CONTENT PROVIDED BY

November 2013 Redmondmag.com

Redmond

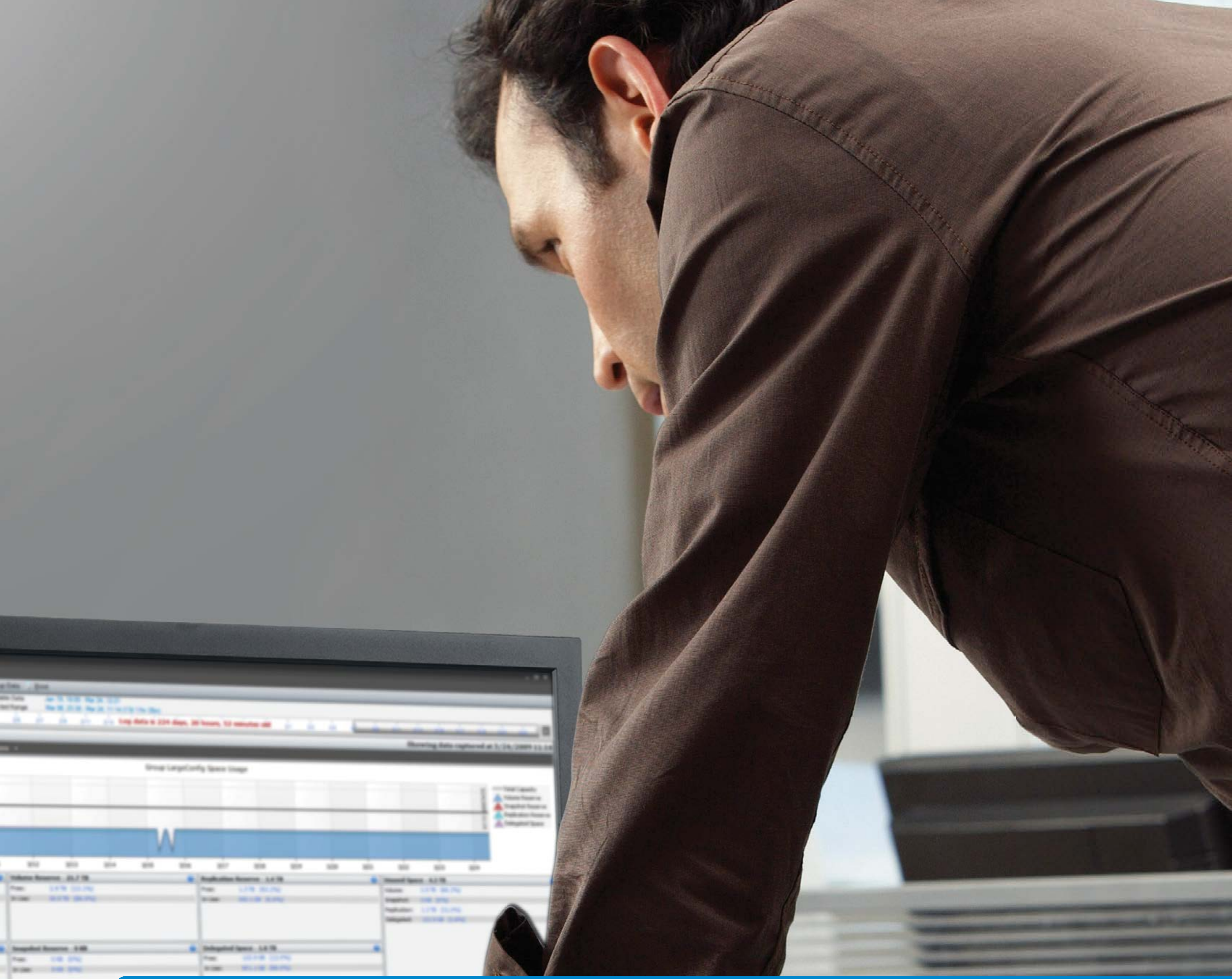
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

Use Windows Azure as a Backup Target

How to connect four backup and recovery software tools to the Microsoft public cloud to protect and archive your data. *Page 1*

> Software Simplifies Exchange Recovery *Page 10*

1105 MEDIA



Using Windows Azure as a Backup Target

How to connect four backup and recovery software tools to the Microsoft public cloud to protect and archive your data.

