

Create Rescue VM from DualPass Encrypted VMs with automated process of unlocking disks_Encryption

Last updated by | Emily Anderson | Jun 14, 2022 at 9:12 AM PDT

Tags

cw.Azure-Encryption

cw.How-To

MICROSOFT CONFIDENTIAL

All content in this article is Microsoft Confidential and this data is considered covered under the Non-Disclosure Agreement (NDA).

This data should not be shared outside of the Microsoft Global Support organization, unless otherwise specified.

For more information, see *Microsoft Privacy Statement* [☐](#).

Contents

- What is this automated process
- Why this automated process was created
- Advantages
- Scenarios where ca be used (but not limited to them)
- Supported features\scenarios
- Limitations
- Prerequisites
- What it does
 - Additional checks and actions:
 - Diagram
- Restore VM
- Additional scripts used by the main script:
- Troubleshooting logs:
- Useful troubleshooting details
- How to use the script
 - 1. Download\Upload script to Azure cloud shell \$HOME dir...
 - Option 1 - Download the script from github repository to t...
 - Option 2 - Upload the script from your local machine to to...
 - 2. Run the script
- Video walkthrough
 - Windows
 - Create a Windows Rescue VM without Hyper-V installed (-...
 - Create a Windows Rescue VM with Hyper-V installed (-ena...
 - Linux
 - Create a Linux Rescue VM
 - Create a Linux Rescue VM with unmanaged disks (the proc...
- Need additional help or have feedback?

What is this automated process

This automated process is actually a powershell script

The script was designed to create a rescue environment only for VMs which are encrypted with Dual Pass (older version - with AAD) BEK and KEK

Why this automated process was created

- There are times when you need to troubleshoot a VM in scenarios like: Os no boot, connectivity issues or others.
- There are other tools that can help you in this process for the connectivity scenarios like Run command, serial console, remote powershell, psexec, but often this tools cannot be used for different reasons
- In a no boot scenario, you are limited in troubleshooting and the most common path is to create a rescue environment (create a rescue VM, attach a copy of the broken OS disk as a data disk to this VM and maybe install Hyper-V role and create a VM inside Hyper-V)
- For non-encrypted VMs, you can easily create a rescue environment either manually or using Az VM repair

What about when that VM is encrypted?

- When that VM is encrypted with Single Pass (newest version - without AAD), to create a rescue environment you can use either the manual process or Az VM repair which supports creating a rescue environment for single pass encrypted VMs
- When that VM is encrypted with Dual Pass (older version - with AAD), the only method of creating a rescue environment is to do it manually since Az Vm repair doesn't support dual pass encrypted VMs

The answer to why this process was created is, to automate the process of creating a rescue VM and if necessary install Hyper-V and configure VM inside Hyper-V for broken VMs that are encrypted with Dual Pass (older version - with AAD)

Advantages

- This is an automated process for creating all necessary resources for starting the troubleshooting process for VMs which are encrypted with Dual Pass (older version - with AAD)
- This powershell script was designed to be used from Azure cloud shell, to eliminate the need of powershell prerequisites needed in the manual process and which caused delays or additional issues due to the diversity of environments in terms of Powershell version, Os version, user permissions, internet connectivity etc.
- The duration for this process using this script is between 4 minutes and 15 minutes (depending on the option selected), which far more less than the manual process which can take hours or even days depending on the complexity of scenarios, environment variables, customer limitations, level of expertise
- Reduced risk of human errors in gathering and using encryption settings
- Available backups in case of the worst scenarios
- No internet access is required for the Rescue VM which is useful for users with restricted environments
- The use of the script, has no limitations that were found regarding the operating system versions (Window or Linux) **supported in Azure**
- Possibility and compatibility to chose the most common and newest operating system version, Window or Linux, to create the rescue environment
- Insignificant number of initial input data needed to run this script
- Available execution\troubleshooting logs that can be used to investigate\improve the runtime of this script

