elastifile

Cross-Cloud Data Fabric

ECFS (Elastifile Cloud File System) 3.1.X
Google Cloud Platform (GCP)

Deployment Guide

February 2019

Document Revision: 0.1

Important Notice

This document is delivered subject to the following conditions and restrictions:

- This guide contains proprietary information belonging to Elastifile Inc. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of Elastifile Inc. products.
- No part of contents may be used for any other purpose, disclosed to any person or firm, translated or reproduced by any means, electronic and mechanical, without the express prior written permission of Elastifile Inc..
- The text and graphics are for the purpose of illustration and reference only, based on the current version of the product(s) described in this document.
- The software described in this document is furnished under a license agreement. The software may be used or copied only in accordance with the terms of that agreement.
- Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- Elastifile Inc. makes no warranty of any kind with regard to this printed material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Elastifile Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.
- Brand or product names are trademarks of their respective companies or organizations.

Table of Contents

1. Introduction **4**

1.1 Document Scope 4

1.2 System Overview 4

1.2.1 Installation Flow 4

2. Defining Your GCP Account to Support ECFS **5**

2.1 Defining Your GCP Service Account Roles 5

3. Installing the ECFS **8**

3.1 Installing the ECFS using GCP Marketplace 8

3.2 Installing the ECFS Using the GCP Console 11

3.3 Installing the ECFS Using the GCP Cloud Shell 14

3.3.1 Authenticating Your GCP Account 15

3.3.2 Running the ECFS Installation 15

4. Logging in to ECFS **17**

5. Configuring and Deploying ECFS **18**

Appendix A. Configuring a CentOS Client for Operation with ECFS **26**

A.1 Creating a CentOS Instance (Optional) 26

A.2 Configuring the NFS Mount 26

A.3 Add NFS 26

A.4 Mounting the Elastifile Service 27

1. Introduction

1.1 Document Scope

This guide describes the installation process for creating ECFS (Elastifile Cloud File System) 3.1.X systems in the Google Cloud Platform (GCP) environment.

1.2 System Overview

There are several main types of entities in an ECFS system:

- ECFS Management System (EMS) - the ECFS management instance that controls the ECFS system.
- Controller - an instance that provides storage resources and client access.
- Services - an instance that provides additional services such as replication for disaster recovery.

The EMS and controller entities should not be used for any other purpose.

The EMS and controllers are installed on GCP instances.

1.2.1 Installation Flow

The installation flow consists of the following main steps:

1. Defining your GCP account to support ECFS instances (see Section 2 - Defining Your GCP Account to Support ECFS).

Defining your GCP account is not required if you are installing a system using the GCP Marketplace.

2. Deploying an ECFS (see Section 3 - Installing the ECFS).

2. Defining Your GCP Account to Support ECFS

Defining your GCP account is not required if you are installing a system using the GCP Marketplace.

To deploy an ECFS system on the Google Cloud Platform (GCP), you need to perform the following procedures:

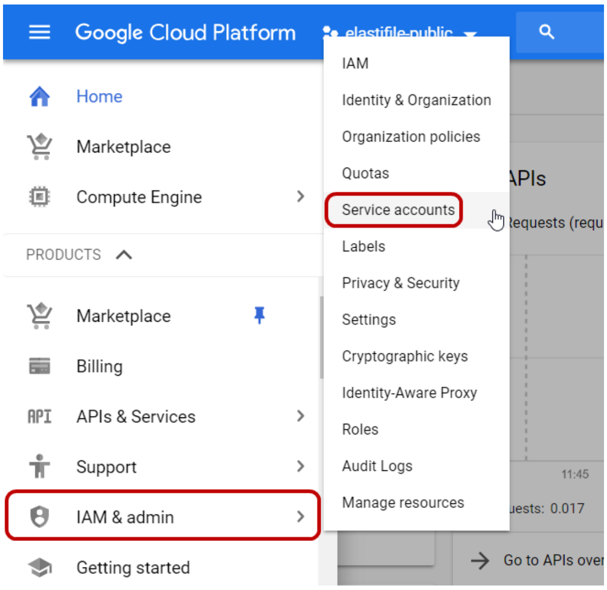
1. Make sure you have a GCP account.
2. Define a project in which you will install the ECFS system.
3. Define the service account roles - see Section 2.1 - Defining Your GCP Service Account Roles

2.1 Defining Your GCP Service Account Roles

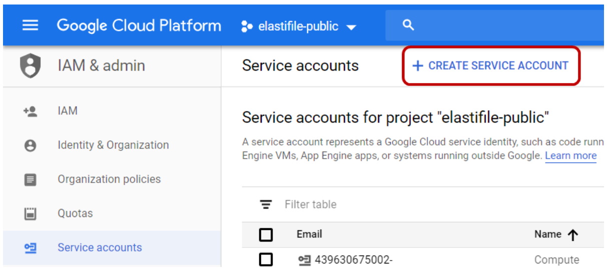
You need to define a service account and assign certain roles to enable you to create ECFS storage nodes in the project.

To define a service account and assign the roles:

1. In the Google Cloud Platform Console, click **IAM & admin**. and click **Service accounts**.



2. Click **CREATE SERVICE ACCOUNT**.

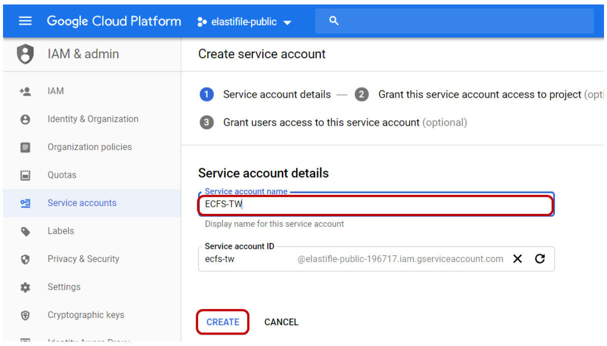


Service accounts for project "elastifile-public"

A service account represents a Google Cloud service identity, such as code runn
Engine VMs, App Engine apps, or systems running outside Google. Learn more

□	Email	Name ↑
□	439630675002-	Compute

3. In **Service account name**, type a name for the service account you are creating and click **CREATE**.



Create service account

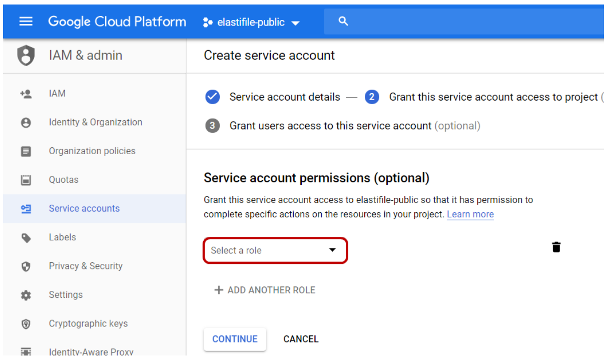
1 Service account details — 2 Grant this service account access to project (opt
3 Grant users access to this service account (optional)

Service account details

Service account name: ECFS-TW
Display name for this service account

Service account ID: ecfs-tw @elastifile-public-196717.iam.gserviceaccount.com

4. Click **Select a role**.



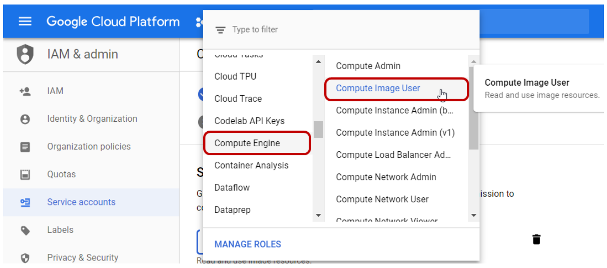
Create service account

Service account details — 2 Grant this service account access to project (
3 Grant users access to this service account (optional)

Service account permissions (optional)

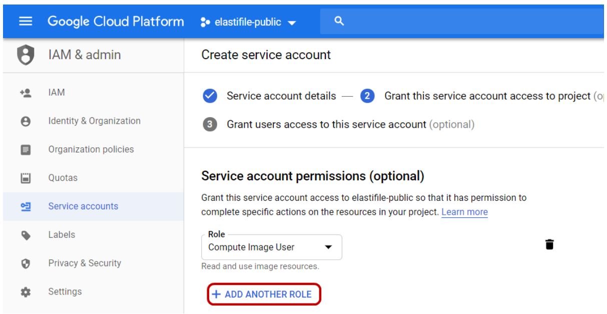
Grant this service account access to elastifile-public so that it has permission to complete specific actions on the resources in your project. Learn more

5. Click **Compute Engine**, then click **Compute Image User**.



Compute Image User
Read and use image resources.

6. Click **+ ADD ANOTHER ROLE**.



Create service account

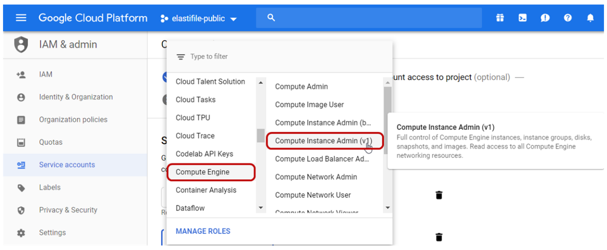
Service account details — 2 Grant this service account access to project (o
3 Grant users access to this service account (optional)

Service account permissions (optional)

Grant this service account access to elastifile-public so that it has permission to complete specific actions on the resources in your project. Learn more

Role: Compute Image User
Read and use image resources.

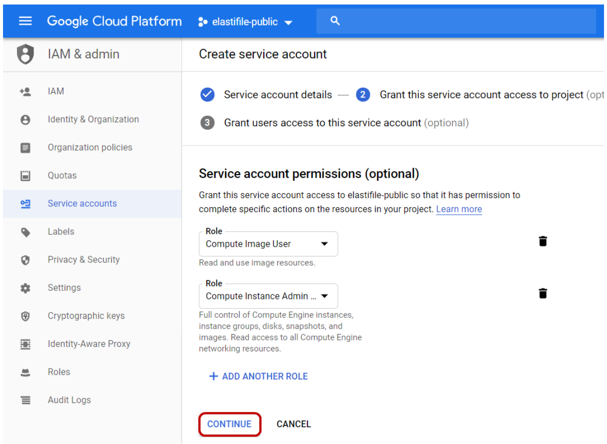
7. Click **Select a role**, click **Compute Engine**, then click **Compute Instance Admin (v1)**.



unt access to project (optional) —

Compute Instance Admin (v1)
Full control of Compute Engine instances, instance groups, disks, snapshots, and images. Read access to all Compute Engine networking resources.

