ADR-0021 - Rotating keys and Encrypting Virtual Disks ✔️

Context and Problem Statement

Context

Requirements to achieve Data Protection are the following:

- Disks in Azure need to be encrypted
- Keys for encryption need to be rotated
- Single file restore is a nice to have, at the moment is not possible neither for Azure Backup (Back up and restore encrypted Azure VMs - Azure Backup) nor Veeam Backup for Azure (Considerations and Limitations - Veeam Backup for Microsoft Azure Guide)

Problem Statement

Current approach (**Azure Disk Encryption**) have some drawbacks:

1. It's incompatible with key auto-rotation. Azure Disk Encryption will continue using original encryption key, even after it has been auto-rotated (Creating and configuring a key vault for Azure Disk Encryption on a Windows VM - Azure Virtual Machines)

> ❌ This will drive to dead end due to the impossibility to access VMs when original keys are disabled or removed when expired

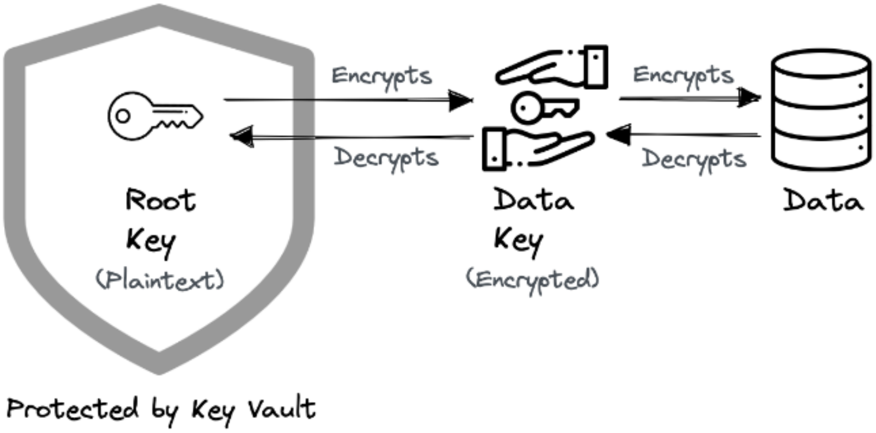
2. Single file restore does not work at the moment with **Azure Disk Encryption**; full restore of the entire disk is needed to access a single file, making it an expensive and time-consuming task

Considered Options

Azure Disk Encryption Set

(Server-side encryption of Azure managed disks - Azure Virtual Machines)

It uses envelope encryption, allowing you to rotate the keys periodically without impacting the VMs. When rotating the keys, Storage service re-encrypts the **data encryption** keys only with the new **customer-managed keys**

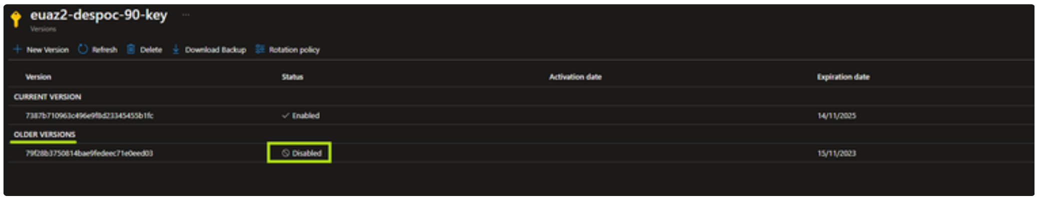


PoC

PoC was needed to validate Problem Statement; also to check options to migrate current approach from using ADE to DES:

1.Validating Problem Statement

Force key-rotation with the current solution on a test VM, and disable original key

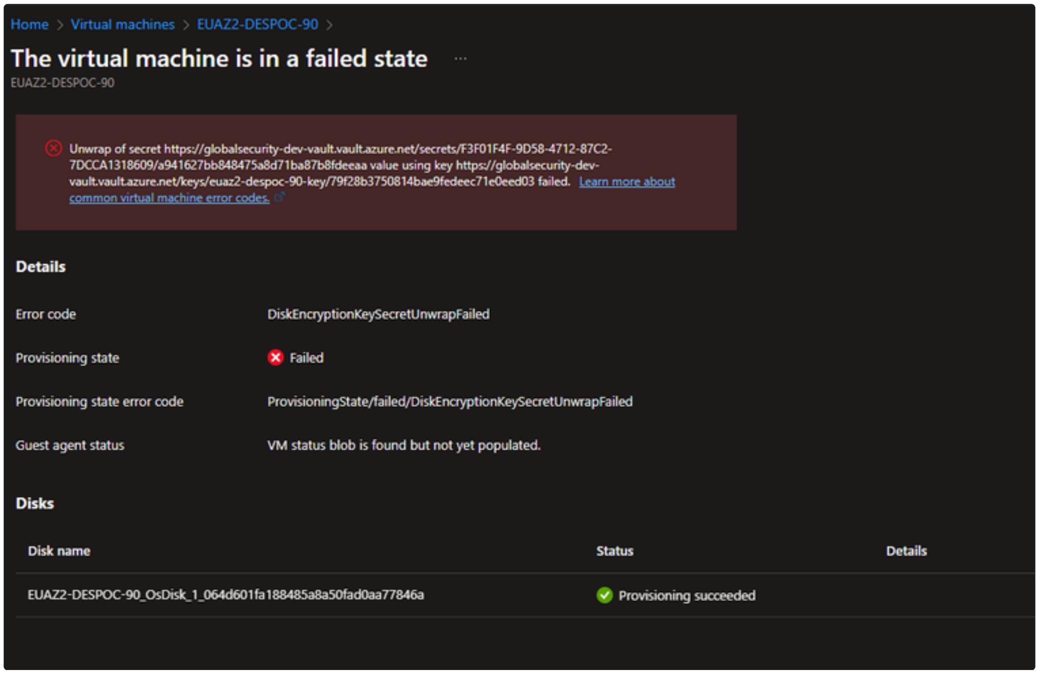


euaz2-despoc-90-key ···

Versions

Version	Status	Activation date	Expiration date
CURRENT VERSION			
7387b710963c496e9f8d23345455b1fc	✓ Enabled		14/11/2025
OLDER VERSIONS			
79f28b3750814bae9fedeec71e0eed03	⦸ Disabled		15/11/2023

- Disabling the key on 14/11/23 didn't cause any “damage” to the V/M
- After rebooting the VM the day after, 15/11/2023, faced this error, and VM was unable to boot again anymore:



The virtual machine is in a failed state ···

EUAZ2-DESPOC-90

Unwrap of secret https://globalsecurity-dev-vault.vault.azure.net/secrets/F3F01F4F-9D58-4712-87C2-7DCCA1318609/a941627bb848475a8d71ba87b8fdeeaa value using key https://globalsecurity-dev-vault.vault.azure.net/keys/euaz2-despoc-90-key/79f28b3750814bae9fedeec71e0eed03 failed. Learn more about common virtual machine error codes.

