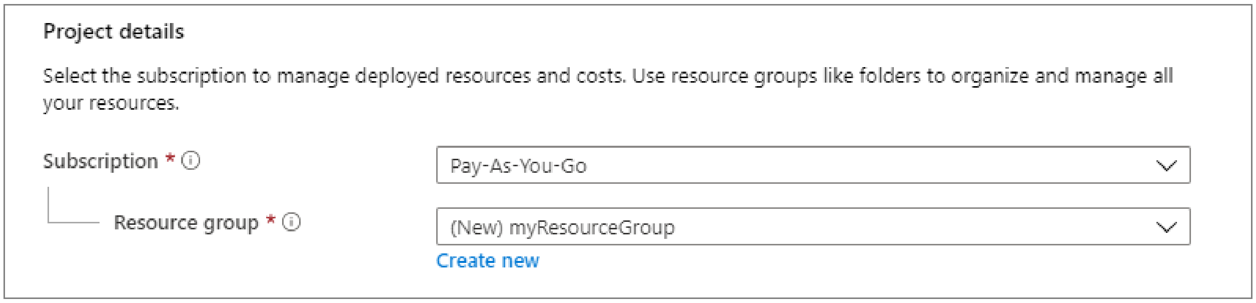
Create a Linux virtual machine in the Azure portal

1. Sign in to Azure
    a. Sign in to the Azure portal.
2. Create virtual machine
    a. Enter virtual machines in the search.
    b. Under Services, select Virtual machines.
    c. In 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 myResourceGroup for the name.*.

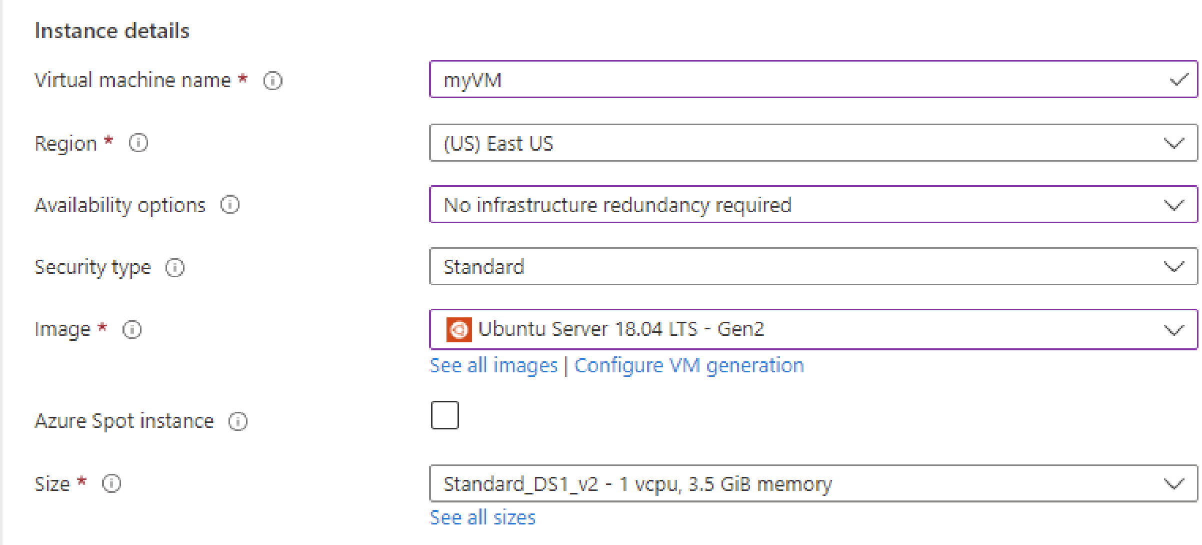


Project details

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 Create new

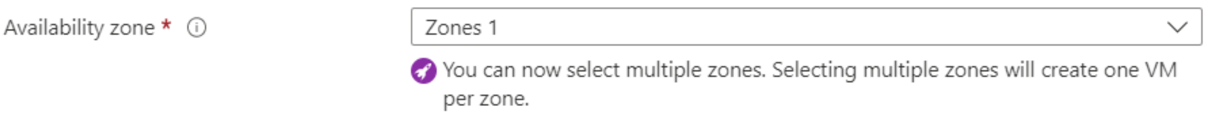
    e. Under Instance details, enter myVM for the Virtual machine name, and choose Ubuntu Server 22.04 LTS - Gen2 for your Image. Leave the other defaults. The default size and pricing is only shown as an example. Size availability and pricing are dependent on your region and subscription.



