elastifile

Cross-Cloud Data Fabric

Elastifile 2.7.0

Google Cloud Platform (GCP)

Launcher Deployment Guide

June 2018

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

2. Installing the ECFS Using the GCP Launcher **5**

3. Deploying Elastifile **8**

Appendix A. Configuring a CentOS Client for Operation with Elastifile **13**

A.1 Creating a CentOS Instance (Optional) 13

A.2 Configuring the NFS Mount 13

A.3 Add NFS 13

1. Introduction

1.1 Document Scope

This guide describes the installation process for creating Elastifile 2.7.0 systems in a Google Cloud Platform (GCP) environment using the ECFS GCP Launcher.

1.2 System Overview

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

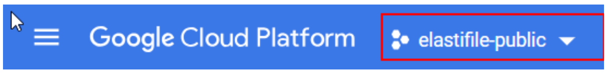
- Elastifile Management System (EMS) - the Elastifile management instance that controls the Elastifile system.
- Controller - an instance that provides storage resources and client access.
- Application services - an instance that provides additional services such as replication for disaster recovery.

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

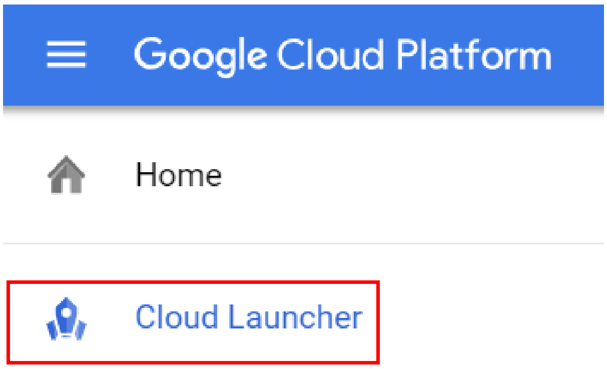
The EMS and controllers are installed on GCP instances.

2. Installing the ECFS Using the GCP Launcher

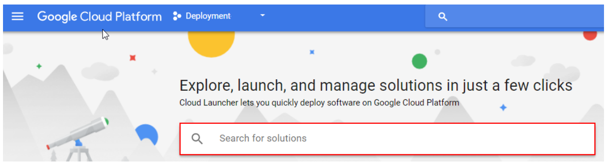
1. In the Google Cloud Platform Console, select your project.



2. Click **Cloud Launcher**.



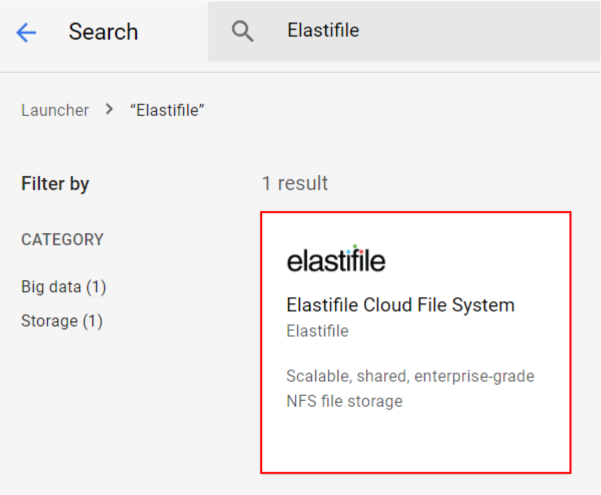
3. In the Search for solutions bar, type Elastifile.



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.

