WorkshopPLUS

Microsoft Azure Infrastructure as a Service (IaaS)

Introduction to Microsoft Azure Backup

Student Lab Manual

V1.1, November 2, 2015

Information in this document is subject to change without notice. The example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarked, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, MS, Windows, Windows NT, MSDN, Active Directory, BizTalk, SQL Server, SharePoint, Outlook, PowerPoint, FrontPage, Visual Basic, Visual C++, Visual J++, Visual InterDev, Visual SourceSafe, Visual C#, Visual J#,  and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names herein may be the trademarks of their respective owners.

Contents

[Introduction to Microsoft Azure Backup 4](#_Toc433351426)

[Exercise 1 - Azure Backup 4](#_Toc433351427)

[Prerequisites 4](#_Toc433351428)

[Task 1 - Creating a backup vault 5](#_Toc433351429)

[Task 2 - Restore data from Azure 10](#_Toc433351430)

[Task 3 - Protect Azure Virtual Machines 11](#_Toc433351431)

[Task 4 - Restore an Azure virtual machine 14](#_Toc433351432)

[Pick a recovery point 14](#_Toc433351433)

[Restore operation 17](#_Toc433351434)

[Restoring Domain Controller VMs 18](#_Toc433351435)

[Single DC 18](#_Toc433351436)

[Multiple DCs 18](#_Toc433351437)

# Introduction to Microsoft Azure Backup

In this lab, you will create a recovery vault to protect files, folders and an Azure virtual machine.

You'll learn:

* How to create an Azure Recovery Services vault
* How to protect local Windows files to Azure
* How to protect Azure virtual machines

# Exercise 1 - Azure Backup

## Prerequisites

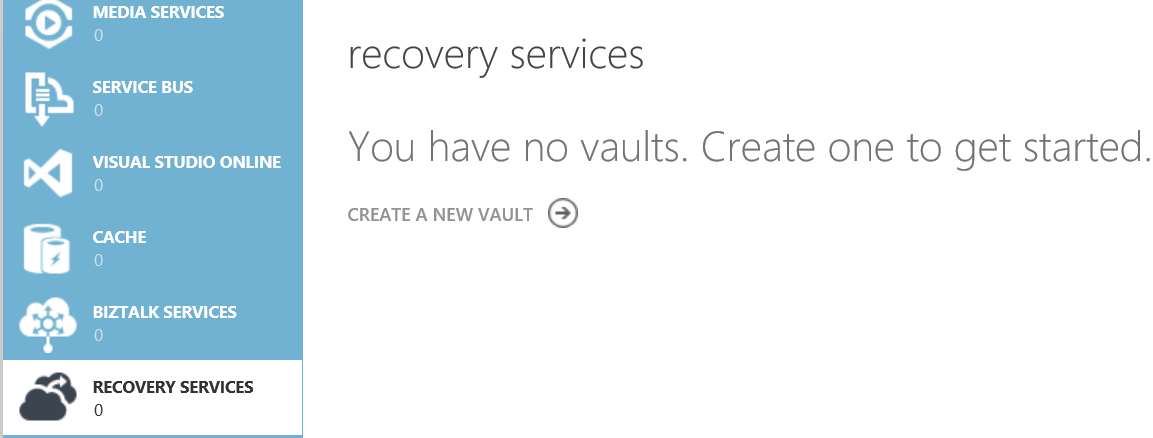
The following is required to complete this hands-on lab:

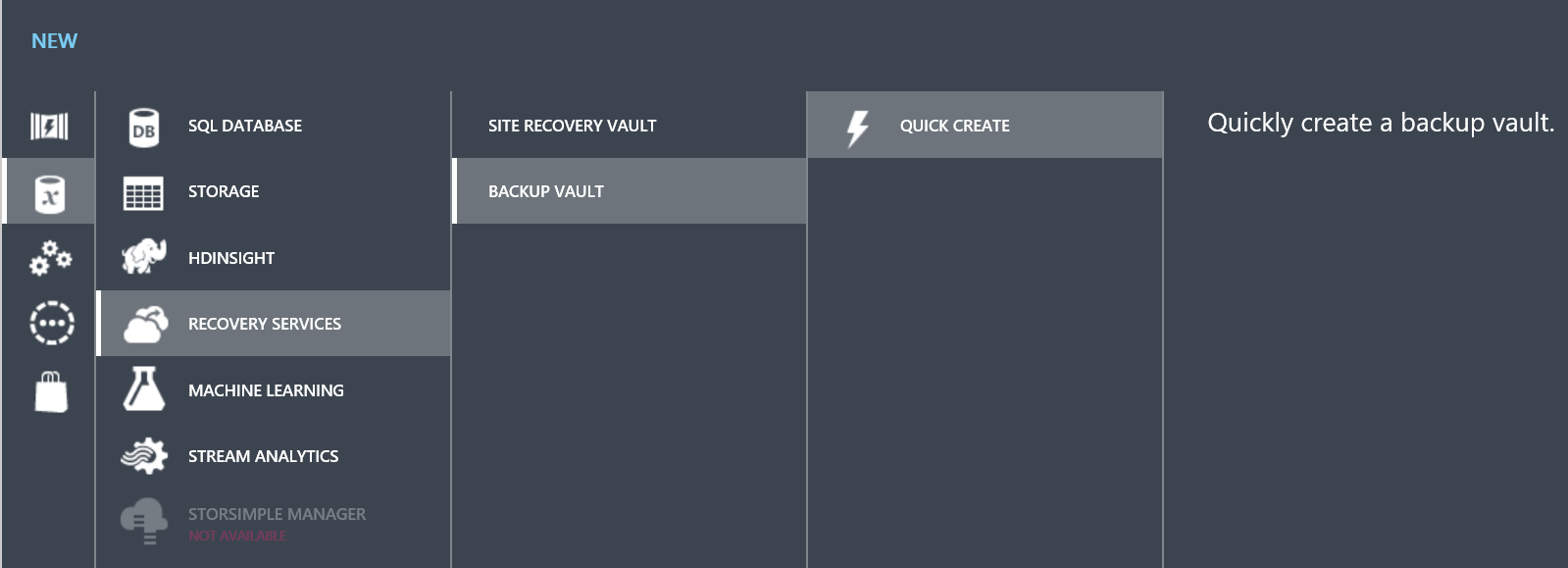
* [Web](http://www.microsoft.com/windowsazure/sdk/) browser
* Windows client or server machine
* A Microsoft Azure subscription

