EonStor GS/GSe Cloud-Integrated Feature Guide

Application Note

Version 1.0 (October 2016)

Abstract:

This document introduces key concepts of the cloud-integrated functions on EonStor GS/GSe and demonstrates the detailed configuration process with the EonOne.

Legal Information

All Infortrend products, including the product customers have purchased from Infortrend, will be subject to the latest Standard Warranty Policy available on the Infortrend website:

http://www.infortrend.com/global/Support/Warranty

Infortrend may from time to time modify, update or upgrade the software, firmware or any accompanying user documentation without any prior notice. Infortrend will provide access to these new software, firmware or documentation releases from certain download sections of our website or through our service partners. Customer will be responsible for maintaining updated version of the software, firmware or other documentation by downloading or obtaining from Infortrend, and installing designated updated code, including but not limited to firmware, microcode, basic input/out system code, utility programs, device drivers, and diagnostics delivered with Infortrend product.

Before installing any software, applications or components provided by a third party, customer should ensure that they are compatible and interoperable with Infortrend product by checking in advance with Infortrend. Customer is solely responsible for ensuring the compatibility and interoperability of the third party's products with Infortrend product. Customer is further solely responsible for ensuring its systems, software, and data are adequately backed up as a precaution against possible failures, alternation, or loss.

For any questions of hardware/ software compatibility, and the update/ upgrade code, customer should contact Infortrend sales representative or technical support for assistance.

To the extent permitted by applicable laws, Infortrend will NOT be responsible for any interoperability or compatibility issues that may arise when (1) products, software, or options not certified and supported by Infortrend are used; (2) configurations not certified and supported by Infortrend are used; (3) parts intended for one system are installed in another system of different make or model.

Trademarks

Infortrend, the Infortrend logo, EonOne and EonStor are registered trademarks of Infortrend Technology, Inc. Other names prefixed with "IFT" and "GS" are trademarks of Infortrend Technology, Inc.

All other names, brands, products or services are trademarks or registered trademarks of their respective owners.

Contact Information

Customer Support

Contact your system vendor or visit the following support site.

http://www.infortrend.com/global/Support/Support

Headquarter (Asia / Taiwan)

Infortrend Technology, Inc.

8F., No.102, Sec. 3, Jhongshan Rd., Jhonghe Dist., New Taipei City 23544, Taiwan
Tel: +886-2-2226-0126 Fax: +886-2-2226-0020 Email, Technical Support, Website

Middle East Infortrend Sales Representative

Email, Technical Support, Website

India Infortrend Sales Representative

Email, Technical Support, Website

Oceania Infortrend Sales Representative

Email, Technical Support, Website

Japan

Infortrend Japan, Inc.

6F Okayasu Bldg., 1-7-14 Shibaura, Minato-Ku, Tokyo, 105-0023 Japan
Tel: +81-3-5730-6551 Fax: +81-3-5730-6552 Email, Technical Support, Website

Americas

Infortrend Corporation

435 Lakeside Dr. Sunnyvale, CA. 94085, USA
Tel: +1-408-988-5088 Fax: +1-408-988-6288 Email, Technical Support, Website

China

Infortrend Technology, Ltd.

Room 403,Block D, Ocean International Center, Dis. Chaoyang, Beijing, China
Tel: +86-10-6310-6168 Fax: +86-10-59648252 Email, Technical Support, Website

Infortrend 华南办事处

上海市浦东新区塘桥路 180 号 202 室

Tel: +86-10-6310-6168 / 8586-6916/ 8586-1801 Fax: +86-10-59648252
Email, Technical Support, Website

Infortrend 华东办事处

广州市天河区天河北路 620 号瑞安创逸 T1 栋 3111 室

Tel: +86-10-6310-6168 / 8586-6916/ 8586-1801 Fax: +86-10-59648252
Email, Technical Support, Website

Infortrend 西南办事处

成都市高新区天华一路 99 号天府软件园 B3 栋四楼 V04 室

Tel: +86-10-6310-6168 / 8586-6916/ 8586-1801 Fax: +86-10-59648252
Email, Technical Support, Website

Infortrend 南京办事处

江苏省南京市雨花台区软件大道 119 号丰盛商汇 5 栋 102

Tel: +86-10-6310-6168 / 8586-6916/ 8586-1801 Fax: +86-10-59648252
Email, Technical Support, Website

Europe (EMEA)

Infortrend Europe LTD.

5 Ringway Centre, Edison Road, Basingstoke, Hampshire, RG21 6YH, UK
Tel: +44-1256-305-220 Fax: +44-1256-305-221 Email, Technical Support, Website

Czech Republic Infortrend Sales Representative

Email, Technical Support, Website

France Infortrend Sales Representative

Email, Technical Support, Website

Germany/ Infortrend Deutschland GmbH

Email, Technical Support, Website

Italy Infortrend Sales Representative

Email, Technical Support, Website

Poland Infortrend Sales Representative

Email, Technical Support, Website

Spain / Portugal Infortrend Sales Representative

Email, Technical Support, Website

Table of Contents

Preface

The purpose of this application note is to provide users with knowledge on the working mechanisms and steps related to the use of the cloud gateway features with the EonStSor GS/GSe storage systems. Infortrend continues to develop the best storage solutions to fulfill customers' expectations and requirements and periodically releases information about hard- and software updates online. Therefore, Infortrend recommends users check the official website for latest news, the customer support system for latest firmware and software, or, in the case of a product malfunction or a feature that is not working as intended, contact an Infortrend technical support professional.

Audience

This Application Note is intended for Infortrend customers, partners, and employees who are installing and/or configuring the EonStor GS/GSe systems.

What's in This Guide

This guide contains the following topics:

"About the cloud gateway features" explains the mechanisms of the cloud-integrated functions.

"Using the cloud gateway features" demonstrates how to use the cloud-integrated functions on the EonOne software.

"Disaster Recovery" shows how to retrieve data back from cloud service providers to EonStor GS/GSe storage devices.

What You Should Know Before Reading

This Application Note assumes that you are familiar with basic server, storage, and networking concepts and configurations.

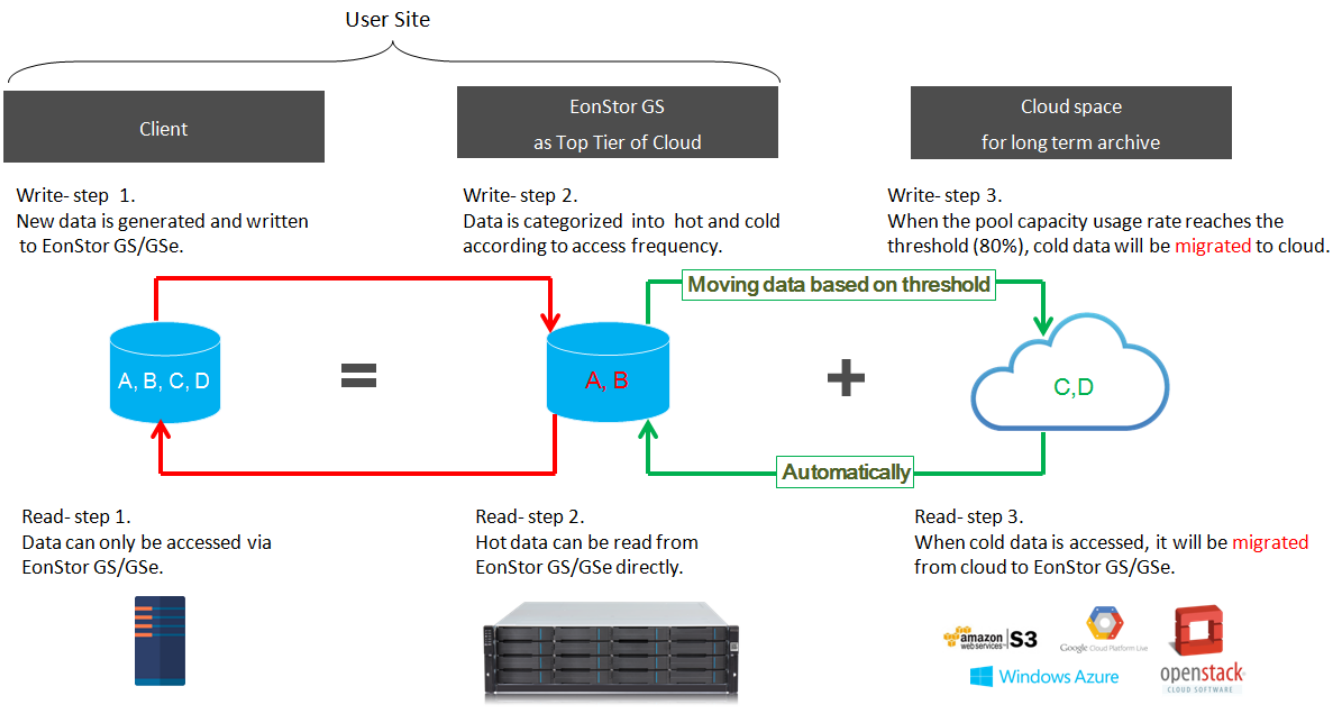
About the Cloud Gateway Features

By using the cloud gateway features provided with EonStor GS/GSe storage devices, users will be able to access their own cloud services by setting volumes to **Cloud Tiering** mode or **Cloud Caching** mode, which makes a supported cloud storage service either as **an extra storage capacity provider** or **a remote backup site**. Moreover, EonStor GS/GSe allows users to back up the snapshots of their volumes onto cloud storage. When pools or volumes are deleted by accident or due to improper operations, there is still a way to bring the data back online.

The following explains the mechanisms of the cloud gateway features. If you have any problem when applying the cloud gateway features in your environment, please **contact us**.

1-1. Cloud Tiering Mode

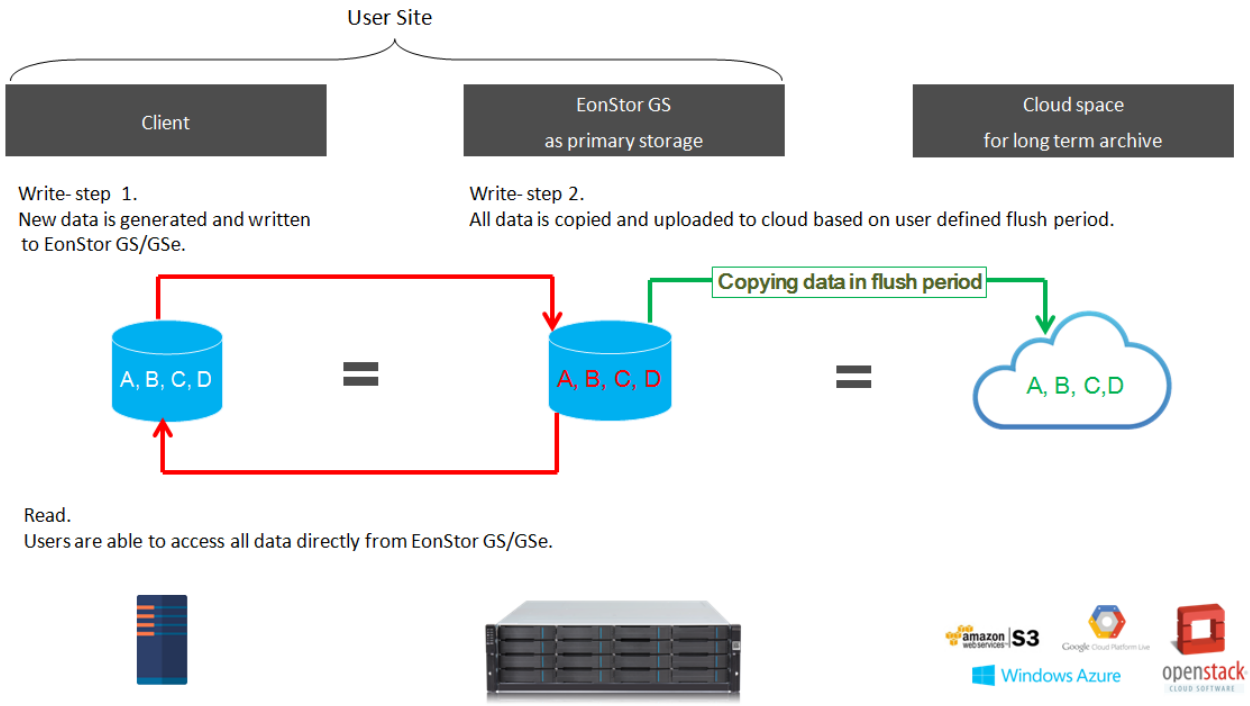
With the Cloud Tiering mode, a cloud bucket is used as a storage tier in the EonStor GS/GSe storage system for flexible capacity expansion and budget planning. The system itself keeps frequently accessed data (generally called hot data) in the local volume and moves the rest to the cloud tier. Therefore, users do not have to buy a whole new set of storage system for minor storage capacity overhead.



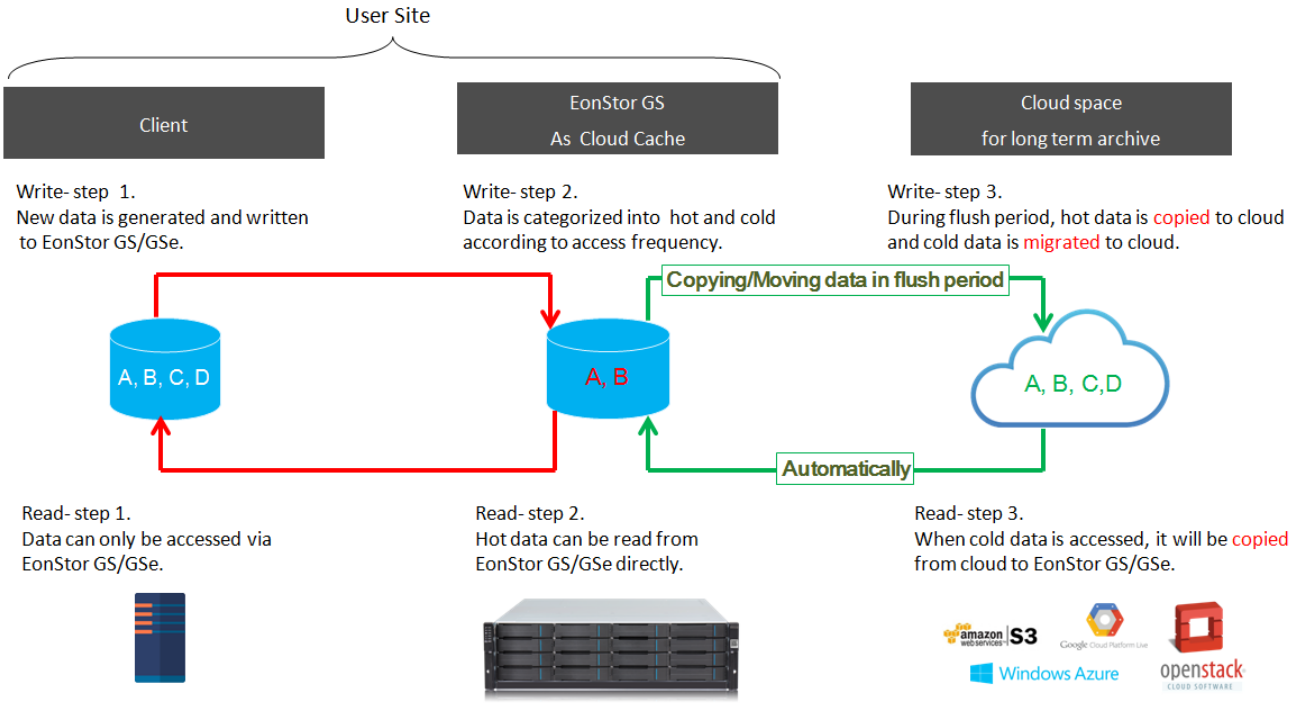
1-2. Cloud Caching Mode

The Cloud Caching mode enables the EonStor GS/GSe storage systems to copy data from the local site to cloud buckets. Cloud Caching is further divided into fully cache mode and non-fully cache mode. If a volume is set to fully cache mode, the cloud storage will be treated as a remote backup site and the data will be stored in both the local site and the cloud storage. If a volume is set to non-fully cache mode, all the data will be uploaded onto the cloud but only frequently accessed data will be stored in the local storage. In this case, the EonStor GS/GSe device functions like a reading cache and writing buffer, accelerating access speed for data on the cloud storage.

1-2-1. Fully Cache

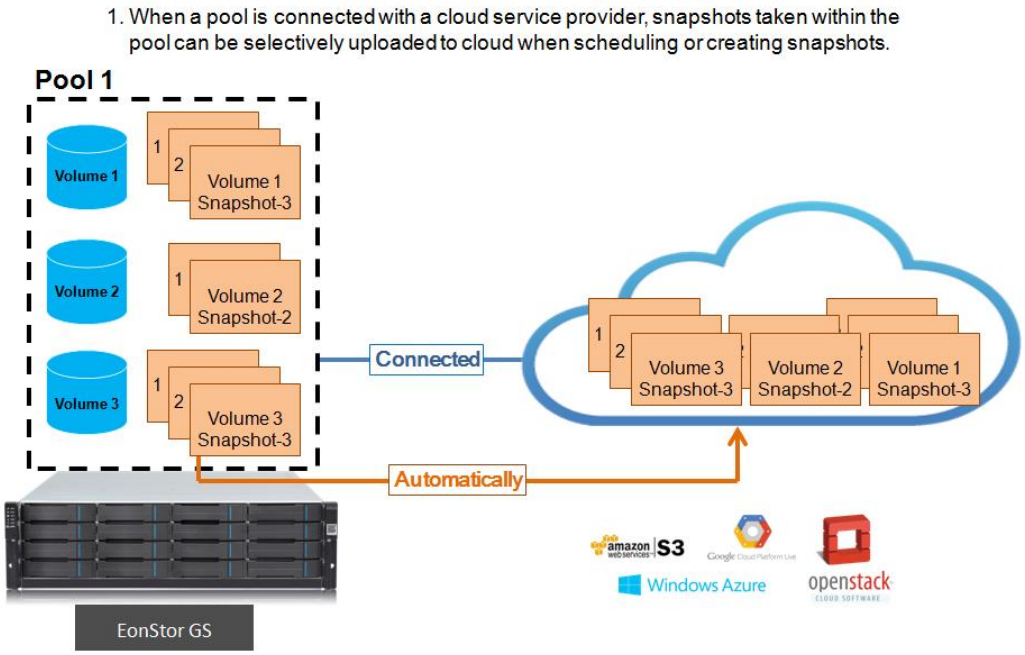


1-2-2. Non-fully Cache

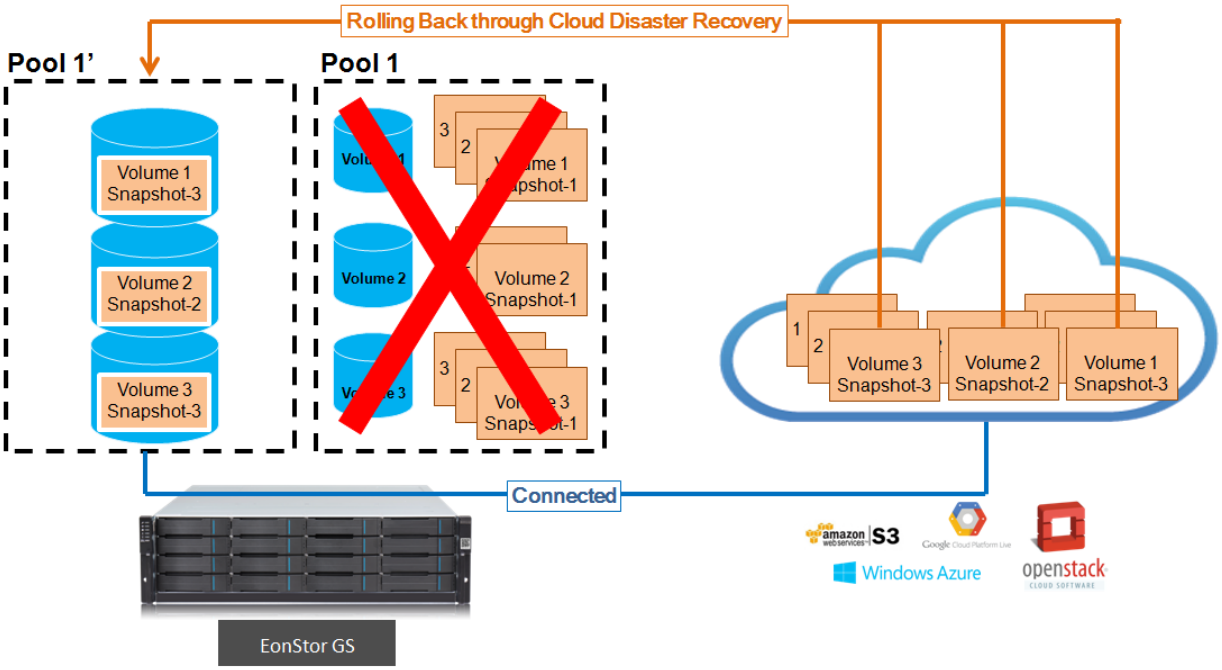


1-3. Snapshot Backup

The Snapshot Backup feature allows users to upload snapshot images onto the cloud storage. When pools were being eliminated by unexpected incidents, the snapshots on the cloud can be used to recover the data and serve as the last line of defense against data loss.



