# BackupAssist v10 beta - Cloud Backup

BackupAssist v10 introduces Cloud Backup, a new backup type that allows you to use Amazon AWS or Microsoft Azure for your backup destination. This user guide is for the **BackupAssist v10 beta** build and explains how to use the new Cloud Backup option.

# The BackupAssist v10 beta builds

This beta build has been released so that users can test and try out the new Cloud Backup option. The feedback we get will help us improve this new feature and give users a chance to provide input.

The user interface and options are the same as BackupAssist v9, but when you create a backup job there will be a new option called Cloud Backup. The icons and buttons on the *Create a new backup job* screen have been redesigned for the new Cloud Backup option, as shown below.

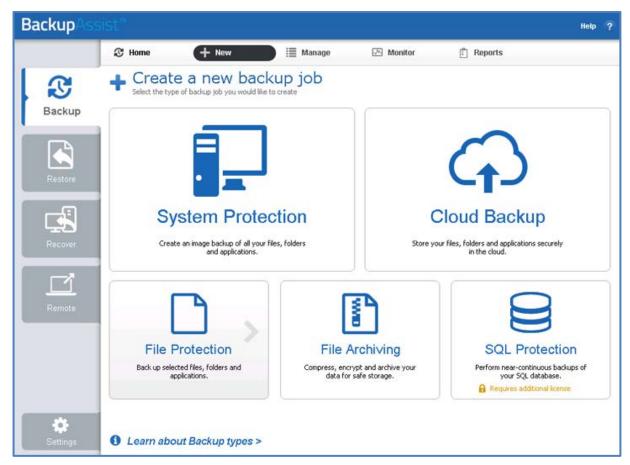


Figure 1: The new backup selection screen

Using and testing the BackupAssist v10 beta is as simple as selecting Cloud Backup when you create a backup job. You will however need to create an account with your chosen cloud provider.

**Note**: The BackupAssist v10 beta build should not be used to back up production servers.

# What is cloud storage

Cloud storage allows you to store data in remote data centers across the internet. This remote storage is provided as a service and is configured using a web interface.

# Advantages:

- Scalability your storage will scale with your needs and the total storage available can be increased by updating your subscription package.
- Affordability you do not need to purchase or maintain storage devices or storage servers.
- Security- your data is encrypted.
- Availability cloud computing uses data centers that have a better level of availability than could be achieved with your own local servers.

# How to create cloud storage

Before you can back up to a cloud destination, you will need create an account with Amazon AWS or Microsoft Azure and configure that account for cloud storage.

There are two steps to setting up cloud storage for BackupAssist.

### Step 1 - Create an account

To do this, go to the website of your chosen cloud provider. Setting up an account involves providing business information and payment details.

To create an account:

- For Amazon AWS, start here <u>https://aws.amazon.com/</u>
- For Microsoft AZURE, start here <u>https://azure.microsoft.com/</u>

Information about free accounts:

- For Amazon AWS, start here <u>https://aws.amazon.com/s3/</u>
- For Microsoft AZURE, start here <u>https://azure.microsoft.com/en-us/free/</u>

### Step 2 – Storage configuration

Once you have your accounts set up, you can configure the cloud storage.

For AZURE, this will mean configuring a storage account.

You can have multiple storage accounts and the process is documented by Microsoft. You can start <u>here</u>.

For AWS, this will mean configuring a user.

You can create multiple users and the process is documented by Amazon. You can start here.

**Note**: Microsoft Azure uses containers and Amazon (AWS) uses buckets to store data. You do not need to create buckets or containers. BackupAssist will do this when it creates the backup.

# Getting storage information for BackupAssist

Once you have the cloud storage set up, BackupAssist will need the access keys that the cloud service provider uses to allow access to your cloud storage. These keys are entered into BackupAssist when you create the Cloud Backup job. This section explains how to get these keys for AZURE and Amazon AWS.

