Cloud protection with Windows Azure Backup

Sky Blue

Microsoft offers the Windows Azure Backup service, which lets you back up data from servers in the cloud. This removes the need for your own infrastructure, and the service alleviates privacy concerns by using continuous encryption. By Thomas Joos

Microsoft is continuing to offer new features – both for installable ("on premise") software as well as services that run in the Azure cloud. A recent example of a new cloud feature is Windows Azure Backup [1], which gives users the ability to back up in the cloud. The Windows Azure service latches on to the internal data backup feature in Windows Server 2012/2012 R2 and lets you create a custom schedule for data backups to the cloud. Windows Azure can run in parallel with existing backups or as a complete data backup solution. Data is encrypted in the cloud and, of course, during transmission, to stay safe from prying eyes.

With Windows Azure, you can even back up entire virtual servers, including their configurations, in the cloud. The service is compatible with the new Windows Server 2012 R2, even in the Essentials edition, as well as with older products, like Windows Server 2008 R2. Billing is based on the compressed files that are stored in the cloud during a billing period of one month [2].

Getting Started

To use or test Windows Azure Backup, you need a free Windows Azure account. Windows Azure is integrated into Windows backup after installing the client software and can be enabled and configured separately from a local backup. In contrast to SkyDrive and others, Windows Azure is for backing up data only, not for sharing data.

Additionally, you need an agent that can save the data online in Windows Azure; you will find this on the Azure portal [3]. The familiar Windows backup interface is used for backing up and restoring. You can also control the process in Windows PowerShell; a separate module exists for this.

Windows Azure supports incremental backups, in which case it only transfers the changed blocks. Data is encrypted by the agent and also stored encrypted in Windows Azure. After completing a backup, Azure automatically checks the integrity of the data. You can use a policy to set an automatic expiration date for older backups.

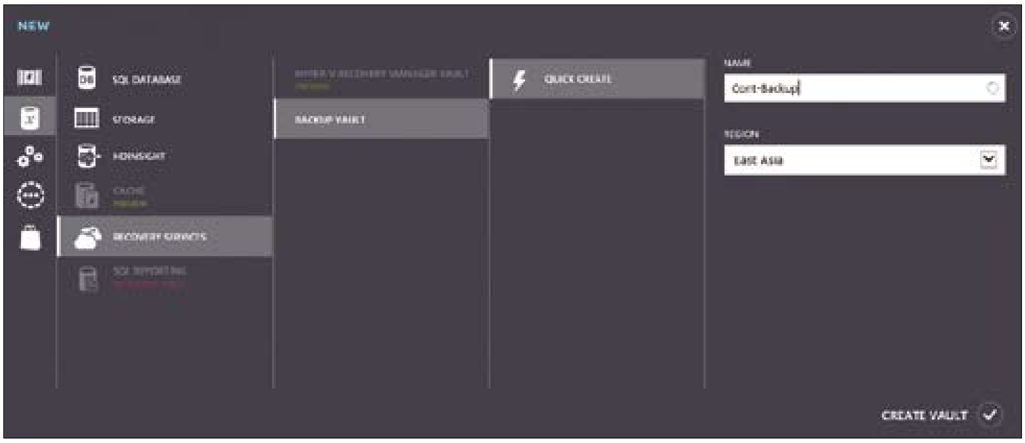
The service particularly makes sense when using Windows Server 2012 R2 Essentials or the Essentials environment server role in other editions of Windows Server 2012 R2. To set up and use the service, wizards are available in the Windows Server R2 Essentials dashboard. However, you can manage backups in Windows Azure via the System Center Data Protection Manager. Companies can use this to back up some data locally and other

Lead Image © Oleksiy-Mark, 123RF.com

data in the cloud.

The agent is proxy-capable, which can simplify the process of connecting to the Internet.

To set up the backup on a server, first install Windows Server Backup. This is done in Server Manager from *Manage | Add Roles and Features*. Install the *Windows Server Backup* feature. In Windows Server 2012 R2 Essentials, the feature is installed by default.