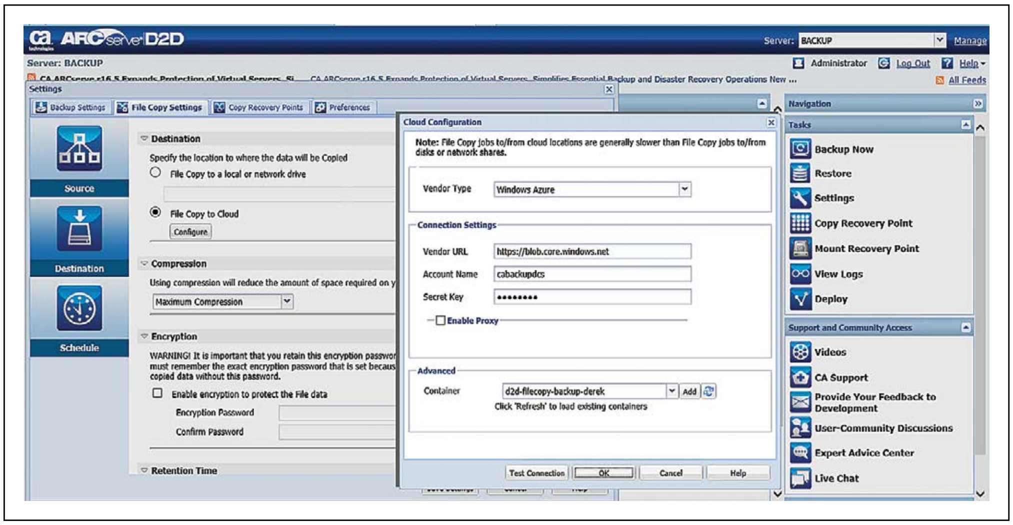
BY DEREK SCHAULAND

Nothing will cut your career short more quickly than losing critical data because it wasn't properly backed up. And of course having that data properly backed up assumes it can be easily recovered. It doesn't matter if it's lost to disaster or inadvertently deleted. Data must be backed up.

Microsoft Windows Azure has become one of the most formidable alternatives to Amazon.

Now that many organizations are backing up or archiving their data to public cloud services, users expect to recover data more quickly than they could when it was stored on tape. Amazon Web Services Inc. (AWS) is the most widely used and dispersed cloud storage provider with its Simple Storage Service (Amazon S3) and Glacier archive offerings. There's no shortage of other services providers of all sizes. Microsoft Windows Azure has become one of the most formidable alternatives to Amazon, now that its long-awaited infrastructure services are available.

Windows Azure infrastructure services are especially appealing to those looking to augment their Windows Server-based applications. Support for Linux instances also makes Windows Azure infrastructure



Server: BACKUP

Settings

Destination

Specify the location to where the data will be Copied

○ File Copy to a local or network drive

● File Copy to Cloud

Compression

Using compression will reduce the amount of space required on y

Maximum Compression

Encryption

WARNING! It is important that you retain this encryption passwor must remember the exact encryption password that is set becaus copied data without this password.

□ Enable encryption to protect the File data

Encryption Password

Confirm Password

Retention Time

Cloud Configuration

Note: File Copy jobs to/from cloud locations are generally slower than File Copy jobs to/from disks or network shares.

Vendor Type: Windows Azure

Connection Settings

Vendor URL: https://blob.core.windows.net

Account Name: cabackupdcs

Secret Key: ••••••••

□ Enable Proxy

Advanced

Container: d2d-filecopy-backup-derek

Click 'Refresh' to load existing containers

Figure 1. *The ARCserve Cloud Configuration Web dialog will let you connect to Windows Azure for file copy.*

Several leading backup and recovery solutions now support Windows Azure as a target.

services an attractive target for backup and recovery. Analysts and ISVs alike say many enterprises are already using it for backup and recovery or are planning to do so.

Several leading backup and recovery solutions now support Windows Azure as a target, although you must have a Microsoft account to set up a storage bucket. You can set up an account at **windowsazure.com**. The key backup and recovery solutions designed to natively use Windows Azure as a target include CA ARCserve, CommVault Simpana, Veeam Backup & Replication Cloud Edition and Vision Solutions Double-Take 7.0. Listed here in alphabetical order is how to configure each solution for Windows Azure.

CA ARCserve D2D
CA Technologies
ca.com

Workstation pricing starts at $445.20 (for a five pack). Windows Server and Linux server pricing starts at $732. Per-socket pricing (which also includes CA ARCserve Backup and file-only replication) starts at $795. Per-terabyte pricing (which includes CA ARCserve D2D, CA ARCserve Backup and file-only replication) is also available.

CA added a file copy component to its ARCserve Disk-to-Disk (D2D) software. This allows off-site file replication based on policies and filters configured against your servers. Using the application in a test environment has proven quite effective.

Using the Web interface to configure the application (which runs on your local ARCserve server) was a nice change from other "Application Windows." ARCserve D2D interacts with Windows Azure, but not in a way I had expected. When configuring backups, the target is traditional and can be locally attached or networked. Where Windows Azure comes to the table is on file copy. ARCserve D2D uses a configured policy to send data to the offsite container in Windows Azure once you have it configured. To get D2D and Windows Azure communicating, follow these steps:

When configuring backups, the target is traditional and can be locally attached or networked.

