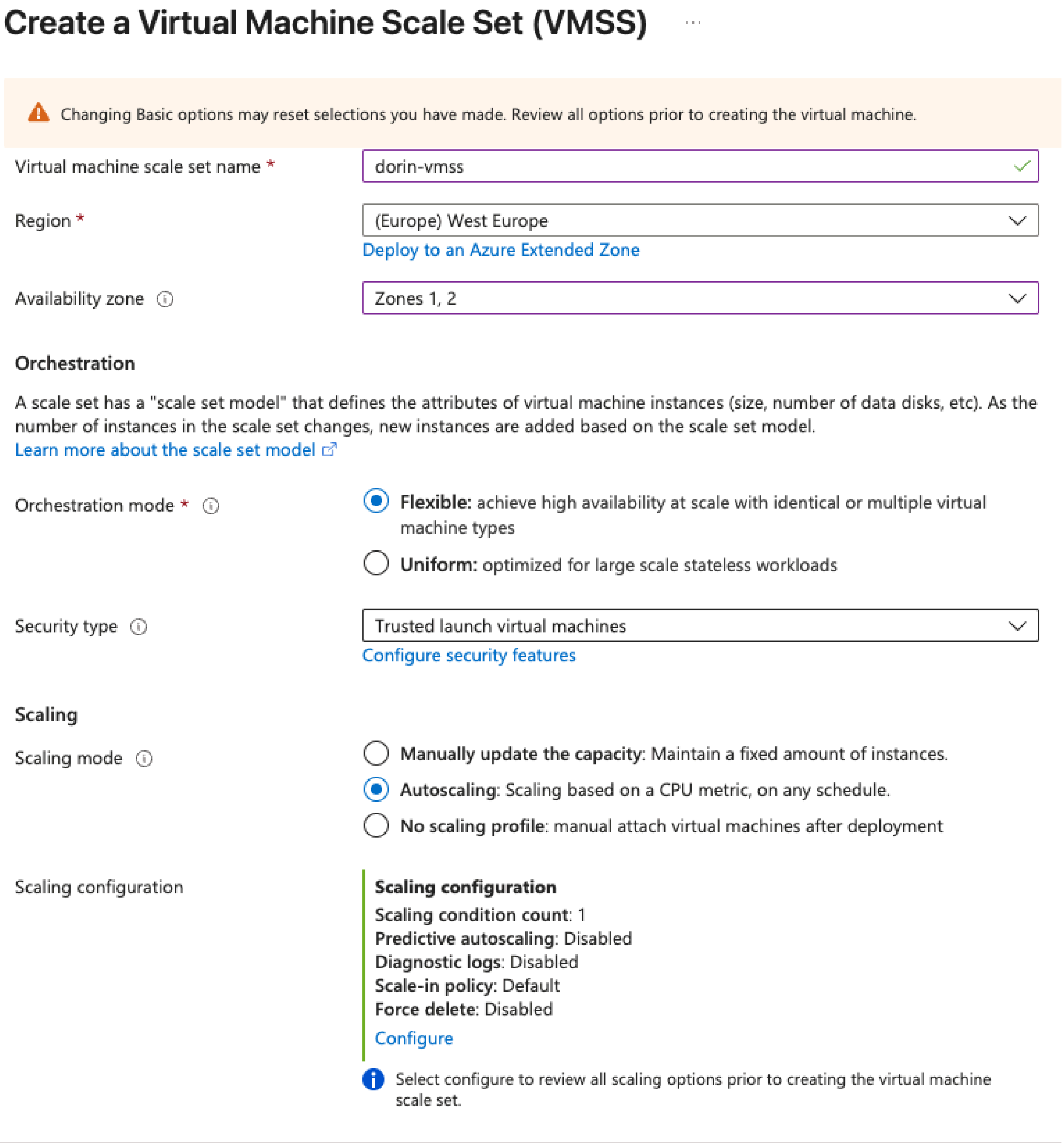
Recovery point consistency All restore points

Time	Consistency	Recovery Type
9/17/2025, 8:34:54 PM	Application Consistent	Snapshot

Create Virtual Machine Scale Set

1. Go to Azure Portal → Virtual Machine Scale Sets → + Create.
2. Basics tab:
    a. Subscription: select your subscription.
    b. Resource group: create new → rg-vmss-demo.
    c. Scale set name: vmss-demo.

d. Region: West Europe.
e. Availability zone: Zones 1, 2.
f. Orchestration mode: Flexible.
g. Security type: Trusted launch virtual machines.
h. Scaling: choose Autoscaling.



