Introduction

3 minutes

Suppose you work for a warehouse company that's transitioning to the cloud. Currently, you use a hybrid environment consisting of on-premises Windows servers, Azure Virtual Machines (VMs), and Azure Active Directory. Your company has developed a custom in-house business-to-business (B2B) infrastructure, supporting secure order management with your suppliers. Some of your suppliers use Linux servers, and you run several Linux servers in Azure to support these suppliers.

Your security policies mandate that data must be encrypted using your own encryption keys, and that your company is responsible for managing these keys.

Your admin team already uses PowerShell for on-premises server management. You'll deploy and test many Azure VMs, and intend to use Azure Resource Manager templates to automate this process.

Here, we'll look at the types of protection available for VM disks, so you can decide if Azure Disk Encryption (ADE) is the best choice for a given scenario. We'll then enable ADE on existing VM disks, and use templates to enable ADE for new VM deployments.

Learning objectives

In this module, you will:

- Determine which encryption method is best for your VM
- Encrypt existing VM disks using the Azure portal
- Encrypt existing VM disks using PowerShell
- Modify Azure Resource Manager templates to automate disk encryption on new VMs

Next unit: Encryption options for protecting Windows and Linux VMs

Continue >

‹ Previous Unit 2 of 7 ⌄ Next ›

✓ 100 XP

Encryption options for protecting Windows and Linux VMs

8 minutes

Suppose your company's trading partners have security policies who require their trading data is protected with strong encryption. You use a B2B application that runs on your Windows servers, and stores data on the server data disk. Now that you're transitioning to the cloud, you need to demonstrate to your trading partners that data stored on your Azure VMs cannot be accessed by unauthorized users, devices, or applications. You need to decide on a strategy for implementing encryption of your B2B data.

Your audit requirements dictate that your encryption keys be managed in-house, and not by any third party. You're also concerned that the performance and manageability of your Azure-based servers is maintained. So before you implement encryption, you want to be sure that there won't be a performance hit.

What is encryption?

Encryption is about converting meaningful information into something that appears meaningless, such as a random sequence of letters and numbers. The process of encryption uses some form of **key** as part of the algorithm that creates the encrypted data. A key is also needed to perform the decryption. Keys may be ***symmetric***, where the same key is used for encryption and decryption, or ***asymmetric***, where different keys are used. An example of the latter is the **public-private** key pairs used in digital certificates.

Symmetric encryption

Algorithms that use symmetric keys, such as Advanced Encryption Standard (AES), are typically faster than public key algorithms, and are often used for protecting large data stores. Because there's only one key, procedures must be in place to prevent the key from becoming publicly known.

Asymmetric encryption

With asymmetric algorithms, only the private key member of the pair must be kept private and secure; as its name suggests, the public key can be made available to anyone without compromising the encrypted data. The downside of public key algorithms, however, is that they're much slower than symmetric algorithms, and cannot be used to encrypt large amounts of data.

Key management

In Azure, your encryption keys can be managed by Microsoft or the customer. Often the demand for customer-managed keys comes from organizations that need to demonstrate compliance with HIPAA, or other regulations. Such compliance may require that access to keys is logged, and that regular key changes are made and recorded.

Azure disk encryption technologies

The main encryption-based disk protection technologies for Azure VMs are:

- Storage Service Encryption (SSE)
- Azure Disk Encryption (ADE)

Storage Service Encryption is performed on the physical disks in the data center. If someone were to directly access the physical disk the data would be encrypted. When the data is accessed from the disk, it is decrypted and loaded into memory.

Azure Disk Encryption encrypts the virtual machine's virtual hard disks (VHDs). If VHD is protected with ADE, the disk image will only be accessible by the virtual machine that owns the disk.

It's possible to use both services to protect your data.

Storage Service Encryption

Azure Storage Service Encryption (SSE) is an encryption service built into Azure used to protect data at rest. The Azure storage platform automatically encrypts data before it's stored to several storage services, including Azure Managed Disks. Encryption is enabled by default using 256-bit AES encryption, and is managed by the storage account administrator.

Storage Service Encryption is enabled for all new and existing storage accounts and cannot be disabled. Your data is secured by default; you don't need to modify your code or applications to take advantage of Storage Service Encryption.

Storage Service Encryption does not affect the performance of Azure storage services.

Azure Disk Encryption

Azure Disk Encryption (ADE) is managed by the VM owner. It controls the encryption of Windows and Linux VM-controlled disks, using **BitLocker** on Windows VMs and **DM-Crypt** on Linux VMs. BitLocker Drive Encryption is a data protection feature that integrates with the operating system, and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. Similarly, DM-Crypt encrypts data at rest for Linux before writing to storage.

ADE ensures that all data on VM disks are encrypted at rest in Azure storage, and ADE is required for VMs backed up to the Recovery Vault.

With ADE, VMs boot under customer-controlled keys and policies. ADE is integrated with Azure Key Vault for the management of these disk-encryption keys and secrets.

> ⓘ **Note**
>
> ADE does not support the encryption of Basic tier VMs, and you cannot use an on-premises Key Management Service (KMS) with ADE.

When to use encryption?

Computer data is at risk when it's in transit (transmitted across the Internet or other network), and when it's at rest (saved to a storage device). The at-rest scenario is the primary concern when protecting data on Azure VM disks. For example, someone might download the Virtual Hard Disk (VHD) file associated with an Azure VM, and save it on their laptop. If the VHD is not encrypted, the contents of the VHD are potentially accessible to anyone who can mount the VHD file on their computer.

For operating system (OS) disks, data such as passwords are encrypted automatically, so even if the VHD is not itself encrypted, it's not easy for such information to be accessed. Applications may also automatically encrypt their own data. However, even with such protections, if someone with malicious intent were to gain access to a data disk, and the disk itself was not encrypted, they might then be in a position to exploit any known weaknesses in that application's data protection. With disk encryption in place, such exploits are not possible.

Storage Service Encryption (SSE) is part of Azure itself, and there should be no noticeable performance impact on the VM disk IO when using SSE. Managed disks with SSE are now the default, and there should be no reason to change it. Azure Disk Encryption (ADE) makes use of VM operating system tools (BitLocker and DM-Crypt), so the VM itself has to do some work when encryption or decryption on VM disks is being performed. The impact of this additional VM CPU activity is typically negligible, except in certain situations. For instance, if you have a CPU-intensive application, there may be a case for leaving the OS disk unencrypted to maximize performance. In a situation such as this, you can store application data on a separate encrypted data disk, getting you the performance you need without compromising security.

