Prepared by : Almog Gal

For : guytwena@gmail.com

Snapshot manager automation via azure automation account using powershell tutorial and requirements.

About The runbook:

This runbook takes incremental snapshost of a specified VM disk's every one hour. The retention of the snapshots is 24 hours. Also the runbook sends notification through email whether the snapshot was successful or not and if the deletion of the old snapshots was successful or not.

Requirements:

1. Have an Azure account with a valid subscribtion.
2. Create an automation account in the resource group where the VM is allocated .
3. Download the following modules to your automation account (automation account → shared resources → modules → add a module): Az.accounts, Az.Compute, AzureAD, AzureRM.Compute, AzureRM.profile, AzureRM.Resources, AzureVmSnapshots.
4. Two runbooks: "snapshot manager.ps" - the main runbook and "certificate_generated.ps" - a runbook for generating a self signed certificate.

Tutorial:

1. In your Automation account, open an reunbook and name it "snapshot manager'. Then just copy the runbook's code in there.
2. For the runbook to recognize which disk belongs to which VM you will need to add a tag to the VM's disks which you want to snapshot (home → <resource group name> → <VM name> → <OS/data disk name> → tags). Then add a tag named "vm" with the value "<VM name>".
3. `Connect to azure cli and run this command: az ad sp create-for-rbac --name snap1 --role "Owner" --scopes /subscriptions/<subscription id>/resourceGroups/<resource group name>.` **`save the output to a notepad file.`**

4. The runbook runs through an identity called an App. Create an app (Home → App registrations) and call it as you want (with default settings). You will get generated IDs: **application ID** and **tenant ID**. Save them in a notepad file for later.
5. Now we will need to create a schedule to run the runbook every hour. Create a new schedule (automation account → shared resources → schedules). Name it "snapshot_schedule" and set it to recurring for every hour.
6. Now we will need to connect the schedule to the runbook (automation account → runbooks → "snapshot manager" → resources → schedules).
7. Edit the runbook (automation account → runbooks → "snapshot manager" → edit). Notice that at line 2 and 3 you have consistence parameters: resource group name ($RG_NAME) and the VM name ($VM_NAME). Change them to fit your azure environment.

8. Create SendGrid account, register an email to send mail. Create an API to connect and send emails from SendGrid. Save the API key to use for the runbook.
9. Add to the runbook all the relevent parametrs.
10. Make sure you publish the runbook (automation account → runbooks → “snapshot manager” → edit → publish) so you can run it as an automation.

UPDATED SCRIPT WITH EMAIL

```
# consistence paramters
$RG_NAME = "rg1"
$VM_NAME = "test1"
$DEST_EMAIL = "almoggal11@gmail.com"
$FROM_EMAIL = "ofirgal11@outlook.com"
# scopes moudles of automation account
Enable-AzureRmAlias -Scope Process
# Forces the script to use proper TLS
[System.Net.ServicePointManager]::SecurityProtocol =
[System.Net.SecurityProtocolType]::Tls12



# Connect to azure with password: az ad sp create-for-rbac --name snap1
--role "Disk Snapshot Contributor" --scopes
/subscriptions/<subscription id>/resourceGroups/<resource group name>
$TENANT_ID = "d597d379-d9d9-4ebb-9052-f2d218fabbc1"
$PASSWORD = "GgP8Q~avP4ybYgcV-MhxW2HBSuLnexjo3vGkfa87"
$APP_ID = '1bd7809d-c862-4566-ba36-02cff3caaa92'

$passwd = ConvertTo-SecureString $PASSWORD -AsPlainText -Force
$pscredential = New-Object
System.Management.Automation.PSCredential($APP_ID, $passwd)
Connect-AzAccount -ServicePrincipal -Credential $pscredential -Tenant
$TENANT_ID



# get all disks.
$disk_list = Get-AzureRmResource -ResourceType
"Microsoft.Compute/disks"

# get the current time of the snapshot with '_' format
$snapshot_time = Get-Date -Format "_dd_MM_yyyy_HH_mm"

# Contect of summery mail
$content = ""
```

```
# create incremental snapshots of VM_NAME disks.
foreach($disk in $disk_list){
    #$tags = $disk.Tags
    if($disk.Tags.Values -eq $VM_NAME){
        $snapshot_name = $disk.name + $snapshot_time
        try{
            $disk_snap = Get-AzDisk -DiskName $disk.name
-ResourceGroupName $RG_NAME
            $snapshotConfig = New-AzSnapshotConfig -SourceUri
$disk_snap.Id -Location $disk_snap.Location -CreateOption Copy
-Incremental -Tag @{vm=$VM_NAME}
            New-AzSnapshot -ResourceGroupName $RG_NAME -SnapshotName
$snapshot_name -Snapshot $snapshotConfig | Out-Null
            $s_snap = "SNAPSHOT TAKE OF $snapshot_name SUCCEEDED `n"
            $content += $s_snap
        }
        # if the snapshot take has failed
        catch{
            $err_msg = $($PSItem.Exception.Message.ToString())
            #Write-Output $err_msg
            $f_snap = "SNAPSHOT TAKE OF $snapshot_name FAILED: $err_msg
`n"
            $content += $f_snap
        }
    }
}

# Delete snapshots after 24 hours of VM_NAME disks
$snapshots = Get-AzSnapshot
foreach($snapshot in $snapshots){
    # for every snapshot of the vm
    if($snapshot.Tags.values -eq $VM_NAME){
        # if the snapshot exists more then 24 hours
        $snapshot_name = $snapshot.name
        if($snapshot.TimeCreated -lt
(Get-Date).AddDays(-1).ToUniversalTime()){
            try{
                Remove-AzSnapshot -ResourceGroupName $RG_NAME
-SnapshotName $snapshot_name -ErrorAction Stop -Force;
                $s_snap = "SNAPSHOT DELETION OF $snapshot_name
SUCCEEDED `n"
                $content += $s_snap
            }
```