Instance details

Virtual machine name * ⓘ	myVM ✓
Region * ⓘ	(US) East US
Availability options ⓘ	No infrastructure redundancy required
Security type ⓘ	Standard
Image * ⓘ	Ubuntu Server 18.04 LTS - Gen2 See all images | Configure VM generation
Azure Spot instance ⓘ	□
Size * ⓘ	Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory See all sizes

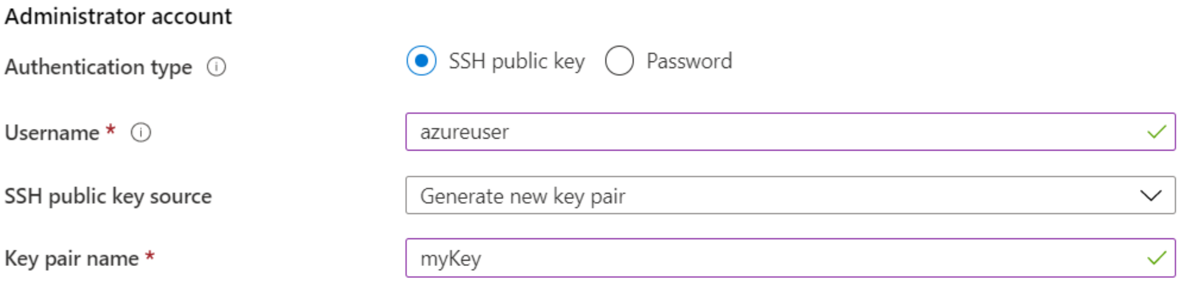
Note: Some users will now see the option to create VMs in multiple zones.



Availability zone * ⓘ Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone.

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



Administrator account

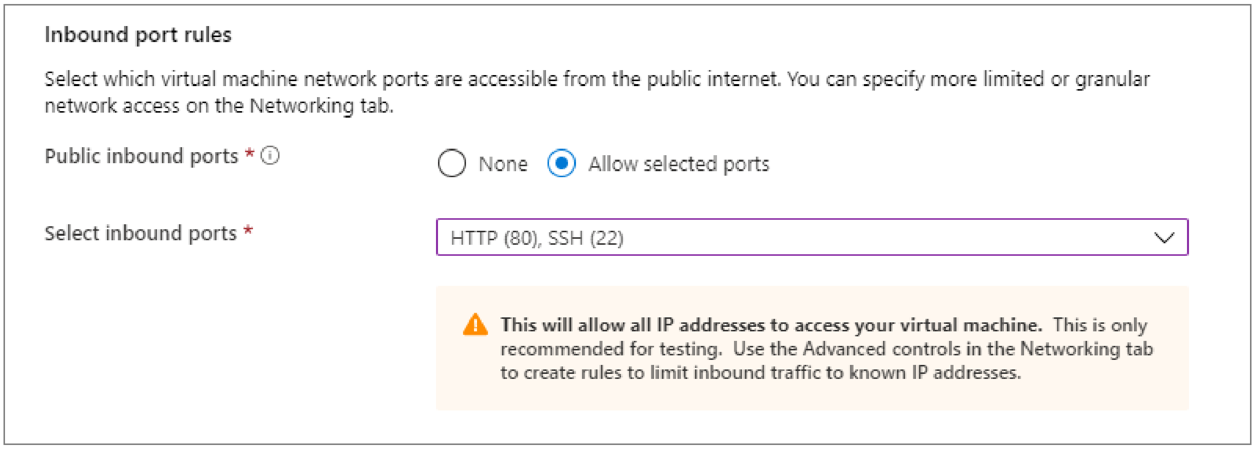
Authentication type ⓘ ● SSH public key ○ Password

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

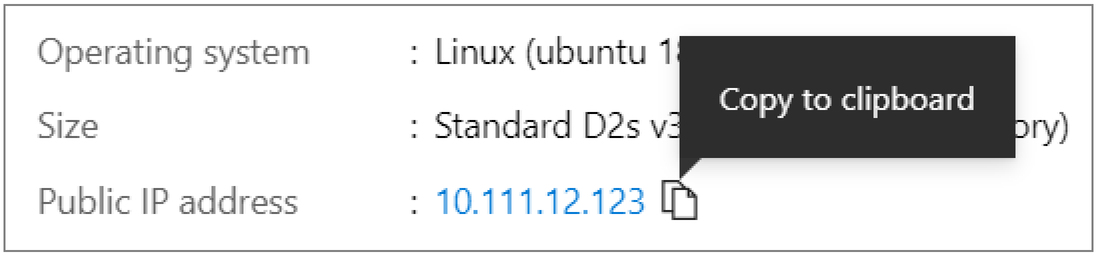
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

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 resource. Your key file will be download 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

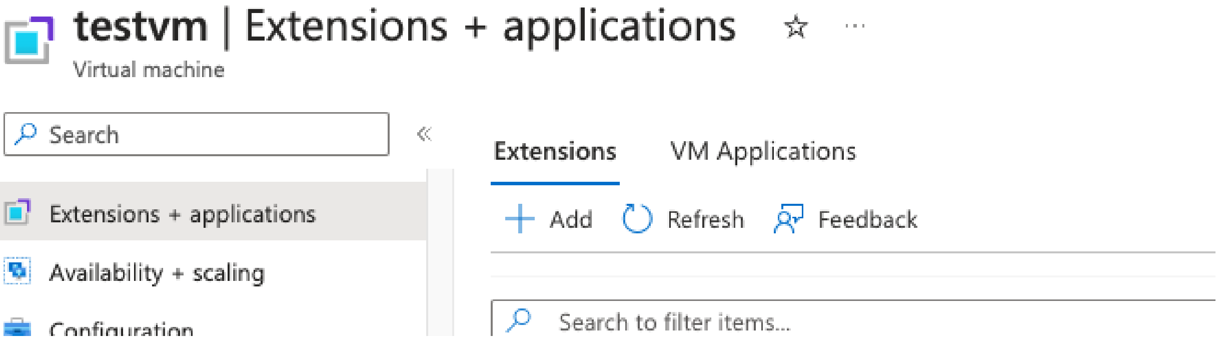
Connect to virtual machine

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**. 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.