- Additional checks during this process to reduce or prevent the risk of a script failure due to the variety of environments
- Additional explanatory details offered during the process, which helps the user to learn also theoretical aspects along the way
- Error handling for the most common errors in terms of auto-resolving or guidance for the manual process of resolving the issue
- Offers the possibility of using the script multiple times if the troubleshooting scenario requires this

Scenarios where ca be used (but not limited to them)


VM's operating system is not booting properly VM has connectivity issues and other available tools cannot be used or this process like:

- User cannot connect using RDP\SSH
- Network card issues (Vm isolated)
- Public IP issues

Supported features\scenarios

- VM encrypted with Pass (older version - with AAD) BEK and KEK
- VMs with Managed and Unmanaged disks
- VMs with Windows\Linux existing supported operating systems
- Add up to 5 name\value pairs as tags for the rescue VM
- Existing resource groups
- Existing Storage containers (for unmanaged disks)
- Existing Vnet\Subnet
- Attach existing NSG to NIC of the Rescue VM
- Restricted environments, since no internet access is required for the Rescue VM to be created, configured and for the data disk to be unlocked. All the necessary resources are downloaded or created directly in azure drive and then pushed to the rescue VM using Invoke-AzVMRunCommand

Limitations

- The script was designed to be used **only** on VMs which are encrypted with Dual Pass (older version - with AAD)
- The script was designed to be used **only** in [Azure Cloud Shell](#) 

Prerequisites

- User needs to have access to Get\create snapshots, disks, resource groups, additional resources necessary for creating a VM like, NICs, public IPs, VNETs, NSGs and to create a new VM
- User needs to have access to Azure cloud shell
- User needs to have access to his Azure Active Directory (for assigning proper permissions to AAD Application to have access (like list and create) to the keys and secrets from Key Vault). Even though this script doesn't really need this kind of access, it will be needed in the recreate process of this VM once the issue was fixed since swapping disks are not supported for Dual Pass (older version - with AAD) encrypted disks.

What it does

It creates a rescue environment to be able to troubleshoot the actual issue of impacted VM

Detailed steps:

- Creates a copy of the OS disk of impacted VM
- Removes encryption settings from the disk created to be able to attach it to rescue VM
- Outputs encryption settings as a reference
- Creates a rescue VM with the option of choosing the operating system version depending if it is Windows or Linux
- Copies encryption settings to the rescue VM to that Azure platform to attach the 'BEK Volume' which contains the unlock key.
- Attaches the copy for the OS disk of impacted VM as a data disk to the Rescue VM
- Creates a script that will stored in cloud drive that will be sent using Invoke-AzVMRunCommand to the rescue VM and will unlock the disk
- If used, the -enablenested parameter creates a script that will stored in cloud drive that will be sent using Invoke-AzVMRunCommand to the rescue VM and will install Hyper-V role and reboot VM.
- If used, the -enablenested parameter creates another script that will stored in cloud drive that will be sent using Invoke-AzVMRunCommand to the rescue VM and will configure\create VM inside Hyper-V from the data disk attached, after putting the data disk and BEK Volume offline
- Creates an "Unlock Disk" powershell script on the desktop for different troubleshooting scenarios
- Deletes all the additional scripts used by the main script from the cloud drive

Additional checks and actions:

Checks

If VM exists

What is the Key Vault Permission model

If user has the role 'Key Vault Administrator' for Azure role-based access control Key Vault Permission m

No check
available

If role assignment or access policy creation fails due to user permissions issue

If Vm is encrypted with Dual Pass

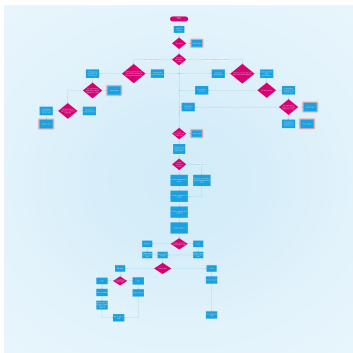
If Vm is encrypted with BEK or KEK

If Resource group exists

Diagram


Please check the diagram with the detailed steps

(click on the image to open the diagram in a new tab in full size)



Restore VM

- As mentioned, this script creates a rescue environment to be able to troubleshoot the actual issue of impacted VM.
- Once the issue was resolved, to be able to bring online the fixed VM from the rescue environment back in Azure, since "swap disk" feature is not supported\working on dual pass encrypted VMs, another script was created which will recreate the original VM from the fixed disks, by deleting original VM and recreate it back and then encrypt it again with dual pass.