Details

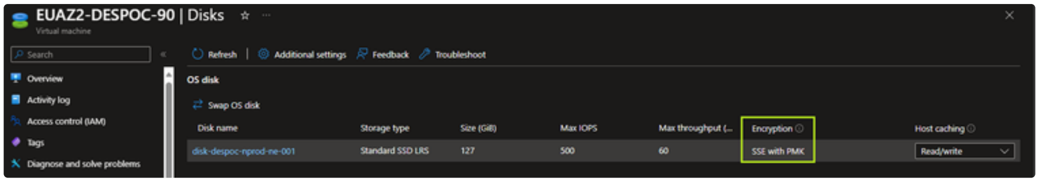
Error code	DiskEncryptionKeySecretUnwrapFailed
Provisioning state	✗ Failed
Provisioning state error code	ProvisioningState/failed/DiskEncryptionKeySecretUnwrapFailed
Guest agent status	VM status blob is found but not yet populated.

Disks

Disk name	Status	Details
EUAZ2-DESPOC-90_OsDisk_1_064d601fa188485a8a50fad0aa77846a	✓ Provisioning succeeded	

2.Testing migration from ADE to DES

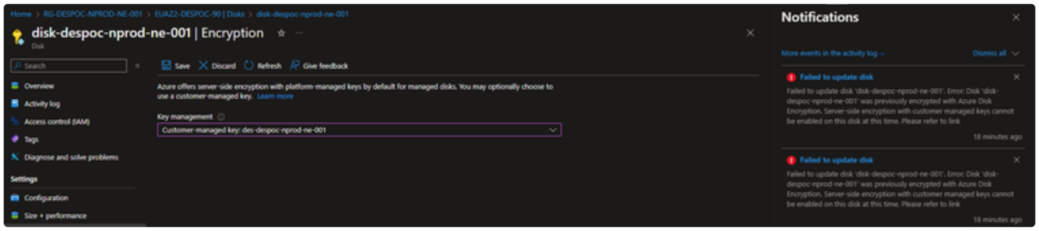
Test VM disk, previously encrypted with ADE, is decrypted



OS disk

Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption	Host caching
disk-despoc-nprod-ne-001	Standard SSD LRS	127	500	60	SSE with PMK	Read/write

Implemented Disk Encryption Set and associated test VM disk headed to the following error message:


Home > RG-DESPOC-NPROD-NE-001 > EUAZ2-DESPOC-90 | Disks > disk-despoc-nprod-ne-001
disk-despoc-nprod-ne-001 | Encryption
Disk
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Size + performance
Save
Discard
Refresh
Give feedback
Notifications
More events in the activity log →
Dismiss all

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. Learn more

Key management: Customer-managed key: des-despoc-nprod-ne-001

Failed to update disk

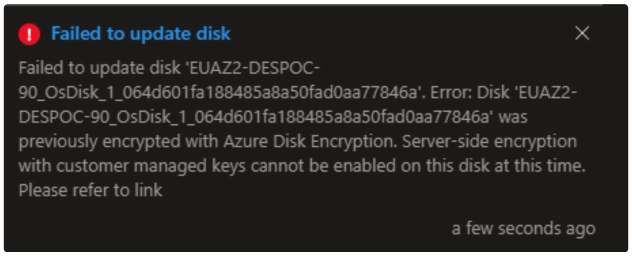
Failed to update disk 'disk-despoc-nprod-ne-001'. Error: Disk 'disk-despoc-nprod-ne-001' was previously encrypted with Azure Disk Encryption. Server-side encryption with customer managed keys cannot be enabled on this disk at this time. Please refer to link

18 minutes ago

Failed to update disk

Failed to update disk 'disk-despoc-nprod-ne-001'. Error: Disk 'disk-despoc-nprod-ne-001' was previously encrypted with Azure Disk Encryption. Server-side encryption with customer managed keys cannot be enabled on this disk at this time. Please refer to link