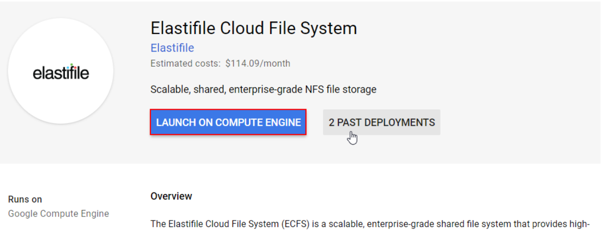


Elastifile Cloud File System

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

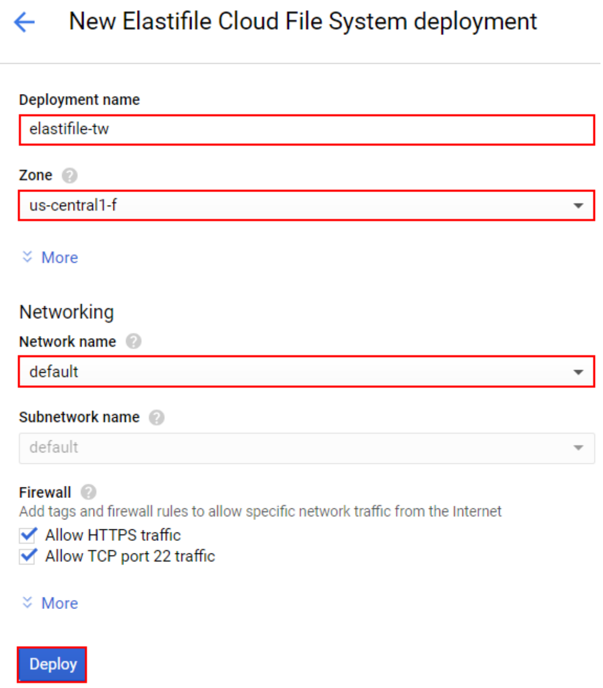
Runs on
Google Compute Engine

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

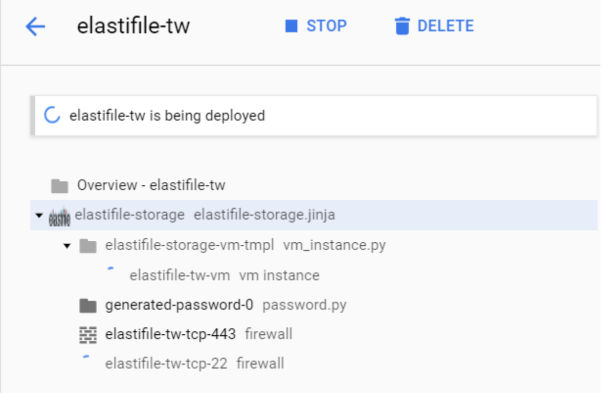
Firewall

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

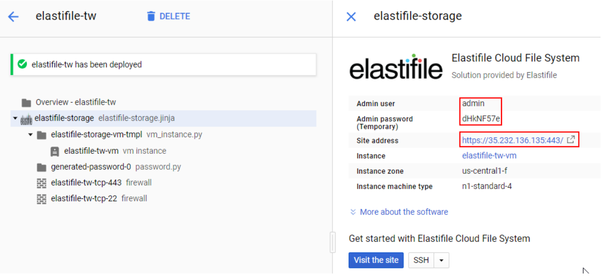
elastifile-tw is being deployed

- 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 Elastifile for the first time.

   b. Click the **Site address** URL to open the Elastifile Management Console.



elastifile-tw

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-storage

Elastifile Cloud File System

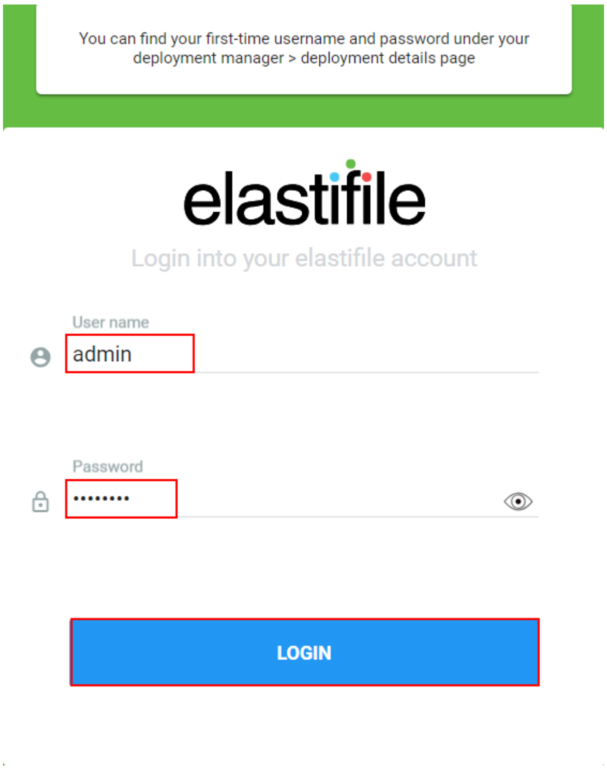
Solution provided by Elastifile

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**.



