

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.infotrend.com/global/Support/Support>

Headquarter (Asia / Taiwan)

Infotrend 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 Infotrend Sales Representative

[Email](#), [Technical Support](#), [Website](#)

India Infotrend Sales Representative

[Email](#), [Technical Support](#), [Website](#)

Oceania Infotrend Sales Representative

[Email](#), [Technical Support](#), [Website](#)

Japan

Infotrend 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

Infotrend Corporation

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

China

Infotrend 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](#)

Infotrend 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](#)

Infotrend 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](#)

Infotrend 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](#)

Infotrend 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

| | |
|---|-----------|
| Legal Information | 2 |
| Contact Information | 3 |
| Table of Contents | 5 |
| Preface | 6 |
| Audience | 6 |
| What's in This Guide | 6 |
| What You Should Know Before Reading | 6 |
| About the Cloud Gateway Features | 7 |
| 1-1. Cloud Tiering Mode | 7 |
| 1-2. Cloud Caching Mode | 8 |
| 1-2-1. Fully Cache | 8 |
| 1-2-2. Non-fully Cache | 8 |
| 1-3. Snapshot Backup | 9 |
| Using the cloud gateway features | 11 |
| 2-1. Synchronizing time in a time zone | 11 |
| 2-2. Creating a pool | 11 |
| 2-3. Connecting your pool with a cloud service provider | 12 |
| 2-3-1. Amazon S3 | 12 |
| 2-3-2. Aliyun Object Storage Service | 21 |
| 2-3-3. Microsoft Azure | 25 |
| 2-3-4. Openstack Swift | 29 |
| 2-3-5. Google Cloud | 31 |
| 2-4. Creating cloud-integrated volumes | 39 |
| Disaster Recovery | 42 |
| 3-1. Configuring bucket information | 42 |
| 3-2. Configuring storage space | 44 |

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 EonStor 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.

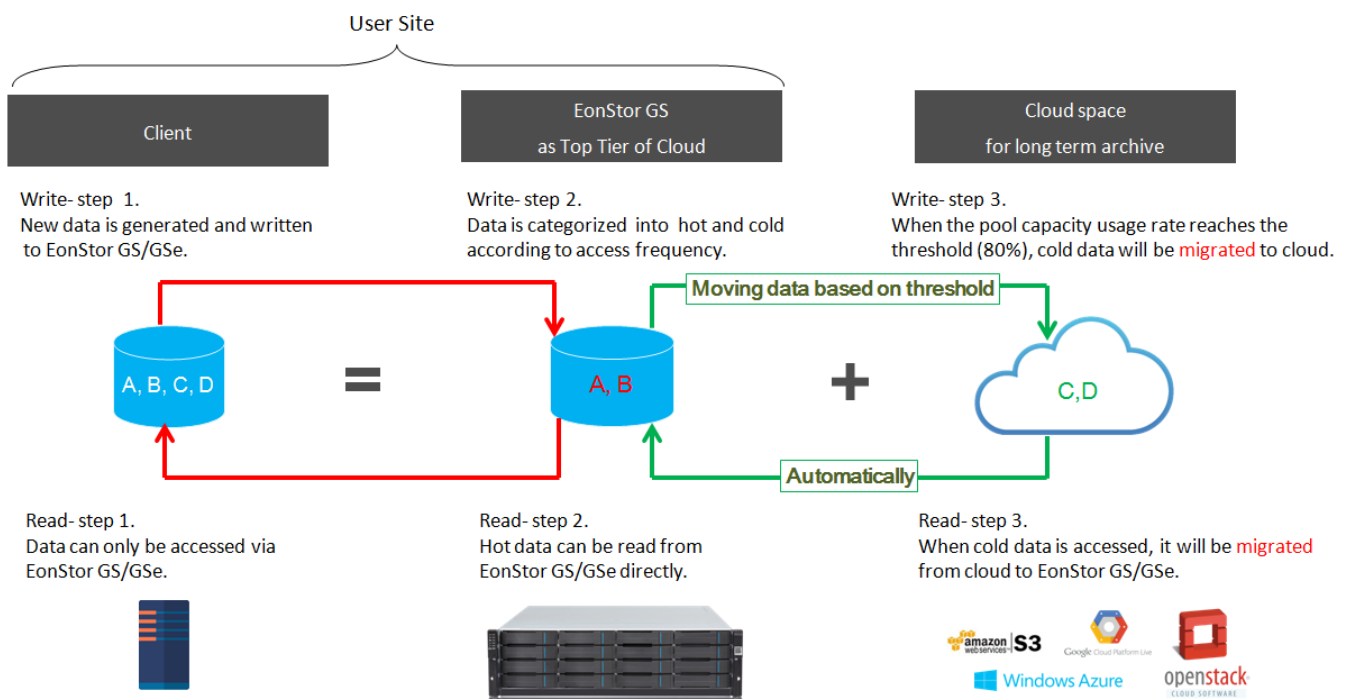
About the Cloud Gateway Features

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

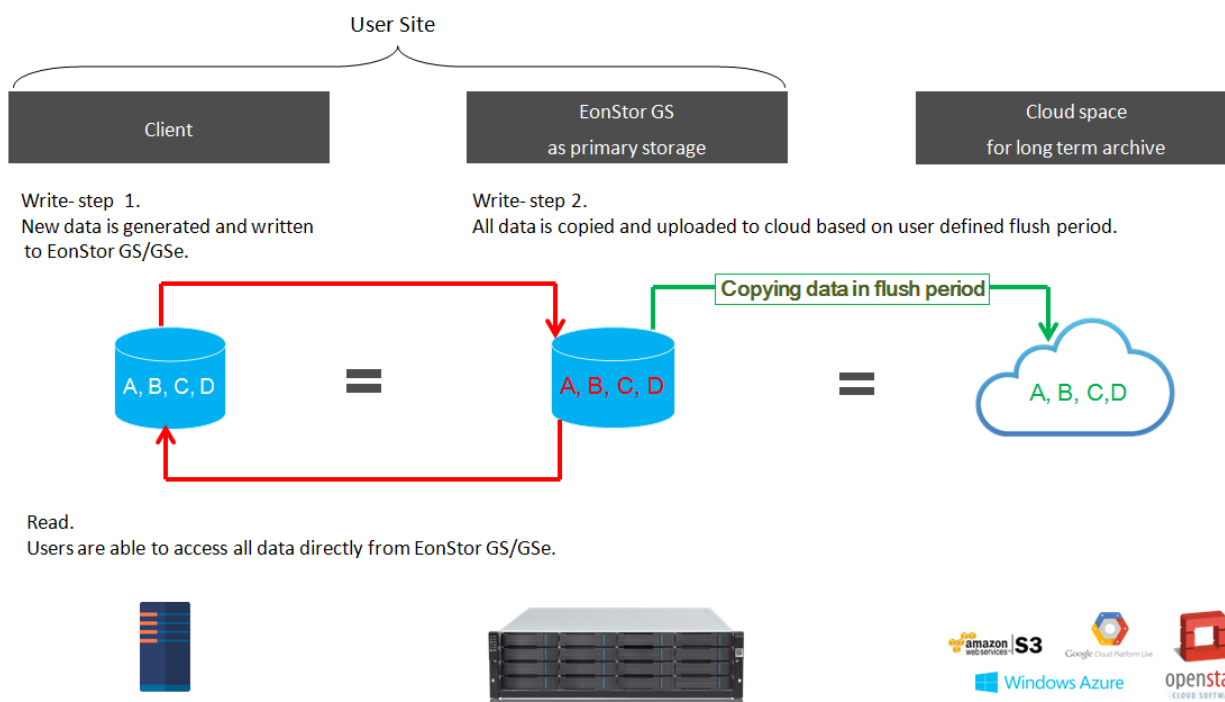
With the Cloud Tiering mode, a cloud bucket is used as a storage tier in the EonStor GS/GSe storage system for flexible capacity expansion and budget planning. The system itself keeps frequently accessed data (generally called hot data) in the local volume and moves the rest to the cloud tier. Therefore,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