8. Click **CONTINUE**.



Create service account

✓ Service account details — 2 Grant this service account access to project (opt

3 Grant users access to this service account (optional)

Service account permissions (optional)

Grant this service account access to elastifile-public so that it has permission to complete specific actions on the resources in your project. Learn more

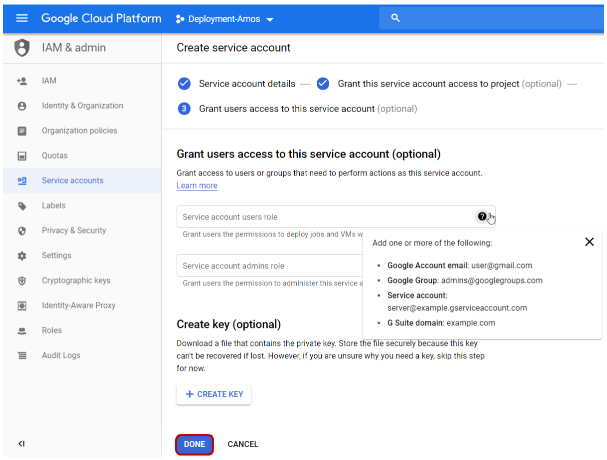
Role: Compute Image User

Read and use image resources.

Role: Compute Instance Admin ...

Full control of Compute Engine instances, instance groups, disks, snapshots, and images. Read access to all Compute Engine networking resources.

9. Click **DONE**.



Create service account

✓ Service account details — ✓ Grant this service account access to project (optional) —

3 Grant users access to this service account (optional)

Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. Learn more

Service account users role

Grant users the permissions to deploy jobs and VMs w

Service account admins role

Grant users the permission to administer this service a

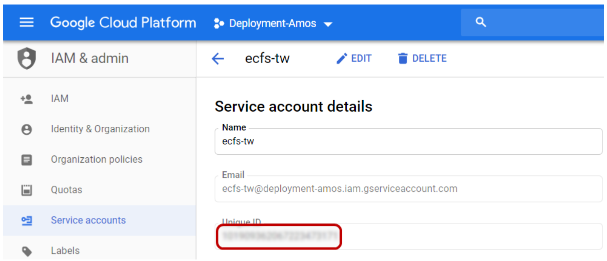
Add one or more of the following:

- **Google Account email**: user@gmail.com
- **Google Group**: admins@googlegroups.com
- **Service account**: server@example.gserviceaccount.com
- **G Suite domain**: example.com

Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

10. Your newly created service account appears in the Service Accounts window. Click the account name and copy the Unique ID and send it and your GCP account name to Elastifile customer support.



ecfs-tw

Service account details

Name: ecfs-tw

Email: ecfs-tw@deployment-amos.iam.gserviceaccount.com

Unique ID: [redacted]

11. Wait for confirmation from Elastifile customer support before proceeding with cloud deployment.

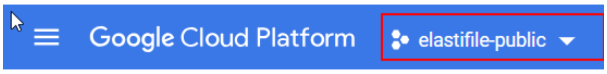
3. Installing the ECFS

This section describes how to install and configure the ECFS. You can install the ECFS using any of the following methods:

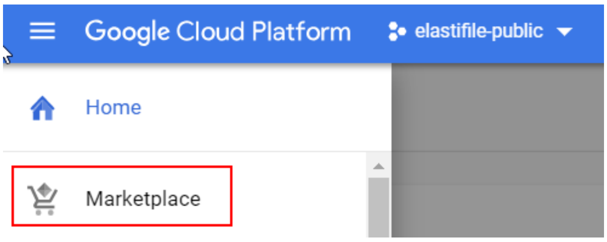
- via the GCP Marketplace - see Section 3.1 - Installing the ECFS using GCP Marketplace
- via the GCP Console - see Section 3.2 - Installing the ECFS Using the GCP Console
- via the GCP Cloud Shell - see Section 3.3 - Installing the ECFS Using the GCP Cloud Shell

3.1 Installing the ECFS using GCP Marketplace

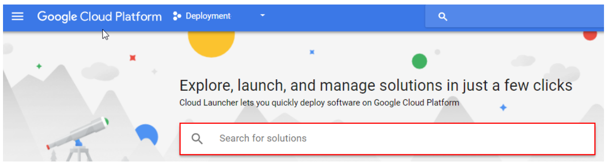
1. In the Google Cloud Platform Console, select your project.



2. Click **Marketplace**.



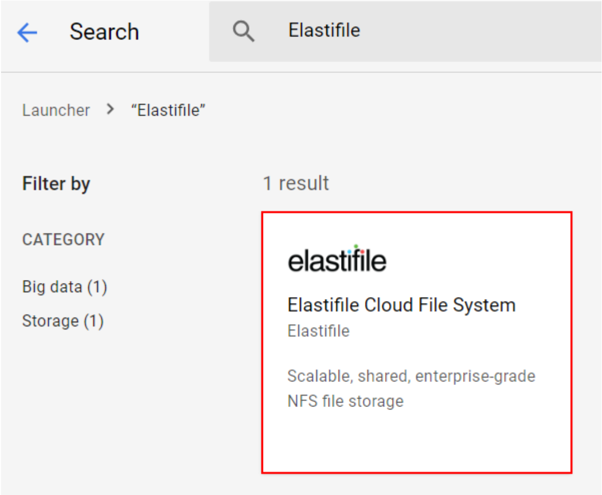
3. In the Search for solutions bar, type Elastifile.



Explore, launch, and manage solutions in just a few clicks

Cloud Launcher lets you quickly deploy software on Google Cloud Platform

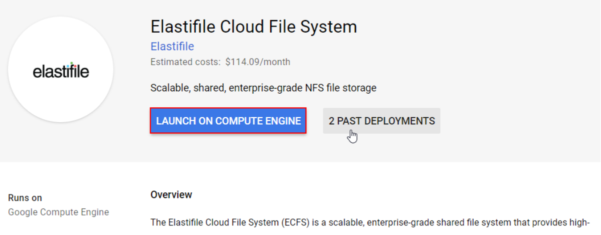
4. In the results, click **Elastifile Cloud File System**.



Elastifile Cloud File System
Elastifile

Scalable, shared, enterprise-grade NFS file storage

5. Click **LAUNCH ON COMPUTE ENGINE**.

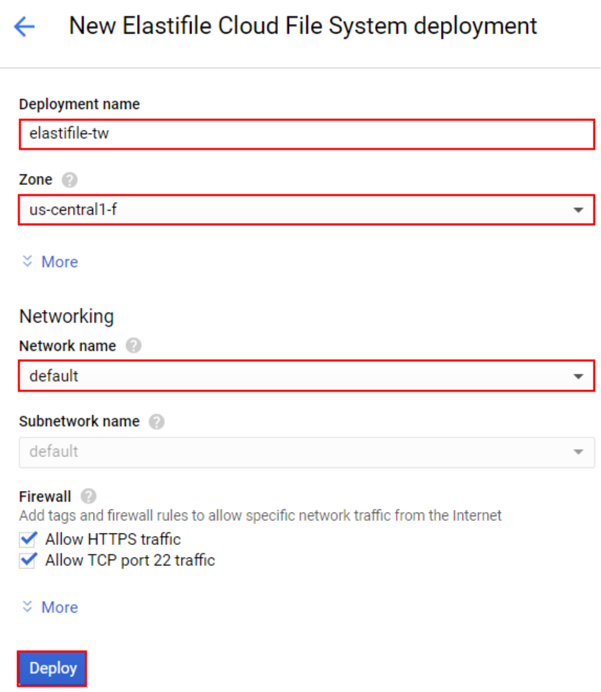


Elastifile Cloud File System
Elastifile
Estimated costs: $114.09/month
Scalable, shared, enterprise-grade NFS file storage

Runs on
Google Compute Engine

Overview
The Elastifile Cloud File System (ECFS) is a scalable, enterprise-grade shared file system that provides high-

6. Type a **Name** for your instance, select a **Zone** and click the **Network name** arrow and select a network.
7. Click **Deploy**.



New Elastifile Cloud File System deployment

Deployment name: elastifile-tw

Zone: us-central1-f

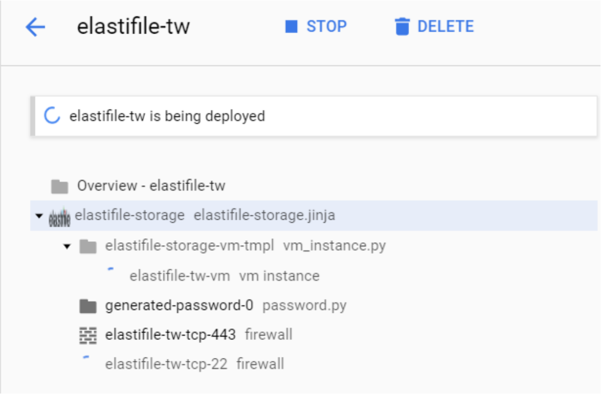
Networking

Network name: default

Subnetwork name: default

Firewall
Add tags and firewall rules to allow specific network traffic from the Internet
☑ Allow HTTPS traffic
☑ Allow TCP port 22 traffic

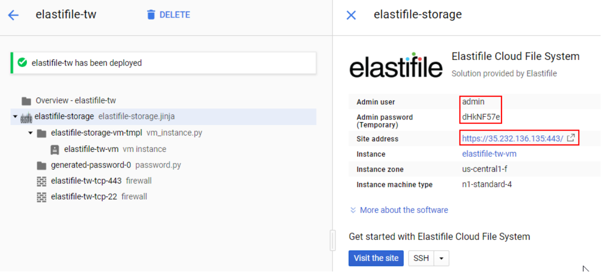
8. Your system starts deploying.



elastifile-tw is being deployed

Overview - elastifile-tw
elastifile-storage elastifile-storage.jinja
elastifile-storage-vm-tmpl vm_instance.py
elastifile-tw-vm vm instance
generated-password-0 password.py
elastifile-tw-tcp-443 firewall
elastifile-tw-tcp-22 firewall

9. When the system is deployed:
   a. Note the **Admin user**, **Admin password (Temporary)** for logging into ECFS for the first time.
   b. Click the **Site address** URL to open the ECFS Management Console.



elastifile-tw has been deployed

Overview - elastifile-tw
elastifile-storage elastifile-storage.jinja
elastifile-storage-vm-tmpl vm_instance.py
elastifile-tw-vm vm instance
generated-password-0 password.py
elastifile-tw-tcp-443 firewall
elastifile-tw-tcp-22 firewall

