Azure Services offered by Dell

Azure Backup Agent Set Up Guide

Azure Services by Dell

Azure Backup Agent Set Up Guide

Introduction

Azure Backup is a scalable solution for protecting your data in the Azure cloud and optionally can be integrated with Microsoft System Center Data Protection Manager for advanced workload protection running in your datacenter in VMs or on physical servers.

- Data protection schedules can be daily, monthly, weekly, and yearly with retention up to 99 years in Azure
- Protects workloads running in Azure, in VMs, or on physical servers
- Centralized monitoring and reporting across on premises and Azure

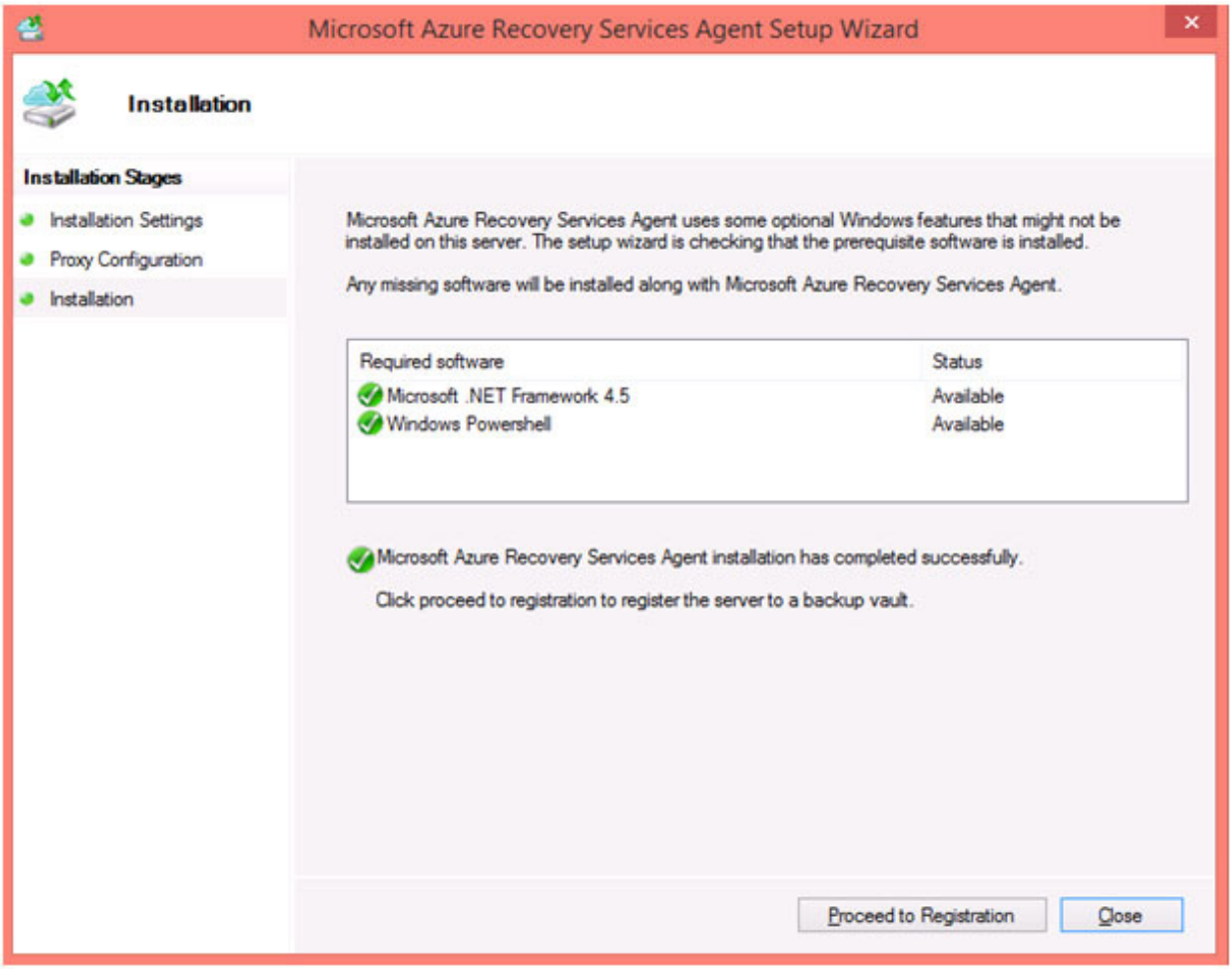
This set up guide provides step by step instructions and information necessary to download, install and register the Azure Backup agent and to configure the Azure Back up Service. This guide is intended to be followed in the order in which it is organized.