2. When the pool is deleted due to unexpected incidents, users can use the snapshot images on the cloud to recover the original data.



Using the cloud gateway features

You can have your EonStor GS/GSe integrated with the cloud by following the steps below:

Step 1. Synchronize time in the time zone.

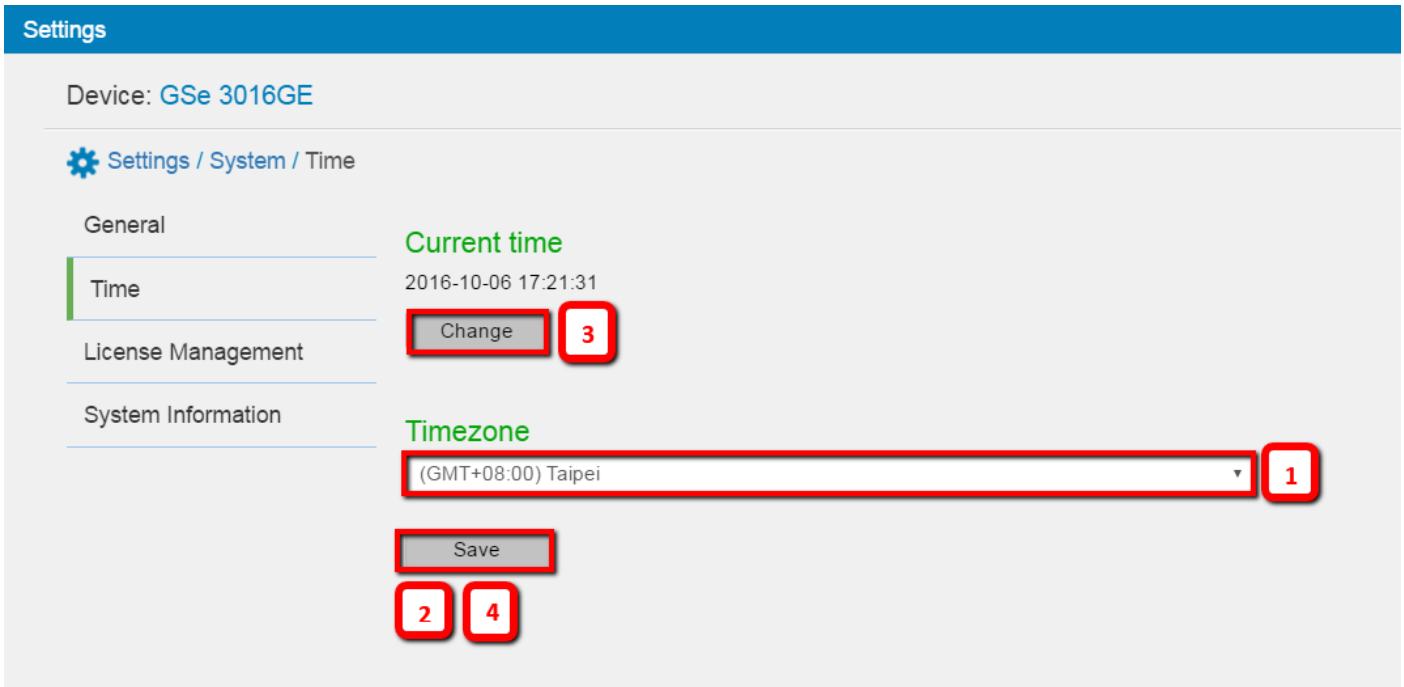
Step 2. Create a Pool.

Step 3. Connect your pool with a cloud service provider.

Step 4. Create cloud integrated volumes.

2-1. Synchronizing time in a time zone

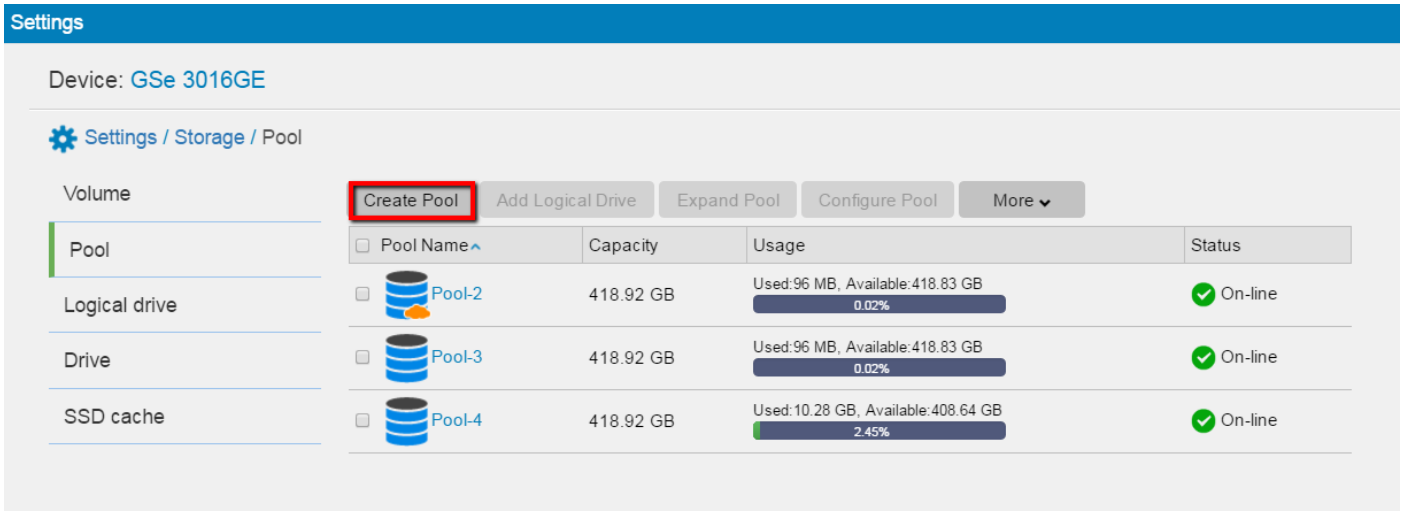
EonStor GS/GSe needs to be synchronized with the current time in a time zone. Go to **EonOne → Settings → System → Time**. Set the **time zone**, click **Save**, then click **Change** and set the time, daylight saving time, or you can set the network time server to synchronize with the correct time automatically.



2-2. Creating a pool

Go to **EonOne → Settings → Storage → Pool**, click **Create** and finish the settings.

Note: If you already have a pool, skip this step.



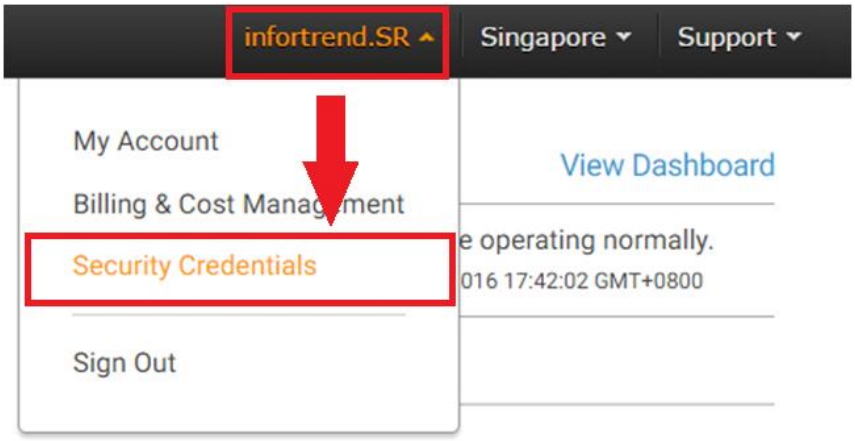
2-3. Connecting your pool with a cloud service provider

2-3-1. Amazon S3

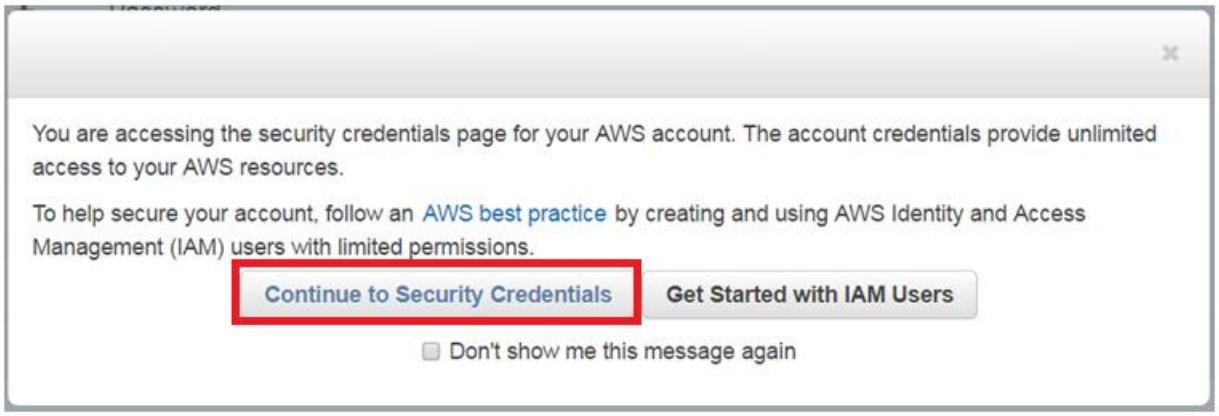
This section explains how to obtain access credentials and create cloud buckets on Amazon S3 via EonOne. There are two ways to obtain the access credentials on Amazon S3, via the root access keys or the IAM access keys.

1. Retrieving Root Access Keys

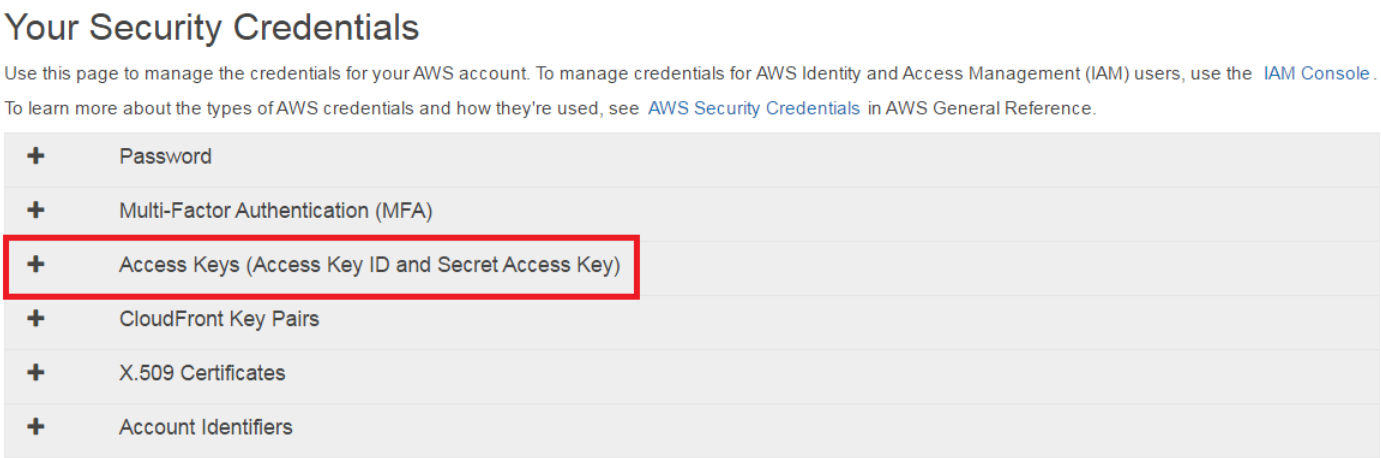
(1) Register an account and log into the account. After login, click **Security Credentials** in the username's drop-down list.



(2) Click **Continue to Security Credentials**.



(3) Click on the **Access Keys (Access Key ID and Secret Access Key)** option. You can see a list of all your active and deleted root access keys.

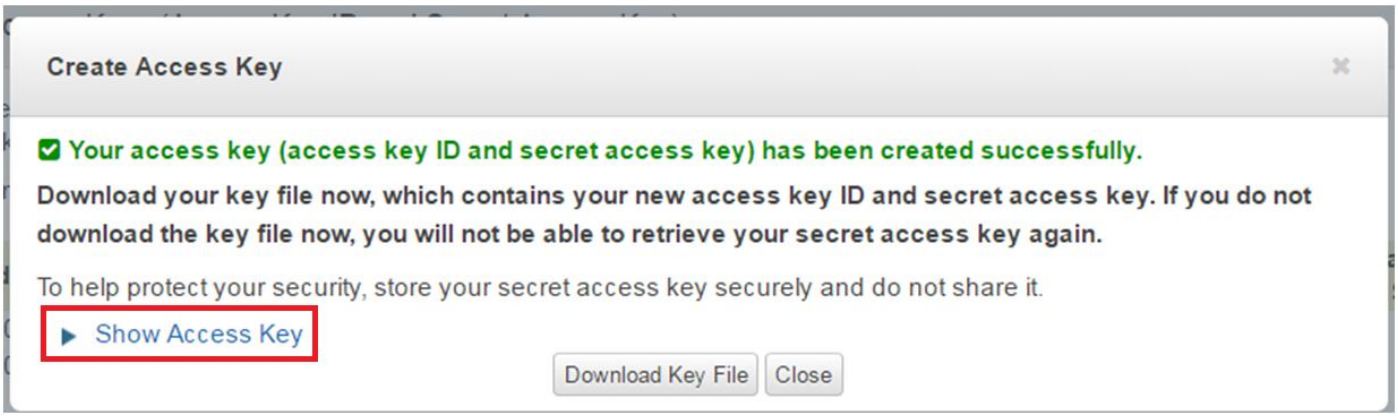


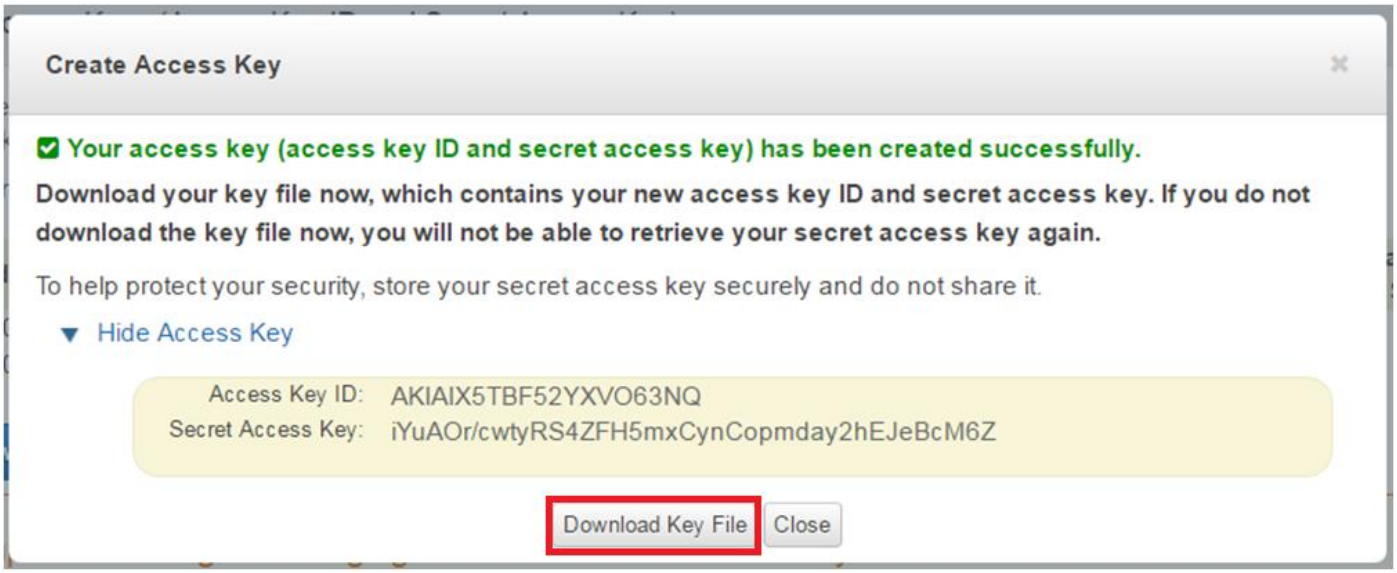
Note: You cannot retrieve an existing secret key. You can see the secret key only once immediately after creating it. Therefore, in order to get a secret key, you will need to create a new pair of access key and

secret key.

(4) To generate a new access key, click **Create New Access Key.**

(5) Click **Show Access Key** to have them displayed on the screen. You can download it to your machine as a file and open it whenever needed. To download it, click the **Download Key File** button.

