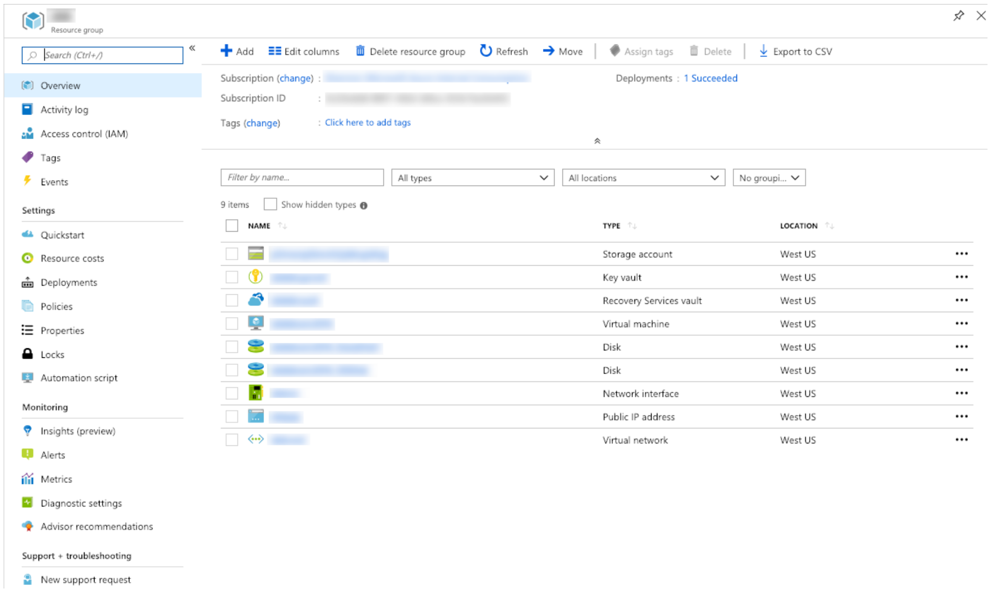
Azure Backup

Use GitHub Repo to Deploy Infrastructure

1. Open up a browser and head to the following website: aka.ms/bcdr-resil
2. On the top right-hand side of the webpage, either clone the repo locally or download a .zip file of the code/guides.
3. Go into the backup folder and locate all files.
4. Launch **deploy-bkresil-Env.ps1** inside a code editor (Visual Studio, Visual Studio Code, PowerShell ISE, Atom, etc.).
5. Running these commands will require the AzureRM module or the AZ module with the alias enabled.
6. Input variables for Hack Name, Subscription (use the Subscription Id), and Location.
7. Follow the steps inside the PowerShell script to connect your Azure account/subscription, build a new resource group, create a Key Vault, and input a secret. The code prompts for the secret reference name to be "VMPassword," but note that name can be changed. Ensure you know and remember both the username and password for later in the section. Hold off on step 6 until you perform a few tasks in the parameters json file.
8. Take note of the admin userName. Leaving it as is will work to get comfortable with deploying infrastructure from code, or you can change that information around.
9. Use the resource ID you extracted from the PowerShell script to call upon the Key Vault secret within the adminPassword parameter.
10. Pick a prefix for the envPrefixName (initials would be great).
11. Leave the other parameters as is.
12. Run step 6 from the PowerShell script and that will deploy the infrastructure to your subscription. The end result will look like this:



Subscription (change) : [redacted]

Subscription ID : [redacted]