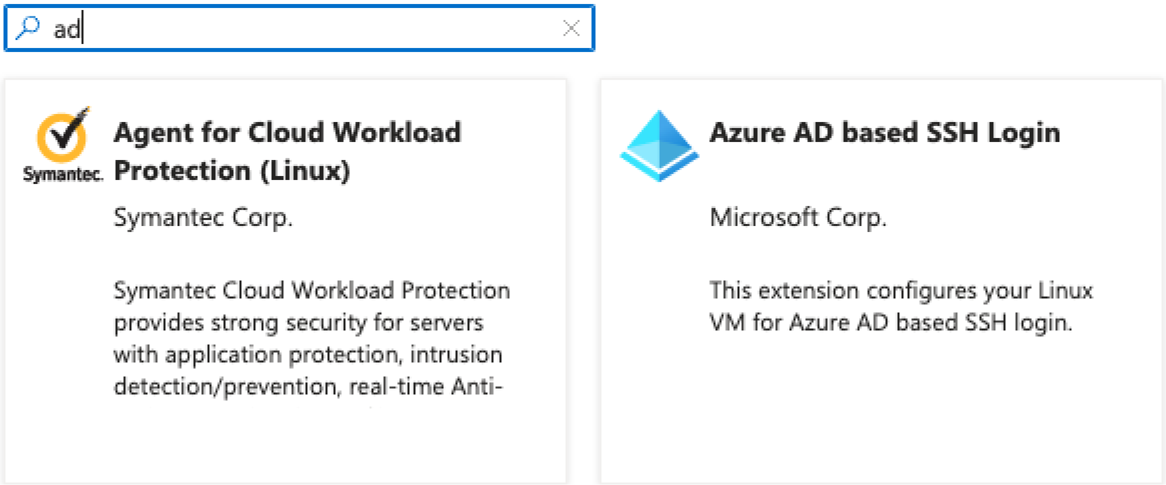
```
ssh -i ~/Downloads/myKey.pem azureuser@10.111.12.123
```

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".



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. 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 "Azure Active Directory" from the sidebar.
   c. Under "Azure AD login", you'll have options to "Add user" or "Add group".
      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".