Create a Virtual Machine Scale Set (VMSS) ...

⚠ Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

Virtual machine scale set name * dorin-vmss ✓

Region * (Europe) West Europe
Deploy to an Azure Extended Zone

Availability zone ⓘ Zones 1, 2

Orchestration

A scale set has a "scale set model" that defines the attributes of virtual machine instances (size, number of data disks, etc). As the number of instances in the scale set changes, new instances are added based on the scale set model.
Learn more about the scale set model

Orchestration mode * ⓘ
● **Flexible:** achieve high availability at scale with identical or multiple virtual machine types
○ **Uniform:** optimized for large scale stateless workloads

Security type ⓘ Trusted launch virtual machines
Configure security features

Scaling

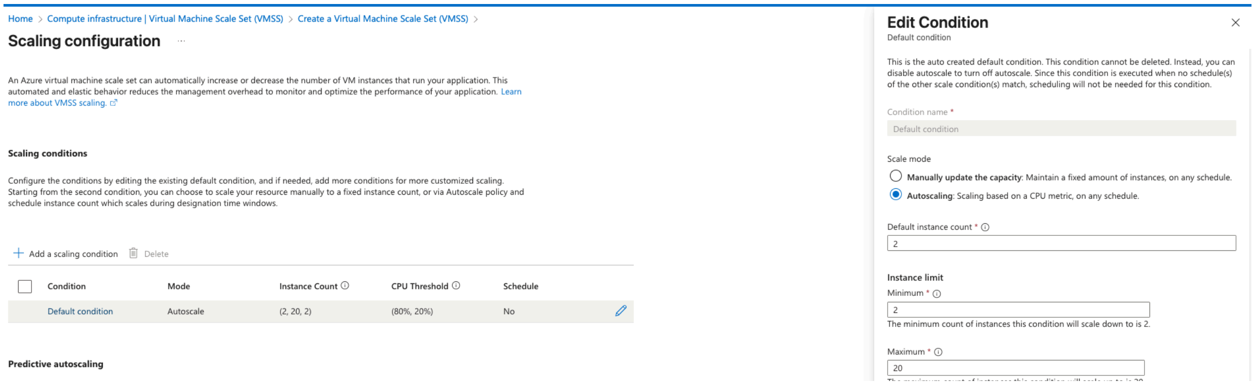
Scaling mode ⓘ
○ **Manually update the capacity**: Maintain a fixed amount of instances.
● **Autoscaling**: Scaling based on a CPU metric, on any schedule.
○ **No scaling profile**: manual attach virtual machines after deployment

Scaling configuration
Scaling configuration
Scaling condition count: 1
Predictive autoscaling: Disabled
Diagnostic logs: Disabled
Scale-in policy: Default
Force delete: Disabled
Configure

ⓘ Select configure to review all scaling options prior to creating the virtual machine scale set.

3. Set scaling configuration
   a. Default instance count: 2. (Start with 2 VMs running.)

    b. Minimum instances: 2. (Never go below 2 for availability.)
    c. Maximum instances: 20. (Scale out to handle heavy traffic.)
    d. Scale out rule: Add 1 VM if CPU > 80%. (More servers when traffic is high.)
    e. Scale in rule: Remove 1 VM if CPU < 20%. (Save costs when traffic is low.)
    f. Scale-in policy: Default (balances across zones). (Removes the “safest” VM first.)



Home > Compute infrastructure | Virtual Machine Scale Set (VMSS) > Create a Virtual Machine Scale Set (VMSS) >

Scaling configuration ···

An Azure virtual machine scale set can automatically increase or decrease the number of VM instances that run your application. This automated and elastic behavior reduces the management overhead to monitor and optimize the performance of your application. Learn more about VMSS scaling.

Scaling conditions

Configure the conditions by editing the existing default condition, and if needed, add more conditions for more customized scaling. Starting from the second condition, you can choose to scale your resource manually to a fixed instance count, or via Autoscale policy and schedule instance count which scales during designation time windows.

+ Add a scaling condition   Delete

□	Condition	Mode	Instance Count	CPU Threshold	Schedule
	Default condition	Autoscale	(2, 20, 2)	(80%, 20%)	No

Predictive autoscaling

Edit Condition

Default condition

This is the auto created default condition. This condition cannot be deleted. Instead, you can disable autoscale to turn off autoscale. Since this condition is executed when no schedule(s) of the other scale condition(s) match, scheduling will not be needed for this condition.