Tags (change) : Click here to add tags

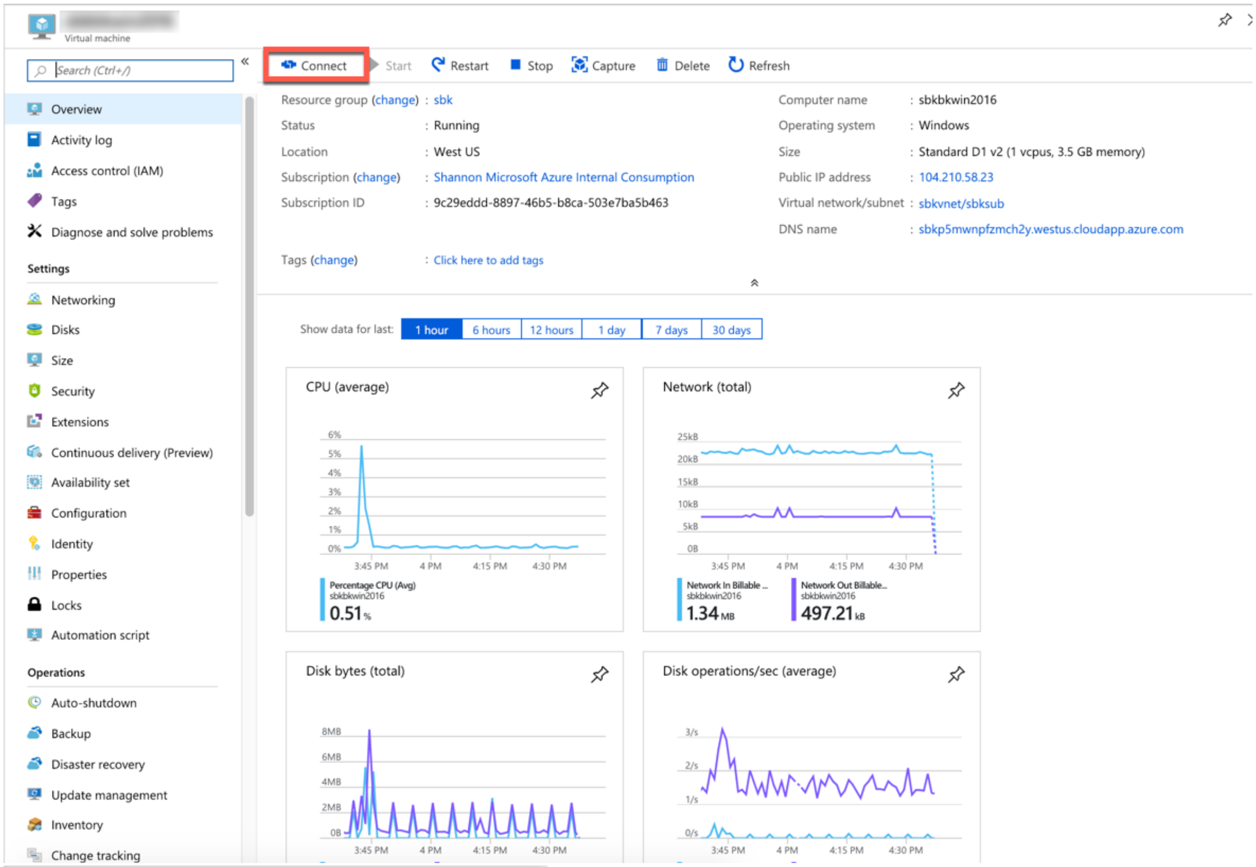
Deployments : 1 Succeeded

9 items

NAME	TYPE	LOCATION
[redacted]	Storage account	West US
[redacted]	Key vault	West US
[redacted]	Recovery Services vault	West US
[redacted]	Virtual machine	West US
[redacted]	Disk	West US
[redacted]	Disk	West US
[redacted]	Network interface	West US
[redacted]	Public IP address	West US
[redacted]	Virtual network	West US

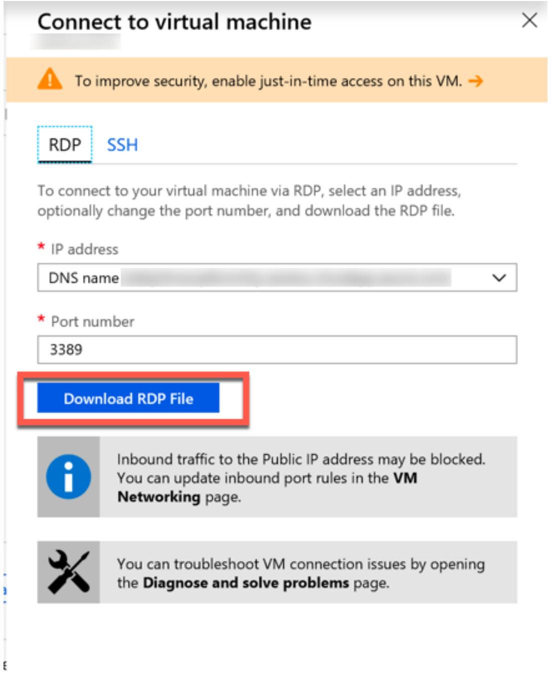
CREATE FILES ON SERVER DESKTOP

1. RDP to your VM from Azure. Click on the VM from the portal and then "Connect."



Resource group (change) : sbk
Status : Running
Location : West US
Subscription (change) : Shannon Microsoft Azure Internal Consumption
Subscription ID : 9c29eddd-8897-46b5-b8ca-503e7ba5b463
Tags (change) : Click here to add tags

Computer name : sbkbkwin2016
Operating system : Windows
Size : Standard D1 v2 (1 vcpus, 3.5 GB memory)
Public IP address : 104.210.58.23
Virtual network/subnet : sbkvnet/sbksub
DNS name : sbkp5mwnpfzmch2y.westus.cloudapp.azure.com


Connect to virtual machine

[redacted]

To improve security, enable just-in-time access on this VM. →

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

* IP address

DNS name [redacted]

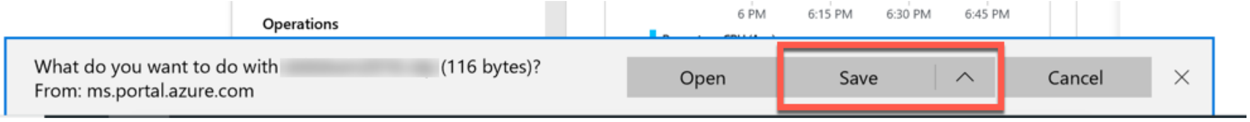
* Port number

3389

Inbound traffic to the Public IP address may be blocked. You can update inbound port rules in the **VM Networking** page.

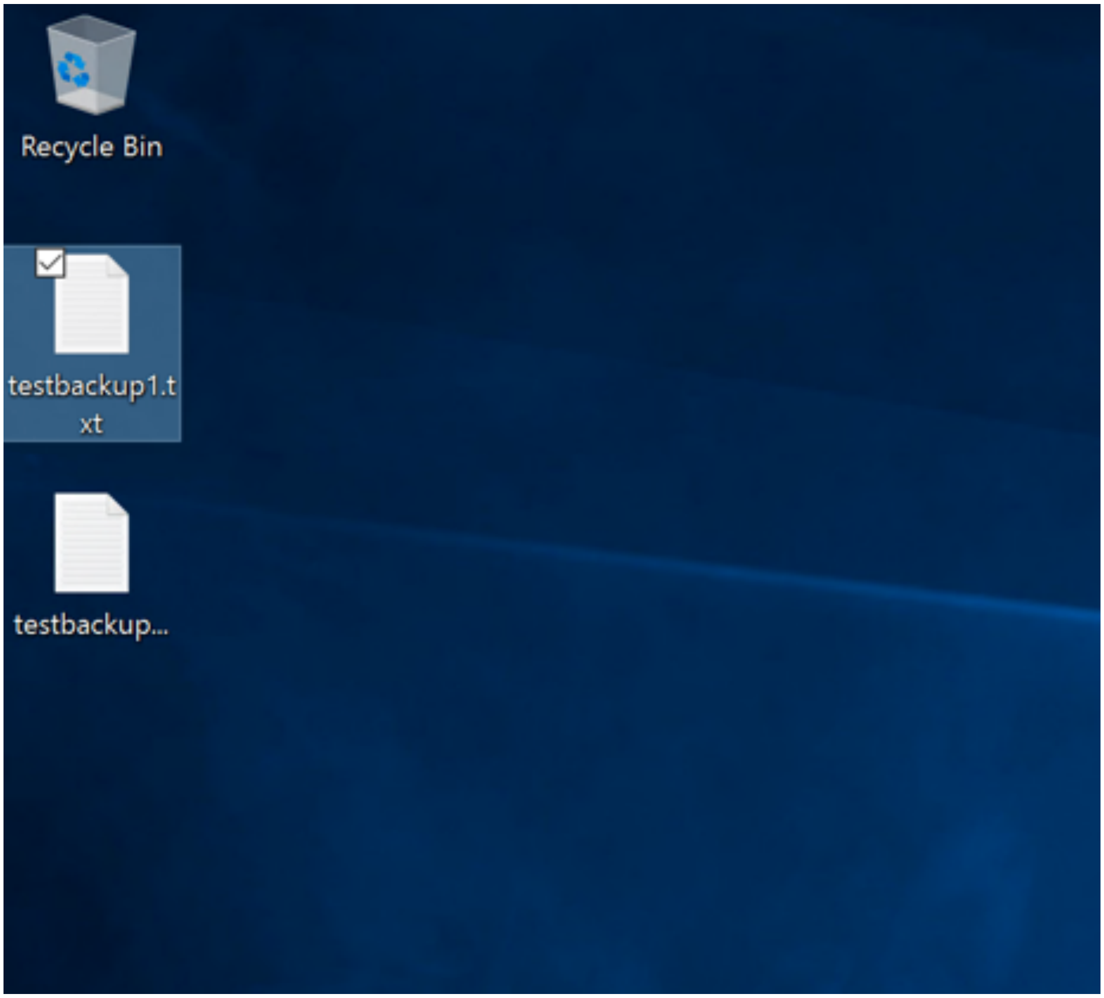
You can troubleshoot VM connection issues by opening the **Diagnose and solve problems** page.

