ECFS (Elastifile Cloud File System) 2.7.X
Dedicated Storage Mode (DSM)

Installation Guide

August 2018

Document Revision: 1.0

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

1.1 Document Scope

This guide describes the installation process for creating ECFS 2.7.X systems based on Dedicated Storage Mode (DSM).

1.2 Installation Overview

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

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

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

EMSs are installed on virtual or physical hosts and controllers are installed on physical servers.

1.3 Installation Flow

The installation flow consists of the following main steps:

1. Validating requirements and configurations of the network and server hardware (see Section 2 - Hardware Requirements).
2. Preparing the environment (see Section 3 - Preparing the Environment for Installation).
3. Setting up the ECFS system as follows:
   - deploying a primary EMS on a separate VM or physical server (see Section 4 - Installing the EMS).
   - deploying controllers on servers (see Section 6 - Deploying ECFS).
   - deploying a secondary EMS on an additional VM or physical server (see Section 7 - Installing the Secondary EMS).

The primary EMS, controllers and secondary EMS are all installed from a Linux machine that runs the Elastifile installer file.

2. Hardware Requirements

2.1 General

Ensure that your hardware is compatible with the latest Red Hat Hardware Compatibility List.

2.2 Network

2.2.1 Switch

ECFS's Data Network expects a 10GbE connection. In addition, we highly recommend a dedicated VLAN with MTU 9000 (jumbo) frame support for its internode data communication. ECFS uses the VLAN to isolate its internal IP scheme.

The network switch should meet the following port configuration requirements:

- Minimum 10GbE full duplex; 25/40/100GbE also supported
- MTU=9000 - highly recommended
- Dedicated VLAN (trunk or access mode) - highly recommended

ECFS requires using two 10GBe switches minimum (one switch for each ECFS network).

2.2.2 NICs

NICs used in the ECFS networks should meet the following requirements:

- 2 x 10GbE for the data network
- 10GbE minimum for the client network
- SR-IOV must be off for DSM

2.3 Storage

2.3.1 Storage Devices

- Up to 12 devices per Dedicated Storage node
- Maximum device size: 4TB
- Minimum data center grade devices:
  - NVMe SSD
  - SATA SSD

2.3.2 Disk Controllers

No RAID Controller is needed.

If the Disk Controller has a RAID controller, disable it and configure the controller to operate in JBOD mode.

2.4 Host Resources

2.4.1 EMS Hardware Requirements

The EMS can be installed as a physical server or a virtual server on VMware or KVM.

If installing on a virtual server using VMware, use VMware Paravirtual SCSI controllers.

Each EMS requires the following resources:

- CPU:
  - Intel-based, 4th generation and higher
  - 4 virtual or physical cores minimum
- RAM: 8GB minimum
- SSD: 64GB minimum

2.4.2 Controller Hardware Requirements

Each ECFS controller requires:

- CPU:
  - Intel-based, 4th generation and higher, dual-socket
  - 6 cores minimum per CPU
  - Up to 16 cores per CPU (ECFS uses up to 20 cores, the kernel uses spare cores)
  - Hyperthreading disabled.

- RAM: 96GB to 256GB RAM (DDR4 or higher).
- SSD: Boot device with minimum 128GB, 3.2 DWPD, or 256GB with 1.6 DWPD.

2.4.3 Replication Agent Hardware Requirements (optional)

The replication agent can be installed as a physical server or a virtual server on VMware or KVM.

If installing on a virtual server using VMware, use VMware Paravirtual SCSI controllers.

Each replication agent requires:

- CPU:
  - Intel-based, 4th generation and higher
  - 4 virtual or physical cores minimum.
  - Supports up to 4 concurrent bidirectional replications. Number of CPUs can be increased to support more concurrent replications.
  - Hyperthreading: Supported
- RAM: 16GB RAM minimum (should be increased if CPU count increases). Recommended: 4GB per CPU core
- SSD: Boot device with minimum 38GB.

3. Preparing the Environment for Installation

3.1 Servers

3.1.1 High Performance Server Optimizations

The following procedures are not mandatory for the deployment of ECFS, but are highly recommended for optimizing its performance.

3.1.1.1 Configuring the Server BIOS

1. Disable HyperThreading (usually under a sub-menu for features such as CPU, Processor, Performance, Advanced BIOS, CPU Feature, Tweaker).
2. Set CPU power mode to **Full Performance**.
3. Enable Pass-through mode for the RAID controller. This is required to be able to assign specific drivers to ECFS, and to let ECFS control the drivers properly.

3.1.2 Servers

- Make sure you have access to two VMs or physical servers (for primary and secondary EMSs) that comply with the requirements described in Section 2.4 - Host Resources.
- The VMs/physical servers for the EMS, controllers and replication agents must have Centos Minimal 7.4 (1708) pre- installed with partitioning configured as per Elastifile requirements as described in Appendix A - Configuring CentOS Partitions for ECFS.