Condition name *: Default condition

Scale mode

○ **Manually update the capacity**: Maintain a fixed amount of instances, on any schedule.

● **Autoscaling**: Scaling based on a CPU metric, on any schedule.

Default instance count *: 2

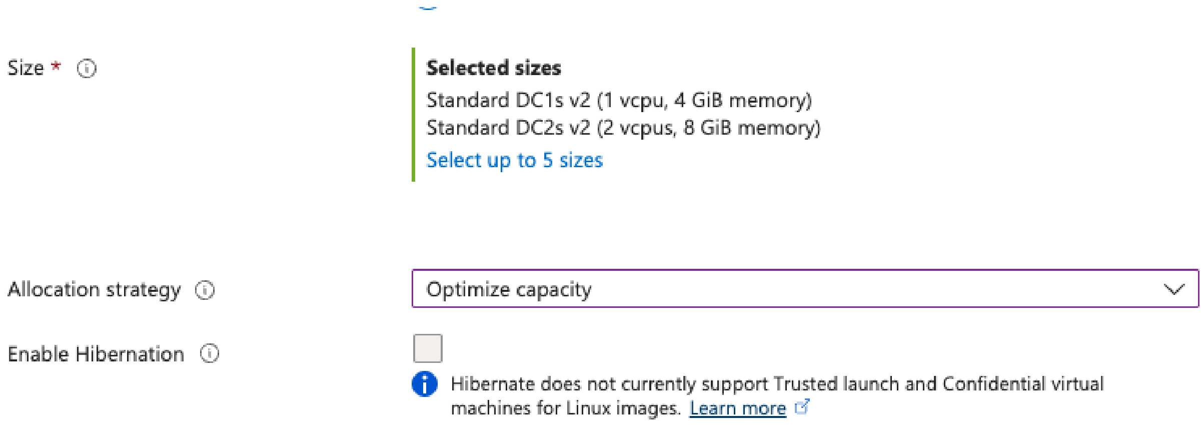
Instance limit

Minimum *: 2

The minimum count of instances this condition will scale down to is 2.

Maximum *: 20

4. Image: Ubuntu Server 24.04 LTS (x64). (OS template used for all VMs.)
5. VM size: Standard_B2s (or DC1s). (Defines CPU + RAM per VM.)
6. Authentication type: SSH public key. (Secure login method for Linux VMs.)
    a. Username: azureuser. (Default admin account on the VM.)
7. Disks: Only OS disk. (No extra data disks, keeps it simple.)
8. Spot instances: Disabled. (Prevents random eviction — ensures stability.)



Size *

Selected sizes

Standard DC1s v2 (1 vcpu, 4 GiB memory)

Standard DC2s v2 (2 vcpus, 8 GiB memory)

Select up to 5 sizes

Allocation strategy: Optimize capacity

Enable Hibernation: □

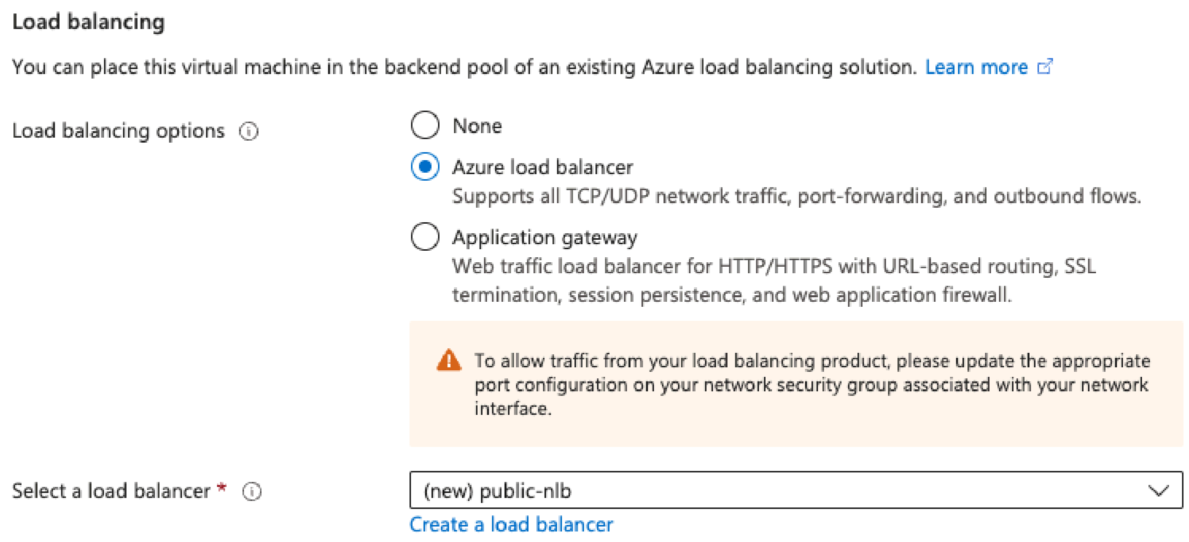
Hibernate does not currently support Trusted launch and Confidential virtual machines for Linux images. Learn more