- The script which will recreate the original VM from the fixed disks can be found in the (restore process) [repository](#) .
- A Wiki for the restore script can be found here: [Recreate DualPass Encrypted VM from fixed encrypted disk_Encryption](#)

Additional scripts used by the main script:

Additional Scripts added\created in Azure cloud shell drive and sent to Rescue VM	Operating System
\$HOME/Unlock-Disk	Windows
\$HOME/Install-Hyper-V-Role	Windows
\$HOME/EnableNested	Windows

Additional Scripts added\created in Azure cloud shell drive and sent to Rescue VM	Operating System
<code>\$HOME/linux-mount-encrypted-disk.sh</code>	Linux

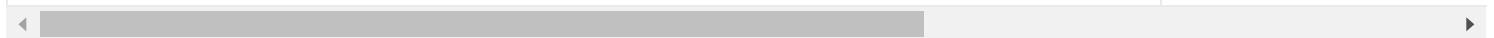


Useful scripts in Rescue VM	Operating System
<code>C:\Unlock Disk\Unlock disk.ps1</code>	Windows
<code>C:\Users\Public\Desktop\Unlock disk.ps1</code>	Windows
<code>C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\unlock_disk.bat</code>	Windows



Troubleshooting logs:

Logs in the Azure cloud shell drive	Tool
<code>\$HOME/CreateRescueVMScript_Execution_log.txt</code>	Powershell script



Logs in the Rescue VM	Operating System
c:\Unlock Disk\Unlock-Disk-log.txt	Windows
c:\Unlock Disk\EnableNested-log.txt	Windows
c:\Unlock Disk\Install-Hyper-V-Role-log.txt	Windows
/var/log/vmrepair/vmrepair.log	Linux

Useful troubleshooting details

- The name of the copy of the OS disk that will be created and attached to the Rescue VM follow this pattern: 'fixed_*i*originalOsDiskName where i' is incremental if a disk with the same name already exists. Note that disk name will be truncated if the number of characters is greater than "50"
- For Windows Rescue VMs, once a user RDP to that VM, the Hyper-V manager will be started automatically
- If the rescue VM is rebooted, data disk should be automatically unlocked after 1-2 minutes
- If for some reason disk doesn't unlock automatically or you need to unlock manually the disks during troubleshooting, user can unlock encrypted data disk using 'Unlock disk.ps1' script from desktop
- VM created inside Hyper-V is configured to allow outbound connectivity to internet
- VM created inside Hyper-V is configured to be accessible from the Rescue VM (via RDP, ping, etc..)
- For Linux VM, this is how the output of "lsblk" looks like on the rescue VMs if the broken VM doesn't have LVM and if it does:

With LVM:

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
sda	8:0	0	64G	0	disk	
└sda1	8:1	0	500M	0	part	/boot
└sda2	8:2	0	63G	0	part	
└└rescuevg-tmplv	253:0	0	2G	0	lvm	/tmp
└└rescuevg-usrlv	253:1	0	10G	0	lvm	/usr
└└rescuevg-homelv	253:2	0	1G	0	lvm	/home
└└rescuevg-varlv	253:3	0	8G	0	lvm	/var
└└rescuevg-rootlv	253:4	0	2G	0	lvm	/
└sda14	8:14	0	4M	0	part	
└sda15	8:15	0	495M	0	part	/boot/efi
sdb	8:16	0	16G	0	disk	
└sdb1	8:17	0	16G	0	part	/mnt
sdcc	8:32	0	128G	0	disk	
└sdcc1	8:33	0	500M	0	part	/tmp/dev/sdc1
└sdcc2	8:34	0	500M	0	part	/investigateroot/boot
└sdcc3	8:35	0	2M	0	part	
└sdcc4	8:36	0	63G	0	part	
└└osencrypt	253:5	0	63G	0	crypt	
└└└rootvg-tmplv	253:6	0	2G	0	lvm	/investigateroot/tmp
└└└rootvg-usrlv	253:7	0	10G	0	lvm	/investigateroot/usr
└└└rootvg-optlv	253:8	0	2G	0	lvm	/investigateroot/opt
└└└rootvg-homelv	253:9	0	1G	0	lvm	/investigateroot/home
└└└rootvg-varlv	253:10	0	8G	0	lvm	/investigateroot/var
└└└rootvg-rootlv	253:11	0	2G	0	lvm	/investigateroot
sdd	8:48	0	48M	0	disk	
└sdd1	8:49	0	46M	0	part	/mnt/azure_bek_disk
sr0	11:0	1	1024M	0	rom	

