Azure for Disaster Recovery Camp   
Hands-On Labs

## Labs

Lab 0: **Login to the Azure Portal** – Preliminary lab requirements  
Lab 1: **Backup an Azure Virtual Machine** – Backup an Azure VM using the built-in portal tools  
Lab 2: **Using Azure Backup** – Use Azure Backup to simulate backing up an physical on-prem server to Azure  
Lab 3: **Copy Files with AZCopy** - Use the command line tool to copy VHD files to Azure Storage Accounts  
Lab 4: (Optional) **Backup a Windows Client to Azure** - Backup your local client machine to Azure Backup.

## Lab Requirements

The following components are required to successfully complete this Hands-on Lab:

* A Microsoft Azure Account and Credentials
* A modern web-browser with HTML5 and JavaScript enabled
* Remote Desktop Client connection software
* Internet connectivity
* Identification for building access
* 10” or larger screen recommended
* Your own wireless hotspot (if you have one)
* The ability to install software (admin rights) for the installation of the AZCopy Tool.

Through the labs, you will be required to name some items in a unique manner due to Azure external DNS requirements. When needed, we suggest adding a prefix or appending your initials or name to the names of components in the lab.

Lab 0 - Login to the Azure Portal

In this task you will login into the Azure Portal to ensure your subscription is ready to go.

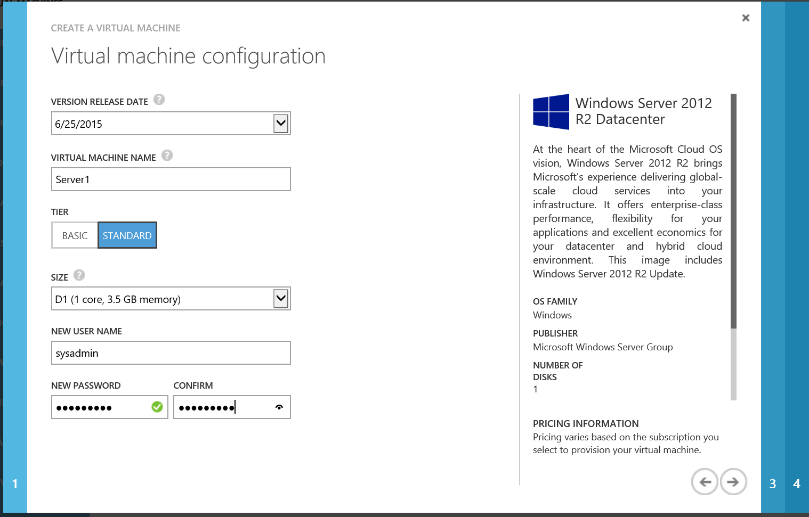
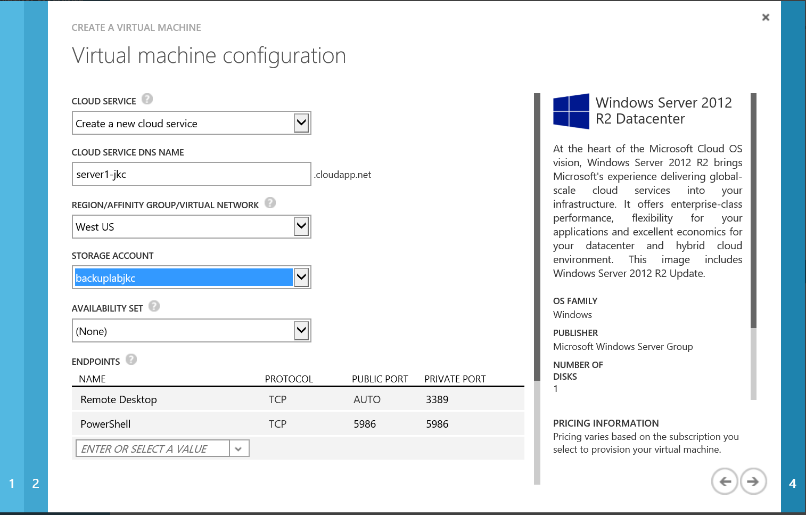
Perform the following tasks:

1. Open a browser, and then navigate to **http://manage.windowsazure.com**.
2. Click **PORTAL** located at the top of the Microsoft Azure site.
3. Log in using your Microsoft Azure credentials for your Microsoft Azure subscription.
4. If this is your first time logging into your Azure management portal, close the WINDOWS AZURE TOUR.

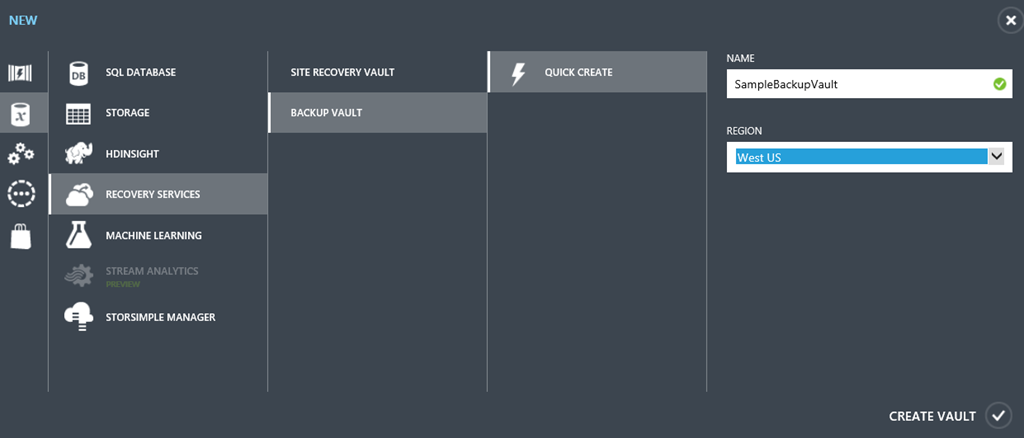
## Lab 1 - Backup an Azure VM

In this lab, you will use the Azure Portal to backup an Azure Virtual Machine.

#### Create a new Storage Group and Virtual Machine

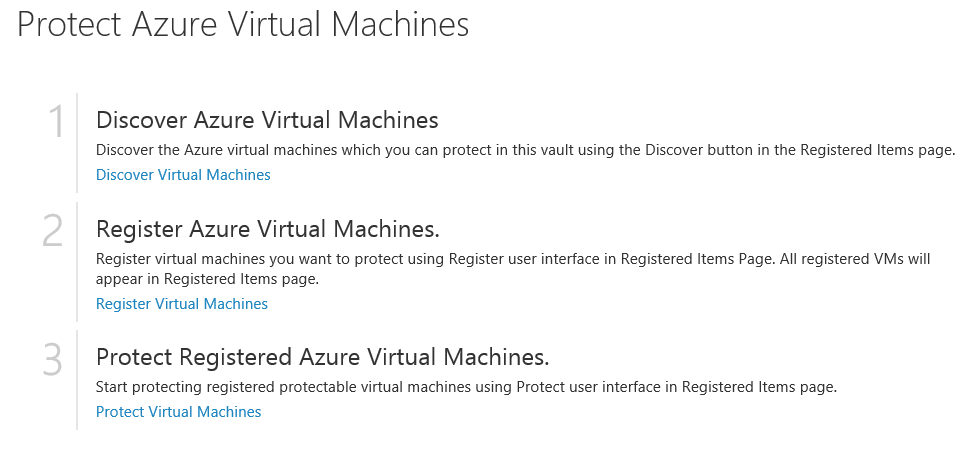
1. Log into the Azure Portal at <http://manage.windowsazure.com>
2. On the lower left, select “NEW”
3. Select **DATA SERVICES -> STORAGE -> QUICK CREATE**
4. For the Storage Account Configuration, use:
   1. URL – **backuplab<unique>** Use “backuplab” and something unique to you to complete the FQDN.
   2. Location – **West US** (You are welcome to use any location, just use that same region throughout all the labs for consistency.)
   3. Replication - **Locally Redundant**
5. Select **COMPUTE -> VIRTUAL MACHINE -> FROM GALLERY**
6. For Image, select   
   **Windows Server 2012 R2 Datacenter**
7. For Virtual Machine Configuration, use:
   1. Version Release Date - <most recent date>
   2. Virtual Machine Name – SERVER1
   3. Tier – Standard
   4. Size – A1
   5. Username – **sysadmin**
   6. Password – **Passw0rd!**
8. For the second configuration page, use:
   1. Cloud Service – Create New
   2. Cloud Service Name – <must be unique for you>
   3. Region – **West US**
   4. Storage Account - <Select the account your created in Step #4
   5. Availability Set – None
   6. Endpoints – Leave as default
9. Leave the final page of the configuration wizard at its defaults and click the checkmark at the bottom right to create the virtual machine. (It will take a few minutes to configure the virtual machine, continue on in the lab.)

#### Create a Backup Vault

1. On the lower left, select **“NEW”**
2. Select **DATA SERVICES -> RECOVERY SERVICES -> BACKUP VAULT -> QUICK CREATE**
3. For the Vault Configuration, use:
   1. Name – **“BackupLabVault”**
   2. Region – **West US**

#### Protect a Virtual Machine

Wait for your virtual machine status to become “running” before continuing with the lab steps.

1. Go to "Recovery Services" on the left hand scroll bar. Click on your backup vault and you will be on the quick start page indicating that your vault was created. Click the **“Registered Items”** tab at the top. You will have no items registered.
2. Click the **“Discover”** icon in the bottom navigation bar.
3. Once the discover process completes, click “**Register”** to access a list of Azure Virtual Machines. Check the box next to your server, then click the checkmark at the bottom right of wizard to continue. Wait for the status of your VM to become “**Registered**”.
4. Click the **Policies** tab.
5. Review the “DefaultPolicy” and edit it to perform the backup as soon as possible. Backups can be scheduled on any half hour segment. Set the backup time to be the next closest ½ hour mark.  (You will have to de-select the already-checked time before selecting your new backup time.) Save your changes.
6. Click on the “Recovery Services” tab on the far left of the Azure portal. Then click on the name of the backup vault you just created. Confirm that you are on the “quick launch” page (denoted by a cloud in the navigation bar) and scroll all the way to the bottom of the page. Under Protect Azure Virtual Machines choose the “Protect Virtual Machines” link under number 3. 
7. Click **“Protect”** from the bottom navigation bar.Select your server from the list of registered servers. Configure protection using the DefaultPolicy that you edited.  
   
8. The backup job with take about 15 minutes and may start a few minutes after your selected time. Wait until the backup job is completed. You can check the status of the jobs using the **Jobs** tab.

#### Restore a Virtual Machine

1. Once your backup job completes, go to your list of Virtual Machines, delete your Server-1. Do not retain the disks.
2. Go to **RECOVERY SERVICES** and select your backup vault.
3. Go to the **Protected Items** tab.
4. Highlight your server name and you should have one recovery point. Select **Restore** from the bottom navigation.
5. Step through the wizard to select the recovery point (you will only have one option) and kick off the restoration. It will take about 20 minutes for the server to be recovered.