2. When the terminal services file downloads, open up the file and connect to the VM in Azure using your username/password from when you made the Key Vault secret.



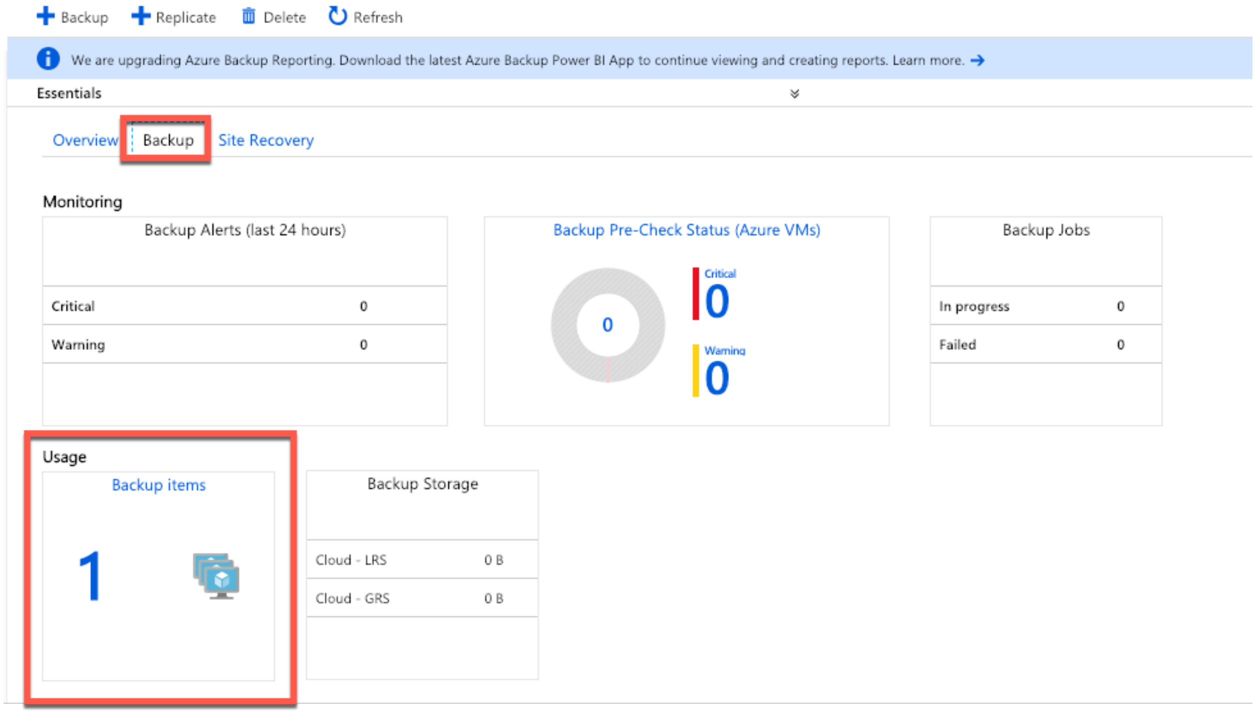
What do you want to do with [redacted] (116 bytes)?
From: ms.portal.azure.com

3. Create 2 files on the desktop of the server.



CONFIGURE BACKUPS

1. Ensure the VM registers to the Recovery Services Vault by clicking on the Backup tab. If you receive any errors during the ARM template deployment, try re-running the template. Click on "Backup Items."