How to use the script

Important:

Please use a new page of Azure Cloud Shell before running the script, since Azure Cloud Shell has a timeout period of 20 minutes of inactivity.


If Azure Cloud Shell times out the script is running, the script will stop at the time of the timeout.

If the script is stopped until it finishes, environment might end up in an 'unknown state'.


If for some reason Azure Cloud shell still times out, manually delete all the resources created until that point, and run again the script.

1. Download\Upload script to Azure cloud shell \$HOME directory



Option 1 - Download the script from github repository to the Azure cloud shell drive:

- Open [Script repository](#) 
- Check what is the latest available version of the script
- Modify the command bellow to download the latest version of the script in to the \$HOME directory of your Azure cloud shell session.

Invoke-WebRequest -Uri "https://raw.githubusercontent.com/gabriel-petre/ADE/main/Create_Rescue_VM_from_DualPas

- Open [Azure Cloud Shell](#) 
- Paste the command and enter to download the script in to the \$HOME directory of your Azure cloud shell session.

Option 2 - Upload the script from your local machine to to the Azure cloud shell drive:

- Download the latest version of the script "Create_Rescue_VM_from_DualPass_Encrypted_Vm" from the [repository](#) 
- Open [Azure Cloud Shell](#) 
- Click on the Upload\Download\Manage file share icon, click on upload and select from your local machine the script you previously downloaded

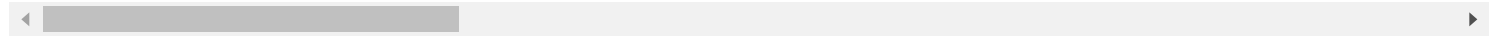
2. Run the script

- Open [Azure Cloud Shell](#)
- From the left up corner section, select 'Powershell'
- See below examples on how to run the script:

```
Create_Rescue_VM_from_DualPass_Encrypted_Vm_1.0.ps1
[-SubscriptionID]
[-VmName]
[-VMRgName]
[-RescueVmName]
[-RescueVmRg]
[-CopyDiskName]
[-RescueVmUserName]
[-RescueVmPassword]
[-associatepublicip]
[-enablenested]           #For Windows VMs only
[-NewVnetAndSubnet]
[-VnetName]
[-SubnetName]
[-VnetRG]
[-NicNsgName]
[-NicNsgRG]
[-NsgRdpSshAllowRules]
[-TagName1]
[-TagValue1]
[-TagName2]
[-TagValue2]
[-TagName3]
[-TagValue3]
[-TagName4]
[-TagValue4]
[-TagName5]
[-TagValue5]
```

Example 1 of how to run the script (Managed and Unmanaged disks):

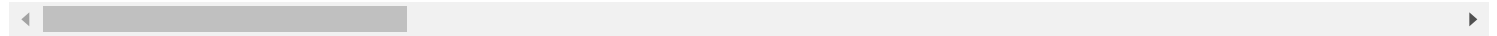
```
./Create_Rescue_VM_from_DualPass_Encrypted_Vm_1.0.ps1 -SubscriptionID "<Subscription ID>" -VmName "<Impacted V
```