9. A network load balancer is required
    a. Without a load balancer, every VM in your scale set would need its own public IP. With autoscaling, new VMs get created and deleted — meaning their IPs keep changing. That makes it almost impossible for clients to know *where* to connect.
    b. The load balancer makes sure requests are spread across all available VMs (round robin or by rules). This prevents one VM from being overloaded while others sit idle.

c. Load balancing options: Azure Load Balancer. (Distributes traffic across VM instances.)

d. Select load balancer: Create new → lb-vmss-demo. (Load balancer resource to manage traffic.)

e. This ensures all VM instances are reachable through one public IP.



Load balancing

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

Load balancing options
○ None
● Azure load balancer
Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.
○ Application gateway
Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.

⚠ To allow traffic from your load balancing product, please update the appropriate port configuration on your network security group associated with your network interface.

Select a load balancer * : (new) public-nlb

Create a load balancer

10. Advanced – Add Cloud-init

a. In Advanced tab → Custom data, paste the provided #cloud-config.

b. What it does:

i. Installs nginx, nodejs, npm.

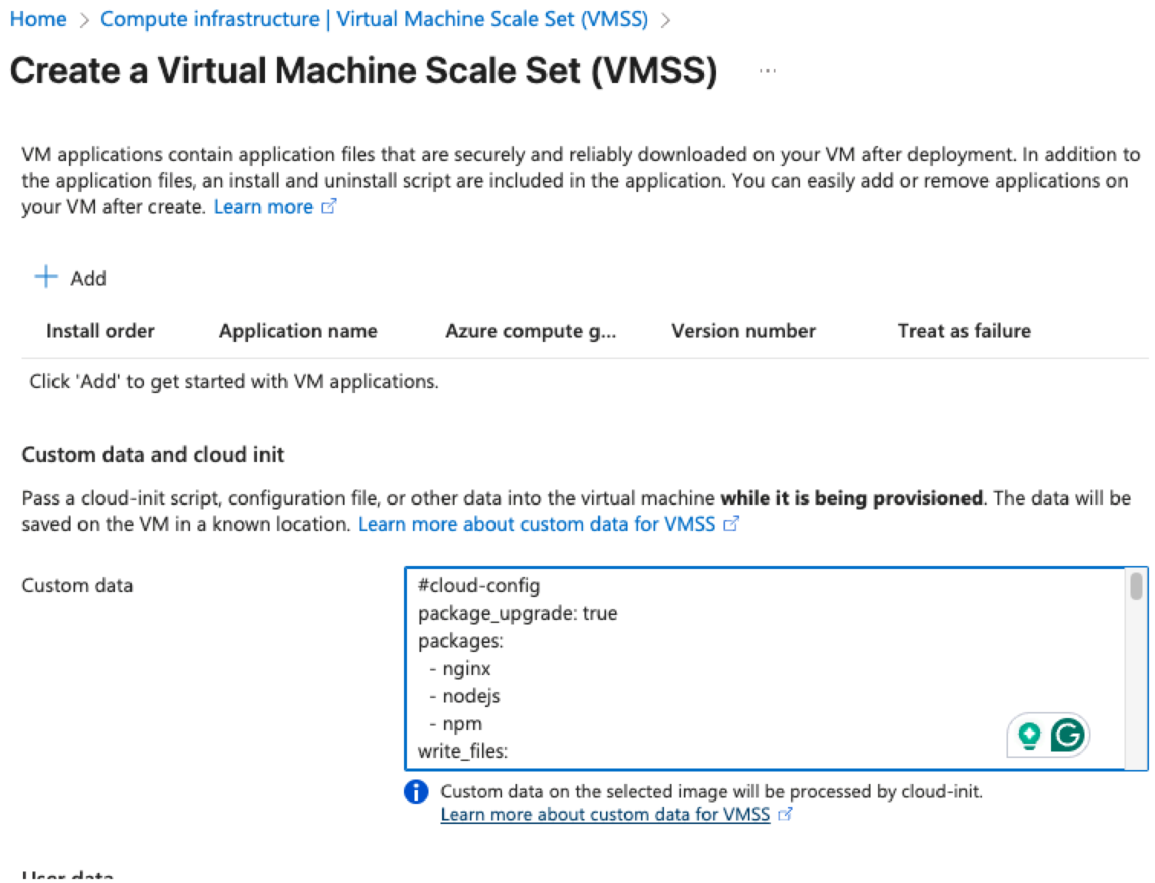
ii. Configures Nginx as a reverse proxy to forward traffic to Node.js.

