S3 Storage Settings

S3 Storage Regions

Region	Area Code
Australia GlobalSwitch DC1	au-nsw-gbl1
Australia Equinix SYD4	au-nsw-eqx4
Australia Sydney	au-nsw
Thailand Bangkok NTT DC1	th-bkk
Mongolia Ulaanbaatar	mn
Mongolia Ulaanbaatar GEMNET DC1	mn-gem1
Hong Kong	hk
Hong Kong Equinix HK2	hk-eqx2
Philippines	ph
Philippines Carmona DC1	ph-crm1
Kyrgyzstan	kg
Kyrgyzstan - NSP DC1	kg-nsp1
Indonesia	id
Indonesia - Area31 DC1	id-area31
Australia LEDC NSW Datacenters	au-nsw-ledc
Australia NSW Newcastle	au-nsw-ledc-ncle1
Australia NSW Dubbo	au-nsw-ledc-dbo1

WHERE S3 ENDPOINT URL is

areacode.s3.rackcorp.com

EG au-nsw-ledc-ncle1.s3.rackcorp.com to force data to newcastle data center, Australia

How to install s3cmd for RackCorp

INSTALL PACKAGES

CentOS 8+ / Rocky Linux / RPM-based Linux

```
yum install s3cmd
```

Debain / Ubuntu / .deb based linux

```
apt install s3cmd
```

CONFIGURATION

Demo Read-Only Access Key / Secret

Access Key: F4LV2SVMHUOL1UOD2LLF **Secret Key:** plax+zs9eSmvLVl2E7Wc8fRyv+cyuq7vYgQi7E/6 **Default Region:** US **S3 Endpoint:** s3.rackcorp.com **DNS Template (if required):** %(bucket)s.s3.rackcorp.com

(You can create your own inside our portal SERVICES -> STORAGE -> S3 CREDENTIALS / S3 BUCKETS)

```
[demo@demohost demo]# s3cmd --configure
```

Enter new values or accept defaults in brackets with Enter. Refer to user manual for detailed description of all options.

```

```

Access key and Secret key are your identifiers for Amazon S3. Leave them empty for using the env variables. Access Key: F4LV2SVMHUOL1UOD2LLF Secret Key: plax+zs9eSmvLVl2E7Wc8fRyv+cyuq7vYgQi7E/6 Default Region [US]:

```

```

Use "s3.amazonaws.com" for S3 Endpoint and not modify it to the target Amazon S3. S3 Endpoint [s3.amazonaws.com]: s3.rackcorp.com

```

```

Use "%(bucket)s.s3.amazonaws.com" to the target Amazon S3. "%(bucket)s" and "%(location)s" vars can be used if the target S3 system supports dns based buckets. DNS-style

bucket+hostname:port template for accessing a bucket [%(bucket)s.s3.amazonaws.com]: %(bucket)s.s3.rackcorp.com

Encryption password is used to protect your files from reading by unauthorized persons while in transfer to S3 Encryption password: Path to GPG program [/bin/gpg]:

When using secure HTTPS protocol all communication with Amazon S3 servers is protected from 3rd party eavesdropping. This method is slower than plain HTTP, and can only be proxied with Python 2.7 or newer Use HTTPS protocol [Yes]:

On some networks all internet access must go through a HTTP proxy. Try setting it here if you can't connect to S3 directly HTTP Proxy server name:

New settings: Access Key: F4LV2SVMHUOL1UOD2LLF Secret Key: plax+zs9eSmvLVl2E7Wc8fRyv+cyuq7vYgQi7E/6 Default Region: US S3 Endpoint: s3.rackcorp.com DNS-style bucket+hostname:port template for accessing a bucket: %(bucket)s.s3.rackcorp.com Encryption password: Path to GPG program: /bin/gpg Use HTTPS protocol: True HTTP Proxy server name: HTTP Proxy server port: 0

Test access with supplied credentials? [Y/n] Y Please wait, attempting to list all buckets... Success. Your access key and secret key worked fine :-)

Now verifying that encryption works... Not configured. Never mind.

```
Save settings? [y/N] YConfiguration saved to '/home/demo/.s3cfg'
```

Recommended Client Software

While there is no formal (*RFC documented*) '**S3 Protocol**', the RackCorp S3 storage platform supports largely conforms to what the industry largely follow, that being the protocol implemented by Amazon. This means that most client software that has '**native S3**' or '**AWS S3**' support, will typically work with RackCorp S3, given the correct configuration.

If you experience issues with any particular functionality or client software that you believe should work, please feel free to raise a support ticket and we will investigate.

S3 Security Considerations

There are many use-cases for S3 storage, one of which is hosting of static web content. This requires your bucket to have **'PUBLIC READ ENABLED'** permissions selected in the bucket configuration. This means that anyone with a URL to a resource stored in your bucket will be able to access it without requiring any credentials or authentication. This is perfect for static images and other content, for use behind a CDN or for objects in-bedded into your website/mobile application.

If you are not using your bucket for hosting of static web content, you **must** ensure that the **'PUBLIC READ DISABLED'** permissions are selected. This ensures that only valid users with an access + secret keypair can access resources in your bucket.

Additionally, you can use a **'Presigned URL'** for both uploading and accessing of data in buckets, in the same way that you would here: (AWS S3 - presigned urls). This is the preferred approach for all common use cases as it reduces any potential exposure of data stored in your buckets.

For assistance on the points above, please feel free to raise a support request for clarifications.

S3 Storage White-label Partner Services

RackCorp also extends all of the above S3 Storage Regions to our white-label partner programme where you assign your s3.<yourhostname> nameservers to RackCorp hosted DNS. Please contact sales@rackcorp.com for further information.

Revision #6
Created 1 March 2022 07:44:38 by Stephen D
Updated 28 November 2023 05:19:54 by RackCorp