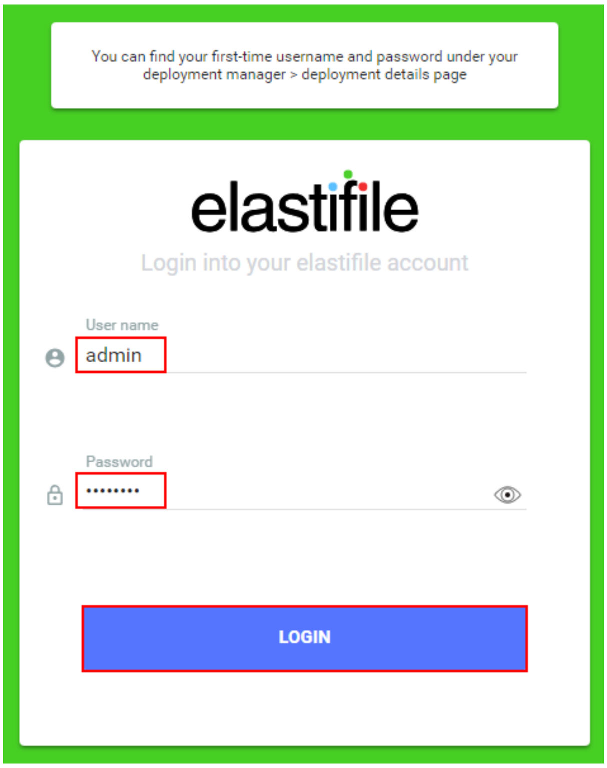
Elastifile Cloud File System
Solution provided by Elastifile

Admin user	admin
Admin password (Temporary)	dHkNF57e
Site address	https://35.232.136.135:443/
Instance	elastifile-tw-vm
Instance zone	us-central1-f
Instance machine type	n1-standard-4

Get started with Elastifile Cloud File System

The default self-signed SSL certificate requires dismissing the browser security warning to proceed. To load your own SSL certificate (optional), see Section 1 - Loading Your SSL Certificate (Optional).

10. Type the credentials you noted in Step 9 and click **LOGIN**.



You can find your first-time username and password under your deployment manager > deployment details page

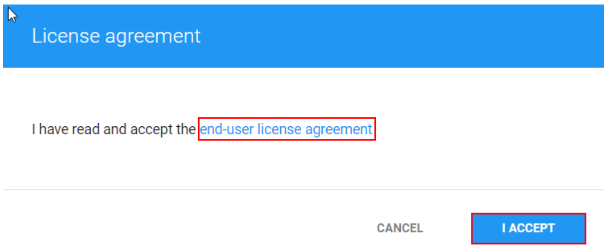
elastifile

Login into your elastifile account

User name: admin

Password: ••••••••

11. If this is the first time you are logging in, click I ACCEPT if you agree with the terms of the Elastifile license agreement (EULA).

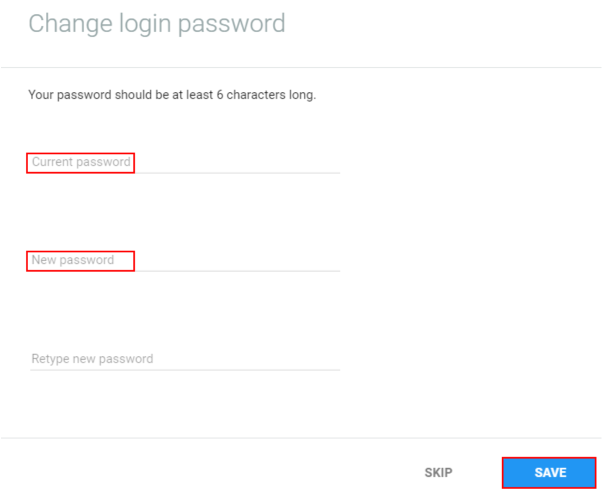


License agreement

I have read and accept the end-user license agreement

To download the Elastifile EULA, click end-user license agreement.

12. If required, change the temporary password to a password of your choice and click **SAVE**.



Change login password

Your password should be at least 6 characters long.

Current password

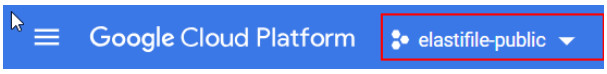
New password

Retype new password

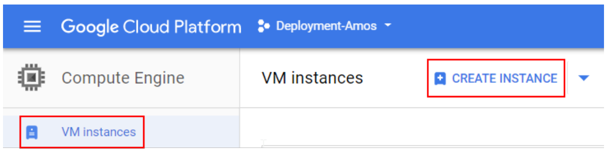
3.2 Installing the ECFS Using the GCP Console

Make sure you have performed all the steps in Section 2.1 - Defining Your GCP Service Account Roles and you received confirmation from Elastifile customer support before proceeding.

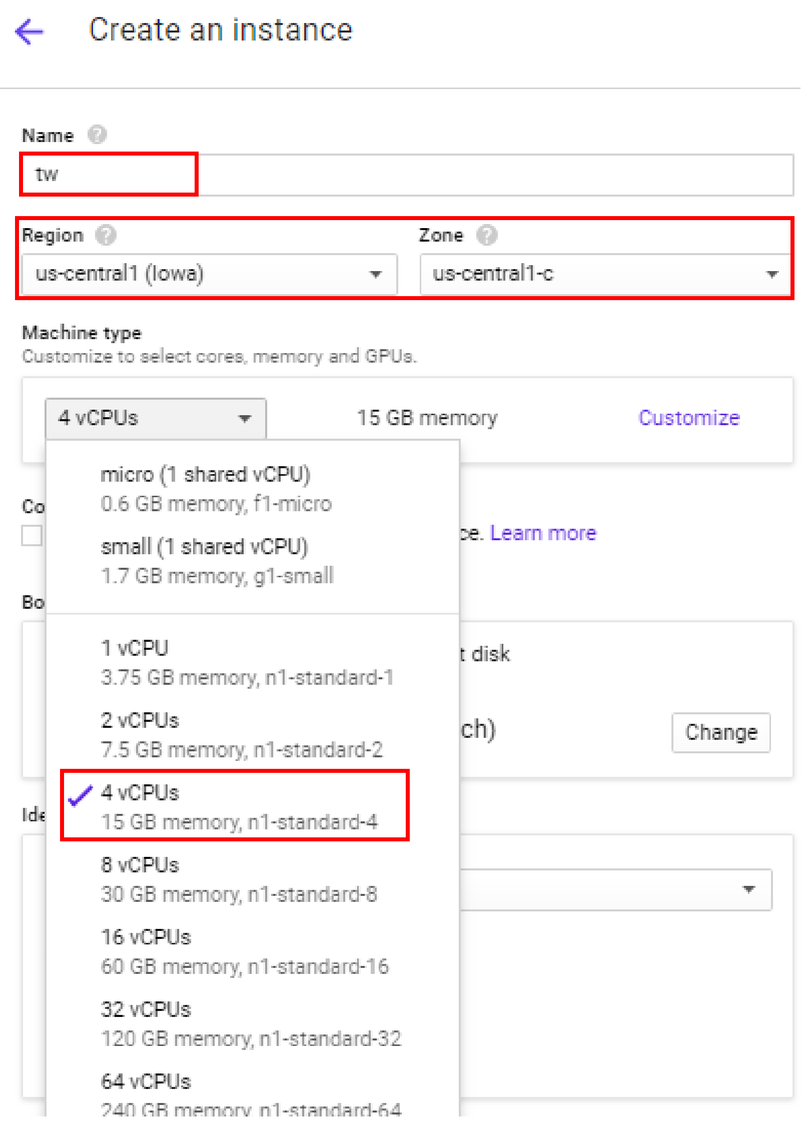
1. In the Google Cloud Platform Console, select your project.



2. Click **Compute Engine**, click **VM Instances** and click **CREATE INSTANCE**.



3. Type a **Name** for your instance, select a **Zone**, click the **Machine type** arrow and select **4 vCPUs**.



Create an instance

Name: tw

Region: us-central1 (Iowa)

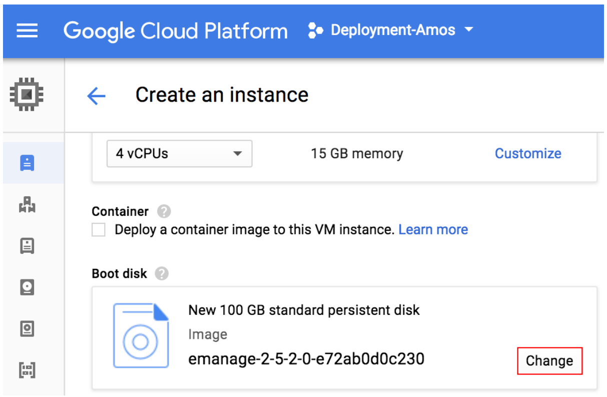
Zone: us-central1-c

Machine type
Customize to select cores, memory and GPUs.

4 vCPUs — 15 GB memory — Customize

micro (1 shared vCPU)
0.6 GB memory, f1-micro
small (1 shared vCPU)
1.7 GB memory, g1-small
1 vCPU
3.75 GB memory, n1-standard-1
2 vCPUs
7.5 GB memory, n1-standard-2
✓ 4 vCPUs
15 GB memory, n1-standard-4
8 vCPUs
30 GB memory, n1-standard-8
16 vCPUs
60 GB memory, n1-standard-16
32 vCPUs
120 GB memory, n1-standard-32
64 vCPUs
240 GB memory, n1-standard-64
Co
Bo
Ide
ce. Learn more
t disk
ch)
Change

4. Under **Boot disk**, click **Change**.



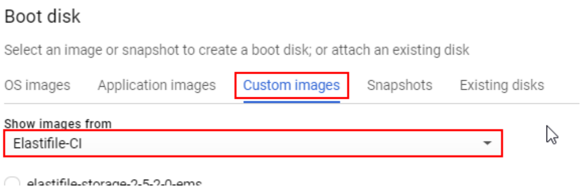
Create an instance

4 vCPUs — 15 GB memory — Customize

Container
□ Deploy a container image to this VM instance. Learn more

Boot disk
New 100 GB standard persistent disk
Image
emanage-2-5-2-0-e72ab0d0c230

5. Click **Custom images**, click the **Show images from** arrow and click **Elastifile-CI**.



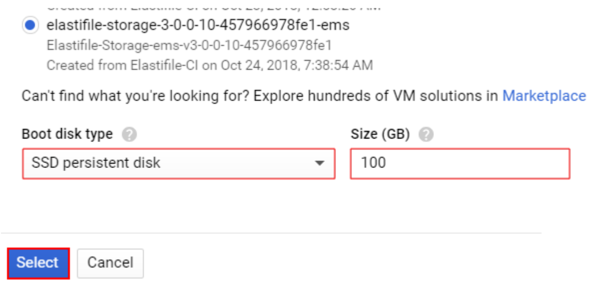
Boot disk

Select an image or snapshot to create a boot disk; or attach an existing disk

Show images from: Elastifile-CI

○ elastifile-storage-2-5-2-0-ems

6. In the list of images, click the required image (request this information from Elastifile Customer Support), change **Boot disk type** to **SSD persistent disk** and **Size (GB)** to 100. Click **Select**.