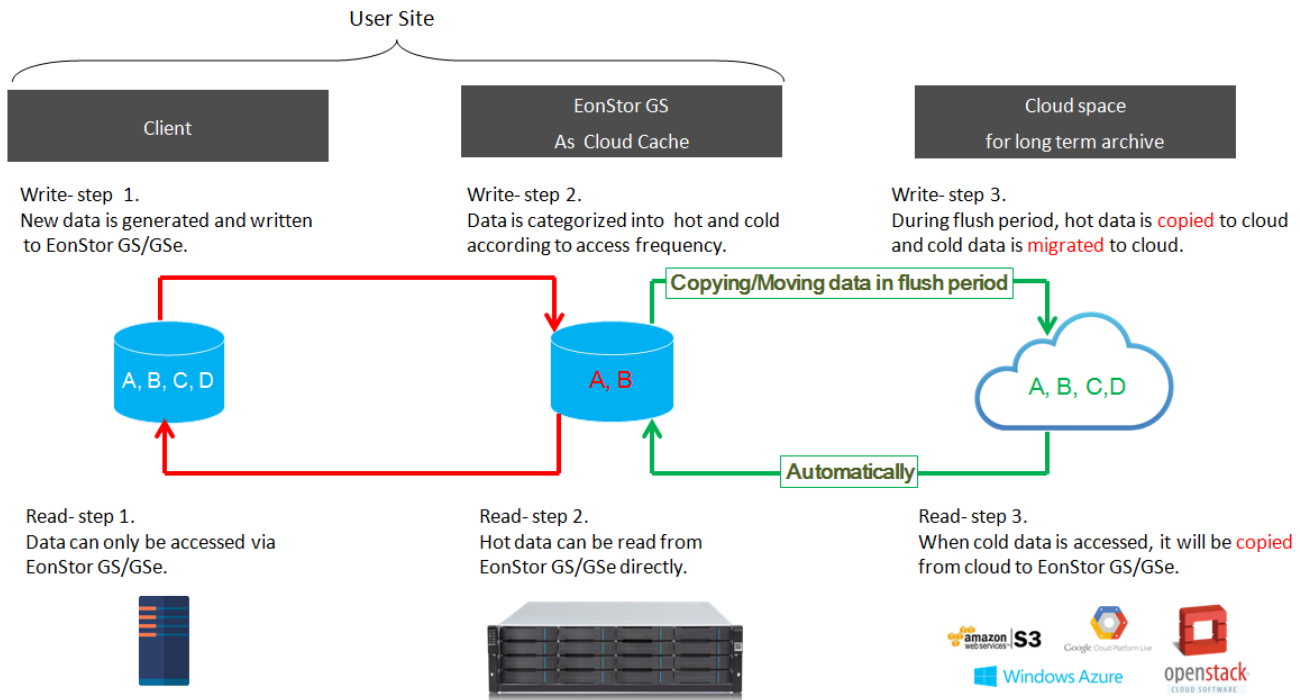
1-2. Cloud Caching Mode

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

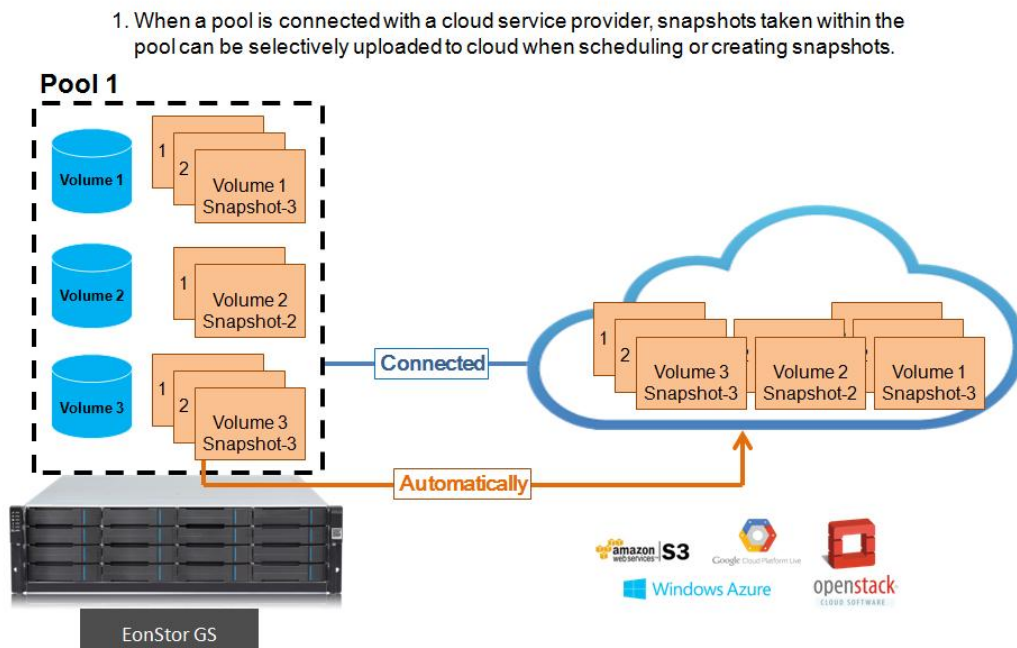


1-2-2. Non-fully Cache



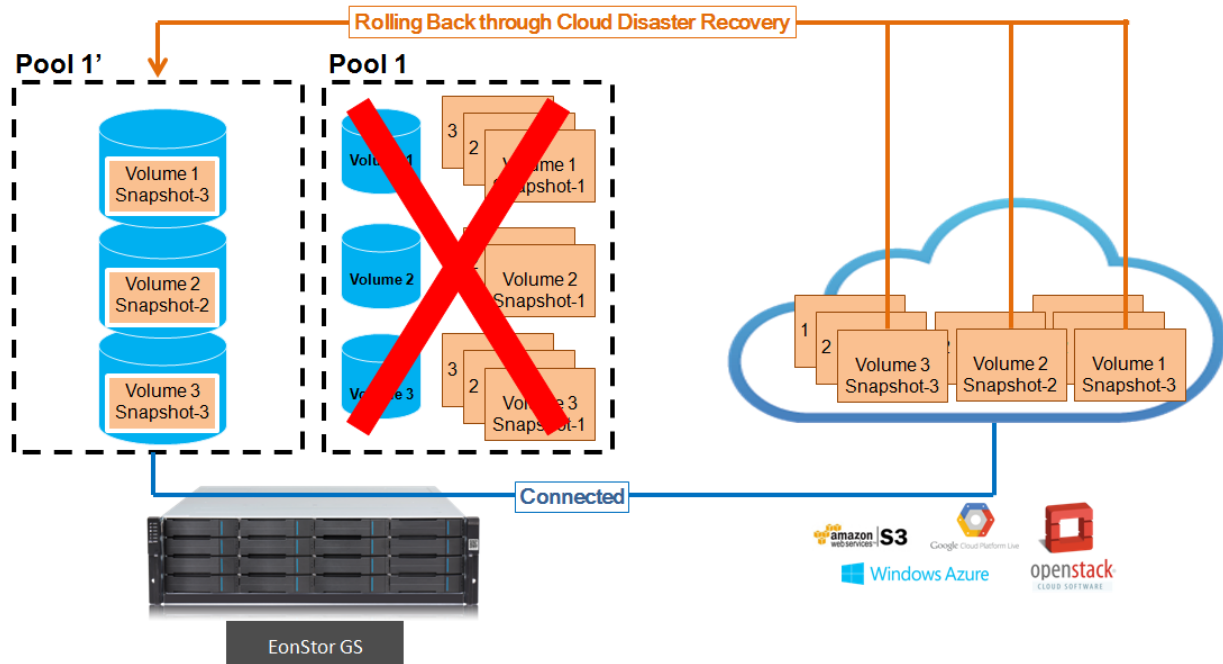
1-3. Snapshot Backup

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.



About the Cloud Gateway Features

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.

Settings

Device: GSe 3016GE

Settings / Storage / Pool

Volume

Pool

Logical drive

Drive

SSD cache

Create Pool Add Logical Drive Expand Pool Configure Pool More ▾

| Pool Name | Capacity | Usage | Status |
|-----------|-----------|---|-----------|
| Pool-2 | 418.92 GB | Used: 96 MB, Available: 418.83 GB 0.02% | ✓ On-line |
| Pool-3 | 418.92 GB | Used: 96 MB, Available: 418.83 GB 0.02% | ✓ On-line |
| Pool-4 | 418.92 GB | Used: 10.28 GB, Available: 408.64 GB 2.45% | ✓ On-line |

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

[2-3-1. Amazon S3](#)

[2-3-2. Aliyun Object Storage Service](#)

[2-3-3. Microsoft Azure](#)

[2-3-4. Openstack Swift](#)

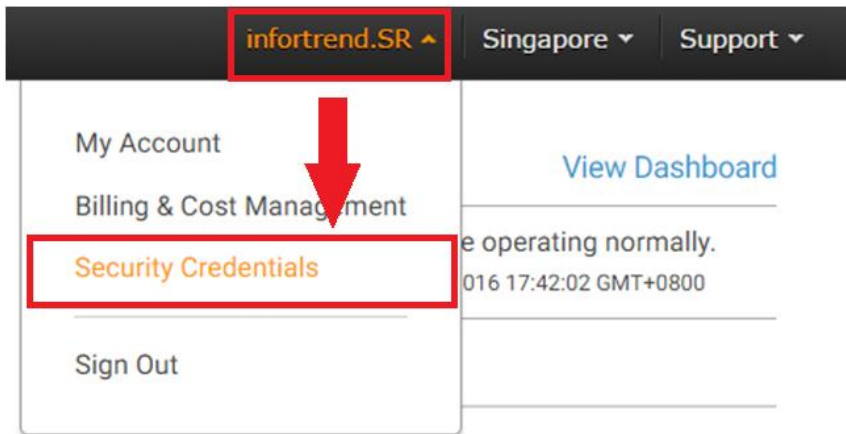
[2-3-5. Google Cloud](#)

2-3-1. Amazon S3

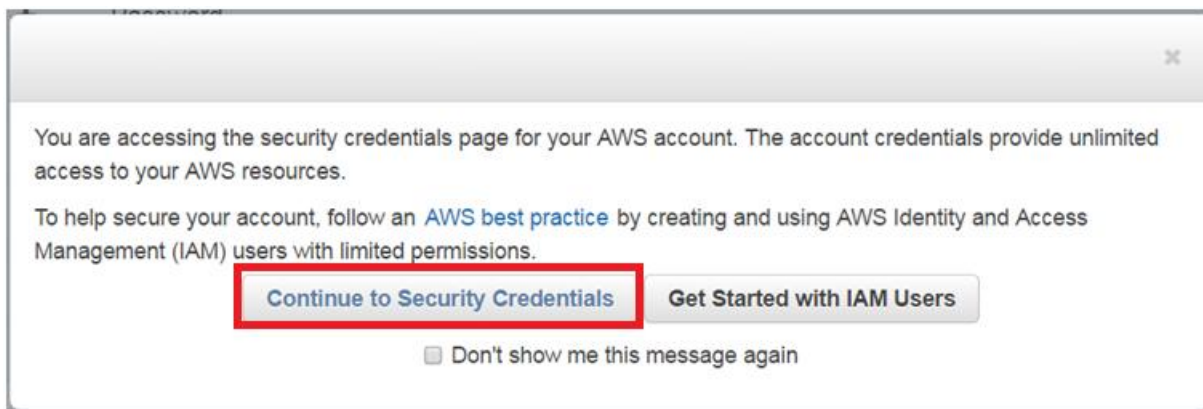
This section explains how to obtain access credentials and [create cloud buckets on Amazon S3 via EonOne](#). There are two ways to obtain the access credentials on Amazon S3, via [the root access keys](#) or [the IAM access keys](#).

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.

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

| | |
|---|---|
| + | Password |
| + | Multi-Factor Authentication (MFA) |
| + | Access Keys (Access Key ID and Secret Access Key) |
| + | CloudFront Key Pairs |
| + | X.509 Certificates |
| + | Account Identifiers |

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**.

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

+

 Password

+

 Multi-Factor Authentication (MFA)

-

 Access Keys (Access Key ID and Secret Access Key)

You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the [signing documentation](#). For your protection, store your access keys securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days.

Note: You can have a maximum of two access keys (active or inactive) at a time.

| Created | Deleted | Access Key ID | Last Used | Last Used Region | Last Used Service | Status | Actions |
|----------------------------------|---------|---------------|-----------|------------------|-------------------|--------|---------|
| <div>Create New Access Key</div> | | | | | | | |

(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.