## Lab 2 – Using Azure Backup

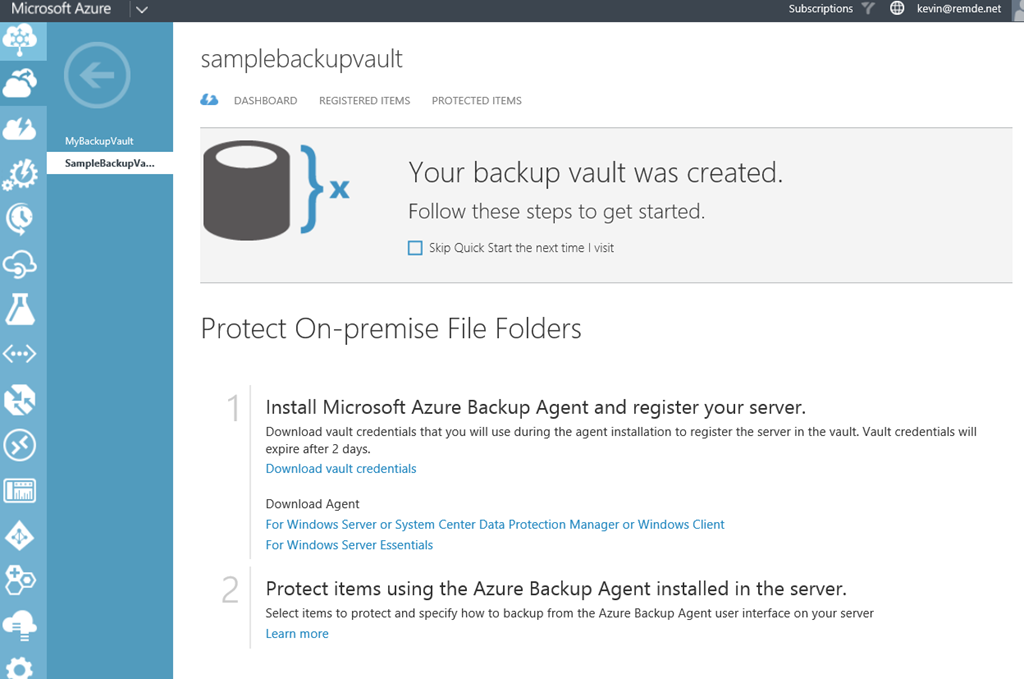
In this lab, you will simulate using Azure as a backup destination for a Windows Server or client device you have on-prem. To avoid installing the backup client on your local workstation, you will build a Windows Server in Azure to use as the source machine.

#### Create a Virtual Machine as your Source Server

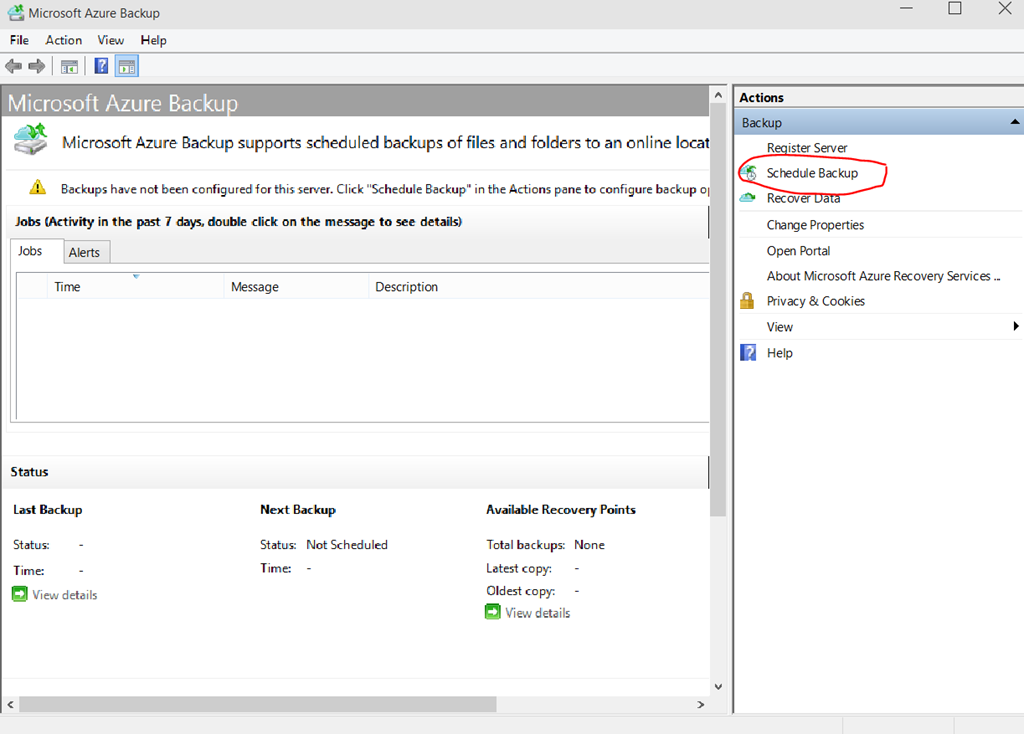
1. Go to **COMPUTE -> VIRTUAL MACHINE -> QUICK CREATE.** Enter a unique name for your server (such as SERVER02 and add something unique like your initials to this server name), select the same region you used in Lab 1 and set a username and password. We recommend sysadmin/Passw0rd!

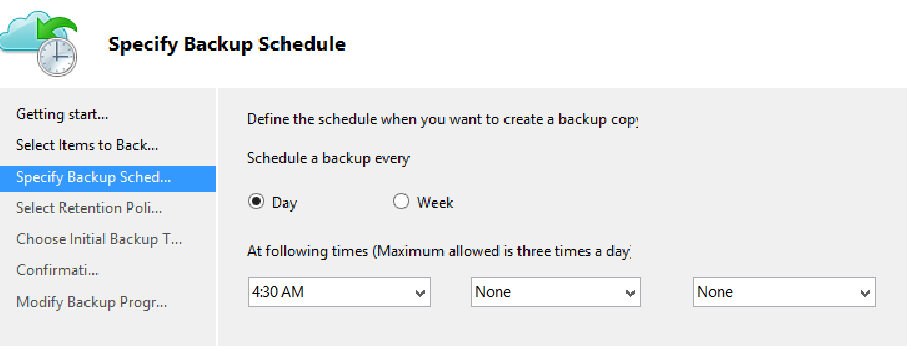
#### Establish a Trust to Azure

To establish a secure trust between your backup vault and the server being backed up, you will need to download the vault credentials. These credentials will be used to initially register a server or workstation or to recover items to a new machine. Because you will need to install these credentials directly on the machine, log into your newly created VM.

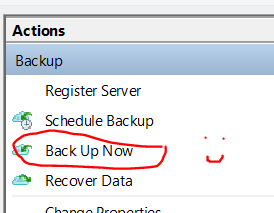
1. Once it is in a running state, select your newly created virtual machine. Click **Connect** from the bottom navigation bar and log into it via RDP.
2. Server Manager should launch automatically. Select **Local Server** and turn off IE’s Enhanced Security mode.
3. Launch File Explorer and create the C:\Important\_Stuff folder on your server. Inside that folder, create a blank txt file or other document called “This Is Very Important.txt” (You will be backing up this folder later in the lab.)
4. While still on the RDP Console of Server2, click on the Windows button in the bottom left hand of the screen and launch Internet Explorer. Navigate to <http://manage.windowsazure.com>. Log into your Azure Subscription.
5. On the left-hand navigation, scroll to **RECOVERY SERVICES.**
6. Click the name of the backup vault you created in Lab 1 to get to the Quick Start page. Click **Download Credentials**. Save the file some you’ll remember on the machine to be backed up. *In a production environment, you’ll want to treat these credential files with care.*
7. Return to the Quick Start page and download the backup agent for **Windows Server or System Center Data Protection Manager or Windows Client** and run it to install.
8. For the purposes of the lab, you can accept all the defaults. The agent will install any other missing required components. Select "I do not want to use Microsoft Updates" for this lab exercise.
9. If the client software does not automatically launch, click on the Windows button, go to Start, type in Azure, then click on Microsoft Azure Backup. In the right hand menu action pane click on **Register Server** in order to associate your server with your Azure subscription.
10. When prompted, browse to the location you saved your vault credentials and then click **Next.**
11. On the **Encryption Settings** page, you can either generate or enter your own Passphrase. Enter a local drive to save the passphrase file for this lab, however in production these passphrases should be kept somewhere secure.
12. Click “Finish” to complete the registration process.
13. Once finished with registration click “Close”. This will return you to the Microsoft Azure Backup client software.

#### Configure the Back Up Job

At this point, you have done all the configuration of your server to backup data to Azure. If you return to the Backup Vault configuration in the Azure portal, you will see the name of the server listed in the “protected” tab. In the next steps, you’ll configure your backup job.

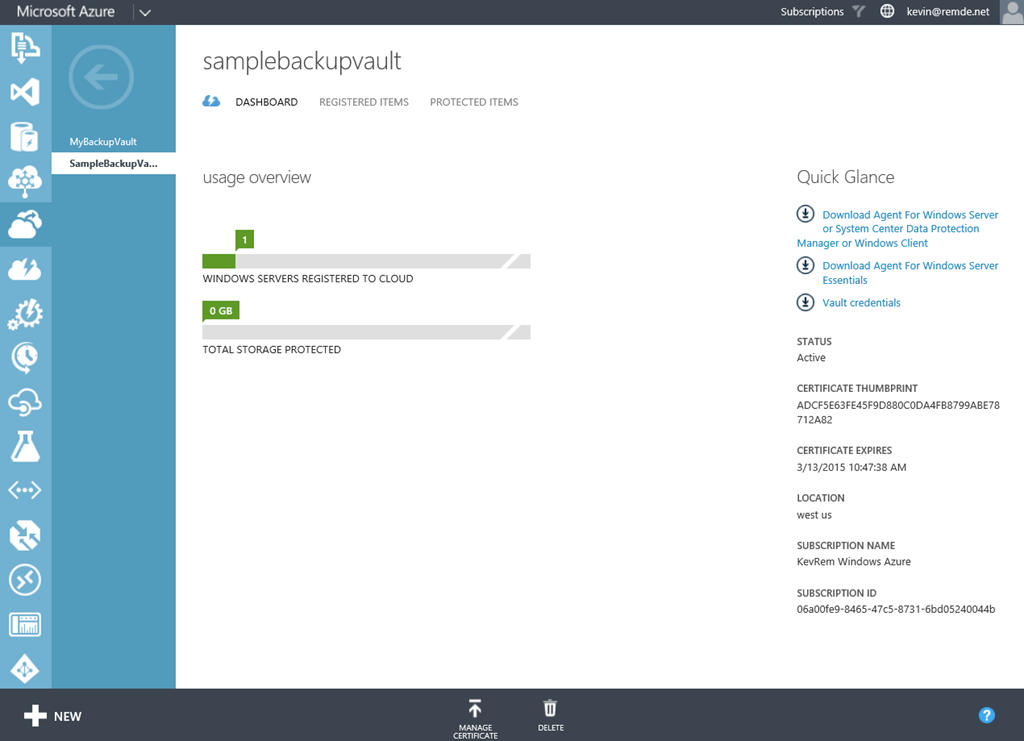
1. In the Microsoft Azure Backup tool, in the Actions pane, click on “Schedule Backup”.
2. Click “Next” on the Getting Started page to move onto the “Select Items to Backup” portion of the wizard.
3. Browse to and select the “C:\Important\_Stuff” folder you created earlier. Click “Next”.
4. On the “Specify Backup Schedule” page notice that you can choose to backup daily at a certain time, or during specific days of the week. Scheduled your backup for daily at 4:30am, then click “next”. 
5. On the “Select Retention Policy” page, review the options for retaining the backed-up data. You do not need to make any adjustments for lab. Accept the defaults and click “next”.
6. On the “Choose Initial Backup Type”, use the **"Automatically over the network"** default setting. You do have the option to “seed” your backup in an “offline” way as well.
7. On the “Confirmation” page, review your selections and click “Finish” to create the backup schedule.

No backup has launched yet, but would happen based on the schedule you’ve set.

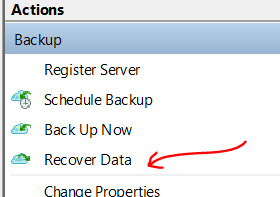
1. Click the **“Back Up Now”** option in the Actions pane.
2. On the resulting **Confirmation** page, click **“Back Up”.** Leave the console open to watch the status of this small backup job until it is completed. For larger jobs, you can close the status window and let the launched job run in the background.
3. Delete the file "This Is Very Important.txt" from your server. We will now verify the backup and restore the file.

#### Verify the Data in the Backup Vault

To confirm that the backup was successful, review the status of the Backup Vault in Azure.

1. Return to the Azure Portal and navigate to the **RECOVERY SERVICES** section. Click on the Backup Vault.
2. Select the **Dashboard** tab, you will see that you have one server registered with 0 GB protected. (The small size of the file backed up doesn’t register in the portal dashboard.)
3. Select the **Registered Items** tab, notice that Azure Virtual Machine is still listed from the previous lab. Drop down the menu and select “Windows Server” then click on the checkmark to the right to see the newly added on-prem server listed. This is where you can delete registrations of decommissioned servers as well.
4. Select the **Protected Items** tab. Here you can see some basic information about what is protected. A file folder with only one recovery point available.