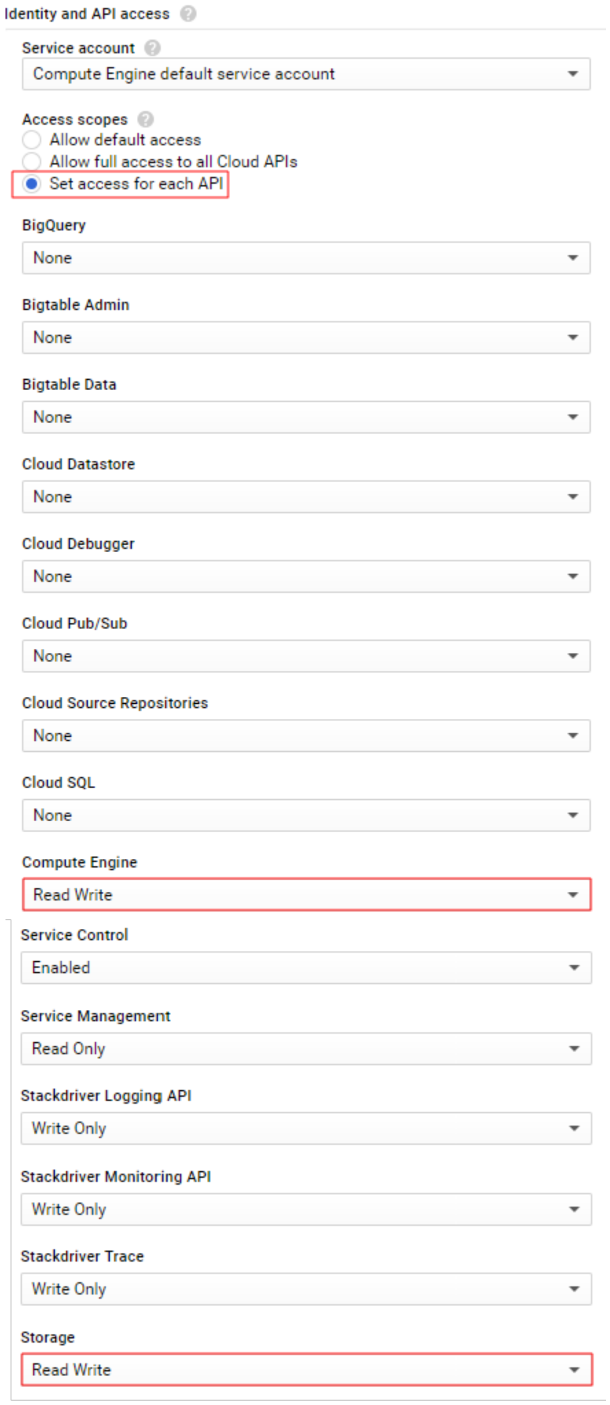


● elastifile-storage-3-0-0-10-457966978fe1-ems
Elastifile-Storage-ems-v3-0-0-10-457966978fe1
Created from Elastifile-CI on Oct 24, 2018, 7:38:54 AM

Can't find what you're looking for? Explore hundreds of VM solutions in Marketplace

Boot disk type: SSD persistent disk
Size (GB): 100

7. Under **Identity and API access**, under **Access scopes**, click **Set Access for each API**. Set **Compute Engine** and **Storage** parameters to **Read Write**.



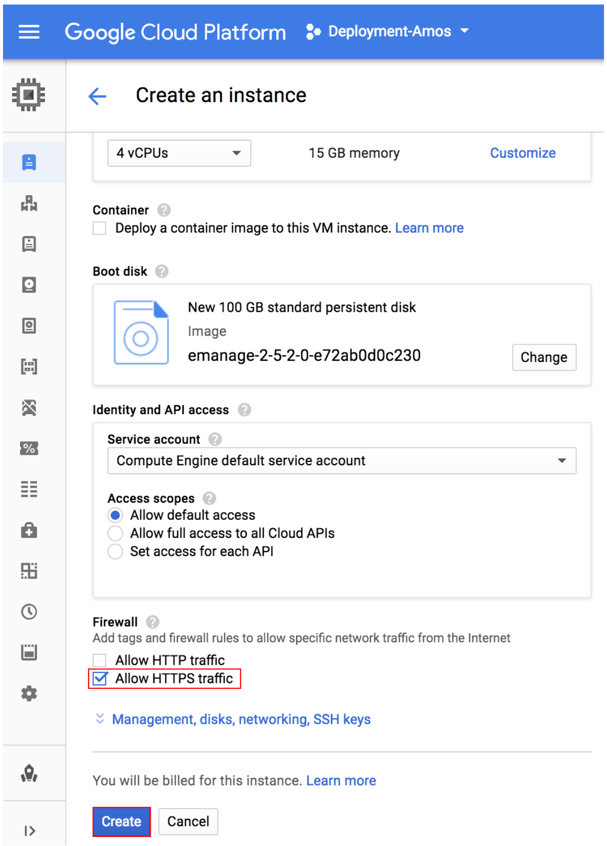
Identity and API access

Service account: Compute Engine default service account

Access scopes
○ Allow default access
○ Allow full access to all Cloud APIs
● Set access for each API

BigQuery: None
Bigtable Admin: None
Bigtable Data: None
Cloud Datastore: None
Cloud Debugger: None
Cloud Pub/Sub: None
Cloud Source Repositories: None
Cloud SQL: None
Compute Engine: Read Write
Service Control: Enabled
Service Management: Read Only
Stackdriver Logging API: Write Only
Stackdriver Monitoring API: Write Only
Stackdriver Trace: Write Only
Storage: Read Write

8. Under **Firewall**, select the **Allow HTTPS traffic** check box, and click **Create**.



4 vCPUs 15 GB memory

Container
☐ Deploy a container image to this VM instance. Learn more

Boot disk
New 100 GB standard persistent disk
Image
emanage-2-5-2-0-e72ab0d0c230

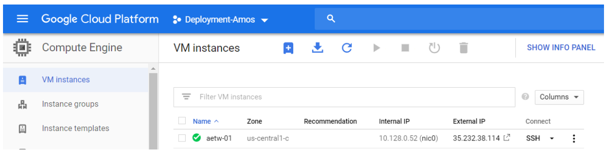
Identity and API access
Service account
Compute Engine default service account

Access scopes
● Allow default access
○ Allow full access to all Cloud APIs
○ Set access for each API

Firewall
Add tags and firewall rules to allow specific network traffic from the Internet
☐ Allow HTTP traffic
☑ Allow HTTPS traffic

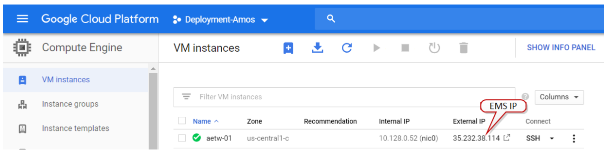
You will be billed for this instance. Learn more

9. Click **VM Instances**. The EMS you installed appears in the list of VM instances.



Name	Zone	Recommendation	Internal IP	External IP	Connect
aetw-01	us-central1-c		10.128.0.52 (nic0)	35.232.38.114	SSH

10. Click the EMS **External IP** to open the ECFS Management Console.



Name	Zone	Recommendation	Internal IP	External IP	Connect
aetw-01	us-central1-c		10.128.0.52 (nic0)	35.232.38.114	SSH

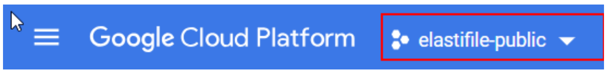
The default self-signed SSL certificate requires dismissing the browser security warning to proceed. To load your own SSL certificate (optional), see Section 1 - Loading Your SSL Certificate (Optional).

3.3 Installing the ECFS Using the GCP Cloud Shell

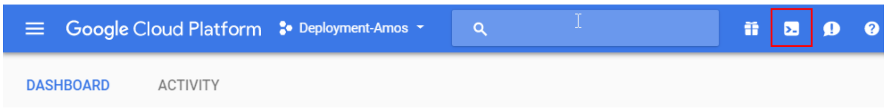
Make sure you have performed all the steps in Section 2.1 - Defining Your GCP Service Account Roles and you received confirmation from Elastifile customer support before proceeding.

3.3.1 Authenticating Your GCP Account

1. In the Google Cloud Platform Console, select your project.



2. Click **Activate Google Cloud Shell**.



3. In the GCP Cloud Shell, run the following::

```
gcloud config set project <project id>
.
.
gcloud config set account <your_google_username>
```

- The project ID appears in the GCP Dashboard.
- Your google username is the email address you use to log into the GCP console.

3.3.2 Running the ECFS Installation

The term "eManage" in the installation script refers to the EMS machine.

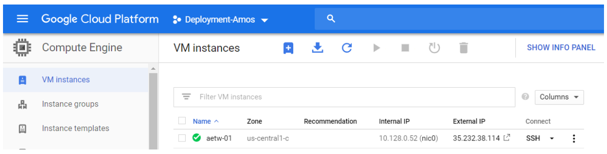
1. In the GCP Cloud Shell, run the following:

```
gcloud compute instances create <ems name> --image
https://www.googleapis.com/compute/v1/projects/elastifile-ci/global/images/<ems image> --
service-<your service account ID> --machine-type n1-standard-4 --subnet <subnet name> --zone
<zone-region> --scopes=cloud-platform --tags=https-server
```

- <ems name> is the name you will assign to the EMS. Elastifile recommends to use a name that will reflect the system name.
- <ems image> is the image name provided to you by Elastifile Customer Support.
- <your service account ID> is the ID of the service account you defined in Section 2.1 - Defining Your GCP Service Account Roles.
- <subnet name> is the name of the subnet if you will not be using the default subnet (optional).
- <region-zone> is your preferred GCP region and zone. For example: `us-central1-c`

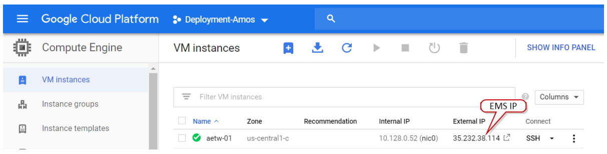
Example:

2. Click **Compute Engine** and select your project. The EMS you installed appears in the list of VM instances.



	Name	Zone	Recommendation	Internal IP	External IP	Connect
□	aetw-01	us-central1-c		10.128.0.52 (nic0)	35.232.38.114	SSH

3. Click the EMS **External IP** to open the ECFS Management Console.



	Name	Zone	Recommendation	Internal IP	External IP	Connect
□	aetw-01	us-central1-c		10.128.0.52 (nic0)	35.232.38.114	SSH

The default self-signed SSL certificate requires dismissing the browser security warning to proceed. To load your own SSL certificate (optional), see Section 1 - Loading Your SSL Certificate (Optional).