Create Access Key

✔

Your access key (access key ID and secret access key) has been created successfully.

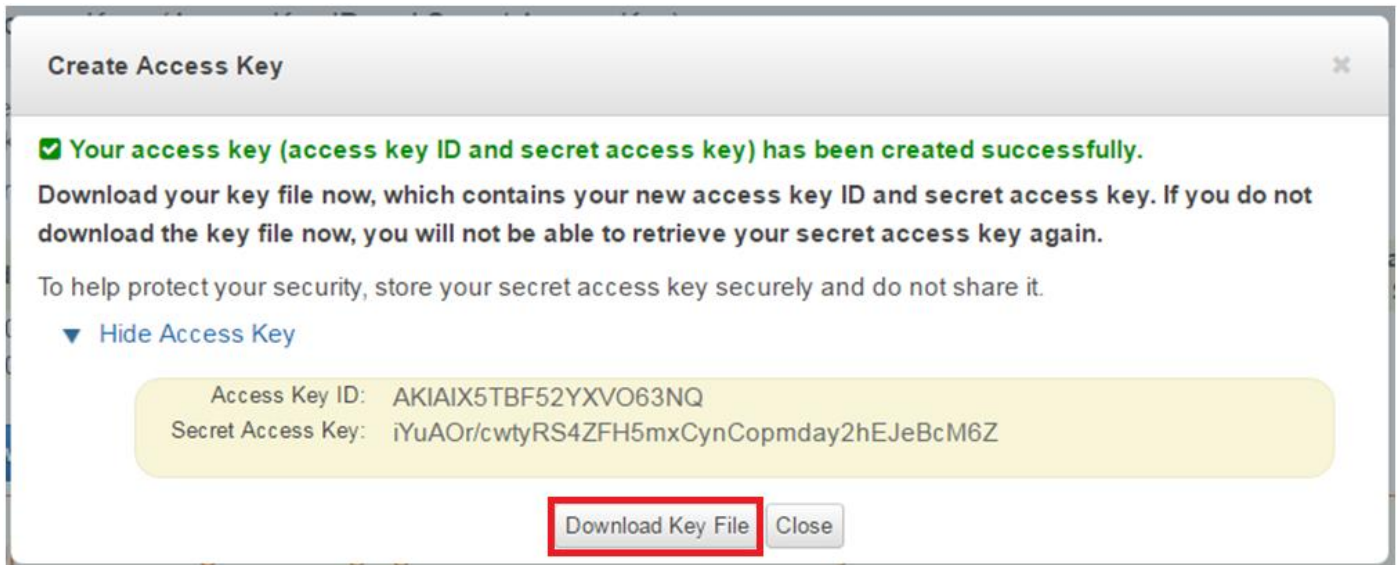
Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.

To help protect your security, store your secret access key securely and do not share it.

Show Access Key

Download Key File

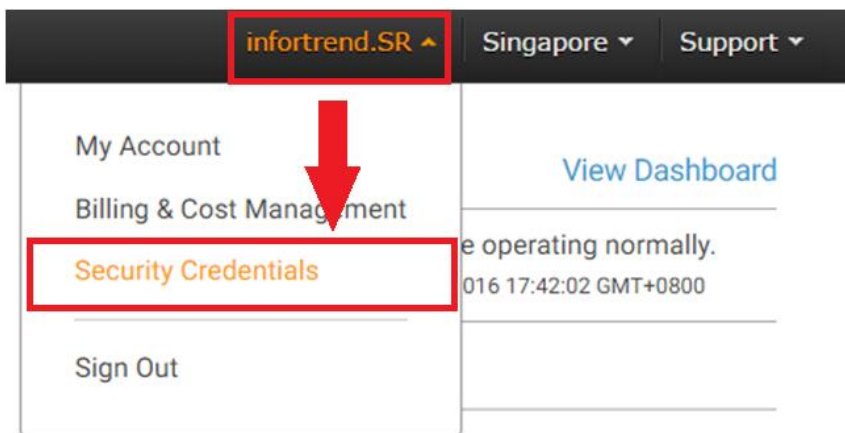
Close



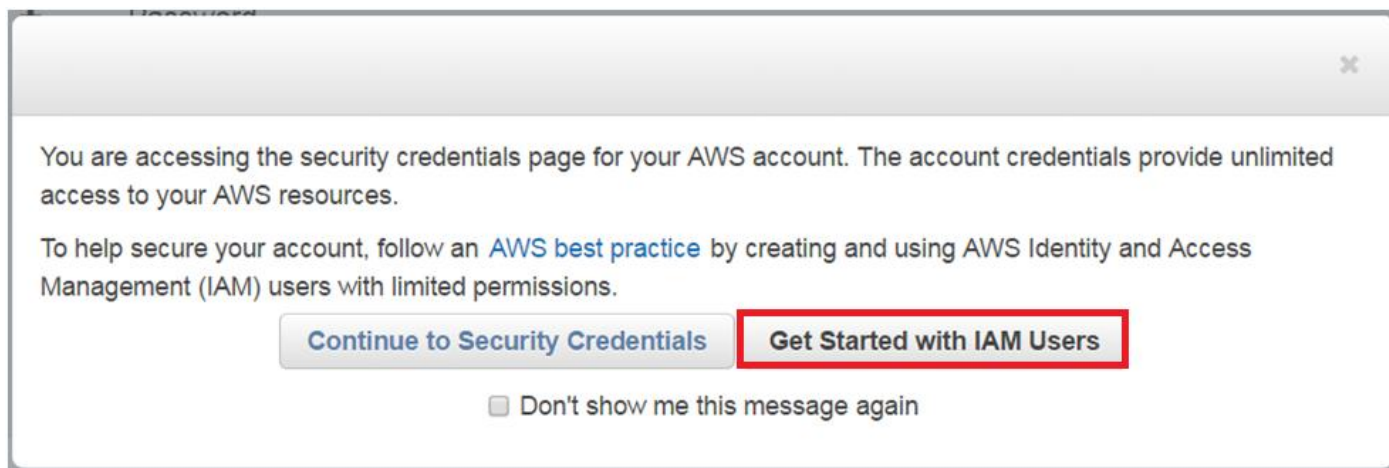
Attention! If you do not write down the key or download the key file to your computer before you click **Close** or **Cancel**, you will no longer be able to retrieve the secret key again. In such cases, the only thing you can do is deleting the pair of keys and then create new ones.

2. Retrieving IAM Access Keys

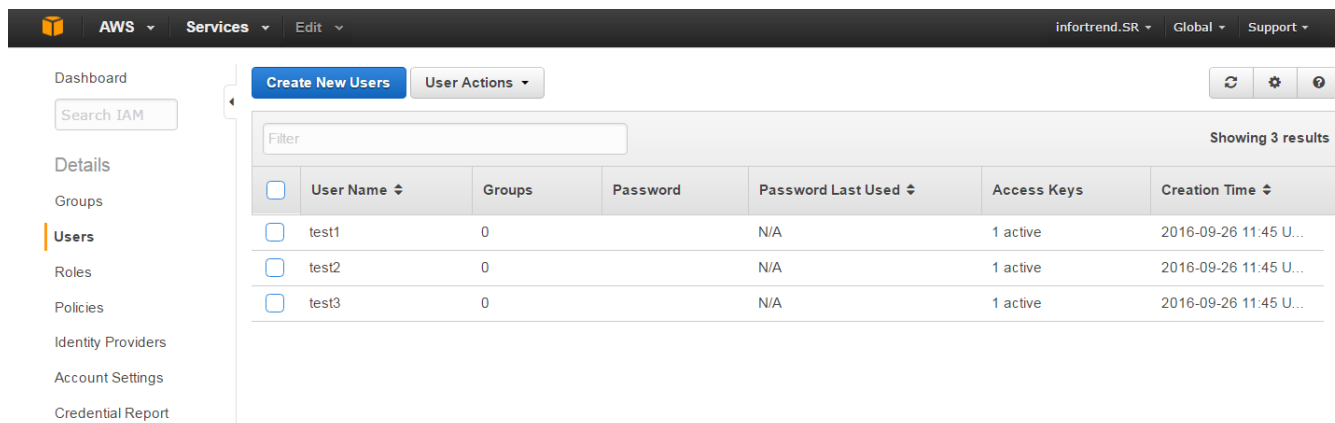
(1) Register an account and log into the account. After login, click **Security Credentials** in the username's drop-down list.



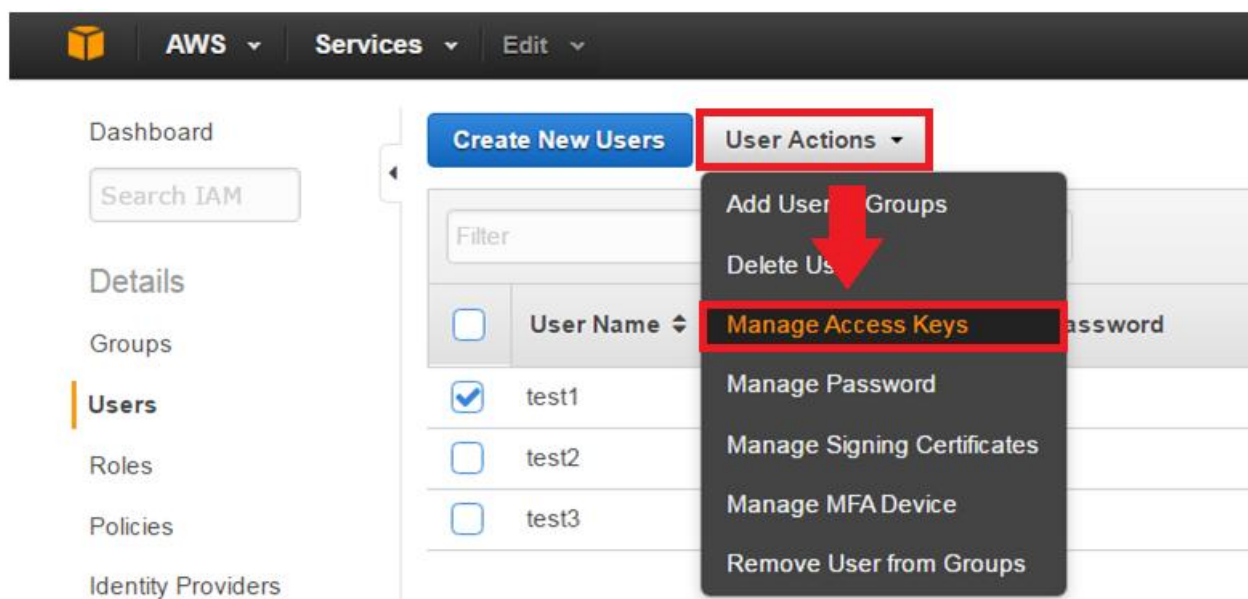
(2) Click the **Get Started with IAM Users** button.