1. Log in to the ARCserve D2D Web console with a user account in the domain or on the server.
2. Select settings from the Getting Started console (or the navigation bar on the right).
3. Under Backup Settings, select the backup target location.
4. Select the amount of information to back up (the entire machine or specific files), the compression level and the number of recovery points to retain.
5. Click the Schedule button to specify a schedule for the backup, including when to run full and incremental backup jobs.
6. For advanced options such as specifying administrator credentials for the likes of SQL Server or Exchange, select the Advanced button to configure specific items related to these applications.
7. On the Pre/Post Backup Settings page, you can specify any commands to run before or after the backup job.
8. Once the backup job configuration is complete, click the File Copy Settings tab at the top of the Web dialog (see **Figure 1**, p. 2).
9. Check the Enable File Copy box to turn the feature on.
10. Click Add to create a file copy policy. From there, you specify a source drive and a filter criteria to determine which files get copied to Windows Azure (*.dll to copy all of the DLL files from the source to the Windows Azure cloud).
11. When this is configured, click Destination. This is where you point the ARCserve D2D application at a storage bucket in Windows Azure.
12. Select File Copy to Cloud and click the Configure Button. Note: ARCserve D2D preconfigures the Windows Azure URL when you choose Windows Azure as the provider. Do not change the URL because the configuration won't if the URL isn't correct.
13. Enter your Account name as configured in Windows Azure.
14. Enter the Secret Key for the specified Windows Azure account.
15. Click the Add button next to the dropdown for a container. Here, you specify the name of the container that will be created to hold your data. The name will be prepended with text to help ARCserve D2D recognize the container.
16. Click Test Connection to validate your settings.
17. Click OK to save the file copy configuration for Windows Azure.

18. Click Schedule to specify the number of backups to perform before the copy is performed.
19. Click Save Settings to save the backup job.

The file copy process isn't immediate. It's configured to happen after a specified number of backups have run. So if you specify this to happen after one backup, then it would happen right away. ARCserve D2D doesn't care if backups are full or incremental, just that the specified number of backups have occurred.

Once that threshold is met, files meeting the specified policy are pushed off to the container in Windows Azure. This works more like a replication or traditional copy offshoring than using Windows Azure as a direct backup target. For organizations looking for both local and cloud backup, though, this might be a really good fit.

Using Windows Azure as a native backup target requires a version of ARCserve running on Windows Server. If you're using ARCserve on Linux, you can create a Common Internet File System (CIFS)/ Network File System (NFS) share with help from a third party where a user can back up his data to Windows Azure.

Using Windows Azure as a native backup target requires a version of ARCserve running on Windows Server.

CommVault Simpana
CommVault
commvault.com

$25,000 with 32TB of archive capacity, one year of support and one day of professional services.

CommVault Simpana uses libraries and policies to manage backup jobs and data. When using a cloud provider, these concepts remain in place, but the endpoint in this case is a container within Windows Azure. Simpana relies on the media agent to manage backup jobs, so you'll need to configure at least one media agent component, but it supports multiple components.

To connect Simpana to Windows Azure, complete the following steps:

1. Configure a library to point to Windows Azure by right-clicking Libraries in the console navigation pane and selecting Add (see **Figure 2**, p. 5). Choose Cloud Storage Library.
2. Enter a name for the library and Click OK. Right-click the New Library to add a disk component.
3. In the Add Cloud Storage dialog box, specify a display name, the Windows Azure account, the secret key (with confirmation) and a container name.
4. Click OK. If the container doesn't already exist in your Windows Azure environment, Simpana will create one.
5. Create (or assign) a storage policy for the media agent.
6. Create (or assign) a scheduling policy for the media agent.

The last step involves creating a sub-client policy to specify what data you want a particular job to backup:

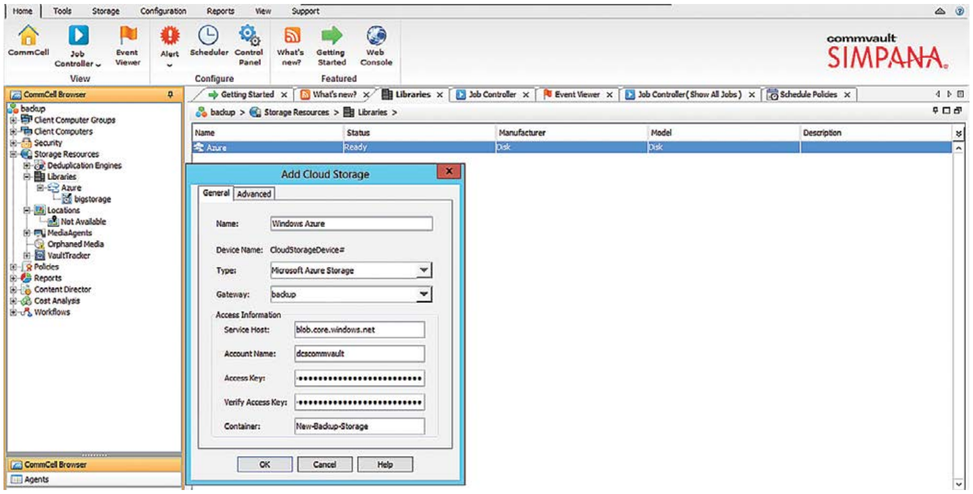
1. Expand Policies.
2. Right-click Sub-client Policies.
3. Select New Sub-client Policy.
4. Specify a name for the set of files to be backed up.
5. Specify options based on the features installed (Windows file system, for example).
6. Click the Add button.
7. On the Content tab, click Add and browse to the folders or files to include.
8. On the Filters tab, specify exclusions (if any).
9. On the Storage Device tab, select the configured storage policy to use for this file set.
10. Click OK on the properties dialog.

CommVault Simpana uses libraries and policies to manage backup jobs and data.

Now that the backup configuration is completed, jobs assigned a scheduling policy will run according to this schedule.