# **AZURE storage keys**

The Microsoft AZURE cloud service allows you to create storage accounts that can be used as backup destinations.

To get the storage keys:

1. Open the AZURE Dashboard.

The Dashboard lists the storage accounts that you have created in the All resources section.

2. Select the Storage Account that you want to use.

The Dashboard will reload for the selected Storage Account.

3. Select Access Keys from the Settings menu.

The Dashboard will show the keys available for the storage account that you selected. Microsoft recommends regenerating new keys regularly and provides two key fields so that you can create a new key, while still having the old key active.

4. Use the **copy** button to take a copy of key that you want to use.

These keys will be needed when you create the backup job. You can perform these steps when creating the backup job, or copy the keys to a file so they can be used later.

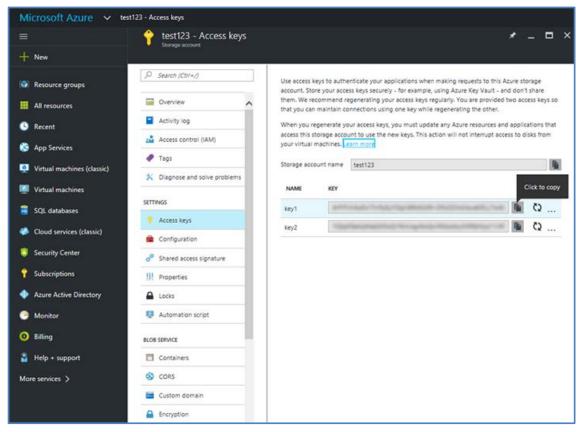


Figure 2: AZURE dashboard - getting storage keys

# Amazon Web Services (AWS) S3 storage keys

Amazon AWS provides cloud storage solutions, one of which is S3. S3 is an easy to use storage solution that can be used as a backup destination. Access to AWS S3 storage is managed using keys, which must be entered into BackupAssist when you create a backup job that uses AWS as a destination.

Amazon has an excellent guide that can be followed to get a copy of the access key here.

To get the access keys:

- 1. Open the AWS Management Console.
- 2. Select the **Services** drop down menu from the top navigation bar.
- 3. Select IAM (Identity & Access Manager).
- 4. Under IAM Resources, select **Users** from the left menu.

These are the users you created for your S3 storage. You could create a user just for BackupAssist.

**Note**: This user must have at least **PowerUserAccess** permission. This is a Policy assigned under the Permissions tab in the AWS web console.

#### 5. Select the user's **Security Credentials** tab.

This will show you the user's Access Key ID, but a secret access key is also required.

#### 6. Select Create Access Key.

This will generate a pop up with the Access Key ID and the Secret Access Key. The Secret key is unique and will not be saved in the console.

#### 7. Select Download Credentials.

These keys will be needed when you create the backup job. You can perform these steps when creating the backup job, or copy the keys to a file so they can be used later.

Dashboard	IAM > Users > Rick				
	* Summary				
Detailis Groups Users Roles	Has Password: No Groups (for this user): 1 Path: /		216562004669 user Rex 14:24 UTC+1100		
Policies Identity Providers	Groups Permissions Secur	ity Credentials	Create Access Key	1	
Account Settings Credential Report	Access Keys Use access keys to make secure REST or Query proto			ey's with anyone.	
Encryption Keys	Learn more about Access Keys Create Access Key		You can manage and recreate these credentials any time.     Hide User Security Credentials    Rick		
	Access Key ID	Create 2016-1	Access Key ID Secret Access Key	Last Used Region	Status
	Sign-In Credentials	me RokDwyer	Close Download Credentials		
	Passwo Last Us				
	Multi-Factor Authenticati Devi		Manage MFA Device		
	Signing Certificat	les None	Manage Signing Cert	ificates	
	SSH keys for AWS CodeComm	-			

Figure 3: Amazon AWS Console - getting access keys

# Creating a cloud backup job

Many of these steps are the same as those for other backup types. BackupAssist's v9 <u>documentation</u> can be referred to for configuration options such as Backup User Identify and the Settings tab options.