#### Restore Deleted Data

1. On your Source Server, minimize the Azure Portal window and launch File Explorer. Delete the file you created in your C:\Important\_Stuff folder.
2. Return to the Microsoft Azure Backup console and click “Recover Data” in the Action pane.
3. On the **Getting Started** page, select “This server”, since the machine was the original backup source and is already registered with the backup vault. If you were on a new machine, you would be prompted to provide the vault credentials before continuing.
4. On the **Select Recovery Mode** page, select “Browse for files” and click “next”.
5. On the **Select Volume and Date** page, use the drop down menu to pick the volume and date available. You will only have one option since you only have one recovery point at this time.
6. On the **Select Items to Recover** page, browse to the file that was deleted, select it and click “next”.
7. On the **Specify Recovery Options** page, review the options to recover to a different location, duplication handling and permissions management. For this lab, leave the defaults and click “next.”
8. On the **Confirmation** page, click “recover” and close the window.
9. Back in the Microsoft Azure Backup console, you can see the recovery job status.
10. Once completed, browse to the file location on the server and verify it was restored.

## Lab 3 – Copy Files with AZCopy

AZCopy is a useful command line tool for copying files with the Azure Cloud Storage. You can use it to copy files up to Azure Storage for backup purposes. You can use it to copy files from one Azure Storage Account to another Azure Storage Account and it will perform a server to server copy. We will cover two scenarios in this lab.

Scenario 1:   
In the first part of this lab you will use the command line tool called AZCopy to recursively copy a subdirectory and files from your local machine to Azure Storage.

Scenario 2:   
In the second part of this lab you will use AZCopy to copy a VHD from one storage account to another.

#### Install AZCopy on your Local Machine

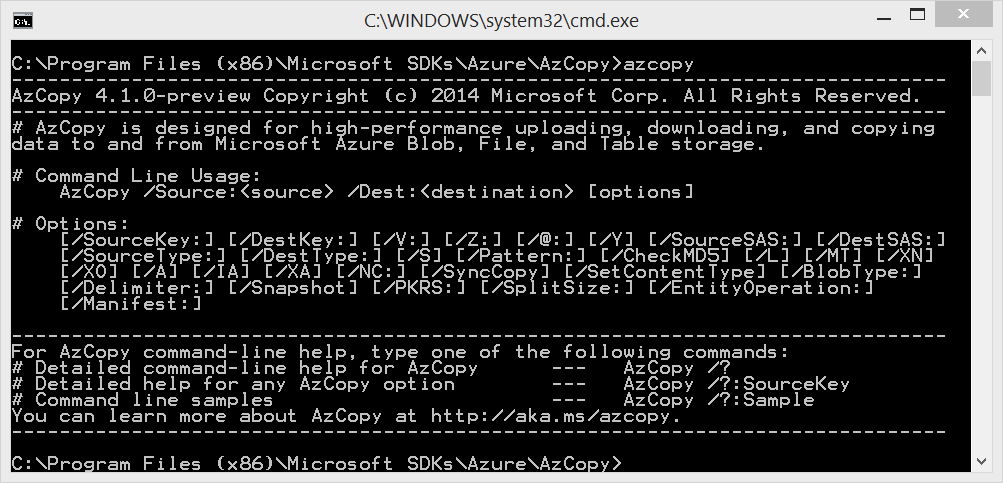
1. Download the AZCopy tool (http://aka.ms/downloadazcopy) and install it on your local machine.
2. Open a command prompt and change to the directory where AZCopy is installed.  
   (By default, the AzCopy installation creates a folder named AzCopy under %ProgramFiles(x86)%\Microsoft SDKs\Azure\ (on 64-bit Windows) or %ProgramFiles%\Microsoft SDKs\Azure\ (on 32-bit Windows).)

At the command prompt enter the following command:

cd "\Program Files (x86)\Microsoft SDKs\Azure\AzCopy"

Press Enter.

1. Type azcopy.exe [enter]  
   You should see this:



#### Locating storage access key; Preparing to copy files

1. Click the Windows button and type in Notepad, then launch Notepad.exe (We will use notepad to keep track of your information and build your commands)
2. Head back to the Azure Management Portal, click on Storage in the left navigation menu, locate the storage account you created in Lab 1. At the **Dashboard** tab, look in the navigation bar at the bottom, click **Manage Access Keys.** Copy your primary key to notepad.
3. On the **Dashboard** tab of your storage account, copy the blob endpoint URL and paste it into notepad. It will be something similar to: *https://<storageaccountname>.blob.core.windows.net or https://*backuplab<unique>*.blob.core.windows.net*
4. Create a folder named “myfolder” on your c: drive. “C:\myfolder”

Copy the "This Is Very Important.txt" into the new folder named c:\myfolder.

#### Upload files from the file system to Blob storage

Due to the time needed to upload a full VHD over shared Wi-Fi, these next steps are demonstrated with basic text files. However, you could use a similar process to upload a VHDs from your local network to Azure.

Using notepad file as a scratch area, build the command for copying your Lab Notes to Azure. In the command below, indicate the source location of your notes file, the correct account name for your storage account, the key for access to your storage account and the proper name of your notes file.  
  
AzCopy /Source:C:\myfolder /Dest:<storage URL>/labfiles /DestKey:key /Pattern: "This Is Very Important.txt"

It will look something similar to this:

|  |
| --- |
| AzCopy /Source:C:\myfolder /Dest:https:// backuplab<unique>.blob.core.windows.net/mycontainer /DestKey:<insert that long key you copied to notepad here> /S /Pattern:\*.txt |

Specifying option /S copies the contents of the specified directory to Blob storage recursively, meaning that all subfolders and their files will be copied as well.

1. Using CTRL-C or right click and “copy” to copy your command from notepad and right click paste to insert the command into your AZCopy window to execute.
2. Once the command completes, you can verify the addition of the containers and the files to your azure storage account by using the Azure portal. Click on the Storage tab, click on your Storage Account, click on the containers tab at the top, lastly browse to your folder or file.

#### Copy a VHD Blob between Storage Accounts

Extra Credit

|  |
| --- |
| As an extra credit exercise work with someone else near you to copy a vhd file from their storage account to your storage account and then import the VHD in as a VM. This is similar to the exercise below but you would use their storage account instead of itcampdata.blob.core.windows.net where we have a vhd for you to copy. There are several ways you can accomplish this including creating a publicly accessible folder or sharing keys. Have fun! |

We placed a VHD file located on an Azure Storage Account that we gave public read access to. This is just an Azure Storage area that has a backup of a VM. You will copy down this VHD file and then build an Azure VM using this VHD disk.

The file is named “WinITcamp-WinITcamp-2015-08-04.vhd” and is located in the “https://itcampdata.blob.core.windows.net/” storage account in a container called “bkup”

Here is the full link:

https://itcampdata.blob.core.windows.net/bkup/WinITcamp-WinITcamp-2015-08-04.vhd

1. Using your notepad file as a scratch area, build the command for copying a VHD blob between storage accounts in Azure. In the command below, indicate the source location of your VHD, the correct accounts name for your storage accounts, the keys for access to your storage accounts. This copy will complete in seconds if within the West US region or about 10-15 minutes to run across US regions.

AzCopy /Source:<storageaccount1 URL>/vhds /Dest:<storageaccount2 URL>/vhds /SourceKey:your-key /DestKey:your-key2 /S

Your command will look similar to this:

|  |
| --- |
| AzCopy /Source:https://itcampdata.blob.core.windows.net/bkup /Dest:https:// backuplab<unique>.blob.core.windows.net/mycontainer /DestKey:<insert your key> /Pattern:WinITcamp-WinITcamp-2015-08-04.vhd /S |

1. Using CTRL-C or right click and “copy” to copy your command from notepad and right click paste to insert the command into your AZCopy window to execute.
2. Once the command completes, you can verify the addition of the VHD to your storage account.

#### Create an VM from your copied disk

1. In the Azure portal, go to the **VIRTUAL MACHINE** section. Click the **DISKS** tab. In this list, you will see all the disks recognized as server VHDs files. At the bottom, click **CREATE.**
2. Enter a reference name for your new disk, such as **Server1-copy**. (This will not change the name of the actual file in the storage account.)
3. Enter the URL for the file you copied to the new storage account.
4. Select the checkbox to indicate that the VHD contains an operating system.
5. Select “Windows” from the Operating System Family. Click the circled checkbox to finish the operation.
6. Select **+NEW** from the bottom right of the Azure Portal to create a new Virtual Machine.
7. Select **COMPUTE -> VIRTUAL MACHINE -> FROM GALLERY**
8. Do not select an operating system image, instead highlight “My Disks” from the bottom left navigation in the wizard. Your newly created disk should be available to select.
9. Give the new virtual machine a name like “**WinITcamp”** and select D1 for the size.
10. For the Cloud Service name page:
    1. Cloud Service – Create New
    2. Cloud Service Name – <must be unique for you>
    3. Region – **West US**
    4. Storage Account - <Select the account where your new copy resides>
    5. Availability Set – None
11. Endpoints – Leave as default
12. Click through the remaining screen without any changes and complete the wizard.
13. Once the machine is running, you can connect via RDP using the same username and password as the original server (sysadmin/Passw0rd!)

AZCopy has more to offer and if you are interested in all it can do for you, take a look at the Azure team blog article here: <https://azure.microsoft.com/en-us/documentation/articles/storage-use-azcopy/>

# Lab 4 (Optional) - Backing up a Windows Client to Microsoft Azure Recovery Services Backup Vault

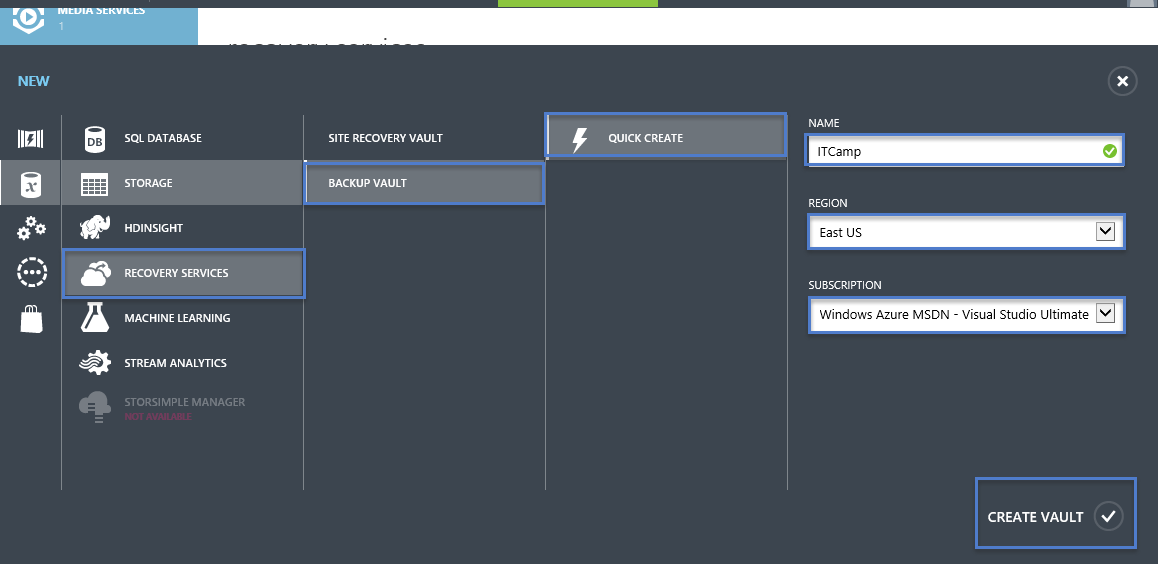
To back up files and data from your Windows Clients, Windows Server or System Center Data Protection Manager (SCDPM) to Azure or when backing up IaaS VMs to Azure, you must create a backup vault in the geographic region where you want to store the data. In this lab, we are going to backup a Windows Client machine to Microsoft Azure. Your machine can be Windows 7, Windows 8, Windows 8.1 or Windows 10. Make sure you have the latest service packs on your machine as well. Backups to a vault can be up to 1.7 Terabytes in size.