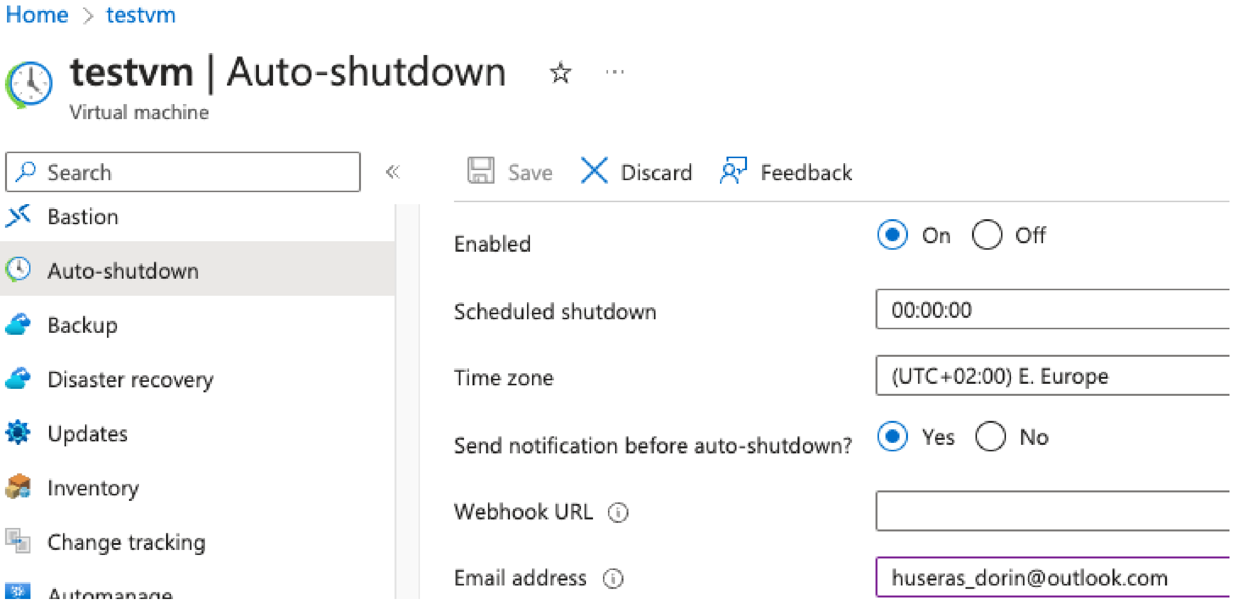
4. SSH Using AAD Credentials:
    a. With the extension installed and access granted:
    b. AAD users or members of the AAD groups you've granted access to can SSH into the VM using:

```
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

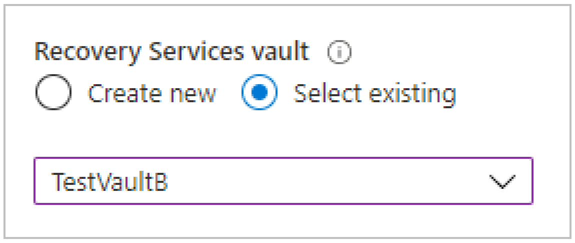
Webhook URL:

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.

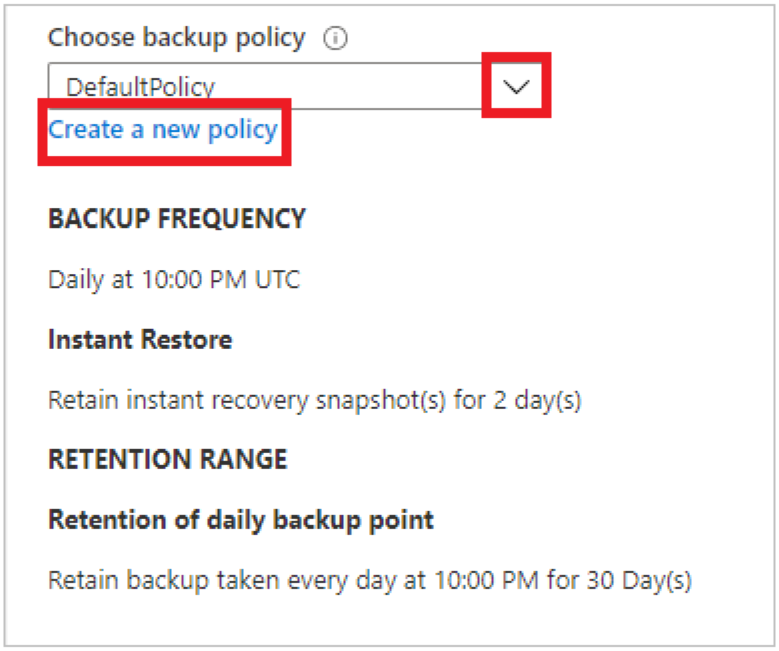


Recovery Services vault ⓘ

○ 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

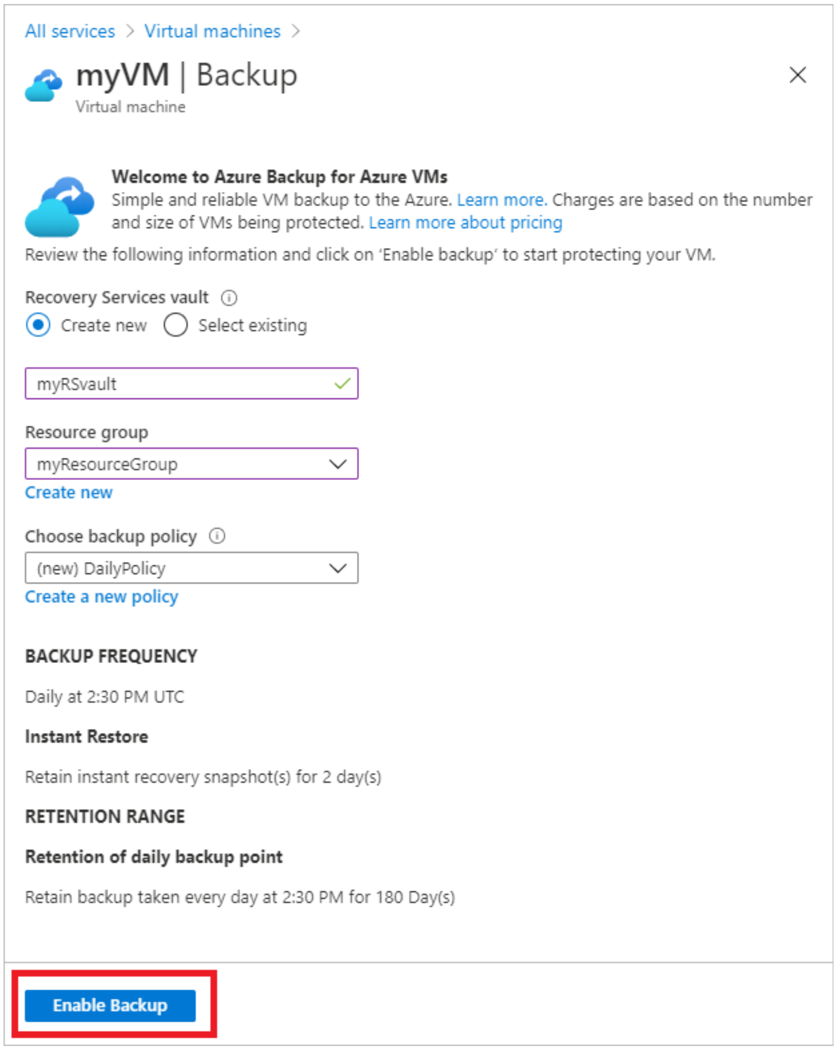
Retain instant recovery snapshot(s) for 2 day(s)

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.



All services > Virtual machines >

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

Create new

Choose backup policy

(new) DailyPolicy

Create a new policy

BACKUP FREQUENCY

Daily at 2:30 PM UTC

Instant Restore

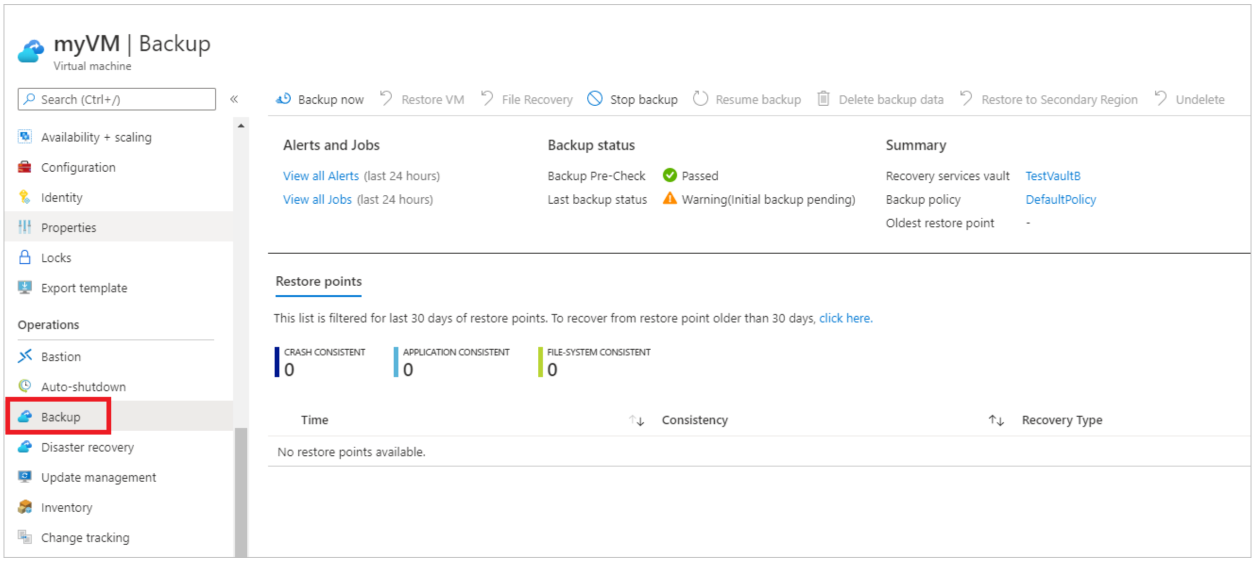
Retain instant recovery snapshot(s) for 2 day(s)

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	APPLICATION CONSISTENT	FILE-SYSTEM CONSISTENT
0	0	0

Time	Consistency	Recovery Type
No restore points available.		

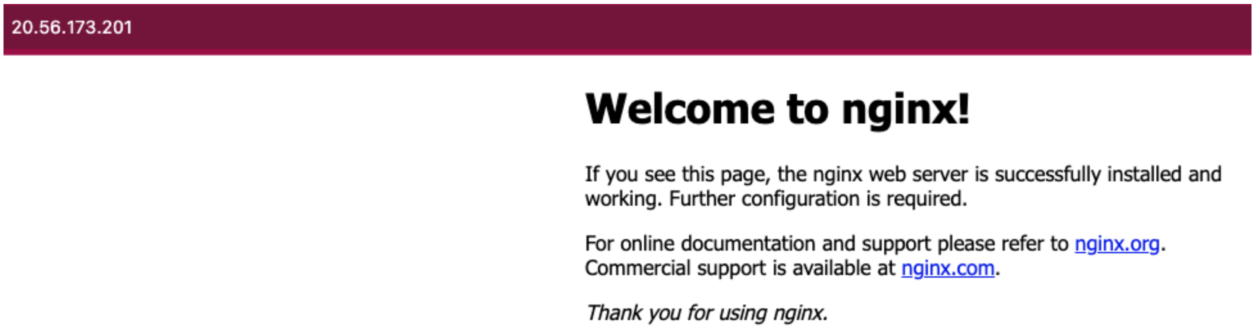
8. After enabling backup, an initial backup run. You can start the initial backup immediately, or wait until it starts in accordance with the backup schedule.