18 minutes ago



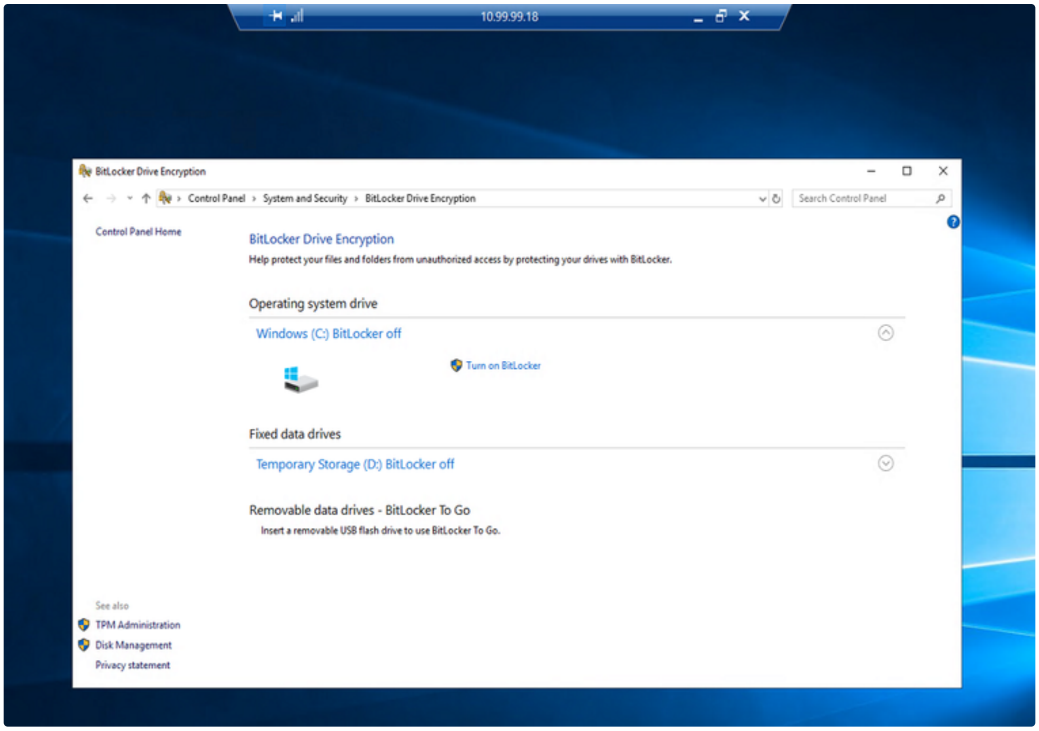
Failed to update disk

Failed to update disk 'EUAZ2-DESPOC-90_OsDisk_1_064d601fa188485a8a50fad0aa77846a'. Error: Disk 'EUAZ2-DESPOC-90_OsDisk_1_064d601fa188485a8a50fad0aa77846a' was previously encrypted with Azure Disk Encryption. Server-side encryption with customer managed keys cannot be enabled on this disk at this time. Please refer to link

a few seconds ago

Tried the following to bypass the issue:

1. Created a snapshot from the Disk and recreated VM from scratch > Same error, Azure identified the disk as previously encrypted by ADE
2. Enabled ADE encryption on the Disk again and disabled it using powershell first, then removed Encryption Extension > Same error as the beginning.
3. Disabled BitLocker on the Gest VM


10.99.99.18
BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Windows (C:) BitLocker off

Turn on BitLocker

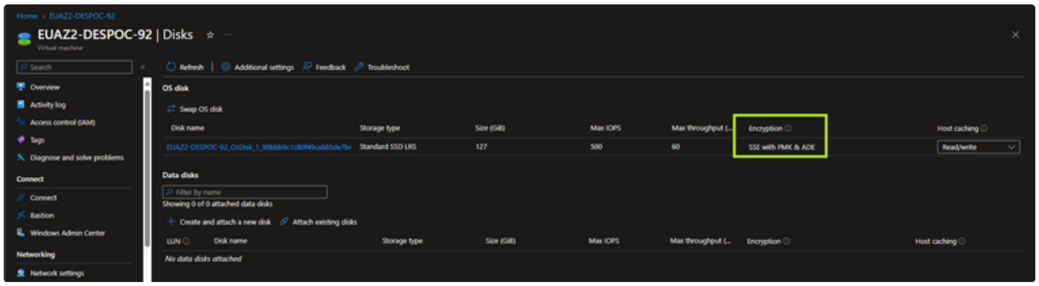
Fixed data drives

Temporary Storage (D:) BitLocker off

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

VM still appearing as using “ADE” encryption



OS disk

Swap OS disk

Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption	Host caching
EUAZ2-DESPOC-92_OsDisk_1_90bbb9c1c80f49ca885de7b4	Standard SSD LRS	127	500	60	SSE with PMK & ADE	Read/write

Data disks

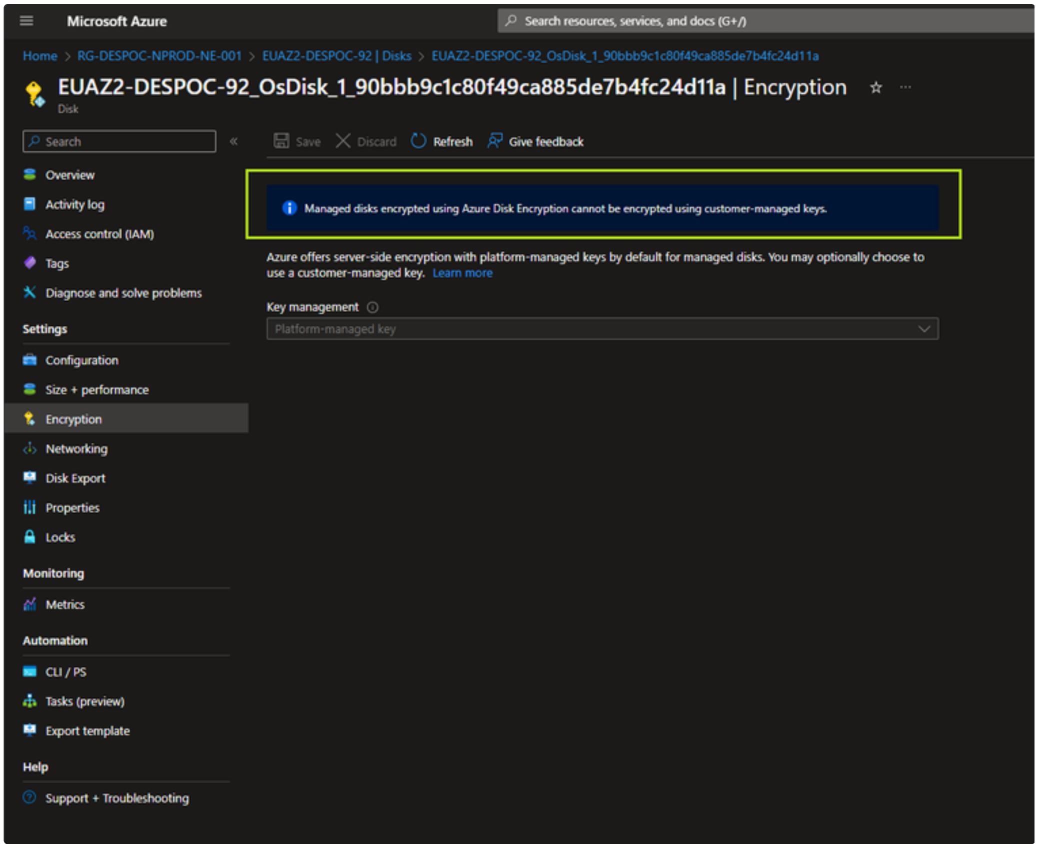
Filter by name

Showing 0 of 0 attached data disks

Create and attach a new disk   Attach existing disks

LUN	Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption	Host caching
No data disks attached							