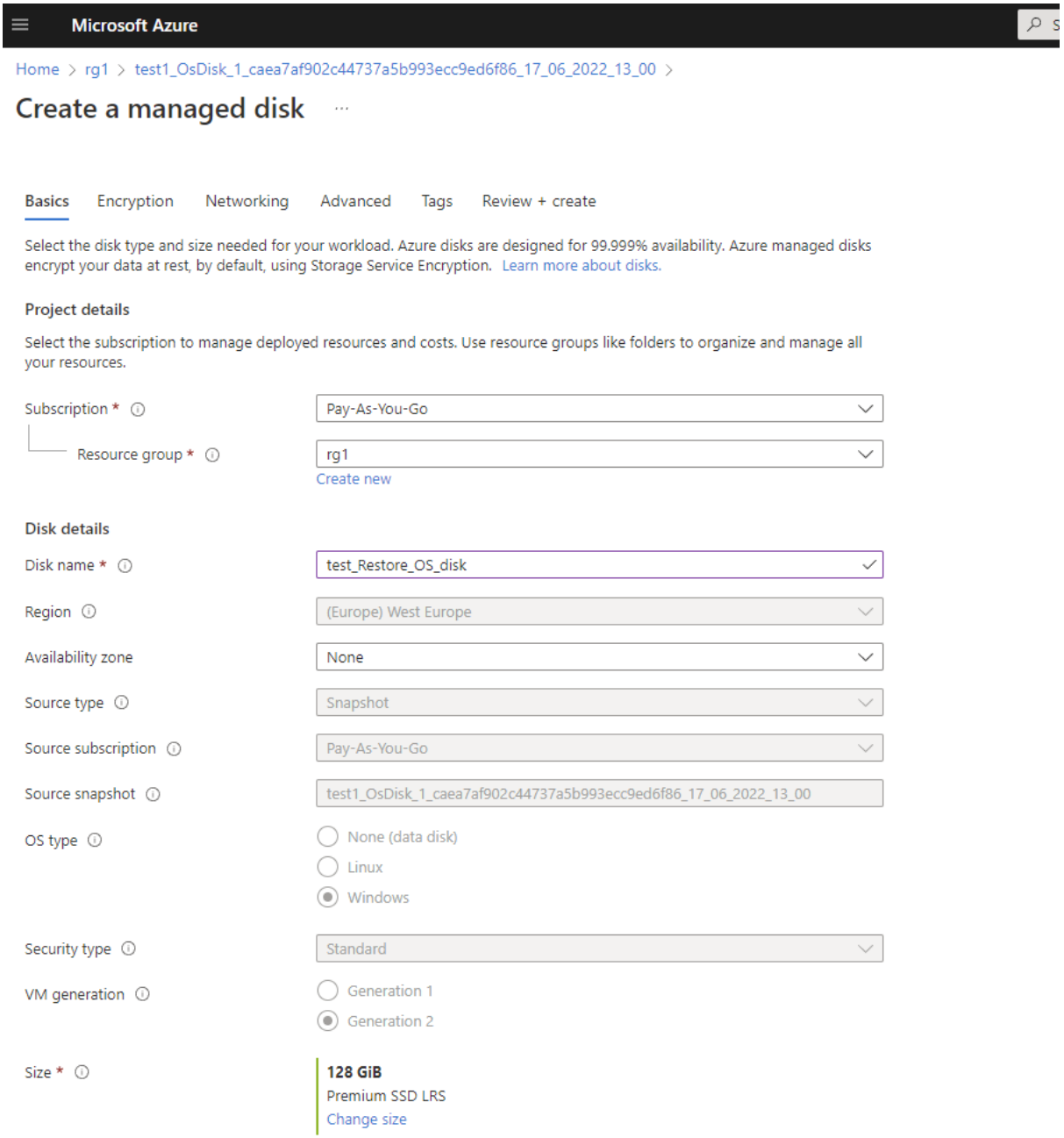
```
            # if deletion has failed
            catch{
                $err_msg = $($PSItem.Exception.Message.ToString())
                $f_snap = "SNAPSHOT DELETION OF $snapshot_name FAILED:
$err_msg `n"
                $content += $f_snap
            }

        }
    }
}
Write-Output $content
# The send grid key from the send grid account
$SENDGRID_API_KEY =
"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"
$headers = New-Object
"System.Collections.Generic.Dictionary[[String],[String]]"
$headers.Add("Authorization", "Bearer " + $SENDGRID_API_KEY)
$headers.Add("Content-Type", "application/json")

# subject of the mail
$subject = "Hourly snapshot of $snapshot_time"

$body = @{
personalizations = @(
    @{
        to = @(
                @{
                    email = $DEST_EMAIL
                }
        )
    }
)
from = @{
    email = $FROM_EMAIL
}
subject = $subject
content = @(
    @{
        type = "text/plain"
        value = $content
    }
)
```

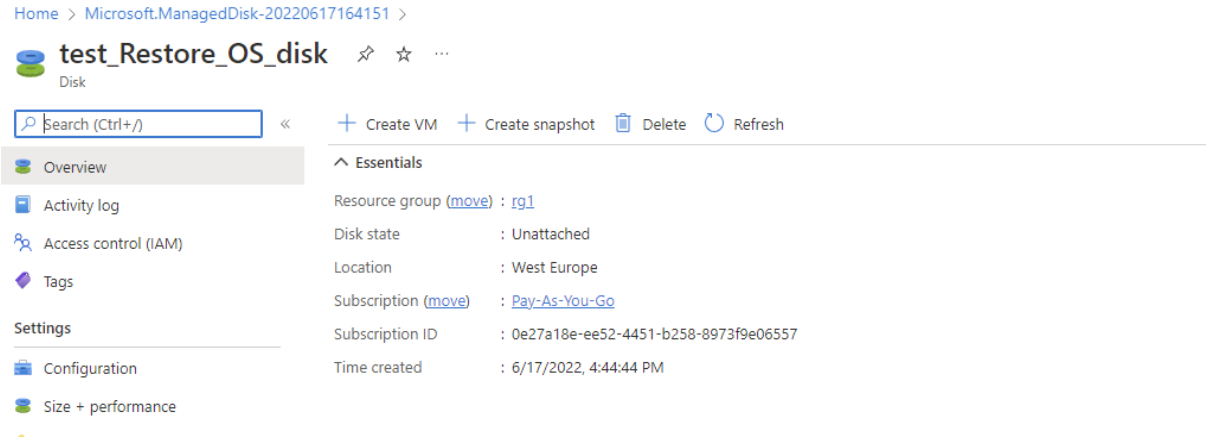
```
}

$bodyJson = $body | ConvertTo-Json -Depth 4

$response = Invoke-RestMethod -Uri
https://api.sendgrid.com/v3/mail/send -Method Post -Headers $headers
-Body $bodyJson
```