(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.

Manage Access Keys ✕

Use access keys to make secure REST or Query protocol requests to any AWS service API.

| Access Key ID | Created | Last Used | Last Used Service | Last Used Region | Status |
|----------------------|---------------------------|-----------|-------------------|------------------|---|
| AKIAJAH4736ARUVTMH5Q | 2016-09-26 11:45 UTC+0800 | N/A | N/A | N/A | Active (Make Inactive Delete) |

Note: For your protection, you should never share your secret keys with anyone. In addition, industry best practice recommends frequent key rotation.
› [Learn more about Access Keys](#)

[Cancel](#) [Create Access Key](#)

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.

Manage Access Keys ✕

Use access keys to make secure REST or Query protocol requests to any AWS service API.

| Access Key ID | Created | Last Used | Last Used Service | Last Used Region | Status |
|----------------------|---------------------------|-----------|-------------------|------------------|---|
| AKIAJAH4736ARUVTMH5Q | 2016-09-26 11:45 UTC+0800 | N/A | N/A | N/A | Active (Make Inactive Delete) |

Note: For your protection, you should never share your secret keys with anyone. In addition, industry best practice recommends frequent key rotation.
› [Learn more about Access Keys](#)

[Cancel](#) [Create Access Key](#)

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

Manage 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.

▼ Hide User Security Credentials



test1

Access Key ID: AKIAJTTJR3CEHR4PZGBA

Secret Access Key: A6nhILLnhk1XQbk0POM4A7YzNTe5zOAGktIHfRnQ

Close

Download Credentials

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.

The screenshot shows the AWS IAM console interface. At the top, there is a navigation bar with the AWS logo, 'AWS' dropdown, 'Services' dropdown, and 'Edit' dropdown. On the left, there is a sidebar with navigation links: Dashboard, Search IAM, Details, Groups, Users (highlighted with an orange bar), Roles, Policies, Identity Providers, and Account Settings. The main content area has a 'Create New Users' button and a 'User Actions' dropdown. Below these is a table with a 'Filter' input field. The table has columns for 'User Name', 'Groups', and 'Password'. The first row is highlighted with a red box and contains the user 'test1' with 0 groups. The second row is 'test2' with 0 groups, and the third row is 'test3' with 0 groups.

| | User Name ↕ | Groups | Password |
|--------------------------|-------------|--------|----------|
| <input type="checkbox"/> | test1 | 0 | |
| <input type="checkbox"/> | test2 | 0 | |
| <input type="checkbox"/> | test3 | 0 | |

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

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like Dashboard, Search IAM, Details, Groups, Users, Roles, Policies, Identity Providers, Account Settings, Credential Report, and Encryption Keys. The 'Users' section is active. The main content area shows the configuration for user 'test1'. Under the 'Summary' tab, details like User ARN, Has Password, Groups, Path, and Creation Time are listed. Below this, there are tabs for Groups, Permissions, Security Credentials, and Access Advisor. The 'Permissions' tab is selected and highlighted with a red box. A red arrow points from this tab to the 'Attach Policy' button, which is also highlighted with a red box. The 'Managed Policies' section below shows a message: 'There are no managed policies attached to this user.'

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

The screenshot shows the 'Attach Policy' page. At the top, it says 'Select one or more policies to attach. Each user can have up to 10 policies attached.' Below this is a table of policies. The search filter is set to 'amazons3'. The table has columns for Policy Name, Attached Entities, Creation Time, and Edited Time. The 'AmazonS3FullAccess' policy is selected with a checkbox, and the 'AmazonS3ReadOnlyAccess' policy is not selected. A red box highlights the 'AmazonS3FullAccess' row, and a red arrow points to the checkbox.

| | Policy Name | Attached Entities | Creation Time | Edited Time |
|-------------------------------------|------------------------|-------------------|---------------------------|--------------------------|
| <input checked="" type="checkbox"/> | AmazonS3FullAccess | 1 | 2015-02-07 02:40 UTC+0800 | 2015-02-07 02:40 UTC+... |
| <input type="checkbox"/> | AmazonS3ReadOnlyAccess | 0 | 2015-02-07 02:40 UTC+0800 | 2015-02-07 02:40 UTC+... |


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

Groups | **Permissions** | Security Credentials | Access Advisor

Managed Policies ^

The following managed policies are attached to this user. You can attach up to 10 managed policies.

[Attach Policy](#)

| Policy Name | Actions |
|--|---|
|  AmazonS3FullAccess | Show Policy Detach Policy Simulate Policy |


Inline Policies v

3. Connecting to GS

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

Settings

Device: GSe 3016GE

 [Settings / Backup & Restore](#)

[Schedule](#)

[Replication](#)

[Snapshot](#)

[Cloud](#)

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

Volume | **Cloud provider** | Disaster Recovery

[Add](#) [Edit](#) [Delete](#)

| | | | | |
|--|---------------------|---------------------------|----------------------------|-----------------------|
| <input type="checkbox"/> Cloud provider ^ | Pool v | Encryption v | Compression v | Status v |
|--|---------------------|---------------------------|----------------------------|-----------------------|

(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**.

Create Cloud Provider

Create the cloud provider.

Pool

Pool-1 (35E556D01EF0B38F)

Cloud vendor

Amazon S3 Storage

Access key

AKIAIUJFSG2A3VQESXHA

Secret key

kz8TD9PrHXAaGvDNm1+JvRLogSQe

Region

Singapore

Node Name

s3-ap-southeast-1.amazonaws.com

Bucket

Create a new bucket

Encryption

☐

Compression

☐

Use SSL

☐

OK

Cancel

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

Settings

Device: GSe 3016GE

Settings / Backup & Restore / Cloud

Schedule

Volume

Cloud provider

Disaster Recovery

Replication

Snapshot

Cloud

Add

Edit

Delete

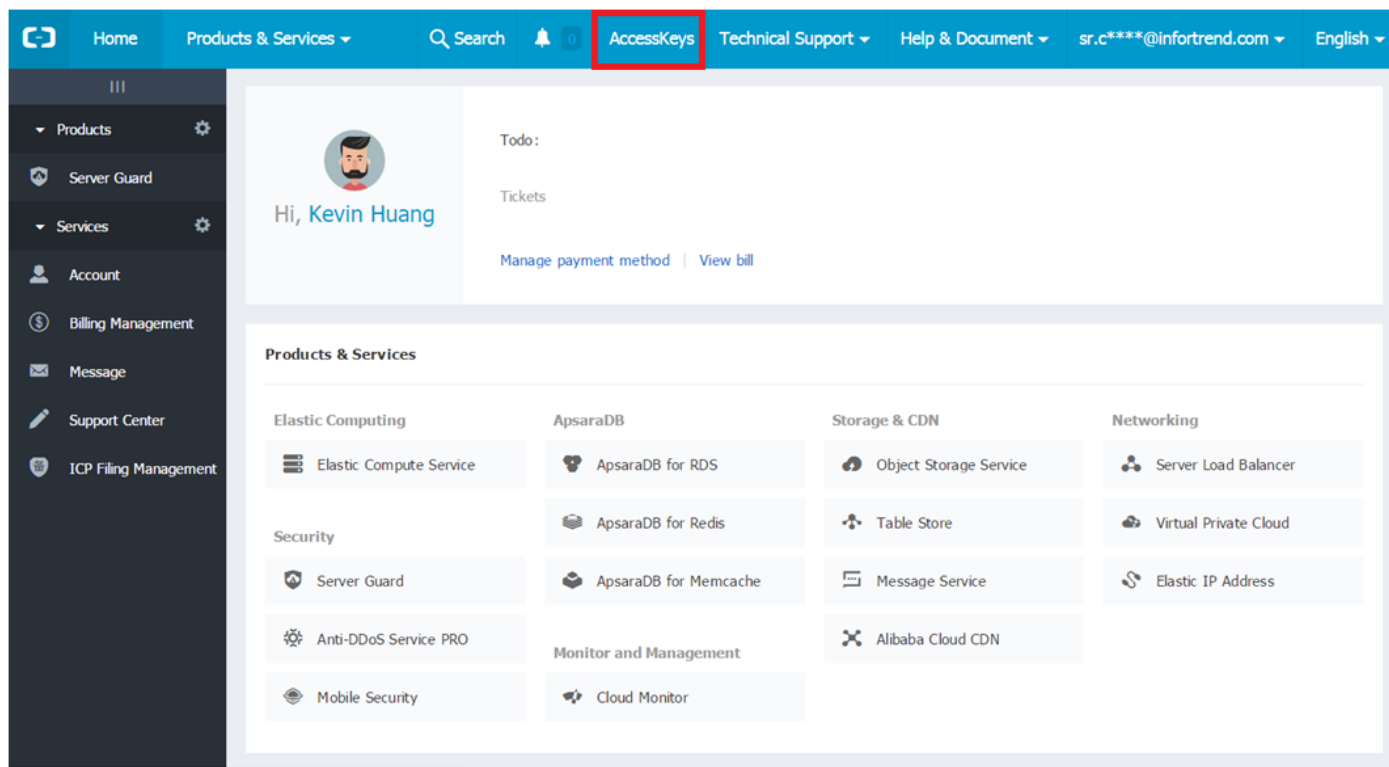
| <input type="checkbox"/> Cloud provider ^ | Pool v | Encryption v | Compression v | Status v |
|--|-----------|--------------|---------------|------------------------|
| <input type="checkbox"/> Amazon S3 Storage | Pool-s3-1 | Disable | Disable | connected |

2-3-2. Aliyun Object Storage Service

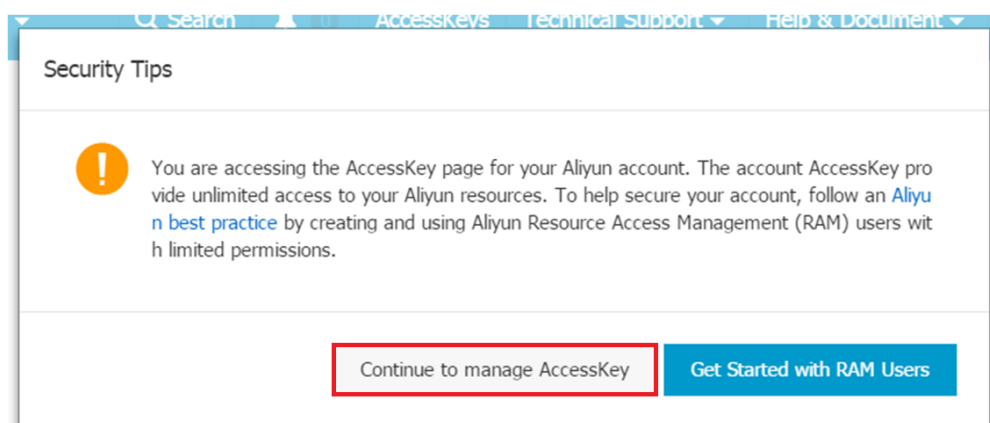
This section explains how to [obtain access credentials](#) and [create cloud buckets on Aliyun OSS via EonOne](#).