4. Logging in to ECFS

To log in to the ECFS system:

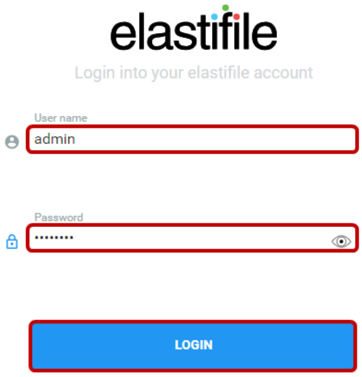
1. In your browser, enter the ECFS Management URL (IP address that appears in the GCP console) and press Enter. The login window appears.

2. Enter the following default values:

   - **Username**: admin
   - **Password**: changeme

   If you installed the EMS through the Google Marketplace, use the password you noted at the end of the installation (see Section 4 - Logging in to ECFS, step 9).

3. Click **LOGIN**.



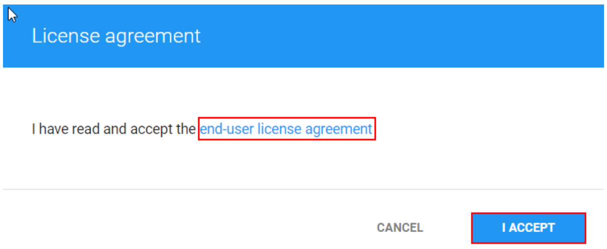
elastifile

Login into your elastifile account

User name: admin

Password: ••••••••

4. If this is the first time you are logging in, click **I ACCEPT** if you agree with the terms of the Elastifile license agreement (EULA).



License agreement

I have read and accept the end-user license agreement

To download the Elastifile EULA, click end-user license agreement.

As this is the first time you are logging in, you are prompted to change your login password.

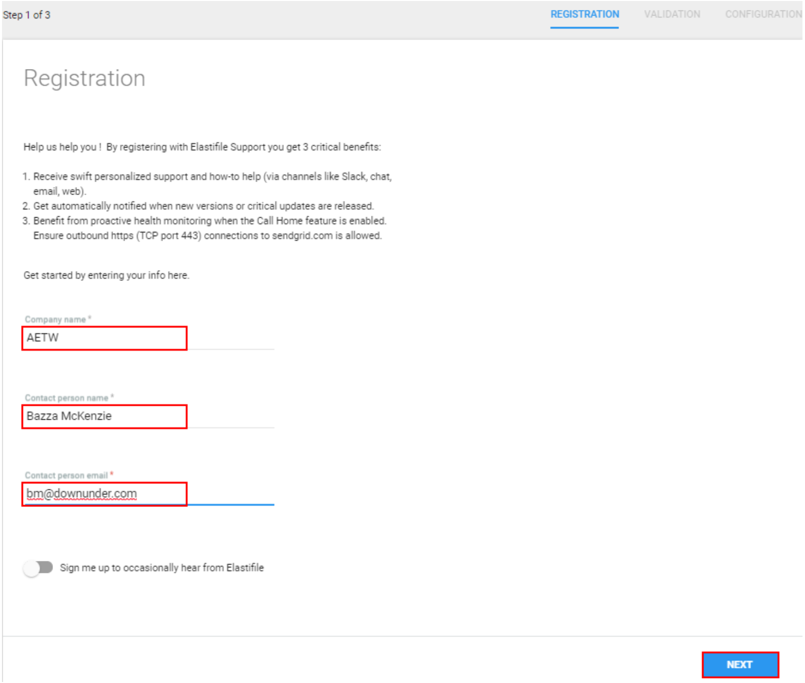
You can now configure the ECFS system.

5. Configuring and Deploying ECFS

After logging into the ECFS and changing the temporary password, you can deploy your system.

To deploy the ECFS:

1. In the **Registration** window, fill in the required details and click **NEXT**.



Step 1 of 3

Registration

Help us help you ! By registering with Elastifile Support you get 3 critical benefits:

1. Receive swift personalized support and how-to help (via channels like Slack, chat, email, web).
2. Get automatically notified when new versions or critical updates are released.
3. Benefit from proactive health monitoring when the Call Home feature is enabled. Ensure outbound https (TCP port 443) connections to sendgrid.com is allowed.

Get started by entering your info here.

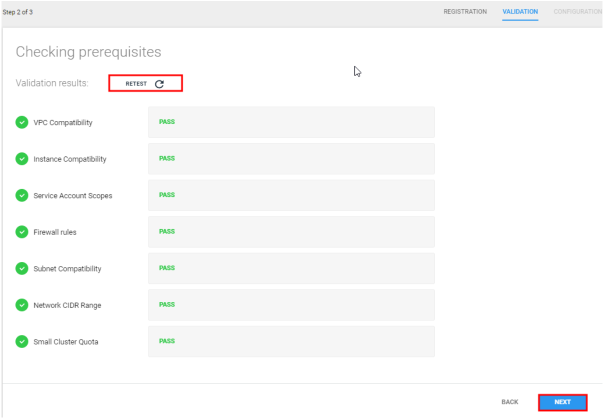
Company name *: AETW

Contact person name *: Bazza McKenzie

Contact person email *: bm@downunder.com

Sign me up to occasionally hear from Elastifile

2. In the **Validation** window, the prerequisites are tested automatically. If a test fails, fix the error and click **RETEST**. If all tests pass, click **NEXT**.



Step 2 of 3

Checking prerequisites

Validation results: RETEST

✓ VPC Compatibility	PASS
✓ Instance Compatibility	PASS
✓ Service Account Scopes	PASS
✓ Firewall rules	PASS
✓ Subnet Compatibility	PASS
✓ Network CIDR Range	PASS
✓ Small Cluster Quota	PASS

If the **VPC Compatibility** test fails, select and delete the installation, then try to reinstall in another VPC (legacy network is not supported).

- Deployment creates firewall rules to allow communication between the ECFS instances. If there is a policy in your project that prevents firewall rule creation, you must manually create the firewall rules as follows:

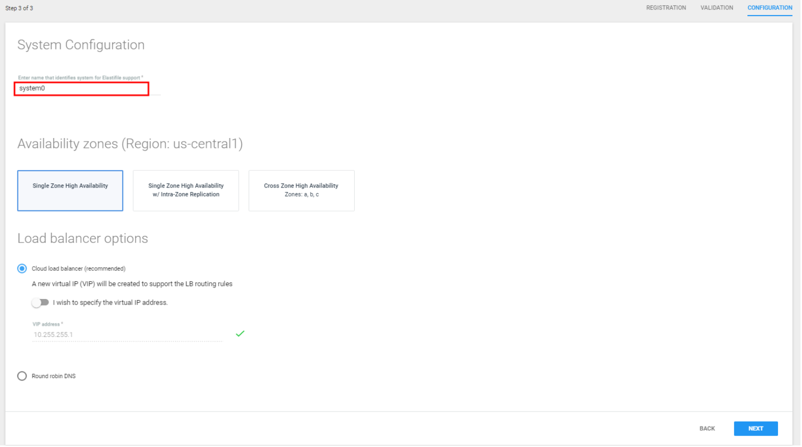
  Name: elastifile-storage-management
  source range: vpc-network cidr
  source tags: elastifile-storage-node, elastifile-replication-node, elastifile-clients
  target tags: elastifile-management-node
  - **ICMP**
  - **TCP**: 22,53,80,8080,443,10014-10018, 10028
  - **UDP**: 53, 123, 6667

  Name: elastifile-storage-service
  source range: vpc-network cidr
  source tags: elastifile-management-node, elastifile-storage-node, elastifile-replication-node, elastifile-clients
  target tags: elastifile-storage-node, elastifile-replication-node
  - **ICMP**
  - **TCP**: 22,111,443,2049,644,4040,4045,10015-10017,8000-9224,12121,32768-60999
  - **UDP**: 111, 2049, 644, 4040, 4045, 6667, 8000-9224,32768-60999

  Name: elastifile-clients
  source tags: elastifile-storage-node
  target tags: elastifile-clients, elastifile-replication-node
  - **UDP**: all

- The firewall rules accept traffic from instances with the elastifile-clients network tag. This tag can be used on customer instances outside the VPC network to access ECFS's storage service.

3. In the **System Configuration** window, type a name (maximum 40 characters) that identifies the system.



System Configuration

Enter name that identifies system for Elastifile support *: system0

Availability zones (Region: us-central1)

Single Zone High Availability | Single Zone High Availability w/ Intra-Zone Replication | Cross Zone High Availability Zones: a, b, c

Load balancer options

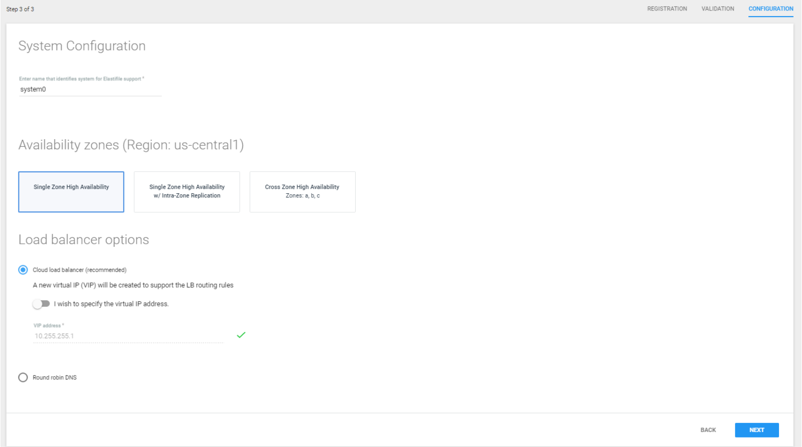
● Cloud load balancer (recommended)
A new virtual IP (VIP) will be created to support the LB routing rules
I wish to specify the virtual IP address.
VIP address *: 10.255.255.1

○ Round robin DNS

You must change the default name (**system0**).