Azure provides two complementary encryption technologies that are used to secure Azure VM disks. These technologies, SSE and ADE, encrypt at different layers, and serve different purposes. Both use AES 256-bit encryption. Using both technologies provides a defense-in-depth protection against unauthorized access to your Azure storage, and to specific VHDs.

Next unit: Encrypt existing VM disks

Continue >

✓ 100 XP ▶

Encrypt existing VM disks

10 minutes

Suppose your company has decided to implement Azure Disk Encryption (ADE) across all VMs. You need to evaluate how to roll out encryption to existing VM volumes. Here, we'll look at the requirements for ADE, and the steps involved in encrypting disks on existing Linux and Windows VMs.

Azure Disk Encryption prerequisites

Before you can encrypt your VM disks, you need to:

1. Create a key vault.
2. Set the key vault access policy to support disk encryption.
3. Use the key vault to store the encryption keys for ADE.

Azure Key Vault

The encryption keys used by ADE can be stored in Azure Key Vault. Azure Key Vault is a tool for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, or certificates. This provides highly available and scalable secure storage, as defined in Federal Information Processing Standards (FIPS) 140-2 Level 2 validated Hardware Security Modules (HSMs). Using Key Vault, you keep full control of the keys used to encrypt your data, and you can manage and audit your key usage.

> ⓘ **Note**
>
> Azure Disk Encryption requires that your key vault and your VMs are in the same Azure region; this ensures that encryption secrets do not cross regional boundaries.

You can configure and manage your key vault with:

Powershell

```PowerShell
New-AzKeyVault -Location <location> `
    -ResourceGroupName <resource-group> `
    -VaultName "myKeyVault" `
    -EnabledForDiskEncryption
```

Azure CLI

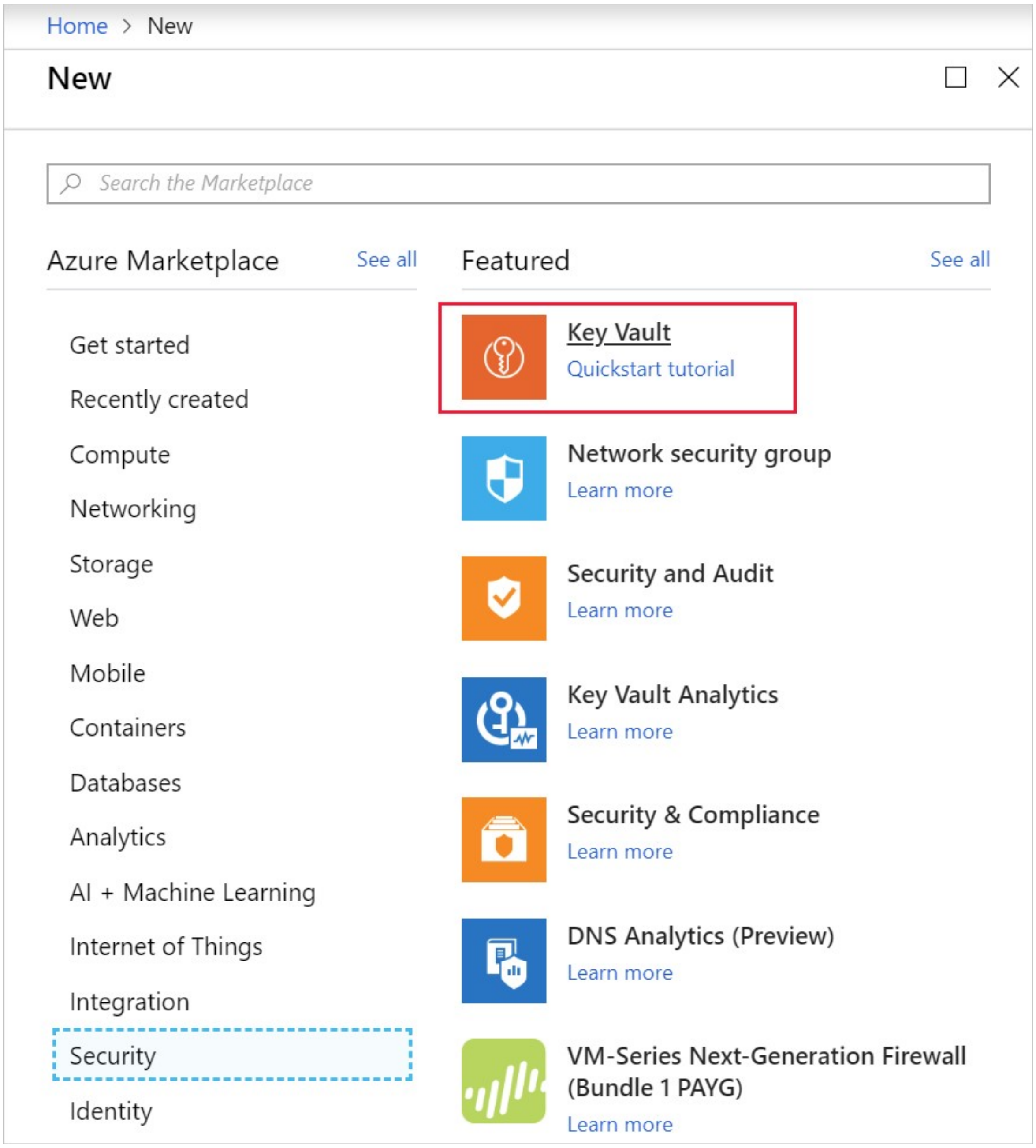
```Azure CLI
az keyvault create \
    --name "myKeyVault" \
    --resource-group <resource-group> \
    --location <location> \
    --enabled-for-disk-encryption True
```

Azure portal

An Azure Key Vault is a resource that can be created in the Azure portal using the normal resource creation process.