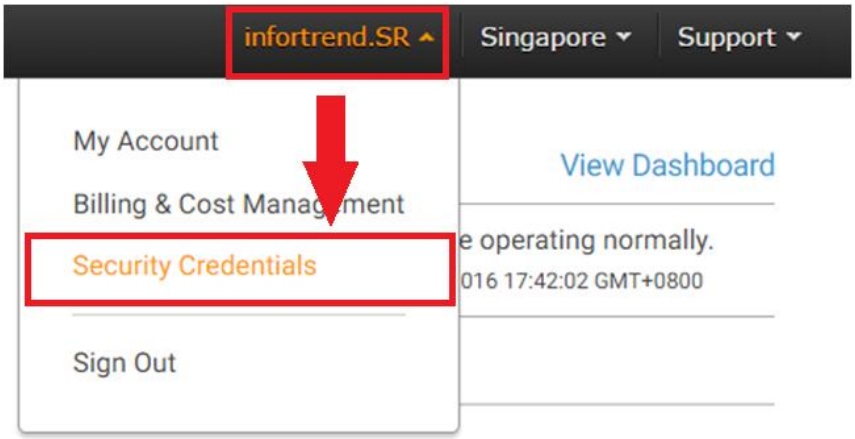




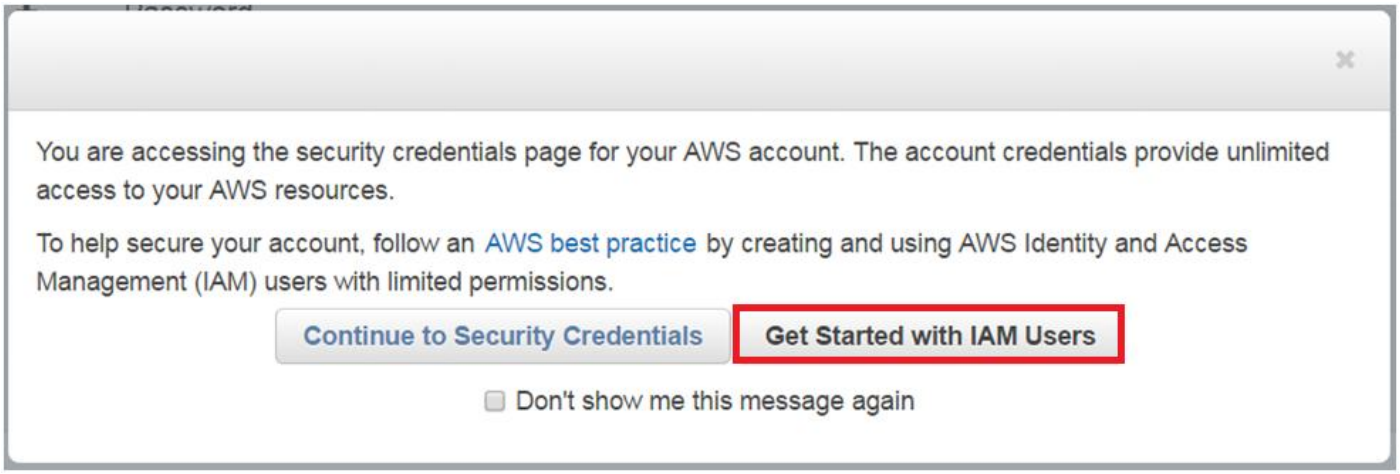
Attention! If you do not write down the key or download the key file to your computer before you click **Close** or **Cancel,** you will no longer be able to retrieve the secret key again. In such cases, the only thing you can do is deleting the pair of keys and then create new ones.

2. Retrieving IAM Access Keys

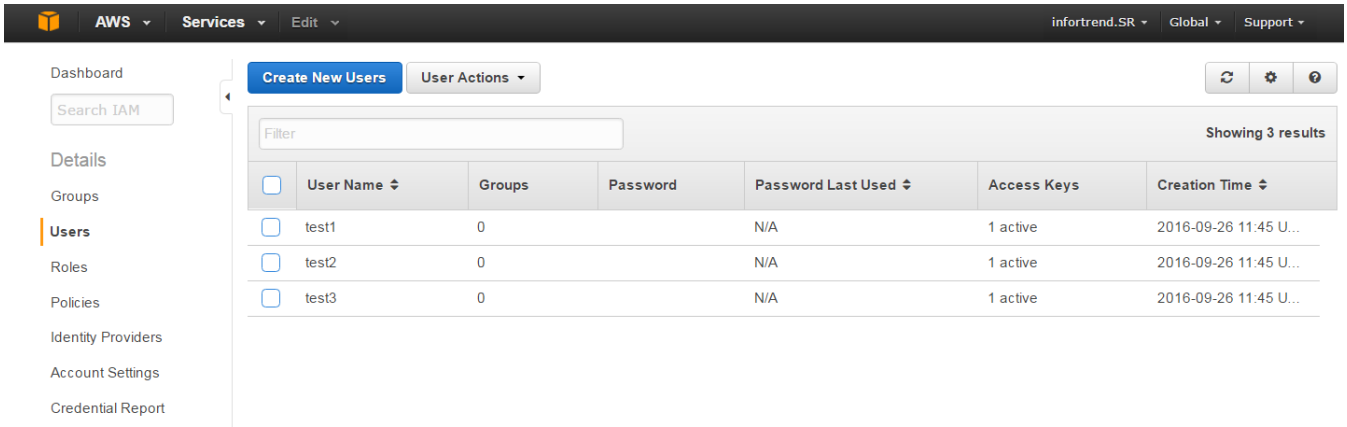
(1) Register an account and log into the account. After login, click **Security Credentials** in the username's drop-down list.



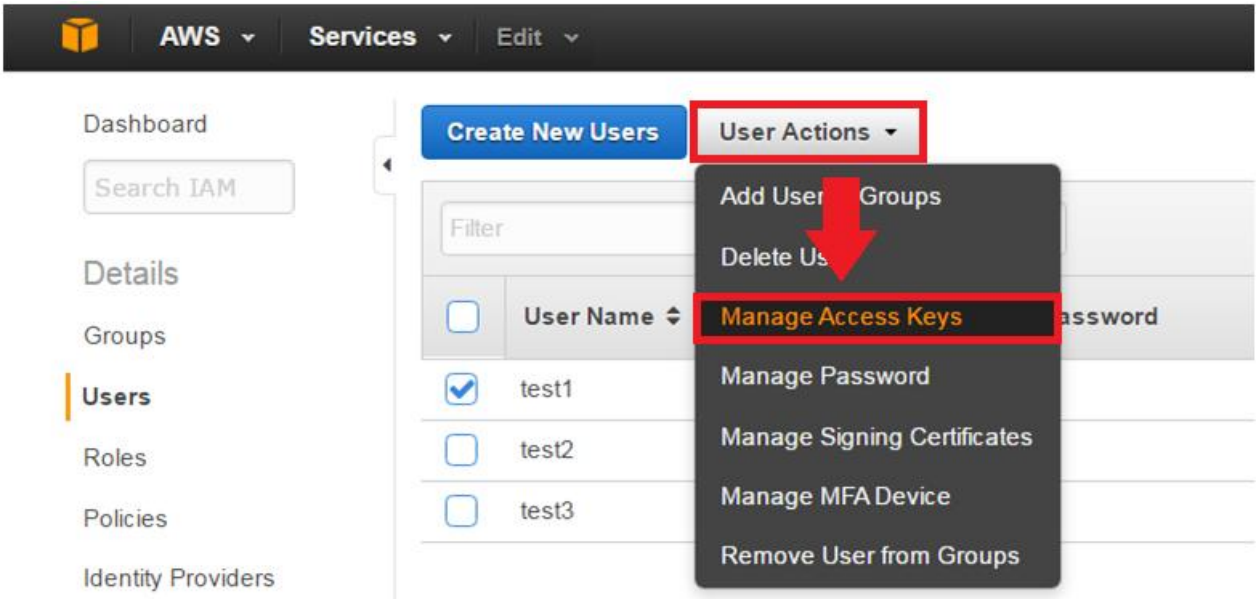
(2) Click the **Get Started with IAM Users** button.



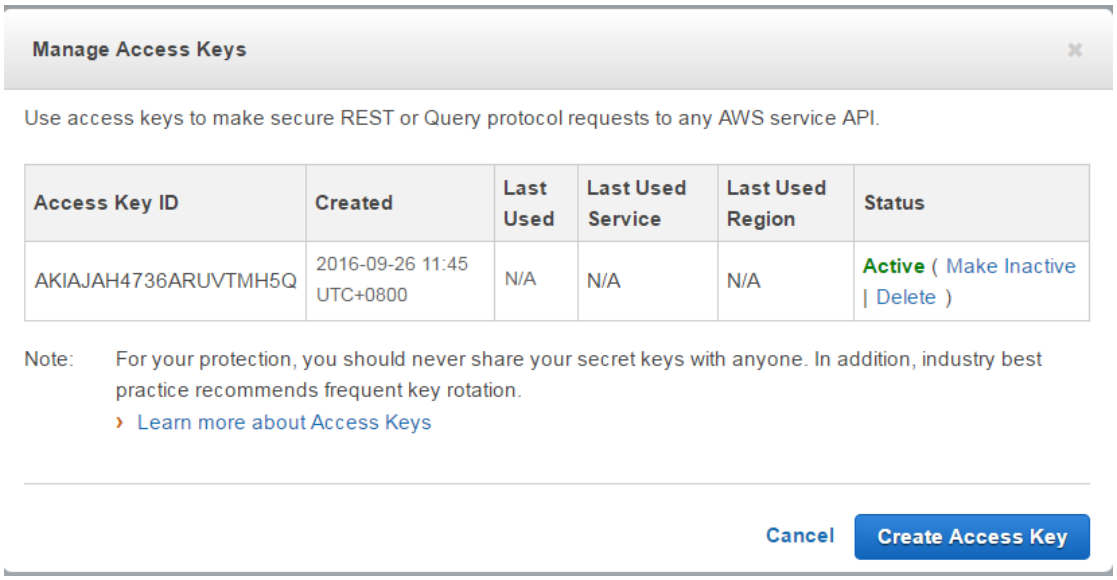
(3) This will lead you to the **IAM Dashboard** where you can manage IAM users and their permissions such as creating new IAM users, adding IAM users to custom groups, granting them certain level of permissions, etc. If you don't have any users created before, click **Create New Users** to create a new user.



(4) To review the IAM access keys, select a particular IAM user and go to **User Actions → Manage Access Keys.**

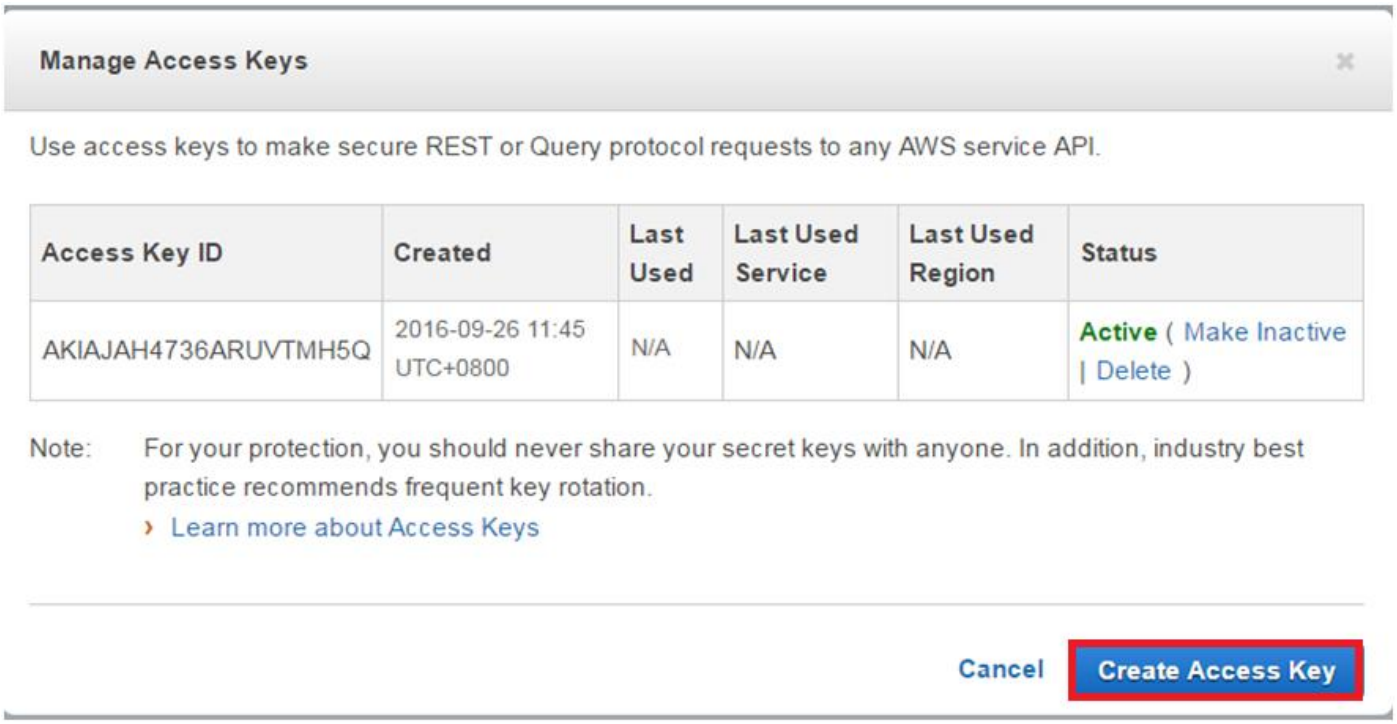


(5) You will see a list of Access Keys for the IAM user.

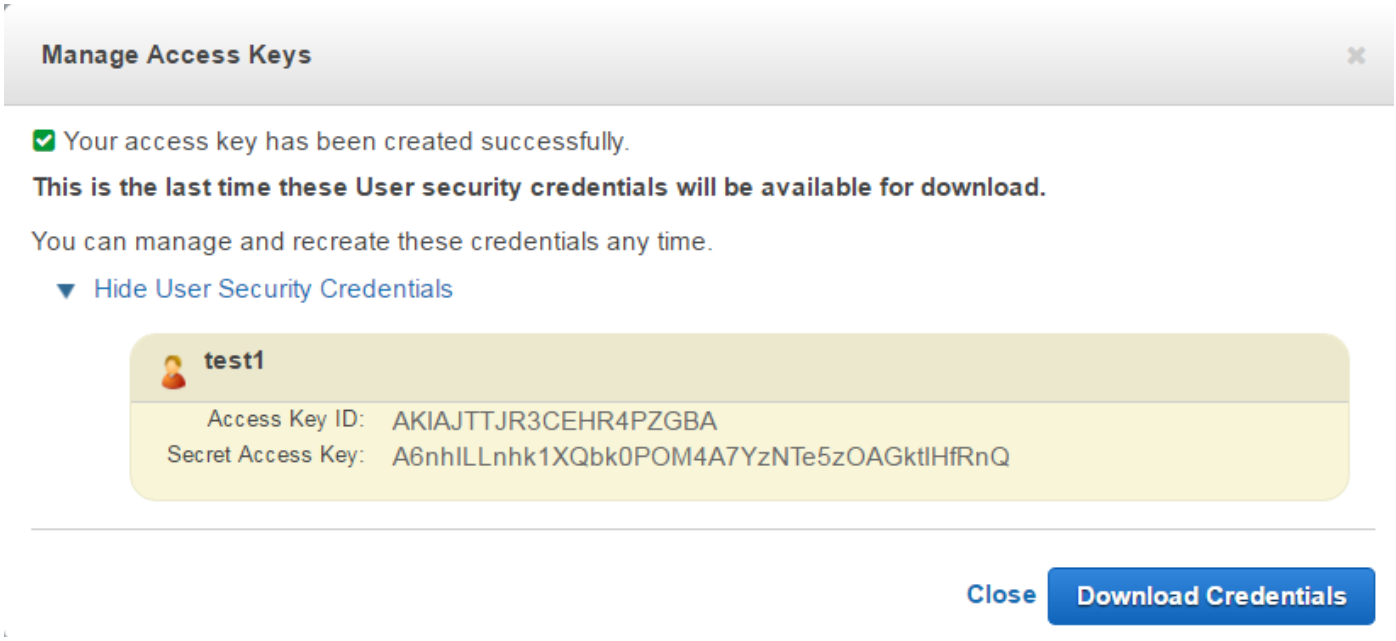


Note: You cannot retrieve the existing secret keys. You can see the secret key only once immediately after creating it. Therefore, in order to get a secret key, you will need to create a new pair of access key ID and secret key.

(6) Click **Create Access Key** to create a new pair of access key ID and secret key.



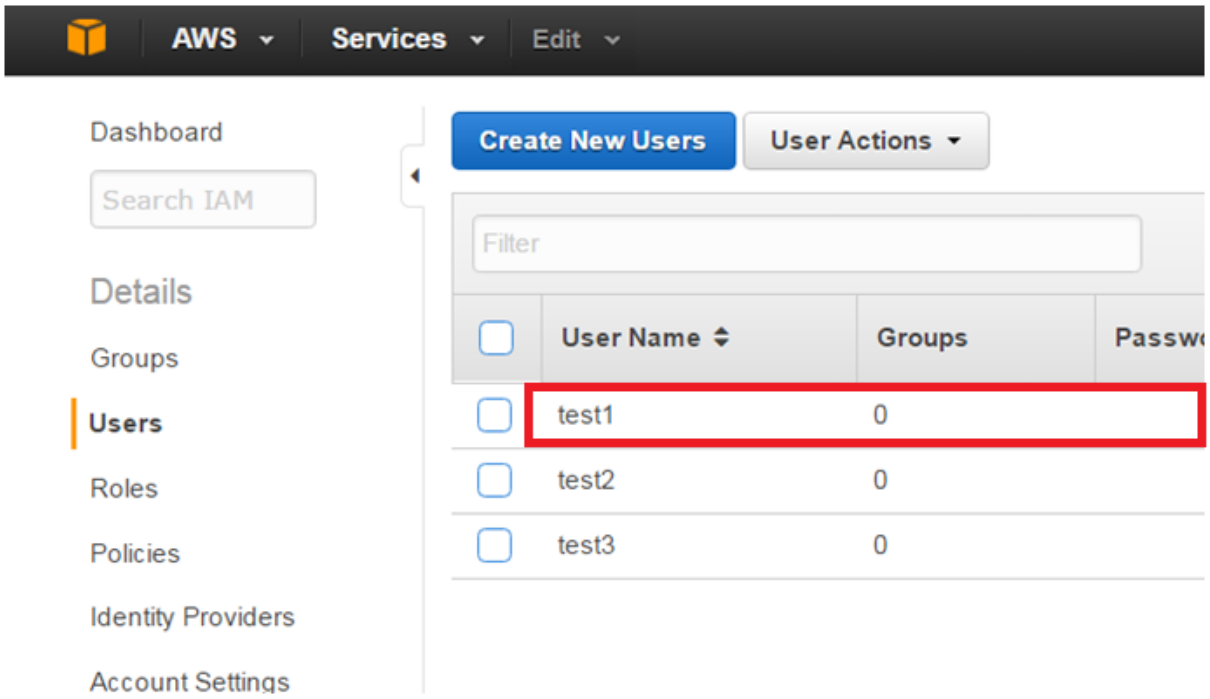
(7) The new access keys will be generated and displayed on the screen.