## Task 1 - Creating a backup vault

1. Navigate to <https://manage.windowsazure.com> and logon to your Azure subscription.
2. On the left side choose “**Recovery Services**”. On the right side, click “**Create new vault**”. Choose **Data Services | Recovery Services | Backup Vault | Quick Create**.

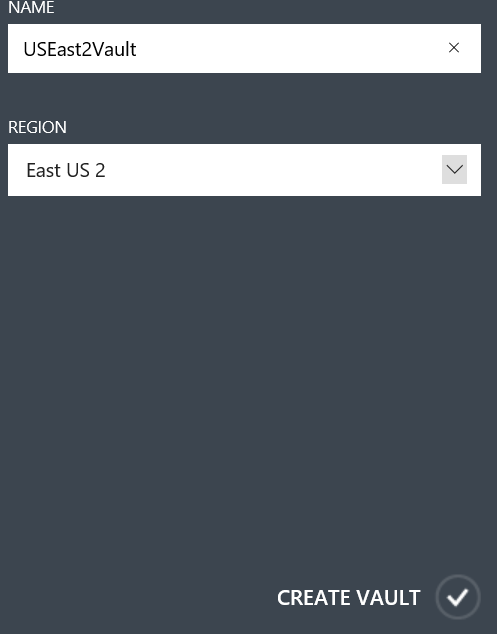
NOTE: *Site Recovery Vaults* are used to connect an on-premises System Center Virtual Machine Manager farm to Azure for seamless replication of on-premises virtual machines.



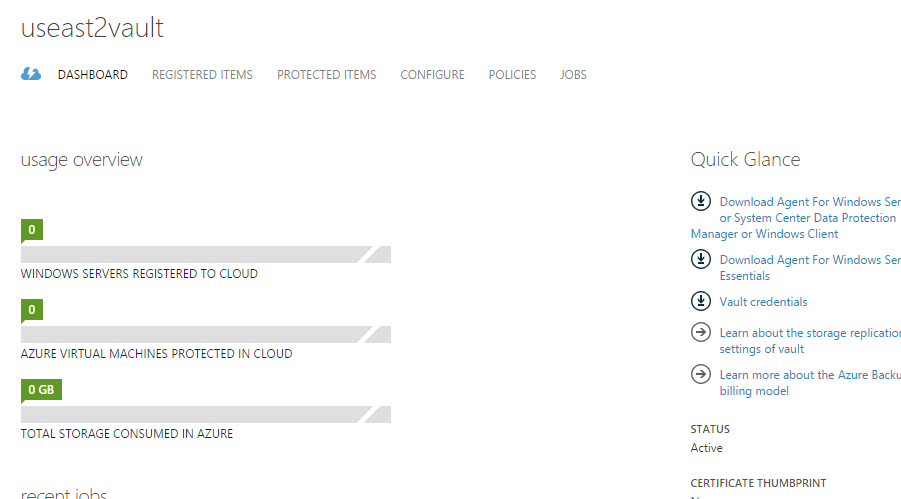


1. Enter a name and location for the vault click “**Create Vault**” to create the vault.

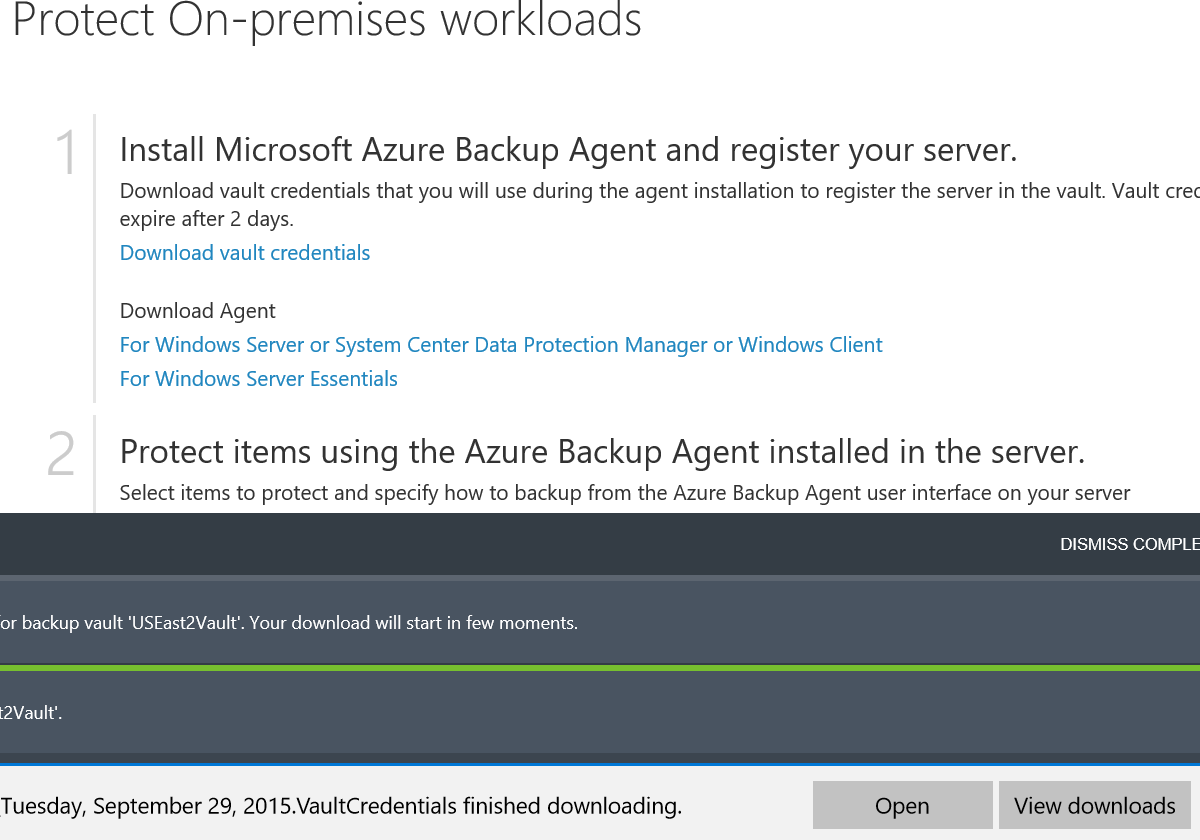
\* Note: When backing up Azure virtual machines the vault needs to be in the same location (date center) as the virtual machines.