To run a created job immediately, complete the following steps:

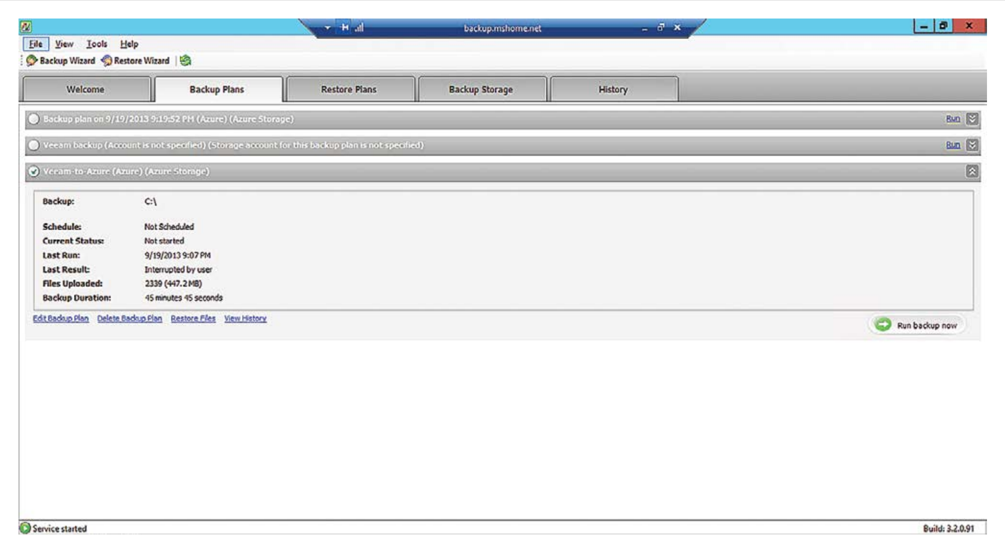
1. Expand Client computers.
2. Expand the computer you wish to back up.
3. Expand the item to be backed up (such as the File system).
4. Right-click the sub-client displayed and select Backup.



Name	Status	Manufacturer	Model	Description
Azure	Ready	Disk	Disk	

Name: Windows Azure
Device Name: CloudStorageDevice#
Type: Microsoft Azure Storage
Gateway: backup
Service Host: blob.core.windows.net
Account Name: dcscommvault
Access Key: •••••••••••••••••••••••••
Verify Access Key: •••••••••••••••••••••••••
Container: New-Backup-Storage

Figure 2. *The Simpana Add Cloud Storage dialog box lets you configure a library residing in Windows Azure.*



Backup plan on 9/19/2013 9:19:52 PM (Azure) (Azure Storage)

Veeam backup (Account is not specified) (Storage account for this backup plan is not specified)

Veeam-to-Azure (Azure) (Azure Storage)

Backup:	C:\
Schedule:	Not Scheduled
Current Status:	Not started
Last Run:	9/19/2013 9:07 PM
Last Result:	Interrupted by user
Files Uploaded:	2339 (447.2 MB)
Backup Duration:	45 minutes 45 seconds

Figure 3. *Implement and manage a backup plan in Windows Azure with the Veeam backup product.*

Simpana works in a modular fashion. You can add each piece of the application as needed.

Once the job is running, you can view progress and task completion on the Job Controller tab. Simpana works in a modular fashion. You can add each piece of the application as needed. That way it can grow as your organization's needs increase. This overview discusses options to connect to Windows Azure and add simple backup data, but Simpana also supports advanced features like deduplication and replication to another server, which may live in Windows Azure. Many of the modules used by Simpana are referred to as "policies." The two policies mentioned in this section (Storage and Scheduling) are basic components to help get your information backed up. For more information about other components, check out CommVault Books Online at **bit.ly/136OHJu**.

The storage policy determines available options for storing backed up data. You can also configure retention, encryption and compression options in a storage policy. A scheduling policy handles the type of backup being performed and when a job should be executed.

CommVault uses separate policies to manage each stage of configuration. This allows for more modular design and reusing certain features across the entire application. With a schedule policy created to execute on Fridays at 5:52 p.m., for example, this abstracts the schedule from the backup job and lets that schedule apply to many other media agents.

Veeam Backup & Replication Cloud Edition
Veeam
veeam.com

Subscription of $449 per socket per year, which includes all the features of the on-premises product.

Veeam Backup & Replication Cloud Edition is an add-on component to Veeam Backup & Replication. Veeam added Windows Azure support as a target by licensing the backup engine from CloudBerry Lab. This has its own set of tools to back up data to multiple cloud services, as well as directly from PCs to Windows Azure. You'll have to install Veeam Backup & Replication version 7 before the Cloud Edition will function. Once you have the installer downloaded and the license key, installation follows the expected Windows Installer wizard path. To configure it with Windows Azure (see **Figure 3**, p. 6), complete the following steps:

The backup engine from CloudBerry Lab has its own set of tools to back up data to multiple cloud services, as well as directly from PCs to Windows Azure.