For more information on Microsoft Azure Recovery Services Backup Vault go to: <http://azure.microsoft.com/en-us/services/backup> For FAQ’s on Microsoft Azure Backup go to: [https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-faq](https://manage.windowsazure.com/)

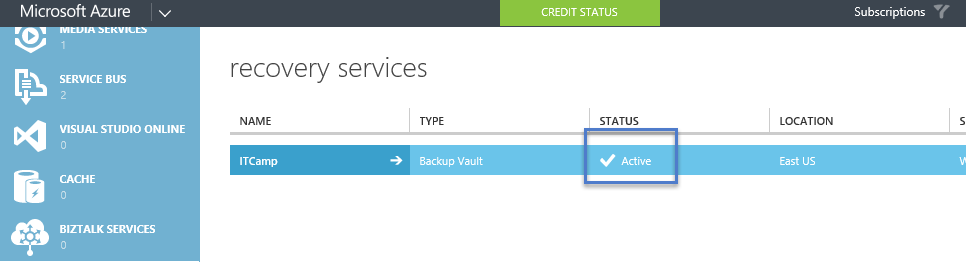
## Create a Backup Vault

1. Sign in to the Management Portal <https://manage.windowsazure.com>
2. Click **New** -> **Data Services** -> **Recovery Services** -> **Backup Vault** and choose **Quick Create**

* For the **Name** parameter, enter a friendly name to identify the backup vault. This needs to be unique for each subscription.
* For the **Region** parameter, select the geographic region for the backup vault. The choice determines the geo to which your backup data is sent. By choosing a geo close to your location, you can reduce the network latency when backing up to Azure.
* Click **Create Vault** to complete the workflow. It can take a while for the backup vault to be created. To check the status, you can monitor the notifications at the bottom of the portal.



1. After the backup vault has been created, a message will tell you the vault has been successfully created and it will be listed in the resources for Recovery Services as **Active**.



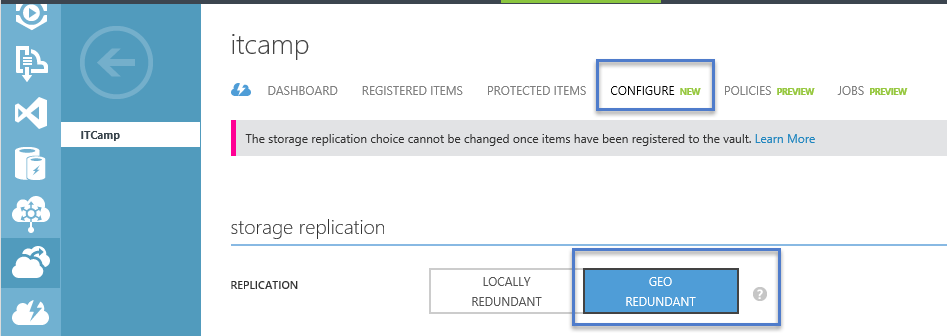
Azure Backup - Storage Redundancy Options

The best time to identify your storage redundancy option is right after vault creation, and before any machines are registered to the vault. Once an item has been registered to the vault, the storage redundancy option is locked and cannot be modified.

Your business needs would determine the storage redundancy of the Azure Backup backend storage. If you are using Azure as a primary backup storage endpoint (e.g. you are backing up to Azure from a Windows Server), you should consider picking (the default) Geo-Redundant storage option. This is seen under the **Configure** option of your Backup vault.

Geo-Redundant Storage (GRS)

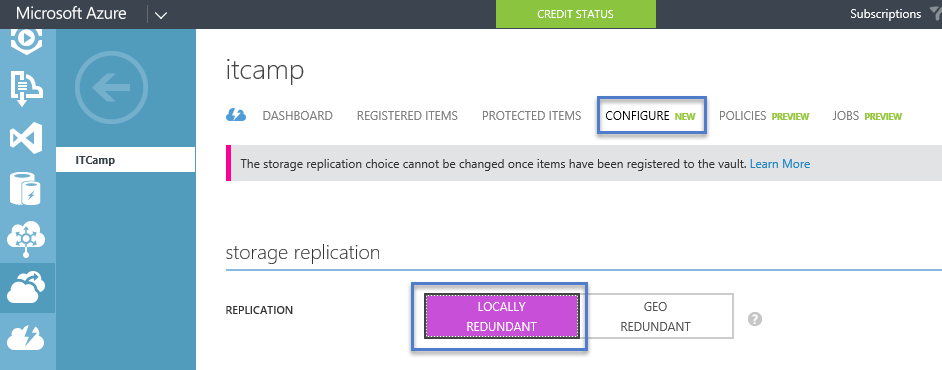
GRS maintains six copies of your data. With GRS, your data is replicated three times within the primary region, and is also replicated three times in a secondary region hundreds of miles away from the primary region, providing the highest level of durability. In the event of a failure at the primary region, by storing data in GRS, Azure Backup ensures that your data is durable in two separate regions.



Locally Redundant Storage (LRS)

Locally redundant storage (LRS) maintains three copies of your data. LRS is replicated three times within a single facility in a single region. LRS protects your data from normal hardware failures, but not from the failure of an entire Azure facility.

If you are using Azure as a tertiary backup storage endpoint (e.g. you are using SCDPM to have a local backup copy on-premises & using Azure for your long term retention needs), you should consider choosing Locally Redundant Storage from the **Configure** option of your Backup vault. This brings down the cost of storing data in Azure, while providing a lower level of durability for your data that might be acceptable for tertiary copies.



Note

* As of March 2015, customers do not have a programmatic (eg: PowerShell) way of creating a backup vault.
* The storage redundancy should be selected right after vault creation, and before any machines are registered to the vault. Once an item has been registered to the vault, the storage redundancy option is locked and cannot be modified.

# **Download Vault Credentials**

# Using vault credentials to authenticate with the Azure Backup service.

The on-premises server (Windows client or Windows Server or SCDPM server) needs to be authenticated with a backup vault before it can back up data to Azure. The authentication is achieved using “vault credentials”. The concept of vault credentials is similar to the concept of a “publish settings” file which is used in Azure PowerShell.

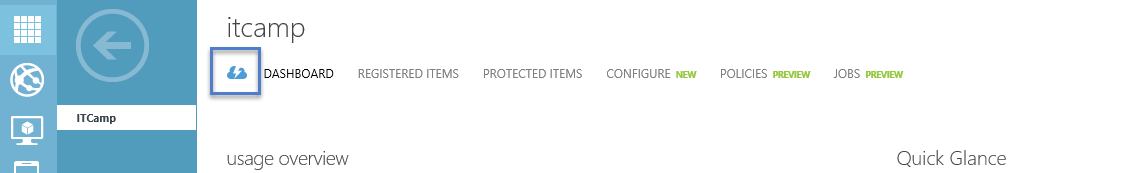
What is the vault credential file?

The vault credentials file is a certificate which is generated by the portal for each backup vault. The portal then uploads the public key to the Access Control Service (or ACS). The private key of the certificate is made available to the user as part of the workflow which is given as an input in the machine registration workflow. This authenticates the machine to send backup data to an identified vault in the Azure Backup service. It is worth calling out that the vault credential is used only during the registration workflow. It is the user’s responsibility to ensure that the vault credentials file is not compromised. If it falls in the hands of any rogue-user, the vault credentials file can be used to register other machines against the same vault. However, as the backup data is encrypted using a passphrase which belongs to the customer, existing backup data cannot be compromised. To mitigate this concern, the vault credentials is set of expire in 48hrs. You can download the vault credentials of a backup vault any number of times – but only the latest vault credential file is applicable during the registration workflow.

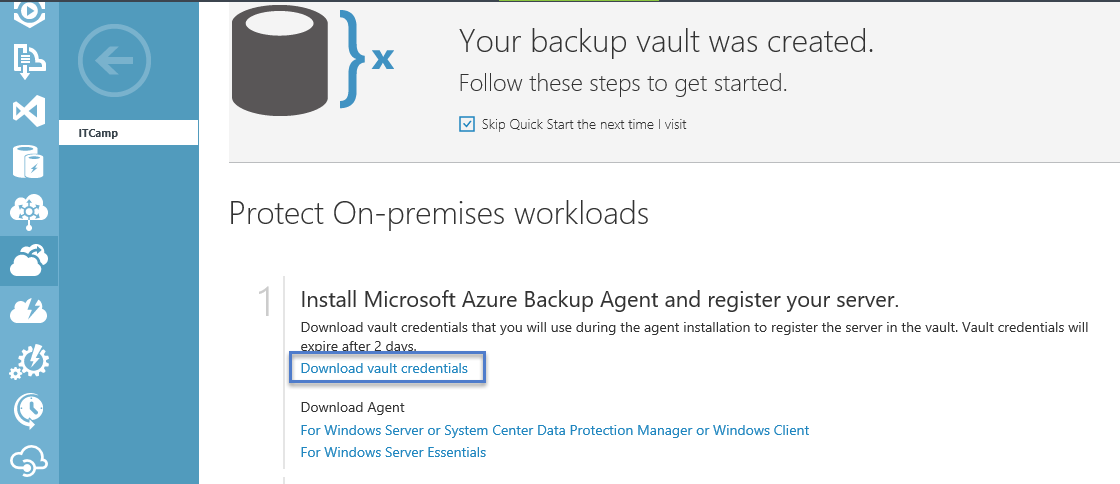
# Download the vault credential file

The vault credential file is downloaded through a secure channel from the Azure portal. The Azure Backup service is unaware of the private key of the certificate and the private key is not persisted in the portal or the service. Use the following steps to download the vault credential to a local machine.

1. If necessary, sign in to the [Management Portal](https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-faq) and click **Recovery Services** in the left navigation pane and select the backup vault which you have created.
2. Click the cloud icon to get to the Quick Start view of the backup vault.



1. On the Quick Start page, click **Download vault credentials**. The portal generates the vault credential file which is made available for download.



1. The portal will generate a vault credential using a combination of the vault name and the current date. Click **Save** to download the vault credentials to the local account's downloads folder, or select Save As from the Save menu to specify a location for the vault credentials.

Notes

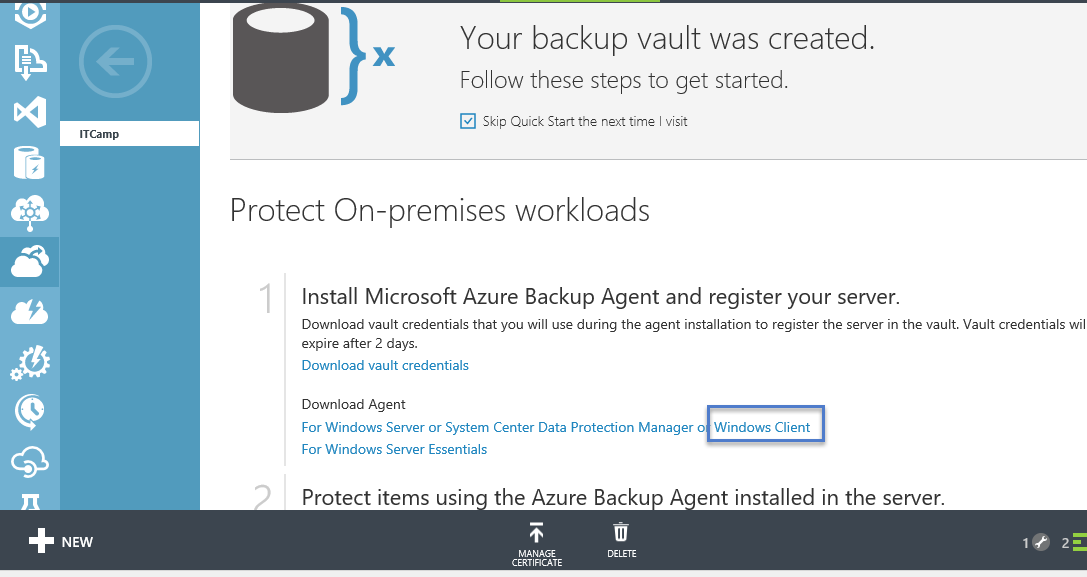
* As of March 2015, users do not have a programmatic (eg: PowerShell) way of downloading vault credentials.
* Ensure that the vault credentials are saved in a location which can be accessed from your machine. If it is stored in a file share/SMB, check for the access permissions.
* The vault credentials file is used only during the registration workflow.
* The vault credentials file expires after 48hrs and can be downloaded from the portal.
* Refer to the Azure Backup [FAQ](https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-faq) for any questions on the workflow.