1. After the vault is created click on the vault name in the portal. This will take you to the dashboard for the vault.



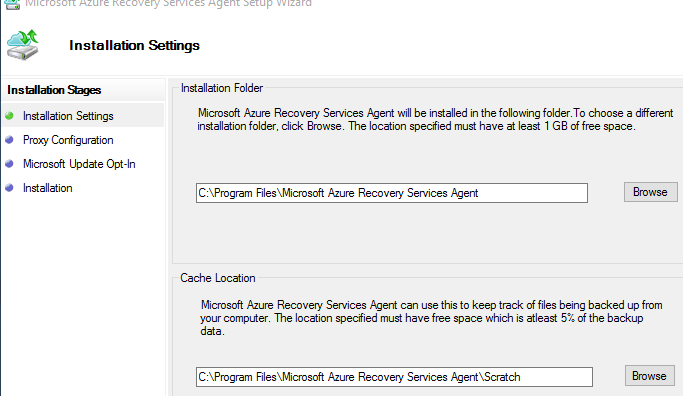
1. Download the vault credentials to your machine by clicking in the **Vault credentials** link. These credentials are needed when you install the backup client on the machine you want to protect.



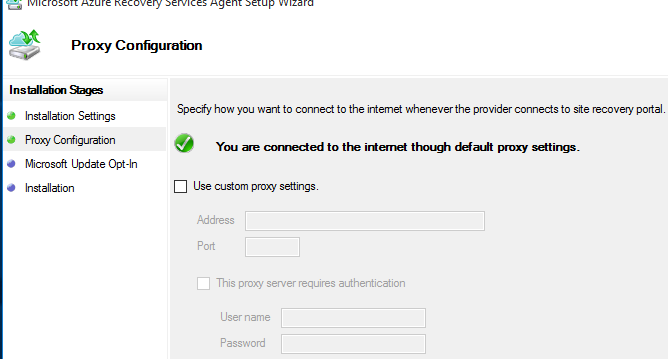
1. Download the “*For Windows Server or System Center Data Protection Manager or Windows Client*” client. There is also a separate client for Windows Server Essentials.
2. Copy the 2 files to the machine you want to backup.



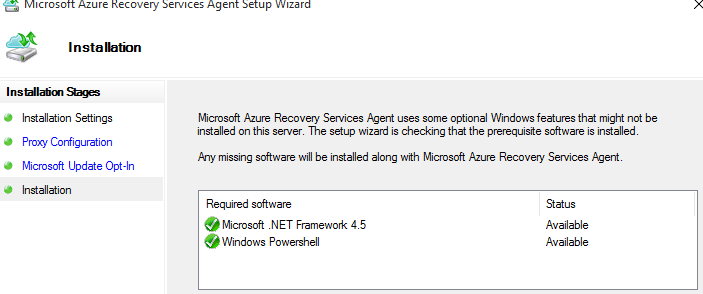
1. Install the **MARSAgentInstaller.exe** client on the machine you wish to backup. Accept UAC prompts for the software. Select an installation location and a cache location.



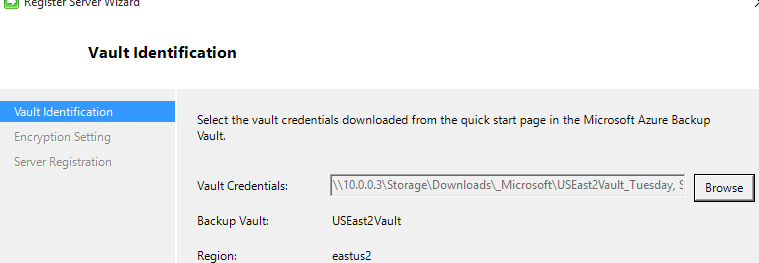
1. Enter any proxy settings needed for the software to connect to the Internet.



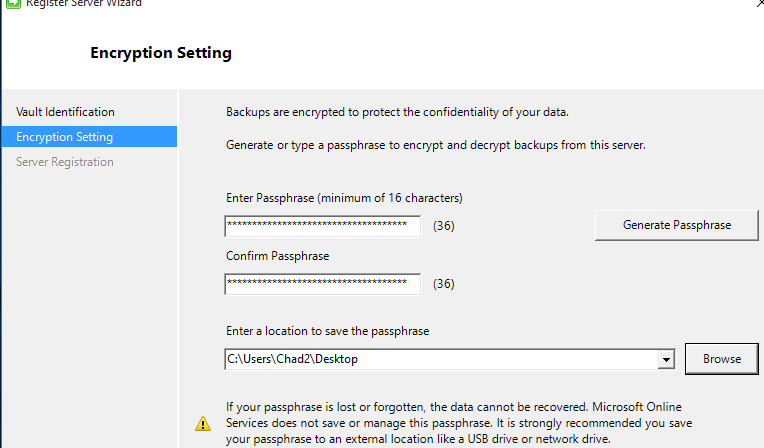
1. Choose Windows Update settings.
2. The software will install the prerequisites of *Windows PowerShell* and .*Net Framework 4.5* if they are not already installed.