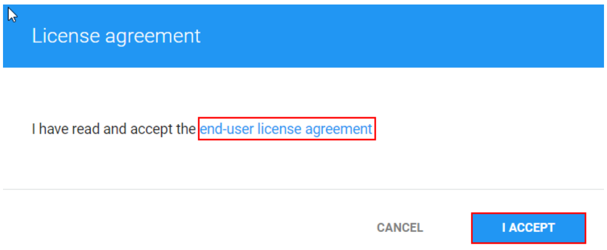
You can find your first-time username and password under your deployment manager > deployment details page

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).

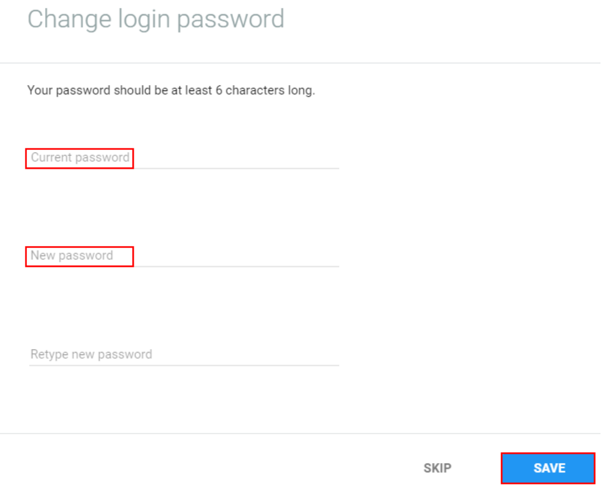


License agreement

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

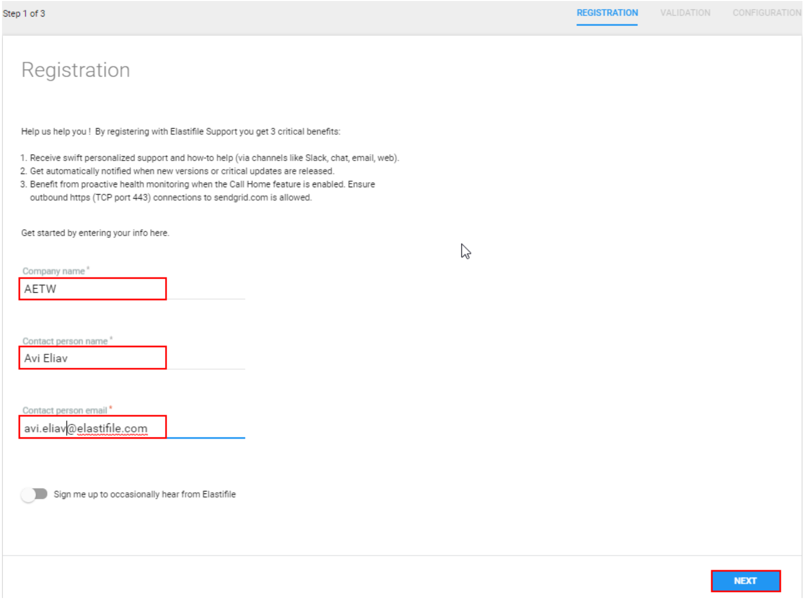
Retype new password

3. Deploying Elastifile

After logging into the Elastifile system 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**.



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.