# Registering your Windows Client machine

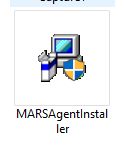
#### Download, install and register the Azure Backup agent

After creating the Azure Backup vault, an agent should be installed on each of your on-premises servers (Windows Server, Windows client or System Center Data Protection Manager server) which enables you to backup data and applications to Azure. This article covers the steps required to setup the Azure Backup agent on a Windows Server or Windows client machine.

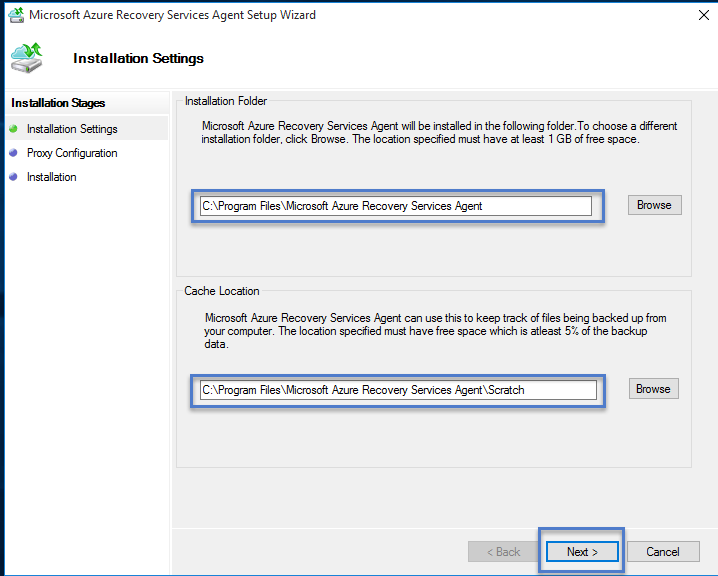
1. If necessary, sign in to the [Management Portal](https://manage.windowsazure.com/), click **Recovery Services**, then select the backup vault that you want to register with a server. The Quick Start page for that backup vault appears.



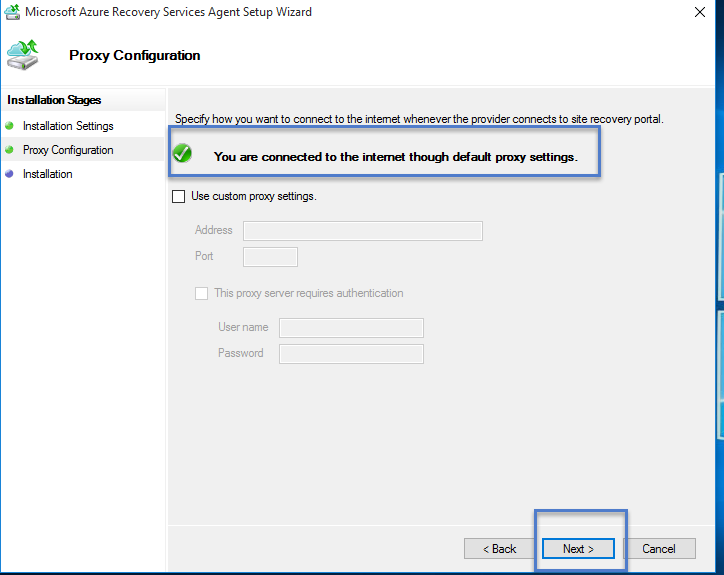
1. On the Quick Start page (below the “Download vault credentials”), click **For Windows Server or System Center Data Protection Manager or Windows client** under **Download Agent** option. Click **Save** to copy it to the local machine.



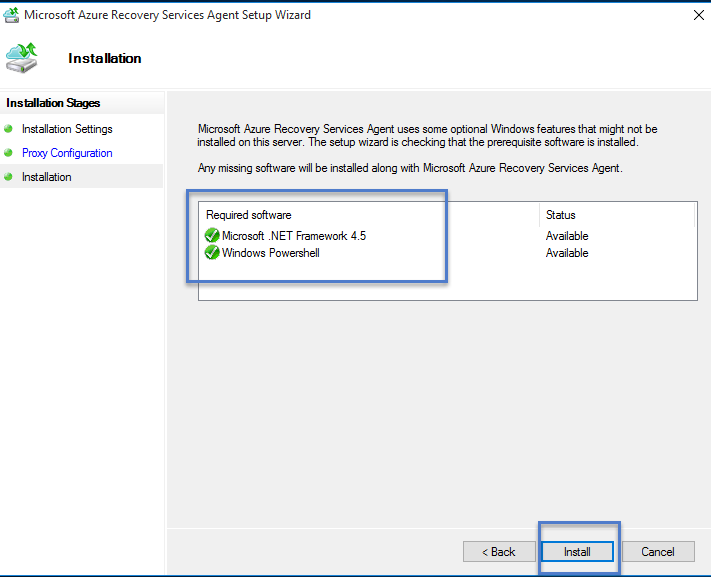
1. Once the agent is downloaded, double click **MARSAgentInstaller.exe** to launch the installation of the Azure Backup agent.
2. Choose the installation folder and folder required for the agent. The cache location specified must have free space which is at least 5% of the backup data.



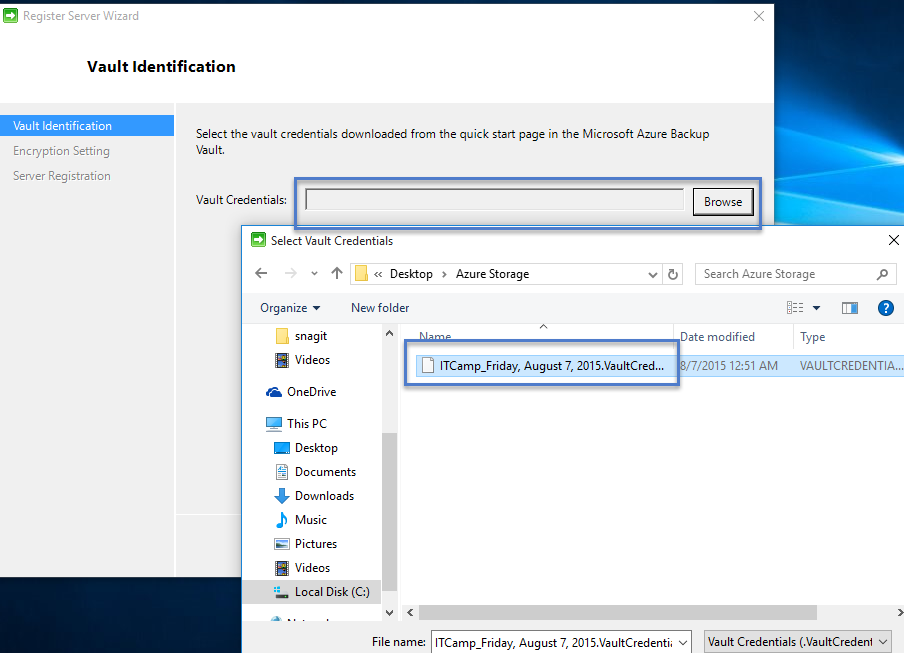
1. If you use a proxy server to connect to the internet, in the **Proxy configuration** screen, enter the proxy server details. If you use an authenticated proxy, enter the user name and password details in this screen.



1. The Azure Backup agent install .NET Framework 4.5 and Windows PowerShell (if it’s not available already) to complete the installation.

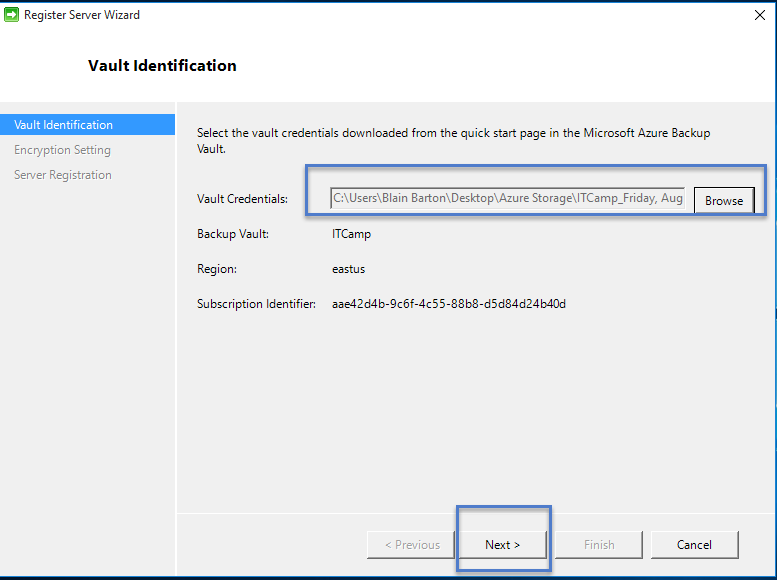


1. Once the agent is installed, click the **Proceed to Registration** button to continue with the workflow.
2. In the vault credentials screen, browse to and select the vault credentials file which was previously downloaded.



**NOTE:**

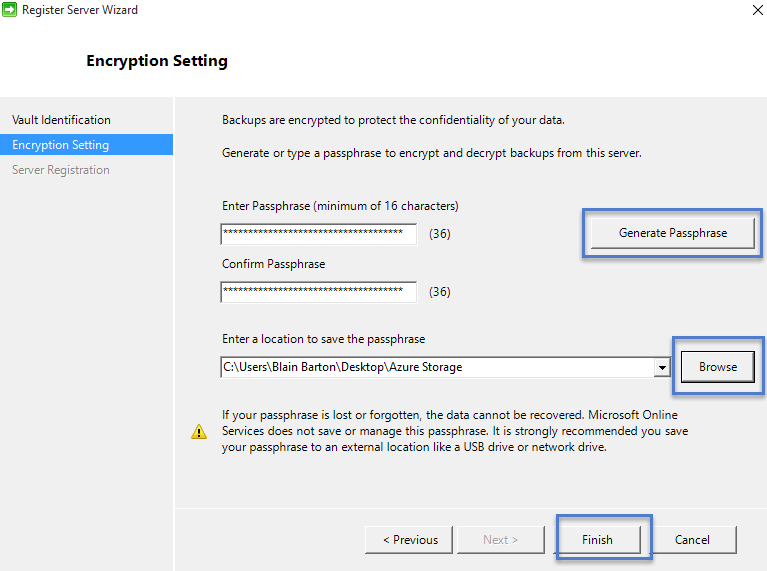
The vault credentials file is valid only for 48 hrs (after it’s downloaded from the portal). If you encounter any error in this screen (e.g “Vault credentials file provided has expired”), login to the Azure portal and download the vault credentials file again.



Ensure that the vault credentials file is available in a location which can be accessed by the setup application. If you encounter access related errors, copy the vault credentials file to a temporary location in this machine and retry the operation.

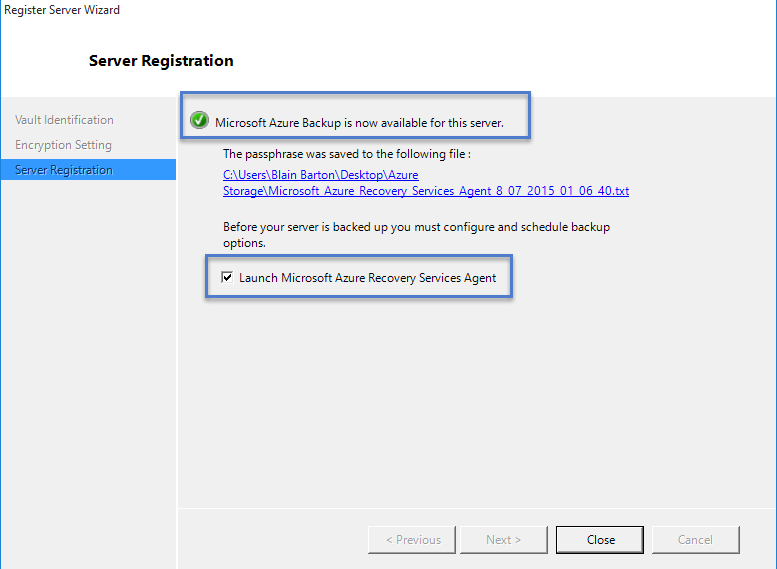
If you encounter an invalid vault credential error (e.g “Invalid vault credentials provided". The file is either corrupted or does not have the latest credentials associated with the recovery service”, retry the operation after downloading a new vault credential file from the portal. This error is typically seen if the user clicks on the Download vault credential option in the Azure portal, in quick succession. In this case, only the second vault credential file is valid.