creating a new VM from disks snapshots

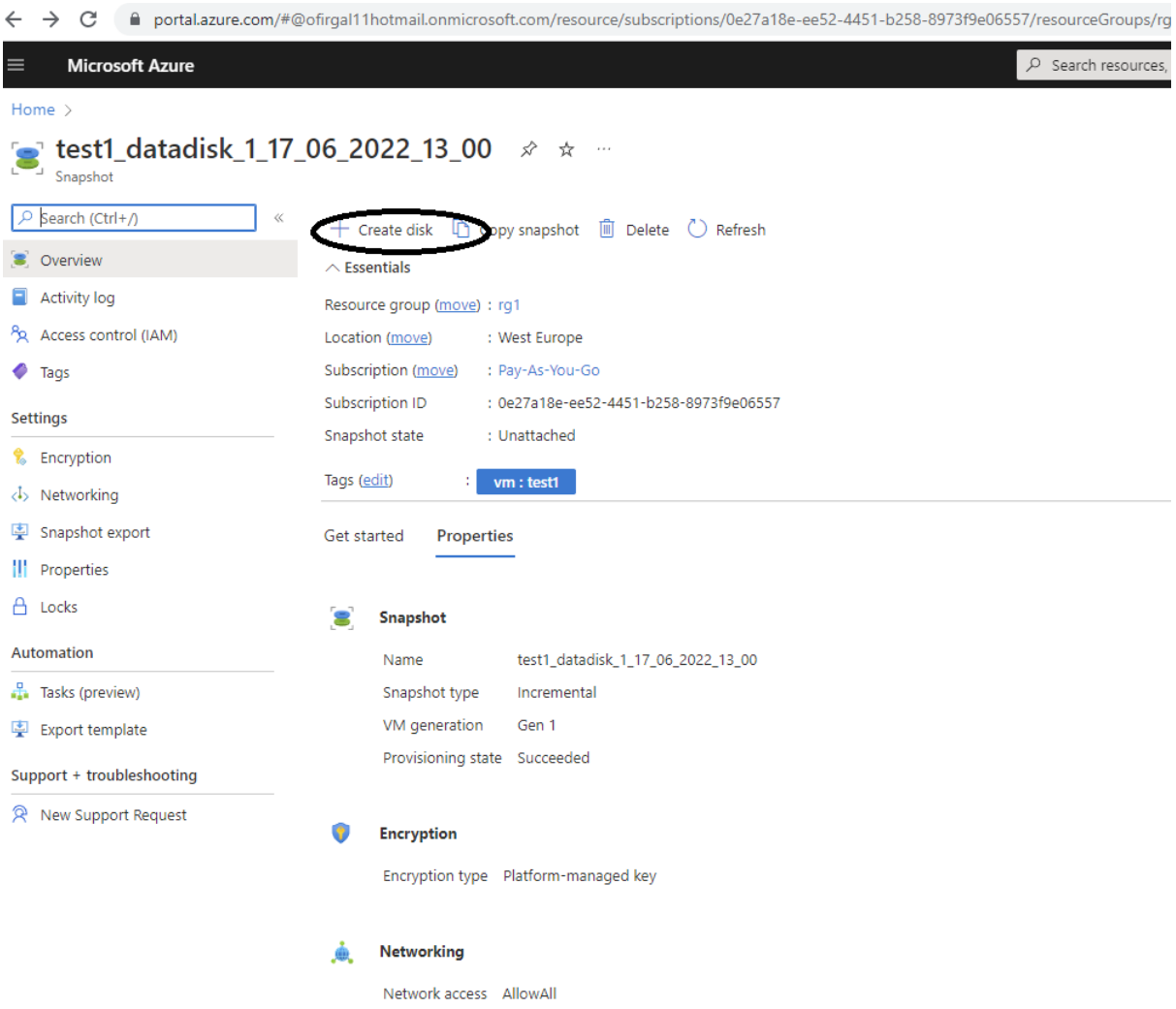
Create DISks from Snapshot for restore machine (OS+DATA disks)

Create OS disk from snapshot (same snapshots need to be used for all disks)- from same time for all (OS+2 data disks snapshots)





Now we create DATA disks from same time as OS disk snapshots



Home > test1_datadisk_1_17_06_2022_13_00 >

Create a managed disk ...

Basics | Encryption | Networking | Advanced | Tags | Review + create

Select the disk type and size needed for your workload. Azure disks are designed for 99.999% availability. Azure managed disks encrypt your data at rest, by default, using Storage Service Encryption. Learn more about disks.

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 * : rg1

Create new

Disk details

Disk name * : test_Restore_DATA_disk

Region : (Europe) West Europe

Availability zone : None

Source type : Snapshot

Source subscription : Pay-As-You-Go

Source snapshot : test1_datadisk_1_17_06_2022_13_00

OS type :
- (•) None (data disk)
- ( ) Linux
- ( ) Windows

Security type : Standard

Size * : **64 GiB**
Premium SSD LRS
Change size

Create a managed disk ...

Validation passed

Basics | Encryption | Networking | Advanced | Tags | **Review + create**

Basics

Subscription	Pay-As-You-Go
Resource group	rg1
Region	West Europe
Disk name	test_Restore_DATA_disk
Availability zone	None
Source type	Snapshot
Source subscription	Pay-As-You-Go
Source snapshot	test1_datadisk_1_17_06_2022_13_00
OS type	None (data disk)
Security type	Standard

Size

Size	64 GiB
Performance tier	P6 - 240 IOPS, 50 MBps (default)
Storage type	Premium SSD LRS