4. In the **Availability zones** area, choose one of the following:

   - **Single Zone High Availability** - Provides high availability within a single availability zone by leveraging the native durability of Google Cloud persistent disks. ECFS data is not replicated, thus enabling use of the entire allocated raw storage capacity.
     When using this option, an unexpected storage node failure may cause a temporary interruption of service. In such instances, the storage node will be automatically restarted and reconnected to the same persistent disk, and normal service will resume. No data will be lost and the resumption of service typically occurs before timeout period expires for most applications .


Step 3 of 3
REGISTRATION
VALIDATION
CONFIGURATION

System Configuration

Enter name that identifies system for Elastifile support *: system0

Availability zones (Region: us-central1)

Single Zone High Availability
Single Zone High Availability w/ Intra-Zone Replication
Cross Zone High Availability Zones: a, b, c

Load balancer options

● Cloud load balancer (recommended)

A new virtual IP (VIP) will be created to support the LB routing rules

I wish to specify the virtual IP address.

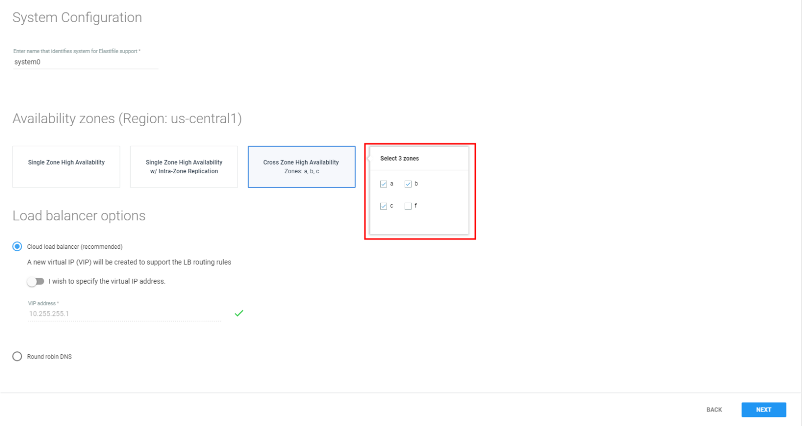
VIP address *: 10.255.255.1 ✓

○ Round robin DNS

   - **Single Zone High Availability w/ Intra-Zone Replication** - Provides high availability within a single availability zone by leveraging ECFS data replication, thus preventing any service interruption in the event of a storage node failure.

   - **Cross Zone High Availability Zones a, b, c** - Provides high availability by leveraging ECFS data replication across multiple availability zones, thus preventing any service interruption in the event of a storage node failure or a full availability zone failure.

     If you select **Cross Zone High Availability Zones a, b, c**, then **Select 3 Zones** appears. Select the check boxes of your required 3 zones.



System Configuration

Enter name that identifies system for Elastifile support *: system0

Availability zones (Region: us-central1)

Single Zone High Availability
Single Zone High Availability w/ Intra-Zone Replication
Cross Zone High Availability Zones: a, b, c

Select 3 zones

☑ a ☑ b

☑ c ☐ f

Load balancer options

● Cloud load balancer (recommended)

A new virtual IP (VIP) will be created to support the LB routing rules

I wish to specify the virtual IP address.

VIP address *: 10.255.255.1 ✓

○ Round robin DNS

5. In the **Load balancer options** area, choose either **Cloud load balancer** or **Round robin DNS** and configure as described following:

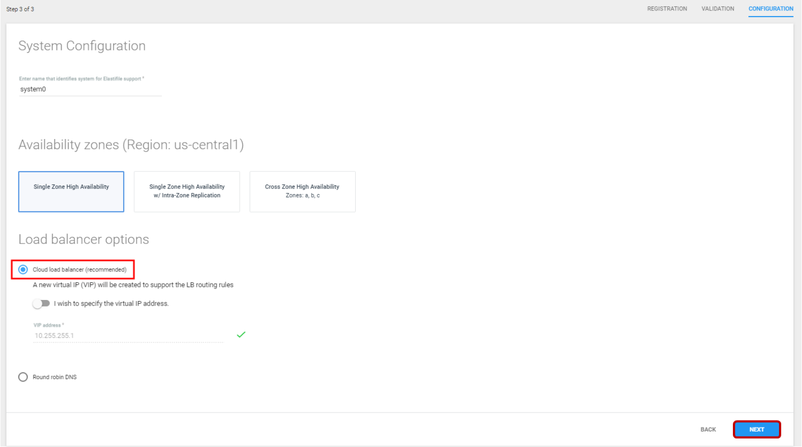
> Elastifile recommends using the Cloud load balancer option. You cannot change this setting later.

- Cloud load balancer:

To configure the VIP automatically:

i. Select **Cloud load balancer**. The system will try to allocate a virtual IP address. If the message **Could not automatically detect an available VIP address** is displayed, skip to the next step (To configure the VIP manually).

ii. Click **Next**.



System Configuration

Enter name that identifies system for Elastifile support *: system0

Availability zones (Region: us-central1)

Single Zone High Availability | Single Zone High Availability w/ Intra-Zone Replication | Cross Zone High Availability Zones: a, b, c

Load balancer options

● Cloud load balancer (recommended)

A new virtual IP (VIP) will be created to support the LB routing rules

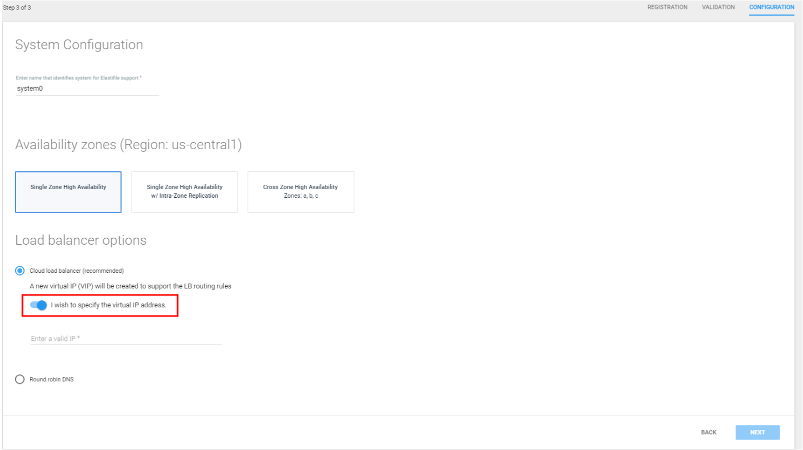
I wish to specify the virtual IP address.

VIP address *: 10.255.255.1 ✓

○ Round robin DNS

To configure the VIP manually:

i. Click the **I wish to specify the virtual IP address** toggle switch and specify an unused virtual IP address.



System Configuration

Enter name that identifies system for Elastifile support *: system0

Availability zones (Region: us-central1)

Single Zone High Availability | Single Zone High Availability w/ Intra-Zone Replication | Cross Zone High Availability Zones: a, b, c

Load balancer options

● Cloud load balancer (recommended)

A new virtual IP (VIP) will be created to support the LB routing rules

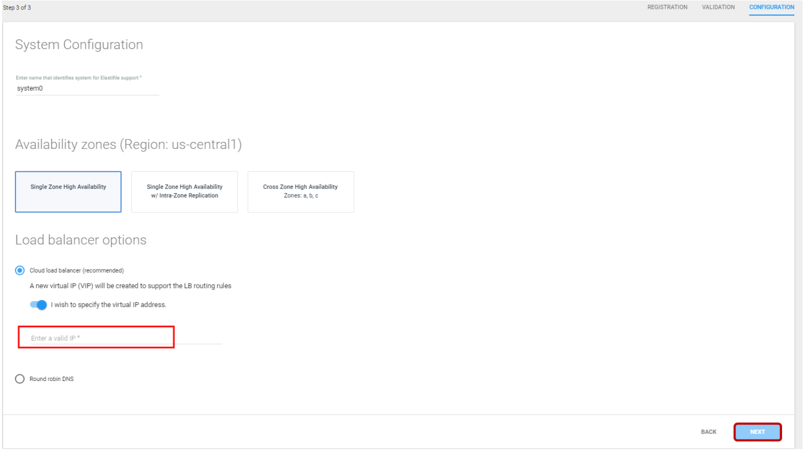
I wish to specify the virtual IP address.

Enter a valid IP *

○ Round robin DNS

ii. Type your required virtual IP address. The IP address is validated.

iii. Click **NEXT**.



System Configuration

Enter name that identifies system for Elastifile support *: system0

Availability zones (Region: us-central1)

Single Zone High Availability | Single Zone High Availability w/ Intra-Zone Replication | Cross Zone High Availability Zones: a, b, c

Load balancer options

● Cloud load balancer (recommended)

A new virtual IP (VIP) will be created to support the LB routing rules

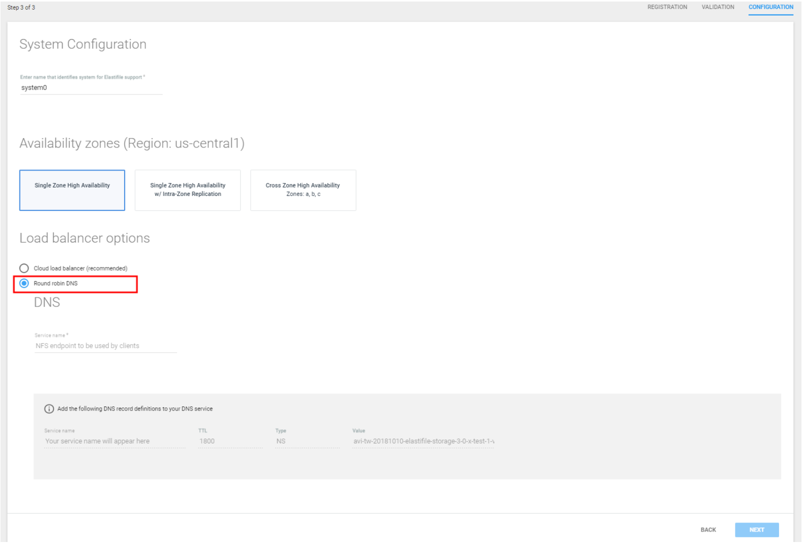
I wish to specify the virtual IP address.