1. Select Set up Backup Plan.
2. Select Windows Azure as the cloud provider, choose Create New Account (or select an existing account if you have an account already) and click Next.
3. Enter a name for the backup plan and click Next.
4. Select a backup mode for the backup plan and click Next. Options include:
   Advanced: lets you store and access encryption and multiple file versions with third-party tools.
   Simple: lets third-party solutions access backup files without encryption or multiple file version support.
   Custom: stores backup files in the specified folder.
   Force Using VSS: should be used when third-party tools will access files while a backup job is in process.
5. Select the drives to back up.
6. Specify filtering options for the backup plan, which are fairly straightforward and offer options to include and exclude file types, skip entire folders, and back up files that have changed since a specified date and time. After selecting an option, click Next.
7. Specify to use compression and the algorithm to use when compressing data. If using compression, specify and confirm a password and click Next.
8. Specify the data purging/retention options for the backup plan and click Next.
9. Provide information for scheduling the job to run once or have recurrence and click Next.
10. If necessary, provide any pre- or post-command-line options for the backup and click Next.
11. Provide any notification options, from mail server names to recipient addresses, and click Next.
12. Once the backup plan is saved, you can select it in the main backup window and click the Run Link to kick off the job immediately. If you specified a schedule you can also wait for

the next runtime for the job to run. You can monitor job progress in the Backup Plans tab of the main cloud backup window.

Vision Solutions Double-Take 7.0
Vision Solutions Inc.
visionsolutions.com

Physical server pricing starts at $1,995 per server. Virtual servers start at $259 per VM.

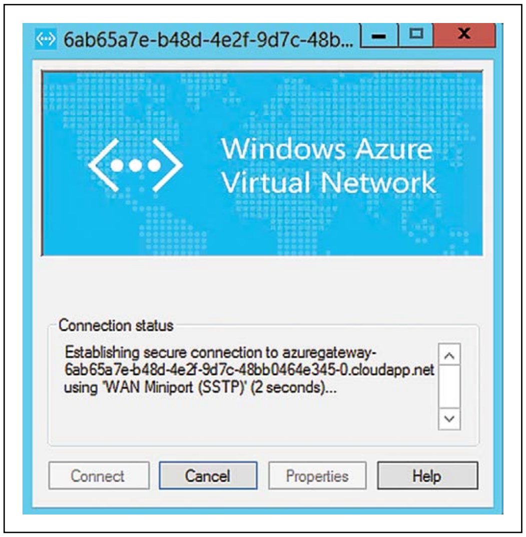
Double-Take 7.0 uses an interesting approach to backup as far as Windows Azure is concerned.

Double-Take 7.0 uses an interesting approach to backup as far as Windows Azure is concerned. To use this product with Windows Azure, you'll have to use a VPN connection to the Windows Azure cloud (see **Figure 4**). Once the VPN exists and the infrastructure is on your local network, you need a target to support replication between the on-premises site and the Windows Azure cloud. While Double-Take 7.0 does allow replication to Windows Azure, the solution works much more like site-to-site replication than a typical backup or disaster recovery solution.

To get stated with Double-Take, you'll need to configure the following in your Windows Azure portal:

- A local network with site-to-site VPN
- A VM at the same level of Windows as the server at your local site

Once these are configured, you're ready to configure the Double-Take application to push data to Windows Azure. At installation, be sure to choose the Move application, which is used for server migrations. On the local server, complete the following steps:



Establishing secure connection to azuregateway-6ab65a7e-b48d-4e2f-9d7c-48bb0464e345-0.cloudapp.net using 'WAN Miniport (SSTP)' (2 seconds)...

Figure 4. *When using Double-Take 7.0, you must connect the source server to a VPN in order to use Windows Azure as a target.*

1. From the Double-Take console, select Add Server and specify the name and credentials for your server.
2. Select the Getting Started page of the console and choose Double-Take Availability to begin configuring protection plans.
3. Select the task "Protect Files, folders, an application or an entire server."
4. Choose the source server from the list of Double-Take servers.
5. Select the workload for your protection job. This can include SQL Server, Files and Folders, Full Server, or Full Server to VMware ESX or Hyper-V. Use the Full Server ESX/Hyper-V job is used to migrate an entire server to a VM within Windows Azure.
6. Specify the Replication rules for the protection job. This lets you decide which files (or types of files) to include or exclude.

7. Because the destination was added to your network through a VPN connection to Windows Azure, it will appear locally. Without this, there's no way to see the destination server.
8. Choose the server in Windows Azure to use as your destination server.
9. Configure the options for the protection job including scheduling, compression, bandwidth limitations and a name for the job.
10. Review the configuration and correct any issues, and click Finish to save the job.

Once the configuration is complete and scheduled, the job can move the data to your new site in Windows Azure. Though the setup is more like a site-to-site configuration than a typical backup to a cloud target, this might fit your needs.

Using Windows Azure with your backup product is often a matter of digging into what you have and determining if there's available support.