1. Retrieving access information

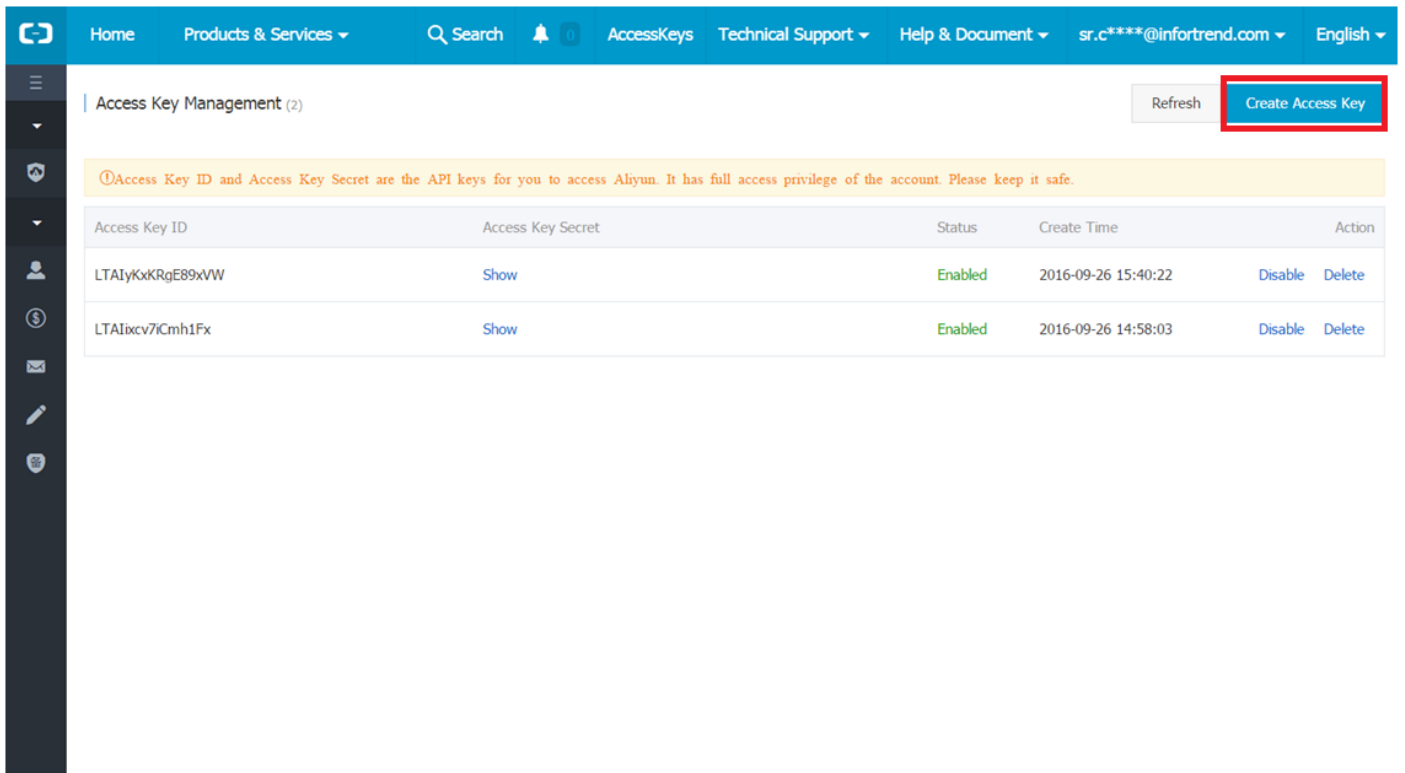
(1) Create and log into your account. After login, click the **AccessKeys** button at the tool bar on the top.



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



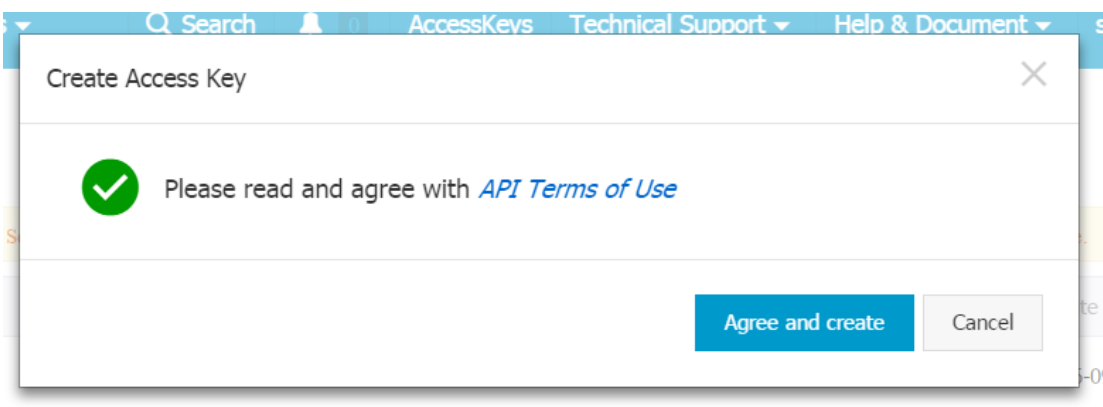
(3) This will lead you to the access key management page. On this page, you can click **Show** to have a hidden Access Key Secret displayed or create a new pair of Access Key ID and Access Key Secret by clicking **Create Access Key**.



The screenshot shows the 'Access Key Management' page. At the top, there is a navigation bar with 'Home', 'Products & Services', 'Search', 'AccessKeys', 'Technical Support', and 'Help & Document'. The user is logged in as 'sr.c****@infortrend.com'. The page title is 'Access Key Management (2)'. A yellow warning banner states: '①Access Key ID and Access Key Secret are the API keys for you to access Aliyun. It has full access privilege of the account. Please keep it safe.' Below this is a table with columns: Access Key ID, Access Key Secret, Status, Create Time, and Action. Two access keys are listed, both with status 'Enabled'. The 'Create Access Key' button in the top right corner is highlighted with a red box.

| Access Key ID | Access Key Secret | Status | Create Time | Action |
|------------------|-------------------|---------|---------------------|----------------|
| LTAIyKxKRgE89xVW | Show | Enabled | 2016-09-26 15:40:22 | Disable Delete |
| LTAIxcv7iCmh1Fx | Show | Enabled | 2016-09-26 14:58:03 | Disable Delete |

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



The screenshot shows a 'Create Access Key' dialog box. It contains a green checkmark icon and the text 'Please read and agree with [API Terms of Use](#)'. At the bottom right, there are two buttons: 'Agree and create' (highlighted) and 'Cancel'.

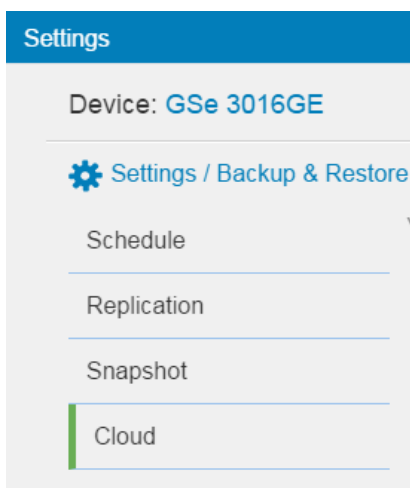
(5) After the new pair of access keys are generated, click **Show** to see the Access Key Secret.

① Access Key ID and Access Key Secret are the API keys for you to access Aliyun. It has full access privilege on

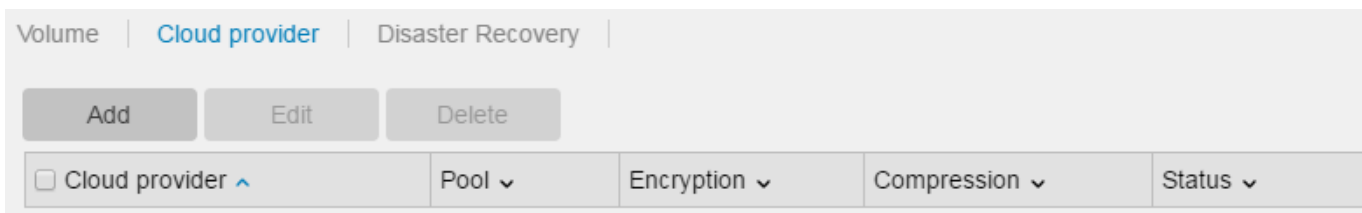
| Access Key ID | Access Key Secret |
|------------------|--|
| LTAIyKxKRgE89xVW | Show |
| LTAIxcv7iCmh1Fx | oXHEQghkNIEDX3RPIa6h3BWfkFSC05 Hide |

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**.

Create Cloud Provider

Create the cloud provider.

Pool

-- Select --

Cloud vendor

Aliyun Object Storage Service

Access key ID

.

Access key Secret

.