Enter a valid IP *

○ Round robin DNS

- Round robin DNS

  i. Select **Round robin DNS**.



System Configuration

Enter name that identifies system for Elastifile support *
system0

Availability zones (Region: us-central1)

Single Zone High Availability | Single Zone High Availability w/ Intra-Zone Replication | Cross Zone High Availability Zones: a, b, c

Load balancer options

○ Cloud load balancer (recommended)
● Round robin DNS

DNS

Service name *
NFS endpoint to be used by clients

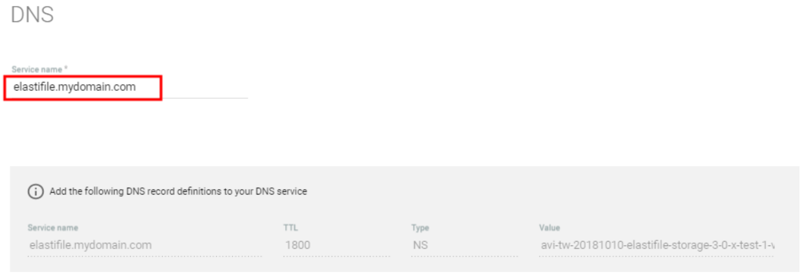
Add the following DNS record definitions to your DNS service

Service name	TTL	Type	Value
Your service name will appear here	1800	NS	avi-tw-20181010-elastifile-storage-3-0-x-test-1-v

  ii. In **Service name**, type a fully-qualified domain name for the NFS endpoint.

  iii. The DNS record definitions appear. Add them to your DNS service.

  iv. Click **NEXT**.



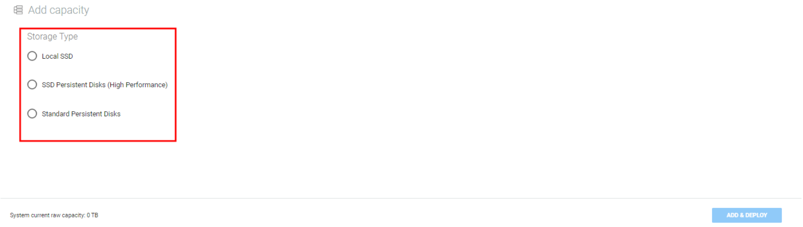
DNS

Service name *
elastifile.mydomain.com

Add the following DNS record definitions to your DNS service

Service name	TTL	Type	Value
elastifile.mydomain.com	1800	NS	avi-tw-20181010-elastifile-storage-3-0-x-test-1-v

6. To add capacity to the ECFS, select the storage suited to your performance requirements and set the size. Choose either:

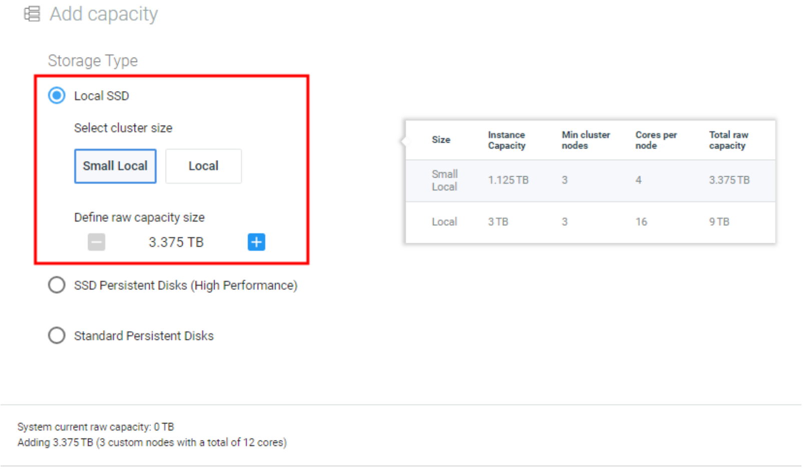


Add capacity

Storage Type
○ Local SSD
○ SSD Persistent Disks (High Performance)
○ Standard Persistent Disks

System current raw capacity: 0 TB

- **Local SSD**
  - In **Select cluster size**, select either:
    - **Small Local**
    - **Local**



Add capacity

Storage Type
● Local SSD

Select cluster size
Small Local | Local

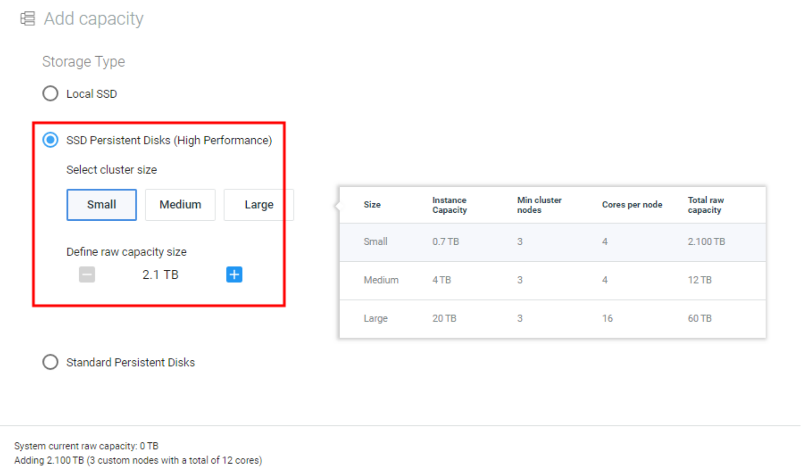
Define raw capacity size
3.375 TB

○ SSD Persistent Disks (High Performance)
○ Standard Persistent Disks

Size	Instance Capacity	Min cluster nodes	Cores per node	Total raw capacity
Small Local	1.125 TB	3	4	3.375 TB
Local	3 TB	3	16	9 TB

System current raw capacity: 0 TB
Adding 3.375 TB (3 custom nodes with a total of 12 cores)

- **SSD Persistent Disks (High Performance)**
  - In **Select cluster size**, select either:
    - **Small**
    - **Medium**
    - **Large**



Add capacity

Storage Type

○ Local SSD

● SSD Persistent Disks (High Performance)

Select cluster size

Define raw capacity size

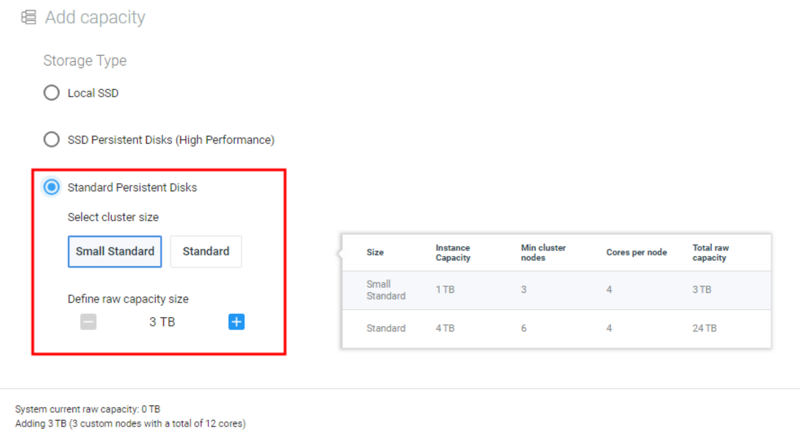
2.1 TB

Size	Instance Capacity	Min cluster nodes	Cores per node	Total raw capacity
Small	0.7 TB	3	4	2.100 TB
Medium	4 TB	3	4	12 TB
Large	20 TB	3	16	60 TB

○ Standard Persistent Disks

System current raw capacity: 0 TB
Adding 2.100 TB (3 custom nodes with a total of 12 cores)

- **Standard Persistent Disks**
  - In **Select cluster size**, select either:
    - **Small Standard**
    - **Standard**



Add capacity

Storage Type

○ Local SSD

○ SSD Persistent Disks (High Performance)

● Standard Persistent Disks

Select cluster size

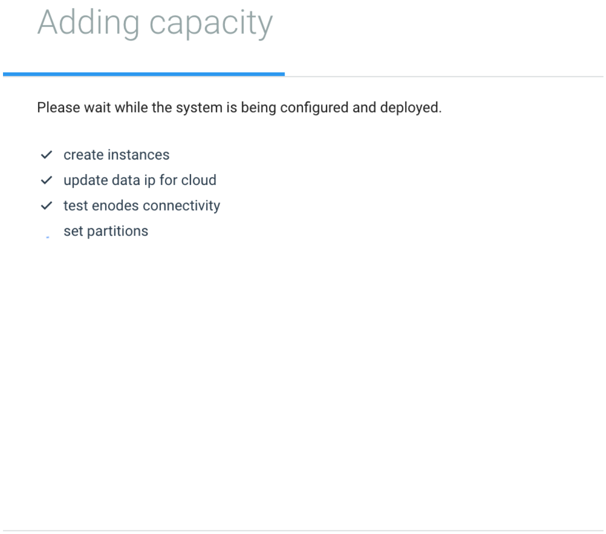
Define raw capacity size

3 TB

Size	Instance Capacity	Min cluster nodes	Cores per node	Total raw capacity
Small Standard	1 TB	3	4	3 TB
Standard	4 TB	6	4	24 TB

System current raw capacity: 0 TB
Adding 3 TB (3 custom nodes with a total of 12 cores)

7. In **Define raw capacity size** set your required size.
8. Click **ADD & DEPLOY**.
9. The ECFS starts configuration and deployment.

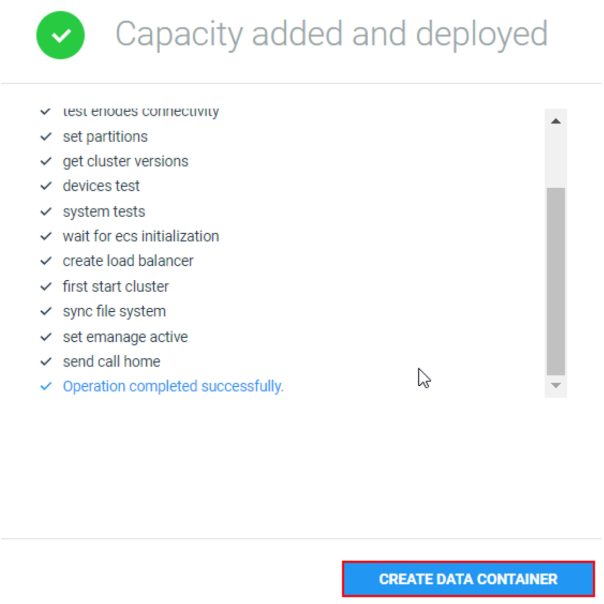


Adding capacity

Please wait while the system is being configured and deployed.