Considerations for Choosing Cloud Backup Software

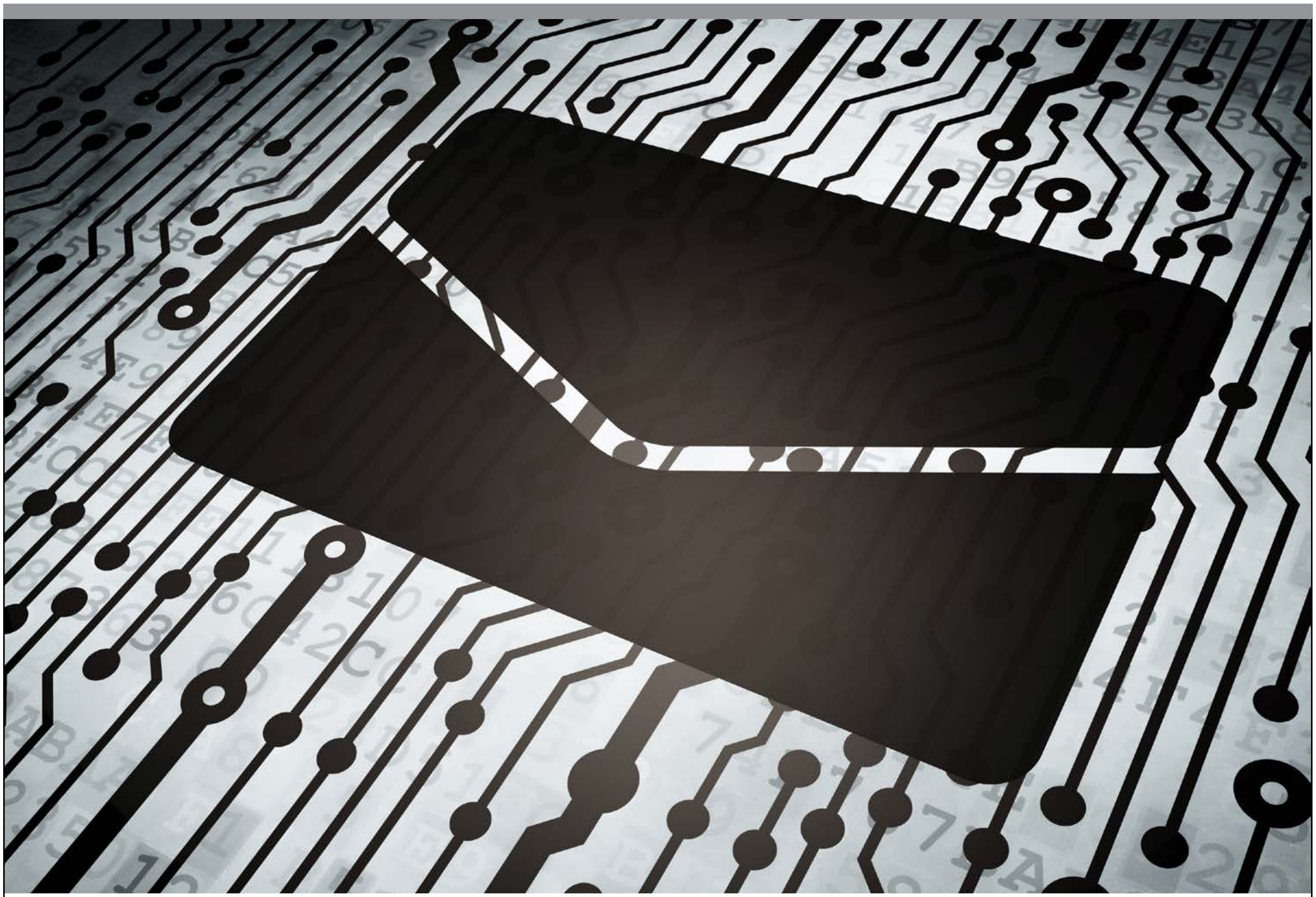
Each of these applications lets you connect to Windows Azure to store your data. Configuration for each was straightforward and didn't take too much to get working. Using Windows Azure with your backup product is often a matter of digging into what you have and determining if there's available support.

While all the products mentioned here are capable of working with Windows Azure, there are other solutions that haven't implemented these features yet. For example, Symantec Corp. is readying a version of its Storage Foundation High Availability for Windows and its Veritas Replicator disaster recovery for Windows Azure, which is in private beta now. If you use another product, check with your vendor to see if support is available or planned for a future release.

If your organization uses a smaller backup application, you might be able to get Windows Azure support from those vendors as well. Some solutions–such as those provided by Cloudberry Lab–are capable of working with many cloud providers, including Windows Azure.

To use these products with the Windows Azure service, you'll need an active subscription from Microsoft. Once your service is configured, you can enter your security information into any of the applications and begin backing up your data to the Windows Azure cloud. R

Derek Schauland has worked in technology for 15 years in everything from a help desk role to Windows systems administration. He has also worked as a freelance writer for the past 10 years. He can be reached at derek@derekschauland.com.



Software Simplifies Exchange Recovery

BY BRIEN M. POSEY

A flexible search interface makes Dell Recovery Manager for Exchange well-suited for e-discovery.

Litigation has become all too common in our society. When an organization is subpoenaed to furnish e-mails exchanged many years ago by employees, administrators are typically asked to perform the grueling task of locating and extracting the required data. Depending on the number of employees and volume of e-mails, finding specific threads is the equivalent of trying to find a needle in a haystack.