1. On the Azure portal menu or from the **Home** page, select **Create a resource**.

2. Search for "Key vault". Click **Create** in the details window.



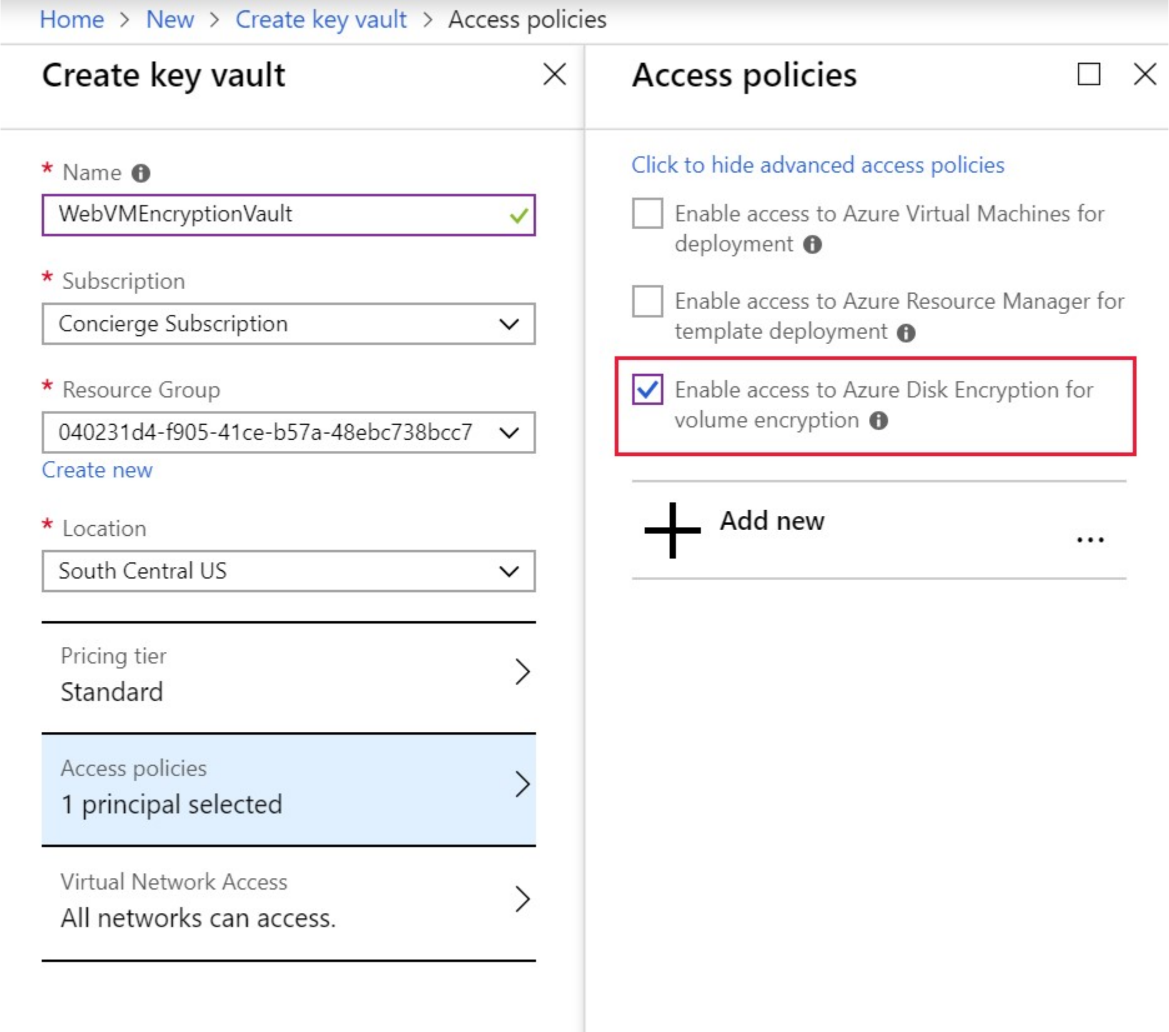
3. Enter the details for the new Key Vault:

    - Enter a **Name** for the Key Vault
    - Select the subscription to place it in (defaults to your current subscription).
    - Select a **Resource Group**, or create a new resource group to own the Key Vault.
    - Select a **Location** for the Key Vault. Make sure to select the location the VM is in.

- You can choose either Standard or Premium for the pricing tier. The main difference is that the premium tier allows for Hardware-encryption backed keys.

4. You must change the Access policies to support Disk Encryption. By default it adds *your* account to the policy.

    - Select **Access policies**
    - Click **Advanced access policies**.
    - Check the **Enable access to Azure Disk Encryption for volume encryption**.
    - You can remove your account if you like, it's not necessary if you only intend to use the Key Vault for disk encryption.
    - Click **OK** to save the changes.



Home > New > Create key vault > Access policies

Create key vault

* Name: WebVMEncryptionVault

* Subscription: Concierge Subscription

* Resource Group: 040231d4-f905-41ce-b57a-48ebc738bcc7

Create new

* Location: South Central US

Pricing tier: Standard

Access policies: 1 principal selected

Virtual Network Access: All networks can access.

Access policies

Click to hide advanced access policies

□ Enable access to Azure Virtual Machines for deployment

□ Enable access to Azure Resource Manager for template deployment

☑ Enable access to Azure Disk Encryption for volume encryption

5. Click **Create** to create the new Key Vault.

Enabling access policies in the key vault

Azure needs access to the encryption keys or secrets in your key vault to make them available to the VM for booting and decrypting the volumes. We covered this for the portal when we changed the **Advanced access policies** above.

There are three policies you can enable.

1. **Disk encryption** - Required for Azure Disk encryption.
2. **Deployment** - (Optional) Enables the Microsoft.Compute resource provider to retrieve secrets from this key vault when this key vault is referenced in resource creation, for example when creating a virtual machine.
3. **Template deployment** - (Optional) Enables Azure Resource Manager to get secrets from this key vault when this key vault is referenced in a template deployment.

Here's how to enable the disk encryption policy. The other two are similar but use different flags.