We are upgrading Azure Backup Reporting. Download the latest Azure Backup Power BI App to continue viewing and creating reports. Learn more. →

Backup Alerts (last 24 hours)	
Critical	0
Warning	0

Backup Pre-Check Status (Azure VMs)

0

Critical 0

Warning 0

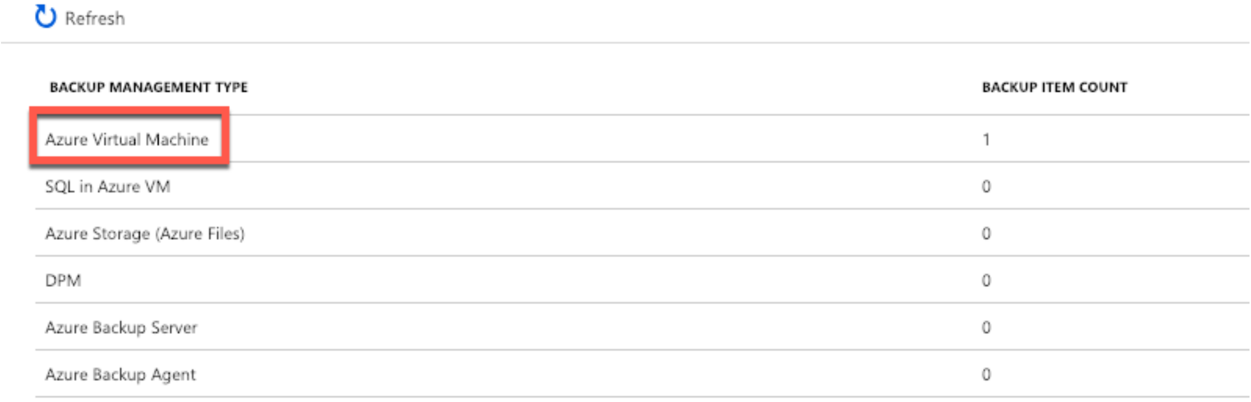
Backup Jobs	
In progress	0
Failed	0

Backup items

1

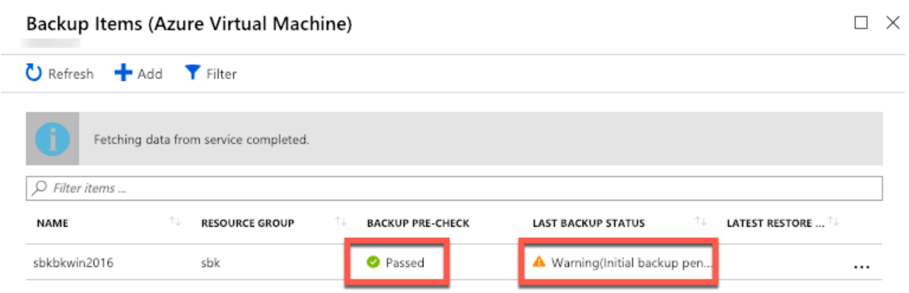
Backup Storage	
Cloud - LRS	0 B
Cloud - GRS	0 B

2. Take note of the Azure Virtual Machine count. Click on that section.



BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	1
SQL in Azure VM	0
Azure Storage (Azure Files)	0
DPM	0
Azure Backup Server	0
Azure Backup Agent	0

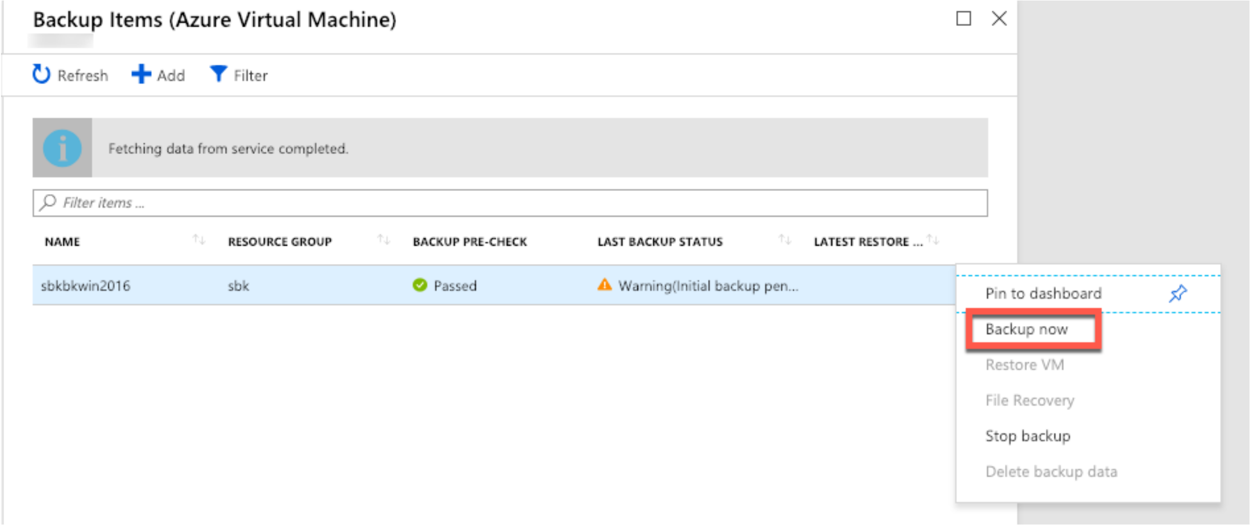
3. You should see the VM you just created, along with a backup pre-check passed green check mark, and a warning, indicating you have not yet backed up your VM.



Fetching data from service completed.

NAME	RESOURCE GROUP	BACKUP PRE-CHECK	LAST BACKUP STATUS	LATEST RESTORE ...
sbkbkwin2016	sbk	✓ Passed	⚠ Warning(Initial backup pen...	...

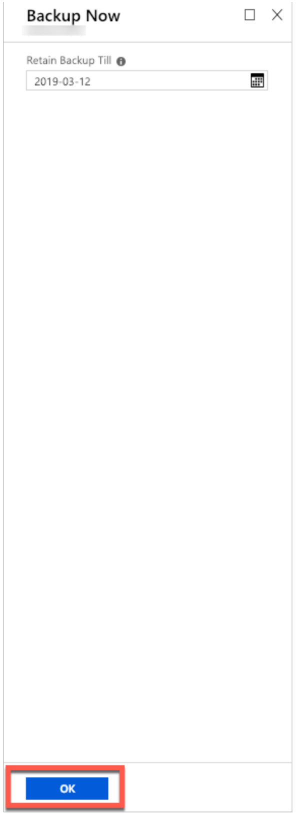
4. Click on the ellipses underneath “Latest Restore” and select “Backup now”:



Fetching data from service completed.