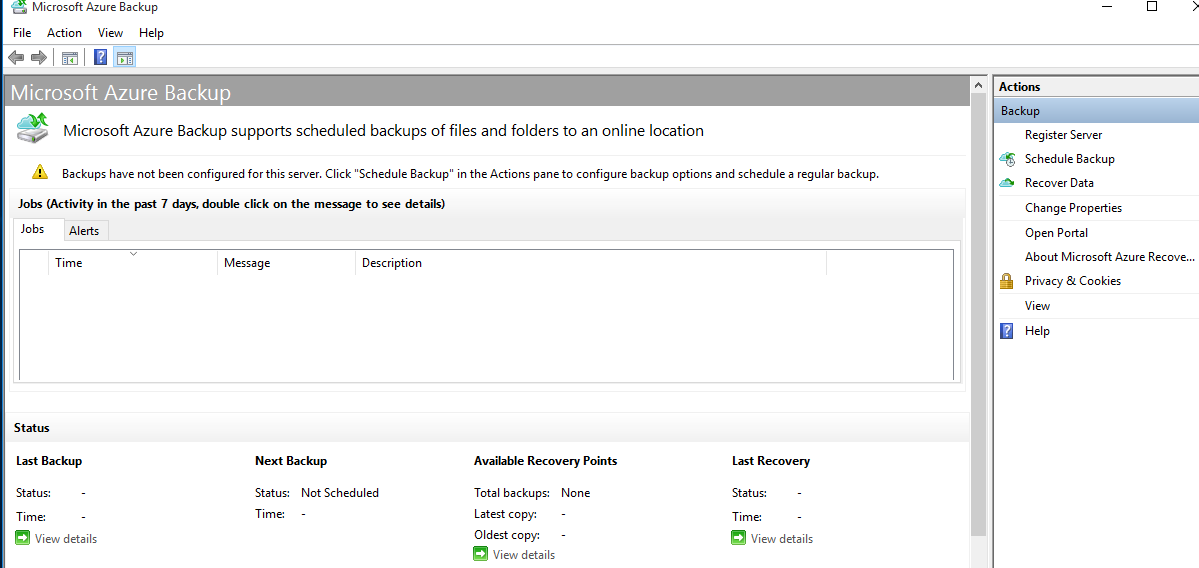
1. Click the “**Proceed to Registration**” button.
2. Click “**Browse**” and select the vault credentials file downloaded from the portal.



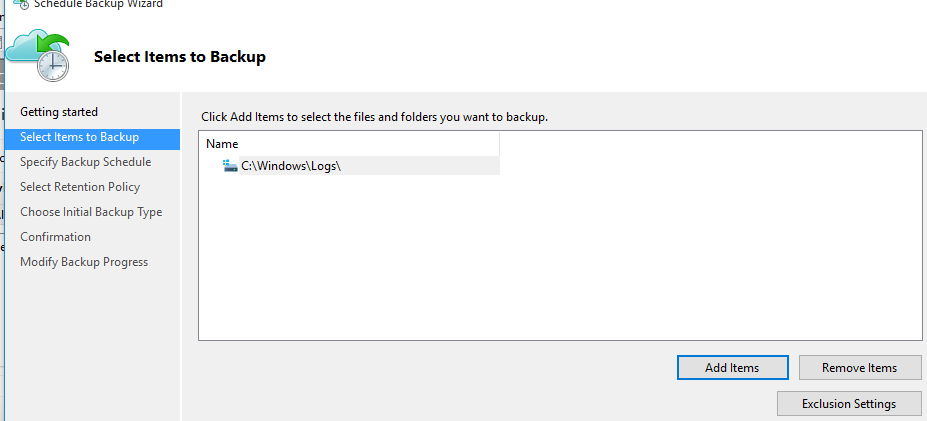
1. Click **Next**.
2. Either enter a passphrase or generate a passphrase. This is used to encrypt your data in Azure and needs to be very strong (at least 16 characters). Browse and enter a location to save the passphrase and keep that file in a save place (Bitlocker encrypted drive for instance).



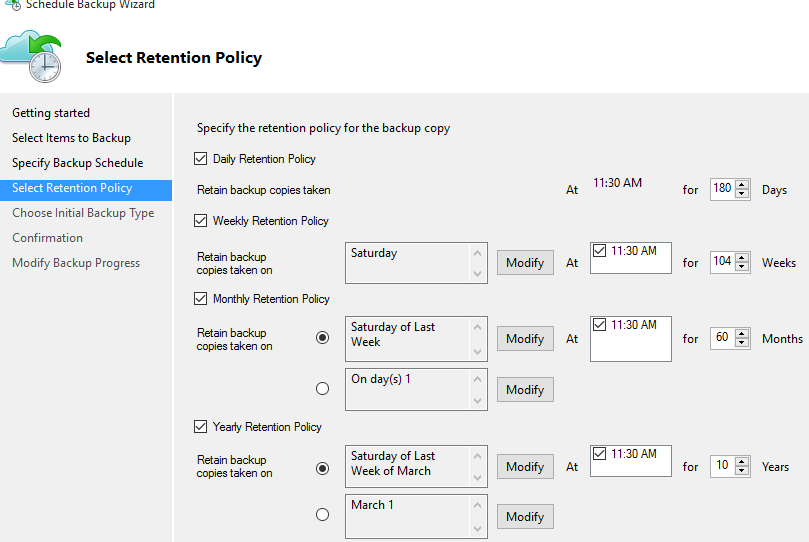
1. Launch the *Microsoft Azure Recovery Services Agent* console.
2. Click the “**Schedule Backup**” link on the right side.