Note: Command above will create a new Vnet\Subnet and place Rescue VM inside, without a public IP, attach as a data disk a copy of the OS disk of the impacted VM and unlock that data disk

Example 2 of how to run the script (Managed and Unmanaged disks):

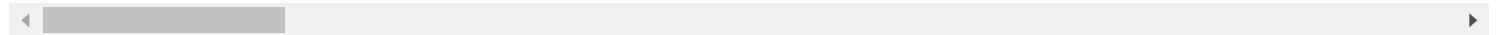
```
./Create_Rescue_VM_from_DualPass_Encrypted_Vm_1.0.ps1 -SubscriptionID "<Subscription ID>" -VmName "<Impacted V
```



Note: Command above will create a new Vnet\Subnet and place Rescue VM inside, create\assign a public IP, create an NSG and assign it to NIC which will allow RDP or SSH, install Hyper-V role, sets the data disk and BEK volume offline and configure\create a Vm inside Hyper-V from the data disks attached, which is a copy of the OS disk of the impacted VM. Once Hyper-V VM will be started, the OS will be able to unlock the data disk since BEK volume is also attached to that VM

Example 3 of how to run the script (Managed and Unmanaged disks):

```
./Create_Rescue_VM_from_DualPass_Encrypted_Vm_1.0.ps1 -SubscriptionID "<Subscription ID>" -VmName "<Impacted V
```



Note: Command above will create a new Vnet\Subnet and place Rescue VM inside, create\assign a public IP and add 5 name\value pairs as TAGs, install Hyper-V role, sets the data disk and BEK volume offline and configure\create a Vm inside Hyper-V from the data disks attached, which is a copy of the OS disk of the impacted VM. Once Hyper-V VM will be started, the OS will be able to unlock the data disk since BEK volume is also attached to that VM

Example 4 of how to run the script (Managed and Unmanaged disks):

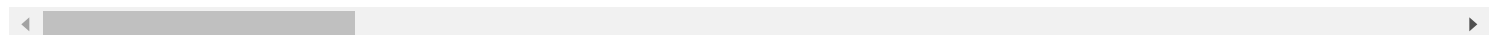
```
./Create_Rescue_VM_from_DualPass_Encrypted_Vm_1.0.ps1 -SubscriptionID "<Subscription ID>" -VmName "<Impacted V
```



Note: Command above will create Rescue VM inside existing VNET and subnet, attach existing NSG to Rescue VM's NIC, create\assign a public IP, install Hyper-V role, sets the data disk and BEK volume offline and configure\create a Vm inside Hyper-V from the data disks attached, which is a copy of the OS disk of the impacted VM. Once Hyper-V VM will be started, the OS will be able to unlock the data disk since BEK volume is also attached to that VM

Example 5 of how to run the script (Managed and Unmanaged disks):

```
./Create_Rescue_VM_from_DualPass_Encrypted_Vm_1.0.ps1 -SubscriptionID "<Subscription ID>" -VmName "<Impacted V
```



Note: Command above will create Rescue VM inside existing VNET and subnet, create\assign a public IP, install Hyper-V role, sets the data disk and BEK volume offline and configure\create a Vm inside Hyper-V from the

data disks attached, which is a copy of the OS disk of the impacted VM. Once Hyper-V VM will be started, the OS will be able to unlock the data disk since BEK volume is also attached to that VM