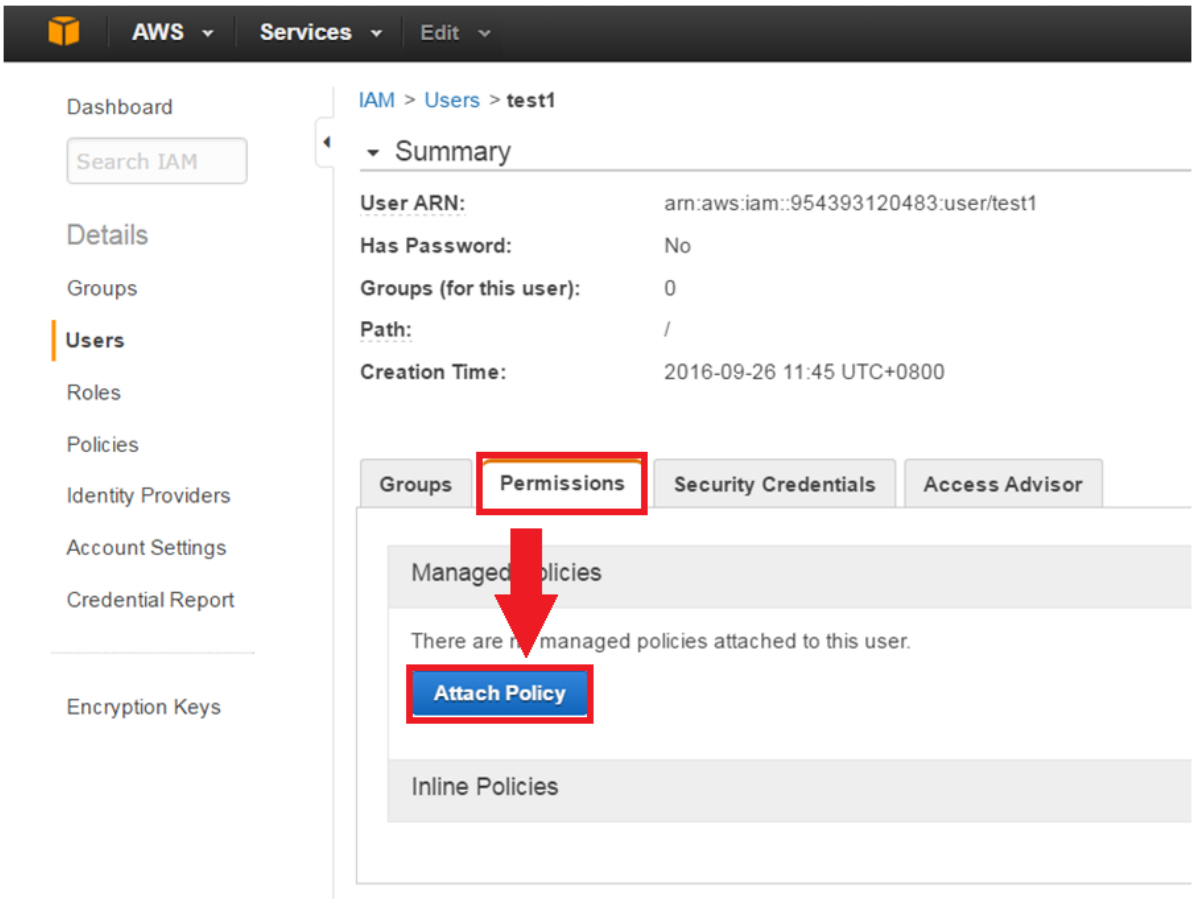
Attention! If you do not write down the key or download the key file to your computer before you click **Close** or **Cancel,** you will no longer be able to retrieve the secret key again. In such cases, the only thing you can do is deleting the pair of keys and then create new ones.

(8) Add permissions to the IAM users

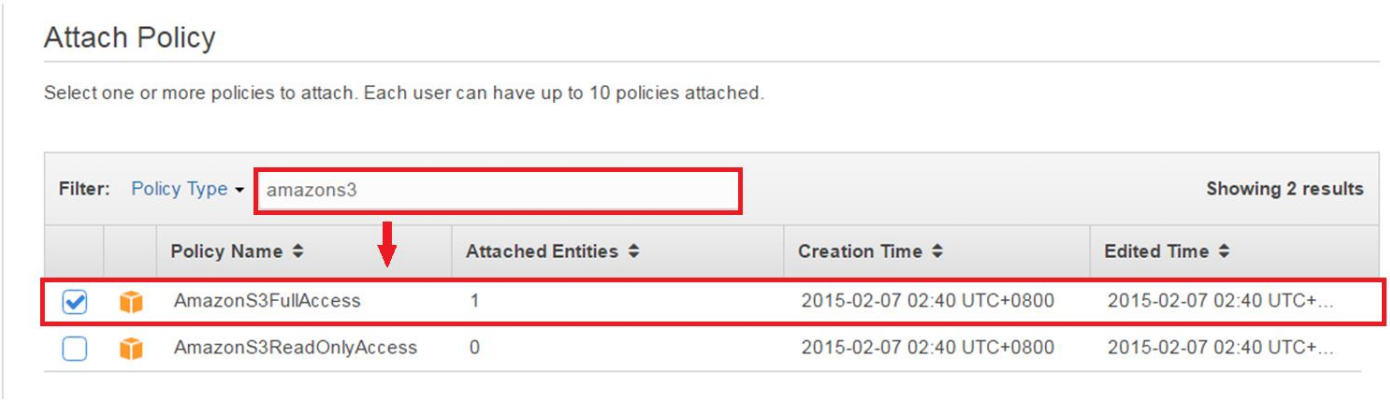
After access keys are generated, you still need to give the user access permissions to use Amazon S3. Click on one of the users you created.



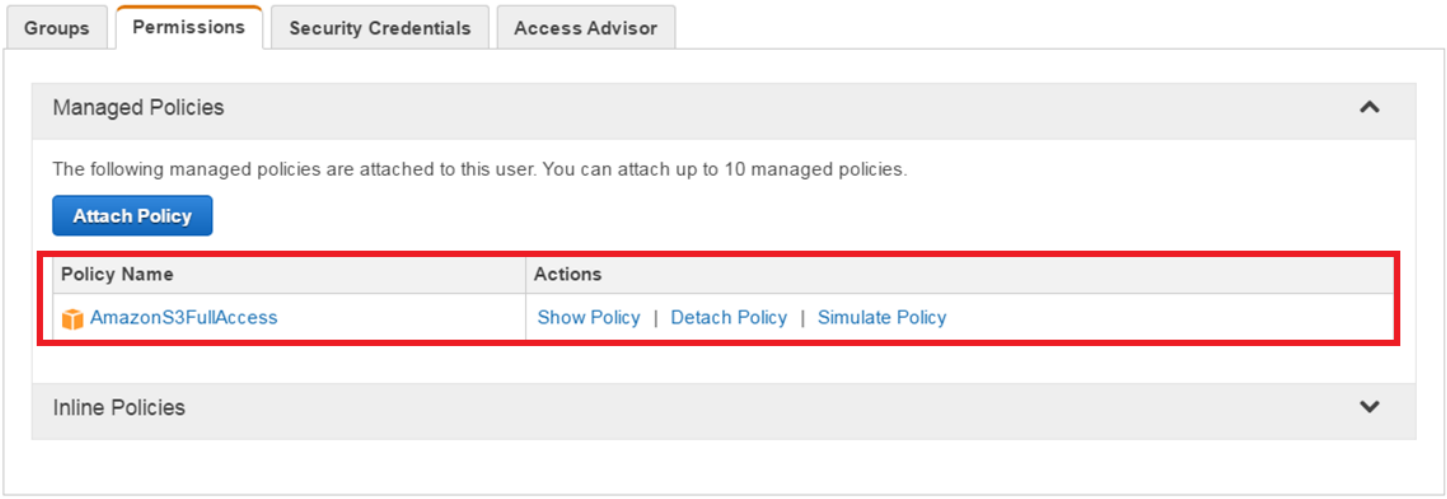
(9) You will be led to the user configuration page. Switch to the **Permissions** page and click **Attach Policy**.



(10) Search for permissions for Amazon S3 and then check the **AmazonS3FullAccess** option.

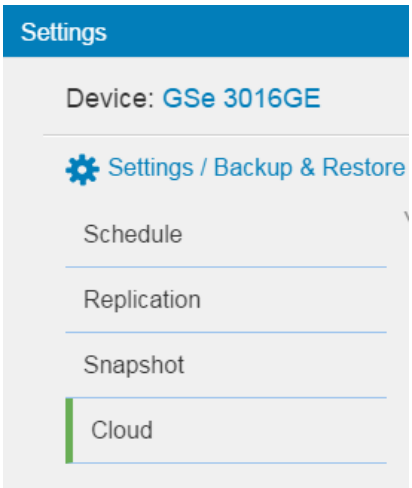


(11) You should see the said policy has been added to the IAM user permissions.

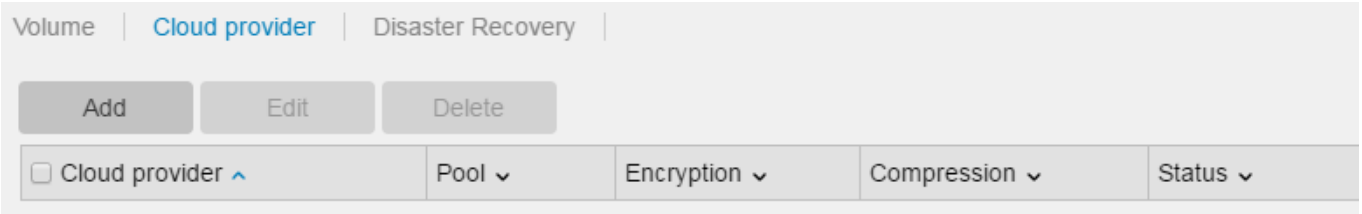


3. Connecting to GS

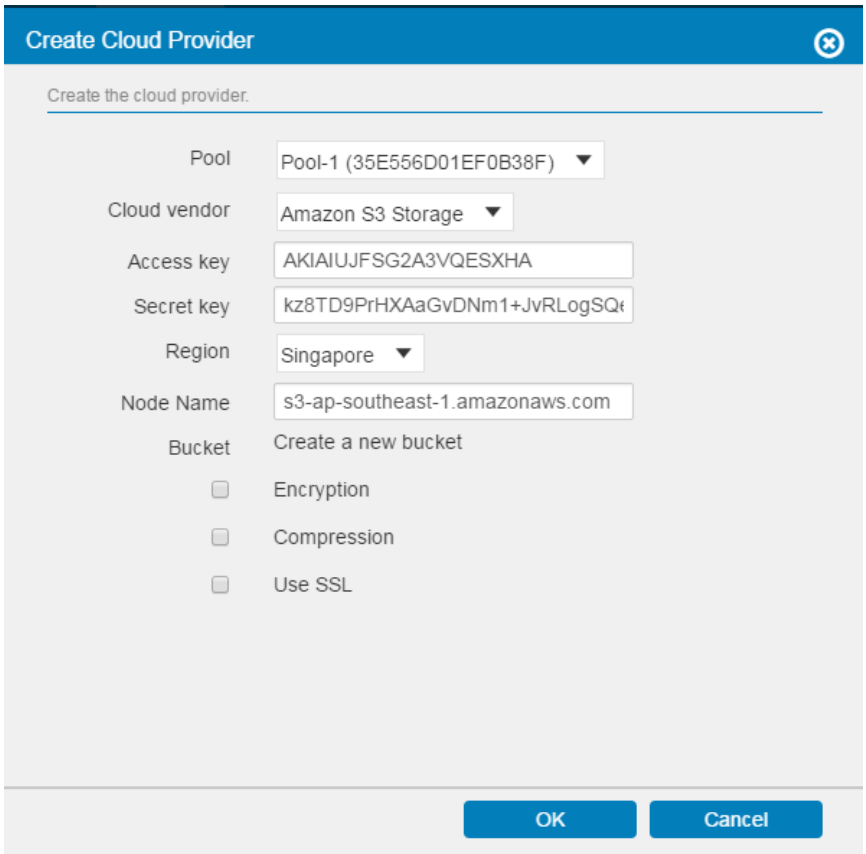
(1) Open EonOne and go to **Settings → Backup & Restore → Cloud**.



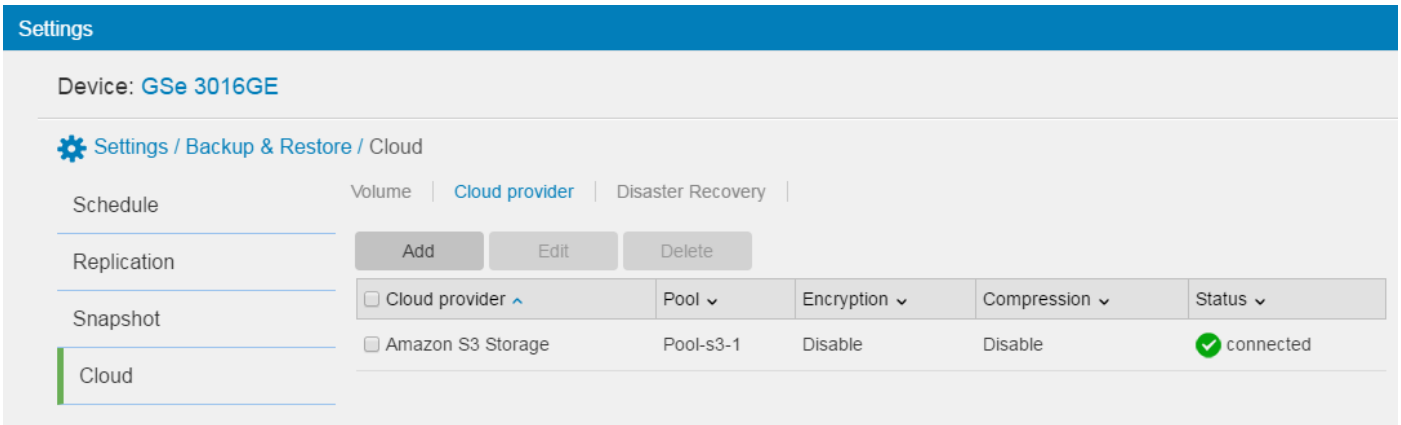
(2) On the Cloud page, switch to the **Cloud provider** page and click **Add**.



(3) Select a pool which you want to connect with a cloud provider, specify the **Cloud vender** and fill in the obtained access information. The **Region** is the location of the data center where your data will be saved. It can be any region but it is usually the region closest to you. Leave the **Node Name** as default and click **OK**.



(4) The connected cloud service provider will be listed.

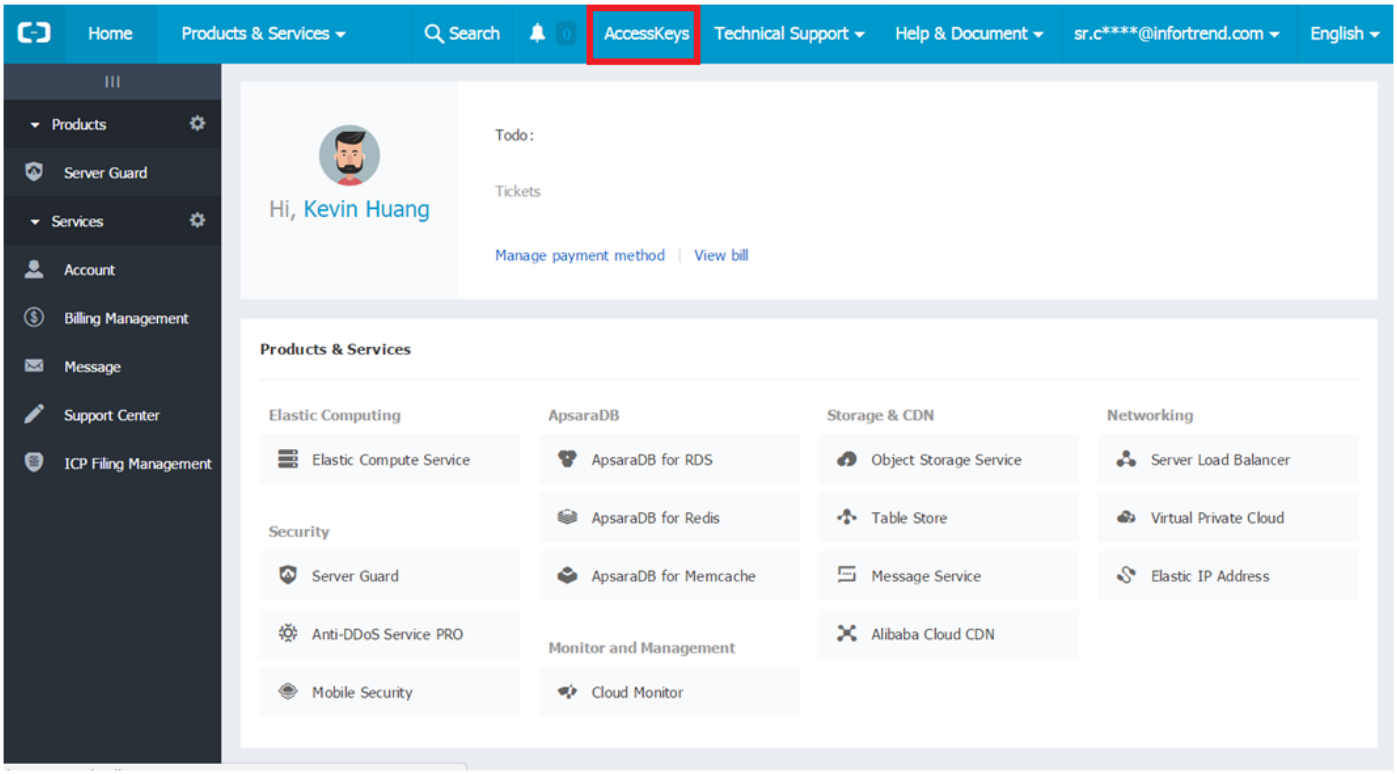


2-3-2. Aliyun Object Storage Service

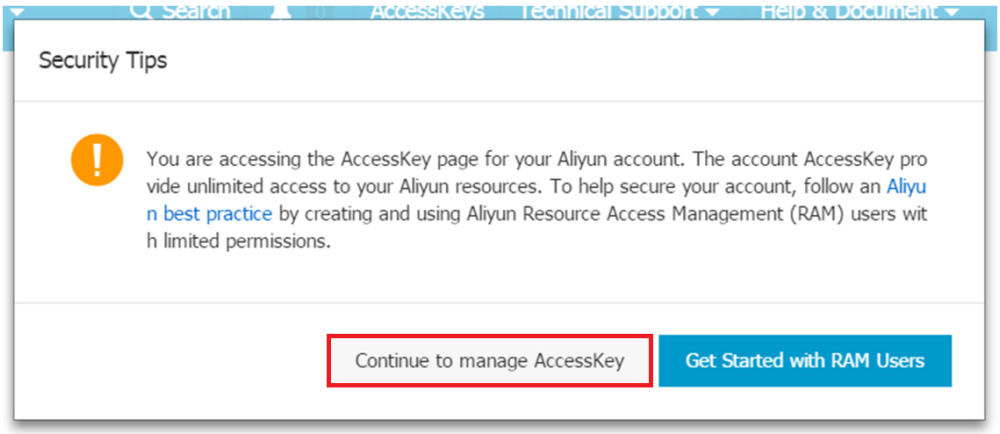
This section explains how to obtain access credentials and create cloud buckets on Aliyun OSS via EonOne.