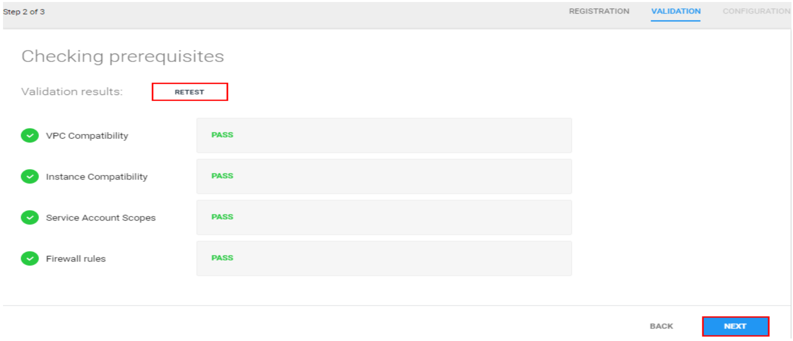
Company name * AETW

Contact person name * Avi Eliav

Contact person email * avi.eliav@elastifile.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**.



Checking prerequisites

Validation results: RETEST

✓ VPC Compatibility	PASS
✓ Instance Compatibility	PASS
✓ Service Account Scopes	PASS
✓ Firewall rules	PASS

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

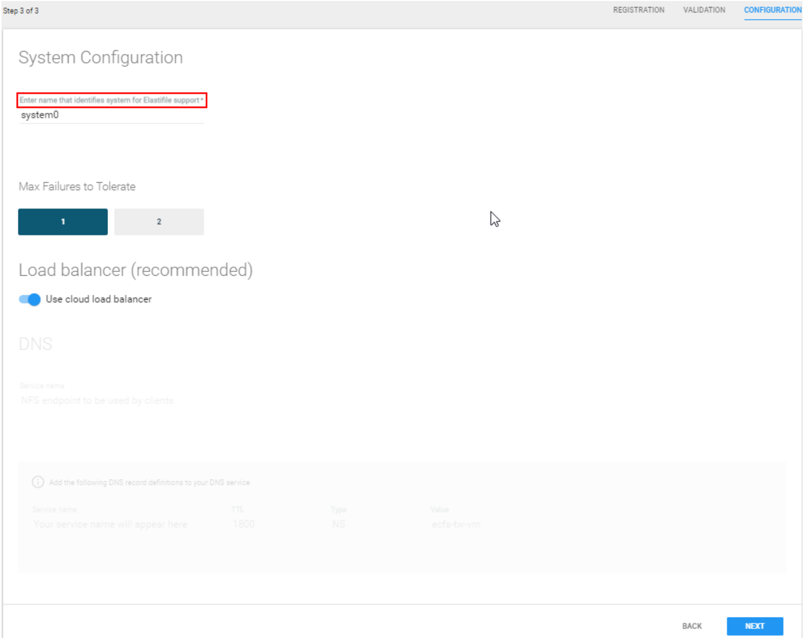
- Deployment creates firewall rules to allow communication between the Elastifile instances. If there is a policy in your project that prevents firewall rule creation, you must manually create the firewall rules as follows:

  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**: 22,53,80,8080,443,10014-10017
  - **UDP**: 53, 123

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

- 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 Elastifile's storage service.

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



System Configuration

Enter name that identifies system for Elastifile support *
system0

Max Failures to Tolerate

Load balancer (recommended)
Use cloud load balancer

DNS

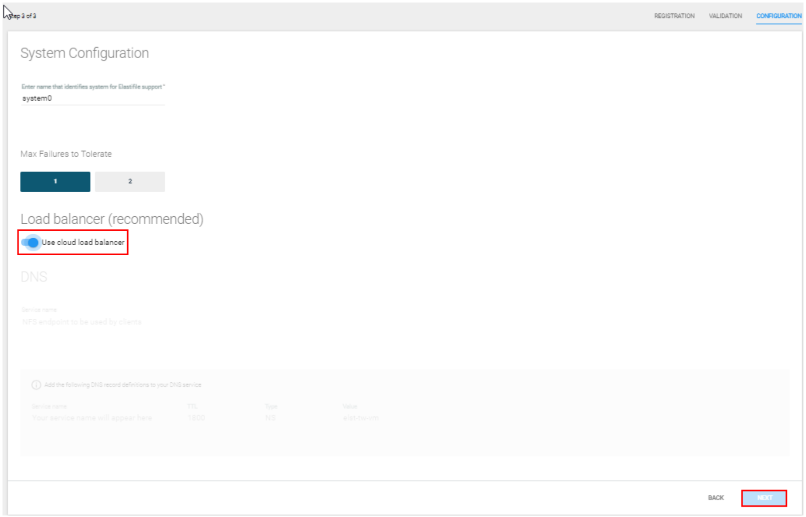
Service name
NFS endpoint to be used by clients

Add the following DNS record definitions to your DNS service

Service name	TTL	Type	Value
Your service name will appear here	1800	NS	ecfs-tw-vm

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

4. The cloud load balancer slider is set to on by default.
   Either:
   - Use the cloud load balancer and click **NEXT**.