    a. Until the initial backup completes, the Last backup status shows as Warning (Initial backup pending).
    b. To see when the next scheduled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

Install 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.



Welcome to nginx!

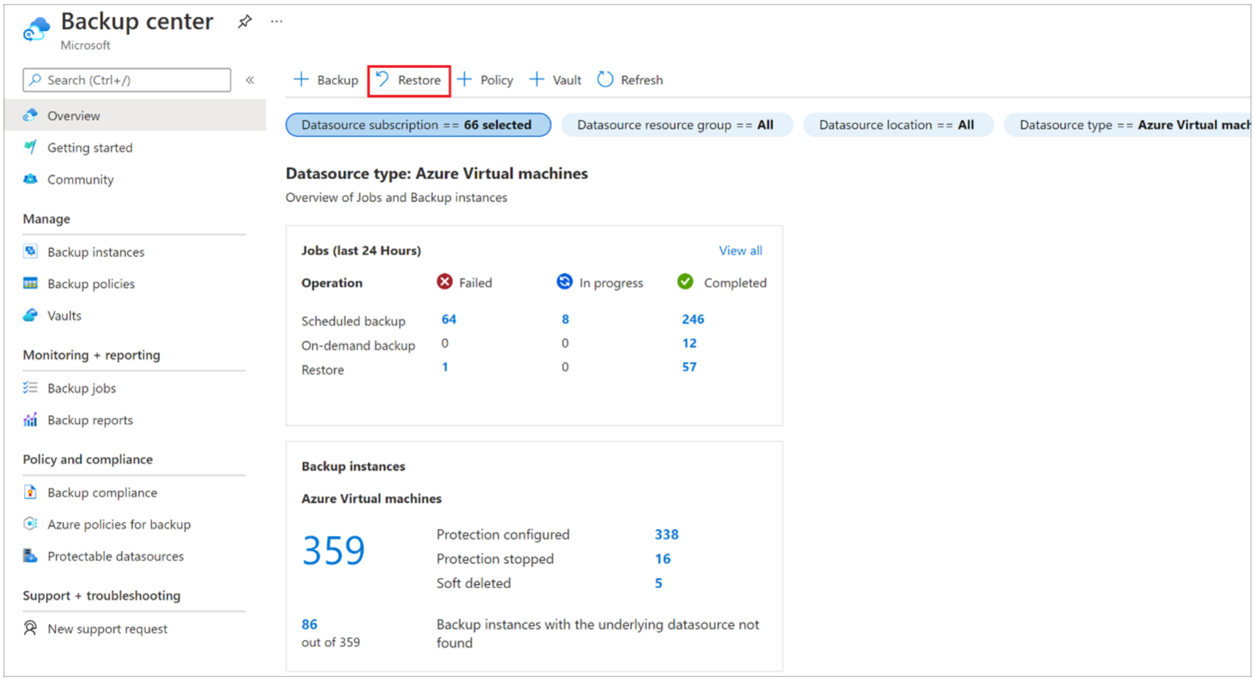
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

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

Thank you for using nginx.

Restore from back-up

1. Navigate to Backup center in the Azure portal and click Restore from the Overview tab.



Datasource subscription == **66 selected** | Datasource resource group == **All** | Datasource location == **All** | Datasource type == **Azure Virtual mach**

Datasource type: Azure Virtual machines
Overview of Jobs and Backup instances

Jobs (last 24 Hours) View all

Operation	Failed	In progress	Completed
Scheduled backup	64	8	246
On-demand backup	0	0	12
Restore	1	0	57

Backup instances

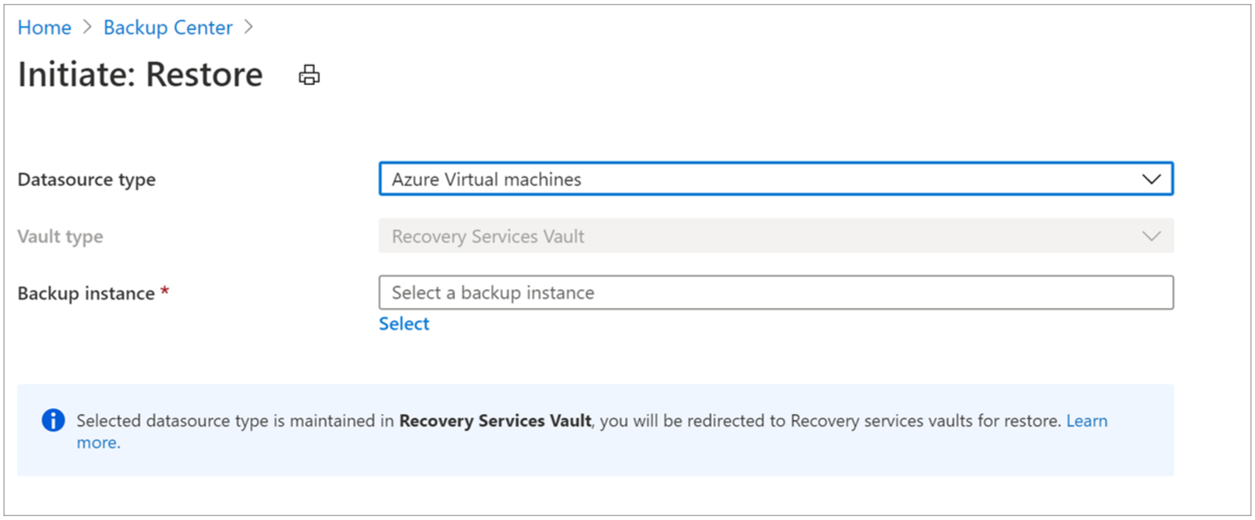
Azure Virtual machines

359

Protection configured	338
Protection stopped	16
Soft deleted	5

86
out of 359 — Backup instances with the underlying datasource not found

2. Select Azure Virtual machines as the Datasource type, and then select a Backup instance.



Home > Backup Center >

Initiate: Restore

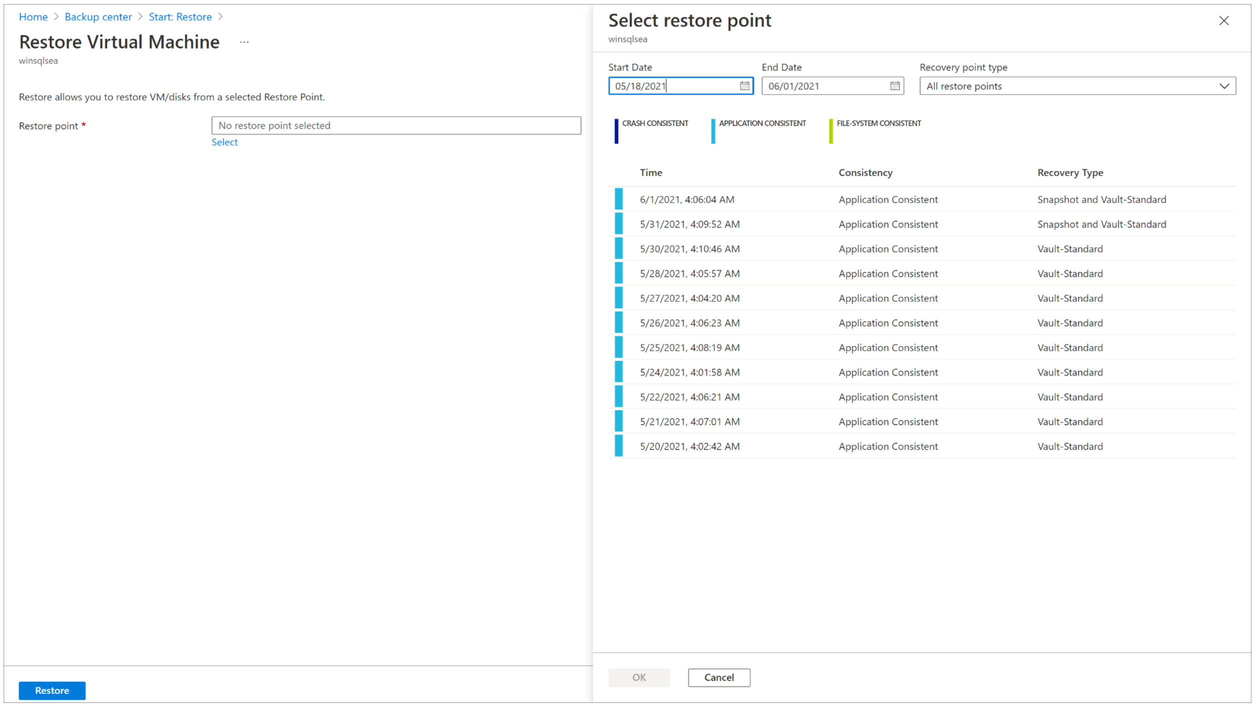