Region

East China 1

Node Name

oss-cn-hangzhou.aliyuncs.com

Bucket

Create a new bucket

Encryption

☐

Compression

☐

Use SSL

☒

OK

Cancel


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

Volume | Cloud provider | Disaster Recovery |

Add

Edit

Delete

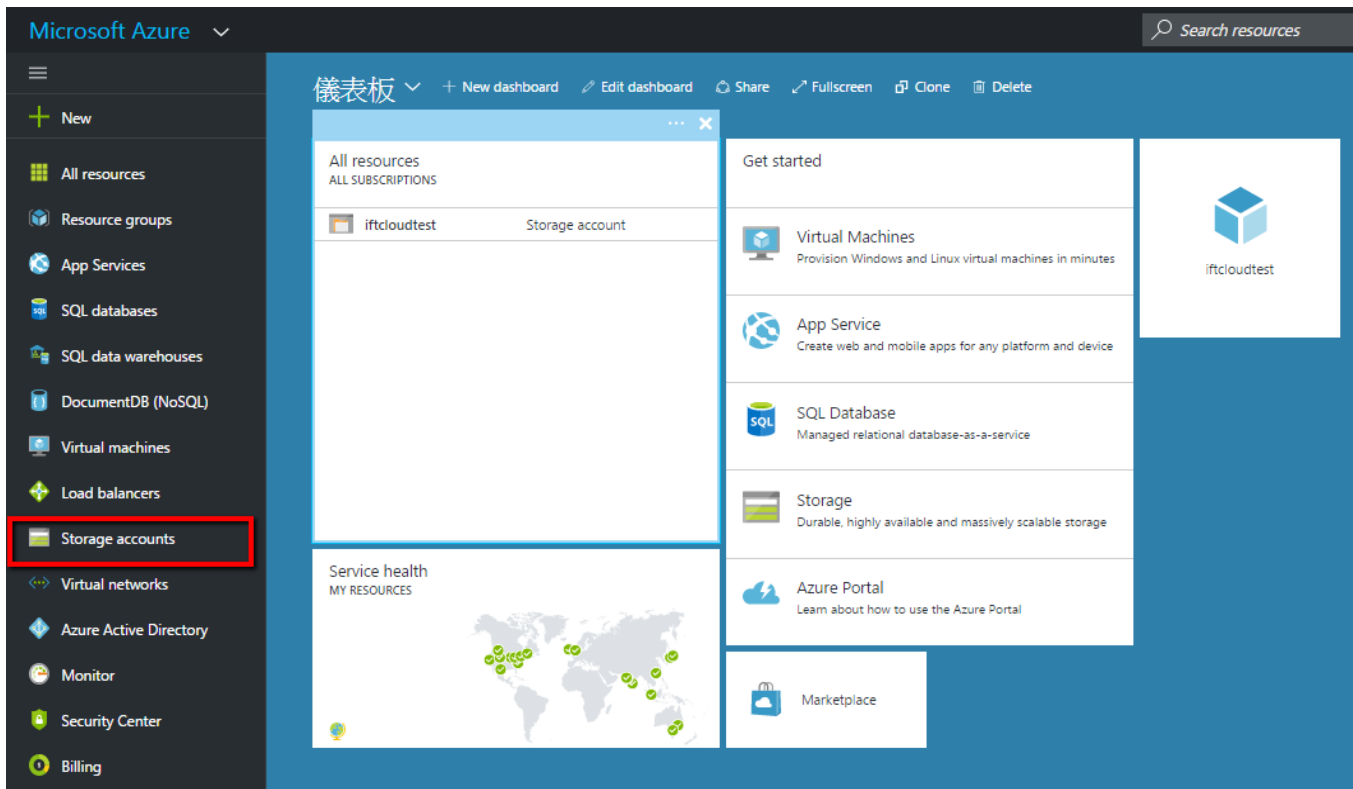
| <input type="checkbox"/> Cloud provider ^ | Pool v | Encryption v | Compression v | Status v |
|--|--------|--------------|---------------|---|
| <input type="checkbox"/> Aliyun Object Storage Service | Pool-1 | Disable | Disable |  connected |

2-3-3. Microsoft Azure

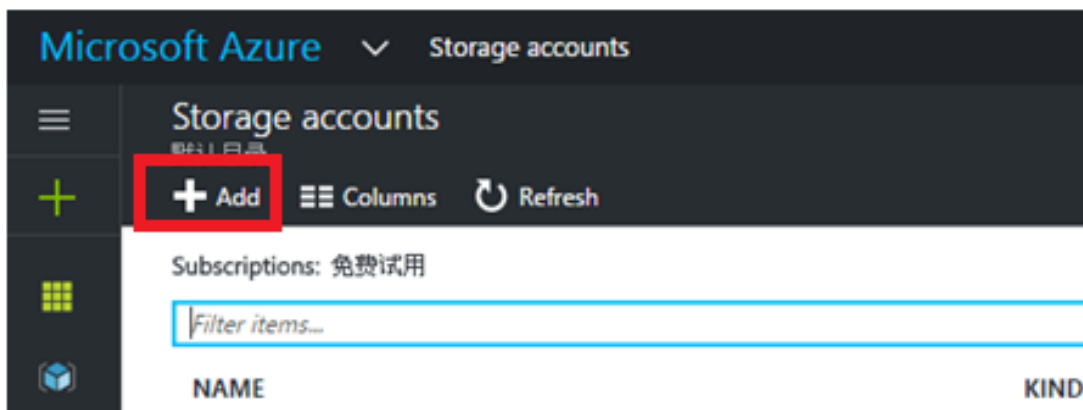
This section explains how to [obtain access credentials](#) and [create cloud buckets on Microsoft Azure via EonOne](#).

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**.

Create storage account

The cost of your storage account depends on the usage [Learn more](#)

* Name ✓

.core.windows.net

Deployment model ☒ Resource manager ☐ Classic

Account kind

Performance ☒ Standard ☐ Premium

Replication

Access tier ☐ Cool ☒ Hot

* Storage service encryption ☒ Disabled ☐ Enabled

* Subscription

* Resource group ☒ Create new ☐ Use existing

✓

* Location

☐ Pin to dashboard

[Create](#) [Automation options](#)

(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.

Using the cloud gateway features

Microsoft Azure Storage accounts > iftcloudtest - Access keys

Subscriptions: 免费试用

Filter items...

NAME

iftcloudtest

SETTINGS

Access keys

Configuration

Custom domain

Search (Ctrl+J)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to data on physical machines. [Learn more](#)

Endpoint

Storage account name: iftcloudtest

| NAME | KEY | Share key |
|------|---|-----------|
| key1 | cDre/Haj87plZlOuiW2SYLh4loFrz/dVwJNQsvg9XQh+JNi | |
| key2 | D47eReeB2KRf7+Y1LAXaD64rA+a3qgPBCEX5SPjtf6nuLE | |

2. Connecting to GS

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

Settings

Device: GSe 3016GE

Settings / Backup & Restore

Schedule

Replication

Snapshot

Cloud

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

Volume | Cloud provider | Disaster Recovery

Add Edit Delete

Cloud provider Pool Encryption Compression Status

(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**.

Create Cloud Provider

Create the cloud provider.

Pool

-- Select --

Cloud vendor

Microsoft Azure Storage

Endpoint

http://iftcloudtest1.blob.core.windows.net

Share key

.

Container

Create a new container

☐ Encryption

☐ Compression

☒ Use SSL

OK

Cancel




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

Volume | Cloud provider | Disaster Recovery |

Add

Edit

Delete

| <input type="checkbox"/> Cloud provider ^ | Pool v | Encryption v | Compression v | Status v |
|--|-----------|--------------|---------------|---|
| <input type="checkbox"/> Aliyun Object Storage Service | Pool-1 | Disable | Disable |  connected |
| <input type="checkbox"/> Amazon S3 Storage | Pool-s3-1 | Disable | Disable |  connected |
| <input type="checkbox"/> Microsoft Azure Storage | Pool-2 | Disable | Disable |  connected |

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.

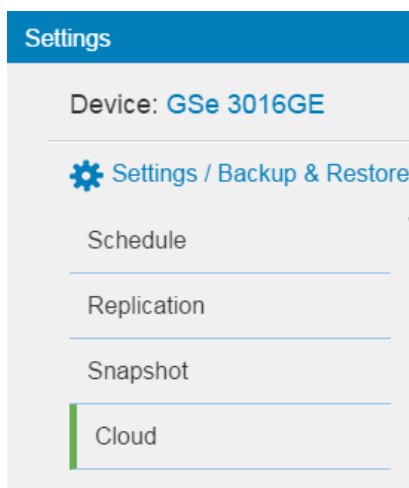
For example, if we add the following line in the **filter-tempauth** section,

user_infortrend_staff01=iftcloud

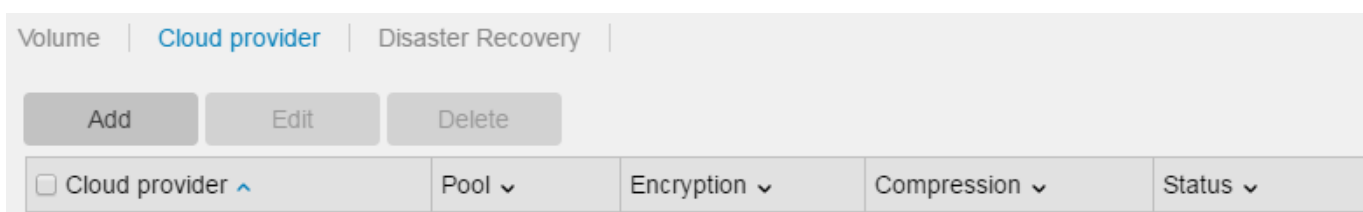
when connecting with EonStor GS/GSe storage systems, **infortrend:staff01** will be the **Access key**, and **iftcloud** will be the **Secret key**.

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.