Launch BackupAssist and follow the steps outlined below:

- 1. Select the **Backup** tab
- 2. Select Create a new backup Job
- 3. Select Cloud Backup

If this is the first time you have created a backup job, you will be asked to provide a *Backup user identity* if one has not been defined.



#### 4. Selections

Select the data and applications that you would like to back up.

	C Home	⊢ New 📄 🗎 Manage	🕅 Mor	nitor [	] Reports		
Backup	ဂ္ဂ Cloud Bad	what do you want to back	up?				
	Usier Identity	Or Refresh	Add netwo	rk path 🕂 Estima	te size		Q. Key
	Selections	⊕-□ > Local Disk (C:)     ⊕-□ > Storage (F:)		lame	Туре	Size	Last modified
store	Destination media Schedule	SRECYCLE.BIN     SRECYCLE.BIN     Badkup Destination     DOCUMENTATION     DOCUMENTATION     File Storage		Constant Constan	1		
	Set up destination	P P P P P P P P P P P P P P P P P	8	<ul> <li>Marketing</li> <li>Public Files</li> <li>Friday.zip</li> </ul>	WinRAR ZIP	3.74 GB	6/24/2016 3:48:
		Work on hand (E:)					
	Prepare media						
1	Name your backup						
note	Shot Mepa.						
¢				1.	101		

Figure 4: Cloud backup – data selection screen

# 5. Destination media

Use this step to select the cloud destination that you want to back your data up to. This step's name will change to the cloud service selected, when you click Next.

Backup Help Reports C Home + New ) i≣ Manage Monitor Cloud Backup Wizard  $\mathbb{S}$ Where do you want your backup? Backup Cloud Selections **Destination media** 0 < Back Next > Cancel

Select Amazon or Azure, and click Next.

Figure 5: System Protection – Destination media

6. Schedule

Use this step to select when you would like the backup job to run and how long you would like the backup to be retained for.

There are two schemes to choose from:

- **Basic** a daily backup from Monday to Friday. Each day, the backup will write over the previous week's backup for that day.
- **Grandfather-father-son** daily backups with weekly, monthly and annual archive backups. The weekly backups are retained for a month and the monthly backups for a year.

To set up the schedule:

- 1. Select a scheme
- 2. Select the time you would like the backup job to run
- 3. Select Next.

To learn more about scheduling options and customizations, see the **Backup tab user guide**.

# 7. Set up destination

This step configures the cloud backup service selected in step 5. There are different settings for Amazon S3 and Microsoft Azure.

#### Amazon S3 bucket settings

C	Cloud Bac	kup Wizard			
Backup		Amazon S3 bucket	settings		
	User Intentity				
	Selections	BackupAssist will creat	te a new bucket using the details prov	ided below.	
	Amazon	Amazon S3 bucket:	-		
		Amazon S3 Region:	us-east-1		
	Schedule		US East (N. Virginia)		
	Set up destination	Access Key ID:			
Recover	Notifications	Secret Access Key:	[		
	Prepara media.	Encryption Password:			
۲ <u>۲</u>	Name your backup	Confirm Encryption			
		Password:			
	Nextereste		Check destination		
		A bucket must not be s	hared between backup jobs or mach	nes.	

#### Amazon S3 bucket

Enter a name for your S3 bucket. BackupAssist will use this name to create the bucket. Provide a different name for each job, because a different bucket must be used by each backup job. This name must follow the conventions explained <u>here</u>

### Amazon S3 Region

Select the region for the data centre where you want your cloud storage to be based.

• Access Key ID

Enter the Access Key ID provided, as explained on page 4 of this guide.

• Secret Access Key

Enter the Secret Access Key ID provided, as explained on page 4 of this guide.

• Encryption Password

Cloud Backup uses encryption to protect your data. Enter and confirm an encryption password. This password will be needed if you perform a restore.