Encryption

Encryption type	Platform-managed key

Advanced

Enable shared disk	No
Enable on-demand bursting	No

Networking

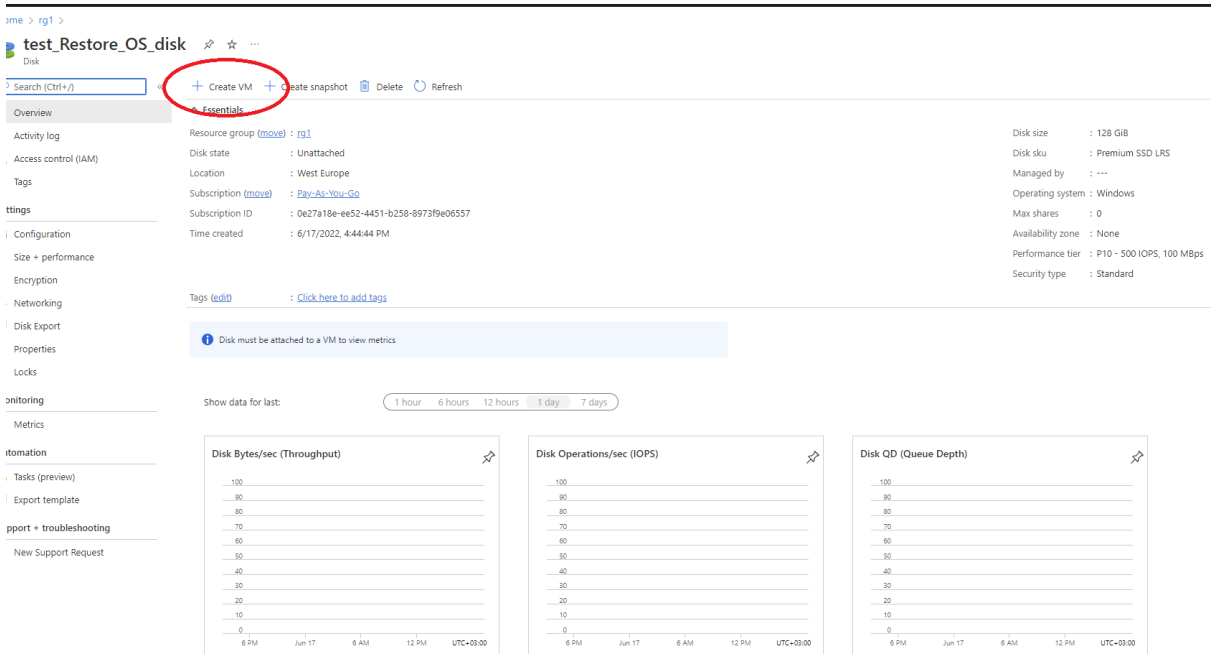
Network access	AllowAll

Tags

(none)

Create another disk (DATA 2) from the same time as the 2 other disks as required

Create a new VM machine from the restored OS IMAGE (use the same machine type as the original machine)



Use the same machine type /network/region /add public IP and RDP
Mark No infra redundancy required on the disk level

Home > rg1 > test_Restore_OS_disk >

Create a virtual machine

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 * : Pay-As-You-Go

Resource group * : rg1

Create new

Instance details

Virtual machine name * :

Region : (Europe) West Europe

Availability options : No infrastructure redundancy required

Security type : Standard

Image * : test_Restore_OS_disk - Gen2

See all images | Configure VM generation

Azure Spot instance :

Size * : Standard_D2s_v3 - 2 vcpus, 8 GiB memory ($154.76/month)

See all sizes

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

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.

Licensing

License type * : Windows server

Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

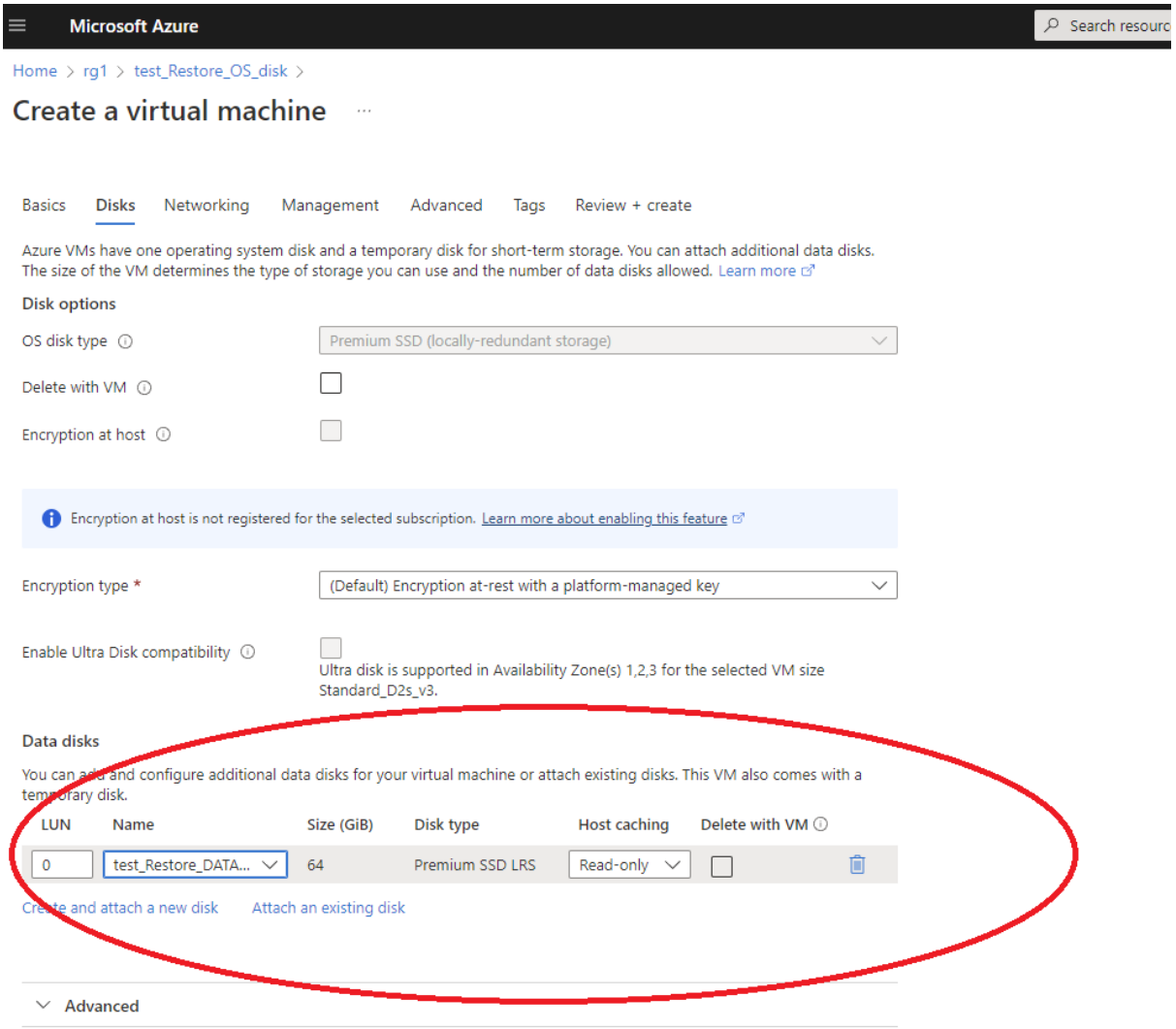
Would you like to use an existing Windows Server license? * :

I confirm I have an eligible Windows Server license with Software Assurance * or Windows Server subscription to apply this Azure Hybrid Benefit.

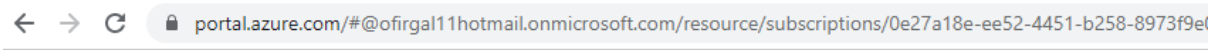
Review Azure hybrid benefit compliance

Review + create | < Previous | Next : Disks >

Attach the 2 DATA disks to the new VM (Lun 0 -data disk1, lun 1- data disk 2)



Use the same network subnet and assign RDP access



Microsoft Azure

Home > rg1 > test_Restore_OS_disk >

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 * : rg1-vnet
Create new

Subnet * : default (10.0.0.0/24)
Manage subnet configuration

Public IP : (new) restor1-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 create rules to limit inbound traffic to known IP addresses.

