

Secure Windows Server Storage



Tim Warner

Microsoft Azure Solutions Architect

@TechTrainerTim TechTrainerTim.com



Overview



Manage Windows BitLocker Drive Encryption (BitLocker)

Manage and recover encrypted volumes

Enable storage encryption by using Azure Disk Encryption

Manage disk encryption keys for IaaS virtual machines



Windows Server 2022: Secure On-premises and Hybrid Infrastructure

Secure the Windows Server Operating System

Secure Hybrid Active Directory Accounts

Configure Hybrid Active Directory Account Security

Remediate Windows Server Security Issues with Azure Services

Secure Windows Server Networking

Secure Windows Server Storage



BitLocker Drive Encryption



BitLocker Drive Encryption

**At rest volume
encryption**

**128/256-bit AES
encryption**

Data privacy

Startup integrity

**Network Unlock for
remote servicing**

**Available for
Windows Server,
Windows Client,
Azure VMs**



Microsoft BitLocker Administration and Monitoring (MBAM)

← →

MBAM SSP Recovery

Get a BitLocker Recovery Key

Use this page if you are locked out of Windows by BitLocker and need to get a BitLocker Recovery Key to regain access to Windows.

NOTE: For security reasons, **your session will expire after 5 minute(s) of inactivity.** You will need to re-enter your information into the form on this page.

1 Enter a BitLocker Key ID

This 32-digit code should be displayed on the BitLocker recovery screen on your computer. Enter a minimum of 8 characters.

Recovery Key ID

Reason

Get Key

2 Your BitLocker Recovery Key

Enter this 48-digit code into the BitLocker recovery screen on your computer.

Learn About

- [What is BitLocker?](#)
- [What is a Key ID?](#)
- [Managing my BitLocker PIN](#)

For all other related issues,
[Contact Helpdesk or IT department.](#)

**End of "extended" support:
July 9, 2024**

AD BitLocker Key Recovery



**Store BitLocker recovery key
in Active Directory**



**Optionally store key package
for restoration scenarios**



**BitLocker Recovery Password
Viewer**

WIN-7Q5QEKE6MRQ Properties

General Operating System Member Of Delegation Location
Managed By Dial-in BitLocker Recovery

BitLocker Recovery Passwords:

Date Added	Password ID
2017-03-05 16:02	07A326F2-DE1A-40EE-AAB2-DFB08182358A

Details:

Recovery Password:
687071-443553-114884-079519-
352000-577181-253946-354332

Computer: WIN-7Q5QEKE6MRQ.example.com
Date: 2017-03-05 16:02:09 -0800
Password ID: 07A326F2-DE1A-40EE-AAB2-DFB08182358A

OK Cancel Apply Help



Demo



1

BitLocker setup

AD key escrow

Recovery process



Azure Disk Encryption



Azure Disk Encryption (ADE)



BitLocker solution for Windows VMs in Azure

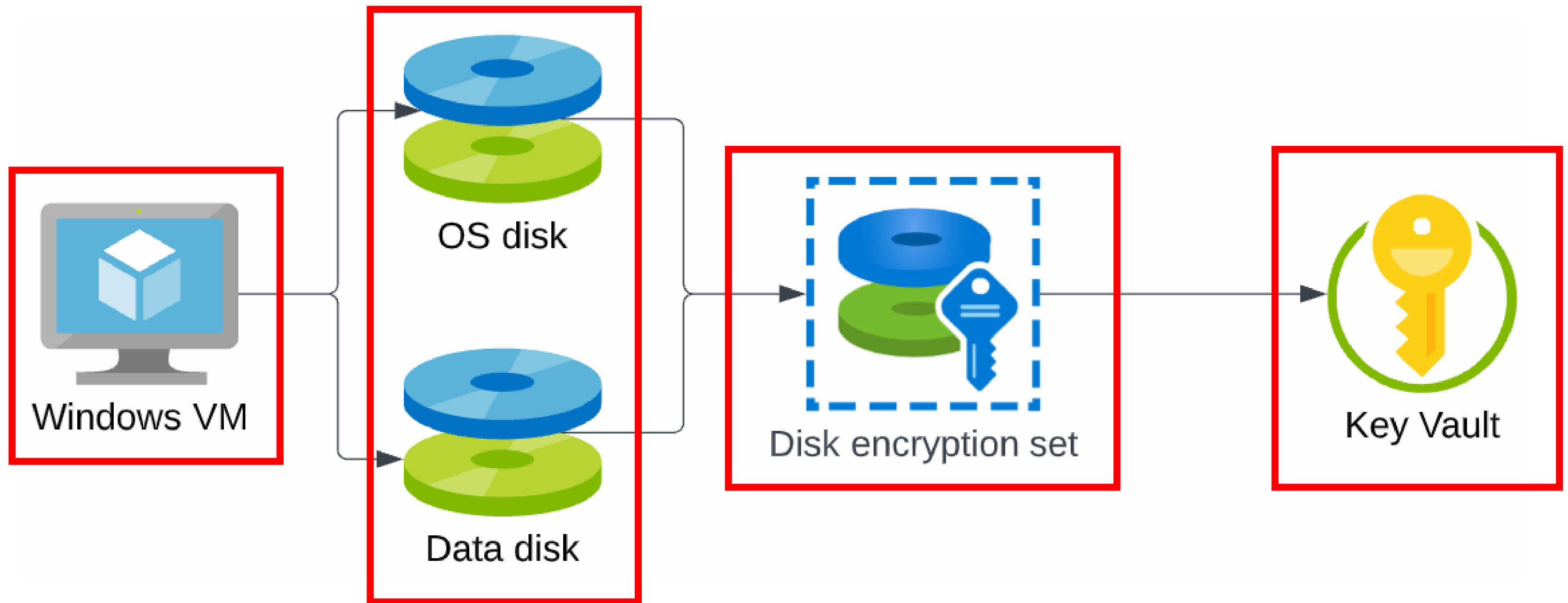
Recovery key stored in Azure Key Vault

Azure VMs must be configured to allow a 256-bit recovery key

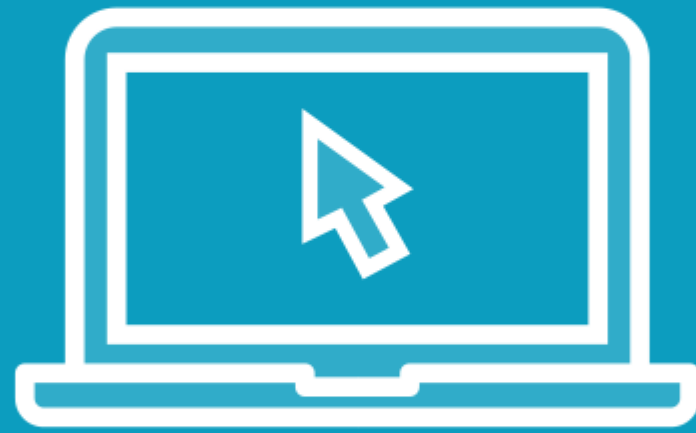
For domain-joined VMs, do not push GPO that specifies TPM enforcement



Azure Disk Encryption (ADE) Components



Demo



2

Key Vault

Disk Encryption Set

Configure ADE

View / back up key



Summary



You should think about data security in all its states:

- At rest
- In transit
- In use

Thanks!

Pluralsight courses: timw.info/ps

Website: timw.info

Email: tim@timw.info