**Note:** It is important that you keep a copy of your password in a safe place, as <u>we cannot</u> retrieve passwords if they are lost or forgotten.

### Check destination

Use the Test connection button to check that the information supplied allows BackupAssist to connect to the cloud storage.

# **Azure container settings**

BackupAss	ist"					Help ?	
	S Home +	New I	Manage	🗷 Monitor	🗂 Reports		
Backup	Cloud Backup Wizard Azure container settings						
Restore Recover Recover Remote	Liber (denity Selections Azure Schedule Set up destination Notifications Proposition and the Name your backup	BackupAssistw Container: Account Name: Access Key: Encryption Pas Confirm Encryp Password:	sword:	ainer using the details pro	vided below.		
Settings			st not be shared bet ow to set up y	ween backup jobs or mad	hines.	Gancel	

Fill in the following fields for the Azure container:

#### Container

Enter a name for your Azure container. BackupAssist will use this name to create the container. Provide a different name for each job, as a different container must be used by each backup job. This name must follow the conventions explained <u>here</u>

### Account Name

Enter the name of the Storage Account that you are backing up to.

• Access Key

Enter the Access Key ID provided, as explained on page 3 of this guide.

• Encryption Password

Cloud Backup uses encryption to protect your data. Enter and confirm an encryption password. This password will be needed if you perform a restore.

**Note:** It is important that you keep a copy of your password in a safe place, as <u>we cannot</u> <u>retrieve</u> passwords if they are lost or forgotten.

#### Check destination

Use the Test connection button to check that the information supplied allows BackupAssist to connect to the cloud storage.

### 8. Notifications

Once a backup job has completed, BackupAssist can send an email to inform selected recipients of the result. This email notification can be enabled during the creation of a backup job, if the mail server has been configured. To learn more, see the <u>Backup tab user guide</u>.

To enable email notifications:

- a. Select, Add an email report notification.
- b. Enter recipients into the Send reports to this email address field.
- c. Enter recipients into the **Also send reports to this email address** field. You can then select the condition under which the email should be sent, using the drop-down box.
- 9. Name your backup

Provide a name for your backup job, and click **Finish**.

# Restoring from a cloud backup

Performing restores is easy and an important part of trying out the new Cloud Backup solution. To perform a restore, simply select the Restore tab and proceed as you would for a BackupAssist v9 restore.

BackupAss					Help ?		
	🕞 Home 🕺 🗙 Tools	🗂 Reports					
	Restore ▶Loc	al and Network Fi	les	Qs	earch		
S	Restore > Loc	4		tegrated Restore Console			- 0 X
Backup	Files on C: 3 badup(s)	Backup details					
	Internet Line Midney Day		edia: 👝 1 actiup location: Tue	luesday solau			
	Last 7 days Last 30 days All Job	1. What to restore	actual accession in the				
Restore	200	E-Cocal Disk (C:)		Name	Type 3ML Document	Size 2.88 kB	Last mod 5/16/201
Treatore	30b(1) Account35058	🖻 🗌 🤪 Administrator		H1T2.aml	XML Document	24.75 kB	3/31/201
		B- C Desitop	rce	H1T3.xml	XML Document	24.74 is	3/31/201
		8-0 <b>0</b> 1 -0 <b>0</b> 1-1					
Recover				Backup	Assist		
-		5 U J 3		Password required	Backup	losist*	
				The backup you are trying to rest	ore is password protec	ted.	
and the second second				Password:			
Remote							
				Abort	Bety	Skip	2
Hyper-V		2. Where to restore					
		To specific location v	C:\Temp\				Browse_
			Overwrite existing file	es v			
*			Bestore NTFS se				
Settings	Discover Backups		Take ownership	of restored files (as DEV-2012R2VAdm		tore	Close
	·				P He		COTO

Figure 6: Cloud Backup restore

When you start the restore process, you will be prompted to enter the password used to encrypt the cloud backup.