PowerShell Copy

```powershell
Set-AzKeyVaultAccessPolicy -VaultName <keyvault-name> -ResourceGroupName
<resource-group> -EnabledForDiskEncryption
```

Azure CLI Copy

```
az keyvault update --name <keyvault-name> --resource-group <resource-group>
--enabled-for-disk-encryption "true"
```

Encrypting an existing VM disk

Once you have the Key Vault setup, you can encrypt the VM using either Azure CLI or Azure PowerShell. The first time you encrypt a Windows VM, you can choose to encrypt either all disks or the OS disk only. On some Linux distributions, only the data disks may be encrypted. To be eligible for encryption, your Windows disks must be formatted as NTFS volumes.

⚠ **Warning**

You must take a snapshot or a backup of managed disks before you can turn on encryption. The `SkipVmBackup` flag specified below tells the tool that the backup is complete on managed disks. Without the backup, you will be unable to recover the VM if the encryption fails for some reason.

With PowerShell, use the `Set-AzVmDiskEncryptionExtension` cmdlet to enable encryption.

PowerShell Copy

```
Set-AzVmDiskEncryptionExtension `
        -ResourceGroupName <resource-group> `
    -VMName <vm-name> `
    -VolumeType [All | OS | Data]
        -DiskEncryptionKeyVaultId <keyVault.ResourceId> `
        -DiskEncryptionKeyVaultUrl <keyVault.VaultUri> `
     -SkipVmBackup
```

For the Azure CLI, use the `az vm encryption enable` command to enable encryption.

Azure CLI Copy

```
az vm encryption enable \
    --resource-group <resource-group> \
    --name <vm-name> \
    --disk-encryption-keyvault <keyvault-name> \
    --volume-type [all | os | data] \
    --skipvmbackup
```

Viewing the status of the disk

You can check whether specific disks are encrypted or not.

PowerShell Copy

```
Get-AzVmDiskEncryptionStatus  -ResourceGroupName <resource-group> -VMName <vm-name>
```

Azure CLI

Copy

```
az vm encryption show --resource-group <resource-group> --name <vm-name>
```

Both of these commands will return the status of each disk attached to the specified VM.

Decrypting drives

You can reverse the encryption through PowerShell using `Disable-AzVMDiskEncryption`.

PowerShell

Copy

```
Disable-AzVMDiskEncryption -ResourceGroupName <resource-group> -VMName <vm-name>
```

For the Azure CLI, use the `vm encryption disable` command.

Azure CLI

Copy

```
az vm encryption disable --resource-group <resource-group> --name <vm-name>
```

These commands disable encryption for volumes of type all for the specified virtual machine. Just like the encrypt version, you can specify a `-VolumeType` parameter `[All | OS | Data]` to decide what disks to decrypt. It defaults to `All` if not supplied.

⚠ **Warning**

Disabling data disk encryption on Windows VM when both OS and data disks have been encrypted doesn't work as expected. You must disable encryption on all disks instead.

In the next exercise, you'll try some of these commands out on a new VM.

Next unit: Exercise - Encrypt existing VM disks

Continue >

✓ 100 XP ▶

Automate secure VM deployments by adding encryption to Azure Resource Manager templates

5 minutes

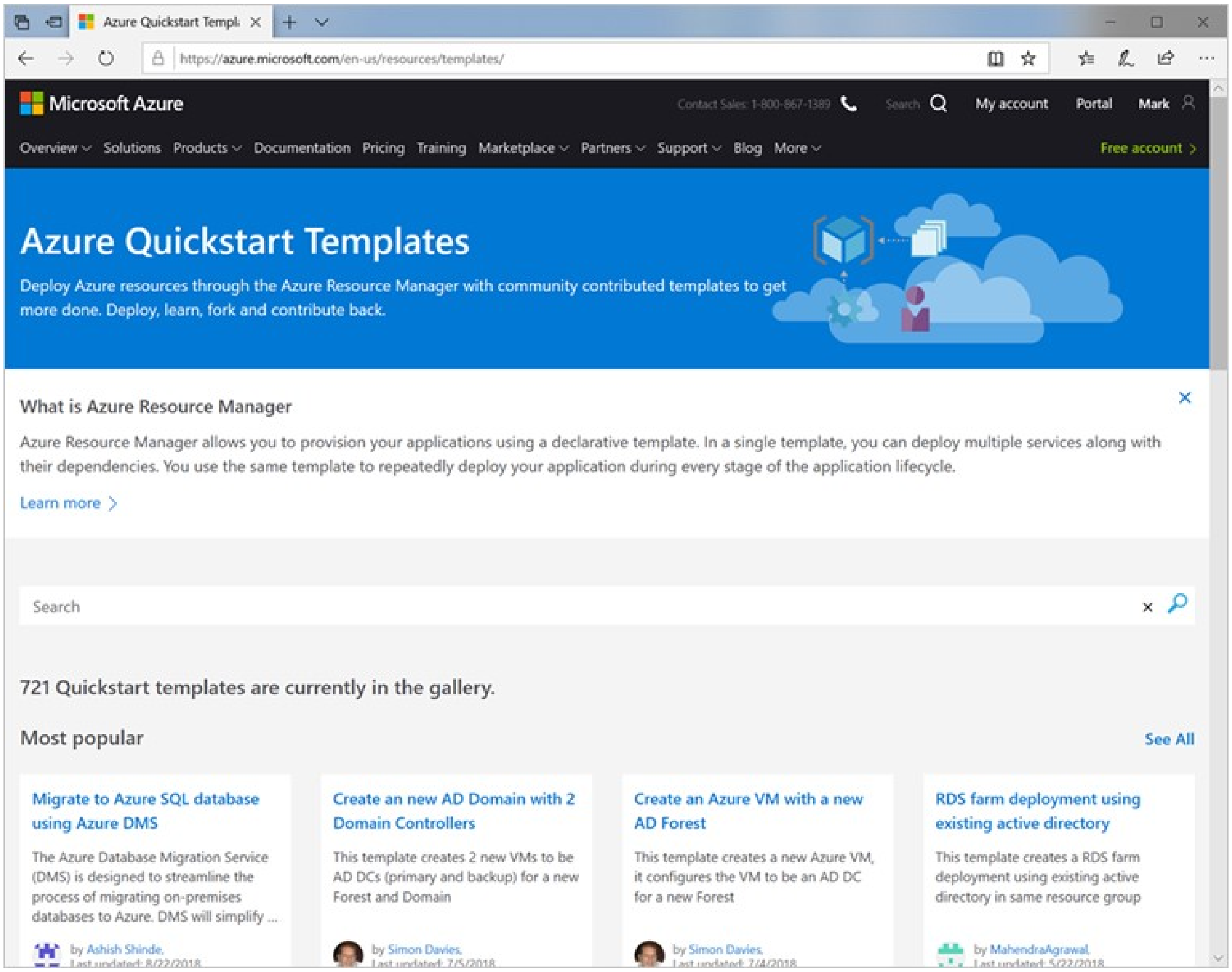
Suppose your company is deploying several servers as part of their cloud transition. VM disks must be encrypted during the deployment, so there's no time when the disks are vulnerable. You want to automate this process, and have to modify the Azure Resource Manager templates to automatically enable encryption.