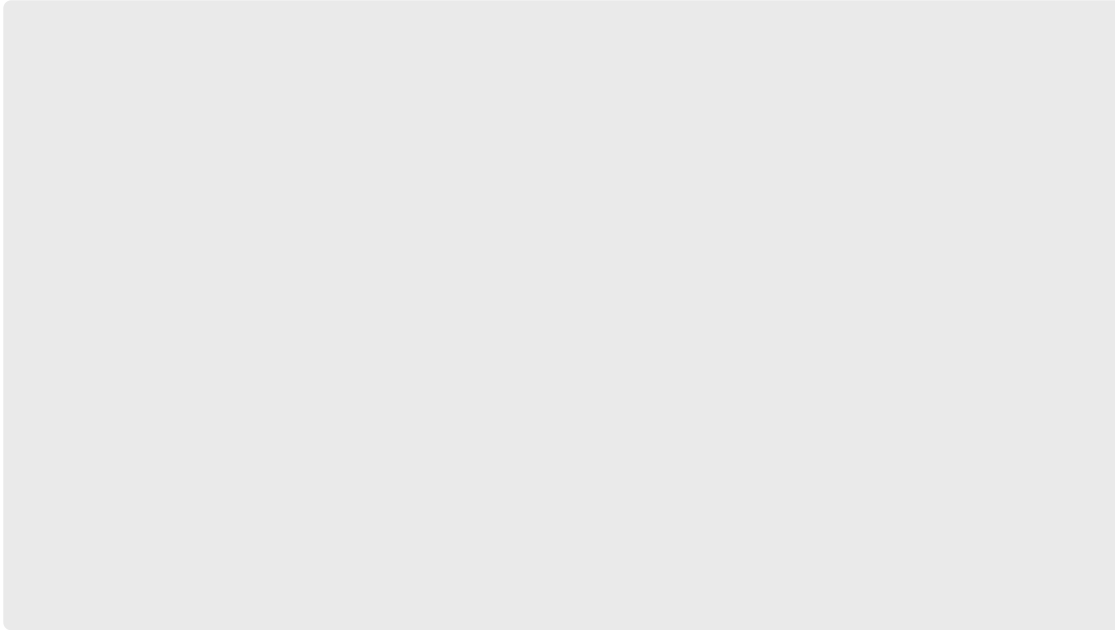
Mandatory parameters	Description
-SubscriptionID	Subscription ID where VM resides
-VmName	The name of the Virtual machine that is experiencing issues
-VMRgName	The resource group name of the Virtual machine that is experiencing iss
-RescueVmName	The name of the Rescue Virtual machine that will be created
-RescueVmRg	The resource group name of the Rescue Virtual machine that will be cre
-CopyDiskName	The name for the copy of the OS disk that will be created, attached to th and unlocked
- RescueVmUserNam e	The username used for accessing the Rescue Virtual machine that will b
- RescueVmPasswor d	The password for the username used for accessing the Rescue Virtual m
- NewVnetAndSubne t	This switch will create a new VNET\Subnet and place the Rescue VM ins Can be used in combination with switch '-NsgRdpSshAllowRules' *If this is not specified, it will ask you to provide the details for opti existing VNET\Subnet

Optional parameters	Description
-associatepublicip	Add a public IP to the Rescue Virtual machine that will be created
-enablenested	<p>Install Hyper-V role, sets the data disk and BEK volume offline and confi Hyper-V from the data disks attached, which is a copy of the OS disk of Once Hyper-V VM will be started, the OS will be able to unlock the data also attached to that VM</p> <p>To be used only for Windows impacted VMs</p>
-VnetName	Name of an existing VNET where the rescue Vm will be placed *
-SubnetName	Name of an existing Subnet in the existing VNET where the rescue Vm v
-VnetRG	Name of the resouce group of the existing VNET where the rescue Vm v
-NicNsgName	Name of an existing NSG that will be attached to the NIC of the Rescue
-NicNsgRG	Name of the resouce group of an existing NSG that will be attached to t
-NsgRdpSshAllowRules	This switch can be used only in combination with '-NewVnetAndSu create a new NSG and add allow inbound rules for RDP or SSH with sou destination 'Any'
-TagName1	First tag Name to be added to the Rescue VM
-TagValue1	First tag Value to be added to the Rescue VM
-TagName2	Second tag Name to be added to the Rescue VM
-TagValue2	Second tag Value to be added to the Rescue VM
-TagName3	Third tag Name to be added to the Rescue VM
-TagValue3	Third tag Value to be added to the Rescue VM
-TagName4	Fourth tag Name to be added to the Rescue VM
-TagValue4	Fourth tag Value to be added to the Rescue VM
-TagName5	The fifth tag Name to be added to the Rescue VM
-TagValue5	The fifth tag Value to be added to the Rescue VM