Datasource type: Azure Virtual machines

Vault type: Recovery Services Vault

Backup instance *: Select a backup instance

Selected datasource type is maintained in **Recovery Services Vault**, you will be redirected to Recovery services vaults for restore. Learn more.

3. Select a VM and click Continue.
4. In the next screen that appears, select a restore point to use for the recovery.



Home > Backup center > Start: Restore >

Restore Virtual Machine

winsqlsea

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

Restore point *: No restore point selected

Select restore point

winsqlsea

Start Date: 05/18/2021

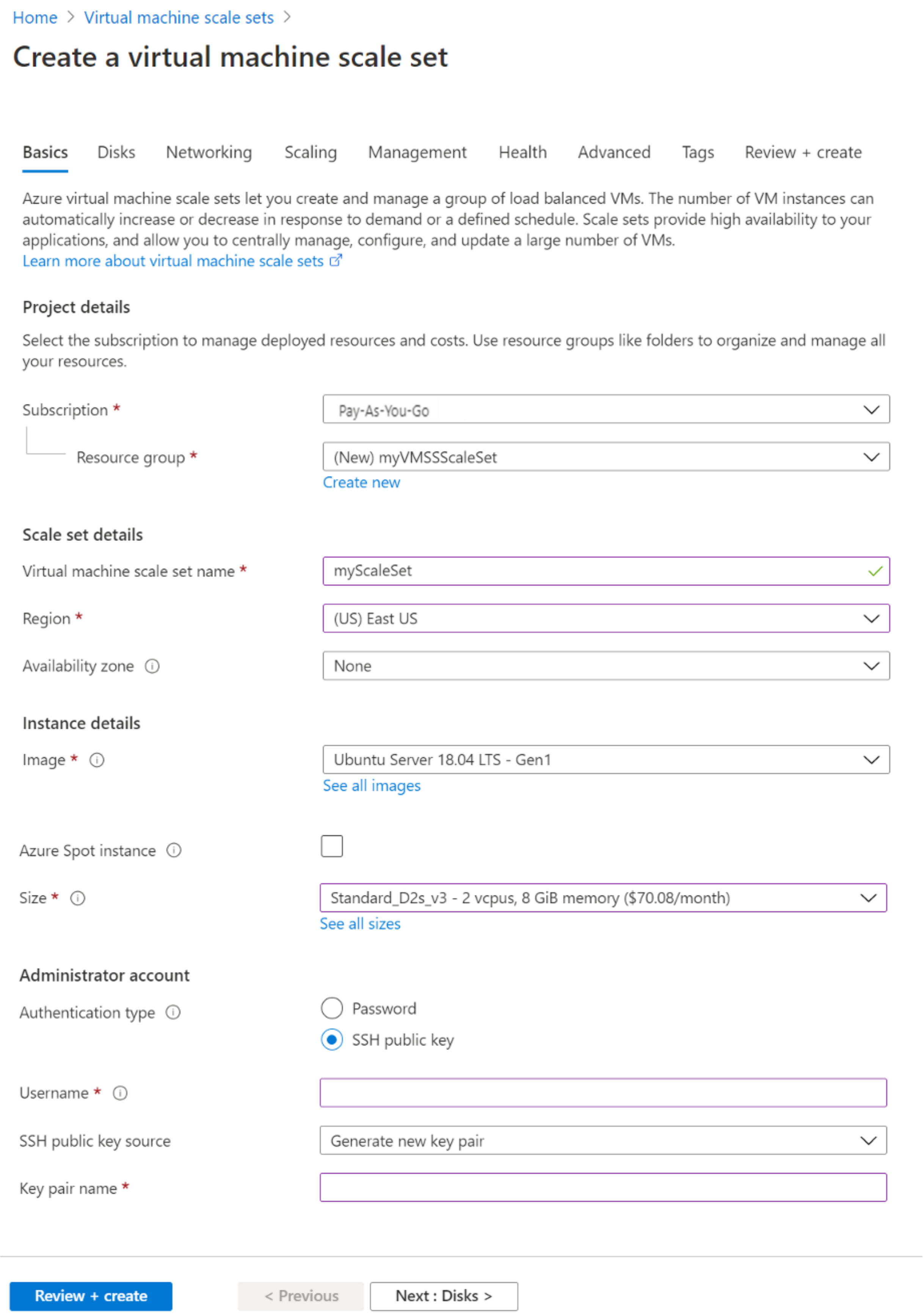
End Date: 06/01/2021

Recovery point type: All restore points

Time	Consistency	Recovery Type
6/1/2021, 4:06:04 AM	Application Consistent	Snapshot and Vault-Standard
5/31/2021, 4:09:52 AM	Application Consistent	Snapshot and Vault-Standard
5/30/2021, 4:10:46 AM	Application Consistent	Vault-Standard
5/28/2021, 4:05:57 AM	Application Consistent	Vault-Standard
5/27/2021, 4:04:20 AM	Application Consistent	Vault-Standard
5/26/2021, 4:06:23 AM	Application Consistent	Vault-Standard
5/25/2021, 4:08:19 AM	Application Consistent	Vault-Standard
5/24/2021, 4:01:58 AM	Application Consistent	Vault-Standard
5/22/2021, 4:06:21 AM	Application Consistent	Vault-Standard