Intended Audience

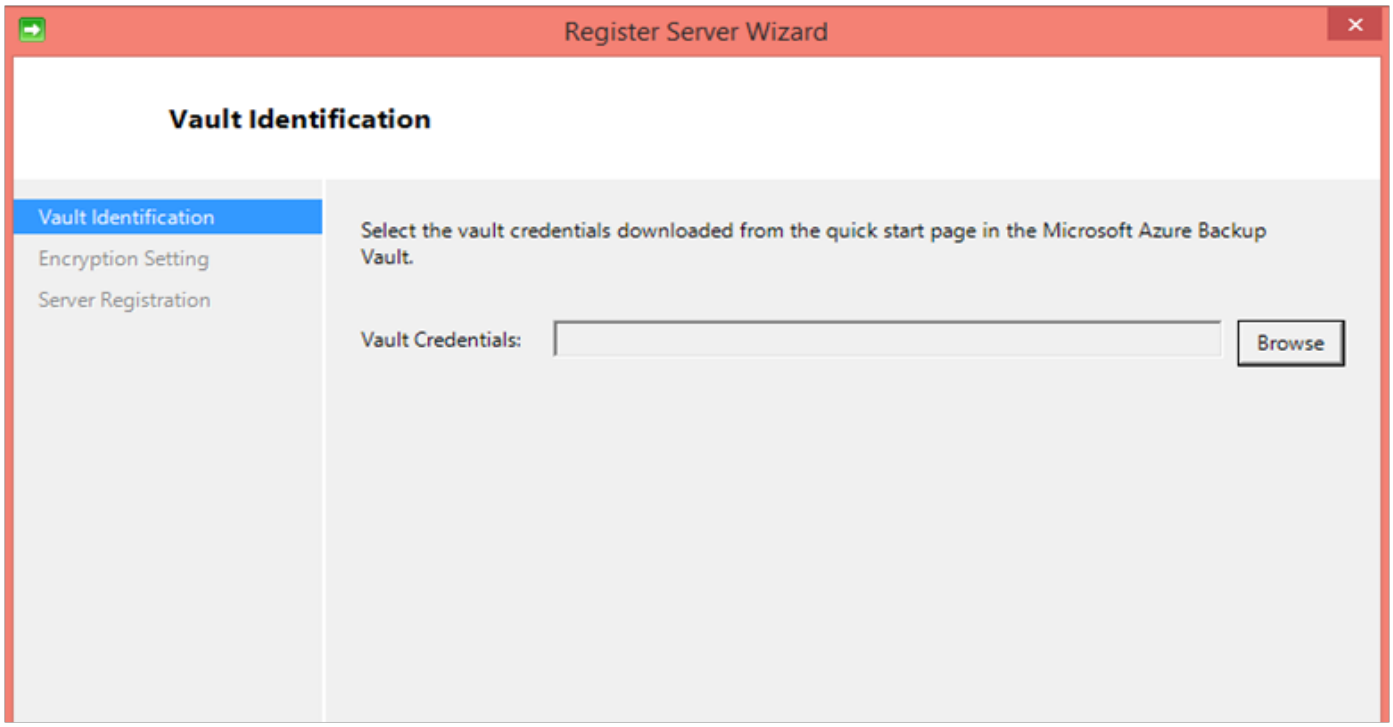
This guide is intended to assist and support Dell customers with installing and configuring Azure Backup Services. This guide assumes the reader is familiar with terminology and procedures typically used for backing up data.

Download, install, and register the Azure Backup agent

1. Download the Azure Backup agent here: http://aka.ms/azurebackup_agent
2. Once the agent is downloaded, double click MARSAgentInstaller.exe to launch the installation of the Azure Backup agent. Choose the installation folder and scratch folder required for the agent. **Note:** The cache location specified must have free space which is at least 5% of the backup data.
3. 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.
4. The Azure Backup agent installs .NET Framework 4.5 and Windows PowerShell (if it's not available already) to complete the installation.
5. Once the agent is installed, click the **Proceed to Registration** button to continue with the workflow.