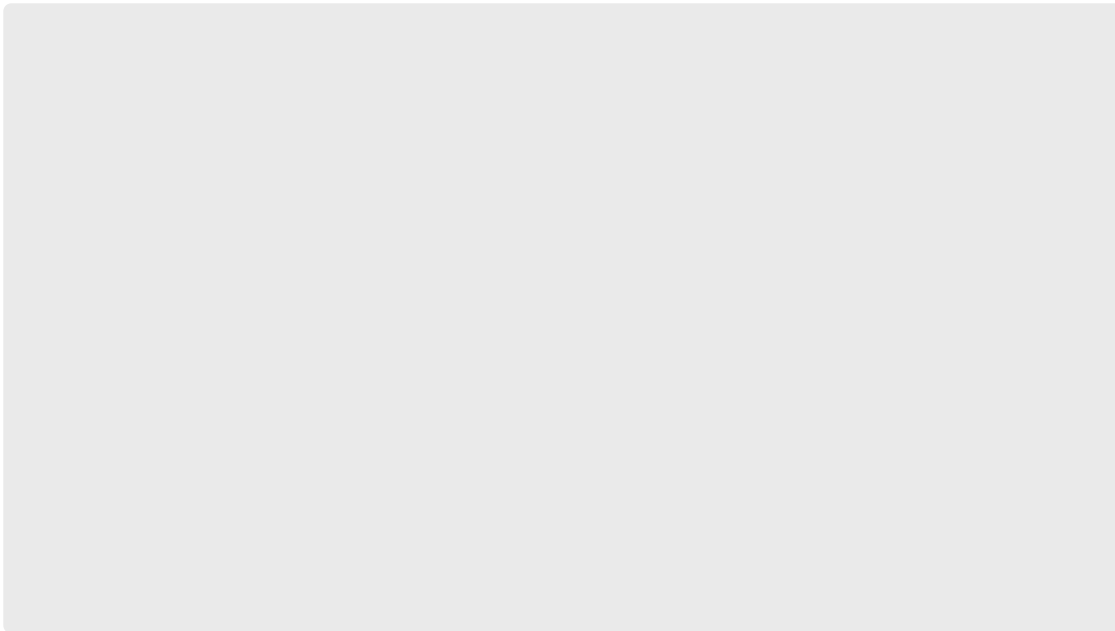
Video walkthrough

Windows

Create a Windows Rescue VM without Hyper-V installed (-enablenested switch was not specified)