Recovery Manager for Exchange
$8 per user account or mailbox, minimum of 50 accounts/mailboxes
Dell Inc. | dell.com | 800-306-9329

Redmond MVP Most Valuable Product

RedmondRating

Installation: 20%	9.2*
Features: 20%	8.5
Ease of use: 20%	9.0
Administration: 20%	9.5
Documentation: 20%	9.5
Overall:	**9.4**

Key:
1: Virtually inoperable or nonexistent
5: Average, performs adequately
10: Exceptional

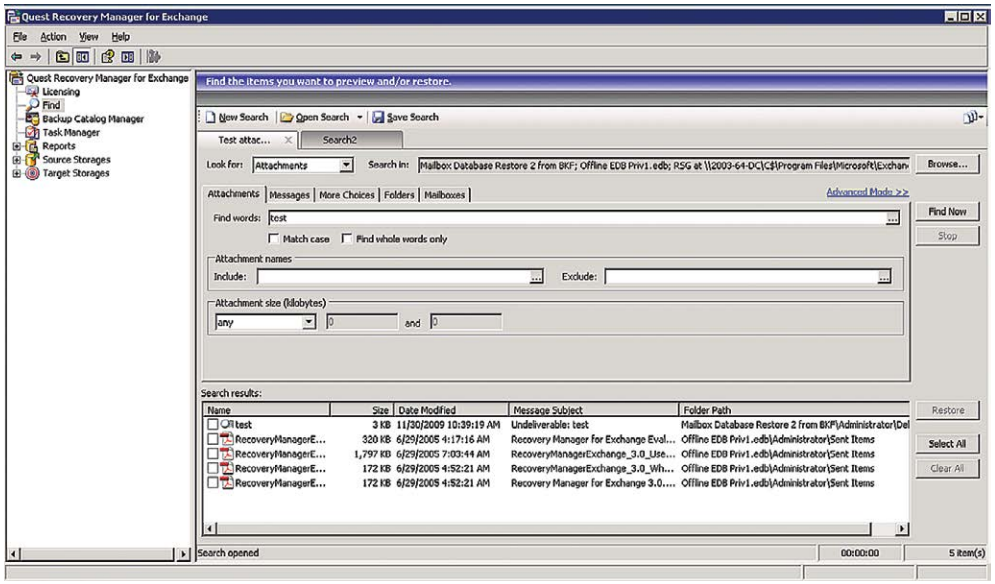
* Because I worked with a cloud-based version, there was no installation process. As such, my score for this category is based solely on the configuration options found within the UI.

Microsoft Exchange Server does contain native e-discovery tools, and in all fairness it has greatly improved over the years.

Microsoft Exchange Server does contain native e-discovery tools, and in all fairness it has greatly improved over the years, most notably with Exchange Server 2013. Even so, the native e-discovery capabilities in Exchange Server can be best described as basic, and are suitable primarily for use in smaller organizations. Thankfully, there are third-party products designed to make e-discovery more practical in larger organizations. One that's well suited for e-discovery is Recovery Manager for Exchange from Dell Inc. The product was developed and marketed by Quest Software; when Dell acquired Quest last year, Dell put its own brand on the portfolio.

Free Trial Version

Normally when I write a software review, I begin by working through the deployment process to get a feel for what's involved. In this case, however, Dell made available a free virtual trial. I write a lot of software reviews and occasionally I find problems with the product I'm reviewing. Whenever that happens, it can be difficult to determine whether the problem is related to a bug in the product or a problem with my configuration. Using a vendor's virtual lab takes the guesswork out of



Look for: Attachments
Search in: Mailbox Database Restore 2 from BKF; Offline EDB Priv1.edb; RSG at \\2003-64-DC\C$\Program Files\Microsoft\Exchan
Find words: test
☐ Match case ☐ Find whole words only
Attachment names
Include:
Exclude:
Attachment size (kilobytes)
any 0 and 0

Search results:

Name	Size	Date Modified	Message Subject	Folder Path
☐ test	3 KB	11/30/2009 10:39:19 AM	Undeliverable: test	Mailbox Database Restore 2 from BKF\Administrator\Del
☐ RecoveryManagerE...	320 KB	6/29/2005 4:17:16 AM	Recovery Manager for Exchange Eval...	Offline EDB Priv1.edb\Administrator\Sent Items
☐ RecoveryManagerE...	1,797 KB	6/29/2005 7:03:44 AM	RecoveryManagerExchange_3.0_Use...	Offline EDB Priv1.edb\Administrator\Sent Items
☐ RecoveryManagerE...	172 KB	6/29/2005 4:52:21 AM	RecoveryManagerExchange_3.0_Wh...	Offline EDB Priv1.edb\Administrator\Sent Items
☐ RecoveryManagerE...	172 KB	6/29/2005 4:52:21 AM	Recovery Manager for Exchange 3.0....	Offline EDB Priv1.edb\Administrator\Sent Items

Search opened 00:00:00 5 item(s)

Figure 1. *Recovery Manager for Exchange quickly rendered results.*

the review process because the virtual environment is presumably optimally configured.