Step 3 of 3

System Configuration

Enter name that identifies system for Elastifile support*: system0

Max Failures to Tolerate: ● 1 ○ 2

Load balancer (recommended)

● Use cloud load balancer

DNS

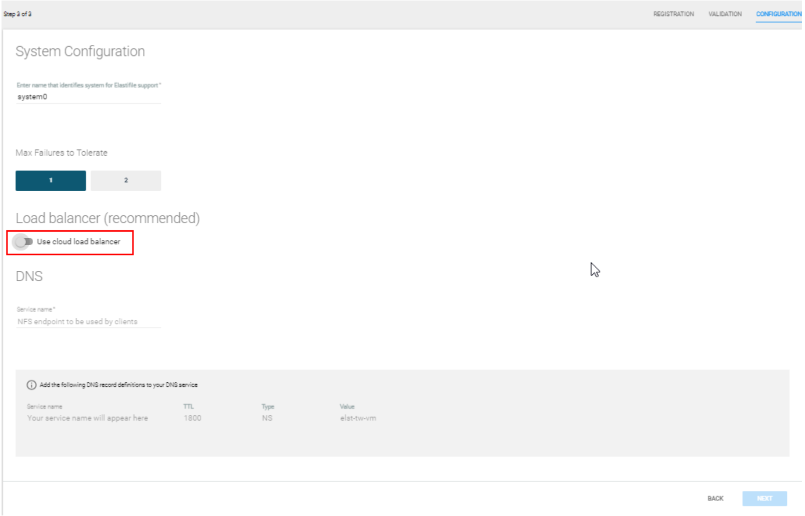
Service name: NFS endpoint to be used by clients

Add the following DNS record definitions to your DNS service

Service name	TTL	Type	Value
Your service name will appear here	1800	NS	elst-tw-vm

Elastifile recommends using the cloud load balancer. You cannot change this setting later.

   - Move the slider left to use the DNS service that runs on the EMS. The DNS service provides a single hostname for NFS clients to access all nodes in the cluster entered as domain name format.



Step 3 of 3

System Configuration

Enter name that identifies system for Elastifile support*: system0

Max Failures to Tolerate: ● 1 ○ 2

Load balancer (recommended)

○ Use cloud load balancer

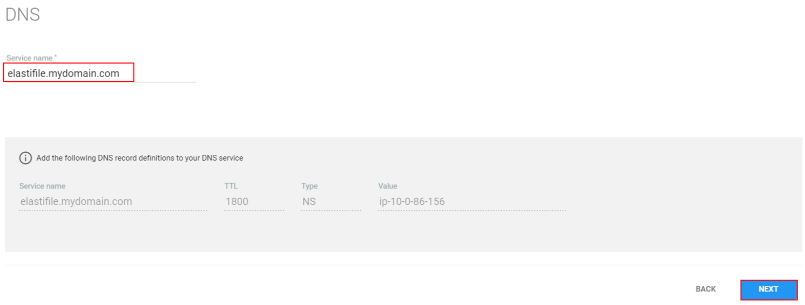
DNS

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	elst-tw-vm

     i. In **Service name**, type a fully-qualified domain name for the NFS endpoint.
     ii. The DNS record definitions appear. Add them to your DNS service.
     iii. Click **NEXT**.



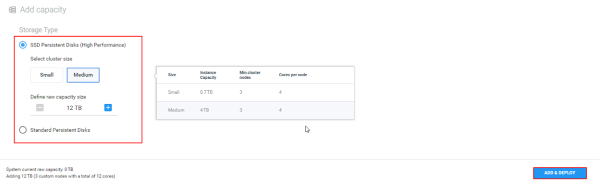
DNS

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	ip-10-0-86-156

5. To add capacity to the ECFS, select the storage suited to your performance requirements and costs, and click **ADD & DEPLOY**.