Tried to disable ADE encryption but not possible. When checking Key management on the disk:



EUAZ2-DESPOC-92_OsDisk_1_90bbb9c1c80f49ca885de7b4fc24d11a | Encryption

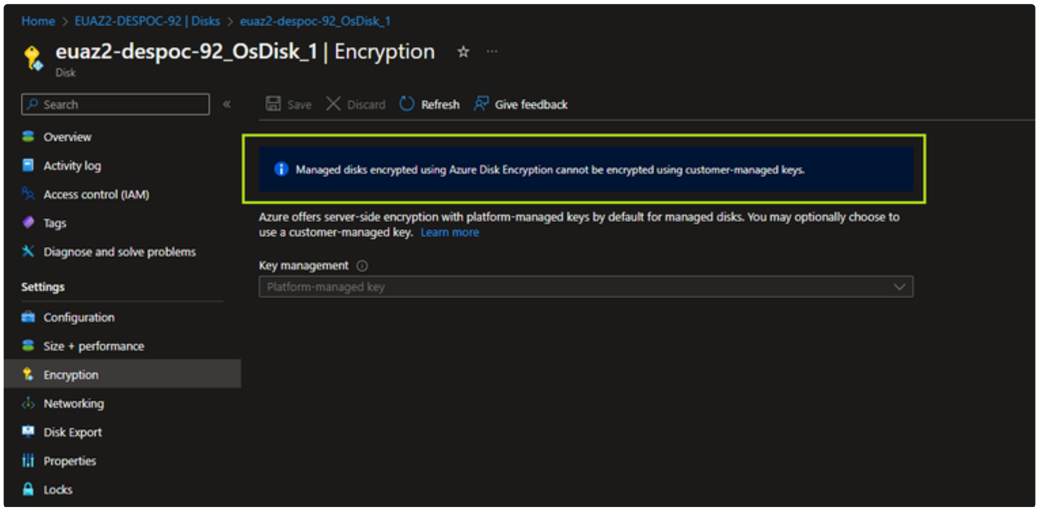
Disk

Managed disks encrypted using Azure Disk Encryption cannot be encrypted using customer-managed keys.

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. Learn more

Key management: Platform-managed key

Also, created snapshot from the disk once BitLocker was disabled but still showing same message:



euaz2-despoc-92_OsDisk_1 | Encryption

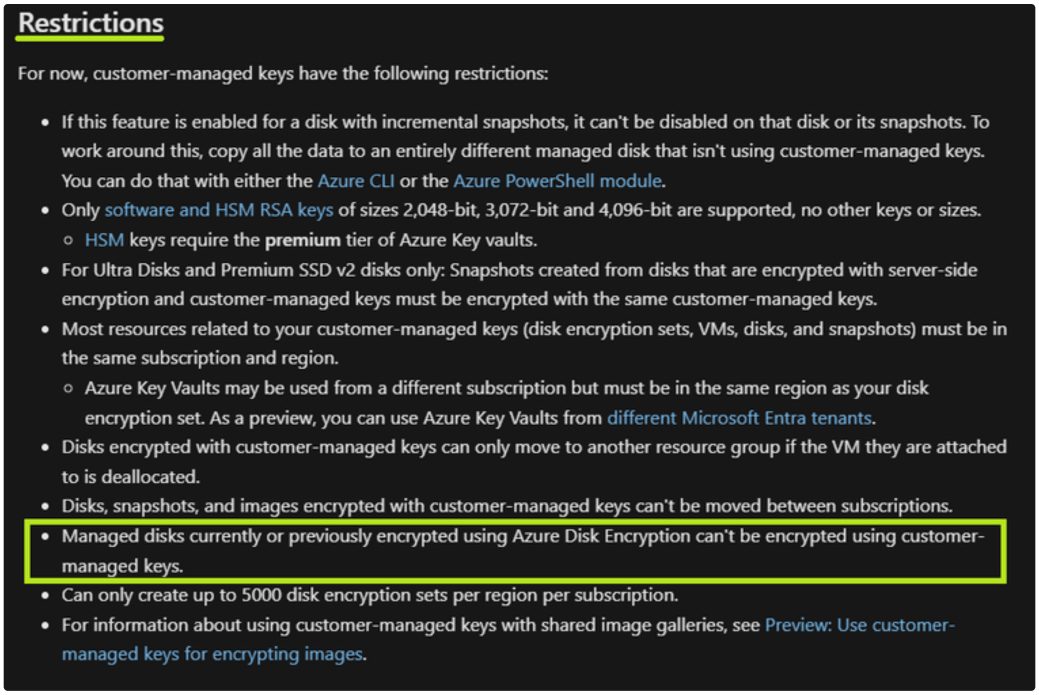
Disk

Managed disks encrypted using Azure Disk Encryption cannot be encrypted using customer-managed keys.