iii. Creates a simple Node.js Express app.

iv. Starts the app automatically.

c. This means every new VM in the scale set configures itself at boot.

```
#cloud-config
package_upgrade: true
packages:
  - nginx
  - nodejs
  - npm
write_files:
  - owner: www-data:www-data
    path: /etc/nginx/sites-available/default
    defer: true
    content: |
      server {
        listen 80;
        location / {
          proxy_pass http://localhost:3000;
          proxy_http_version 1.1;
          proxy_set_header Upgrade $http_upgrade;
          proxy_set_header Connection keep-alive;
          proxy_set_header Host $host;
          proxy_cache_bypass $http_upgrade;
        }
      }
  - owner: azureuser:azureuser
    path: /home/azureuser/myapp/index.js
    defer: true
    content: |
      var express = require('express')
      var app = express()
      var os = require('os');
      app.get('/', function (req, res) {
        res.send('Hello World from host ' + os.hostname() + '!')
      })
      app.listen(3000, function () {
        console.log('Hello world app listening on port 3000!')
      })
runcmd:
  - service nginx restart
  - cd "/home/azureuser/myapp"
  - npm init
  - npm install express -y
  - nodejs index.js
```



Home > Compute infrastructure | Virtual Machine Scale Set (VMSS) >

Create a Virtual Machine Scale Set (VMSS) ...

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

Install order	Application name	Azure compute g...	Version number	Treat as failure
Click 'Add' to get started with VM applications.				

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 VMSS

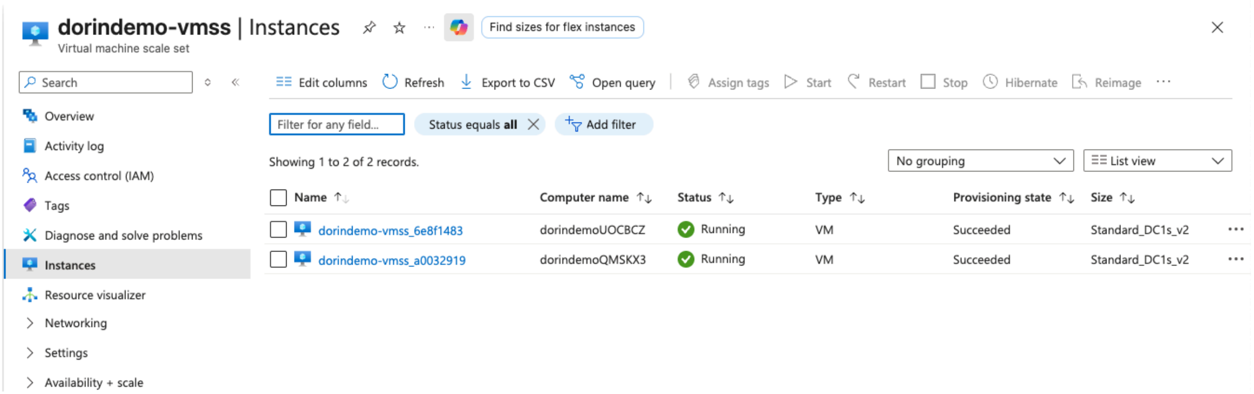
Custom data

```
#cloud-config
package_upgrade: true
packages:
  - nginx
  - nodejs
  - npm
write_files:
```

Custom data on the selected image will be processed by cloud-init.
Learn more about custom data for VMSS

User data

11. Review + Create
    a. Review settings. (Azure validates config, estimates cost.)
    b. Click Create. (Deploys VMSS, load balancer, scaling rules, and VMs.)