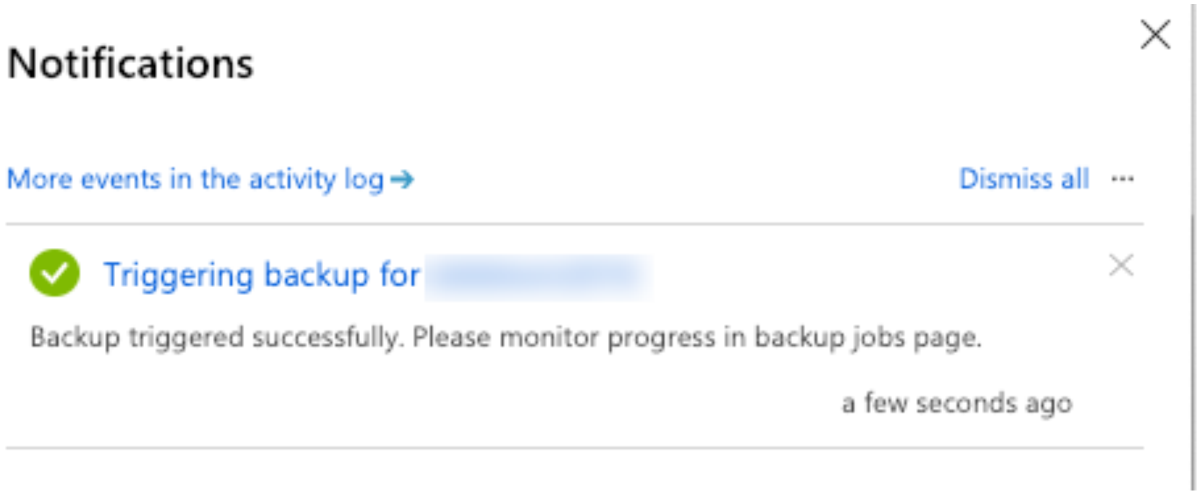
NAME	RESOURCE GROUP	BACKUP PRE-CHECK	LAST BACKUP STATUS	LATEST RESTORE ...
sbkbkwin2016	sbk	✓ Passed	⚠ Warning(Initial backup pen...	

5. Keep the pre-populated date and click “OK”:



Retain Backup Till: 2019-03-12

6. This task triggers a job, which can be monitored on the backup jobs page.



Notifications

More events in the activity log →

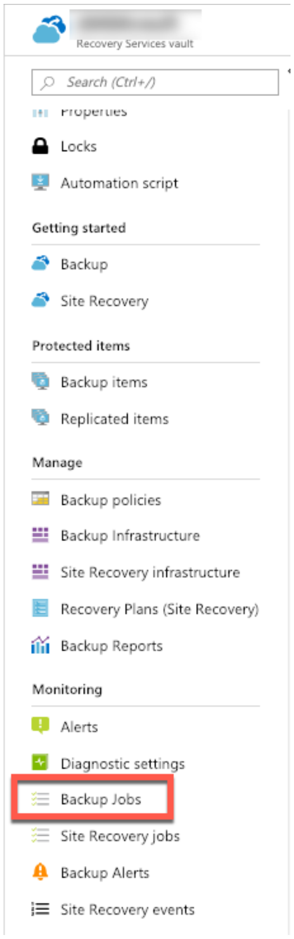
Dismiss all ···

Triggering backup for [redacted]

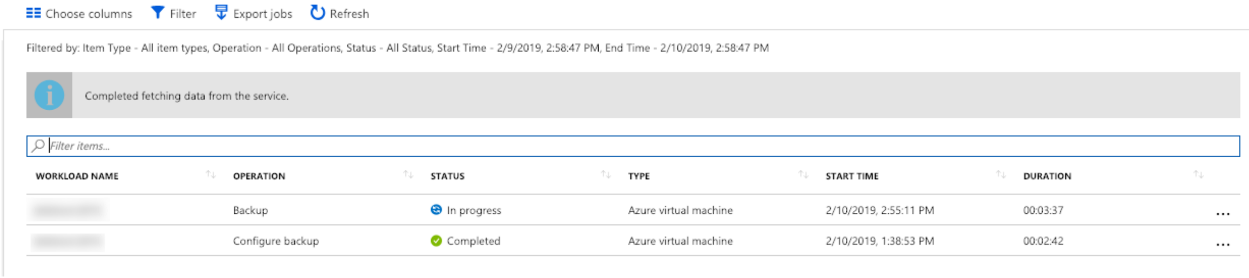
Backup triggered successfully. Please monitor progress in backup jobs page.

a few seconds ago

7. Underneath "Monitoring", you will see a Backup Jobs listed. Click on the Backup Jobs:



8. You should see the progress of your backup job. While this process finishes, start in on the Availability Zones lab:



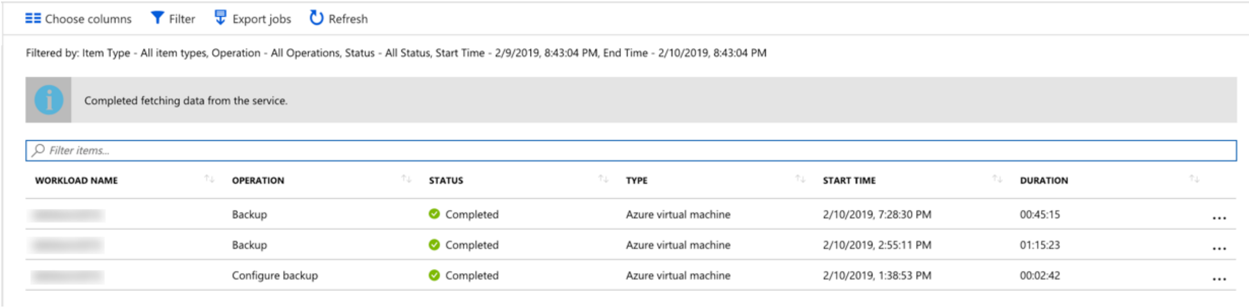
Filtered by: Item Type - All item types, Operation - All Operations, Status - All Status, Start Time - 2/9/2019, 2:58:47 PM, End Time - 2/10/2019, 2:58:47 PM

Completed fetching data from the service.