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. Learn more

Key management: Platform-managed key

Found out evidence of this behavior on the following restriction list on **Disk Encryption Set** (Server-side encryption of Azure managed disks - Azure Virtual Machines)

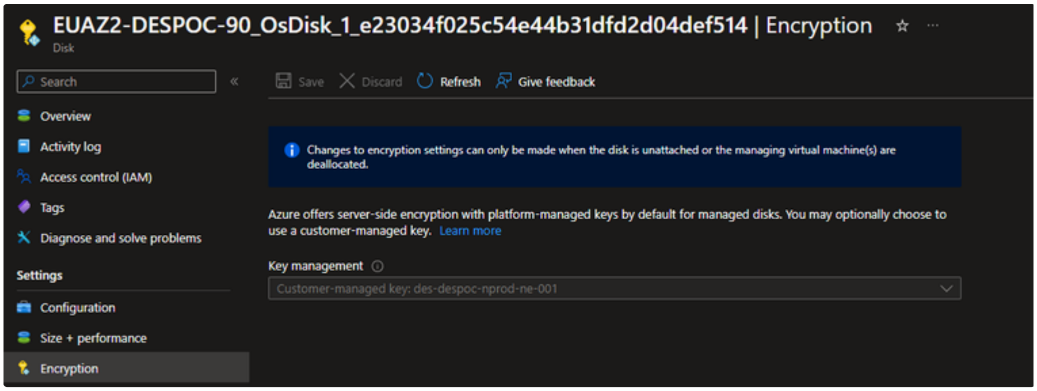


Restrictions

For now, customer-managed keys have the following restrictions:

- If this feature is enabled for a disk with incremental snapshots, it can't be disabled on that disk or its snapshots. To work around this, copy all the data to an entirely different managed disk that isn't using customer-managed keys. You can do that with either the Azure CLI or the Azure PowerShell module.
- Only software and HSM RSA keys of sizes 2,048-bit, 3,072-bit and 4,096-bit are supported, no other keys or sizes.
  - HSM keys require the **premium** tier of Azure Key vaults.
- For Ultra Disks and Premium SSD v2 disks only: Snapshots created from disks that are encrypted with server-side encryption and customer-managed keys must be encrypted with the same customer-managed keys.
- Most resources related to your customer-managed keys (disk encryption sets, VMs, disks, and snapshots) must be in the same subscription and region.
  - Azure Key Vaults may be used from a different subscription but must be in the same region as your disk encryption set. As a preview, you can use Azure Key Vaults from different Microsoft Entra tenants.
- Disks encrypted with customer-managed keys can only move to another resource group if the VM they are attached to is deallocated.
- Disks, snapshots, and images encrypted with customer-managed keys can't be moved between subscriptions.
- Managed disks currently or previously encrypted using Azure Disk Encryption can't be encrypted using customer-managed keys.
- Can only create up to 5000 disk encryption sets per region per subscription.
- For information about using customer-managed keys with shared image galleries, see Preview: Use customer-managed keys for encrypting images.

3.Create new Disk with Disk Encryption Set and rotate the encryption key

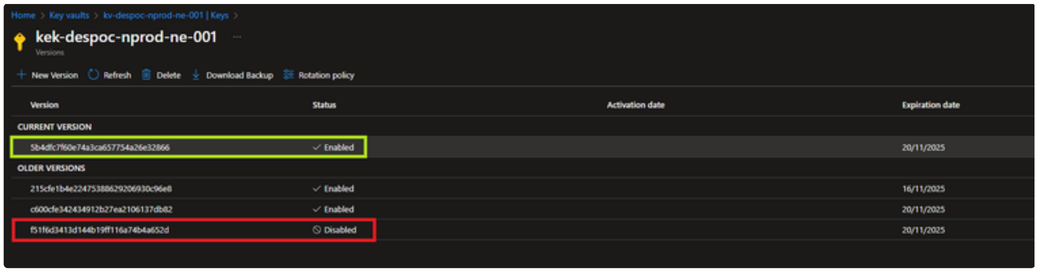


Changes to encryption settings can only be made when the disk is unattached or the managing virtual machine(s) are deallocated.

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. Learn more

Key management: Customer-managed key: des-despoc-nprod-ne-001

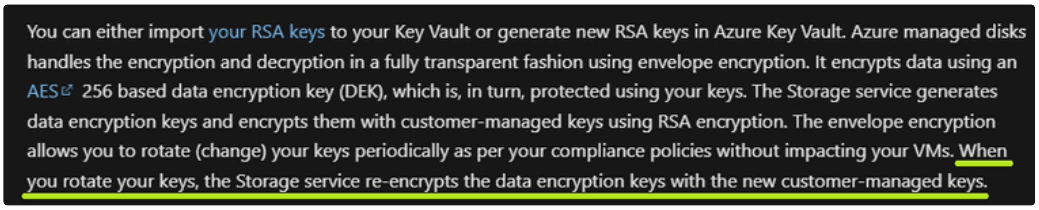
Original key used to encrypt (red and disabled), current key for encryption after several rotations (green and enabled



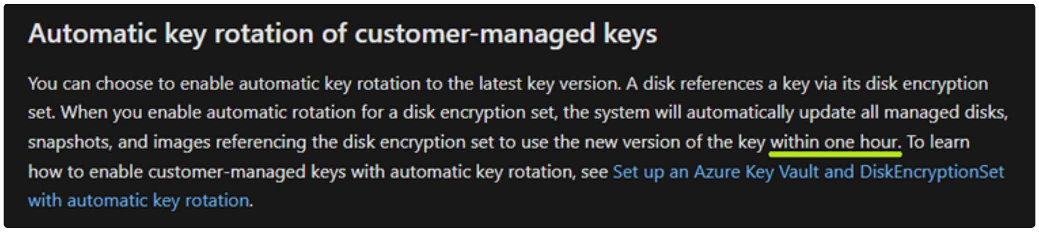
Home > Key vaults > kv-despoc-nprod-ne-001 | Keys >
kek-despoc-nprod-ne-001 ···
Versions
New Version
Refresh
Delete
Download Backup
Rotation policy

Version	Status	Activation date	Expiration date
CURRENT VERSION			
5b4dfc7f60e74a3ca657754a26e32866	✓ Enabled		20/11/2025
OLDER VERSIONS			
215cfe1b4e22475388629206930c96e8	✓ Enabled		16/11/2025
c600cfe342434912b27ea2106137db82	✓ Enabled		20/11/2025
f51f6d3413d144b19ff116a74b4a652d	⊘ Disabled		20/11/2025

Expected behavior after rotating the keys:



You can either import your RSA keys to your Key Vault or generate new RSA keys in Azure Key Vault. Azure managed disks handles the encryption and decryption in a fully transparent fashion using envelope encryption. It encrypts data using an AES 256 based data encryption key (DEK), which is, in turn, protected using your keys. The Storage service generates data encryption keys and encrypts them with customer-managed keys using RSA encryption. The envelope encryption allows you to rotate (change) your keys periodically as per your compliance policies without impacting your VMs. When you rotate your keys, the Storage service re-encrypts the data encryption keys with the new customer-managed keys.