1. Click **Next** on the getting started screen.
2. You can add items (files, folders) to backup. You can also set exclusion settings to exclude certain files or folders.
3. Click “**Add Items**” and add some files.



1. Click **Next**.
2. You can create a schedule for backing up the data. Either daily or weekly, up to 3 times per day. Set a daily schedule some in the future and click **Next**.
3. The data that is backed up can be retained. View the default retention policy. You can set daily, weekly, monthly and yearly policies for retaining data. Click **Next**.



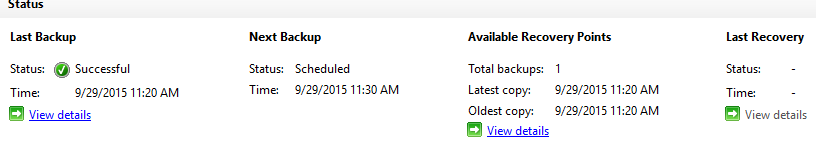
1. Choose the initial backup type.
2. Choose “*Automatically over the network*”, this will back up the files over the Internet to Azure. If you want to backup locally and send the data with a physical drive, you would select Offline backup and enter the settings. Click the “here” link for more information on how to create the offline backup and shipping instructions.
3. Click **Next**.
4. Click **Finish**.
5. If you do not want to wait for the backup to occur at the scheduled time, you can click the “*Back Up Now*” button on the right side.

## Task 2 - Restore data from Azure

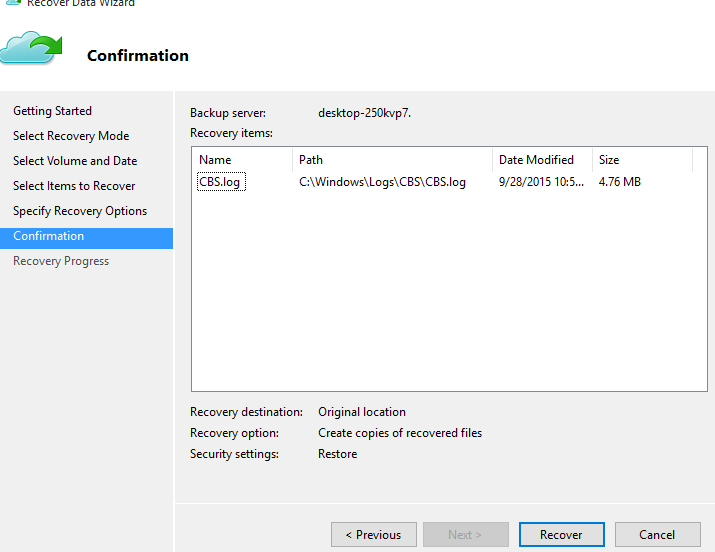
1. Start the **Microsoft Azure Backup** application if it is not already running.



1. You should have a previously successful backup listed in the status and at least 1 total backups listed.

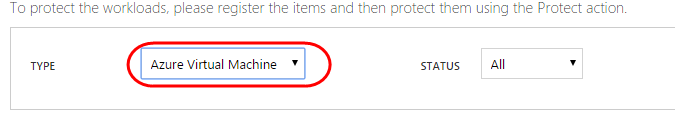


1. Click the “**Recover Data**” link on the right side.
2. If running on the restore on the same computer, select “This Server” on the *Getting Started* screen. Otherwise choose “Another Server” and select the vault credentials file.
3. Click **Next**.
4. Browse or search for the files you want to restore.
5. Select the file/s.
6. On the *Recovery Options* screen and select the location, overwrite and security options.
7. Click **Next**.
8. Click the “**Recover**” button.

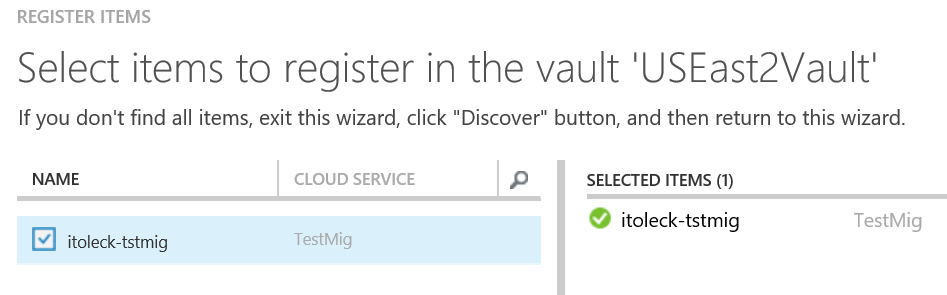


## Task 3 - Protect Azure Virtual Machines

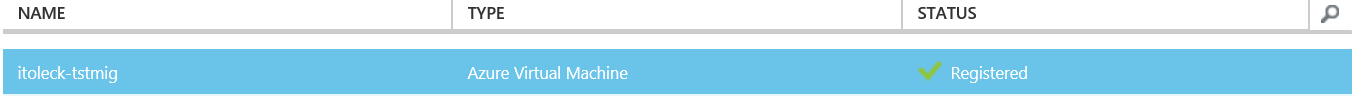
1. Navigate to the Azure management portal and select *Recovery Services*.
2. Select your backup vault. At the top of the page, select the **Registered Items** menu. Make sure that Azure Virtual Machine is selected as the ‘type’.