Here, we'll look at how to use an Azure Resource Manager template to automatically enable encryption for new Windows VMs.

What are Azure Resource Manager templates?

Resource Manager templates are JSON files used to define a set of resources to deploy to Azure. You can write them from scratch, and for some Azure resources, including VMs, you can use the Azure portal to generate them. You'll need to complete the required information for a manual VM deployment, but instead of deploying the VM to Azure, you save the template. You can then *reuse* the template to create that specific VM configuration.

There are example templates available in docs to automate all sorts of administrative tasks. In fact, we could have used one of these templates to encrypt our VM that we just did manually!



Azure Quickstart Templates

Deploy Azure resources through the Azure Resource Manager with community contributed templates to get more done. Deploy, learn, fork and contribute back.

What is Azure Resource Manager

Azure Resource Manager allows you to provision your applications using a declarative template. In a single template, you can deploy multiple services along with their dependencies. You use the same template to repeatedly deploy your application during every stage of the application lifecycle.

Learn more

Search

721 Quickstart templates are currently in the gallery.

Most popular

See All

Migrate to Azure SQL database using Azure DMS

The Azure Database Migration Service (DMS) is designed to streamline the process of migrating on-premises databases to Azure. DMS will simplify ...

by Ashish Shinde,
Last updated: 8/22/2018

Create an new AD Domain with 2 Domain Controllers

This template creates 2 new VMs to be AD DCs (primary and backup) for a new Forest and Domain

by Simon Davies,
Last updated: 7/5/2018

Create an Azure VM with a new AD Forest

This template creates a new Azure VM, it configures the VM to be an AD DC for a new Forest

by Simon Davies,
Last updated: 7/4/2018

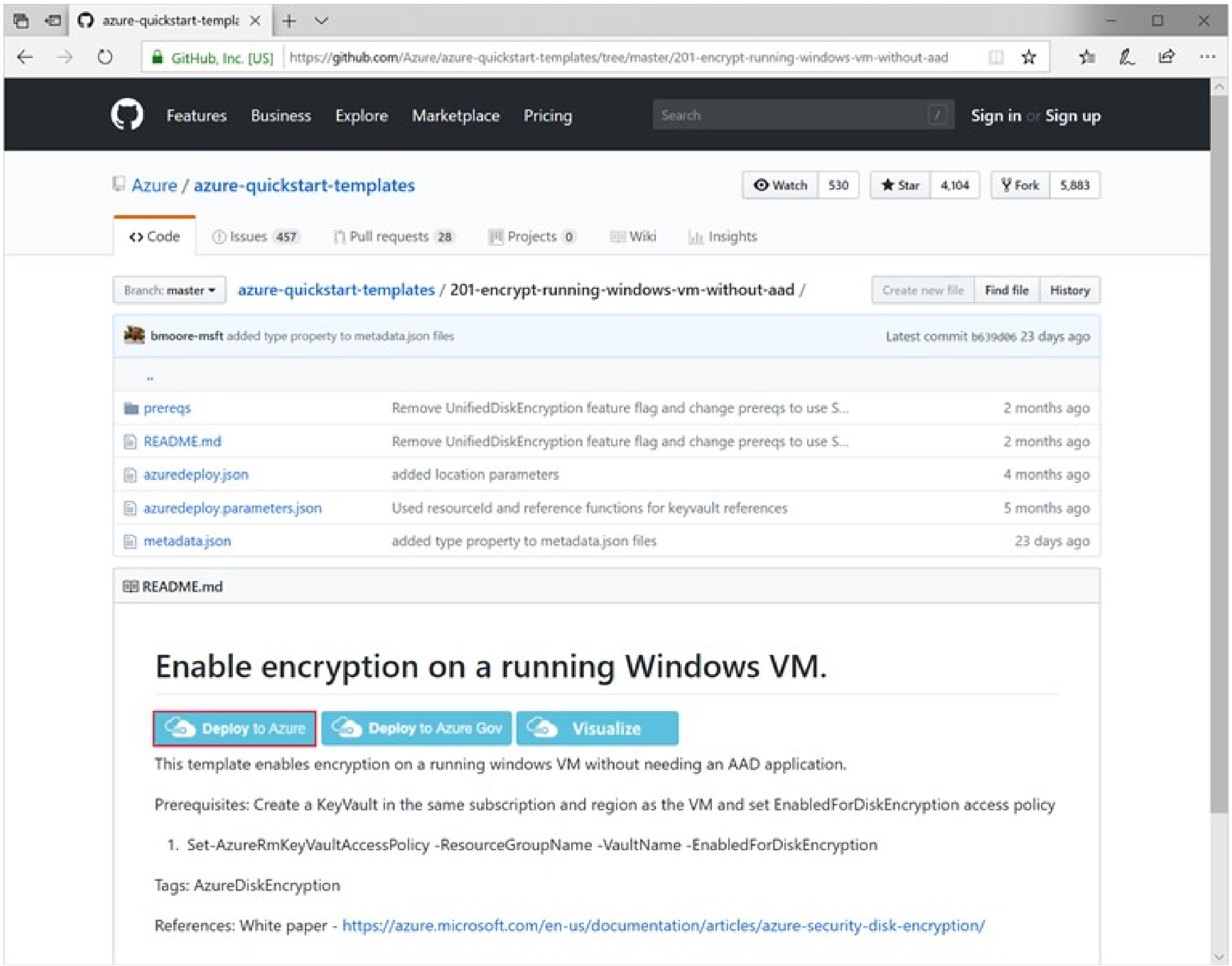
RDS farm deployment using existing active directory