1. Retrieving access information

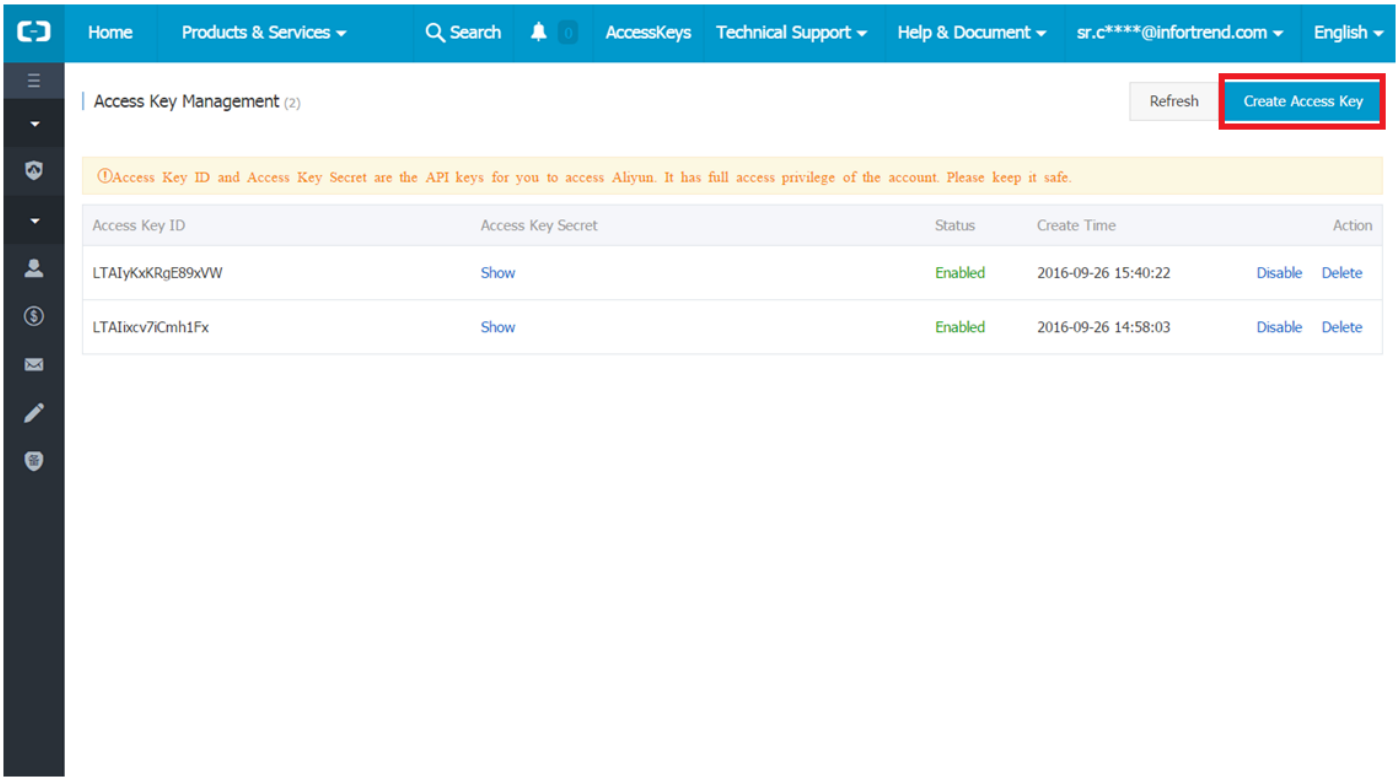
(1) Create and log into your account. After login, click the **AccessKeys** button at the tool bar on the top.



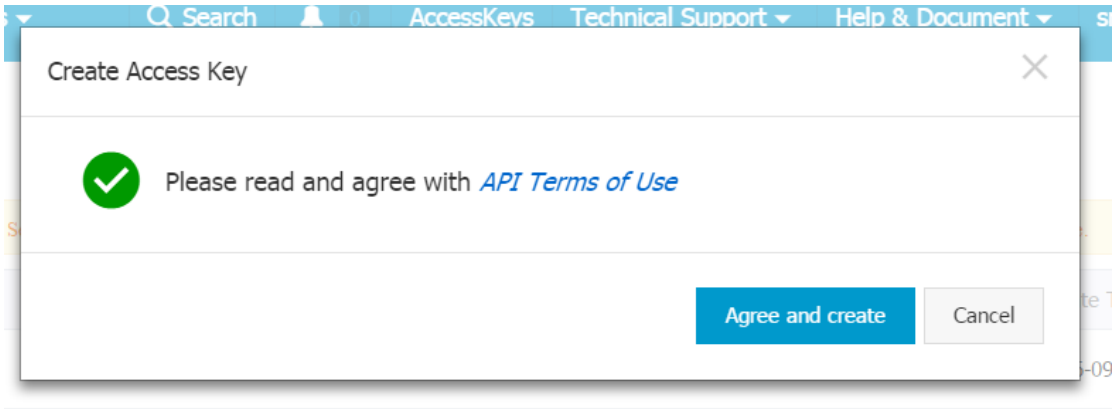
(2) In the pop-up window, click **Continue to manage AccessKey**.



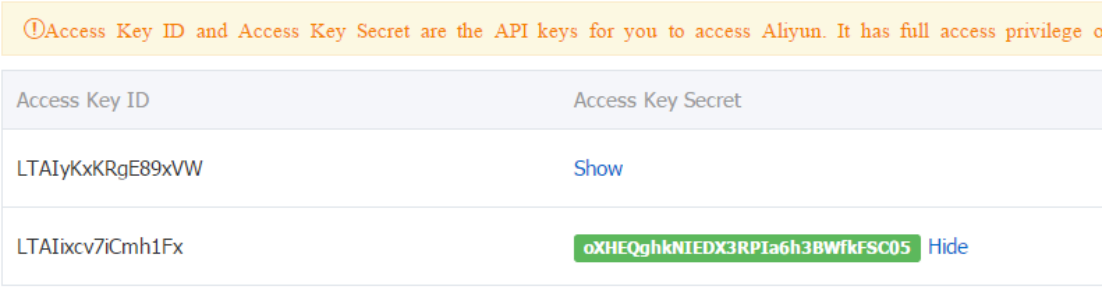
(3) This will lead you to the access key management page. On this page, you can click **Show** to have a hidden Access Key Secret displayed or create a new pair of Access Key ID and Access Key Secret by clicking **Create Access Key**.



(4) Click **Agree and Create** to verify the operation.

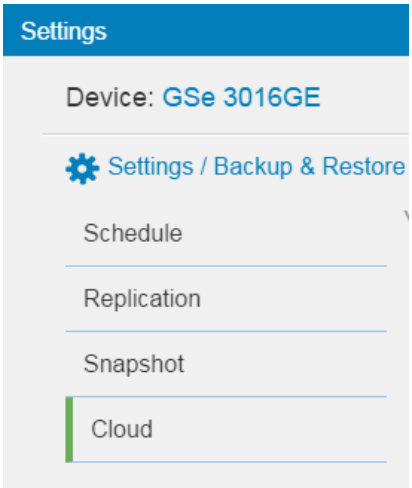


(5) After the new pair of access keys are generated, click **Show** to see the Access Key Secret.

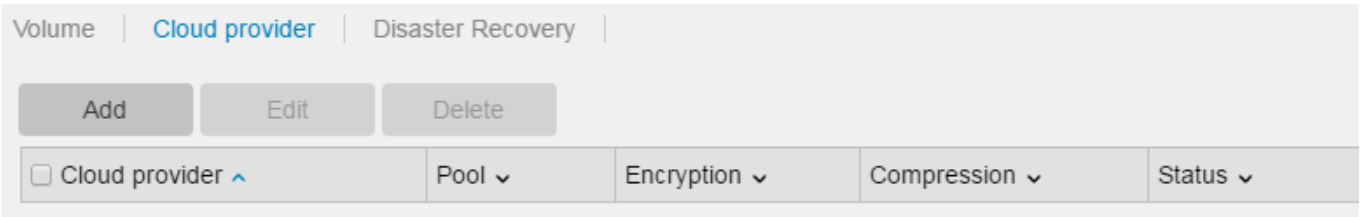


2. Connecting to GS

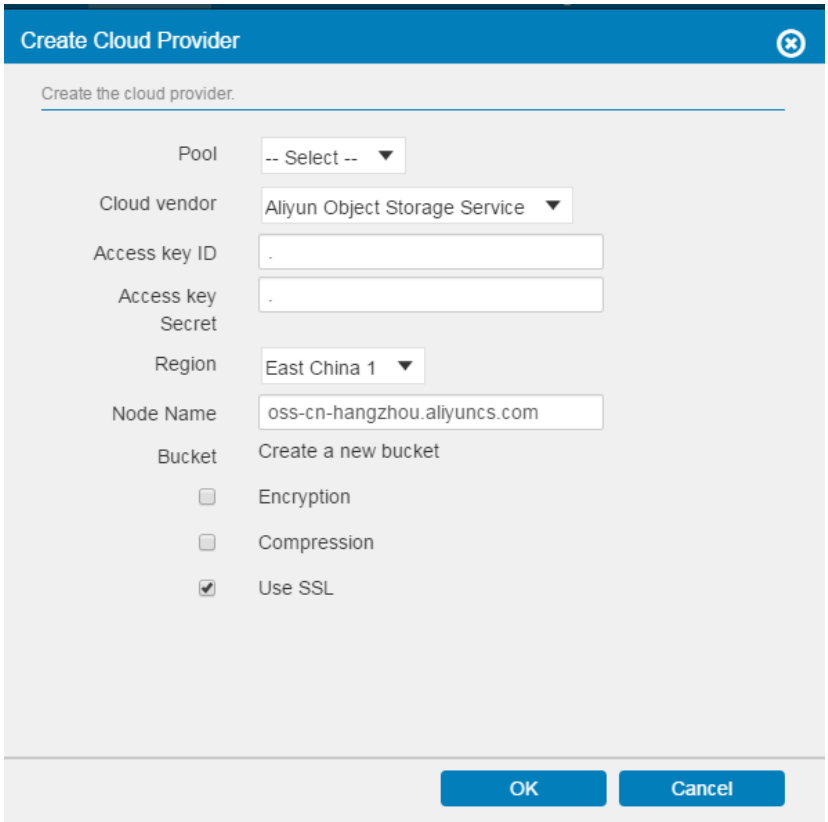
(1) Open EonOne, go to **Settings → Backup & Restore → Cloud**.



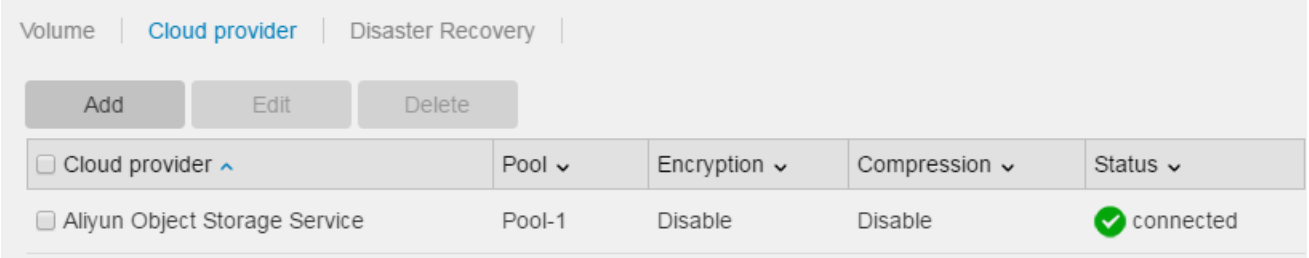
(2) On the Cloud page, switch to the **Cloud provider** page and click **Add**.



(3) Select a pool which you want to connect with a cloud provider, specify the **Cloud vender** and fill in the obtained access information. The **Region** is the location of the data center where your data will be saved. It can be any region but it is usually the region closest to you. Leave the **Node Name** as default and click **OK**.



(4) The connected cloud service provider will be listed.

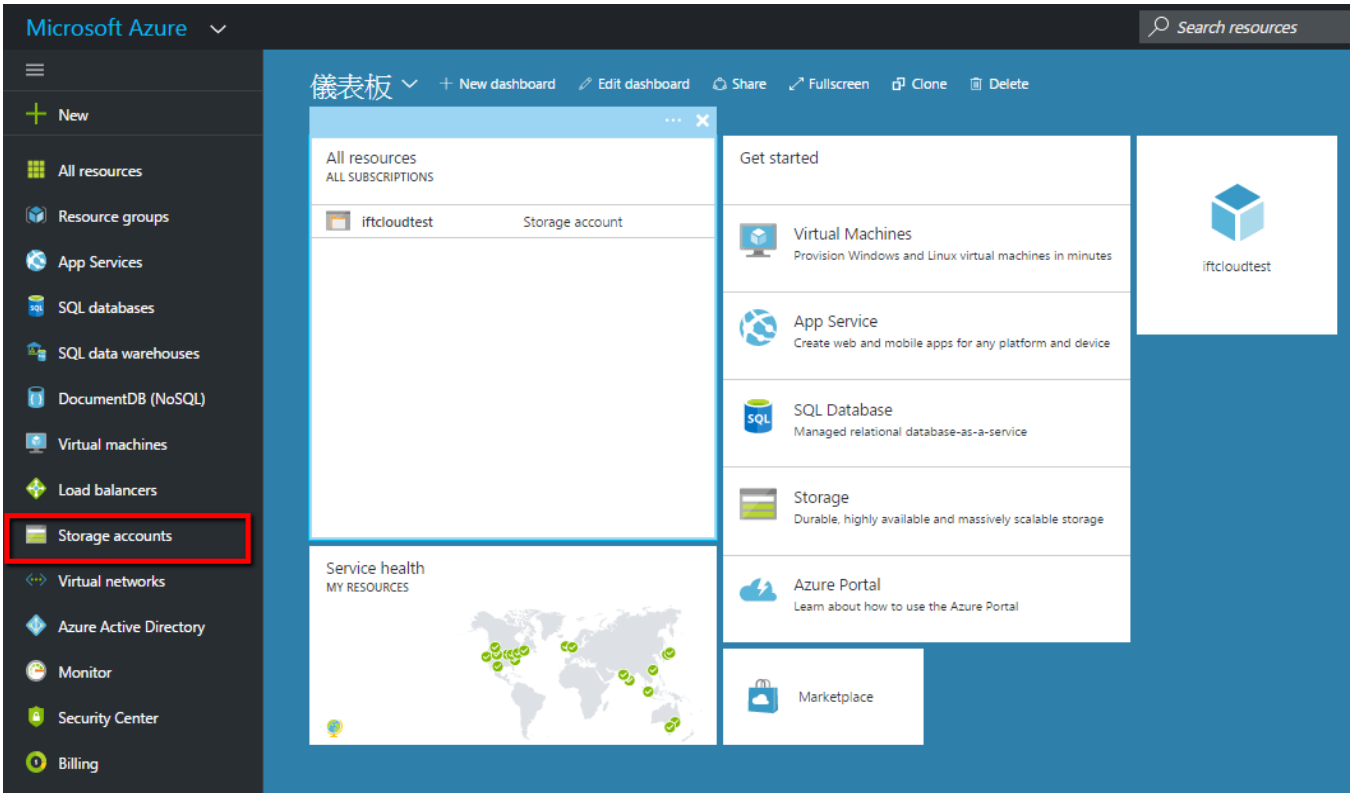


2-3-3. Microsoft Azure

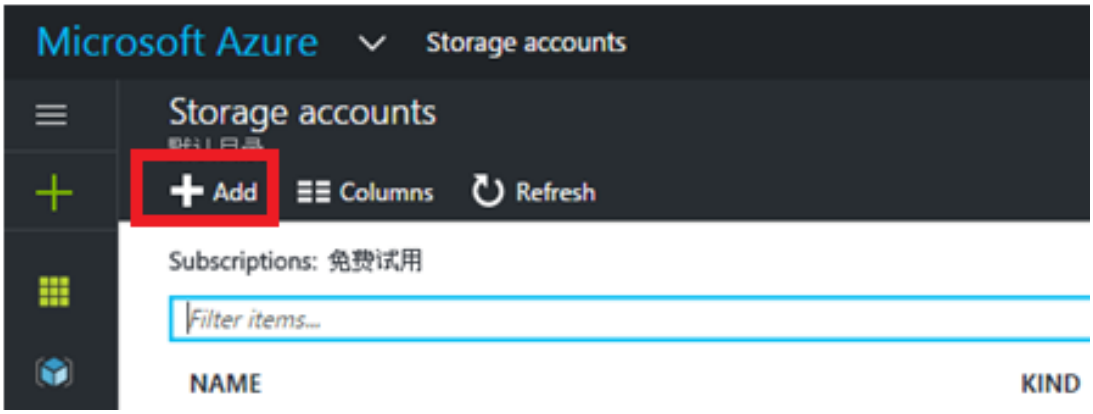
This section explains how to obtain access credentials and create cloud buckets on Microsoft Azure via EonOne.

1. Retrieving access information

(1) Create an account and log into Microsoft Azure. After login, click **Storage Accounts.**

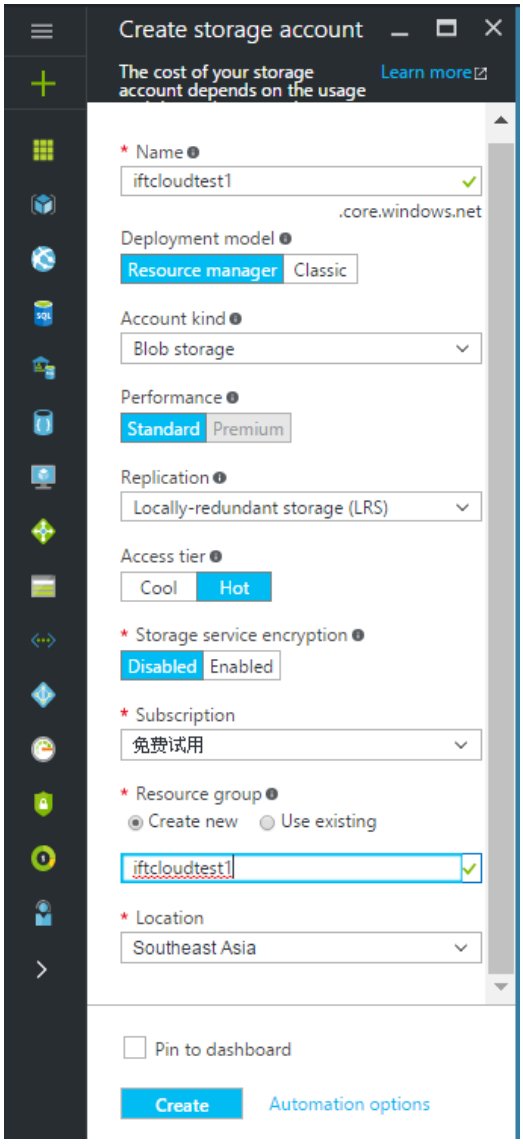


(2) On the storage account page, click **Add**.

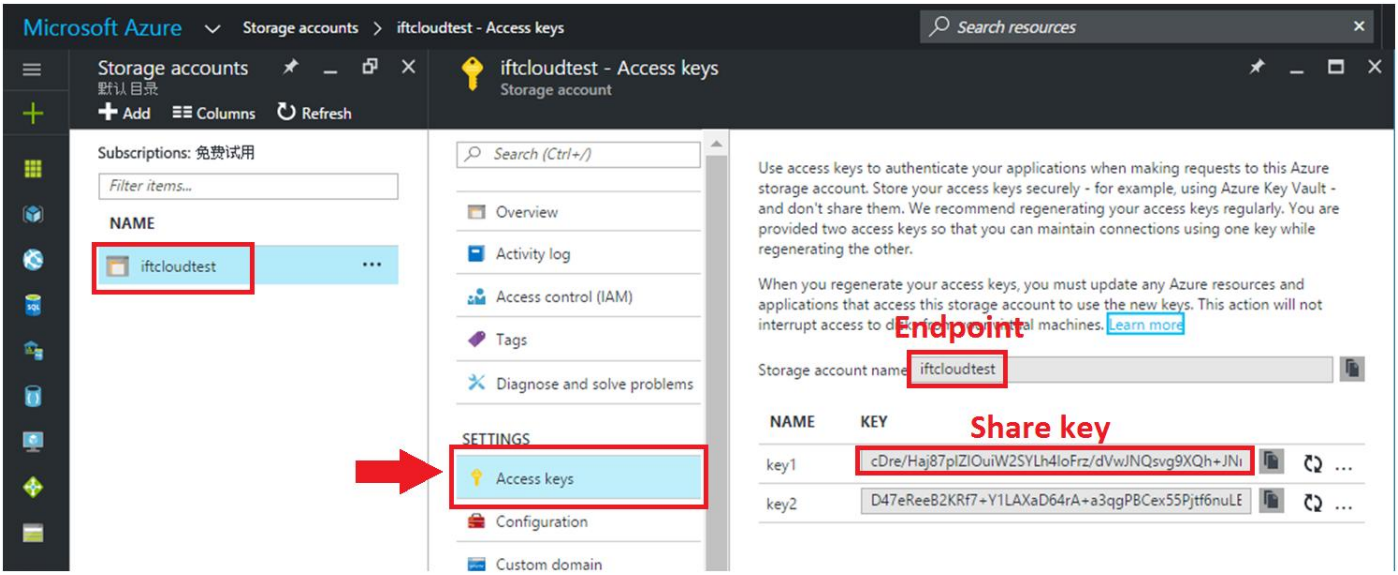


(3) Specify the **Name** of your storage account. You will need to type it in the **Endpoint** name when connecting with EonStor GS/GSe devices.