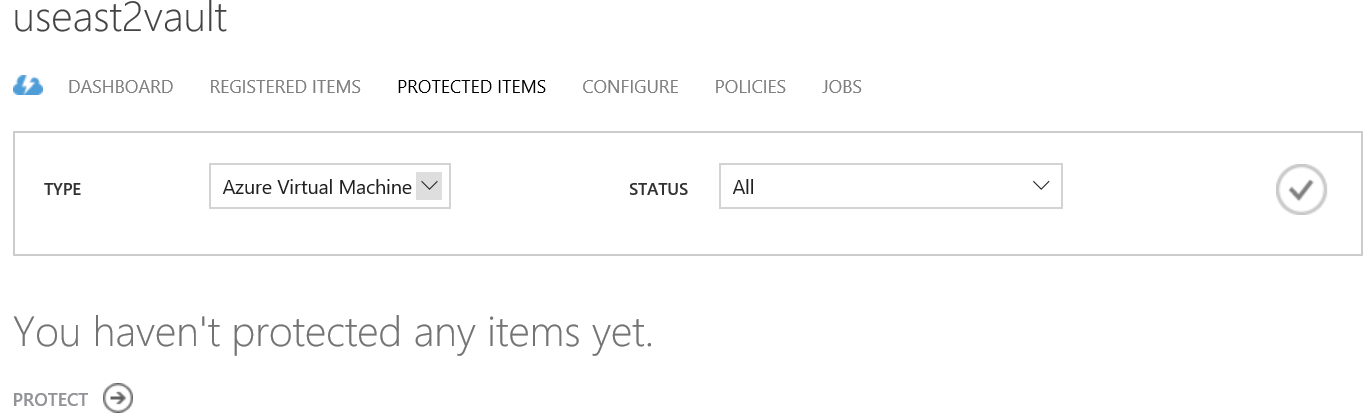
1. Select the **Discover** at the bottom of the page. This process will go out and discover Azure Virtual Machines that are currently protected by Azure Backup. It will not list those machines that are not protected.
2. Click the “**Register**” button to find and register a virtual machine running in the same Azure location. Select the machine/s you want to protect and click the checkmark.



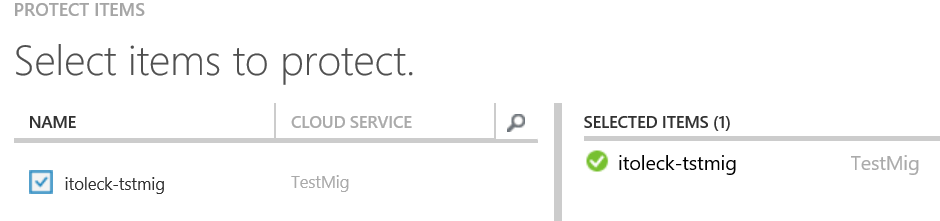
1. After the machine has been registered, it should show up with a green check beside it.



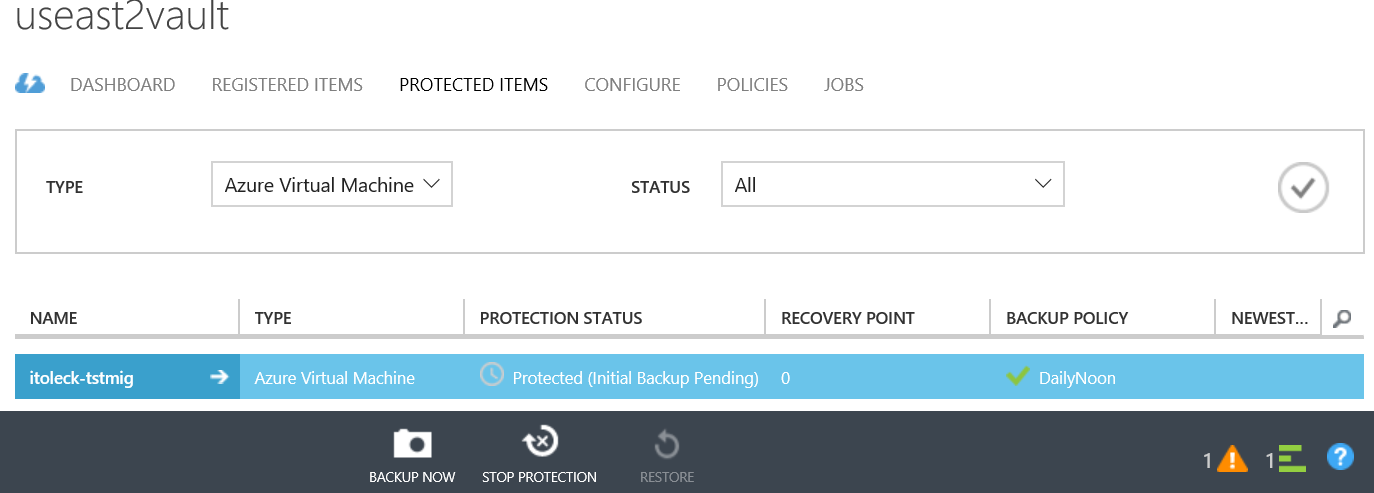
1. After the virtual machine is registered, navigate to the “Protected Items” menu (at the top of the screen).



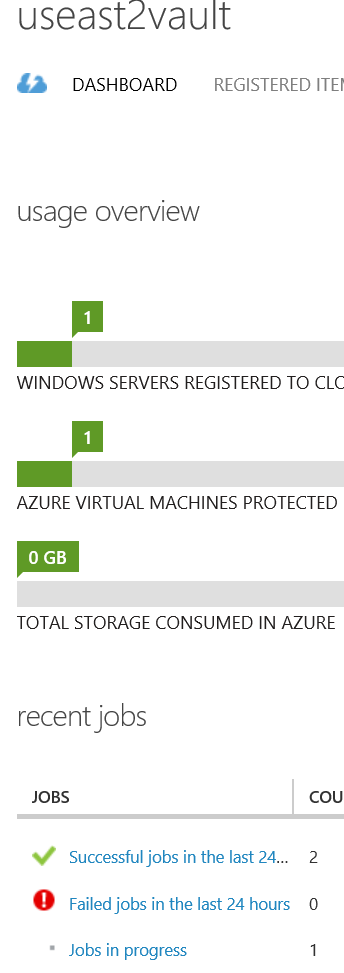
1. Click the “Protect” button and select the machine/s you want to protect.

