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.

Microsoft Azure 🐱 tes	t123 - Access keys		
=	test123 - Access keys	* _ =	×
+ New	And Restance of		
Resource groups	P Search (Ctri+/)	Use access keys to authenticate your applications when making requests to this Azure storage	
All resources	Cverview	them. We recommend regenerating your access keys requiring taket key want and other inner them. We recommend regenerating your access keys requiring. You are provided two access keys so that you can maintain connections using one key while regenerating the other.	
Recent	Activity log	When you regenerate your access keys, you must update any Azure resources and applications that	
App Services	Access control (IAM)	access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. earn more	
	🥒 Tags	Storage account name test123	
Virtual machines (classic)	X Diagnose and solve problems		
Virtual machines	CETTING.	NAME KEY Click to copy	
🥫 SQL databases	Access land	key1 🕅 🖏	
Cloud services (classic)	Access keys	key2 📓 🗘	
Security Center	Contiguration e ^O Shared access signature		
Subscriptions	11 Properties		
Azure Active Directory	🖨 Locks		
Monitor	Automation script		
0 Billing	BLOB SERVICE		
🛓 Help + support	Containers		
More services >	⊗ cors		
	Custom domain		
	Encryption		

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.

	* - Summary				
votalits votope sers coles	User ARN: Has Password. Groups (for this user): Path: Creation Time:	am avs.lom Ne 1 2016-10-18	214062004689 unior Rox 14.34 UTC=1106		
antity Providers	Groups Permissions Security	Credentiats	Create Access Key	-	
Account settings Credential Report	Access Keys One access keys to make secure REST or Query proto Liams more about Access Keys		Your access key has been created successfully. This is the last time these User security credentials will be available for download. You can manage and recreate these credentials any time.	eys with anyone.	
arijinan waya	Cinate Access Key Access Key ID	Creats 2016-1	Hide User Security Credemats Rick Access Key D: Bernel Access Key	Last Used Region	Status Active
	Sign-In Crodontais User Name Password Last Used	RickDwyer Na NGA	Close Download Credentiats Manage Password		
	Mutti-Foctor Authentication Device	No	Manage MFA Device	a)	
	Signing Certificates	hone	Manage Signing Ce	tificates.	

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.

BackupAss	iist!"							Help ?
	🕄 Home	- New	🗮 Manage	⊠ N	Ionitor	🗂 Reports		
Backup	Cloud Bac	Kup Wiza What do y	r <mark>d</mark> ou want to back	up?				
	Dair Idently	C Refresh	Check selections	Add net	vork path 🕂 Estim	ate size		Q, Key
	Selections		al Disk (C:) age (F:)		Name	Туре	Size	Last modified
Restore	Destloation media		SRECYCLE.BIN Backup Destination		Accounting			
	Schedule		DOCUMENTATION File Storage Flare backups		Occumentation Of Marketing	n		
	Set up destination		Restore Destination Skins		Public Files	WinRAR ZIP	3.74 GB	6/24/2016 3:48:0
Recover	Notifications	⊕- ⊡ ⊘ ⊕- ⊡ ⊋ Wor	System Volume Information k on hand (E:)	n				
	Prepare media							
	Name your backup							
Remote	11427-2040-0							
_								
*					•	m		1.1
Settings					(< Back	<u>N</u> ext >	

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 C Home + New 🗐 Manage Monitor Reports ← Cloud Backup Wizard 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

	Cloud Bar	kun Wizard			
Backup		Amazon S3 bucket	settings		
	Alter at the other	Backun Accist will creat	e a new bucket using the details grow	ided below	
	Selections	backup Assist mill a co	e a new bucket using the details prov		
index.	Amazon	Amazon S3 bucket:	[
	Schedule	Amazon S3 Region:	US East (N. Virginia)		
-£1	Set up destination	Access March 19	6		
	Notifications	Access Key ID: Secret Access Key:			_
7		Encryption Password:			
	Name your backup	Password:			
	Notified		Check destination		
	1				
		A bucket must not be s	hared between backup jobs or machi	nes.	
		and the second second second second second			

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 ?
	③ Home 🕂 New 🗎 M	anage 🕑 Monitor	🗊 Reports
Backup	Cloud Backup Wizard	ettings	
Restore Recover	Selections Azure Schedule Container: Set up destination Mobilizations Figure Source Setup Figure Setup F	ate a new container using the details pro	ovided below.
Settings	A container must not	be shared between backup jobs or mar to set up your cloud >	chines.

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.

Backup					Help ?		
	Restore	Reports	loc	0	wareh		
G	Restore FLOC		1 Pos	Integrated Restore Console			= 0 X
Backup	Files on C: 3 tedup(c)	Backup details Job Job(1) Date: 10/26/2016 1:29 PM	edia 🔉 💩 acikup location: Tr	Tuenday Jeoday			
	Job	1. What to restore					
Restore	30b 30b(1) Account/350/8	B Joad Disk (Cr) B Joad Disk (Cr) B Joad Administrator B Joad Desitop B Joad Chylson B Joad Chylson B Joad Chylson	rce	Name HITI-NoSetup.xml MitHIT2.xml MitHIT3.xml	Type XML Document XML Document XML Document	528 2.8818 24.7518 24.7418	Last mod 5/16/201 3/31/201 3/31/201
Record		2		Backup	Assist		
-		1 L L 3		Password required	Backup	isset"	
Remote				The backup you are trying to rest Password:	ore is password protec	ted.	(5)
Hyper-V		2. Where to restore					
		To specific location	C:\Temp\				Browse_
			Overwrite existing	filez 🗸 🗸			
Settings	Discover Backups		Restore NTFS Take ownersh	security attributes ip of restored files (as DEV-2012R2VAdm	nistrator)	store	Close

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.