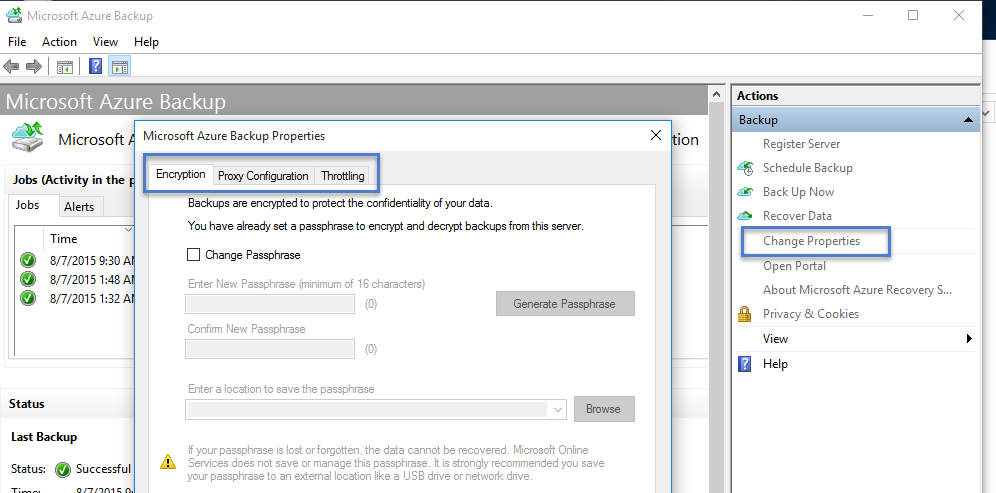
1. In the **Encryption setting** screen, you can either generate a passphrase or provide a passphrase (minimum of 16 characters) and remember to save the passphrase in a secure location.



WARNING:

If the passphrase is lost or forgotten; Microsoft cannot help in recovering the backup data. The end user owns the encryption passphrase and Microsoft does not have any visibility into the passphrase which is used by the end user. Please save the file in a secure location as it would be required during a recovery operation.

1. Once you click the **Finish** button, the machine is registered successfully to the vault and you are now ready to start backing up to Microsoft Azure. 
2. You can modify the settings specified during the registration workflow by clicking the **Change Properties** option in the Azure Backup mmc snap in.

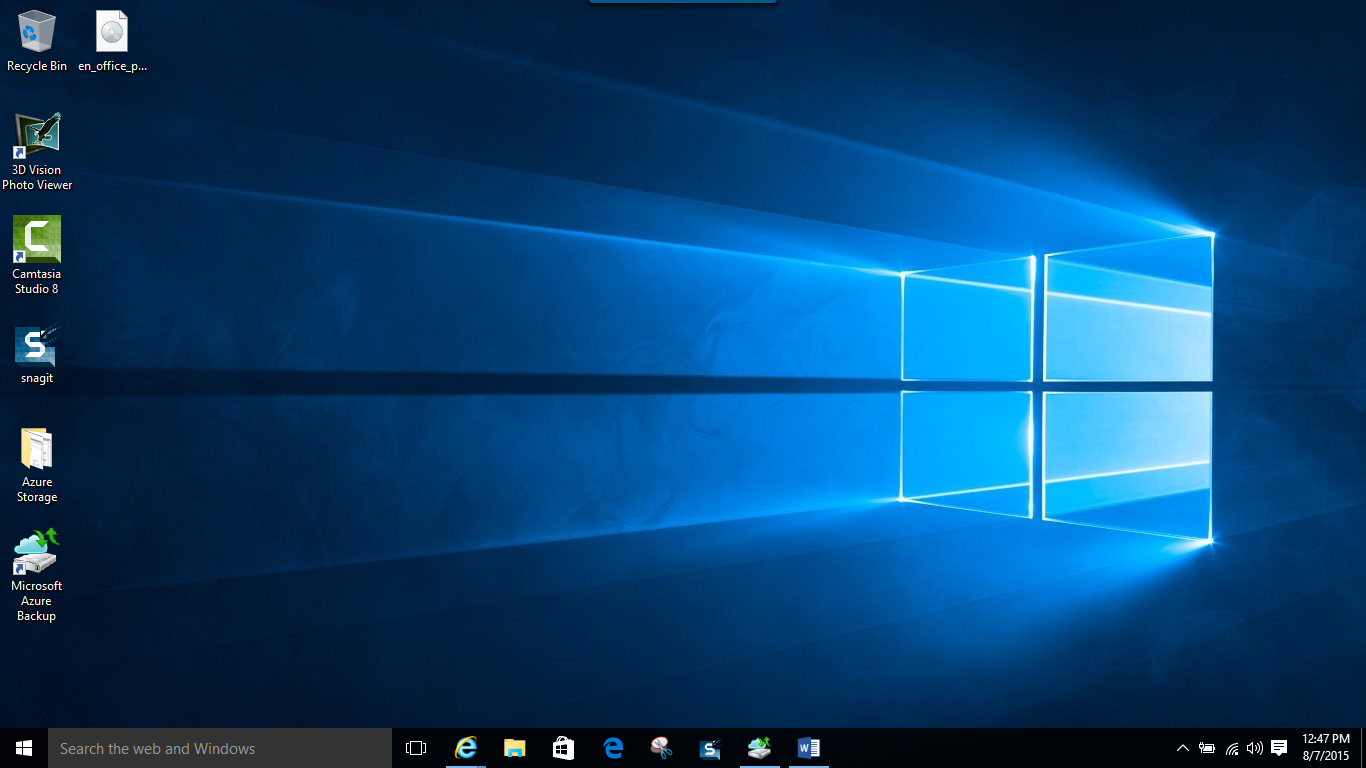


## Backup and restore from a Windows server or Windows client machine

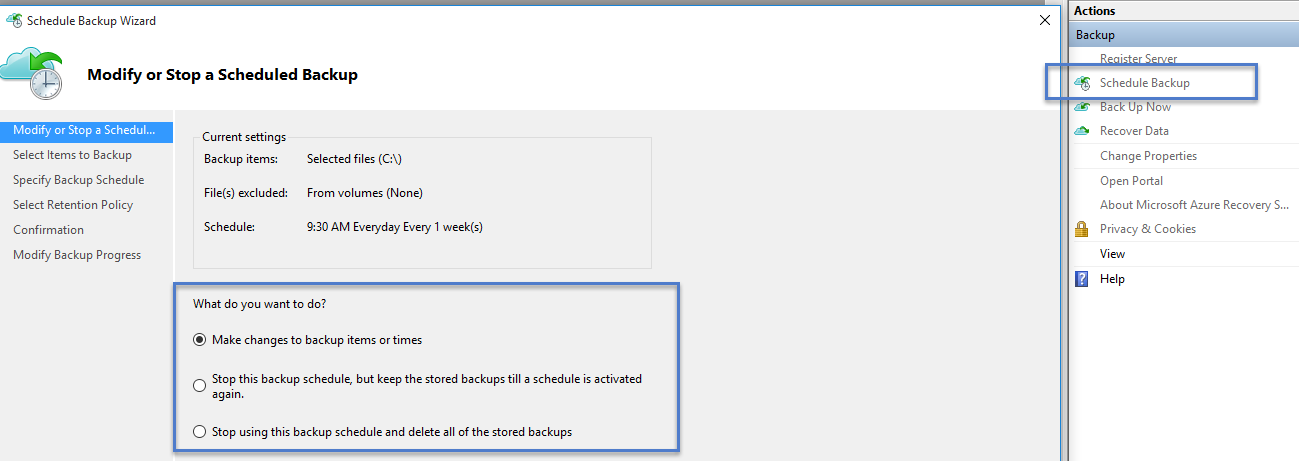
This lab covers the steps required to back up from a Windows server or a Windows client machine. It also covers the steps required to restore the backed up files on the same machine and the steps required to restore the backed up files on any other machine.

#### Scheduling and Backing Up files

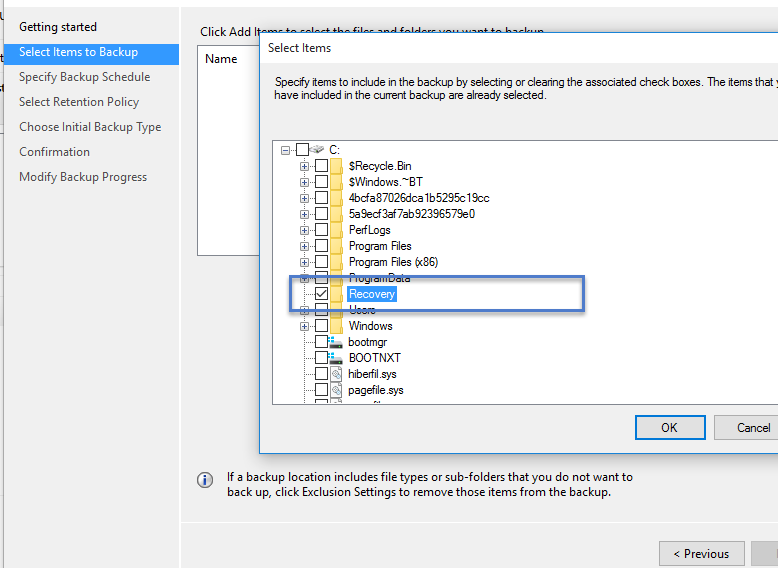
1. Once the machine is registered, open the **Microsoft Azure Backup** from the Desktop.



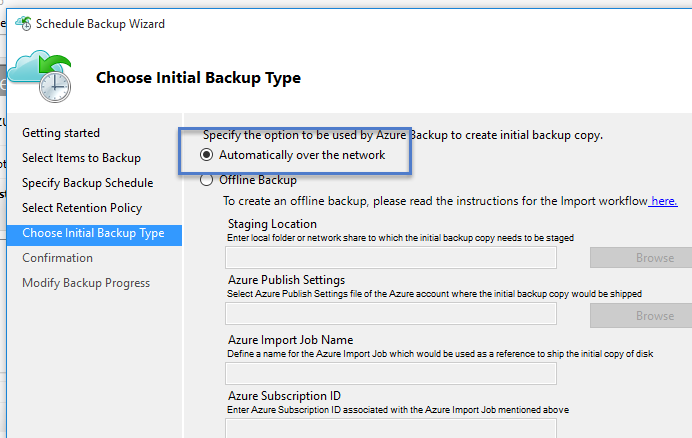
1. Click on **Schedule Backup** (This is for modifying a job and you might not see this for the first time.**)**

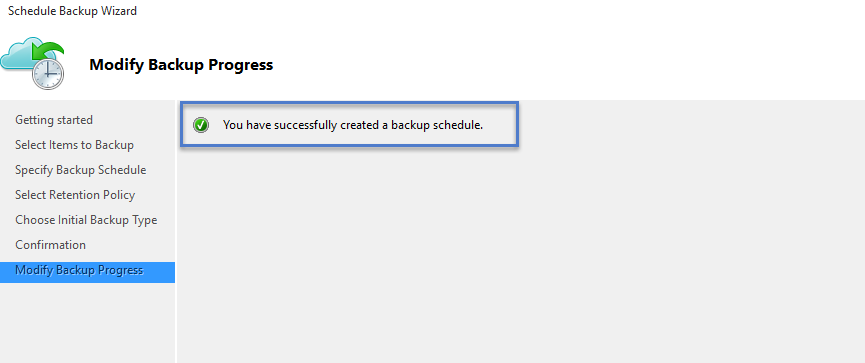


1. Select the items which you wish to back up. Azure Backup on a Windows Server/Windows Client (i.e without System Center Data Protection Manager) enables you to protect files and folders. **Create and pick a folder you want to backup.** In this case we took the c:\recovery folder.