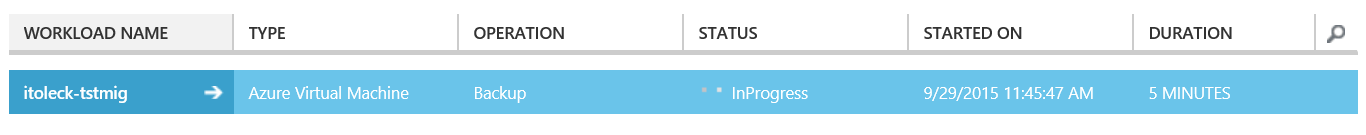


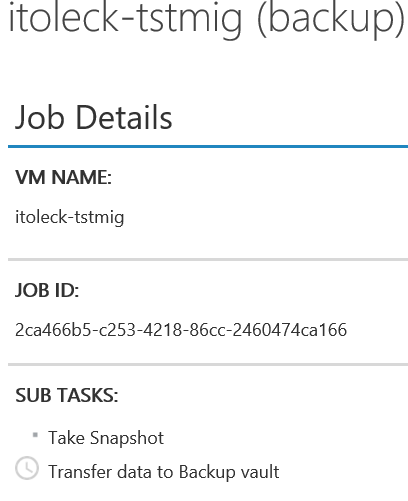
1. Click the **Next** arrow.
2. Set a policy for backing up the virtual machine. You can select the default policy or create a new policy. Select **Create New** and enter a policy name. Select daily and a time in the near future.
3. Click the **Next** arrow.
4. Select the retention policy settings for the backups.
5. Click the complete checkmark.
6. You can also back up the virtual machine manually by clicking the “Backup Now” button.



1. Either wait for the scheduled backup or click the “Backup Now” button.
2. You can view the backup details and policy for a virtual machine by clicking on the name of the virtual machine in the protected items tab.
3. You can also view the backup progress by navigating to the dashboard and selecting the jobs in progress link.

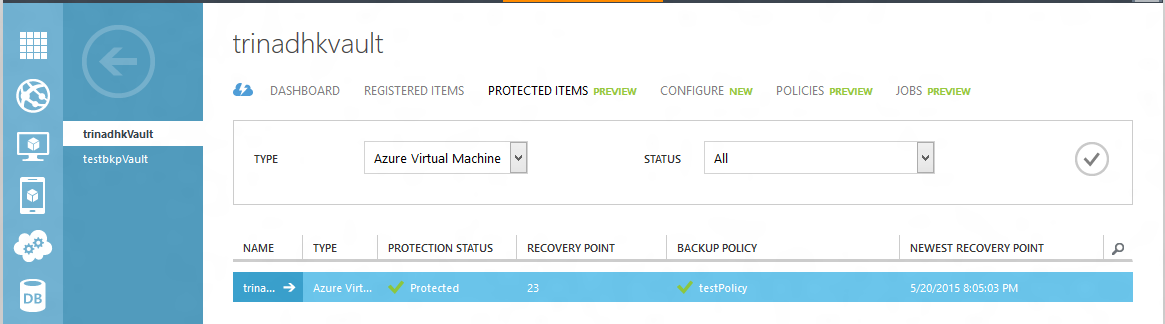






## Task 4 - Restore an Azure virtual machine

1. Choose an item to restore
2. Navigate to the *Protected Items* tab and select the virtual machine you want to restore to a new VM.



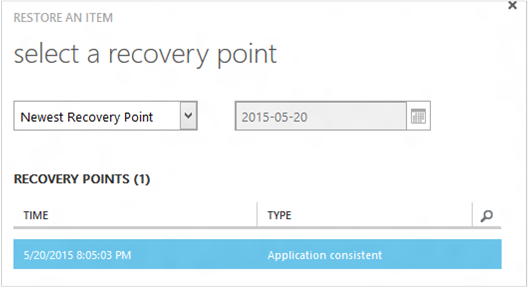
1. The Recovery Point column in the Protected Items page will tell you the number of recovery points for a virtual machine. The Newest Recovery Point column tells you the time of the most recent backup from which a virtual machine can be restored.
2. Click Restore to open the Restore an Item wizard.

Restore an item

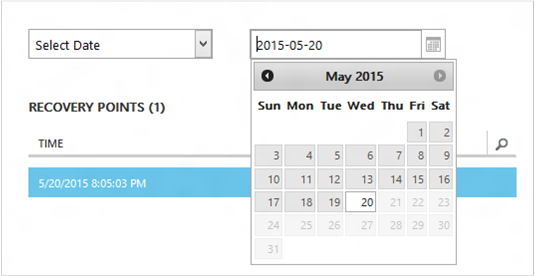
### 

### Pick a recovery point

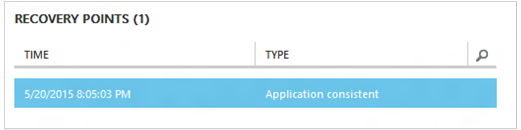
1. On the *select a recovery point* screen, you can restore from the newest recovery point, or from a previous point in time. The default option selected when wizard opens is *Newest Recovery Point*.



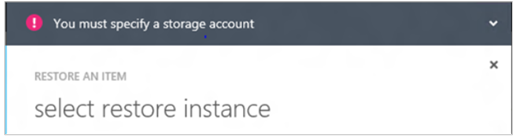
1. To pick an earlier point in time, choose the **Select Date** option in the dropdown and select a date in the calendar control by clicking on the calendar icon. In the control, all dates that have recovery points are filled with a light gray shade and are selectable by the user.