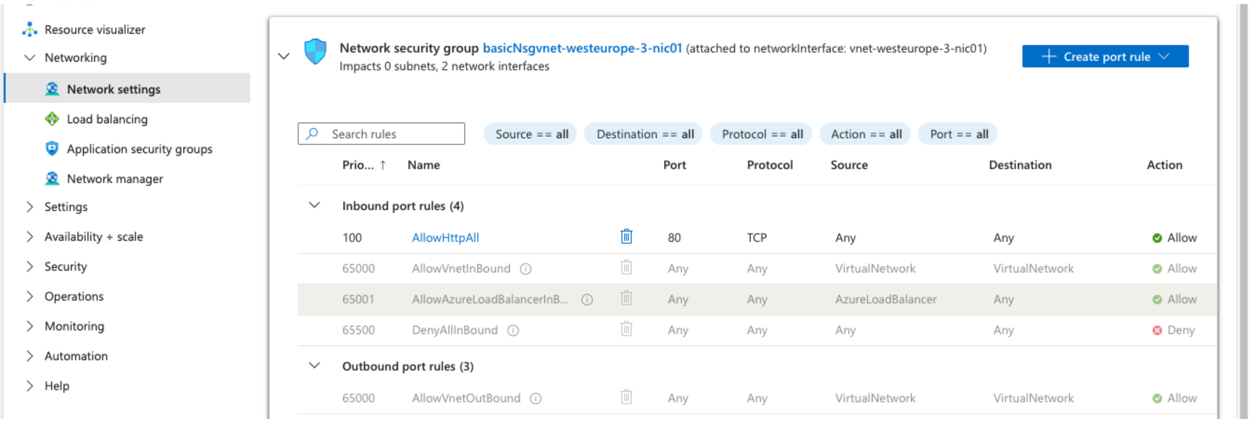


Showing 1 to 2 of 2 records.

Name	Computer name	Status	Type	Provisioning state	Size
dorindemo-vmss_6e8f1483	dorindemoUOCBCZ	Running	VM	Succeeded	Standard_DC1s_v2
dorindemo-vmss_a0032919	dorindemoQMSKX3	Running	VM	Succeeded	Standard_DC1s_v2

Test VMSS scaling capability

1. Allow HTTP traffic
    a. In the Azure Portal, go to your VMSS → Networking → Inbound port rules.
    b. Add a rule to allow TCP/80 (HTTP).
    c. This makes your Nginx + Node.js app accessible via the Load Balancer’s public IP.

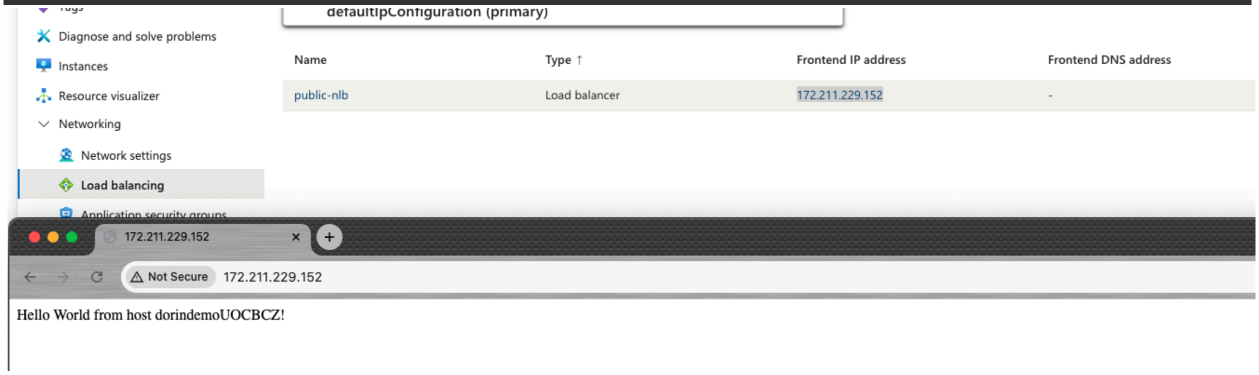


Network security group basicNsgvnet-westeurope-3-nic01 (attached to networkInterface: vnet-westeurope-3-nic01)
Impacts 0 subnets, 2 network interfaces

Prio... ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (4)						
100	AllowHttpAll	80	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound port rules (3)						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow

2. Access the application
    a. Open a web browser and go to the public IP of your Load Balancer (you can find it in the Load balancer → Overview).
    b. You should see the response from your Node.js app:

```
Hello World from host <VM-NAME>!
```