NAME: Cont-Backup

REGION: East Asia

Figure 1: To use Windows Azure backup, you first need a backup vault.

Configuration in the Dashboard

If you are using Windows Server 2012 R2 Essentials, log in to Windows Azure via the Dashboard. On the home screen in the Dashboard, select *Add-Ins* and then *Integrate with Windows Azure Online Backup*. On the right-hand side, log in to Windows Azure. You can use this approach for logging in or register for a trial version on the Windows Azure Backup home page. After creating an account, you can download the client for integrating Windows Azure in the dashboard. Separate agents are available for integration with DPM and Windows Server Backup.

If you want to set up Windows Azure Backup in other editions of Windows Server 2008 or Windows Server 2012/2012 R2, you first need to press the plus sign at the bottom of the screen on the Windows Azure portal. Then, set up a vault in `New\Data Services\Restore Services\Backup Vault`, in which Windows Azure Backup can store its data (Figure 1). The data stored in this vault is encrypted.

Once you have a vault, you will see a new link on the Windows Azure Management Portal, *Recovery Services*; this takes you to your vault. Click the link to manage a certificate for backups, retrieve setup information, and download the Agent for integrating local servers. Authentication between agents and Windows Azure is certificate based.

You need to export the certificate as a `.cer` file to the server with which you will be backing up data in Windows Azure. To do so, launch the local certificate management console, `certlm.msc`, on the server and right-click the certificate after the install. Then, select *All Tasks | Export* to export the certificate to a `.cer` file. You do not need to export the private key. You then import this file into your vault via the Dashboard. When the server connects to Windows Azure, the certificate is recognized and the server integrated. In other words, Windows Azure Backup and the server that you are backing up need the same certificate, regardless of whether you buy a certificate or use an internal certificate.

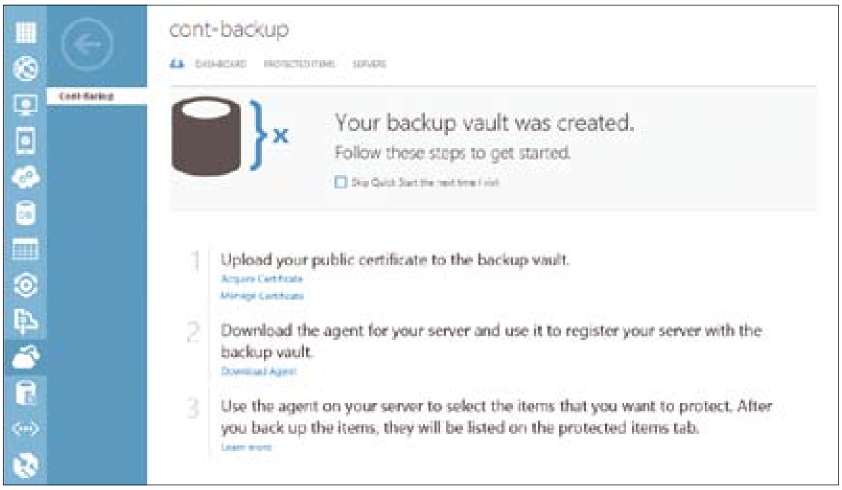
For testing purposes, you can also create a self-signed certificate. To do this, use the `makecert.exe` tool from the Windows SDK 8/8.1 [4]. You will find `makecert.exe` in the `C:\Program Files (x86)\Windows Kits\8.0\bin\x64` directory. You can create a certificate like this:

```
makecert.exe -r -pe -nCN=<Servername> ➚
  -ssmy -sr localmachine-eku ➚
  1.3.6.1.5.5.7.3.2 -len 2048 ➚
  -e01/01/2016 <Certificate>
```

Then, install the certificate you created on the server, export it and upload the exported `.cer` file to Windows Azure Backup – just like any other certificate (Figure 2).

Backup Agent

The servers with the data you will be backing up to the cloud need an agent; you will find one on the Management Portal in Windows Azure.



Your backup vault was created.

Follow these steps to get started.