3.1.3 NICs

Make sure each server includes two 10GbE ports for the data network, and one 10GbE port for the client network.

3.1.3.1 Subnets/VLAN Requirements

The following independent subnets/VLAN are required:

- MGMT for external network interface
- Client network interface for clients' traffic
- DATA1 for Elastifile interconnect network
- DATA2 for Elastifile interconnect network

3.1.3.2 Network and IP Requirements

The network and IP requirements are as follows:

- EMS (for each EMS server installed)
  - 1 IP for EMS external network interface (static or DHCP; DNS entry recommended for external IP)
  - 2 IPs for ECFS interconnect networks (1 per NIC, 2 NICs required)

- Controller - each controller requires:
  - 2 IPs for ECFS interconnect networks (1 per NIC, 2 NICs required)
  - Client network for client traffic as follows:
    - For Layer 2 networks, define one client VIP.
    - For Layer 3 networks, define 20 client VIPs.
- Replication Service Agent - each agent requires:
  - 1 IP for external network interface
  - 1 IP for client network interface

3.2 Network

3.2.1 Configuring DNS

No DNS requirements or configurations are mandatory. However, to simplify the use of the web-based management system, Elastifile recommends that you assign a DNS name for the EMS Virtual IP (VIP).

3.2.2 Management Network IP Type

For the management network, you can either assign a static IP or use a DHCP service.

1. Request (from your IT department) IP addresses for the following:
   - If you will use a Management Network with a static IP:
     - Primary EMS IP
     - Secondary EMS IP
     - EMS virtual IP (VIP)
     - EMS physical network mask
     - Management network gateway
   - If you will use a Management Network with a DHCP service:
     - EMS virtual IP address network mask
     - EMS virtual IP (VIP)

3.2.3 Configuring Physical Switches

Perform the following steps on all ECFS designated data ports:

1. Make sure the port is synced to 10GbE speed - mandatory.
2. Configure MTU 9000 - mandatory.
3. If your network uses VLANs, make sure the designated VLANs are properly tagged through all layers.

3.2.4 Configuring the Network for Replication Service (Optional)

To enable the optional Replication Service, configure the network as follows:

External

- Site A EMS to Site B EMS: HTTP/80 bi-directional
- Site A Replication Service to Site B Replication Service: SSH/22 Bi-directional

Internal

- EMS to Replication Service: HTTP/80 Uni-directional
- EMS to Replication Service: epa/10015 Uni-directional

4. Installing the EMS

The EMS is a VM that controls the controllers in the ECFS system and provides a management console for the administrator. For system redundancy, you can also install a secondary EMS.

This section describes how to install and configure the primary EMS.

After you have deployed the ECFS system, you can install the secondary EMS (see Section 7 - Installing the Secondary EMS).

Before you start installing the EMS, download the Installation Package from Elastifile Support - Software Downloads.

4.1 Installing the Primary EMS

- Make sure the VM or physical server for the primary EMS meet the requirements described in Section 3.1.2 - Servers.
- Run the ECFS installer file (as described below) on a Linux machine with at least 10GB of free disk space. The Linux machine is also used to install the controllers, secondary EMS and replication agents.
- The file names and IP addresses in the following scripts are just examples.

To extract the installer run file on the Linux machine used for installation:

1. Add execute permissions to the run file:

```
$ chmod +x elastifile-installer-2.7.0.12-53043.955ac12f07aa-195.run
```

2. Extract the run file:

```
$ ./elastifile-installer-2.7.0.12-53043.955ac12f07aa-195.run
Verifying archive integrity... All good.
Uncompressing Elastifile DSM Installer 100%
Please run ./bin/elfs-install from target directory
```

To install the primary EMS:

The VMs/physical servers for the EMS, controllers and replication agents must have Centos Minimal 7.4 (1708) pre- installed with partitioning configured as per Elastifile requirements as described in Appendix A - Configuring CentOS Partitions for ECFS.