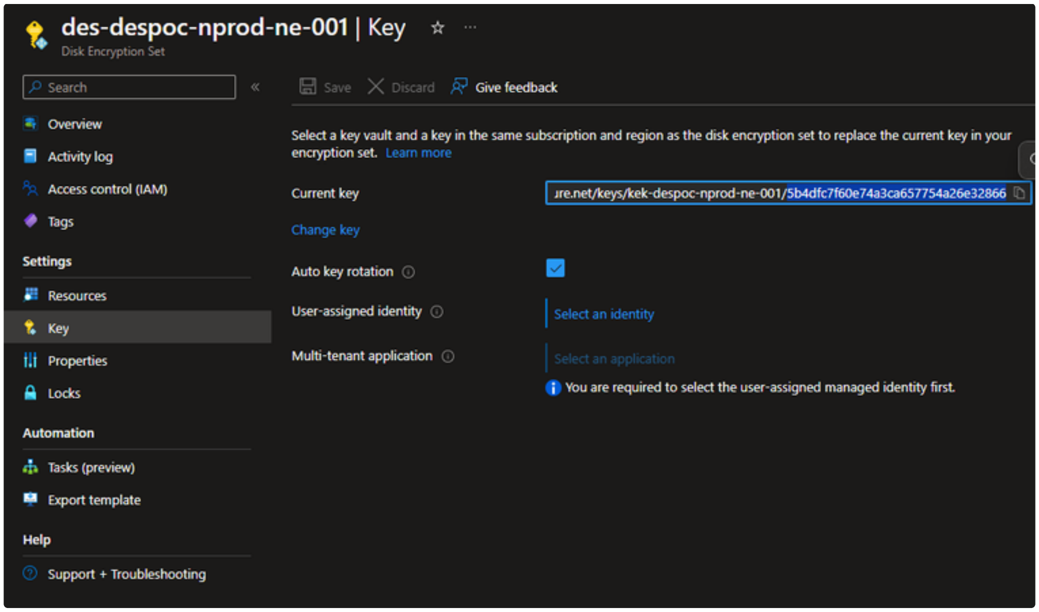


Automatic key rotation of customer-managed keys

You can choose to enable automatic key rotation to the latest key version. A disk references a key via its disk encryption set. When you enable automatic rotation for a disk encryption set, the system will automatically update all managed disks, snapshots, and images referencing the disk encryption set to use the new version of the key within one hour. To learn how to enable customer-managed keys with automatic key rotation, see Set up an Azure Key Vault and DiskEncryptionSet with automatic key rotation.

What actually happened:

- If the VM is up and running, will continue the same, no interruptions
- If the VM is powered off when the rotation happened, 1hour awaiting will be required (disk is re-encrypted)
- DEK (Data Encryption Key) or **data key** which remains the same in the process, is not visible at any level
- KEK (Key Encryption Key) or **master key**, used to encrypt **data key**, is safe into the Key Vault; manual or auto-rotation is possible. Also is possible to change KEK that is using Disk Encryption Set.



des-despoc-nprod-ne-001 | Key

Disk Encryption Set

Select a key vault and a key in the same subscription and region as the disk encryption set to replace the current key in your encryption set. Learn more

Current key: ure.net/keys/kek-despoc-nprod-ne-001/5b4dfc7f60e74a3ca657754a26e32866

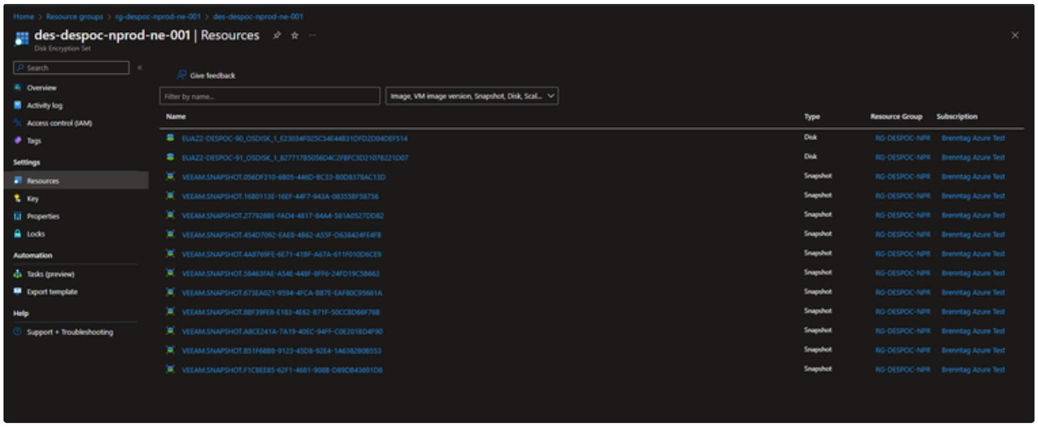
Change key

Auto key rotation ☑

User-assigned identity: Select an identity

Multi-tenant application: Select an application

You are required to select the user-assigned managed identity first.