6. In the vault credentials screen, browse to and select the vault credentials file which was previously downloaded.

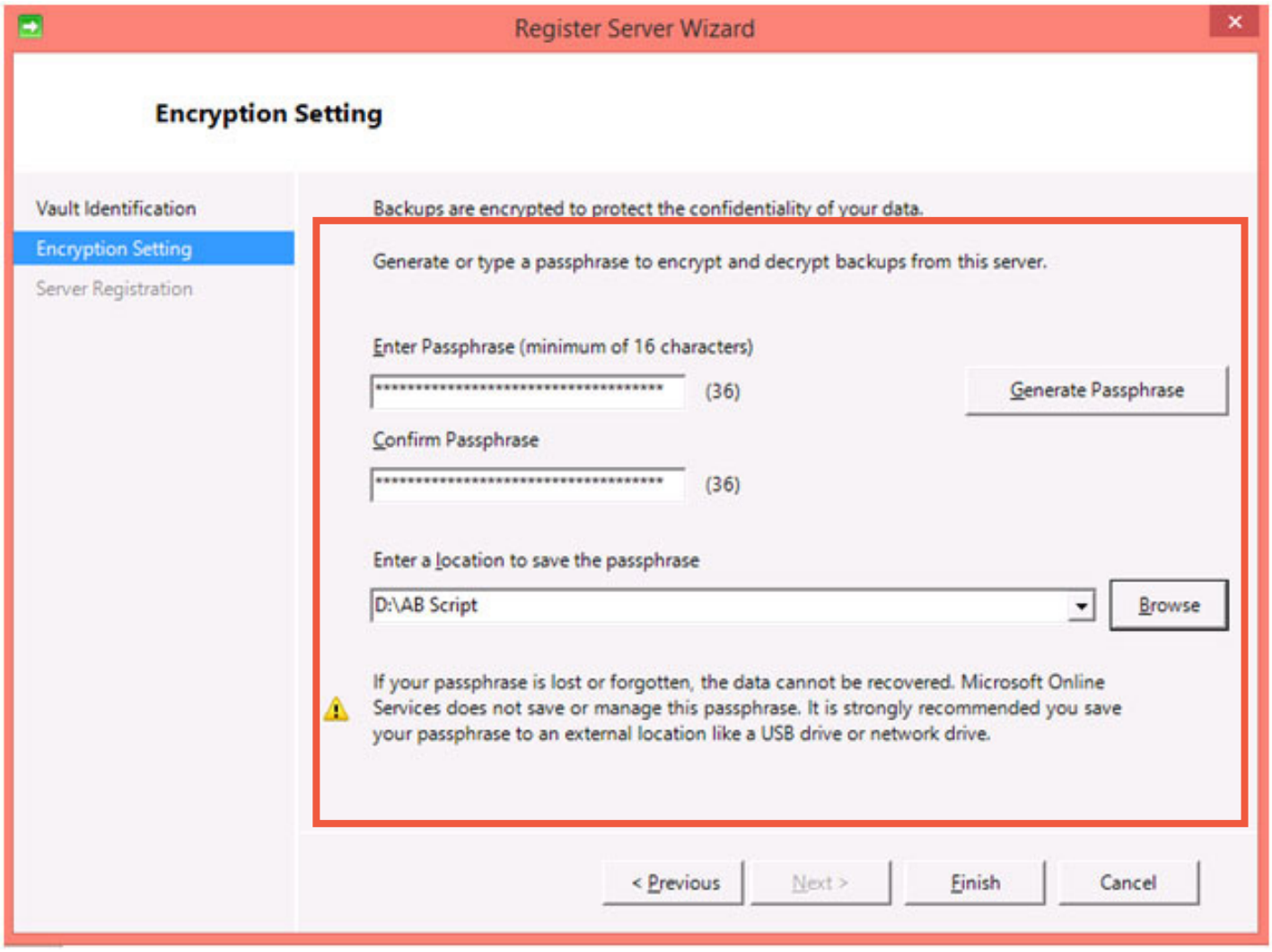


Note: The vault credentials file is valid only for 48 hrs (after it is generated via PowerShell or in the Azure portal). If you encounter any error in this screen (e.g "Vault credentials file provided has expired"), a new vault credentials file will need to be obtained.