Delete public IP and NIC when VM is deleted ☐

Accelerated networking ☐

The selected image does not support 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? ☐

Create a virtual machine ...

Configure monitoring and 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 Microsoft Defender for Cloud 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 [ ]

This image does not support Login with Azure AD.

Auto-shutdown

Enable auto-shutdown [ ]

Guest OS updates

Enable hotpatch [ ]

Hotpatching is available only with Windows Server 2022 Datacenter: Azure Edition Core.

Patch orchestration options: Automatic by OS (Windows Automatic Updates)

Some patch orchestration options are not available for this image. Learn more

Home > rg1 > test_Restore_OS_disk >

Create a virtual machine ...

Validation passed

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

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

test_Restore_OS_disk Image	Standard D2s v3 2 vcpus, 8 GiB memory

Basics

Subscription	Pay-As-You-Go
Resource group	rg1
Virtual machine name	restor1
Region	West Europe
Availability options	No infrastructure redundancy required
Security type	Standard
Image	test_Restore_OS_disk - Gen2
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Username	azureuser
Public inbound ports	RDP
Already have a Windows license?	Yes
License type	Windows Server
Azure Spot	Yes (Stop / Deallocate)
Azure Spot max price	-

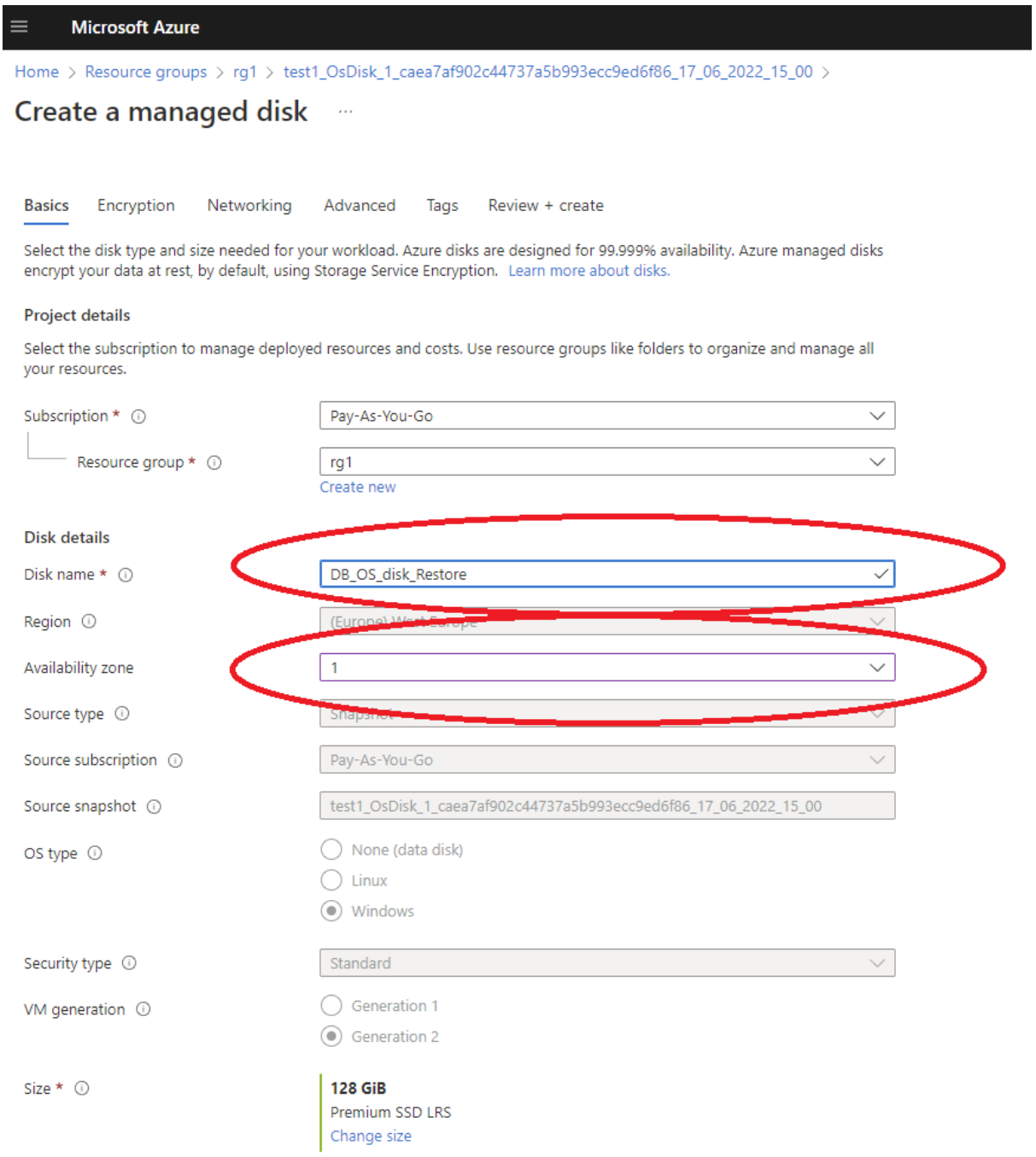
Disks

OS disk type	Premium SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Disabled
Data disks	1
Delete data disk with VM	0 disks enabled
Ephemeral OS disk	No