WORKLOAD NAME	OPERATION	STATUS	TYPE	START TIME	DURATION	
[redacted]	Backup	In progress	Azure virtual machine	2/10/2019, 2:55:11 PM	00:03:37	...
[redacted]	Configure backup	✓ Completed	Azure virtual machine	2/10/2019, 1:38:53 PM	00:02:42	...

RESTORE FILE ON THE VIRTUAL MACHINE

1. After the Availability Zone lab, flip back to the backup job progress. Once you see something like this in the job history, move on to the next step:

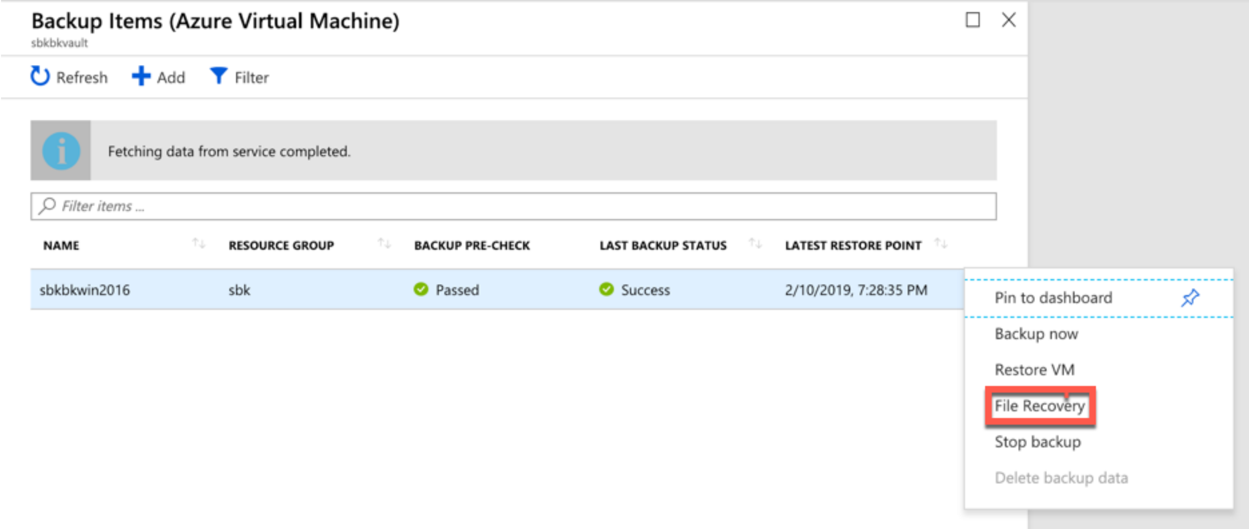


Filtered by: Item Type - All item types, Operation - All Operations, Status - All Status, Start Time - 2/9/2019, 8:43:04 PM, End Time - 2/10/2019, 8:43:04 PM

Completed fetching data from the service.

WORKLOAD NAME	OPERATION	STATUS	TYPE	START TIME	DURATION	
[redacted]	Backup	✓ Completed	Azure virtual machine	2/10/2019, 7:28:30 PM	00:45:15	...
[redacted]	Backup	✓ Completed	Azure virtual machine	2/10/2019, 2:55:11 PM	01:15:23	...
[redacted]	Configure backup	✓ Completed	Azure virtual machine	2/10/2019, 1:38:53 PM	00:02:42	...

2. On the server, delete 1 of the files you created.
3. Click on Backup Items, Azure Virtual Machines,

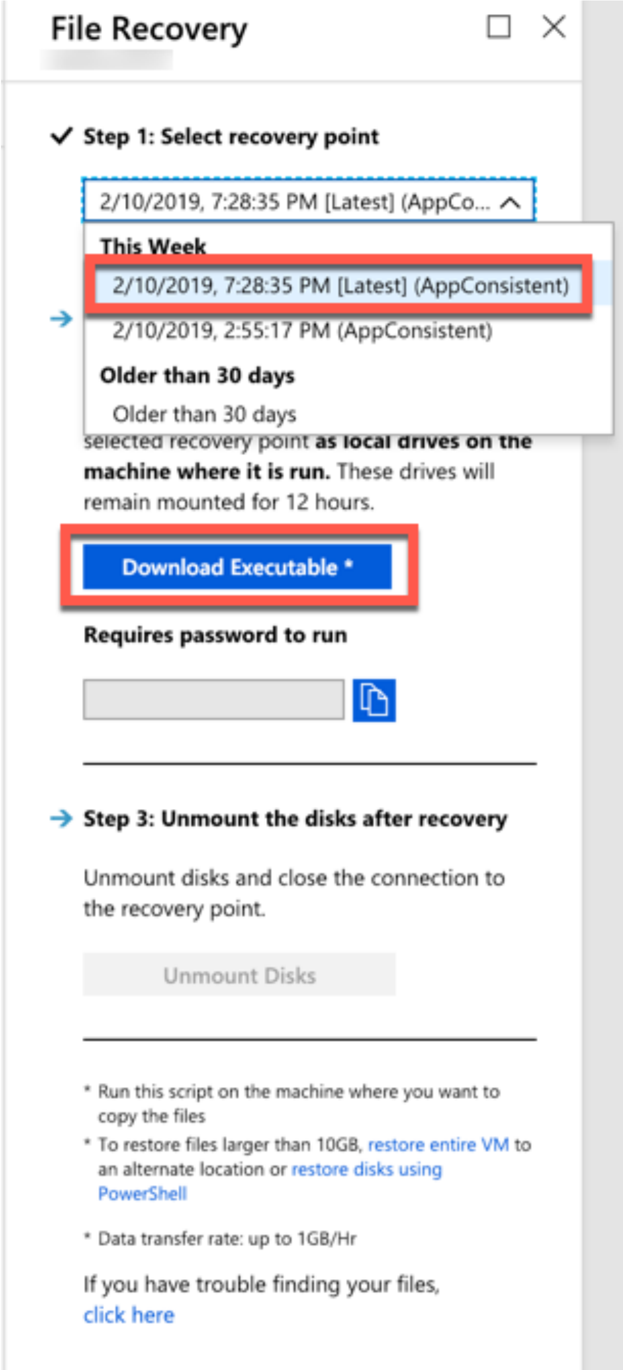


Backup Items (Azure Virtual Machine)
sbkbkvault

Fetching data from service completed.