This template creates a RDS farm deployment using existing active directory in same resource group

by MahendraAgrawal,
Last updated: 5/22/2018

Using GitHub templates

The actual template source is stored in GitHub. You can browse to a template in GitHub and deploy right to Azure from the page.



azure-quickstart-templates / 201-encrypt-running-windows-vm-without-aad /

bmoore-msft added type property to metadata.json files — Latest commit b639d06 23 days ago

..		
prereqs	Remove UnifiedDiskEncryption feature flag and change prereqs to use S...	2 months ago
README.md	Remove UnifiedDiskEncryption feature flag and change prereqs to use S...	2 months ago
azuredeploy.json	added location parameters	4 months ago
azuredeploy.parameters.json	Used resourceId and reference functions for keyvault references	5 months ago
metadata.json	added type property to metadata.json files	23 days ago

README.md

Enable encryption on a running Windows VM.

This template enables encryption on a running windows VM without needing an AAD application.

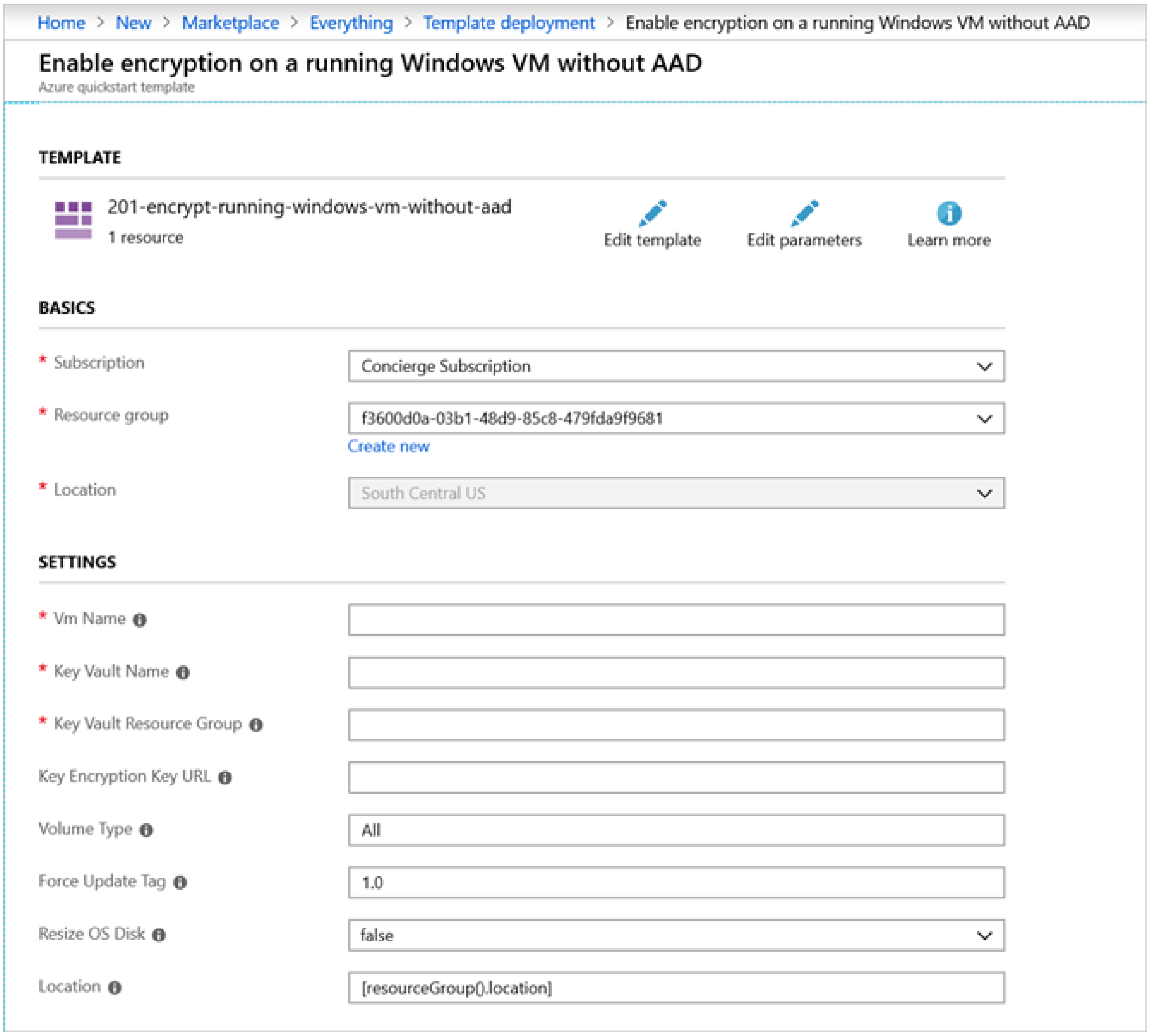
Prerequisites: Create a KeyVault in the same subscription and region as the VM and set EnabledForDiskEncryption access policy

1. Set-AzureRmKeyVaultAccessPolicy -ResourceGroupName -VaultName -EnabledForDiskEncryption

Tags: AzureDiskEncryption

References: White paper - https://azure.microsoft.com/en-us/documentation/articles/azure-security-disk-encryption/

When the template is deployed, Azure will display a list of required input fields.



Home > New > Marketplace > Everything > Template deployment > Enable encryption on a running Windows VM without AAD

Enable encryption on a running Windows VM without AAD

Azure quickstart template

TEMPLATE

201-encrypt-running-windows-vm-without-aad

1 resource

Edit template
Edit parameters
Learn more

BASICS

* Subscription	Concierge Subscription
* Resource group	f3600d0a-03b1-48d9-85c8-479fda9f9681 Create new
* Location	South Central US

SETTINGS

* Vm Name	
* Key Vault Name	
* Key Vault Resource Group	
Key Encryption Key URL	
Volume Type	All
Force Update Tag	1.0
Resize OS Disk	false
Location	[resourceGroup().location]

You can then execute the template to create, modify, or remove resources.

Running templates in the Azure portal

If you already know the template you want to use, or you have saved templates in your Azure account, you can use the **Create a resource** > **Template Deployment** resource to locate and run defined templates in the portal. You can search through templates by name, edit a template to change the parameters or behavior, and execute the template right from the GUI.