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 obtaining a new vault credential file.

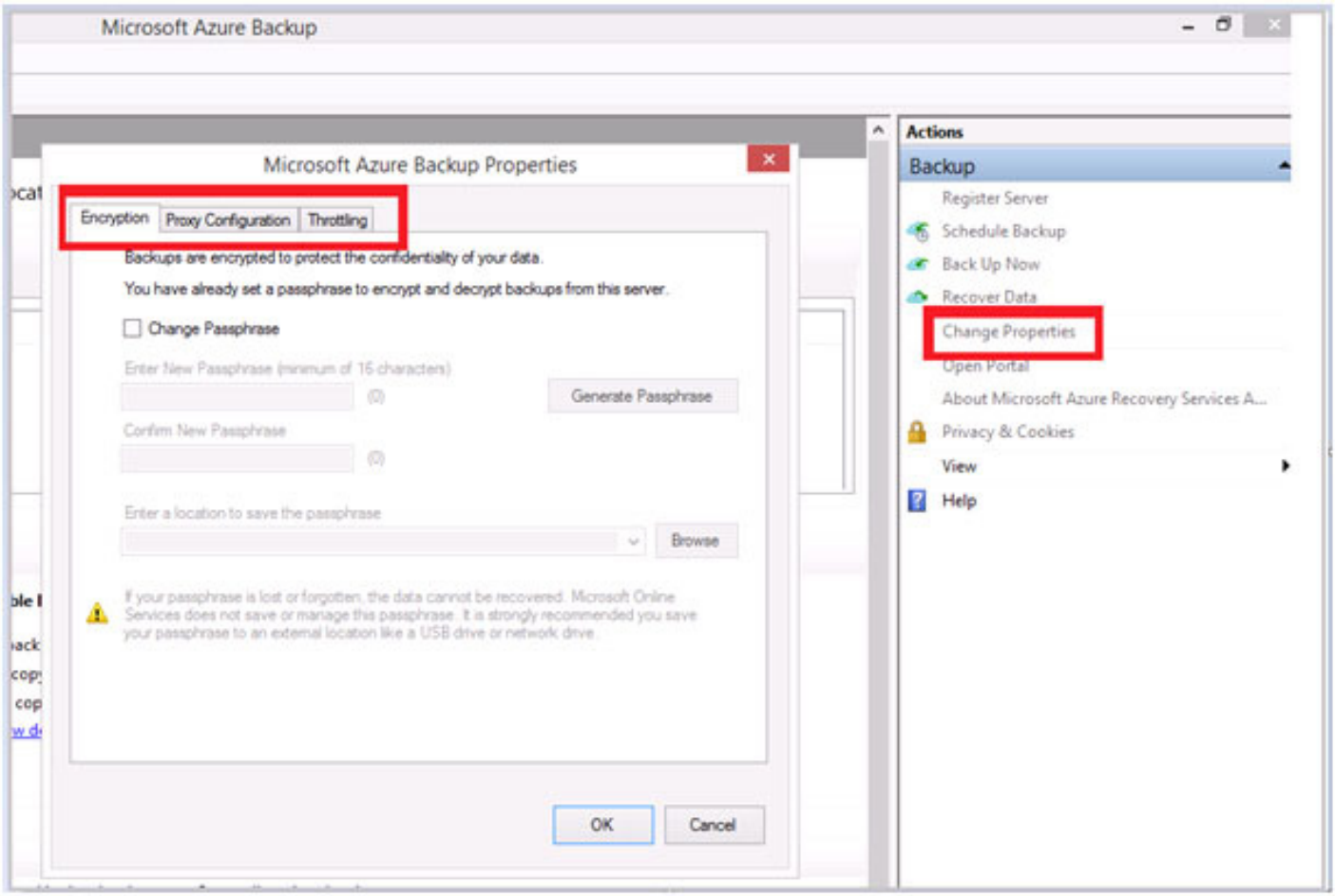
7. In the **Encryption setting** screen, you can either generate a passphrase or provide a passphrase (minimum of 16 characters). Remember to save the passphrase in a secure location.



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 visibility into the passphrase used by the end user. Please save the file in a secure location as it is required during a recovery operation

8. 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.
9. When using Microsoft Azure Backup you can modify the settings specified during the registration workflow by clicking on the **Change Properties** option in the Azure Backup mmc snap in.