NAME	RESOURCE GROUP	BACKUP PRE-CHECK	LAST BACKUP STATUS	LATEST RESTORE POINT
sbkbkwin2016	sbk	✓ Passed	✓ Success	2/10/2019, 7:28:35 PM

4. Pick the latest Application Consistent snapshot and click on Download Executable. For ease of use, download the executable on the Azure virtual machine:



File Recovery

✓ Step 1: Select recovery point

2/10/2019, 7:28:35 PM [Latest] (AppCo...

This Week

2/10/2019, 7:28:35 PM [Latest] (AppConsistent)

2/10/2019, 2:55:17 PM (AppConsistent)

Older than 30 days

Older than 30 days

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

Requires password to run

→ **Step 3: Unmount the disks after recovery**

Unmount disks and close the connection to the recovery point.

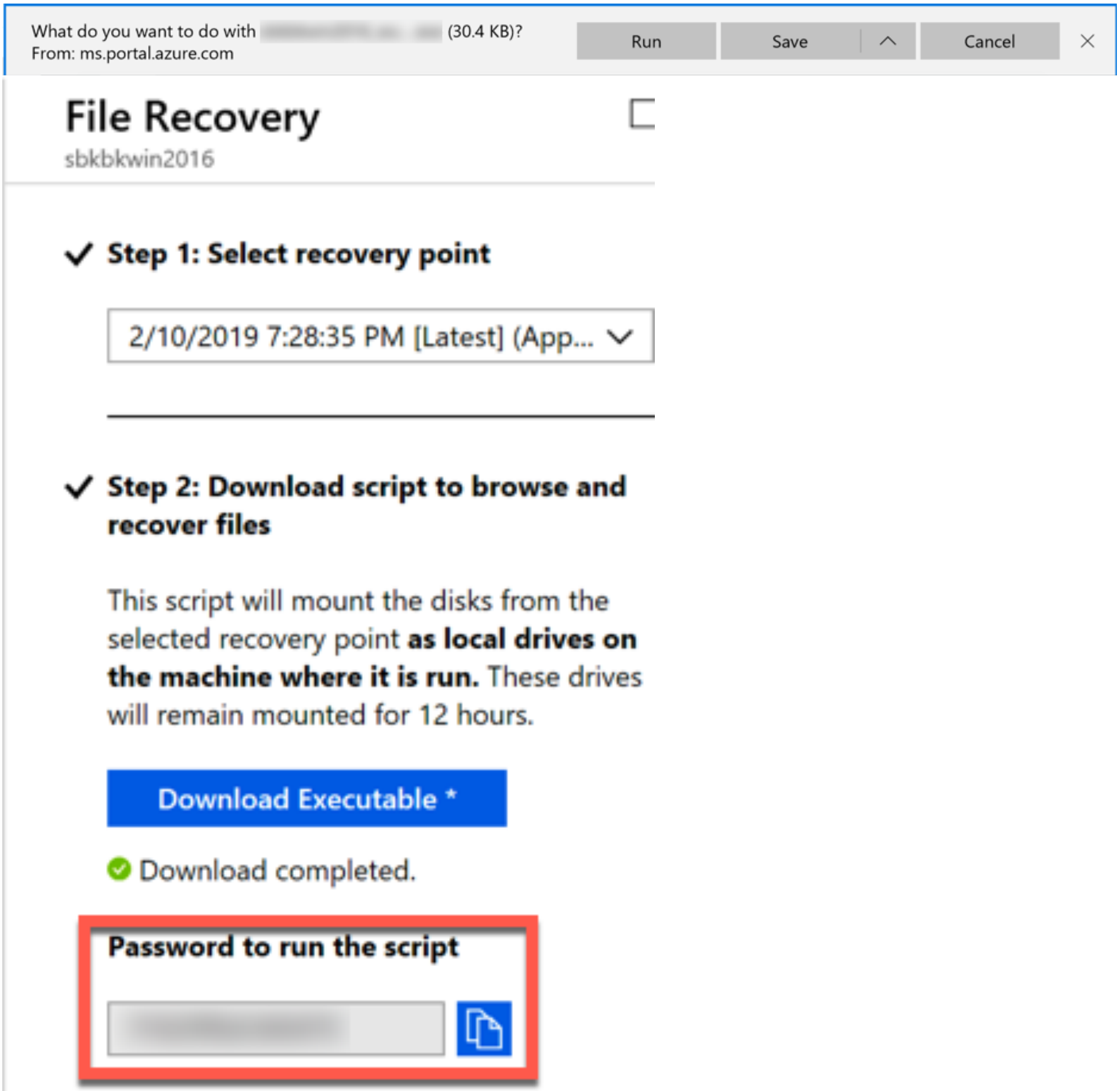
* Run this script on the machine where you want to copy the files

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

* Data transfer rate: up to 1GB/Hr

If you have trouble finding your files, click here

5. Once the executable downloads, you will be prompted to save or run the file. The file needs to run as an elevated account, so saving it locally will help. Additionally, you will be presented with a 1 time password to run the script that restores the file.



What do you want to do with [redacted] (30.4 KB)?
From: ms.portal.azure.com

File Recovery
sbkbkwin2016

✓ Step 1: Select recovery point

2/10/2019 7:28:35 PM [Latest] (App...