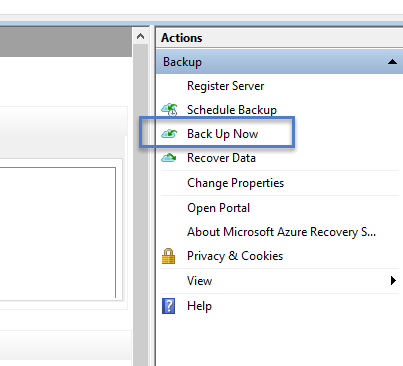


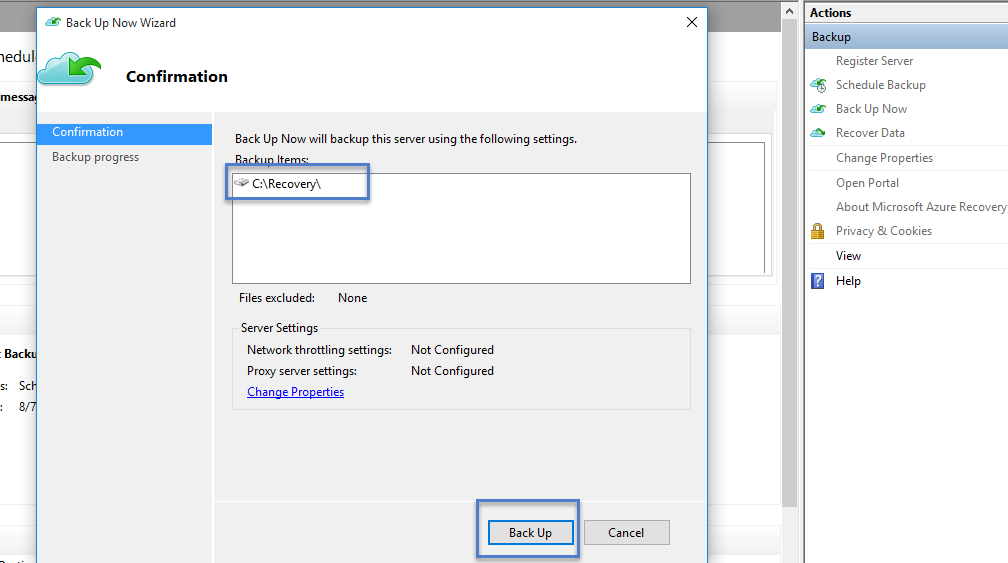
1. Specify the backup schedule and retention policy
2. Choose the method of sending the initial backup. Your choice of completing the initial seeding is dependent on the amount of data you wish to back up and your internet upload link speed. If you plan to back up GB’s/TB’s of data over a high latency, low bandwidth connection, it is recommended that you complete the initial backup by shipping a disk to the nearest Azure data center. If you have a sufficient bandwidth connection we recommend that you complete the initial backup over the network.

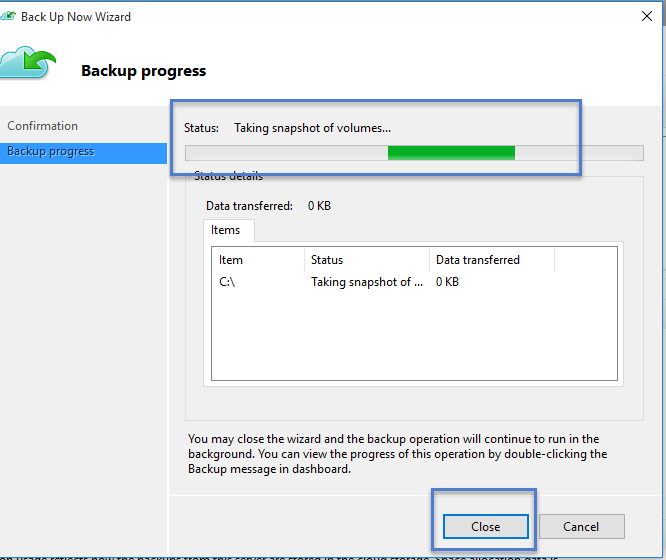


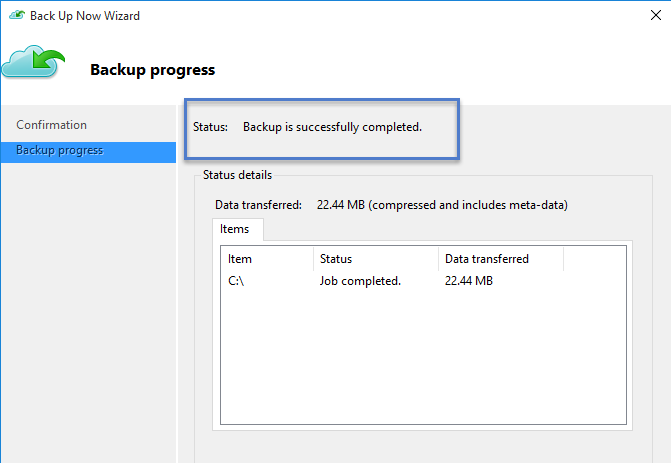


1. Once the process completes, go back to the mmc snap in and click **Back up Now** to complete the initial seeding over the network.







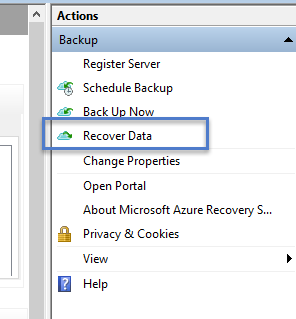


1. Once the initial seeding is completed, the **Jobs** view in the Azure Backup console indicates the status.

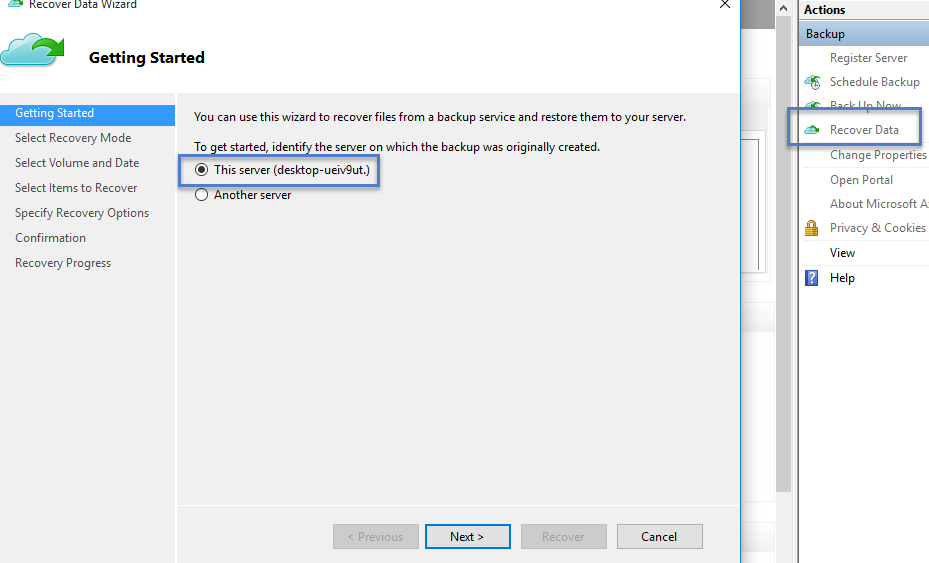
#### Recover data on the same machine

If you accidentally deleted a file and wish to restore the file/volume on the same machine (from which the backup is taken), the following steps will help you recover the data.

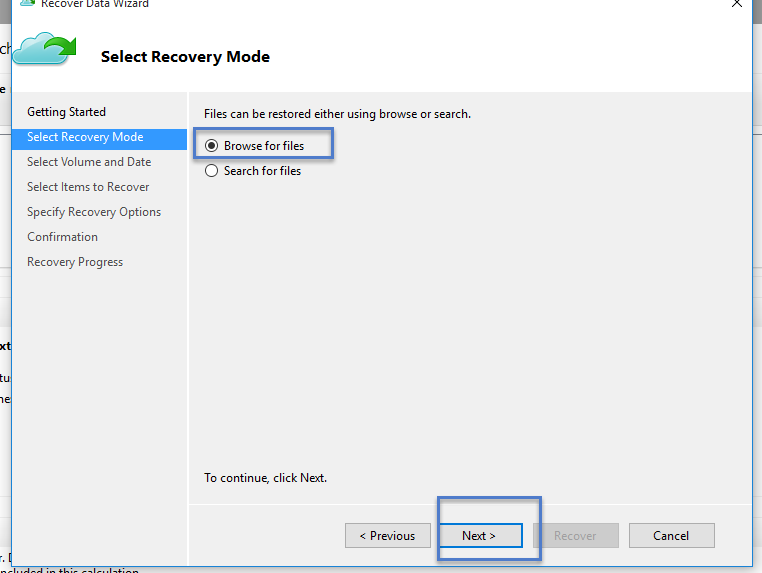
1. Click **Recover Data** to initiate the workflow.

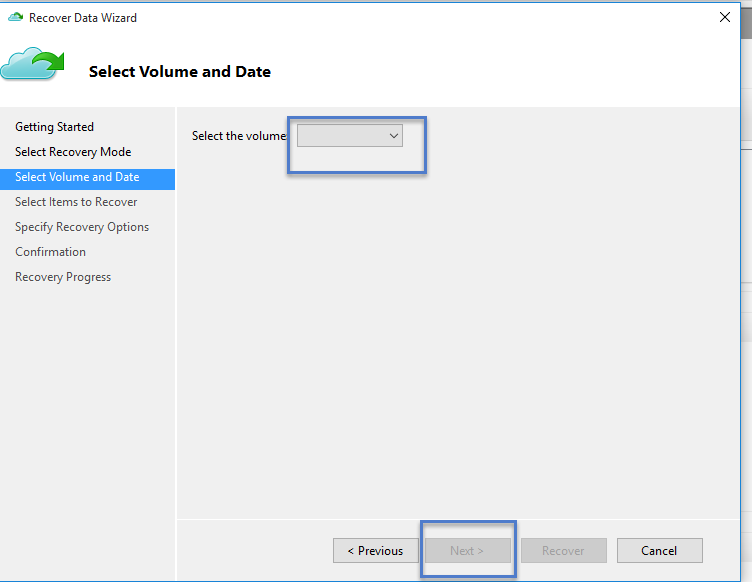


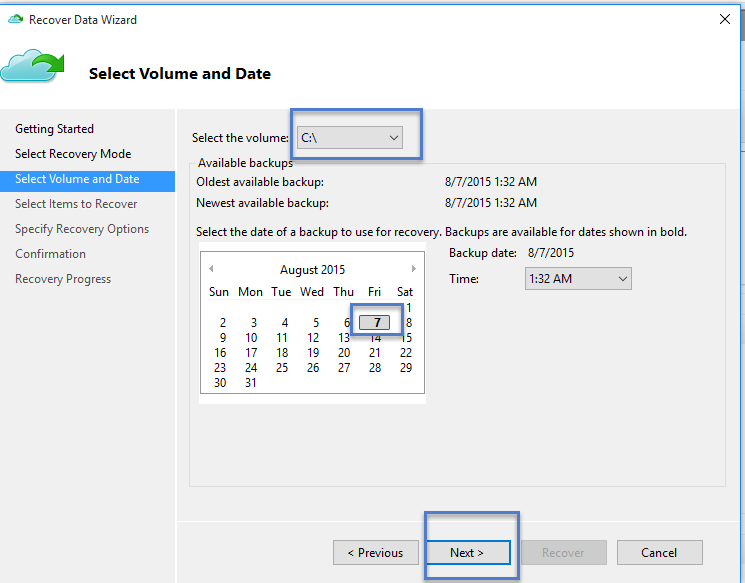
1. Select **This server (*yourmachinename*)** option as you plan to restore the backed up file on the same machine.