✓ create instances
✓ update data ip for cloud
✓ test enodes connectivity
set partitions

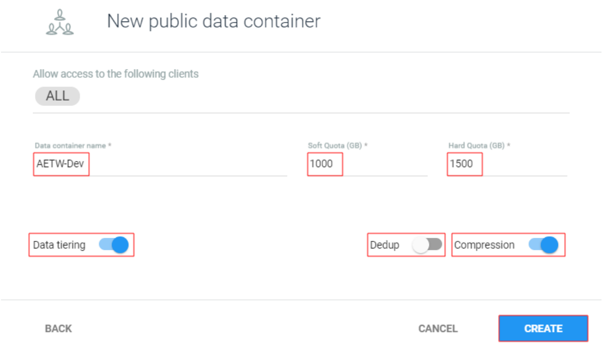
10. When the **Operation completed successfully** message appears, click **CREATE DATA CONTAINER**.



Capacity added and deployed

✓ test enodes connectivity
✓ set partitions
✓ get cluster versions
✓ devices test
✓ system tests
✓ wait for ecs initialization
✓ create load balancer
✓ first start cluster
✓ sync file system
✓ set emanage active
✓ send call home
✓ Operation completed successfully.

11. In the **New public data container** window:
    a. Type a name for your new data container.
    b. Set the soft and hard quotas.
    c. Set the data tiering to enabled or disabled (for more details, see the ECFS Management Console User Guide).



New public data container

Allow access to the following clients: ALL

Data container name *: AETW-Dev

Soft Quota (GB) *: 1000

Hard Quota (GB) *: 1500

Data tiering: on

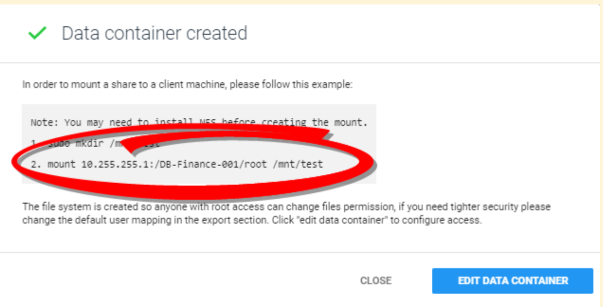
Dedup: off

Compression: on

Data tiering is not applicable if installing and using ECFS on GCP Marketplace.

    d. Select a data policy with corresponding dedup and compression settings.
    e. Click **CREATE**. The data container is created.

Note the mount command to use on your client.



✓ Data container created

In order to mount a share to a client machine, please follow this example:

```
Note: You may need to install NFS before creating the mount.
1. sudo mkdir /mnt/test
2. mount 10.255.255.1:/DB-Finance-001/root /mnt/test
```

The file system is created so anyone with root access can change files permission, if you need tighter security please change the default user mapping in the export section. Click "edit data container" to configure access.

12. You can either click **CLOSE**, or click **EDIT DATA CONTAINER** to configure client access to the data container (for more details, see the ECFS Management Console User Guide).

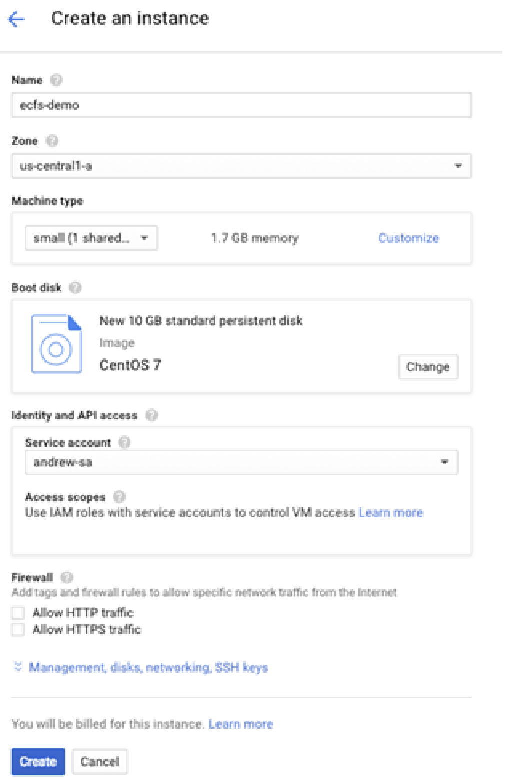
Appendix A. Configuring a CentOS Client for Operation with ECFS

A.1 Creating a CentOS Instance (Optional)

The CentOS client must be in same zone (or for regional instances in the same region) as the ECFS system.

1. Create a Centos instance on a client.

The parameters in the following figure are only examples:



Create an instance

Name: ecfs-demo

Zone: us-central1-a

Machine type: small (1 shared... 1.7 GB memory

Boot disk: New 10 GB standard persistent disk
Image
CentOS 7

Identity and API access

Service account: andrew-sa

Access scopes
Use IAM roles with service accounts to control VM access Learn more

Firewall
Add tags and firewall rules to allow specific network traffic from the Internet
□ Allow HTTP traffic
□ Allow HTTPS traffic

You will be billed for this instance. Learn more

A.2 Configuring the NFS Mount

1. Connect to the client VM via SSH using the following command:

```
gcloud compute --project "<project name>" ssh --zone "<zone name>" "<instance name>"
```

A.3 Add NFS

1. Add the EMS to network interface DNS:

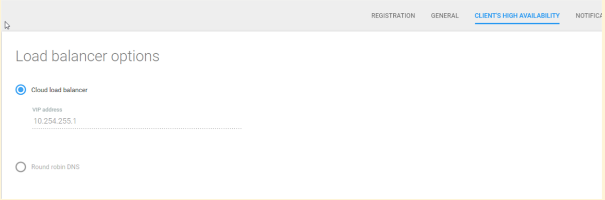
```
$ sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0
PEERDNS=no
DNS1=<EMS IP>
DNS2=8.8.8.8
sudo systemctl restart network
```

2. Verify that the NFS can access the Load Balancer IP / DNS service name specified in the EMS:

To access the DNS service name:

a. In the ECFS Management Console, in the header, click ⚙ (**ADMINISTRATION**), click **System Settings** and click **Client 's High Availability**.

b. Under **Load balancer options**, note the **VIP address** or **Round robin DNS** (only one of them is active, according to what you selected in Step 5) of Section 5 - Configuring and Deploying ECFS).



Load balancer options

● Cloud load balancer

VIP address
10.254.255.1

○ Round robin DNS

```
$ showmount -e <Load Balancer IP/ DNS Service Name>
Export list for <Load Balancer IP/ DNS Service Name>:
....
```

If showmount is not found, install nfs-utils:

```
$ sudo yum install nfs-utils
```

3. Create a directory on which to mount the ECFS NFS:

```
mkdir /mnt/<mount point>
```

A.4 Mounting the Elastifile Service

1. Mount the ECFS NFS using the mount command you noted after the data container was created (see Section 5 - Configuring and Deploying ECFS Step).

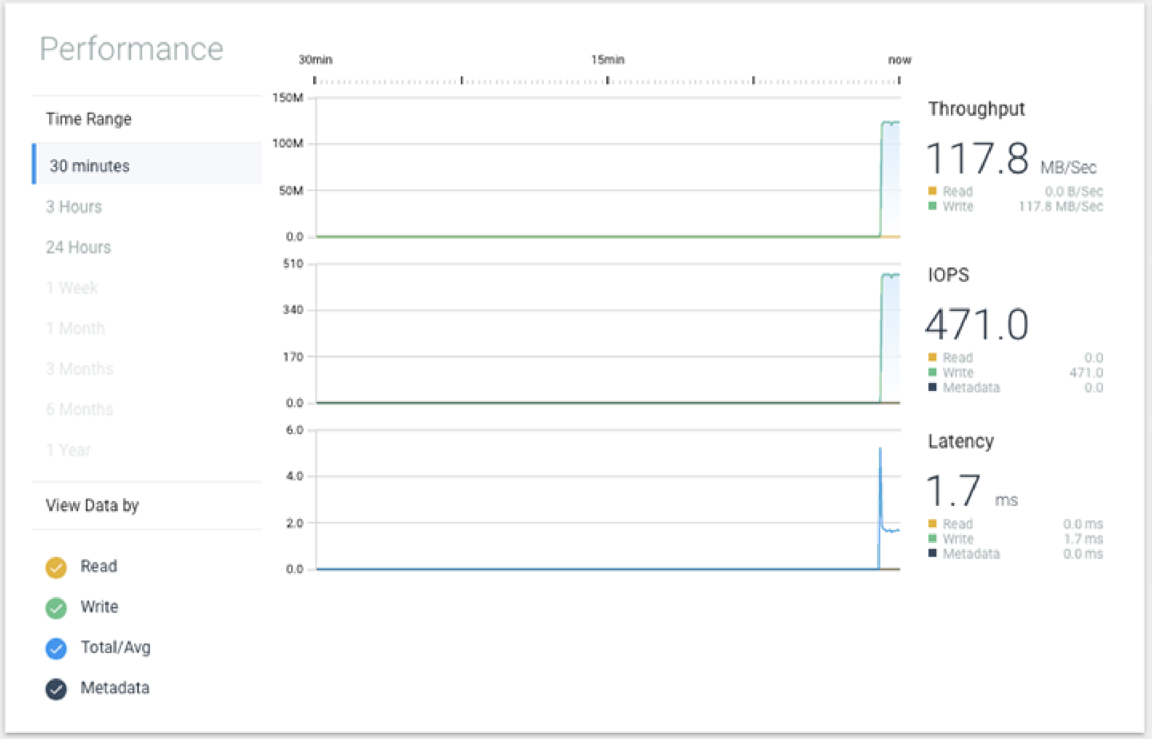
```
mount <XX.XX.X.X:/DC name/root> /mnt/<mount point>
```

For example: mount 10.99.0.2:DC-aetw/root /mnt/finance

2. Verify NFS connectivity and I/O:

```
$ cd /mnt/<mount point
$ dd if=/dev/zero of=/mnt/<mount point>/file1 bs=1GB count=10
10+0 records in
10+0 records out
```

3. In the ECFS Management Console dashboard, view the performance:



Throughput
117.8 MB/Sec
■ Read 0.0 B/Sec
■ Write 117.8 MB/Sec

IOPS
471.0
■ Read 0.0
■ Write 471.0
■ Metadata 0.0

Latency
1.7 ms
■ Read 0.0 ms
■ Write 1.7 ms
■ Metadata 0.0 ms