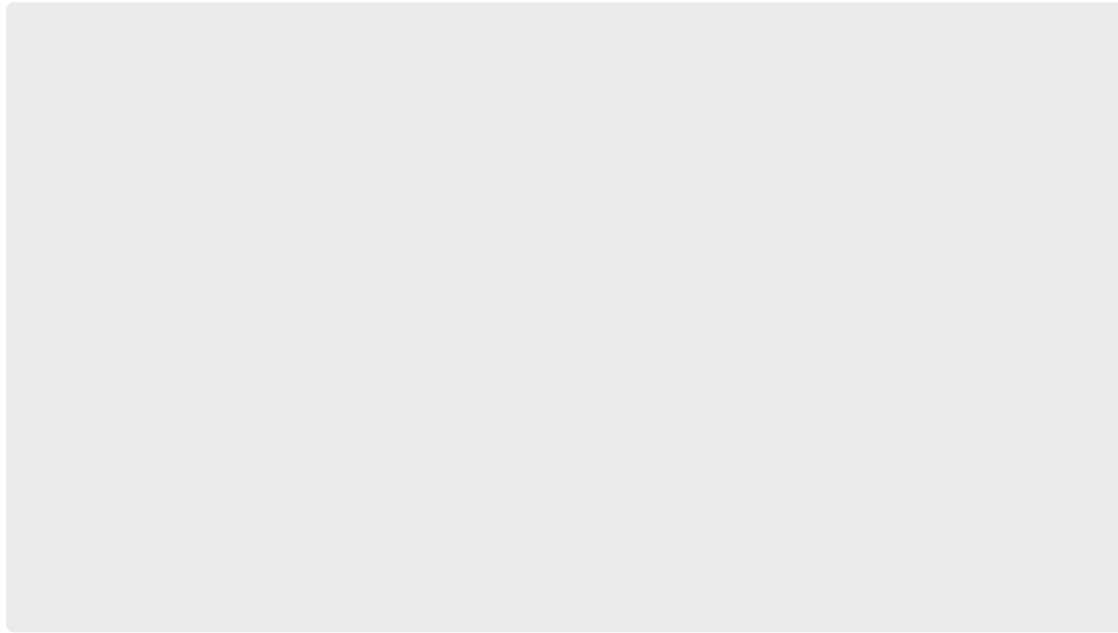


Create a Windows Rescue VM with Hyper-V installed (-enablenested switch was specified)

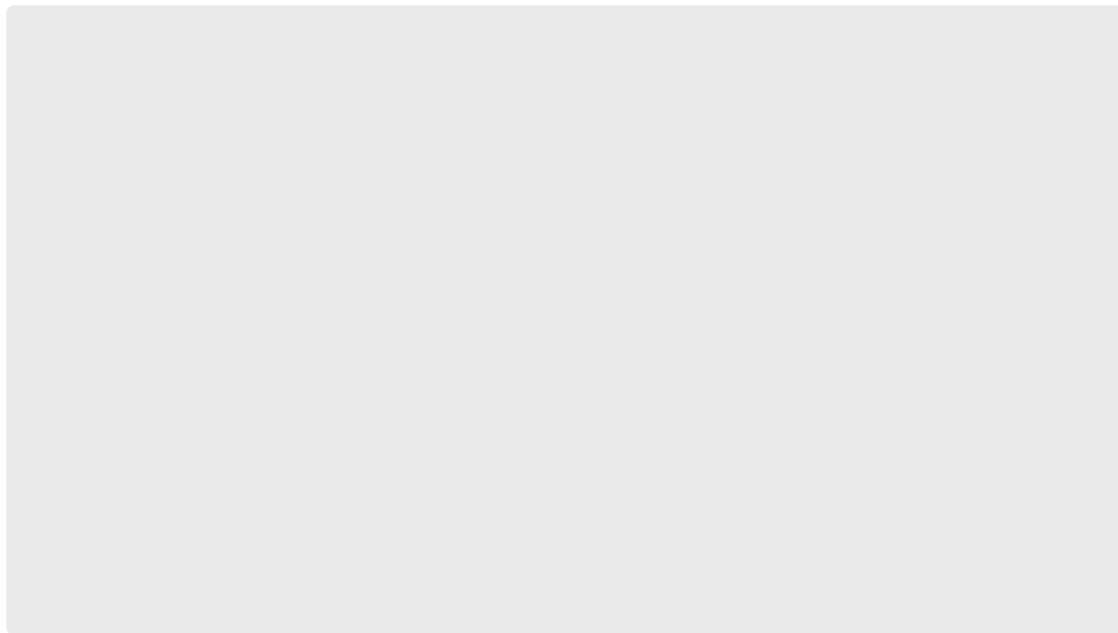


Linux

Create a Linux Rescue VM



Create a Linux Rescue VM with unmanaged disks (the process is the same for Windows VMs with unmanaged disks)



Need additional help or have feedback?

<i>To engage the Azure Encryption SMEs...</i>	<i>To provide feedback on this page...</i>	<i>To provide kudos on this page...</i>
<p>Please reach out to the Azure Encryption SMEs <input type="checkbox"/> for faster assistance.</p> <p>Make sure to use the Ava process for faster assistance.</p>	<p>Use the Azure Encryption Feedback form to submit detailed feedback on improvements or new content ideas for Azure Encryption.</p> <p>Please note the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.</p>	<p>Use the Azure Encryption Kudos form to submit kudos on the page. Kudos will help us improve our wiki content overall!</p> <p>Please note the link to the page is required when submitting kudos!</p>