

Configuring S3 Compatible Cloud Storage

For use with

Backup Exec 16 Feature Pack 2

Contents

S3 Compatible Cloud Storage with Backup Exec 16 FP2	2
Configuring S3 Compatible Cloud Storage with Backup Exec 16 FP2	2
S3 Cloud Pre-Configuration Requirements	3
Creating a Cloud Instance for S3 Compatible Cloud	3
Creating a Cloud Storage Device for S3 Compatible Cloud.....	4

S3 Compatible Cloud Storage with Backup Exec 16 FP2

Backup Exec 16 Feature Pack 2 (Licensed Software) provides S3 compatible cloud storage functionality. Customers can use their own S3 compatible cloud implementation with Backup Exec. When the configuration process is complete, you can create a storage device within the Backup Exec console that can access most S3 compatible cloud environments. S3 compatible environments that are listed in the Backup Exec 16 Hardware Compatibility are considered “**Supported Configurations**”. S3 compatible communications have not been tested in all private cloud environments and may not work in some cases. S3 compatible environments that are not specifically listed in the [Backup Exec 16 Hardware Compatibility List](#) are considered Alternative Configurations. The Backup Exec 16 Hardware Compatibility List defines Alternative Configurations as:

Alternative Configurations: Our Licensed Software is designed to interoperate with many types of systems, applications, and hardware. Sometimes a customer may choose to use our Licensed Software in an "Alternative Configuration", namely, an environment that has not been validated, approved or verified to operate with our Licensed Software or which does not support such Licensed Software or only supports limited functionality. We do not support Alternative Configurations and Support Services do not include supporting Licensed Software in an Alternative Configuration. You are solely responsible for your use of Licensed Software in an Alternative Configuration. A Supported Configuration might be converted into an Alternative Configuration if a vendor modifies one of its components that is part of the original Supported Configuration. As a consequence, your Licensed Software would then be operating in an Alternative Configuration which would not be supported under Support Services. If you experience a problem with the Licensed Software in an Alternative Configuration or if your issue deals with script that was not developed by Veritas or an authorized consulting partner, even though we have no obligation to support such usage, we may ask you to reproduce the problem in a Supported Configuration environment. If the problem can be replicated in a Supported Configuration, we will investigate the problem in that Supported Configuration and attempt to resolve it in the Supported Configuration. If the problem cannot be replicated in a Supported Configuration, then we may elect not to investigate the problem. Please note, in general, we have no obligation to support problems that cannot be replicated in a Supported Configuration.

Configuring S3 Compatible Cloud Storage with Backup Exec 16 FP2

Configuring S3 compatible cloud storage using the S3 Cloud Connector in Backup Exec 16 FP2 is a two-step process:

1. **Create a cloud instance for your cloud** – requires pre-configuration of a user account and buckets in the cloud environment. The cloud location and configuration parameters must be provided to the Backup Exec server by configuring a cloud instance using the Backup Exec Command Line Interface (BEMCLI) (see [Creating a Cloud Instance for S3 Compatible Cloud](#)).

2. **Create a cloud storage device** – in the Backup Exec console by using the storage device configuration wizard and providing the account credentials that can access the S3 compatible cloud location.

S3 Cloud Pre-Configuration Requirements

In the cloud environment, create an account for Backup Exec read/write access. The cloud account credentials, known as the server access key ID and secret access key, must be provided in the Backup Exec console to create the storage device.

The cloud environment must also have buckets configured for Backup Exec use. Buckets represent a logical unit of storage in a cloud environment. As a best practice, create specific buckets to use exclusively with Backup Exec. Each Backup Exec cloud storage device must use a different bucket. Do not use the same bucket for multiple cloud storage devices even if these devices are configured on different Backup Exec servers.

Bucket names must meet the following requirements:

- Can contain lowercase letters, numbers, and dashes (or hyphens)
- Cannot begin with a dash (or a hyphen)

Bucket names that do not comply with the bucket naming convention will not be displayed in the Backup Exec console during storage device configuration.

If SSL mode communications will be used, the cloud server must have a Certificate Authority (CA)-signed certificate. SSL mode communications will fail if the cloud environment does not have a CA-signed certificate. SSL mode communications can be either enabled or disabled when configuring the cloud instance using BEMCLI. If SSL mode is disabled, a CA-signed certificate is not required.

Creating a Cloud Instance for S3 Compatible Cloud

To create a custom cloud instance for an S3 compatible cloud storage server use the BEMCLI command “New-BECloudInstance”. See Technical [Article 000114986](#) for details and examples for the command BECloudInstance and Technical [Article 000116189](#) for the BEMCLI help file.