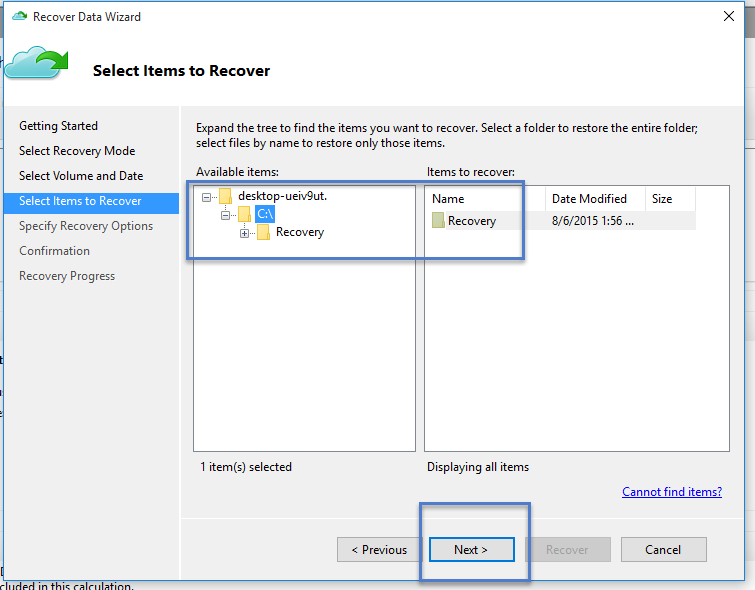
1. You can choose to **Browse for files** or **Search for files**. Leave the default option if you plan to restore one or more files whose path is known. If you are not sure about the folder structure but would like to search for a file, pick the **Search for files** option. For the purpose of this section, we will proceed with the default option.



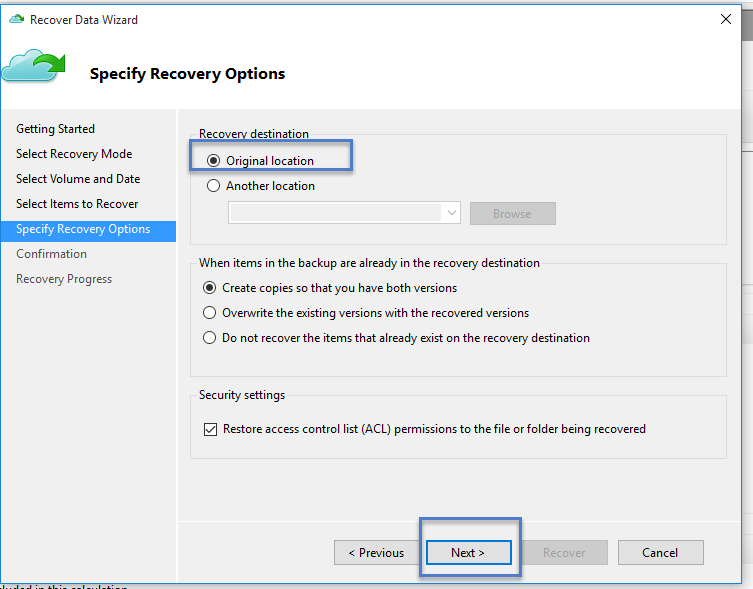
1. Select the volume from which you wish to restore the file. 
2. The screen enables you restore from any point in time. Dates which appear in **bold** in the calendar control indicate the availability of a restore point. Once a date is selected, based on your backup schedule (and the success of a backup operation), you can select a point in time from the **Time** drop down.



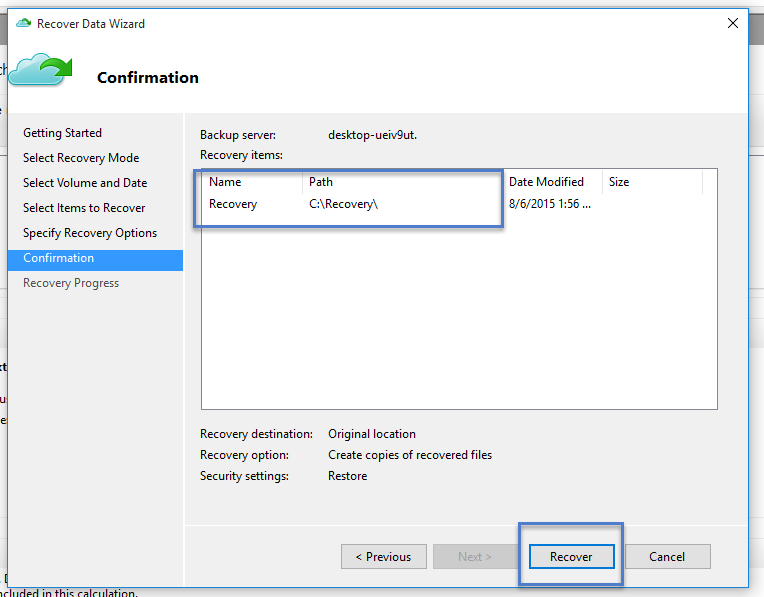
1. Select the items you wish to recover. You can multi-select folders/files which you wish to restore.



1. Specify the recovery parameters.

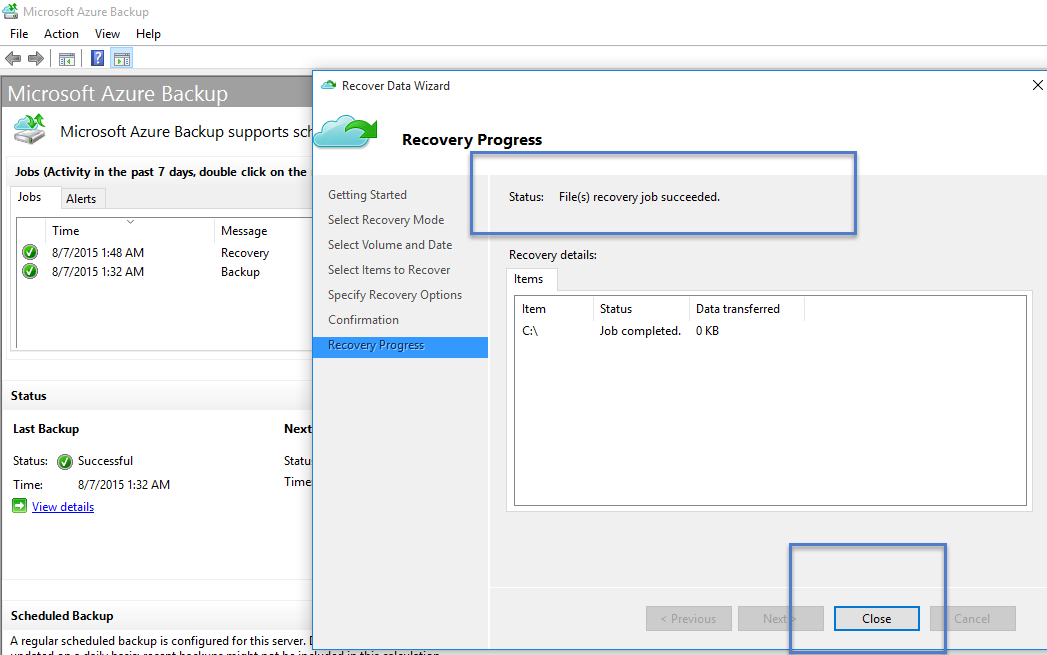


* + You have an option of restoring to the original location (in which the file/folder would be overwritten) or to another location in the same machine.
  + If the file/folder which you wish to restore, exists in the target location, you have the option to either create copies (two versions of the same file), or overwrite the files in the target location or skip the recovery of the files which exist in the target.

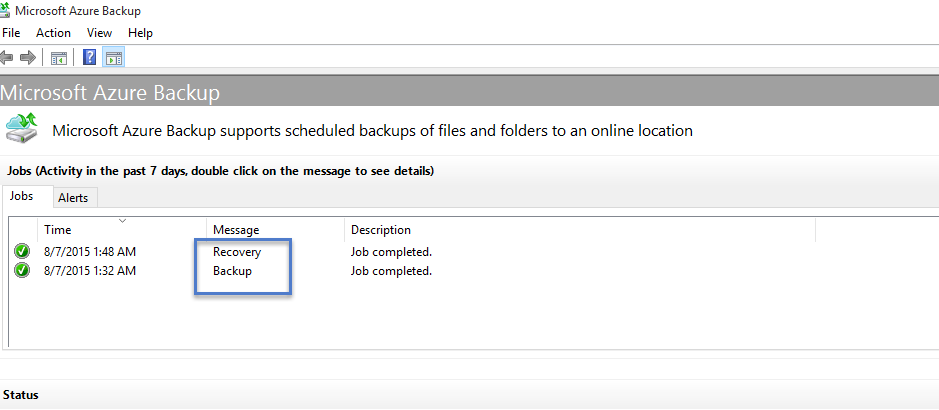


* + It is highly recommended that you leave the default option of restoring the ACLs on the files which are being recovered.

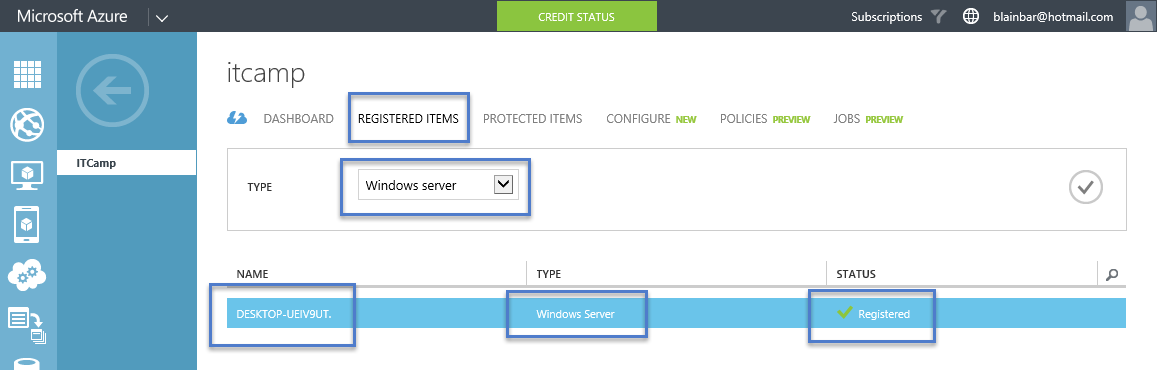
1. Once these inputs are provided, the recovery workflow starts which restores the files to this machine.



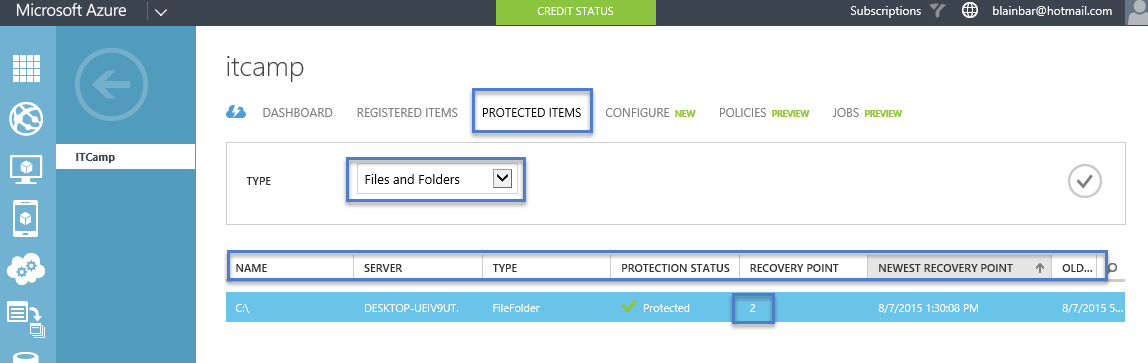
Here you can see the Backup and Recovery status.



If you go back into the Microsoft Azure Recovery Services Backup Vault you can see the **Registered Items**, even though it is a backup up of the client, it will say “Windows Server”.



You can also see the **Protected Items** but not the individual files themselves as the folders and files are stored in blog storage. You can only see the individual folders and files from the Azure Backup Agent on the physical machine.



This concludes “Backing up your files and folders with Microsoft Azure Recovery Services Backup Vault” for Windows Clients, Windows Servers and System Center Data Protection Manager.

For more information on Microsoft Azure Recovery Services Backup Vault go to: <http://azure.microsoft.com/en-us/services/backup> For FAQ’s on Microsoft Azure Backup go to: [https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-faq](https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-faq/)