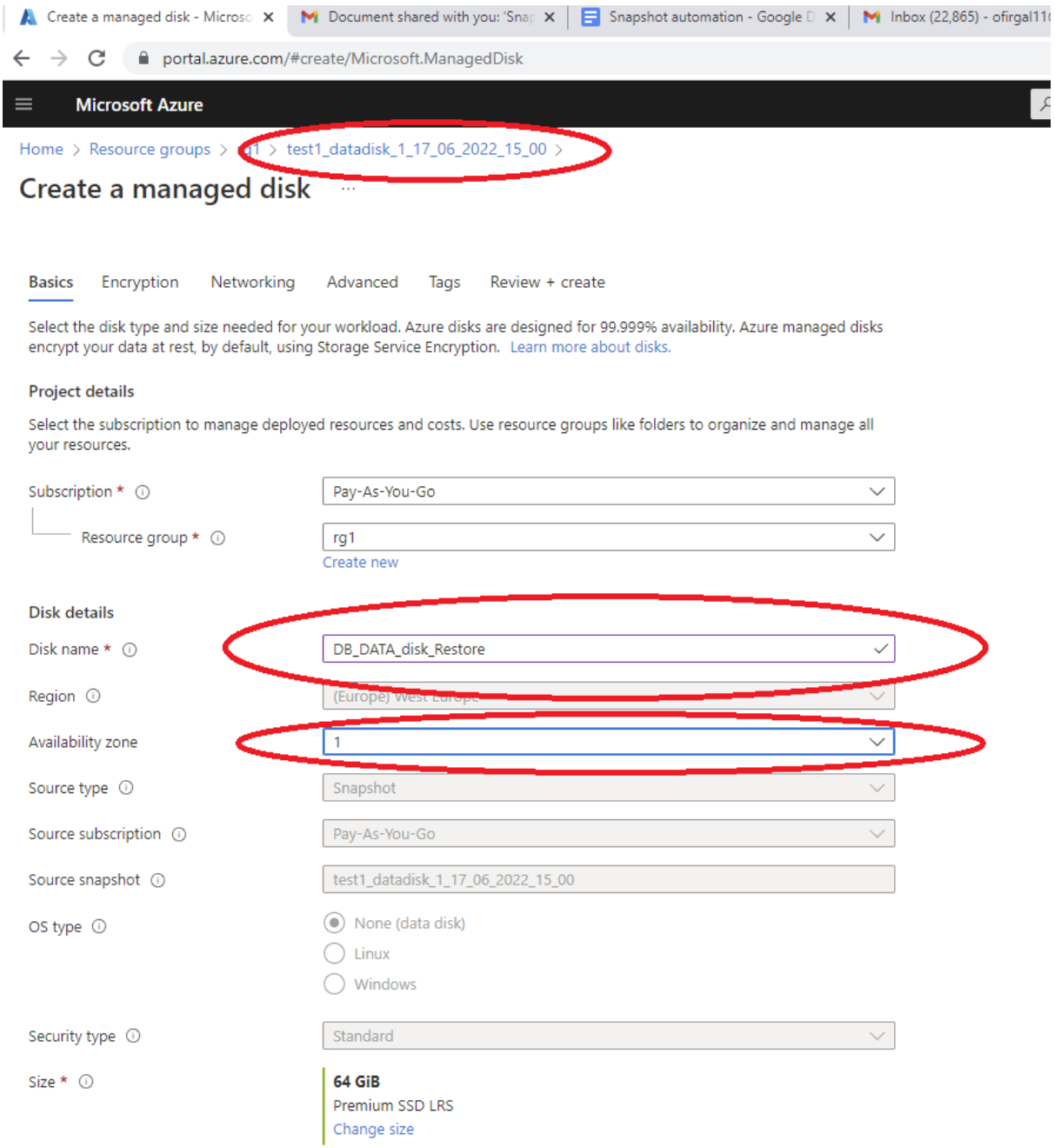
Connect and verify you can access your specific point in time snapshot data

Another option is restoring snapshots to the existing machine - this will reverse the machine data to the time of the snapshot - On production VM - last resort

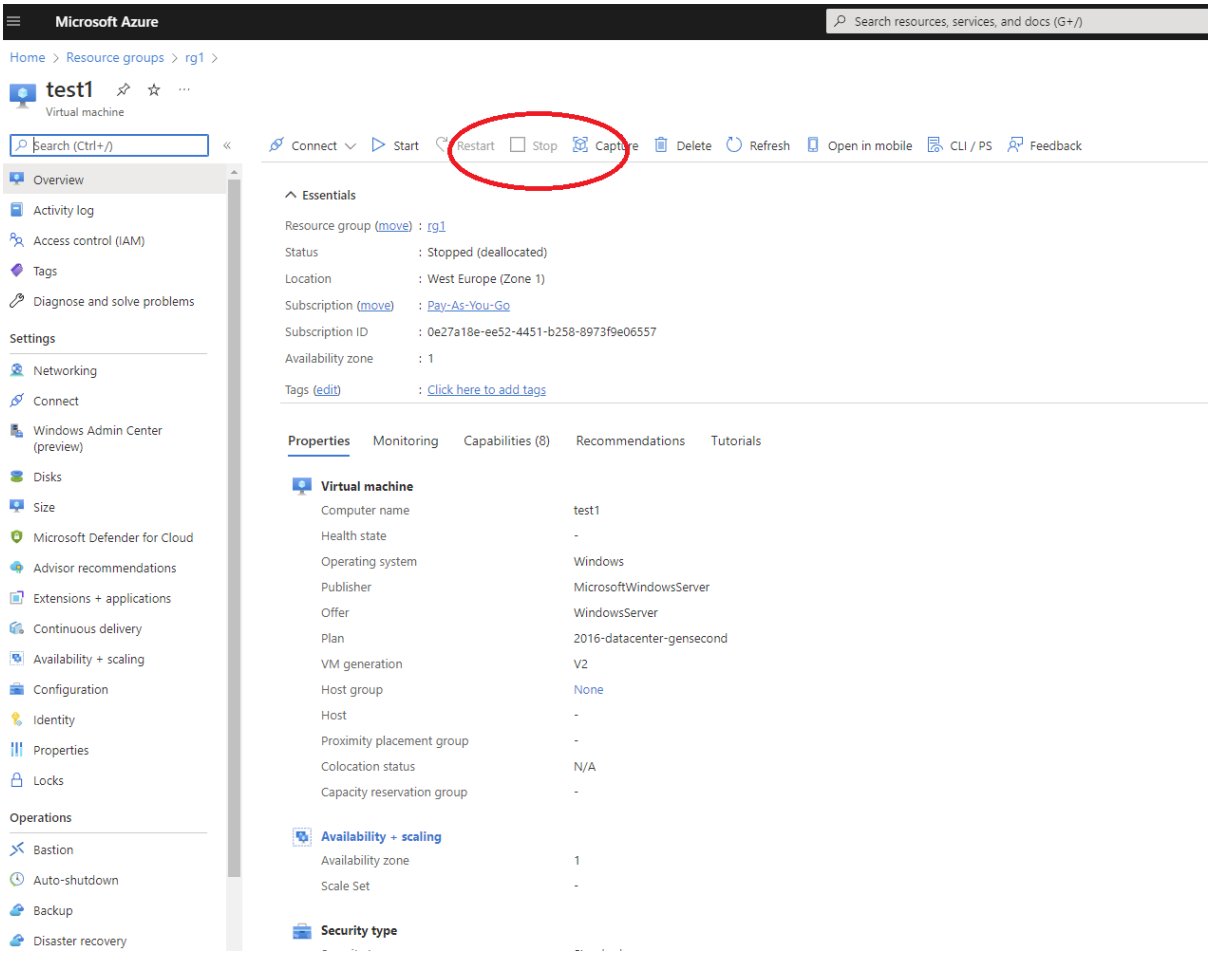
We need to create the disks from Snapshots (OS disk + DATA disk)
OS disk creation from snapshot - same availability zone as VM