5/21/2021, 4:07:01 AM	Application Consistent	Vault-Standard
5/20/2021, 4:02:42 AM	Application Consistent	Vault-Standard

Create Virtual Machine Scale Set

1. Type Scale set in the search box. In the results, under Marketplace, select Virtual Machine Scale Sets. Select Create on the Virtual Machine Scale Sets page, which opens the Create a Virtual Machine Scale Set page.
2. In the Basics tab, under Project details, make sure the correct subscription is selected and select myVMSSResourceGroup from the resource group list.
3. Type myScaleSet as the name for your scale set.
4. In Region, select a region that is close to your area.
5. Under Orchestration, ensure the Uniform option is selected for Orchestration mode.
6. Select a marketplace image for Image. In this example, we have chosen Ubuntu Server 18.04 LTS.
7. Enter your desired username, and select which authentication type you prefer.
    a. A Password must be at least 12 characters long and meet three out of the four following complexity requirements: one lower case character, one upper case character, one number, and one special character. For more information, see username and password requirements.
    b. If you select a Linux OS disk image, you can instead choose SSH public key. Only provide your public key, such as ~/.ssh/id_rsa.pub. You can use the Azure Cloud Shell from the portal to create and use SSH keys.



Create a virtual machine scale set

Azure virtual machine scale sets let you create and manage a group of load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs.

Learn more about virtual machine scale sets

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) myVMSSScaleSet Create new

Scale set details

Virtual machine scale set name *	myScaleSet ✓
Region *	(US) East US
Availability zone ⓘ	None

Instance details

Image * ⓘ	Ubuntu Server 18.04 LTS - Gen1 See all images
Azure Spot instance ⓘ	□
Size * ⓘ	Standard_D2s_v3 - 2 vcpus, 8 GiB memory ($70.08/month) See all sizes

Administrator account

Authentication type ⓘ	○ Password ● SSH public key
Username * ⓘ	
SSH public key source	Generate new key pair
Key pair name *	

8. Select Next to move the other pages.
9. Leave the defaults for the Disks page.
10. On the Networking page, under Load balancing, select the Use a load balancer option to put the scale set instances behind a load balancer.
11. In Load balancing options, select Azure load balancer.
12. In Select a load balancer, select *myLoadBalancer* that you created earlier.
13. For Select a backend pool, select Create new, type *myBackendPool*, then select Create.
14. When you're done, select Review + create.
15. After it passes validation, select Create to deploy the scale set.
16. Explore VMSS configuration