To run BEMCLI on the computer on which Backup Exec is installed you can either

- Go to the taskbar, click Start > All Programs > Veritas Backup Exec > Backup Exec Management Command Line Interface

or

- Launch PowerShell, and then type Import-Module BEMCLI.

From the BEMCLI command line interface run the New-BECloudInstance command with the required parameters, for example:

```
New-BECloudInstance -Name "CloudInstance0001" -Provider "generic-s3" -  
ServiceHost "s3.yourendpoint.com" -SslMode "Disabled" -HttpPort 80 -  
HttpsPort 443
```

Mandatory Parameters:

- **Name:** Name of the new cloud instance. Cloud instance name must match BE naming requirement.
 - Instance names can contain letters, numbers, and dashes (or hyphens).
 - Instance names cannot begin with a dash (or a hyphen).
- **Provider:** Specifies the provider name of the cloud instance. For generic s3 the provider name is 'generic-s3'.
- **ServiceHost:** Specifies the service host of the cloud instance. ServiceHost should be unique for each cloud instance that is created on the Backup Exec server.
- **SslMode:** Specifies the SSL mode that Backup Exec will use for communication with the cloud storage server. The valid values are:
 - Disabled – Do not use SSL.
 - AuthenticationOnly – use SSL for authentication only.
 - Full – use SSL for authentication and data transfer also.

Note: Backup Exec supports only Certificate Authority (CA)-signed certificates while it communicates with cloud storage in the SSL mode. Ensure that the cloud server has CA-signed certificate. If it does not have the CA-signed certificate, data transfer between Backup Exec and cloud provider may fail in the SSL mode. Users may choose to opt out of SSL and set SSLMode as Disabled.

To confirm the command completed successfully, run the BEMCLI command "Get-BECloudInstance". The parameters of the newly configured cloud instance will be displayed. Ensure that the ServiceHost points to the correct S3 compatible cloud implementation, the provider name is accurate and the SSL mode is set correctly. If any parameters are not correct, rerun the New-BECloudInstance command with the corrected parameters.

Creating a Cloud Storage Device for S3 Compatible Cloud

To configure a storage device for an S3 compatible cloud in Backup Exec:

1. On the Storage tab, in the Configure group, click Configure Cloud Storage.
2. Click Cloud storage, and then click Next.
3. Enter a name and description for the cloud storage device, and then click Next.
4. From the list of cloud storage providers, select S3, and then click Next.
5. From the Cloud Storage drop-down, select the name of the instance created with BEMCLI
6. Click Add/Edit next to the Logon account field.
7. On the Logon Account Selection dialog box, click Add.
8. On the Add Logon Credentials dialog box, do the following:
 - In the User name field, type the cloud account access key ID.
 - In the Password field, type the cloud account secret access key.
 - In the Confirm password field, type the cloud account secret access key again.
 - In the Account name field, type a name for this logon account.

The Backup Exec user interface displays this name as the cloud storage device name in all storage device options lists.

9. Click OK twice.
10. Select the cloud logon account that you created in step 8, and then click Next.
11. Select a bucket from the list of buckets that are associated with the server name and the logon account details you provided in earlier screens, and then click Next.
12. Specify how many write operations can run at the same time on this cloud storage device, and then click Next.

This setting determines the number of jobs that can run at the same time on this device. The suitable value for this setting may vary depending on your environment and the bandwidth to the cloud storage. You may choose the default value.
13. Review the configuration summary, and then click Finish.

Backup Exec creates a cloud storage device. **You must restart Backup Exec services to bring the new device online.**
14. In the window that prompts you to restart the Backup Exec services, click Yes.

After services restart, Backup Exec displays the new cloud storage location in the All Storage list.

If the S3 compatible cloud environment is not displayed in the Backup Exec storage device configuration wizard or console, use BEMCLI to ensure the parameters for the cloud instance are correct.

Note: S3 compatible communications have not been tested in all private cloud environments and may not work in some cases. S3 compatible environments that are not specifically listed in the [Backup Exec 16 Hardware Compatibility List](#) are considered Alternative Configurations (see S3 Compatible Cloud Storage with Backup Exec 16 FP2).

Once the S3 compatible cloud storage device is configured in Backup Exec, you can target backup, restore and duplicate jobs to the cloud server. As a best practice, test backup and restore operations should be completed before running regularly scheduled jobs.

Backup Exec Data lifecycle Management will automatically delete expired sets from the cloud server.