1. On the server or VM that will serve as the EMS, obtain machine's IP as follows:

   ip a

2. On the Linux machine, in the directory where the files were extracted, run:

```
```

```
./bin/elfs-install deploy ems --remote --host=<EMS IP> --user=root --password=<password> --ems-
password=<password> --vip=<VIP IP> --ems-host=<EMS IP> --netmask=255.255.0.0
```

The following script is an example of an installation:

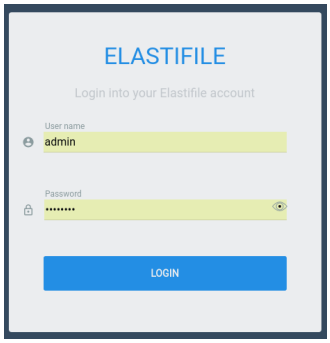
```
$ ./bin/elfs-install deploy ems --remote --host=10.11.133.6 --user=root --password=123456 --ems-
password=changeme --vip=10.11.209.29 --ems-host=10.11.133.6 --netmask=255.255.0.0

Upload release package to server ......................
Unpack release package ...
Configure installer repository
Install core system packages
.....................................................................................................
.....................................................
Install EMS system packages
.....................................................................
Configure core system .
Configure EMS ..........
Starting service Elastifile Platform Agent .
Reconfigure networking .
Register EMS ........
Reboot system ..............................
Waiting for system to start ...
updating system object ......
Configure EMS VIP ..
Shutdown all network connection. ...Disconnecting from 10.11.133.6... done.
...
Done.
Elastifile EMS deployment completed, open https://10.11.133.6 in your browser to access
Elastifile Storage management UI
```

You can now login to the ECFS Management Console as described in Section 5 - Logging in to ECFS.

5. Logging in to ECFS

To log in to the ECFS system:

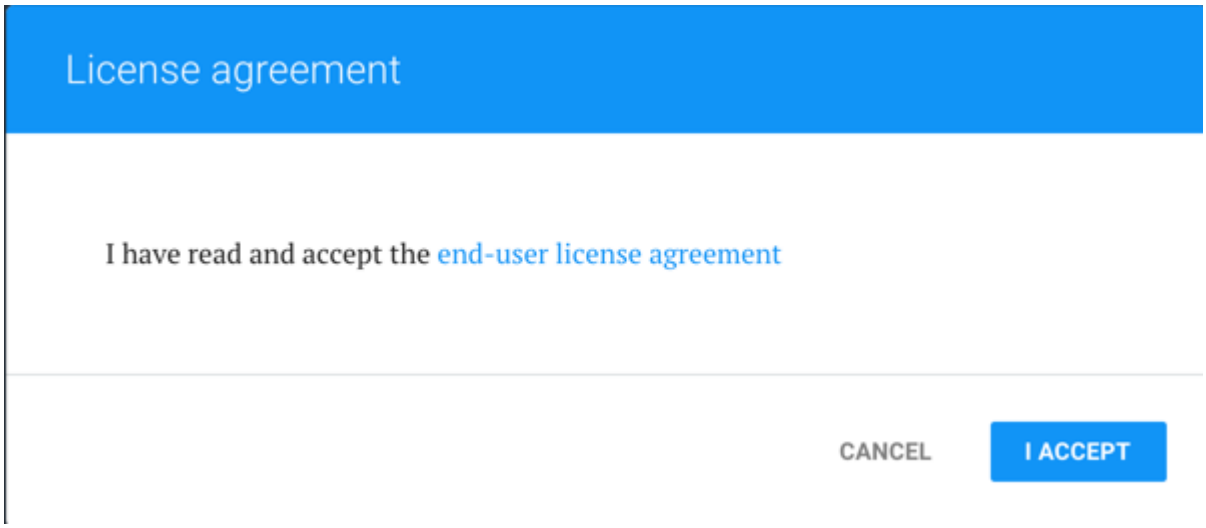
1. In your browser, enter the ECFS Management IP address (used during installation of the primary EMS) and press Enter. The login window appears:



2. Enter the following default values:
   - **Username**: admin
   - **Password**: changeme
3. Click **LOGIN**.

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

4. Accept the license agreement.



You can now deploy the ECFS system entities (nodes and secondary EMS).

6. Deploying ECFS

This section describes deploying the ECFS system in a Dedicated Storage Mode (DSM) environment.

6.1 Setting Up the ECFS System

After logging in to ECFS for the first time, a wizard leads you through setting up an ECFS system:

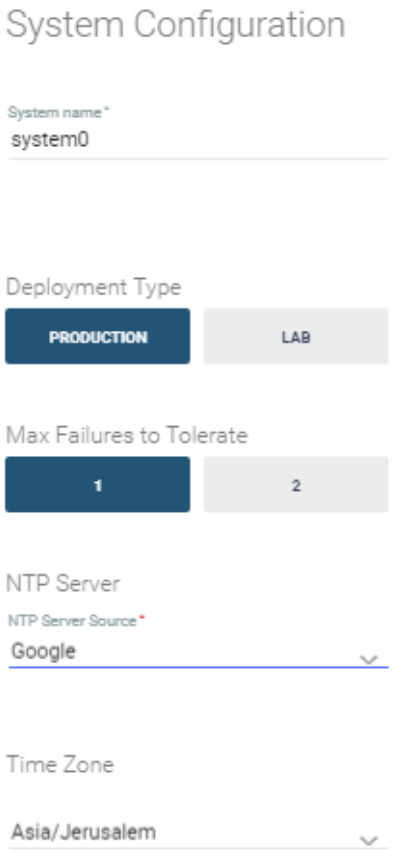
The wizard consists of the following main steps:

1. Configuring general system parameters - see Section 6.1.1 - General System Configuration.
2. Configuring notifications - see Section 6.1.2 - Notifications.
3. Configuring the interconnect network - see Section 6.1.3 - Interconnect Network Configuration.
4. Configuring the client network - see Section 6.1.4 - Configuring the Client Network.