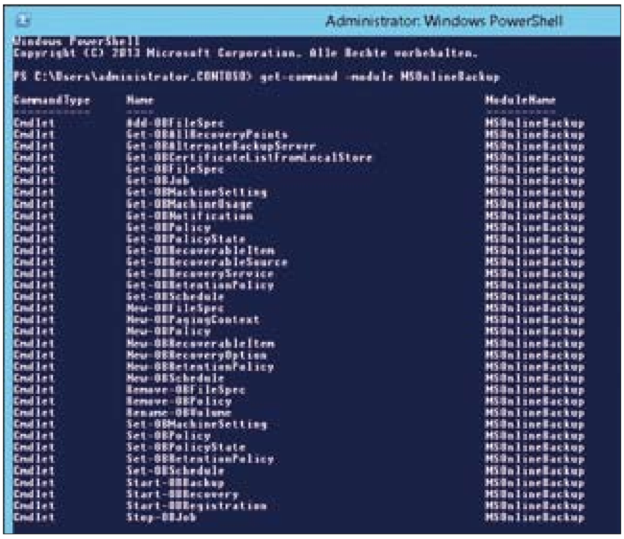
☐ Skip Quick Start the next time I visit

1 Upload your public certificate to the backup vault.
Acquire Certificate
Manage Certificate

2 Download the agent for your server and use it to register your server with the backup vault.
Download Agent

3 Use the agent on your server to select the items that you want to protect. After you back up the items, they will be listed on the protected items tab.
Learn more

Figure 2: The first configuration of Windows Azure backup is in the Windows Azure web interface.



Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Users\administrator.CONTOSO> get-command -module MSOnlineBackup