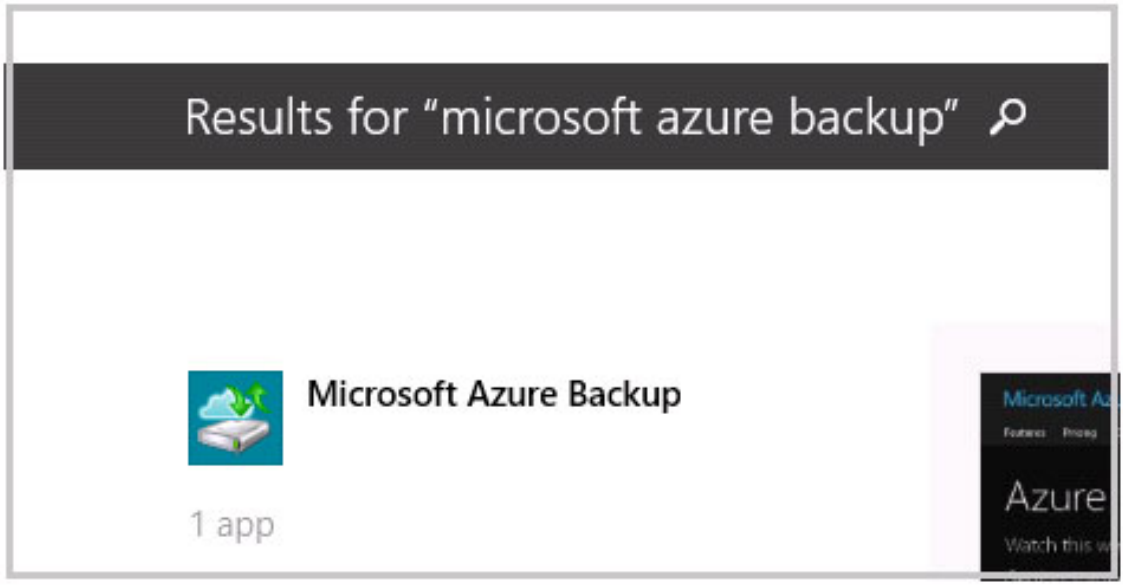


Back up Windows Server or Windows Client files and folders to Azure

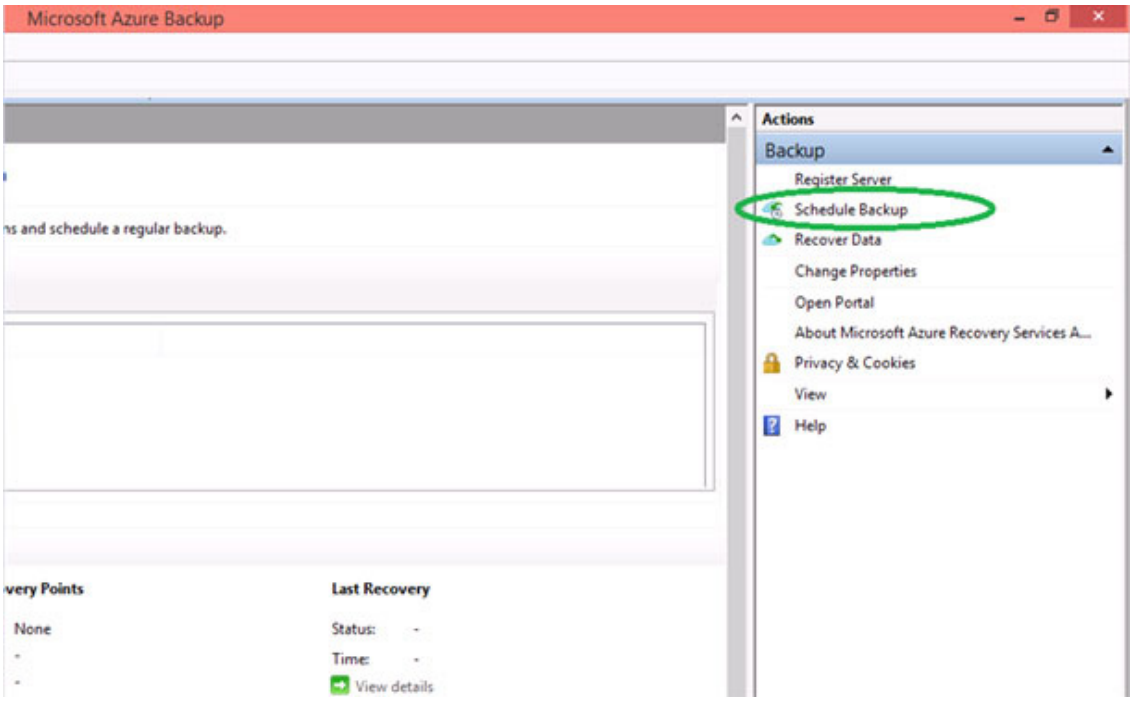
It's easy to back up Windows files and folders to Azure with this simple procedure. If you haven't already done so, complete the prerequisites to prepare your environment to back up your Windows machine before you proceed.