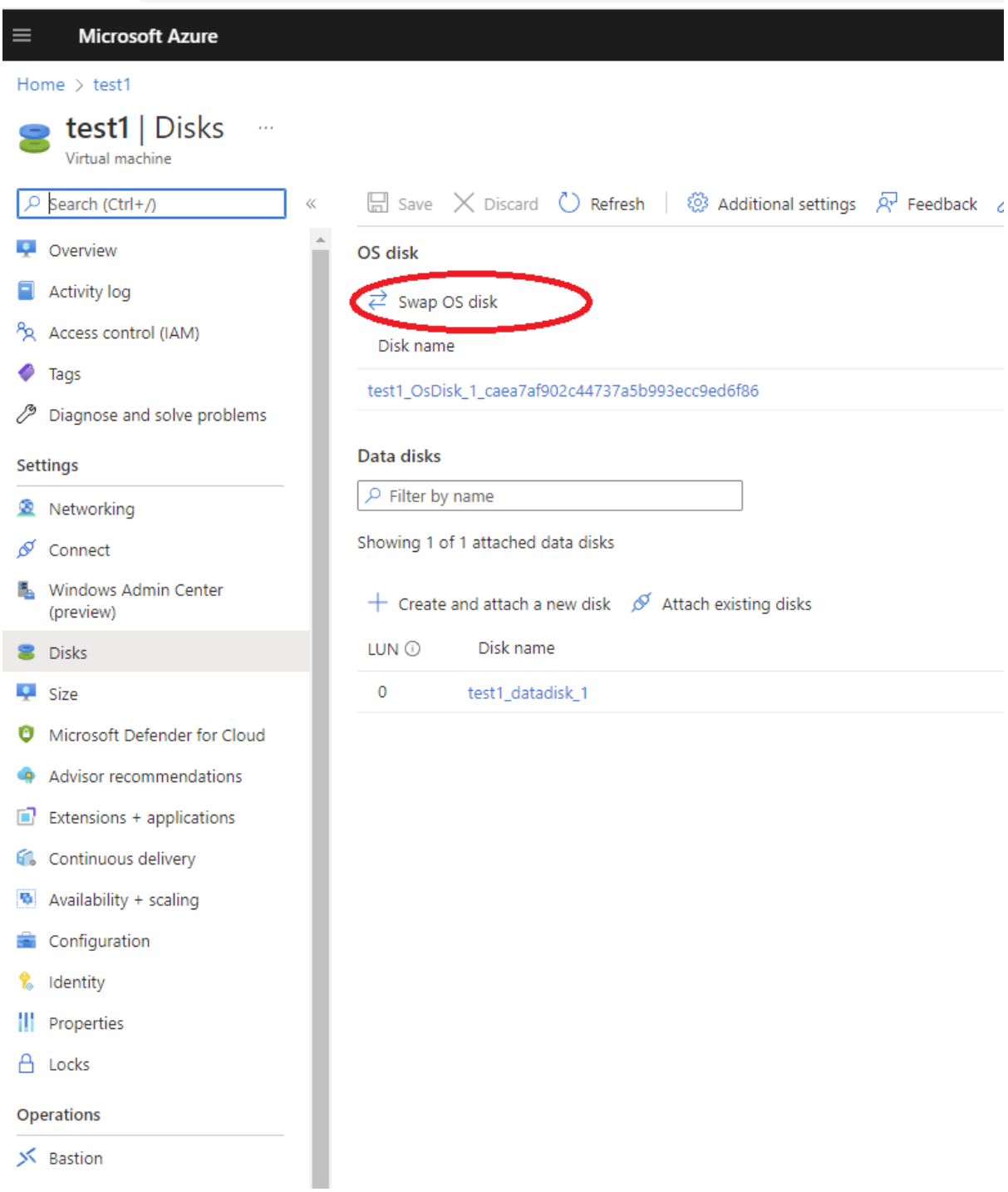
Restore disk from snapshot - data disk - (same snapshot time as OS disk)- SAME AZ