Add capacity

Storage Type

● SSD Persistent Disks (High Performance)

Select cluster size

Small [✓ Medium]

Define raw capacity size

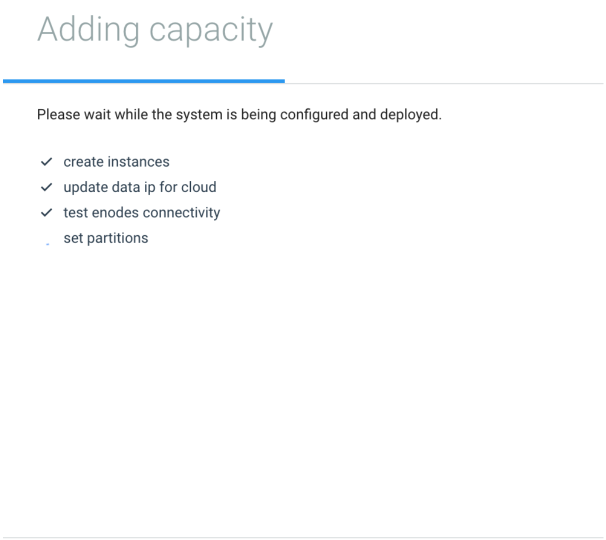
12 TB

○ Standard Persistent Disks

Size	Instance Capacity	Min cluster nodes	Cores per node
Small	0.7 TB	3	4
Medium	4 TB	3	4

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

6. The ECFS starts configuration and deployement.

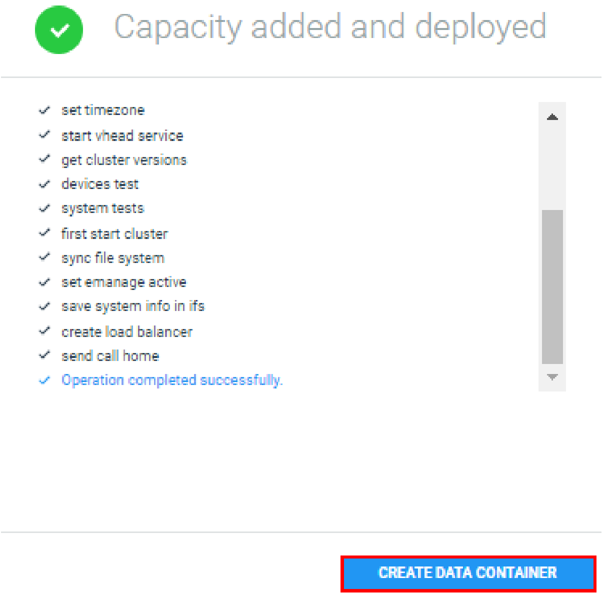


Adding capacity

Please wait while the system is being configured and deployed.

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

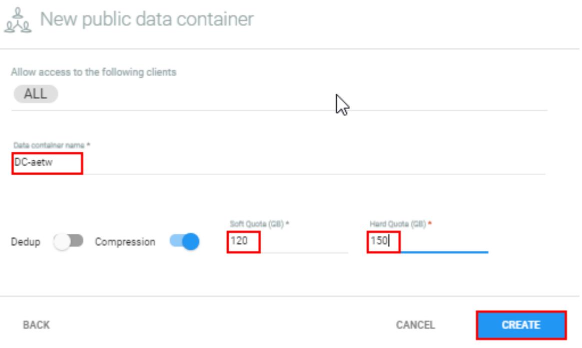
7. When the **Operation completed successfully** message appears, click **CREATE DATA CONTAINER**.



Capacity added and deployed

✓ set timezone
✓ start vhead service
✓ get cluster versions
✓ devices test
✓ system tests
✓ first start cluster
✓ sync file system
✓ set emanage active
✓ save system info in ifs
✓ create load balancer
✓ send call home
✓ Operation completed successfully.