✓ Step 2: Download script to browse and recover files

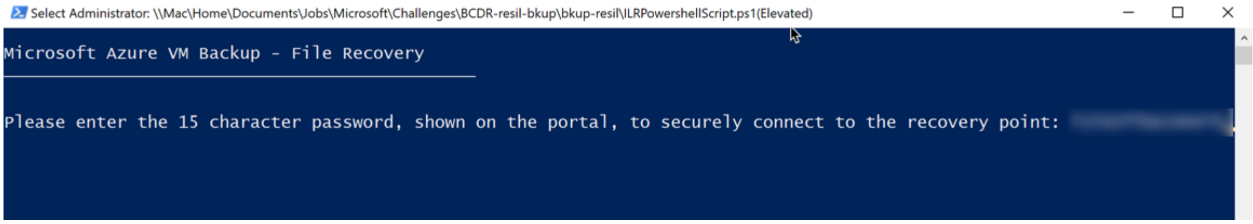
This script will mount the disks from the selected recovery point **as local drives on the machine where it is run.** These drives will remain mounted for 12 hours.

✓ Download completed.

Password to run the script

[redacted]

6. Once the file is launched, PowerShell will open. Input the password generated from downloading the executable file.

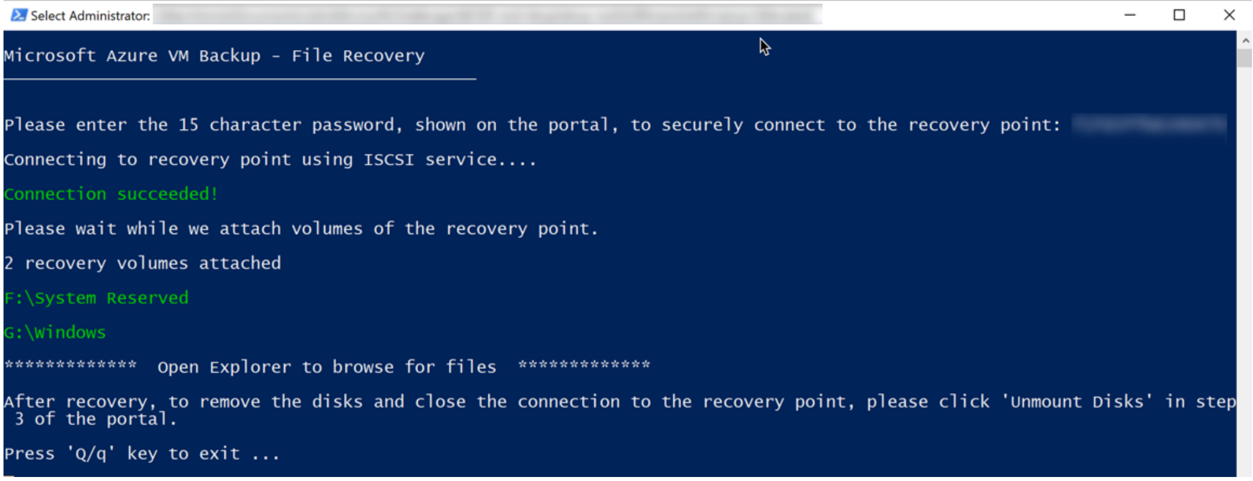


```
Select Administrator: \\Mac\Home\Documents\Jobs\Microsoft\Challenges\BCDR-resil-bkup\bkup-resil\ILRPowershellScript.ps1(Elevated)
```

```
Microsoft Azure VM Backup - File Recovery
______________________________________________

Please enter the 15 character password, shown on the portal, to securely connect to the recovery point: [redacted]
```

7. Upon establishing the connection, Azure Backup will mount the files to the local server.

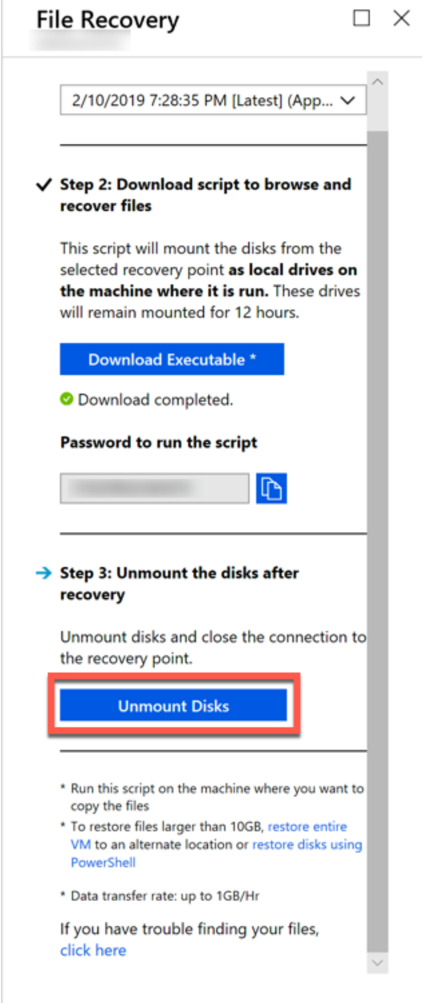


Select Administrator: [redacted]

```
Microsoft Azure VM Backup - File Recovery
_____________________________________________

Please enter the 15 character password, shown on the portal, to securely connect to the recovery point: [redacted]
Connecting to recovery point using ISCSI service....
Connection succeeded!
Please wait while we attach volumes of the recovery point.
2 recovery volumes attached
F:\System Reserved
G:\Windows
*************  Open Explorer to browse for files  *************
After recovery, to remove the disks and close the connection to the recovery point, please click 'Unmount Disks' in step
 3 of the portal.
Press 'Q/q' key to exit ...
```

8. Open up Windows Explorer, browse to the mounted drive, and copy files over to the local desktop.
9. Press Q or q to exit.
10. Ensure you unmount the disks from the server:



File Recovery

[redacted]

2/10/2019 7:28:35 PM [Latest] (App...

✓ **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.

Password to run the script

[redacted]

→ **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 1GB/Hr

If you have trouble finding your files, click here

11. After a few seconds, the drives will disappear.

RESTORE VIRTUAL MACHINE FROM BACKUP

1.