Back up files and folders

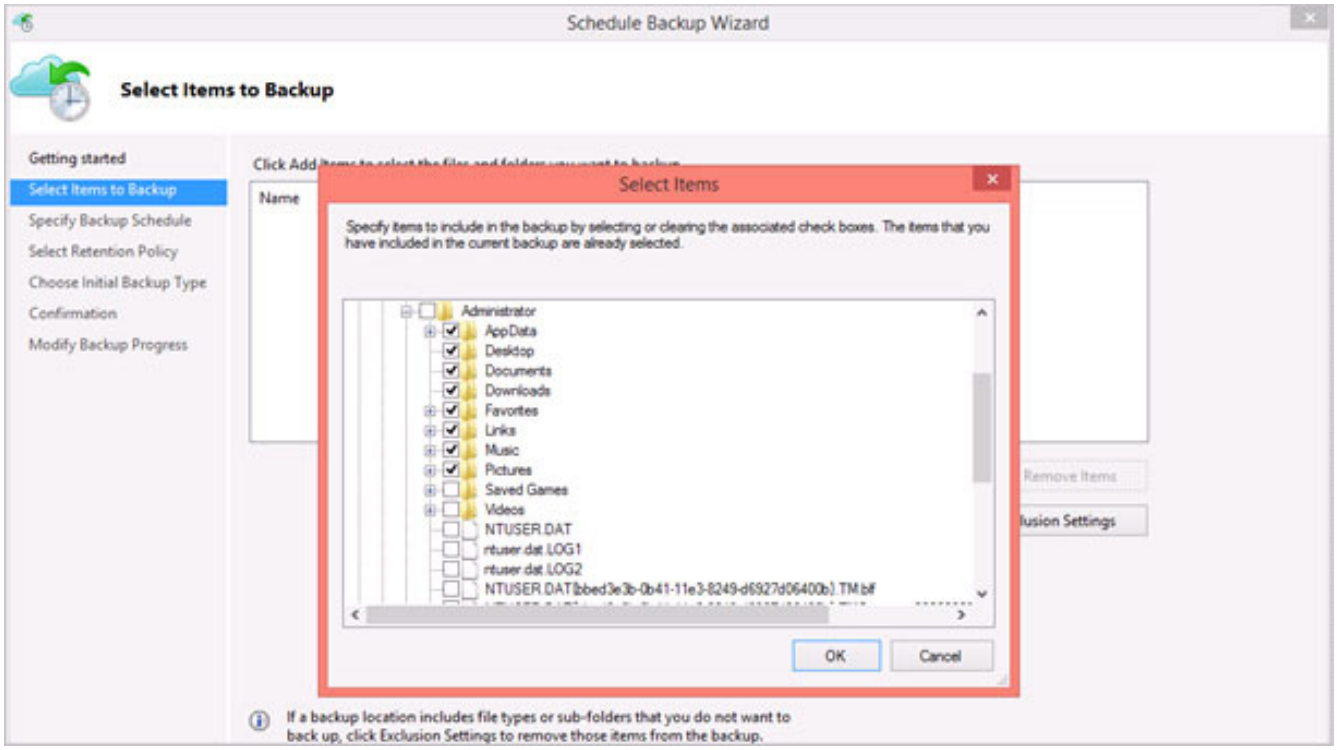
1. Once the machine is registered, open the Microsoft Azure Backup mmc snap-in.