8. Type a name for your new data container, set the soft and hard quotas and click **CREATE**.



New public data container

Allow access to the following clients: ALL

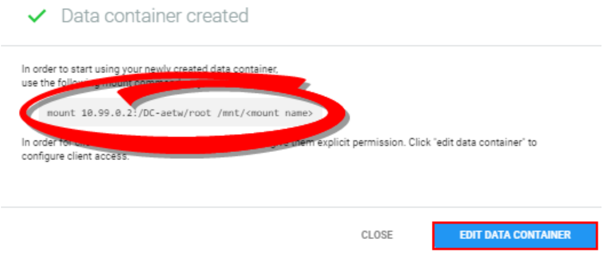
Data container name *: DC-aetw

Dedup ○ Compression ●

Soft Quota (GB) *: 120

Hard Quota (GB) *: 150

9. The data container is created. Note the mount command to use on your client.
To configure client access to the data container, click **EDIT DATA CONTAINER**.



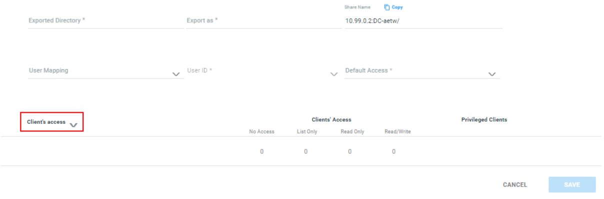
Data container created

In order to start using your newly created data container, use the foll[illegible] mount comm[illegible]

```
mount 10.99.0.2:/DC-aetw/root /mnt/<mount name>
```

In order for [illegible] them explicit permission. Click "edit data container" to configure client access.

10. In the Exports section, click **Client's access**.



Exported Directory *

Export as *

Share Name: 10.99.0.2:DC-aetw/

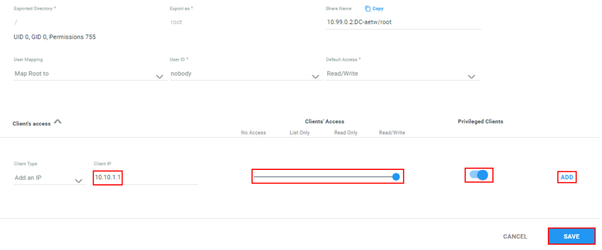
User Mapping

User ID *

Default Access *

Client's access	Clients' Access				Privileged Clients
	No Access	List Only	Read Only	Read/Write	
	0	0	0	0	

11. Type the **Client IP**, set the **Client's Access** to **Read/Write**, set the **Privileged Client** slider to on, click **ADD** and click **SAVE**.



Exported Directory *: /

UID 0, GID 0, Permissions 755

Export as *: root

Share Name: 10.99.0.2:DC-aetw/root

User Mapping: Map Root to

User ID *: nobody

Default Access *: Read/Write

Client's access	Clients' Access				Privileged Clients
	No Access	List Only	Read Only	Read/Write	

Client Type: Add an IP

Client IP: 10.10.1.1

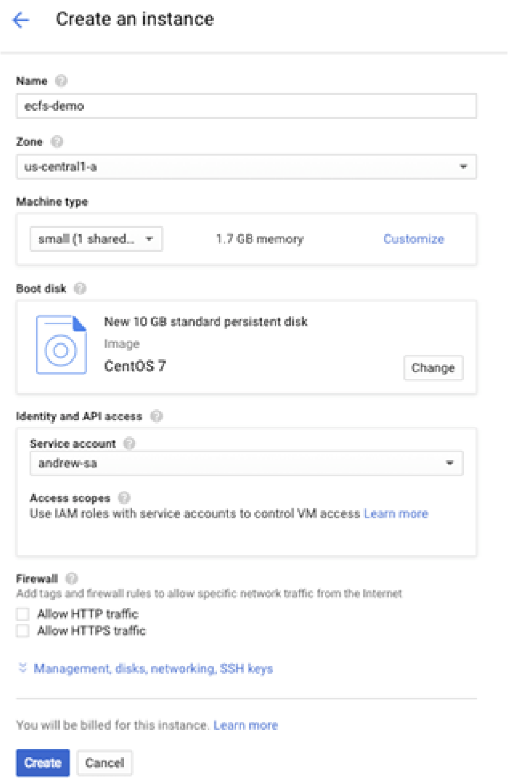
Appendix A. Configuring a CentOS Client for Operation with Elastifile

A.1 Creating a CentOS Instance (Optional)

The CentOS client must be in same zone as the Elastifile 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 DNS service name specified in the EMS.