Tags
Diagnose and solve problems
Instances
Resource visualizer
Networking
Network settings
Load balancing
Application security groups
defaultIpConfiguration (primary)
Not Secure

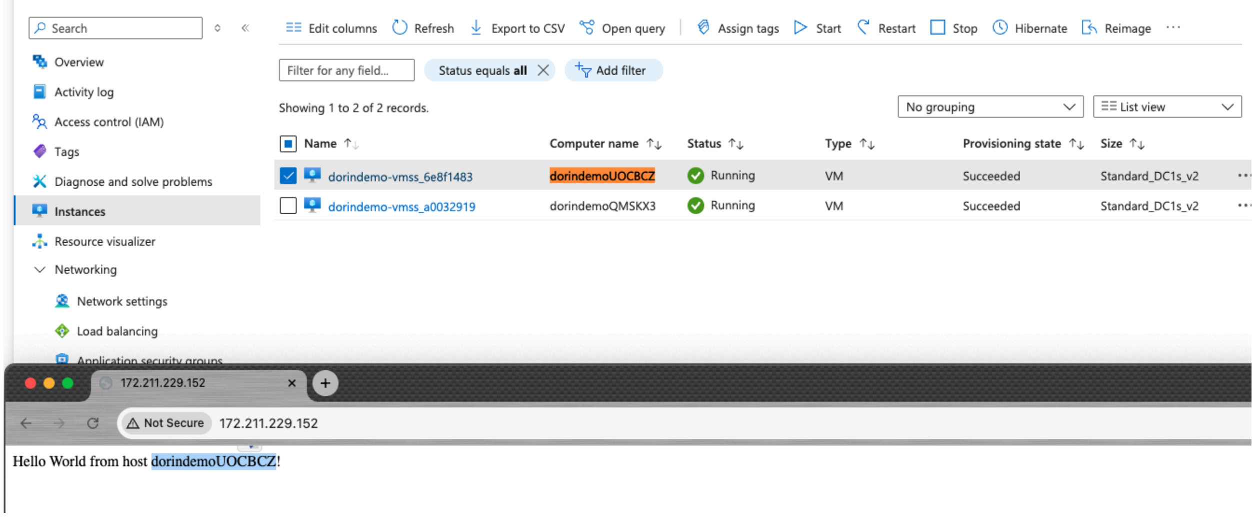
Name	Type ↑	Frontend IP address	Frontend DNS address
public-nlb	Load balancer	172.211.229.152	-

172.211.229.152

Hello World from host dorindemoUOCBCZ!

    c. Each VM will return its own hostname (that’s how you know which VM responded).
3. Simulate removing a VM
    a. From the portal, note the VM name shown in the browser.

b. Go to VMSS → Instances.
c. Select the instance with that name and delete it.



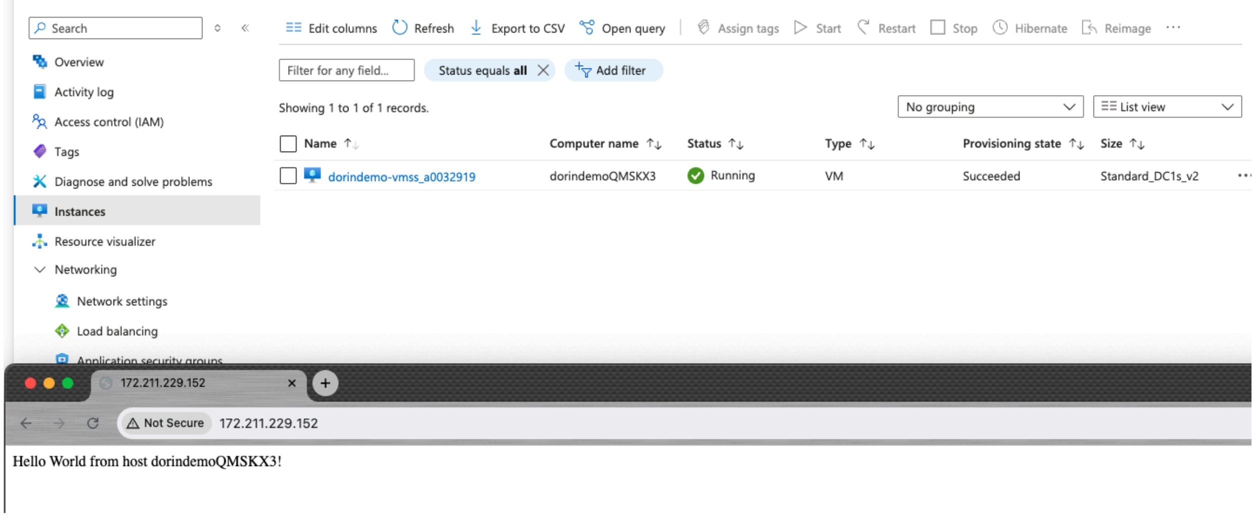
Showing 1 to 2 of 2 records.