Note: For demonstration, we set the **Account kind** to Blob storage. Users can also specify the **Account kind** to other types that can store blob data, such as **General Purpose**.

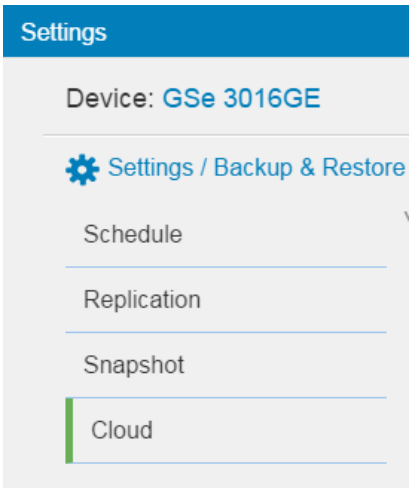


(4) Click on the storage account you just created and a column for the account's settings will appear. Then click **Access keys.** You will see the information needed to connect to EonStor GS/GSe.

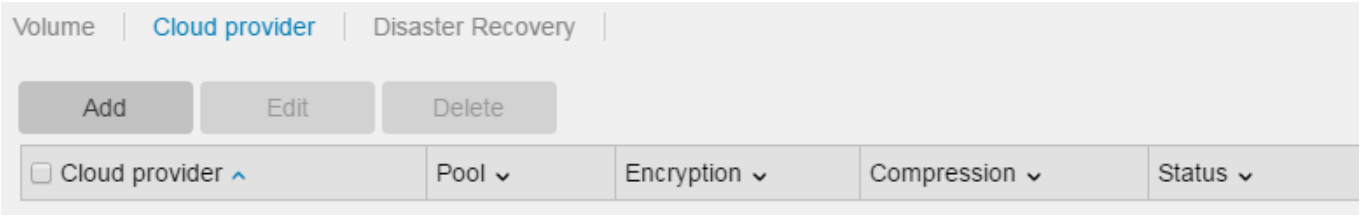


2. Connecting to GS

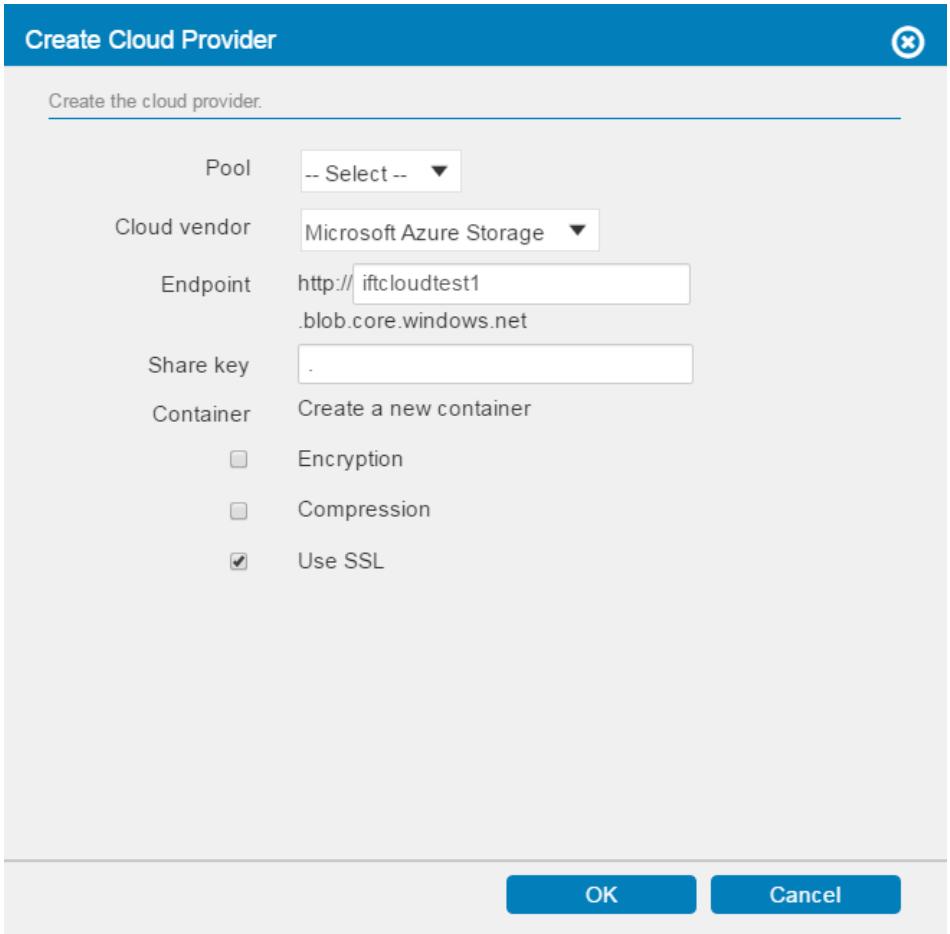
(1) Open EonOne, go to **Settings → Backup & Restore → Cloud**.



(2) On the Cloud page, switch to the **Cloud provider** page and click **Add**.



(3) Select a pool which you want to connect with a cloud provider, specify the **Cloud vender**, fill in the obtained access information and click **OK**.



(4) The connected cloud service provider will be listed.

2-3-4. Openstack Swift

This section explains how to obtain access credentials and create cloud buckets on Openstack Swift via EonOne.

1. Retrieving access information

When your Openstack environment is set, follow the steps below to retrieve access information.

(1) Find and edit the proxy-server configuration file.

Command: **vi /etc/swift/proxy-server.conf**

(2) The configuration file starts with the **DEFAULT** section, find or modify the **bind_ip** and **bind_port**. It will be the **Server IP** and **Port** when connecting with EonStor GS/GSe storage systems.

(3) Next, go to the **filter-tempauth** section, add a line to specify the user group, user name and key.

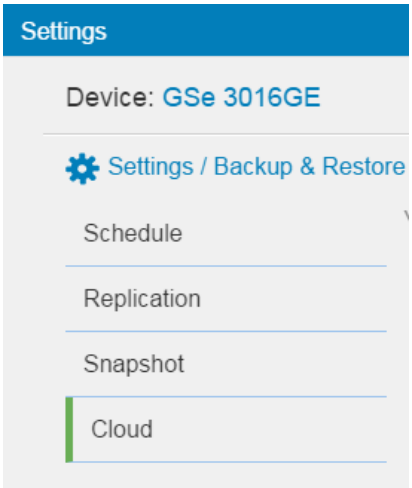
For example, if we add the following line in the **filter-tempauth** section,

user_infortrend_staff01=iftcloud

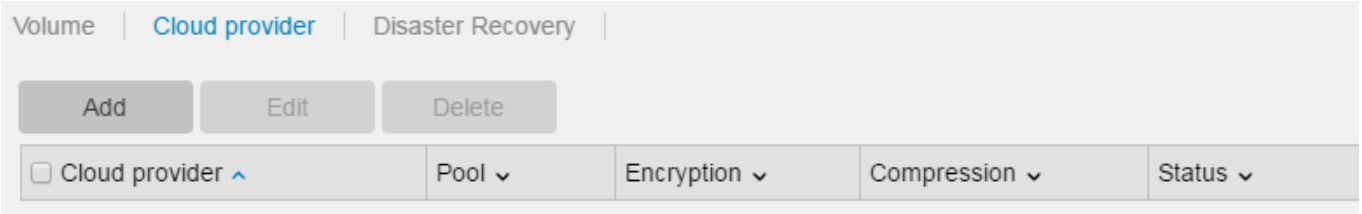
when connecting with EonStor GS/GSe storage systems, **infortrend:staff01** will be the **Access key**, and **iftcloud** will be the **Secret key**.

2. Connecting to GS

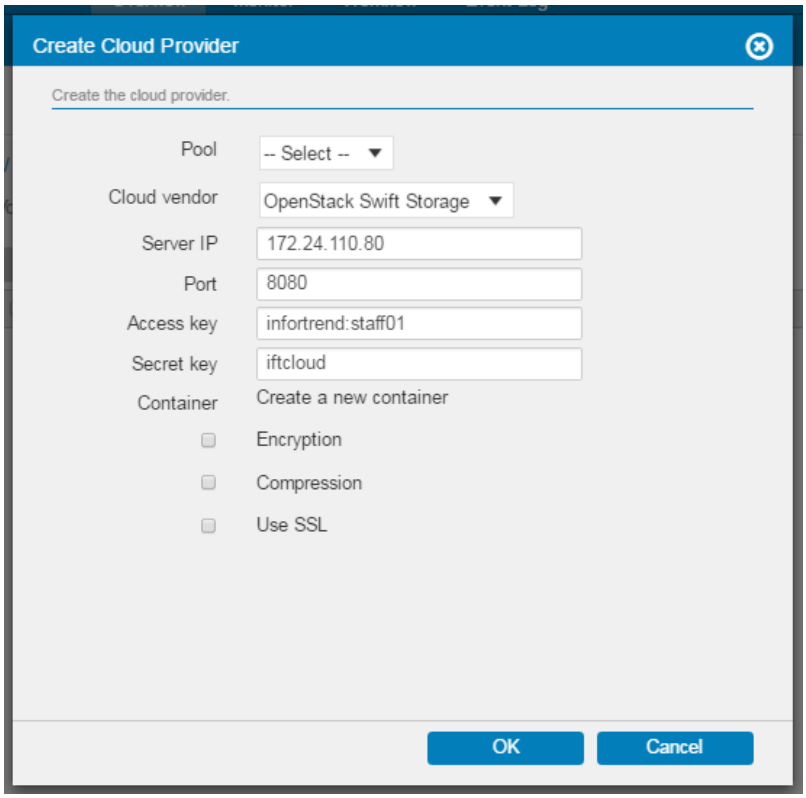
(1) Open EonOne, go to **Settings → Backup & Restore → Cloud**.



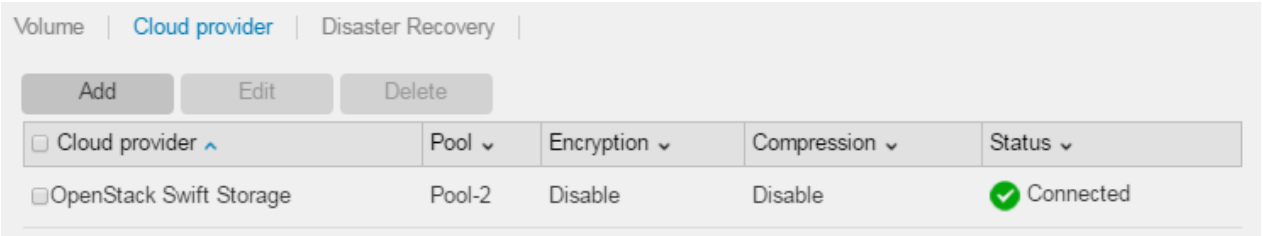
(2) On the Cloud page, switch to the **Cloud provider** page and click **Add**.



(3) Select a pool which you want to connect with a cloud provider, specify the **Cloud vender** and fill in the obtained access information.



(4) The connected cloud service provider will be listed.

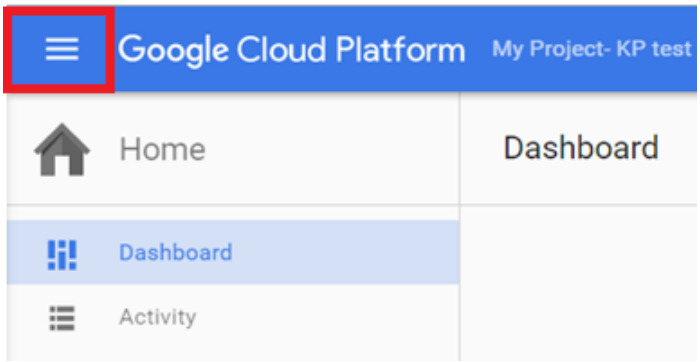


2-3-5. Google Cloud

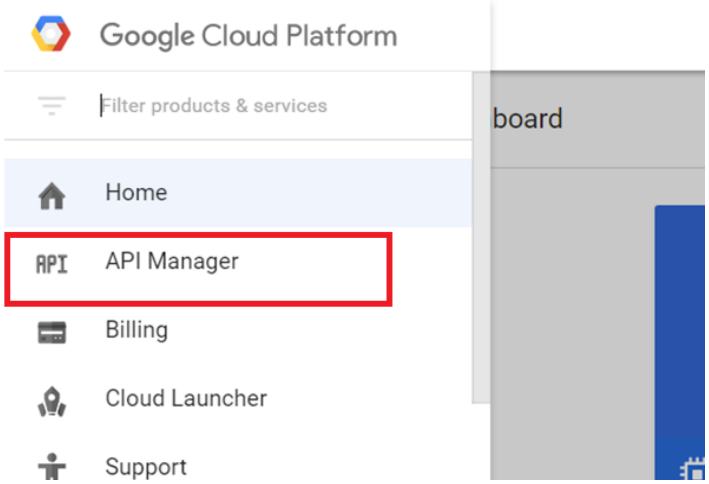
This section explains how to obtain access credentials and create cloud buckets on Google Cloud via EonOne.

1. Retrieving access information

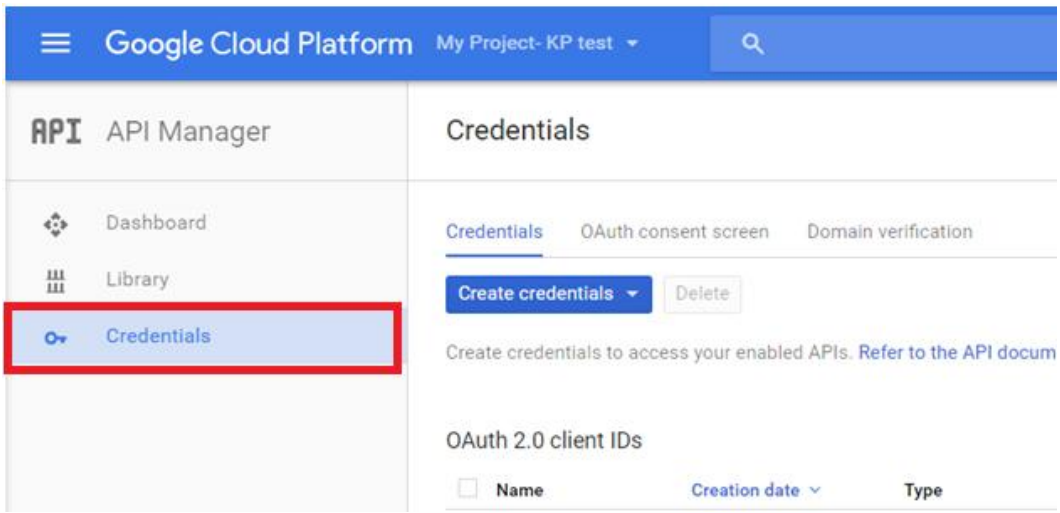
(1) Create a Google Cloud account and log into the account. After login, the Google Cloud platform will help you create your first project. After the project is created, click the **Menu** button on the top-left corner.



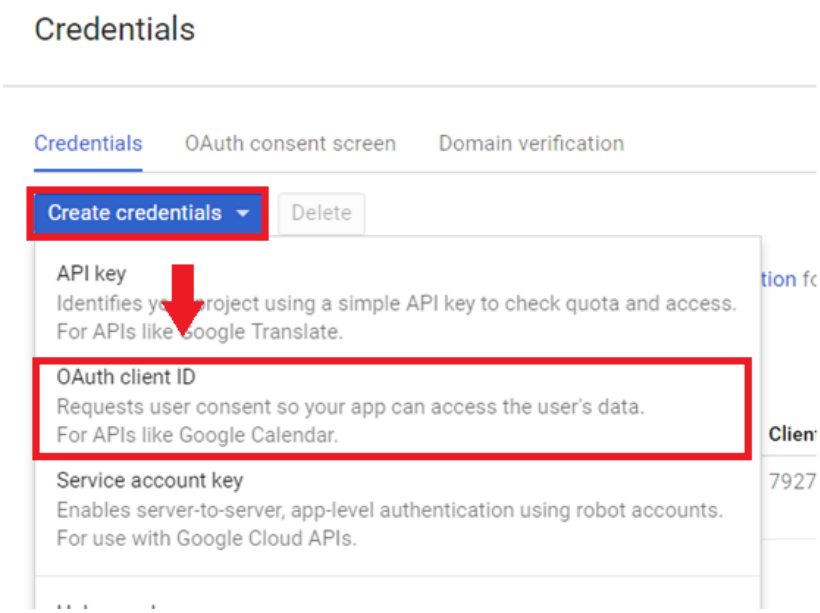
(2) Then click the **API Manager.**



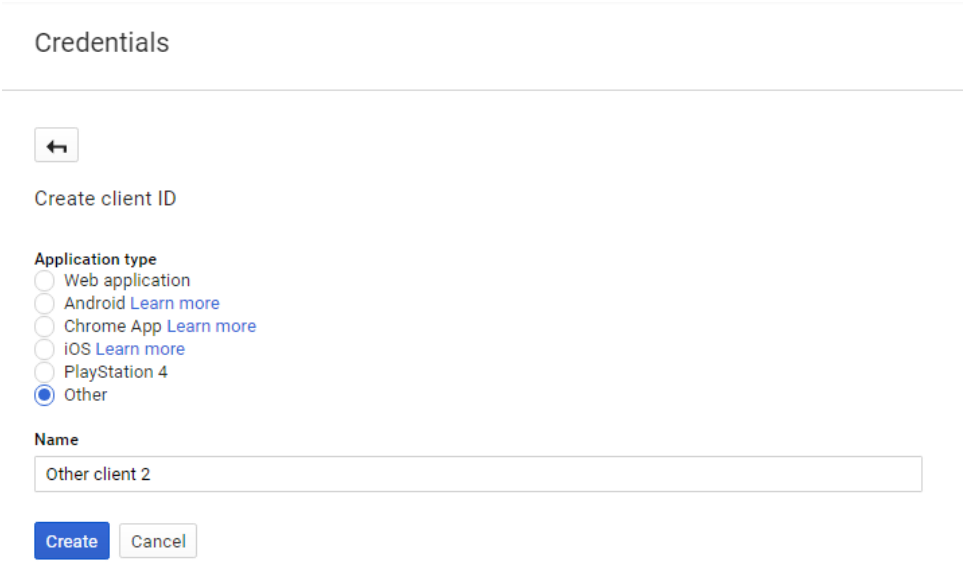
(3) In the **API Manager**, go to the **Credentials** page.



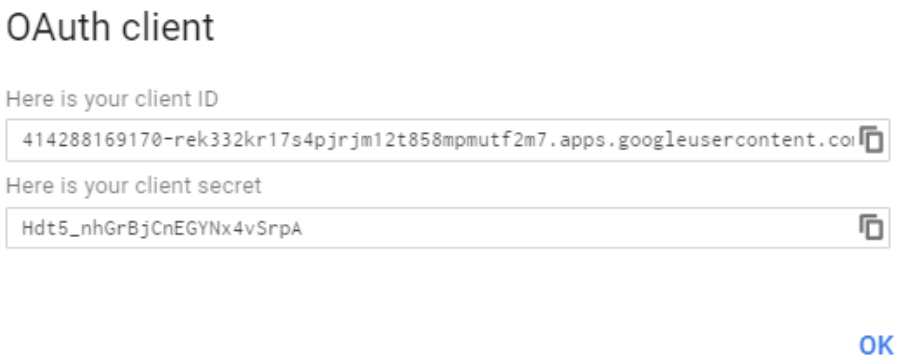
(4) Click **Create credentials** and select **OAuth client ID**.