To access the DNS service name:

a. In the Elastifile Management Console, in the header, click ⚙ (**ADMINISTRATION**).

b. Click **System Settings**.

c. Click **Client Networks**.

d. Scroll down to **Service name**.

```
$ showmount -e <DNS service name>
Export list for <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 Elastifile NFS:

```
mkdir /mnt/<mount name>
```

4. Mount the Elastifile NFS using the mount command you noted after the data container was created (see Section 3 - Deploying Elastifile Step 9):

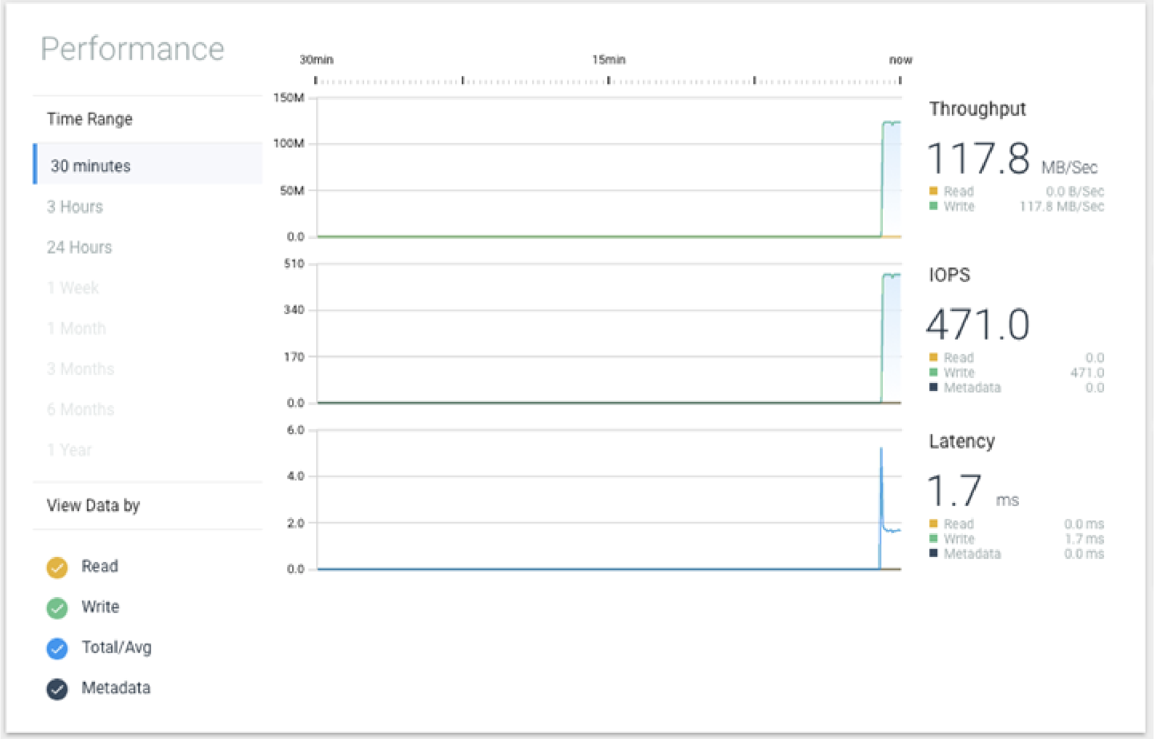
```
mount <XX.XX.X.X:/DC name/root> /mnt/<mount name>
```

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

5. Verify NFS connectivity and throughput:

```
$ cd /mnt/<mount name>
$ dd if=/dev/zero of=/mnt/<mount name>/file1 bs=1GB count=10
10+0 records in
10+0 records out
10000000000 bytes (10 GB) copied, 82.1757 s, 122 MB/s
```

6. In the Elastifile 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