CommandType     Name                                     ModuleName
-----------     ----                                     ----------
Cmdlet          Add-OBFileSpec                           MSOnlineBackup
Cmdlet          Get-OBAllRecoveryPoints                  MSOnlineBackup
Cmdlet          Get-OBAlternateBackupServer              MSOnlineBackup
Cmdlet          Get-OBCertificateListFromLocalStore      MSOnlineBackup
Cmdlet          Get-OBFileSpec                           MSOnlineBackup
Cmdlet          Get-OBJob                                MSOnlineBackup
Cmdlet          Get-OBMachineSetting                     MSOnlineBackup
Cmdlet          Get-OBMachineUsage                       MSOnlineBackup
Cmdlet          Get-OBNotification                       MSOnlineBackup
Cmdlet          Get-OBPolicy                             MSOnlineBackup
Cmdlet          Get-OBPolicyState                        MSOnlineBackup
Cmdlet          Get-OBRecoverableItem                    MSOnlineBackup
Cmdlet          Get-OBRecoverableSource                  MSOnlineBackup
Cmdlet          Get-OBRecoveryService                    MSOnlineBackup
Cmdlet          Get-OBRetentionPolicy                    MSOnlineBackup
Cmdlet          Get-OBSchedule                           MSOnlineBackup
Cmdlet          New-OBFileSpec                           MSOnlineBackup
Cmdlet          New-OBPagingContext                      MSOnlineBackup
Cmdlet          New-OBPolicy                             MSOnlineBackup
Cmdlet          New-OBRecoverableItem                    MSOnlineBackup
Cmdlet          New-OBRecoveryOption                     MSOnlineBackup
Cmdlet          New-OBRetentionPolicy                    MSOnlineBackup
Cmdlet          New-OBSchedule                           MSOnlineBackup
Cmdlet          Remove-OBFileSpec                        MSOnlineBackup
Cmdlet          Remove-OBPolicy                          MSOnlineBackup
Cmdlet          Rename-OBVolume                          MSOnlineBackup
Cmdlet          Set-OBMachineSetting                     MSOnlineBackup
Cmdlet          Set-OBPolicy                             MSOnlineBackup
Cmdlet          Set-OBPolicyState                        MSOnlineBackup
Cmdlet          Set-OBRetentionPolicy                    MSOnlineBackup
Cmdlet          Set-OBSchedule                           MSOnlineBackup
Cmdlet          Start-OBBackup                           MSOnlineBackup
Cmdlet          Start-OBRecovery                         MSOnlineBackup
Cmdlet          Start-OBRegistration                     MSOnlineBackup
Cmdlet          Stop-OBJob                               MSOnlineBackup
```

Figure 3: Displaying the available commands for Microsoft Online Backup in PowerShell.

You do not need to enter any more data to install the agent on the server that you want to back up. The wizard supports Windows Server 2008 R2 SP1 and Windows Server 2012/2012 R2, as well as Windows Server 2012 R2 Essentials and System Center Data Protection Manager 2012 SP1/2012 R2.

Windows Server 2012/2012 R2 Essentials has its own agent. You can set it up after installing the agent using Windows Server Backup or the separate link. You can also script the agent installation at the command line with various options:

- `/q` – Install without feedback
- `/l` – Installation directory (e.g., `/l:"D:\Online-Agent"`)
- `/d` – Uninstall

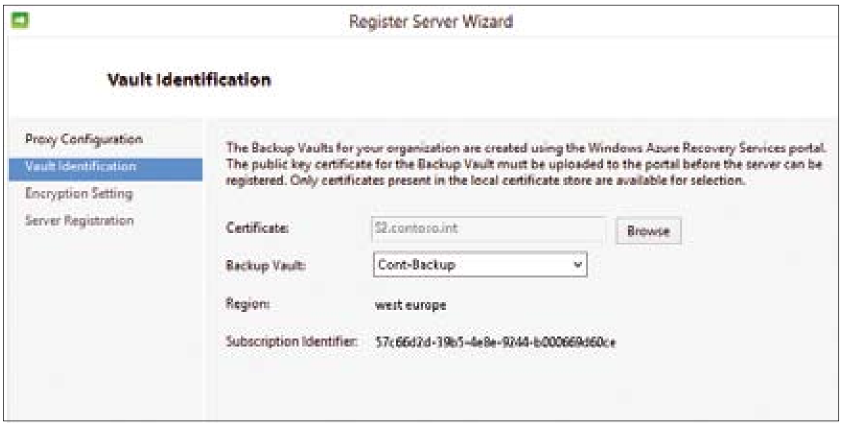
After launching Windows Server Backup, you must register the server as a backup source with Windows Azure. In the following sections, you will learn how to do that. You can remove registered servers from Azure again on the Windows Azure Management Portal. This has the advantage that you can then use the license for a different server. You can register and license multiple servers for one backup ID. All servers can be centrally managed, for example, to restore data from different servers at different locations. Restoration is also wizard-based with a graphical user interface.

Once you have Windows Server Backup and the agent installed, you will find two new icons on the start page of Windows Server 2012/2012 R2: one for the graphical interface and the other for the *Windows Azure Backup Shell*; this is the PowerShell module for online backups. You will also find the graphical interface in the normal management interface of Windows Server 2012/2012 R2 Backup (`wbadmin.msc`). You can also enter the commands for online backup in a normal PowerShell session.

In PowerShell, you can view the available commandlets with `get-command *ob*`. Alternatively, use the command

```
get-command -module MSOnlineBackup
```

(Figure 3). You do not need to load any more modules, because PowerShell in Windows Server 2012 and 2012 R2 loads them automatically when a commandlet is called.



Register Server Wizard

Vault Identification

The Backup Vaults for your organization are created using the Windows Azure Recovery Services portal. The public key certificate for the Backup Vault must be uploaded to the portal before the server can be registered. Only certificates present in the local certificate store are available for selection.

Certificate: S2.contoso.int

Backup Vault: Cont-Backup

Region: west europe

Subscription Identifier: 57c66d2d-39b5-4e8e-9244-b000669d60ce

Figure 4: While setting up the agent, you use a certificate to map it to a vault in Windows Azure.

Registering with the GUI

To start managing the backup, open the management console in the home screen, preferably using `wbadmin.msc`. You will find a shortcut if you search for 'Windows Azure Backup'. Next, select *Online Backup* in the menu; this is below *Local Backup* in the backup management utility on Windows Server 2012/2012 R2. The console checks the installed agents. Click *Register Server*.

Active Directory Optional

In the wizard, select the certificate with which the agent will log into Windows Azure. You can also work with certificates from the Active Directory Certificate Services here.

If you select the certificate during the server setup, the wizard checks whether its counterpart is available in Windows Azure. After that, you can connect to the vault you created previously (Figure 4).

Next, enter the passphrase for encrypting your data; write this down and keep it in a safe place. If the passphrase is lost, you no longer have access to your data backup. As a final step, complete the process for registering. You can then set up the backup.

You will see the registered server on the Windows Azure portal after completing this setup. To do so, press *Recovery Services* and select your vault. All connected servers can be found via the *Servers* menu item. In this window, you can also resolve the link.

Schedule

Once you have registered the server, you can use the management interface

Listing 1: Complex Settings