Home > Resource groups > rg-despoc-nprod-ne-001 > des-despoc-nprod-ne-001

des-despoc-nprod-ne-001 | Resources

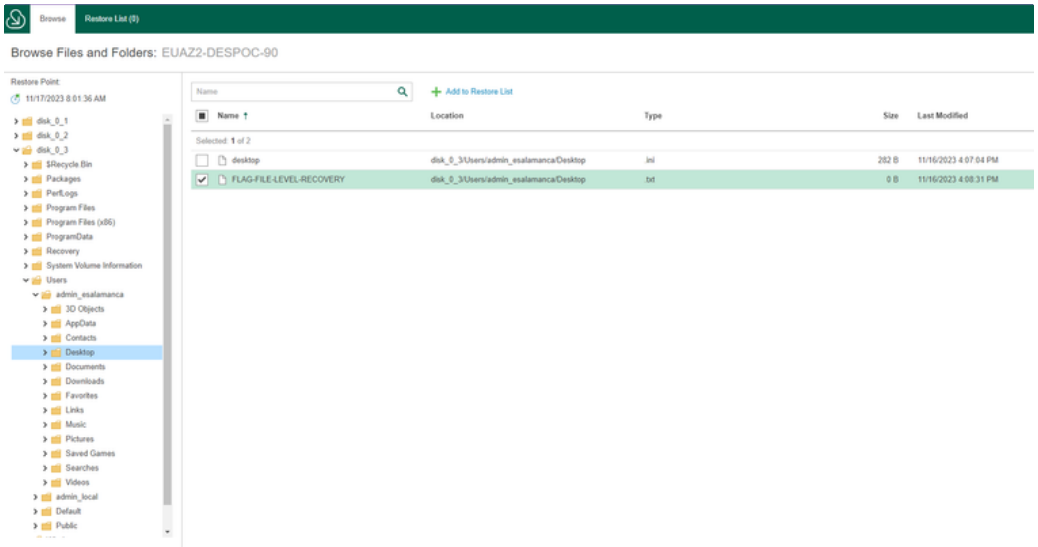
Disk Encryption Set

Image, VM image version, Snapshot, Disk, Scal...

Name	Type	Resource Group	Subscription
EUAZ2-DESPOC-90_OSDISK_1_E23034F025C54E44831DFD2D04DEF514	Disk	RG-DESPOC-NPR	Brenntag Azure Test
EUAZ2-DESPOC-91_OSDISK_1_82771785056D4C2FBFC3D2107B221D07	Disk	RG-DESPOC-NPR	Brenntag Azure Test
VEEAM.SNAPSHOT.056DF310-6805-446D-8C33-B0D8378AC13D	Snapshot	RG-DESPOC-NPR	Brenntag Azure Test
VEEAM.SNAPSHOT.1680113E-16EF-44F7-943A-083558F58756	Snapshot	RG-DESPOC-NPR	Brenntag Azure Test
VEEAM.SNAPSHOT.2779288E-FAD4-4817-84A4-581A0527DD82	Snapshot	RG-DESPOC-NPR	Brenntag Azure Test
VEEAM.SNAPSHOT.454D7092-EAE8-4862-A55F-D638424FE4F8	Snapshot	RG-DESPOC-NPR	Brenntag Azure Test
VEEAM.SNAPSHOT.4A8769FE-6E71-418F-A67A-611F010D6CE9	Snapshot	RG-DESPOC-NPR	Brenntag Azure Test
VEEAM.SNAPSHOT.58463FAE-A54E-448F-8FF6-24FD19C58663	Snapshot	RG-DESPOC-NPR	Brenntag Azure Test
VEEAM.SNAPSHOT.673EA021-9594-4FCA-887E-EAF80C95661A	Snapshot	RG-DESPOC-NPR	Brenntag Azure Test
VEEAM.SNAPSHOT.88F39FE8-E183-4E62-871F-50CCBD66F768	Snapshot	RG-DESPOC-NPR	Brenntag Azure Test
VEEAM.SNAPSHOT.A8CE241A-7A19-40EC-94FF-C0E201BD4F90	Snapshot	RG-DESPOC-NPR	Brenntag Azure Test
VEEAM.SNAPSHOT.851F6888-9123-45D8-92E4-1A6382808553	Snapshot	RG-DESPOC-NPR	Brenntag Azure Test
VEEAM.SNAPSHOT.F1C8EE85-62F1-4681-9088-D89D843691D8	Snapshot	RG-DESPOC-NPR	Brenntag Azure Test

4.Check if single file restore works using DES

Results for a single test file restore using Veeam Backup for Azure ✅

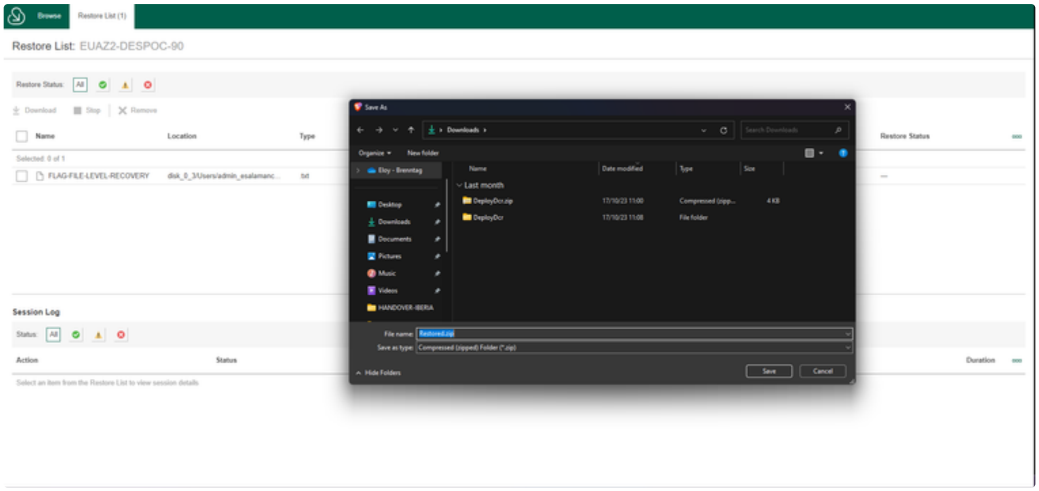


Browse Files and Folders: EUAZ2-DESPOC-90

Restore Point:
11/17/2023 8:01:36 AM

Selected: 1 of 2

	Name	Location	Type	Size	Last Modified
□	desktop	disk_0_3/Users/admin_esalamanca/Desktop	.ini	282 B	11/16/2023 4:07:04 PM
☑	FLAG-FILE-LEVEL-RECOVERY	disk_0_3/Users/admin_esalamanca/Desktop	.txt	0 B	11/16/2023 4:08:31 PM



Restore List: EUAZ2-DESPOC-90

Selected: 0 of 1

	Name	Location	Type	Restore Status
□	FLAG-FILE-LEVEL-RECOVERY	disk_0_3/Users/admin_esalamanc...	.txt	—