Running templates from the command line

Given a URL to a template, you can execute it with Azure PowerShell. For example, we could run the disk encryption template with the following PowerShell command:

PowerShell

Copy

```powershell
New-AzResourceGroupDeployment `
    -Name encrypt-disk `
    -ResourceGroupName <resource-group-name> `
    -TemplateUri https://raw.githubusercontent.com/azure/azure-quickstart-templates/master/201-encrypt-running-windows-vm-without-aad/azuredeploy.json
```

Or, if you prefer the Azure CLI, with the `group deployment create` command.

Azure CLI

Copy

```bash
azure config mode arm
azure group deployment create <my-resource-group> <my-deployment-name> \
    --template-uri https://raw.githubusercontent.com/azure/azure-quickstart-templates/master/201-encrypt-running-windows-vm-without-aad/azuredeploy.json
```

Next unit: Exercise - Use a Resource Manager template to decrypt the VM

Continue ›

‹ Previous Unit 6 of 7 ˅ Next ›

✓ 100 XP

Exercise - Use a Resource Manager template to decrypt the VM

10 minutes

This module requires a sandbox to complete. You have used 2 of 10 sandboxes for today. More sandboxes will be available tomorrow.

Activate sandbox

In this unit, you'll use an Azure Resource Manager template to decrypt our Windows VM we created earlier. We encrypted the OS drive on our Windows VM. However, the OS drive won't have any confidential information on it, so we could leave it unencrypted. Let's use a template to decrypt the OS drive.

Decrypt a VM using an Azure Resource Manager template

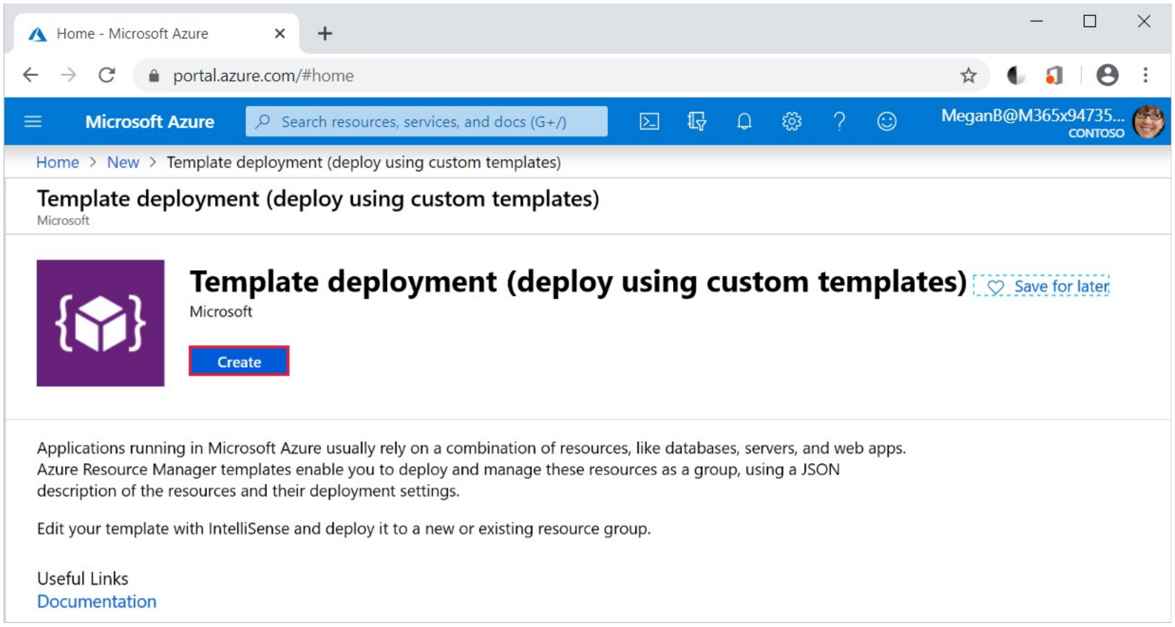
We're going to use a template Microsoft has published on GitHub that is specifically designed to decrypt a running Windows VM.