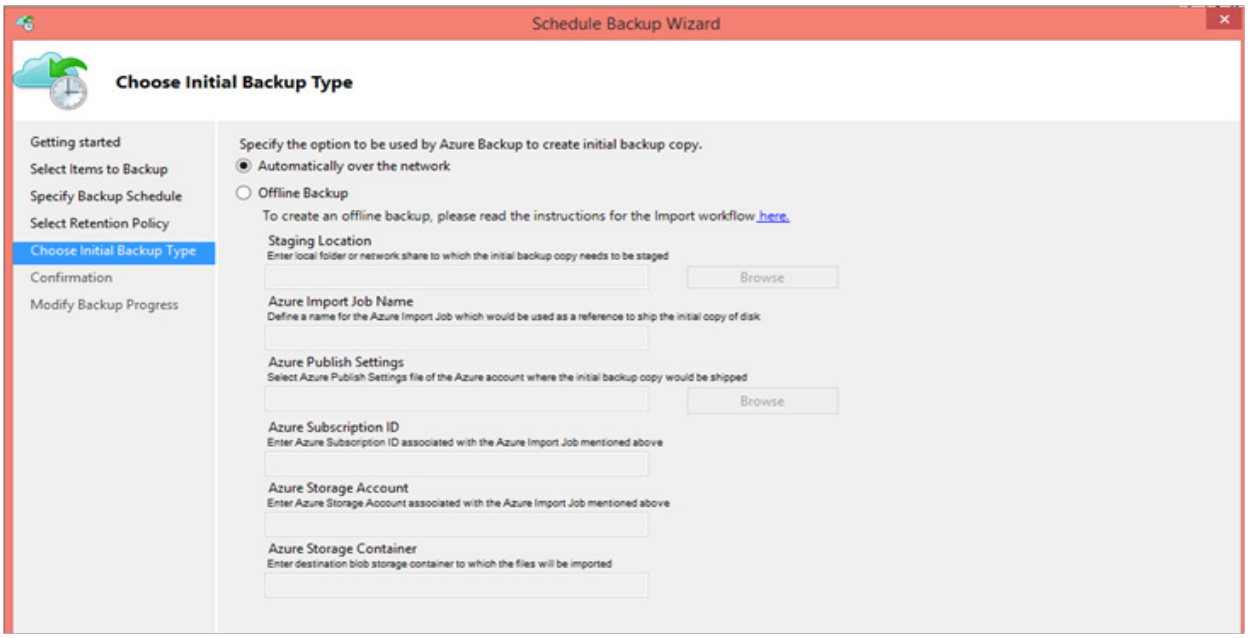
2. Click **Schedule Backup**



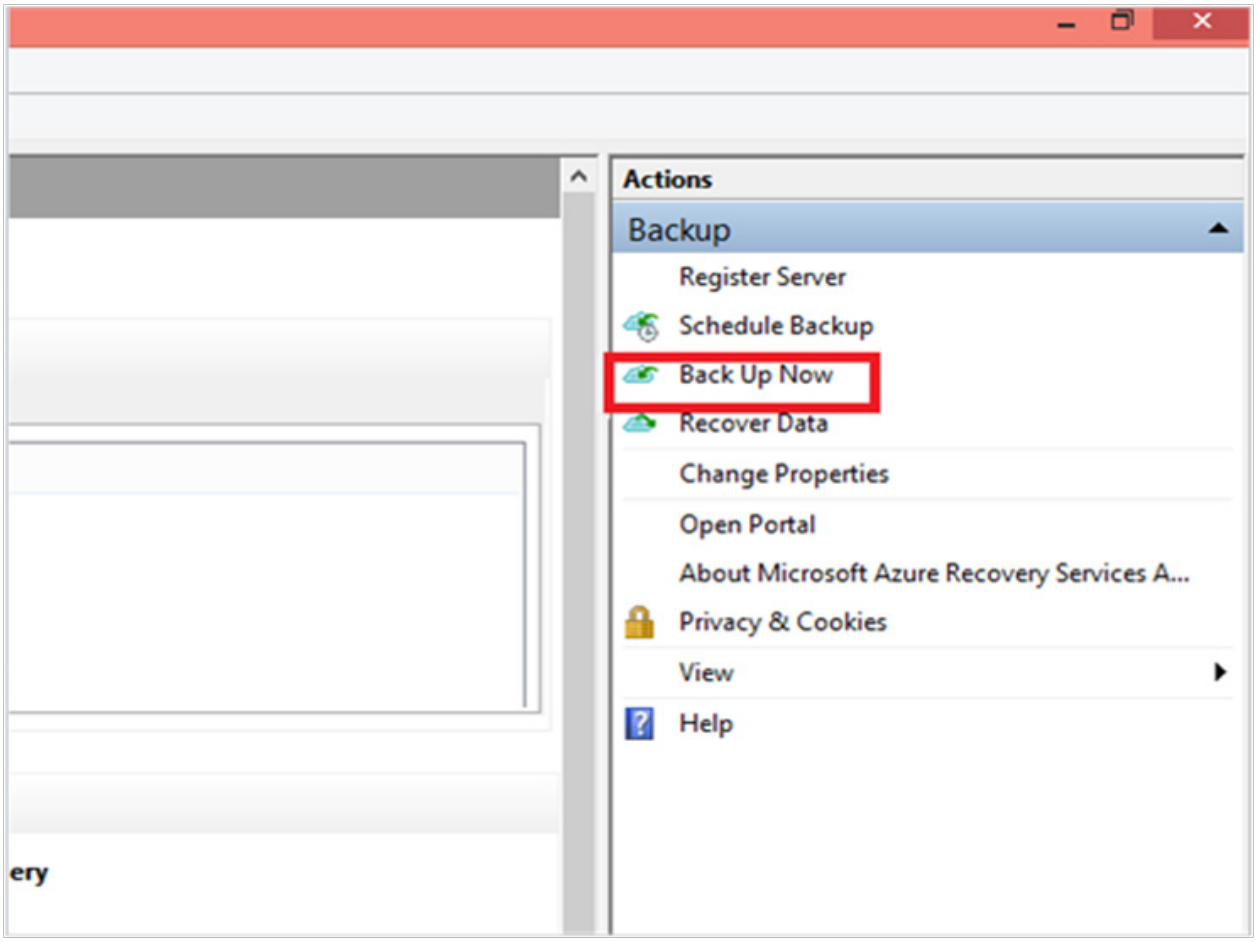
3. Select the items you wish to back up. Azure Backup on a Windows Server/Windows Client enables you to protect files and folders.



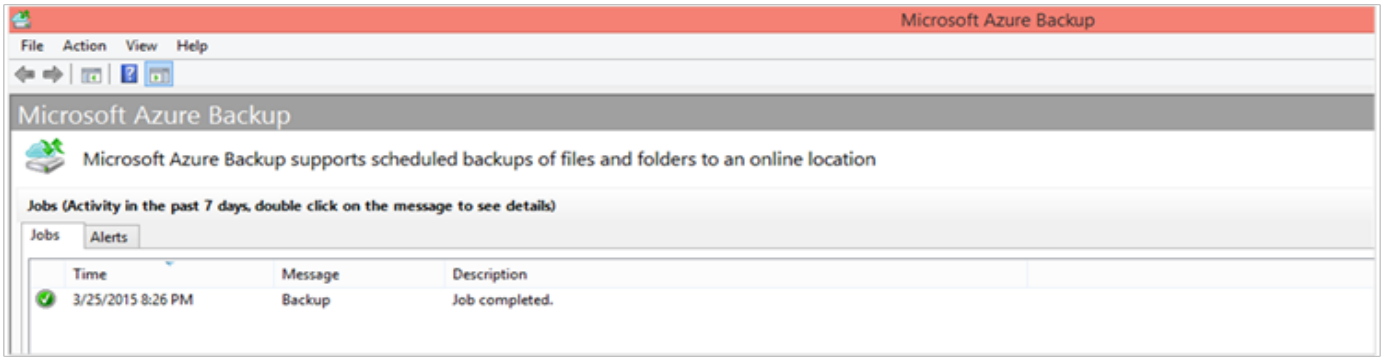
4. Specify the backup schedule and retention policy which is explained in detail in the following article.
5. Choose the method for sending the initial backup. Please note: as of now, the only option that is available for initial back up is 'automatically over the network'. The option to do initial back-ups offline will be made available later this year.



6. After the schedule backup process is completed, go back to the mmc snap in and click **BackUp Now** to complete the initial seeding over the network.



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



Dell Technical Support

Dell Support can be reached by telephone at 1-888-927-4187 or by email: AzureSupport@Dell.com