Last month

Name	Date modified	Type	Size
DeployDcr.zip	17/10/23 11:00	Compressed (zipp...	4 KB
DeployDcr	17/10/23 11:08	File folder	

File name: Restored.zip

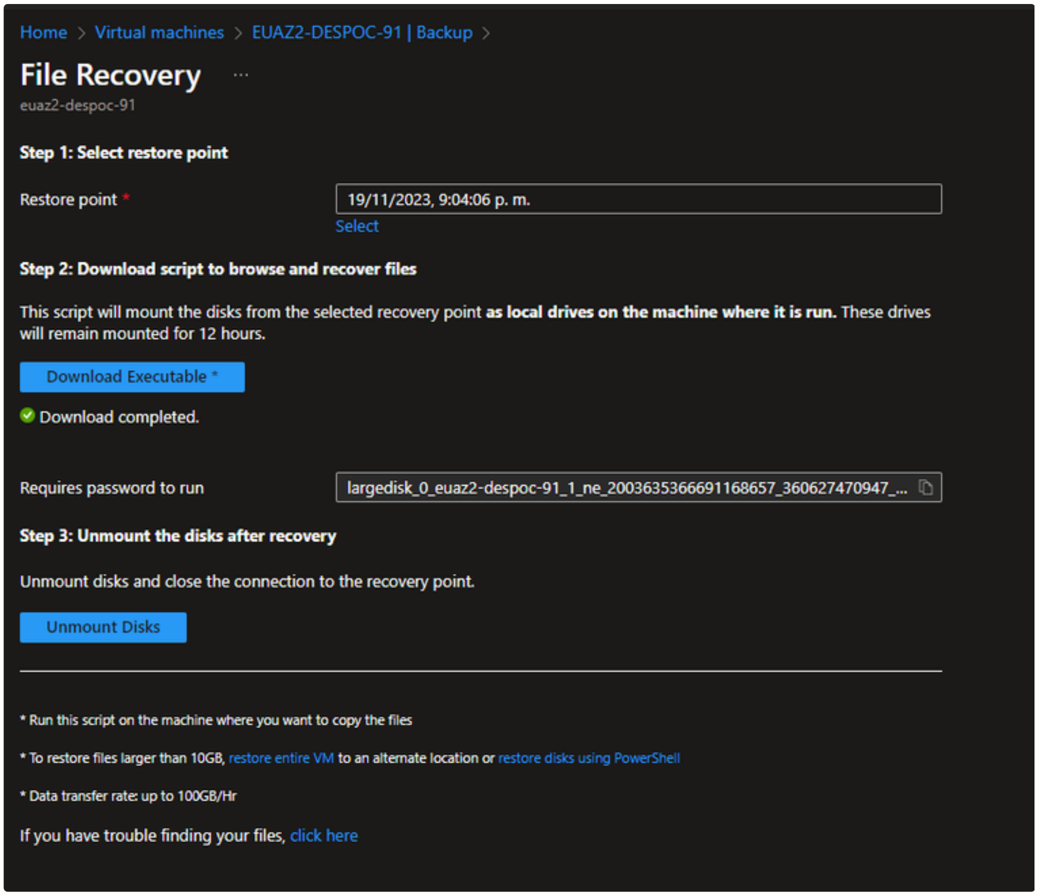
Save as type: Compressed (zipped) Folder (*.zip)

Session Log

Action	Status	Duration

Select an item from the Restore List to view session details

Results for a single test file restore using Azure Backup ✓



File Recovery ...

euaz2-despoc-91

Step 1: Select restore point

Restore point * 19/11/2023, 9:04:06 p. m.

Step 2: Download script to browse and recover files

This script will mount the disks from the selected recovery point **as local drives on the machine where it is run.** These drives will remain mounted for 12 hours.

Download completed.

Requires password to run largedisk_0_euaz2-despoc-91_1_ne_2003635366691168657_360627470947_...

Step 3: Unmount the disks after recovery

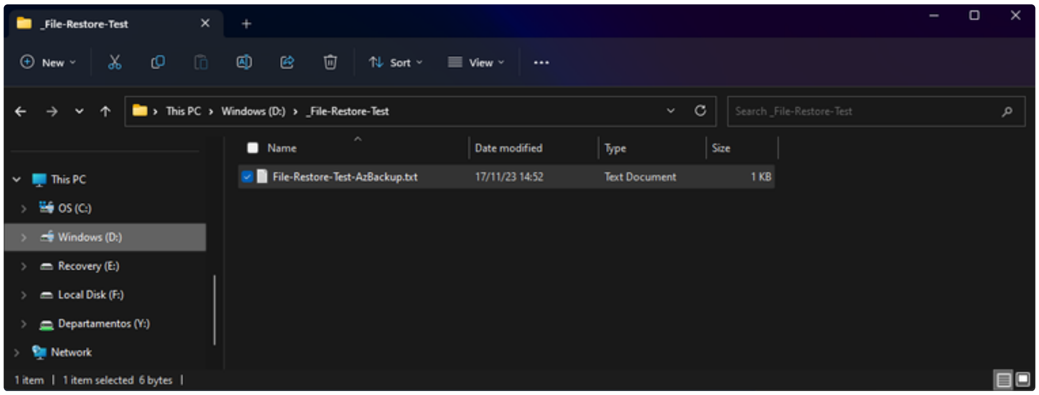
Unmount disks and close the connection to the recovery point.

* Run this script on the machine where you want to copy the files

* To restore files larger than 10GB, restore entire VM to an alternate location or restore disks using PowerShell

* Data transfer rate: up to 100GB/Hr

If you have trouble finding your files, click here



Name	Date modified	Type	Size
File-Restore-Test-AzBackup.txt	17/11/23 14:52	Text Document	1 KB

1 item | 1 item selected 6 bytes |

Decision Outcomes

- Disk Encryption Sets it’s the way of getting Disks encrypted because:
  - Allows single file-level restores natively, for any Backup platform
  - Fully support for encryption key auto-rotation

In practice

Migration Plan for the current VMs: For those VMs already encrypted by ADE (Azure Disk Encryption), there are only 2 options:

1. Re-create VMs from scratch, use Disk Encryption Sets for encryption
2. Use the disks unencrypted