Dell makes the virtual lab freely available to anyone who wants to try out Recovery Manager for Exchange. One word of caution before trying a virtual lab: Upon launching the virtual lab, the software does a few quick checks to make sure your computer meets the prerequisites. This includes checking things such as your browser version, Java version and Internet connectivity. My computer passed the prerequisite check with no problems, yet the lab environment never loaded. Instead I was presented with a blank screen. I eventually discovered that though the virtual lab checks to make sure you have Java installed, it doesn't verify Java is working. An error with Java on my computer kept the virtual lab from running. If you experience similar difficulties, visit the Java Web site at **bit.ly/fXTq5O**.

I want to emphasize the problem I experienced was related to an issue with my computer, not with Recovery Manager for Exchange. While it's true the online prerequisite check didn't detect the problem with Java, I can't fault Dell for the issue because the problem was related to a Web site, not to the Recovery Manager for Exchange software itself.

I was pleased to discover the Recovery Manager for Exchange interface was intuitive.

Interface and Documentation

Though I had previously found Quest's products a bit complex, I was pleased to discover the Recovery Manager for Exchange interface was intuitive, and using the software was a straightforward experience.

I initially chose to abandon the documentation for the purpose of my review, but I've always felt strongly that any commercial software application should include a comprehensive set of documentation, so I downloaded it.

The main documentation is a 236-page PDF; Dell offers a separate quick start guide as well. The way the instructions were presented reminded me of a Microsoft lab manual. The documentation could've benefited from the occasional screen capture, but it's still easy to follow because it's well written.

Performing E-Discovery

Because Recovery Manager for Exchange is an e-discovery product, I started out by performing a simple e-discovery task. I was curious to see how flexible the search interface was and how quickly it would render search results. Because I was working in a lab environment, the only thing I knew going in was that the software was licensed for 200 mailboxes. I had no idea how many mailboxes actually existed or what was in those mailboxes.

Because I really didn't know what to search for, I started out by taking a look at the UI. I noticed it lets you save searches or load saved searches. Because I wasn't sure what kind of data Dell had provided for testing purposes, I went ahead and loaded one of the saved searches. When I did, the results were displayed nearly instantaneously (see **Figure 1**, p. 11).

At first glance, the search interface appears to be used for performing simple date and keyword searches. However, a closer look reveals there are a number of different tabs that can be used for performing more advanced searches.

While I'm on the subject of tabs, take a look at the upper portion of the search interface. You'll notice there's a tab labeled Search2. The purpose of this is to let you perform multiple searches and keep the results of those searches accessible on-screen through a series of tabs. I love this feature because, in my experience, large-scale searches are rarely simple enough to be handled by a single search.

Another thing I found interesting about the search interface is Recovery Manager for Exchange lets you simultaneously search multiple data sources.

Search Sources

Another thing I found interesting about the search interface is Recovery Manager for Exchange lets you simultaneously search multiple data sources. Take a look at the "Search in" field in Figure 2. You can see the search is performed against a mailbox database restore from a BKF file, an offline Exchange Server database and a recovery storage group. Clicking the Browse button reveals a dialog box that allows you to select the individual locations you want to include in the search.

Recovery Manager for Exchange is quite diverse when it comes to data sources you can search. In the demo setup, Dell provided access to a mailbox database restore from a BKF file, an offline Exchange Server database, a recovery storage group, an online Exchange Server database, a Lotus Notes database and a series of PST files. In the search interface, Recovery Manager for Exchange not only provides a list of results, it shows from where each search result came.

I was especially impressed with the software including support for Lotus Notes. Incidentally, Dell used a BKF file to demonstrate the product's ability to search backups, but BKF files are far from being the only supported backup format. All of the major backup vendors are supported. Furthermore, the software even lets you run a comparison between an Exchange Server database and a backup so you can look for discrepancies.

Recovery Manager for Exchange makes it relatively easy to compile various data sources. You can see a list of the currently defined storage locations by clicking on the Source Storages container in the console tree. If you want to add more data sources, all you have to do is right-click on the Source Storages container and choose the Add Storages command from the shortcut menu. Doing so causes the software to launch an intuitive wizard that you can use to make the software aware of a data source. This wizard can access Exchange servers, Lotus Domino databases, PST files and backups. Some backup types are directly accessible, but the software can also interact with various backup applications such as Windows Backup, Microsoft System Center Data Protection Manager, Veritas Backup Exec and many others.

Unfortunately, SharePoint document libraries are not among the data sources supported. This is somewhat surprising considering the native Exchange Server 2013 e-discovery tools include native SharePoint search capabilities. My hope is that Dell will add SharePoint support in the next version.

The software includes several different reports. All of these reports are available through the Reports container.

Reporting Capabilities

The software includes several different reports: Completed Tasks, Completed Searches, Completed Restores, Previewed Messages and Previewed Attachments. All of these reports are available through the Reports container.

Selecting a container displays a list of the various reports available. It creates these reports automatically. The interface contains a series of search options you can use to locate a specific report. The reports can be exported to an Excel spreadsheet or to a PDF file.

The software doesn't appear to offer an option to create custom reports, but the built-in reports will likely be adequate for most organizations. R

Brien M. Posey is a seven-time Microsoft MVP with more than two decades of IT experience. He's written thousands of articles and several dozen books on a wide variety of IT topics. Visit his Web site at brienposey.com.