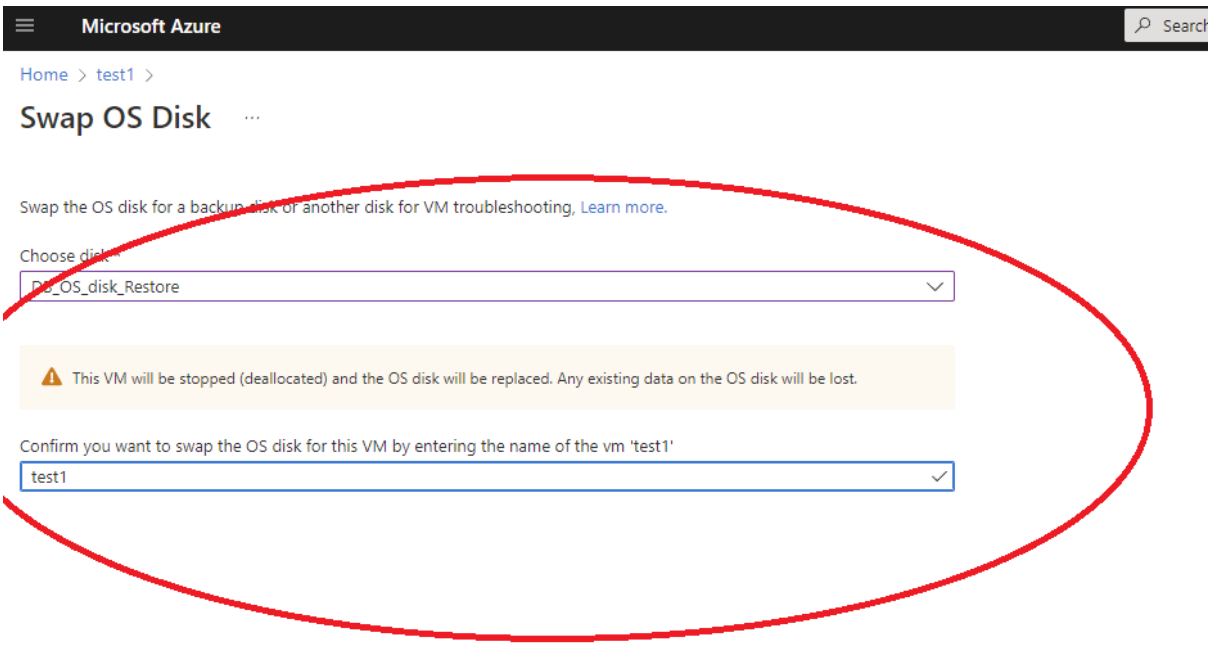


STOP the production machine

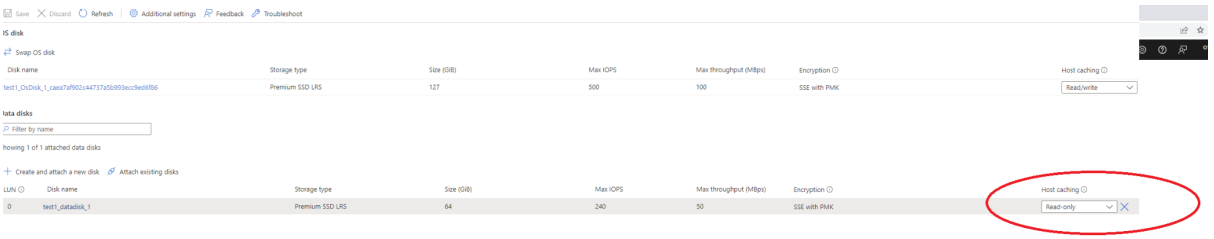


Replace OS disk

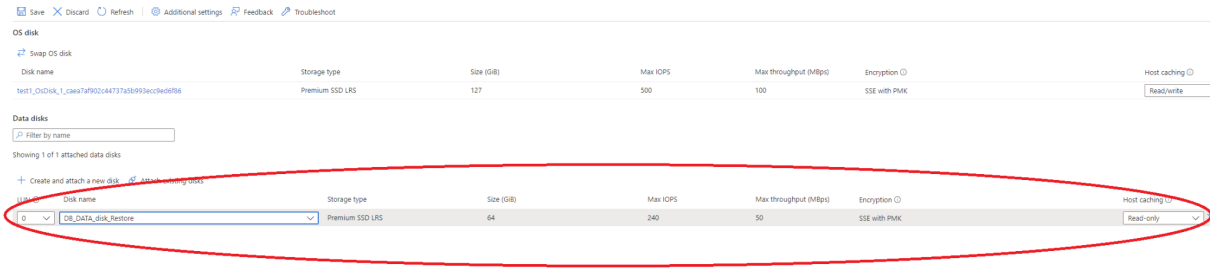

Microsoft Azure
Home > test1
test1 | Disks
Virtual machine
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Windows Admin Center (preview)
Disks
Size
Microsoft Defender for Cloud
Advisor recommendations
Extensions + applications
Continuous delivery
Availability + scaling
Configuration
Identity
Properties
Locks
Operations
Bastion
Save
Discard
Refresh
Additional settings
Feedback
OS disk
Swap OS disk
Disk name
test1_OsDisk_1_caea7af902c44737a5b993ecc9ed6f86
Data disks
Filter by name
Showing 1 of 1 attached data disks
Create and attach a new disk
Attach existing disks
LUN
Disk name
0
test1_datadisk_1



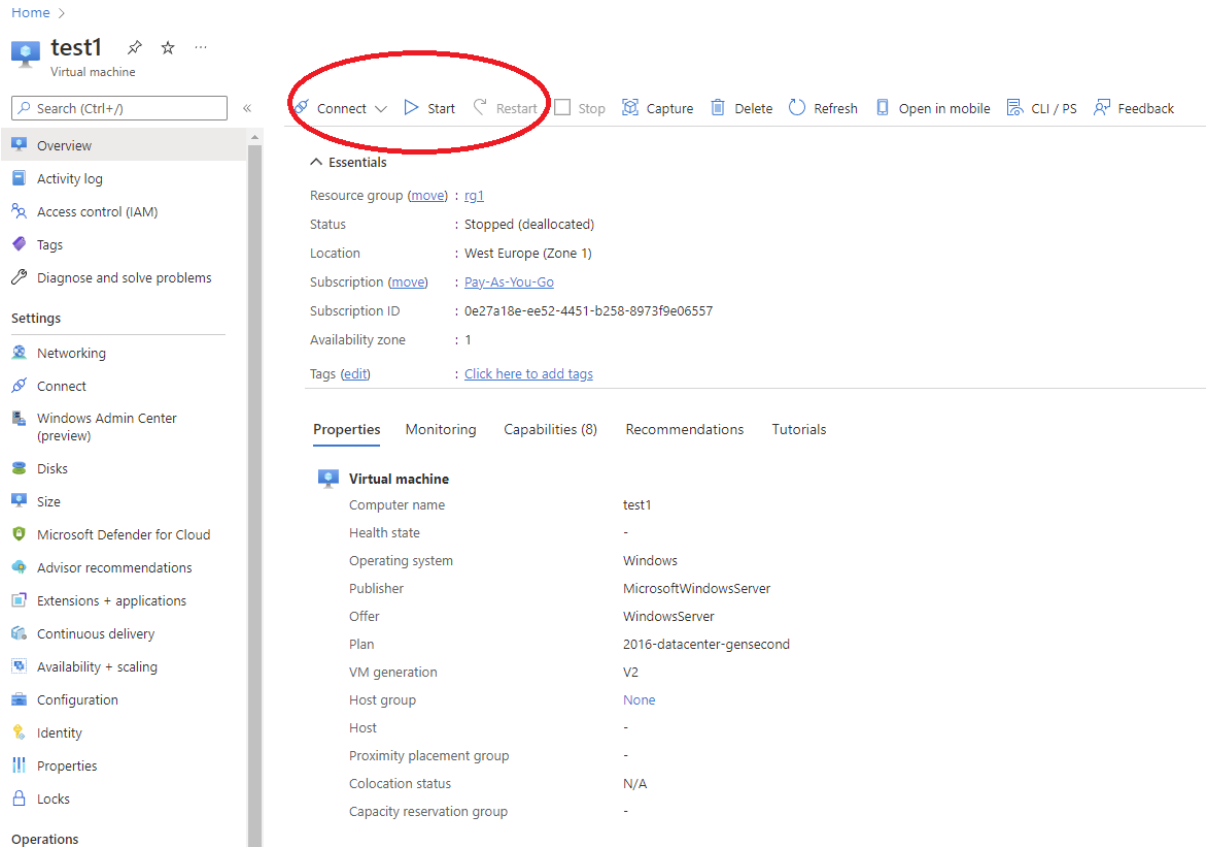
remove data disks



Attach the restore data disks (LUN0 and then data disk 2 LUN 1)



Save and start the VM



Verify that you can access the VM with the snaphot disks (moving back in time to the snaphsots on production VM is last resort)!!!