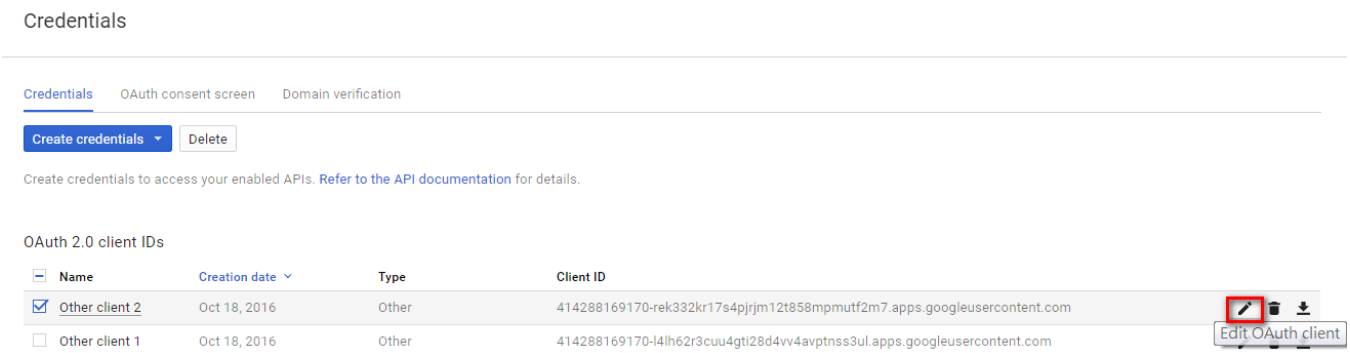
(5) Select **Web application**, specify the client ID **Name**, and click **Create**.

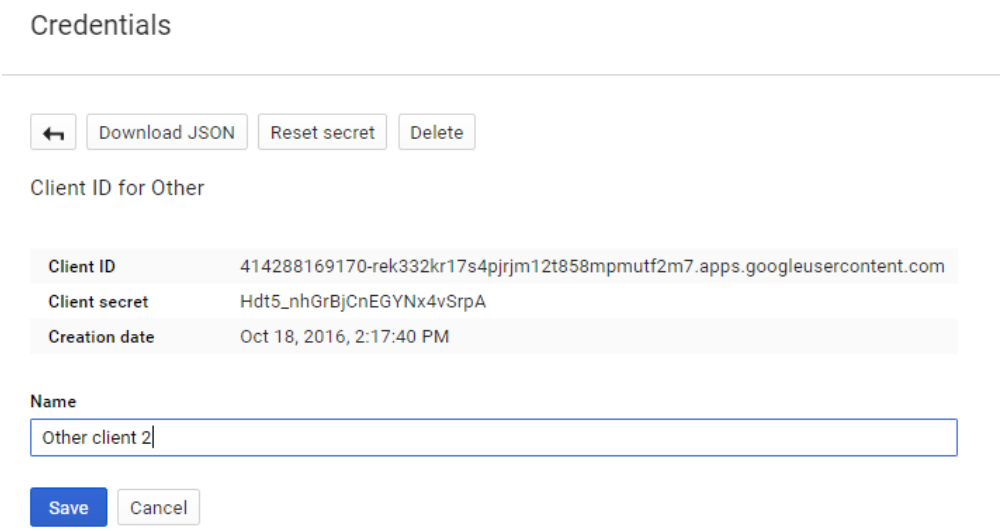


(6) The **client ID** and **client secret** will be displayed.

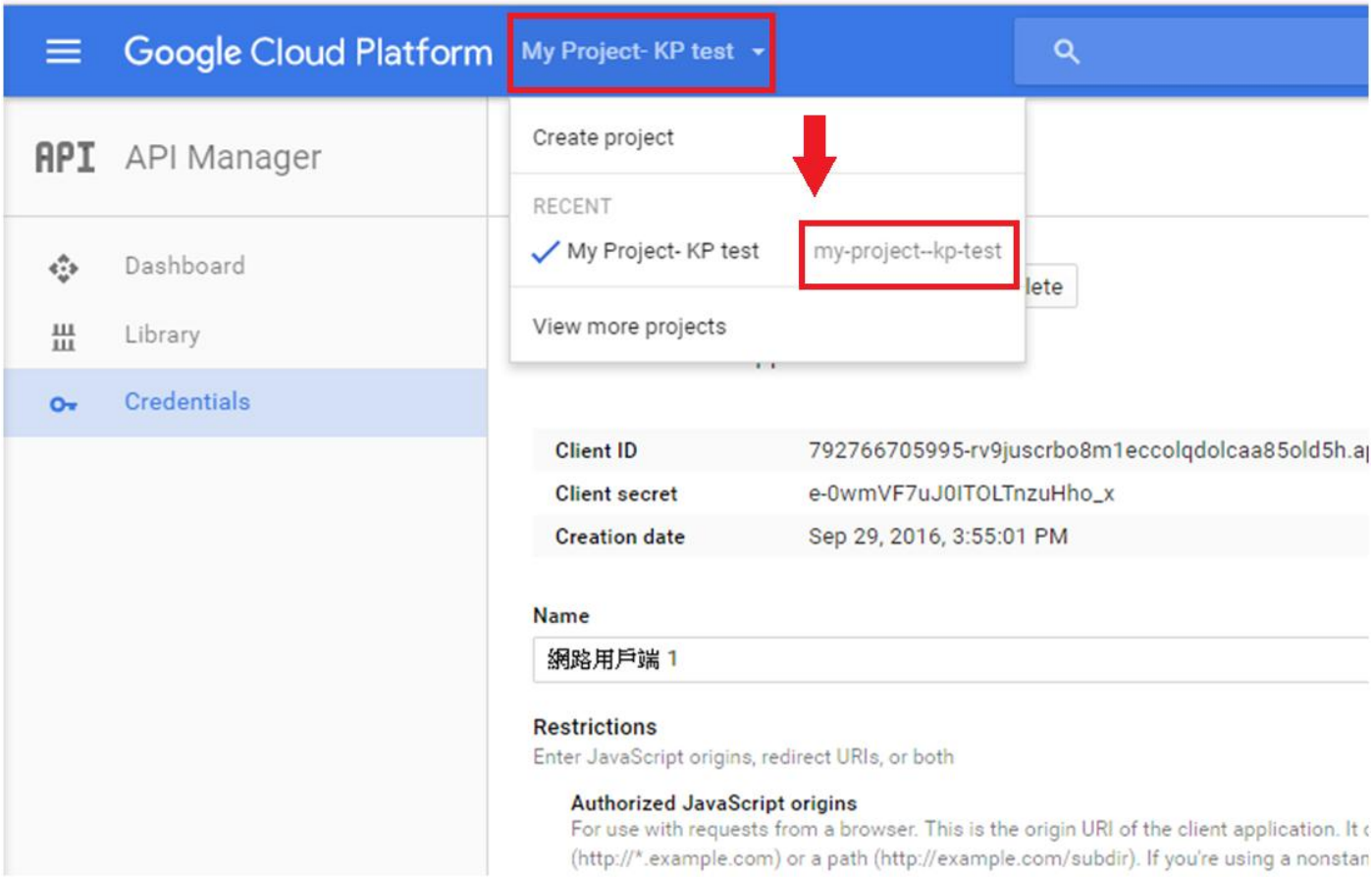


Click **OK** and you can check the access information later in the clients edit page.



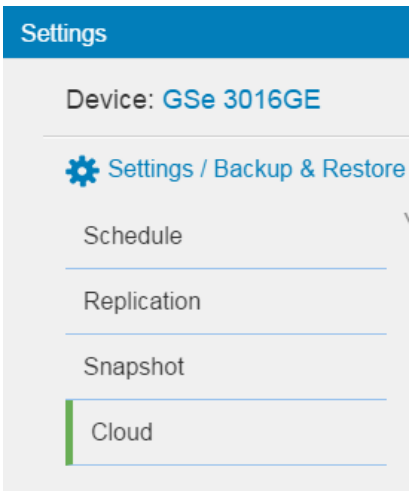


(7) To see the Project ID, click on your project name, and you can see the **project ID**.

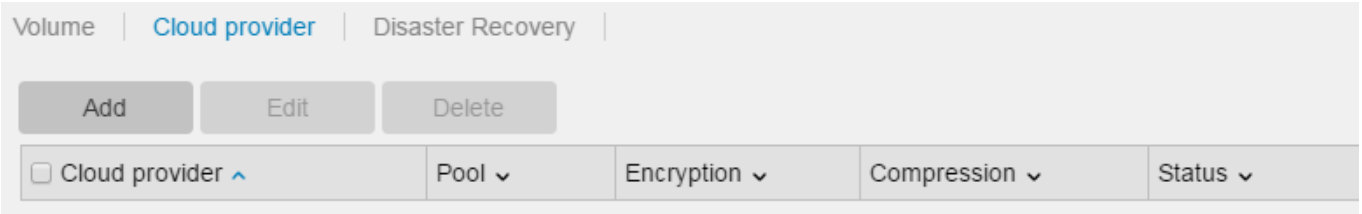


2. Connecting to GS

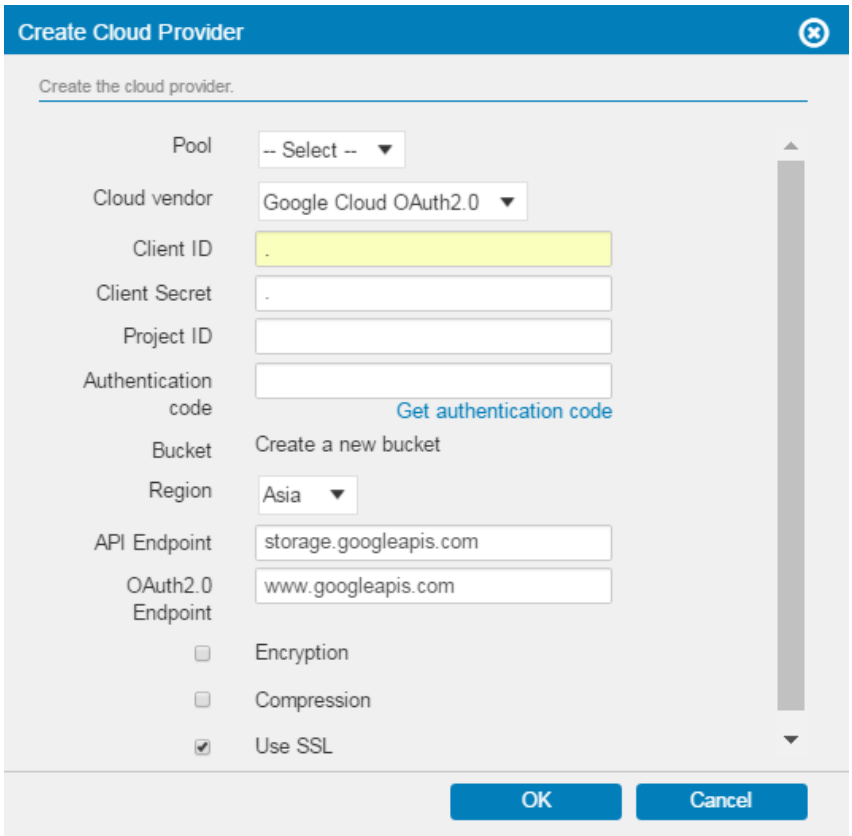
(1) Open EonOne, go to **Settings → Backup & Restore → Cloud**.



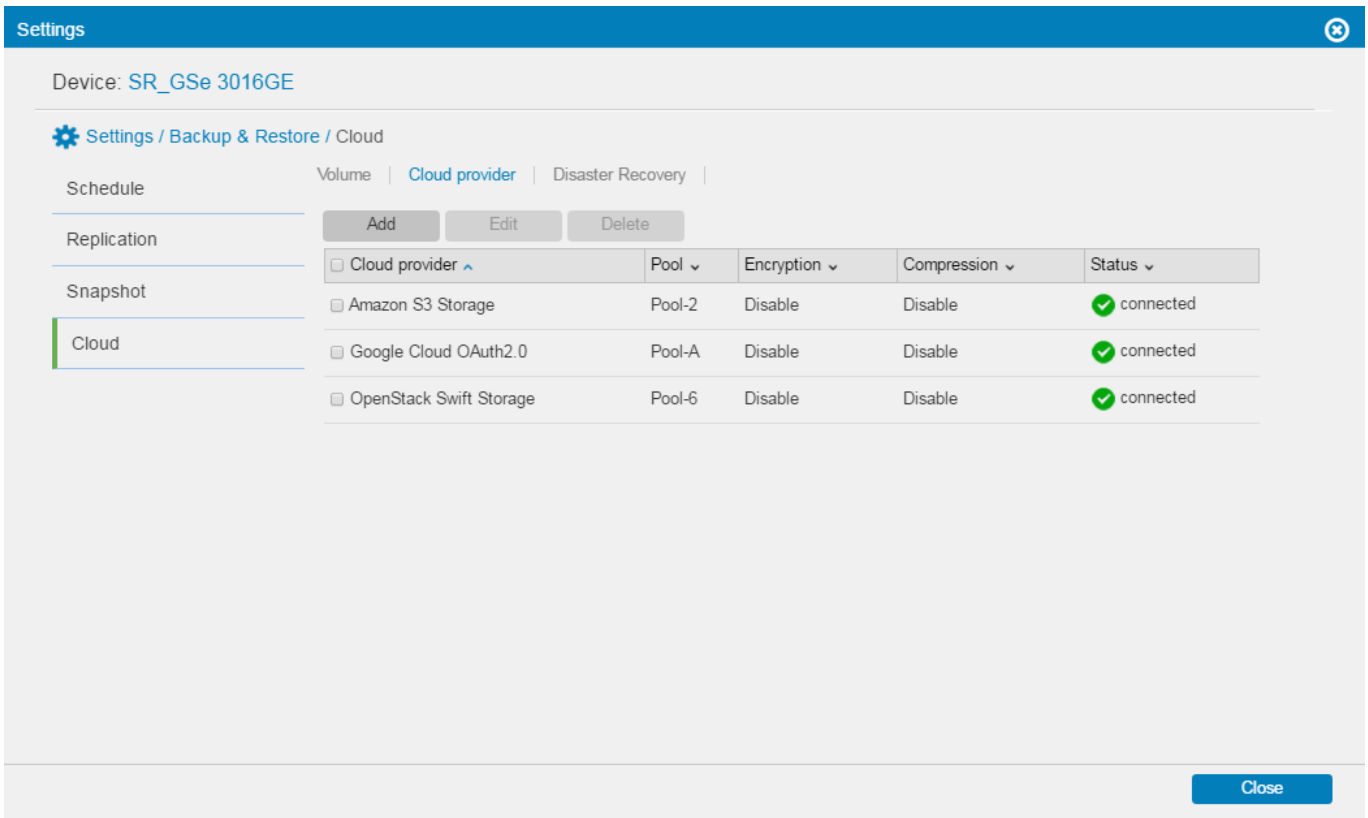
(2) On the Cloud page, switch to the **Cloud provider** page and click **Add**.



(3) Select a pool which you want to connect with a cloud provider, specify the **Cloud vender** and fill in the obtained access information. The **Region** is the location of the data center where your data will be saved. It can be any region but it is usually the region closest to you. Leave the **API Endpoint** and **OAuth2.0 Endpoint** as default and click **OK.**

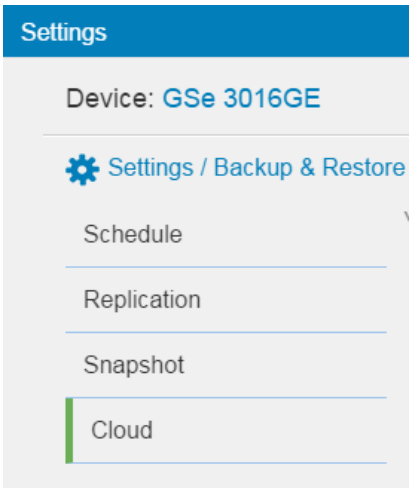


(4) The connected cloud service provider will then be listed.

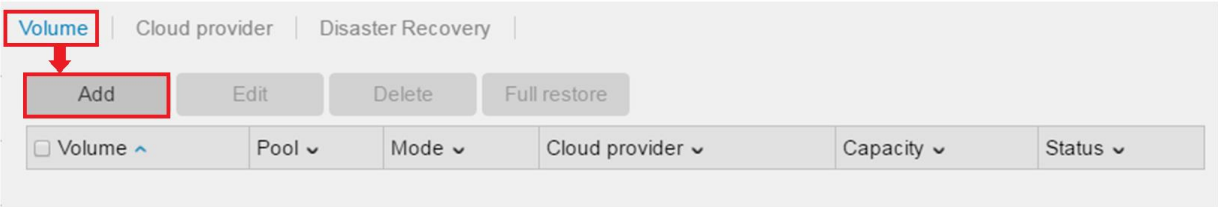


2-4. Creating cloud-integrated volumes

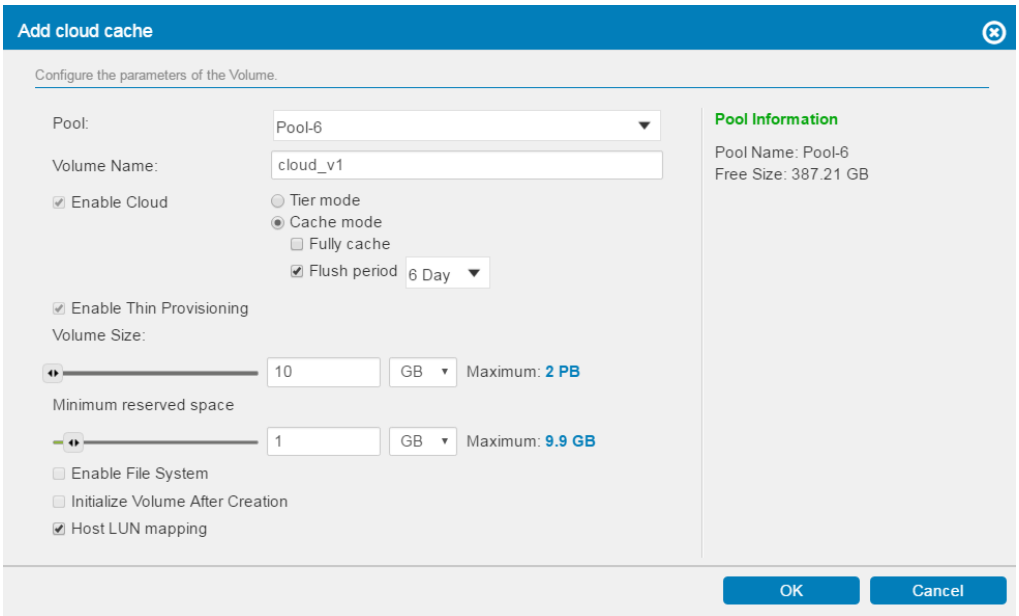
(1) Open EonOne, go to **Settings → Backup & Restore → Cloud**.



(2) On the Cloud page, switch to the **Volume** page and click **Add**.