```
$mon = [System.DayOfWeek]::Monday
$tue = [System.DayOfWeek]::Tuesday
Set-OBMachineSetting -WorkDay "Mo", "Tu" -StartWorkHour "9:00:00" -EndWorkHour "18:00:00"
                     -WorkHourBandwidth (512*1024) -NonWorkHourBandwidth (2048*1024)
```

(`wbadmin.msc`) to set up a schedule for your backups, or you can run an instant backup (e.g., for a local backup). To do this, click on *Backup* | *Schedule Backup* and specify which files you want to include in the backup.

After configuring the data, set the time of the backup. The process is the same as for using the data backup tool. Next, specify how long you want to keep the backup. The wizard replaces older backups with new backups once the retention period has expired. The backups are kept until a newer backup requires the space.

You can only create one cloud backup job, but you can schedule a parallel local backup and cloud backup. This means that you can, for example, use the local backup to back up all your data, and only back up your most important data in the cloud. You can easily launch the cloud backup job at different times and several times a day.

You can also configure backup jobs in PowerShell using a number of commandlets for the process. First, use `New-OBPolicy` to create a new policy for the backup and store it in a variable:

```
$policy = New-OBPolicy
```

Specify the directory you want to include in the backup using a variable:

```
$files = New-OBFileSpec ➘
  -FileSpec C:\data
```

Next, define the schedule for running the backup. You also store this in a variable:

```
$sched = New-OBSchedule ➘
  -DaysofWeek Wednesday ➘
  -TimesofDay 19:30
```

Set up a policy for the retention period:

```
$ret = New-OBRetentionPolicy
```

If you want to change the setting from the default (7 days) to the maximum value (30 days), use the following command:

```
$ret = New-OBRetentionPolicy ➘
  -RetentionDays 30
```

You can also create the policy to launch the backup at the next scheduled time:

```
Add-OBFileSpec -Policy ➘
  $policy-FileSpec $files
```

Next, link the policy with the schedule you created:

```
Set-OBSchedule -policy ➘
  $policy-schedule $sched
Set-OBRetentionPolicy  ➘
  -policy $policy -retentionpolicy $ret
```

If this is the first backup after registering the server, be sure to set the passphrase for the backup:

```
$passphrase = ➘
  ConvertTo-SecureStringPassphrase ➘
  -asplaintext -ForceSet-OBMachineSetting ➘
  -EncryptionPassphrase$passphrase
```

Then, save the entire online backup encryption policy:

```
Set-OBPolicy -policy $policy
```

You can launch a backup that you created previously in PowerShell.

Listing 2: Restore with PowerShell