Volume | Cloud provider | Disaster Recovery |

Add

Edit

Delete

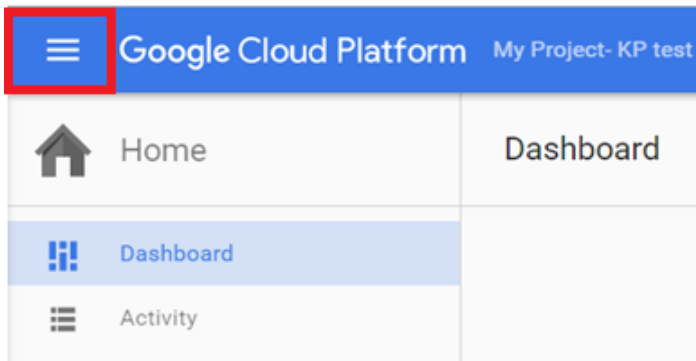
| <input type="checkbox"/> Cloud provider ^ | Pool v | Encryption v | Compression v | Status v |
|--|--------|--------------|---------------|---|
| <input type="checkbox"/> OpenStack Swift Storage | Pool-2 | Disable | Disable |  Connected |

2-3-5. Google Cloud

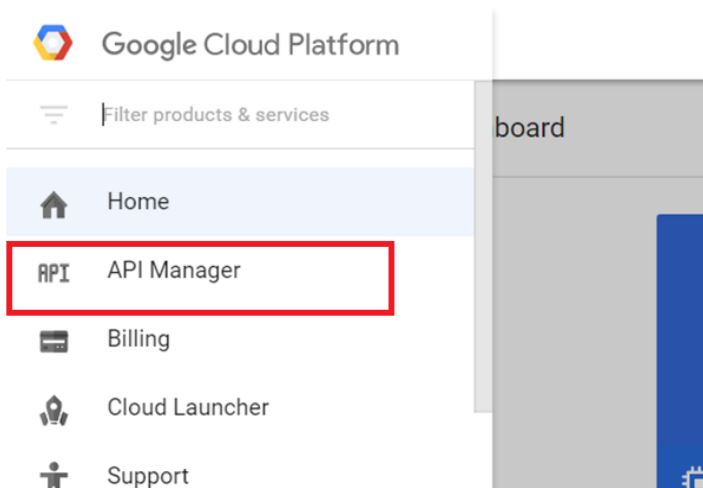
This section explains how to [obtain access credentials](#) and [create cloud buckets on Google Cloud via EonOne](#).

1. Retrieving access information

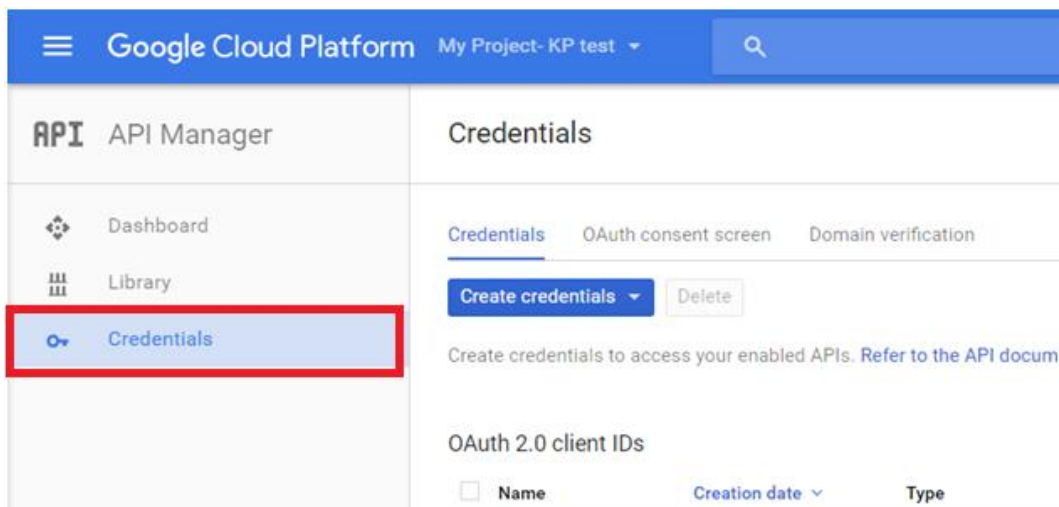
(1) Create a Google Cloud account and log into the account. After login, the Google Cloud platform will help you create your first project. After the project is created, click the **Menu** button on the top-left corner.



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

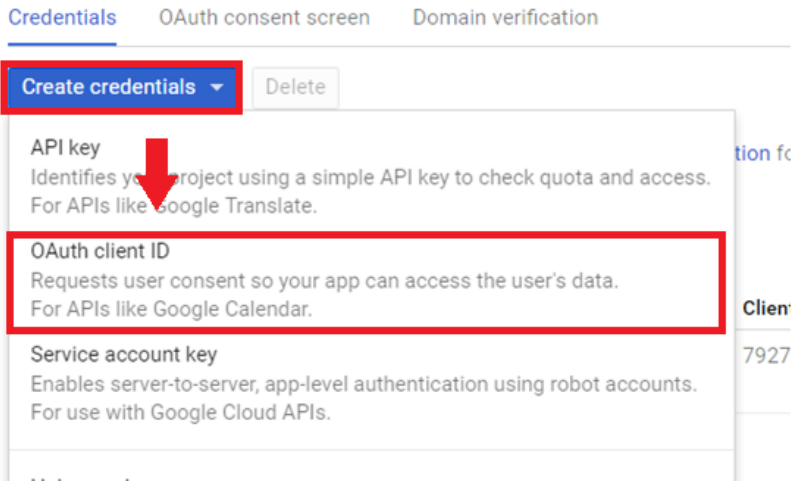


(3) In the **API Manager**, go to the **Credentials** page.



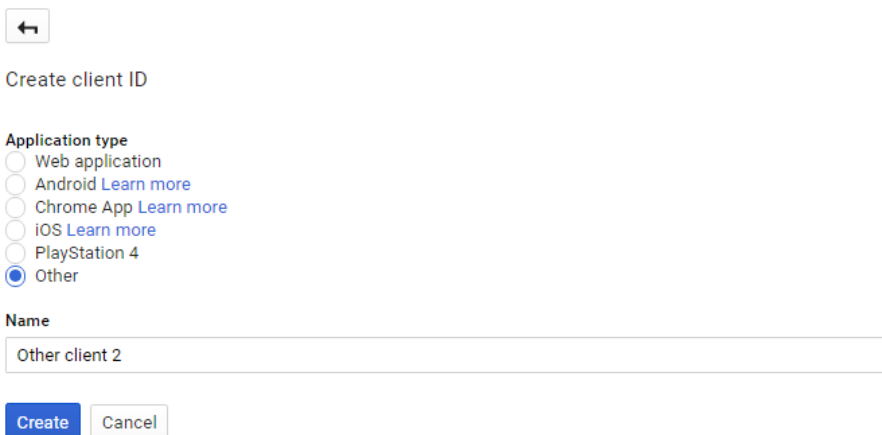
(4) Click **Create credentials** and select **OAuth client ID**.

Credentials



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

Credentials



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

OAuth client

Here is your client ID

414288169170-rek332kr17s4pjrjm12t858mpmutf2m7.apps.googleusercontent.com

Here is your client secret

Hdt5_nhGrBjCnEGYNx4vSrpA

OK

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



Credentials

Credentials OAuth consent screen Domain verification

Create credentials Delete

Create credentials to access your enabled APIs. [Refer to the API documentation](#) for details.

OAuth 2.0 client IDs

| <input type="checkbox"/> | Name | Creation date | Type | Client ID | |
|-------------------------------------|----------------|---------------|-------|--|---|
| <input checked="" type="checkbox"/> | Other client 2 | Oct 18, 2016 | Other | 414288169170-rek332kr17s4pjrjm12t858mpmutf2m7.apps.googleusercontent.com |  |
| <input type="checkbox"/> | Other client 1 | Oct 18, 2016 | Other | 414288169170-l4lh62r3cuu4gti28d4vv4avptnss3ul.apps.googleusercontent.com |  |

Edit OAuth client

Credentials

 Download JSON Reset secret Delete

Client ID for Other

Client ID 414288169170-rek332kr17s4pjrjm12t858mpmutf2m7.apps.googleusercontent.com
Client secret Hdt5_nhGrBjCnEGYNx4vSrpA
Creation date Oct 18, 2016, 2:17:40 PM

Name

Other client 2

Save Cancel

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

The screenshot shows the Google Cloud Platform console interface. The top navigation bar includes the Google Cloud Platform logo and a dropdown menu for the current project, 'My Project- KP test'. The dropdown menu is open, displaying a 'RECENT' list with the following items:

- ✓ My Project- KP test
- my-project-kp-test

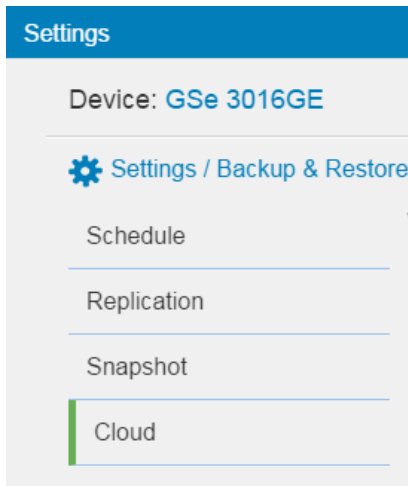
A red arrow points to the 'my-project-kp-test' option. The left sidebar shows the 'Credentials' section, which includes the following information:

| Client ID | 792766705995-rv9jusrbo8m1eccolqdolcaa85old5h.a |
|---------------|--|
| Client secret | e-0wmVF7uJ0ITOLTnzuHho_x |
| Creation date | Sep 29, 2016, 3:55:01 PM |

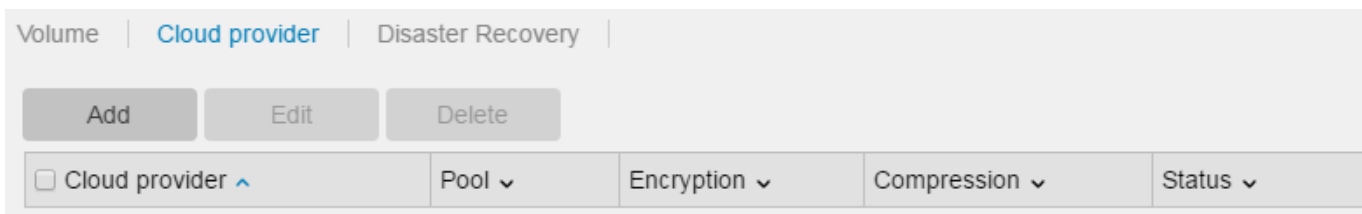
Below the table, the 'Name' field is labeled '網路用戶端 1'. The 'Restrictions' section is also visible, with a note about JavaScript origins.