	Name	Computer name	Status	Type	Provisioning state	Size
☑	dorindemo-vmss_6e8f1483	dorindemoUOCBCZ	Running	VM	Succeeded	Standard_DC1s_v2
☐	dorindemo-vmss_a0032919	dorindemoQMSKX3	Running	VM	Succeeded	Standard_DC1s_v2

172.211.229.152

Hello World from host dorindemoUOCBCZ!

d. Now, refresh your browser → the Load Balancer will route traffic to the other VM in the scale set, and you'll see a different hostname.



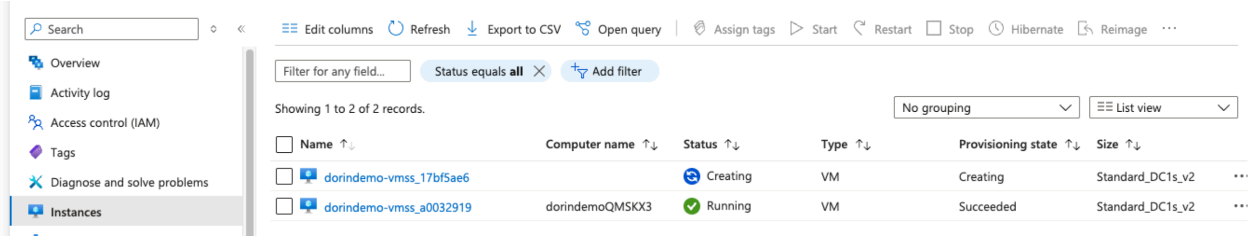
Showing 1 to 1 of 1 records.

	Name	Computer name	Status	Type	Provisioning state	Size
☐	dorindemo-vmss_a0032919	dorindemoQMSKX3	Running	VM	Succeeded	Standard_DC1s_v2

172.211.229.152

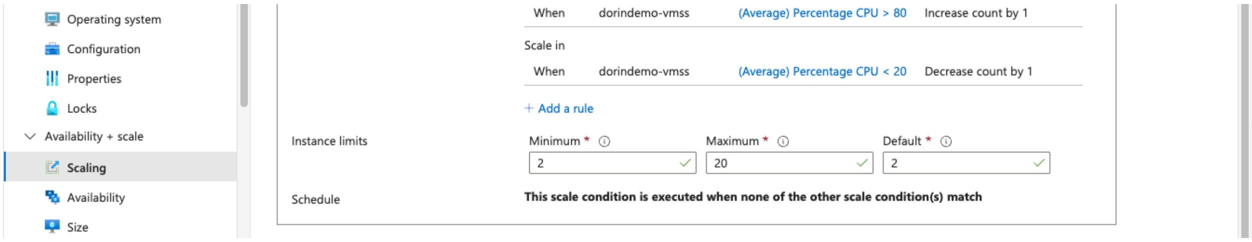
Hello World from host dorindemoQMSKX3!

4. Observe autoscaling recovery
   a. Since your minimum instance count is 2, VMSS will detect that one VM is missing.
   b. Within a few minutes, it will automatically provision a new VM instance.
   c. Refresh your browser again after a while → you'll see the new VM's hostname responding alongside the existing one.



Showing 1 to 2 of 2 records.

	Name	Computer name	Status	Type	Provisioning state	Size
☐	dorindemo-vmss_17bf5ae6		Creating	VM	Creating	Standard_DC1s_v2
☐	dorindemo-vmss_a0032919	dorindemoQMSKX3	Running	VM	Succeeded	Standard_DC1s_v2



When	dorindemo-vmss	(Average) Percentage CPU > 80	Increase count by 1

Scale in

When	dorindemo-vmss	(Average) Percentage CPU < 20	Decrease count by 1

Instance limits

Minimum *	Maximum *	Default *
2	20	2

Schedule

This scale condition is executed when none of the other scale condition(s) match