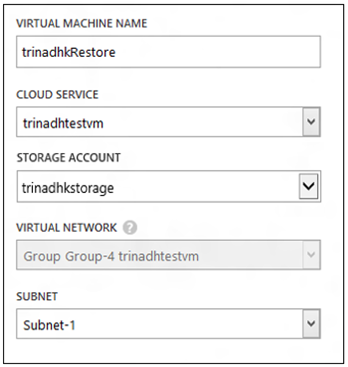
1. Once you click a date in the calendar control, the recovery points available on that date will be shown in recovery points table below. The Time column indicates the time at which the snapshot was taken. The Type column displays the [consistency](https://azure.microsoft.com/documentation/articles/backup-azure-vms/#consistency-of-recovery-points) of the recovery point. The table header shows the number of recovery points available on that day in parenthesis.



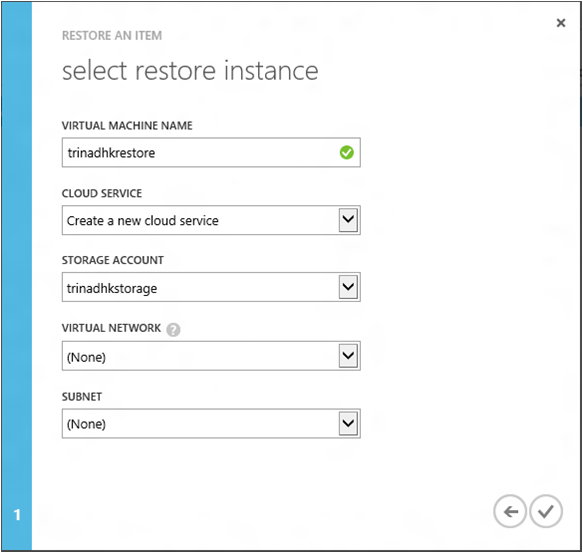
1. Select the recovery point from the Recovery Points table and click the Next arrow to go to the next screen.
2. Specify a destination location
3. On the *Select restore instance* screen specify details of where to restore the virtual machine.
4. Specify the virtual machine name: In a given cloud service, the virtual machine name should be unique. If you plan to replace an existing VM with the same name, first delete the existing VM and data disks and then restore the data from Azure Backup.
5. Select a cloud service for the VM: This is mandatory for creating a VM. You can choose to either use an existing cloud service or create a new cloud service.
6. Whatever cloud service name is picked should be globally unique. Typically, the cloud service name gets associated with a public-facing URL in the form of [cloudservice].cloudapp.net. Azure will not allow you to create a new cloud service if the name has already been used. If you choose to create select create a new cloud service, it will be given the same name as the virtual machine – in which case the VM name picked should be unique enough to be applied to the associated cloud service.
7. We only display cloud services and virtual networks that are not associated with any affinity groups in the restore instance details. [Learn More](https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-migrate-to-regional-vnet/).
8. Select a storage account for the VM: This is mandatory for creating the VM. You can select from existing storage accounts in the same region as the Azure Backup vault. Zone redundant or Premium storage accounts are not supported at this time.
9. If there are no storage accounts with supported configuration, please create a storage account of supported configuration prior to starting restore operation.



1. Select a Virtual Network: The virtual network (VNET) for the virtual machine should be selected at the time of creating the VM. The restore UI shows all the VNETs within this subscription that can be used. It is not mandatory to select a VNET for the restored VM – you will be able to connect to the restored virtual machine over the internet even if the VNET is not applied.
2. If the cloud service selected is associated with a virtual network, then you cannot change the virtual network.



1. Select a subnet: In case the VNET has subnets, by default the first subnet will be selected. Choose the subnet of your choice from the dropdown options. For subnet details, go to Networks extension in the [portal home page](https://manage.windowsazure.com/), go to Virtual Networks and select the virtual network and drill down into Configure to see subnet details.



1. Click the Submit icon in the wizard to submit the details and create a restore job.

### Restore operation

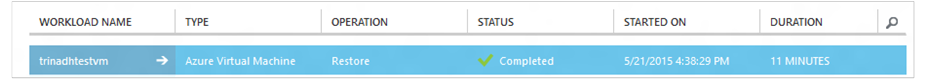
1. Once you have input all the information into the restore wizard and submitted it Azure Backup will try to create a job to track the restore operation.



1. If the job creation is successful, you will see a toast notification indicating that the job is created. You can get more details by clicking the View Job button that will take you to Jobs tab.

Restore job created

1. Once the restore operation is finished, it will be marked as completed in Jobs tab.



1. After restoring the virtual machine you may need to re-install the extensions existing on the original VM and [modify the endpoints](https://azure.microsoft.com/en-us/documentation/articles/backup-azure-restore-vms/virtual-machines-set-up-endpoints) for the virtual machine in the Azure portal.

## Restoring Domain Controller VMs

Backup of Domain Controller (DC) virtual machines is a supported scenario with Azure Backup. However, some care must be taken during the restore process. The restore experience is vastly different for Domain Controller VMs in a single-DC configuration vs. VMs in a multi-DC configuration.

### Single DC

* The VM can be restored (like any other VM) from the Azure portal or using PowerShell.

### Multiple DCs

* When you have a multi-DC environment, the Domain Controllers have their own way of keeping data in sync. When an older backup point is restored *without the proper precautions*, The USN rollback process can wreak havoc in a multi-DC environment. The right way to recover such a VM is to boot it in DSRM mode.
* The challenge arises because DSRM mode is not present in Azure. So to restore such a VM, you cannot use the Azure portal. The only supported restore mechanism is disk-based restore using PowerShell.

WARNING:

* For Domain Controller VMs in a multi-DC environment, do not use the Azure portal for restore! Only PowerShell based restore is supported
* Read more about the [USN rollback problem](https://technet.microsoft.com/library/dd363553) and the strategies suggested to fix it.