1. Sign into the Azure portal with the same account you activated the sandbox with.

2. On the Azure portal menu or from the **Home** page, select **Create a resource**.

3. Type **Template** in the search box.

4. Select **Template deployment (deploy using custom templates)** from the resulting list and click **Create**.



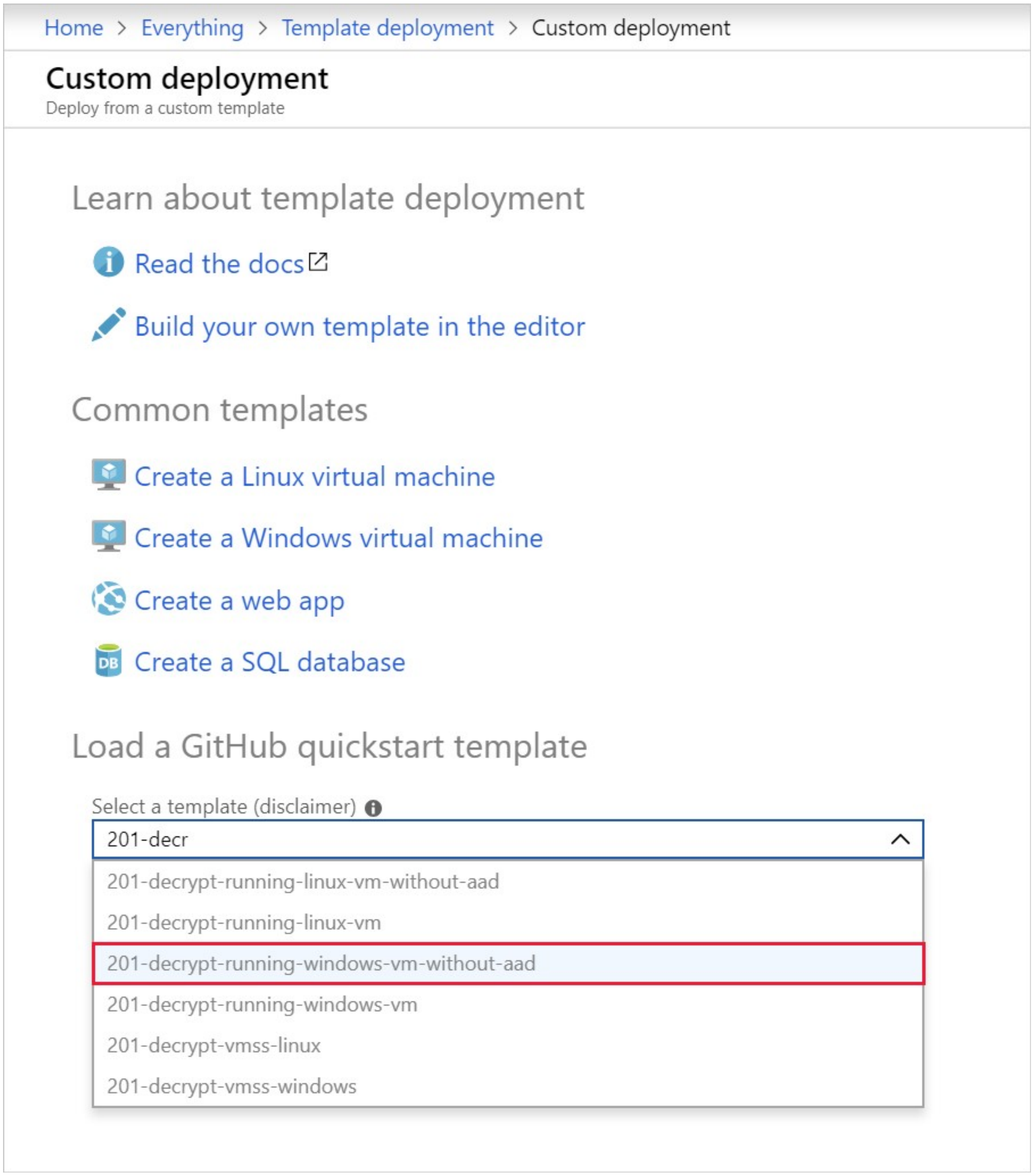
Template deployment (deploy using custom templates)
Microsoft

Template deployment (deploy using custom templates)
Microsoft

Applications running in Microsoft Azure usually rely on a combination of resources, like databases, servers, and web apps. Azure Resource Manager templates enable you to deploy and manage these resources as a group, using a JSON description of the resources and their deployment settings.

Edit your template with IntelliSense and deploy it to a new or existing resource group.

5. In the **Select a template** search box, start typing "201-decrypt" and select the "201-decrypt-running-windows-vm-without-aad" template.



Home > Everything > Template deployment > Custom deployment

Custom deployment

Deploy from a custom template

Learn about template deployment

Read the docs

Build your own template in the editor

Common templates

Create a Linux virtual machine

Create a Windows virtual machine

Create a web app

Create a SQL database

Load a GitHub quickstart template

Select a template (disclaimer)

201-decr

201-decrypt-running-linux-vm-without-aad

201-decrypt-running-linux-vm

201-decrypt-running-windows-vm-without-aad

201-decrypt-running-windows-vm

201-decrypt-vmss-linux

201-decrypt-vmss-windows

6. Click **Select Template** to launch the template runner.

7. In the settings view, enter the following information:

   - Select *Concierge Subscription* for the **Subscription**.
   - Select the sandbox resource group Sandbox RG. This will auto-select the region as well.
   - Enter "fmdata-vm01" for the **VM Name**.
   - Leave the **Volume Type** as *All*.

8. Select the **I agree to the terms and conditions** check box.

9. Click **Purchase** to run the template. Note that there is no cost to this - it's a standard button.

The deployment may take a few minutes to complete.

Verify the encryption status of the VM

1. On the Azure portal menu or from the **Home** page, select **Virtual machines** and select your VM **fmdata-vm01**. Alternatively, you can search for your VM by name from **All Resources**.

2. On the **Virtual machine** pane, under **SETTINGS**, click **Disks**.

3. On the **Disks** pane, notice **Encryption** is not enabled.

Next unit: Summary

Continue ›

✓ 200 XP

Summary

3 minutes

Azure provides Storage Service Encryption (SSE) and Azure Disk Encryption (ADE) to secure Azure VM disks. These technologies work together to provide strong 256-bit encryption, as part of a defense-in-depth approach for the protection of Azure VM disks. It's required that you complete the Azure Disk Encryption prerequisites to enable disk encryption. The Azure Disk Encryption prerequisites configuration script can automate this process. When enabling encryption on new VMs, you can use an Azure Resource Manager template. This ensures that your data is encrypted at the point of deployment, leaving no vulnerabilities.

Clean up

The sandbox automatically cleans up your resources when you're finished with this module.

When you're working in your own subscription, it's a good idea at the end of a project to identify whether you still need the resources you created. Resources left running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

Additional resources

- Troubleshooting Azure VM Disk encryption
- How to encrypt a Linux virtual machine in Azure
- Azure Disk Encryption Overview
- What Linux distributions does Azure Disk Encryption support?.
- Resource Manager templates on GitHub

Check your knowledge

1. True or false: If you enable Azure Disk Encryption (ADE) on a Windows VM, it will use DM-Crypt to encrypt the data on your Virtual Hard Disks.

○ True

● False ✓

Windows VMs are encrypted using BitLocker. Linux VMs will use DM-Crypt.

2. True or false: When using Azure Key Vault to secure keys used for Azure Disk Encryption (ADE), you must ensure the Azure Key Vault access policies are configured to permit at least one security principal.

○ True

● False ✓

You do not need to configure a security principal for ADE, just enabling the key vault for disk encryption is enough.

3. Suppose you create a new VM with a single OS disk and a single data disk. You use all the default options when creating the VM and you have no Azure Key Vault anywhere in your subscription. Which option most accurately describes the encryption state of those disks?

○ Both disks are unencrypted.

○ The OS disk is encrypted using Storage Service Encryption (SSE). The data disk is unencrypted.

● Both disks are encrypted using Storage Service Encryption. ✓

All disks are encrypted using SSE by default. With SSE, Azure manages the keys and automatically decrypts data for any read operations without impact on performance.

Module complete:

Unlock achievement