```
$source = Get-OBRecoverableSource
$item = Get-OBRecoverableItem -Source $source[0]
$FinalItem = Get-OBRecoverableItem -ParentItem $item[0]
$recover_option = New-OBRecoveryOption
Start-OBRecovery -RecoverableItem $FinalItem -RecoveryOption $recover_option
```

To do so, use the `Get-OBPolicy | Start-OBBackup` commandlet.

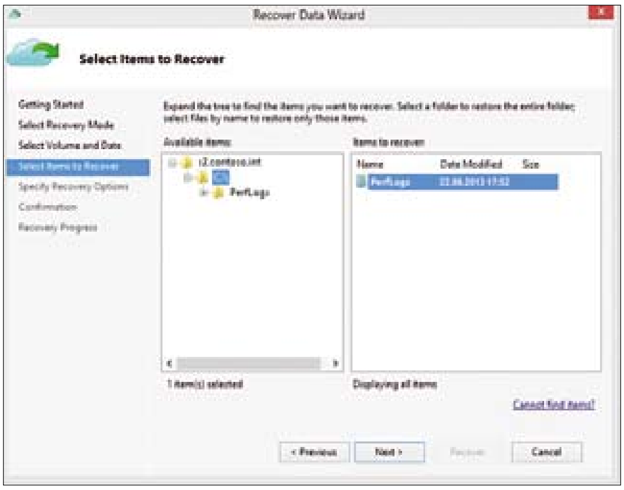
Monitoring and Troubleshooting

You can change the settings for the backup at any time, of course. You can also use Properties/Bandwidth Throttling to limit the bandwidth available to the online backup. You can enter data from 256Kbps to 1Gbps and also specify dates when these values apply. You can also configure these settings in PowerShell. An example is shown in Listing 1.

Keys and Proxies

In the *Encryption* tab, you can change the password for the encryption; *Proxy Configuration* lets you enter the data for the proxy server. You can see the online backup schedule in the Windows Server 2012 task management, *Microsoft Online Backup* section. Again, you can make changes here.

The Azure Backup management console also has a *Warnings* tab, where messages from the service are displayed. They can include messages about storage space or notifications when a new version of the agent becomes available. If you click on a message, you typically see a hint or a link to a website that can help you solve the current problem.



Expand the tree to find the items you want to recover. Select a folder to restore the entire folder; select files by name to restore only those items.

Figure 5: You can restore data from Windows Azure Backup via the Windows Azure Backup management interface or use PowerShell.

The PowerShell `Get-OBJob` command displays an overview of the configured backup job. The agent writes errors to logfiles, in addition to the Event Viewer. You will find them, for example, in the `C:\Program Files\Windows Azure Backup Agent\Temp` directory. In the Event Viewer, you will find more detailed messages under *Application and Service Logs\Cloud Backup*. The backup is handled by the Windows Azure Backup Agent system service. You can restart or stop the service for troubleshooting. At the command line, type either

```
NET START OBENGINE
NET STOP OBENGINE
```

to do so.

Restoring Data

You can restore data with Azure Backup just as from a local backup: Right-click *Backup* and choose to restore. In the wizard, select the data storage device from which you will be restoring the data and at what time. You also need to define a location for the restored data in the window.

When starting the restore, you can also choose a server from which you want to recover data (Figure 5). The wizard shows all the servers that you have registered. Instead of the graphical interface, you can use PowerShell. To do this, store the appropriate data in variables and then start the recovery (Listing 2).

Web Portal-Based Management

You can centralize management of Windows Azure Backup using the Azure portal. To do so, click *Recovery Services* and then select the vault with the servers and data you want to manage. *Dashboard* lets you view the volume of data in the vault, which is important for billing. You can also view your registered servers. *Protected Elements* lets you view your backed up data. Although you cannot access or recover data here, you can see when data was backed up, as well as the servers and disk drives from which the data originated. For information on the individual servers, select *Servers* in the menu, which shows all the registered servers in your portal.

Conclusions

Windows Azure can be a valuable supplement to, or even a complete replacement for, an existing data backup solution for a business. In smaller companies with Windows Server 2012 R2 Essentials, the cloud solution can fully replace a local backup.

Even for smaller branch offices or medium-sized businesses, Windows Azure Backup is very interesting as part of a backup solution. Because the backed up data are encrypted for storage in the Microsoft cloud, they are protected to the greatest extent possible against unauthorized access. ■

Info

[1] Windows Azure Backup: [http://www.windowsazure.com/en-us/services/backup]

[2] Azure pricing: [http://www.windowsazure.com/en-us/pricing/details/storage/]

[3] Management Interface: [https://manage.windowsazure.com/]

[4] Makecert: [http://msdn.microsoft.com/en-us/library/windows/desktop/aa386968(v=vs.85).aspx]