(3) Configure the cloud-integrated Volume



Parameters for cloud-integrated volumes

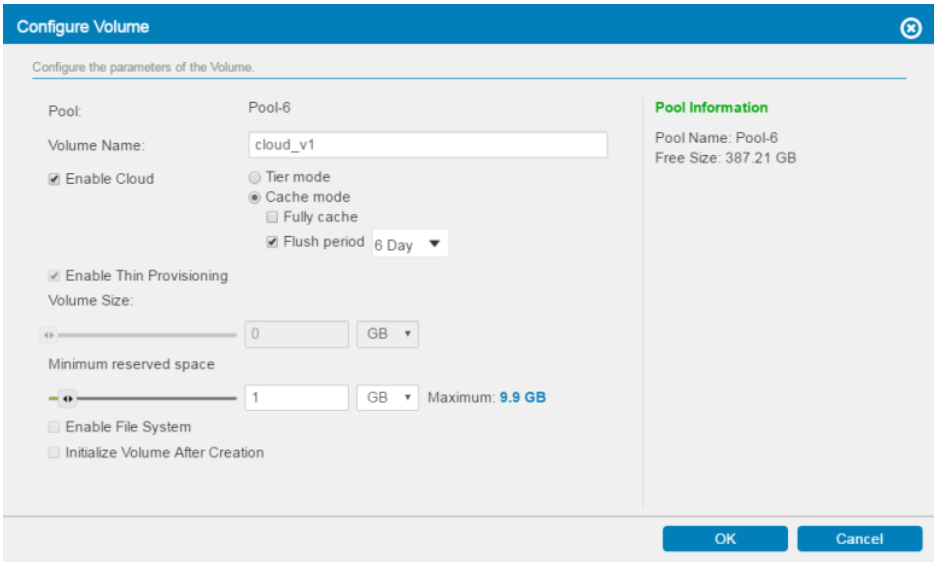
Pool	Choose the pool that has a mapping relationship with a cloud bucket.
Volume Name	Enter the name of the volume.
Volume Size	Specifies the size and unit of the volume. If Thin Provisioning is enabled, the total size of volumes can exceed the size of the pool. The minimum size of a volume is 10GB.
Enable Cloud-Tier mode	If users set the cloud-integrated volume to “Tier mode,” the cloud bucket will be seen as the lowest storage tier. Less frequently accessed data (normally called cold data) will be moved to the cloud when the cloud-integrated volume has reached its capacity threshold. For more information, consult the section **About the Cloud Gateway Features - Cloud Tiering mode**.
Enable Cloud-Cache mode	If users set the cloud-integrated volume to “Cache mode,” all data stored in the volume will be flushed to the cloud according to schedule. If fully cache is enabled, all data will be stored on both the cloud bucket and the local cloud-integrated volume after the flush operation. If fully cache is disabled, all data will be stored on the cloud bucket after flush operation, but only frequently accessed reading data will be available in the local cloud-integrated volume. No matter what method you select, all data will be stored in cloud after the last flush operation and users can recover data based on the last snapshot if necessary. Users can set the data flush schedule by configuring the “Flush Period.” For more information, consult the section **About the Cloud Gateway Features - Cloud Caching mode**
Thin Provisioning & Minimum Reserved Space	In order to expand storage capacity to the cloud buckets, thin-provisioning must be enabled in cloud-integrated volumes. Move the Minimum Reserved Space slide bar to set the percentage of the volume capacity that will be physically allocated as a safe reserve.
Enable File System	Users have to enable this option before creating a folder on the volume. The volume will be mounted to file system.
Host LUN mapping	Map the volume to hosts automatically.

Other Configurations for Cloud Enabled Volumes

Edit

The **Edit** button allows users to change the volume name, cloud enabled modes and minimum reserved space.

Switching cloud enabled mode from tier mode to cache mode is also available.



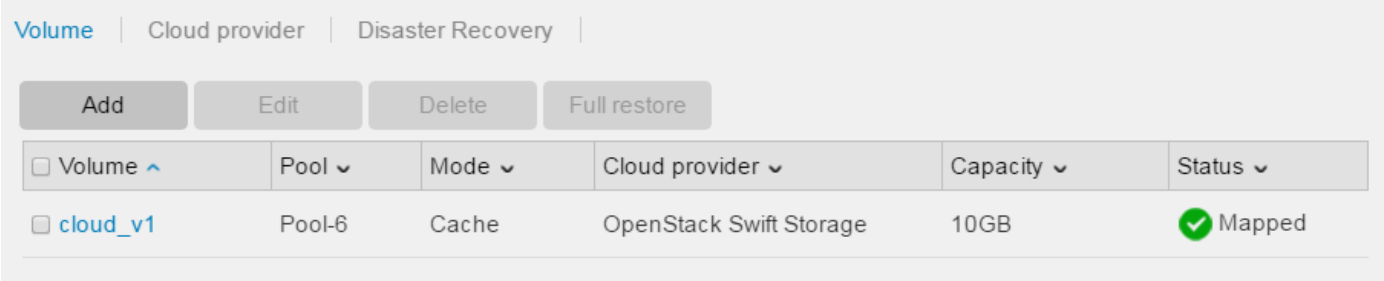
Delete

Select one or more cloud enabled volumes and click the **Delete** button, and the volume(s) will be deleted.

Full restore

This button only works with a cloud cache volume that has the “fully cache” option enabled. Since the cloud bucket has kept the last version of snapshot of the cloud cache volume, the full restore function rolls back the snapshot to recover the cloud cache volume.

(4) The volume will be listed.



Disaster Recovery

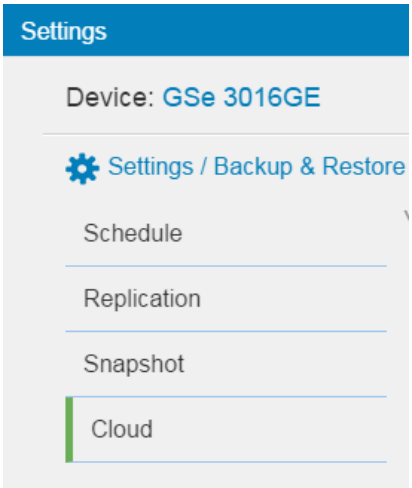
The disaster recovery process for cloud follows the steps described below:

Step 1. Configure bucket information and select the source data that needs to be recovered.

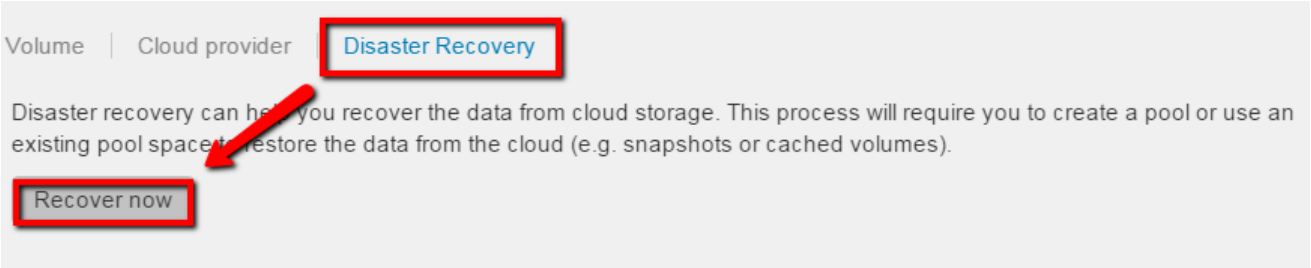
Step 2. Configure storage space.

3-1. Configuring bucket information

(1) Open EonOne, go to **Settings → Backup & Restore → Cloud**.



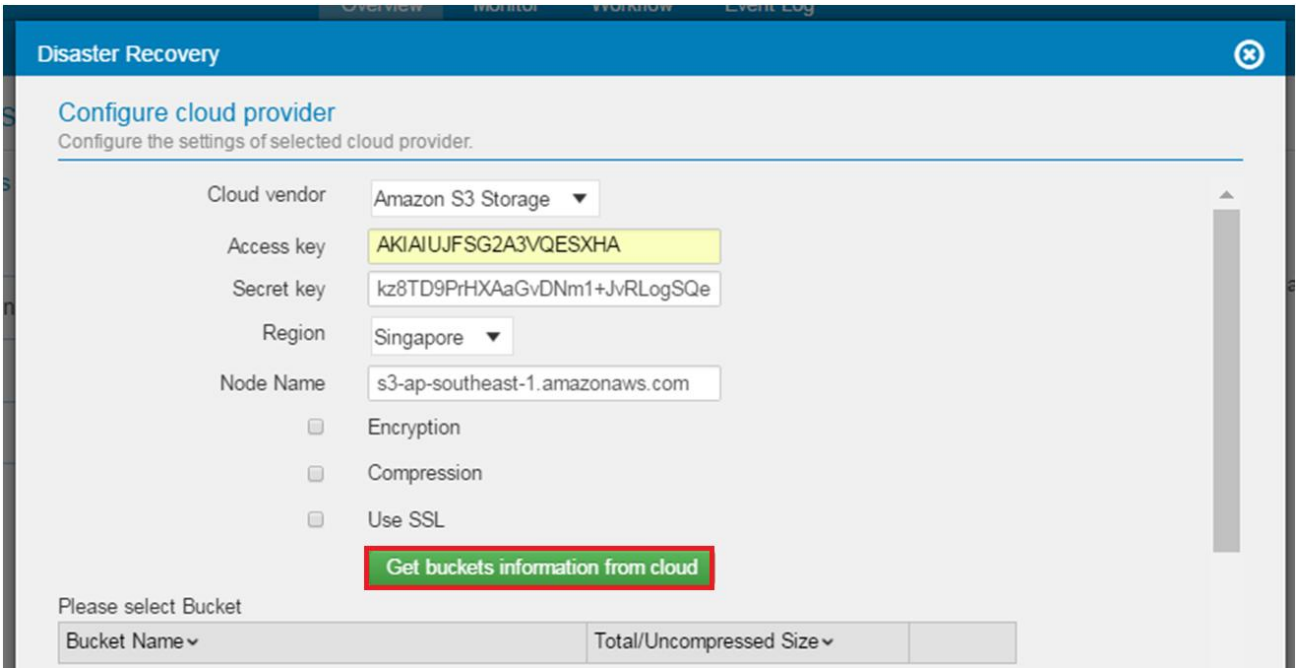
(2) On the Cloud page, switch to the **Disaster Recovery** page and click **Recover now.**



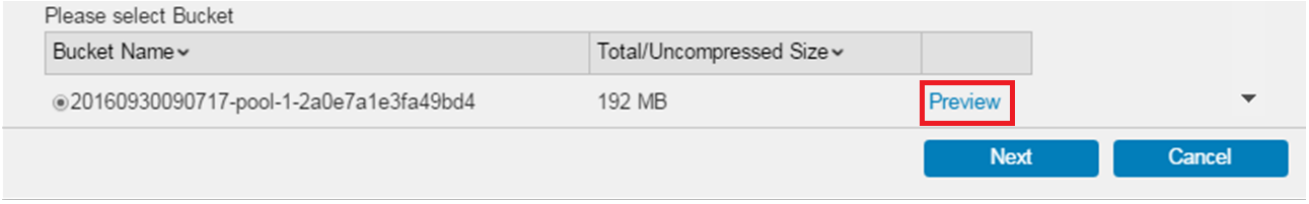
(3) In order to retrieve the bucket information, the system needs your cloud provider access privilege. Select your cloud provider. Enter the credentials and click the **Get bucket information from cloud** button.

The credential requirements may vary with different cloud providers. For example, to verify the user's identity, Amazon S3 needs a paired access key and secret key and Microsoft Azure needs endpoint and

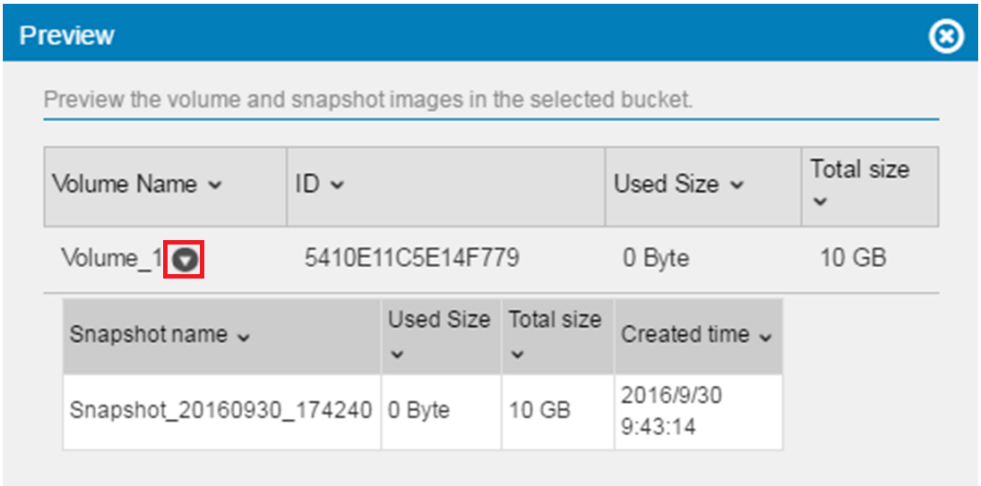
share key information.



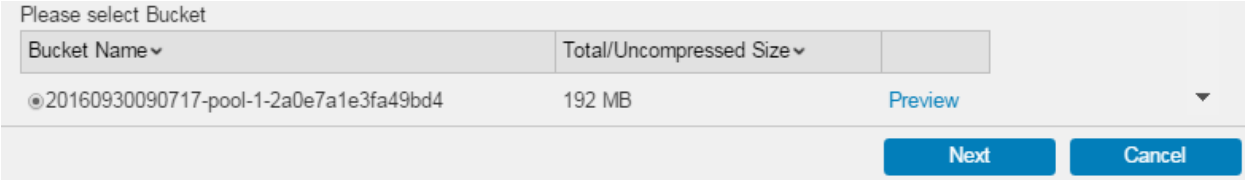
(4) The bucket information will be listed. Users can see the detailed information of the buckets by clicking the **Preview** button.



(5) The bucket preview page shows the information of the volumes in the bucket. You can click on the arrow icon to see the snapshots in the volumes.



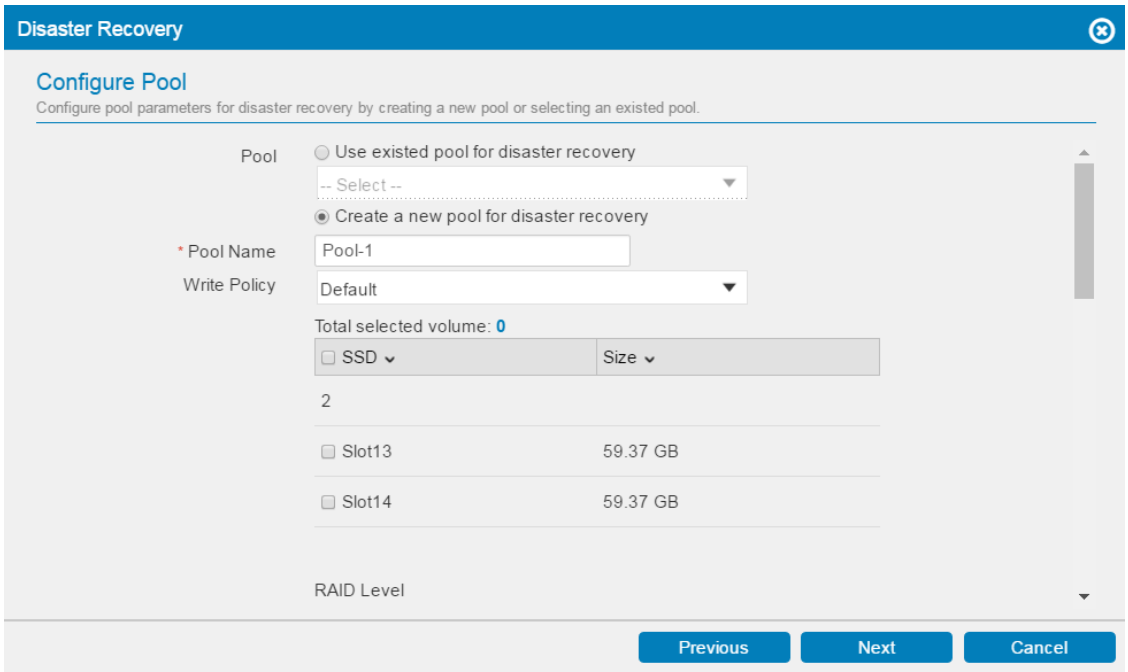
(6) Select the bucket that has the snapshot image that you want to roll back and click **Next**.



3-2. Configuring storage space

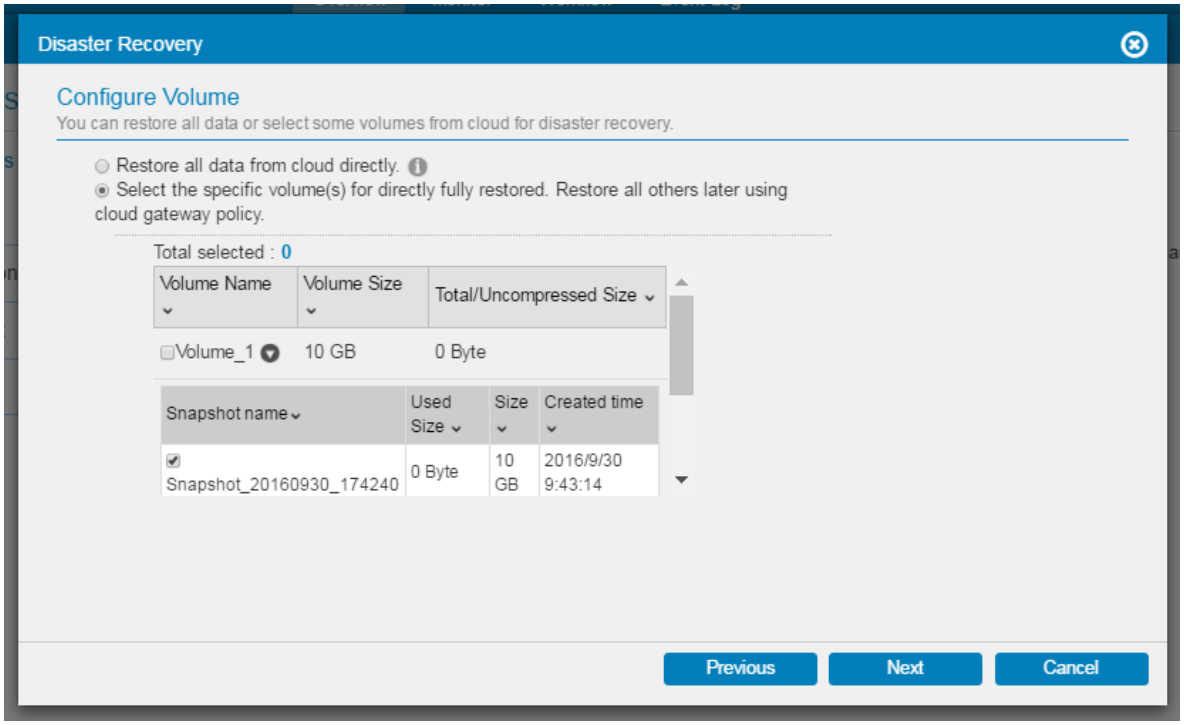
(1) Configure pool

Select an existing pool or create a new one. The disaster recovery process will create a new volume that claims capacity from the pool and then import the snapshot image to the new volume.



(2) Configure volume and data to be recovered

Users can choose to restore all data in the selected bucket or choose to restore specific volumes.



(3) Summary

Verify the configurations you just set on the summary page. Click **OK** to carry out the disaster recovery process or click **Previous** to modify the configuration.