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**.

Create Cloud Provider

Create the cloud provider.

Pool: -- Select --

Cloud vendor: Google Cloud OAuth2.0

Client ID: .

Client Secret: .

Project ID: .

Authentication code: . [Get authentication code](#)

Bucket: Create a new bucket

Region: Asia

API Endpoint: storage.googleapis.com

OAuth2.0 Endpoint: www.googleapis.com

☐ Encryption

☐ Compression

☒ Use SSL

OK Cancel

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

Settings

Device: SR_GSe 3016GE

Settings / Backup & Restore / Cloud

Schedule | Volume | **Cloud provider** | Disaster Recovery

Replication

Snapshot

Cloud

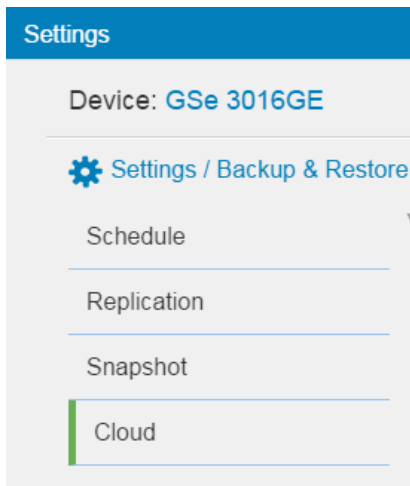
| | Pool | Encryption | Compression | Status |
|--|--------|------------|-------------|-----------|
| <input type="checkbox"/> Cloud provider | Pool-2 | Disable | Disable | connected |
| <input type="checkbox"/> Amazon S3 Storage | Pool-2 | Disable | Disable | connected |
| <input type="checkbox"/> Google Cloud OAuth2.0 | Pool-A | Disable | Disable | connected |
| <input type="checkbox"/> OpenStack Swift Storage | Pool-6 | Disable | Disable | connected |

Close

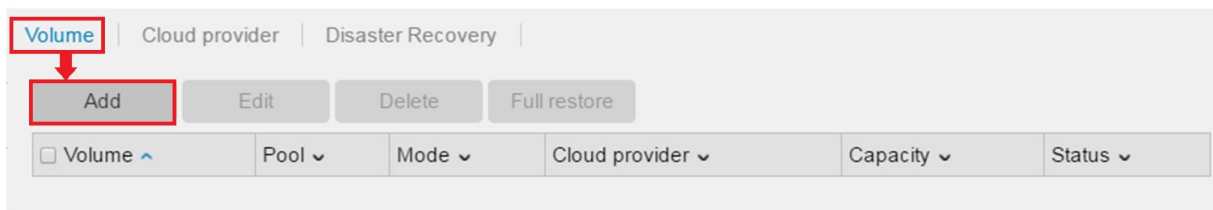


2-4. Creating cloud-integrated volumes

(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

Add cloud cache

Configure the parameters of the Volume.

Pool:

Pool-6

Volume Name:

cloud_v1

☒ Enable Cloud

Tier mode

☒ Cache mode

☐ Fully cache

☒ Flush period 6 Day

☒ Enable Thin Provisioning

Volume Size:

10

GB

Maximum: 2 PB

Minimum reserved space

1

GB

Maximum: 9.9 GB

☐ Enable File System

☐ Initialize Volume After Creation

☒ Host LUN mapping

Pool Information

Pool Name: Pool-6

Free Size: 387.21 GB

OK

Cancel

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 | <p>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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>The minimum size of a volume is 10GB.</p> </div> |
| Enable Cloud-Tier mode | <p>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.</p> <p>For more information, consult the section About the Cloud Gateway Features - Cloud Tiering mode.</p> |
| Enable Cloud-Cache mode | <p>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.</p> <p>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.</p> <p>Users can set the data flush schedule by configuring the “Flush Period.”</p> <p>For more information, consult the section About the Cloud Gateway Features - Cloud Caching mode</p> |
| Thin Provisioning & Minimum Reserved Space | <p>In order to expand storage capacity to the cloud buckets, thin-provisioning must be enabled in cloud-integrated volumes.</p> <p>Move the Minimum Reserved Space slide bar to set the percentage of the volume capacity that will be physically allocated as a safe reserve.</p> |
| 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.

| Volume Cloud provider Disaster Recovery | | | | | |
|---|--------|--------|-------------------------|------------|----------|
| <div>Add Edit Delete Full restore</div> | | | | | |
| <input type="checkbox"/> Volume ^ | Pool v | Mode v | Cloud provider v | Capacity v | Status v |
| <input type="checkbox"/> cloud_v1 | Pool-6 | Cache | OpenStack Swift Storage | 10GB | Mapped |

Disaster Recovery

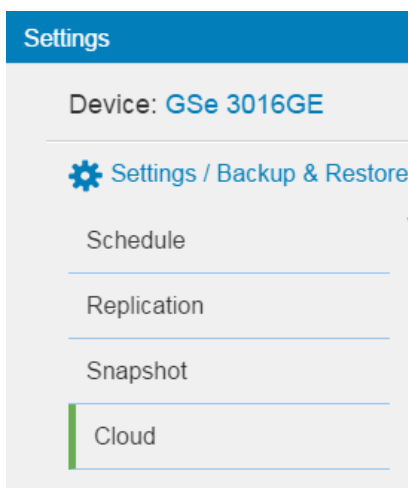
The disaster recovery process for cloud follows the steps described below:

Step 1. [Configure bucket information and select the source data that needs to be recovered](#).

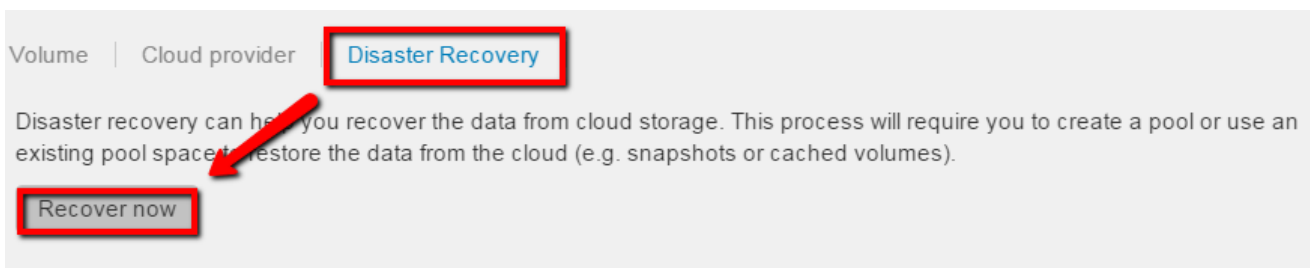
Step 2. [Configure storage space](#).

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.

Configure cloud provider
Configure the settings of selected cloud provider.

Cloud vendor: Amazon S3 Storage

Access key: AKIAIUJFSG2A3VQESXHA

Secret key: kz8TD9PrHXAaGvDNm1+JvRLogSQe

Region: Singapore

Node Name: s3-ap-southeast-1.amazonaws.com

☐ Encryption

☐ Compression

☐ Use SSL

Get buckets information from cloud

Please select Bucket

| Bucket Name | Total/Uncompressed Size |
|-------------|-------------------------|
|-------------|-------------------------|

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

Please select Bucket

| Bucket Name | Total/Uncompressed Size | |
|--|-------------------------|----------------|
| 20160930090717-pool-1-2a0e7a1e3fa49bd4 | 192 MB | Preview |

Next Cancel

(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.

Preview
Preview the volume and snapshot images in the selected bucket.

| Volume Name | ID | Used Size | Total size |
|-------------|------------------|-----------|------------|
| Volume_1 | 5410E11C5E14F779 | 0 Byte | 10 GB |

| Snapshot name | Used Size | Total size | Created time |
|--------------------------|-----------|------------|-------------------|
| Snapshot_20160930_174240 | 0 Byte | 10 GB | 2016/9/30 9:43:14 |

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

Please select Bucket

| Bucket Name ▾ | Total/Uncompressed Size ▾ | |
|--|---------------------------|---------------------------|
| ● 20160930090717-pool-1-2a0e7a1e3fa49bd4 | 192 MB | Preview ▾ |

[Next](#) [Cancel](#)

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.

Disaster Recovery ⓘ

Configure Pool
Configure pool parameters for disaster recovery by creating a new pool or selecting an existed pool.

Pool ☐ Use existed pool for disaster recovery
-- Select -- ▾

☒ Create a new pool for disaster recovery

* Pool Name

Write Policy

Total selected volume: 0

| <input type="checkbox"/> SSD ▾ | Size ▾ |
|---------------------------------|----------|
| 2 | |
| <input type="checkbox"/> Slot13 | 59.37 GB |
| <input type="checkbox"/> Slot14 | 59.37 GB |

RAID Level ▾

[Previous](#) [Next](#) [Cancel](#)

(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.

Disaster Recovery

Configure Volume

You can restore all data or select some volumes from cloud for disaster recovery.

☐ Restore all data from cloud directly.
 ☒ Select the specific volume(s) for directly fully restored. Restore all others later using cloud gateway policy.

Total selected : 0

| Volume Name | Volume Size | Total/Uncompressed Size |
|-------------|-------------|-------------------------|
| Volume_1 | 10 GB | 0 Byte |

| Snapshot name | Used Size | Size | Created time |
|--------------------------|-----------|-------|-------------------|
| Snapshot_20160930_174240 | 0 Byte | 10 GB | 2016/9/30 9:43:14 |

Previous
Next
Cancel

(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.

Disaster Recovery

Summary

Confirm the summary of disaster recovery.

Cloud provider:

Cloud vendor: Amazon S3 Storage
 Region: Singapore
 Node Name: s3-ap-southeast-1.amazonaws.com
 Encryption: No
 Compression: No
 Use SSL: No

Pool Informations:

Pool Name: Pool-DR
 Storage Tiering: Disable
 Write Policy: Default
 Assignment: SlotA
 Member drives (SAS): Tier Index:0 / 10 Drives
 RAID Level: Non RAID
 Stripe Size: 128K

Previous
OK
Cancel