The parameters you enter in the above steps cannot be changed after you configure the system in Section 6.1.4 - Configuring the Client Network.

6.1.1 General System Configuration

1. In this step of the wizard, define the system configuration, as explained in the following figure and table:



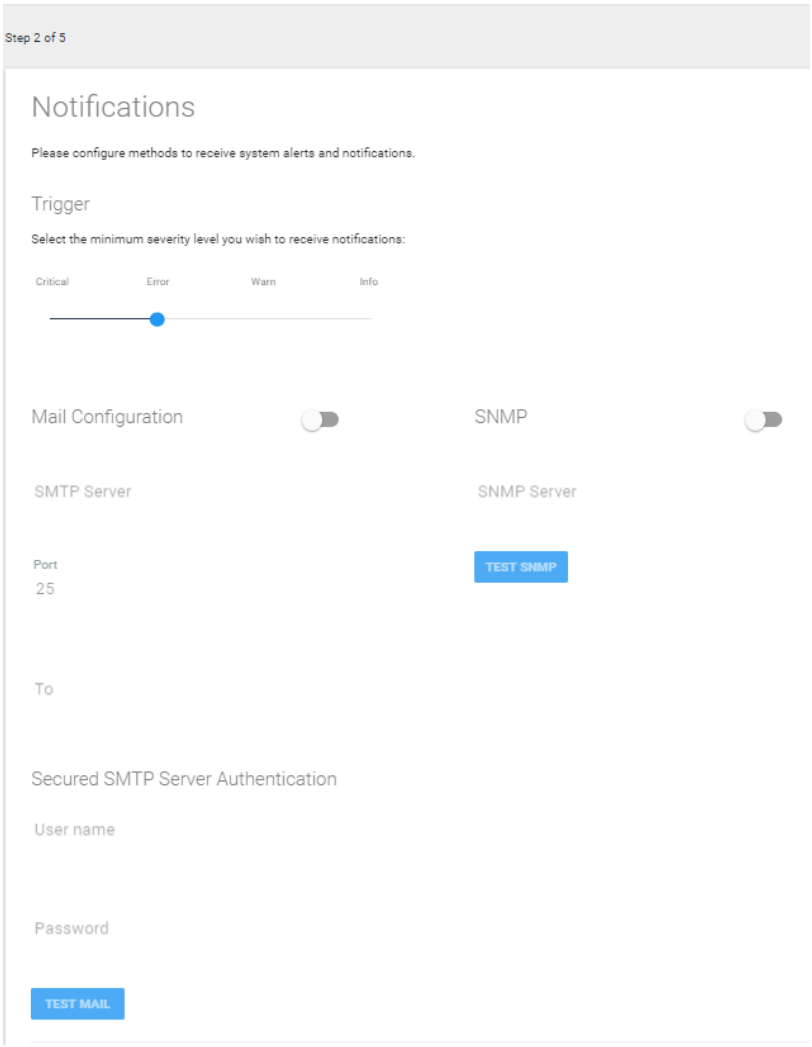
Details	Description
System name	Enter a name (maximum 40 characters) that identifies the system.
Deployment Type	Select **PRODUCTION**. This option provides high availability and performance and enforces minimum requirements as specified in Section 2 - Hardware Requirements and Section 3 - Preparing the Environment for Installation.
Max Failures to Tolerate	Select the number of servers that can fail without putting the ECFS system in degraded mode. • **1** - you must have at least three servers in the system to select this option. The system replication level will be set to 2. • **2** - you must have at least five servers in the system to select this option. The system replication level will be set to 3.
NTP Server	Select the time source to synchronize time settings in all system servers. Select one of the following options: • **Manual** - provide the IP address or DNS name of NTP server(s). Multiple NTP servers should be comma-separated. • **Google** - use Google's NTP servers. • **No NTP (Lab Only)** - system will acquire the current time from your browser.
Time Zone	Select the time zone that will be used by the ECFS system.

2. Click **NEXT**. The wizard saves the System Configuration parameters that you entered.

The Next button remains disabled until all mandatory fields have been completed.

6.1.2 Notifications

1. In this step of the wizard, define how to receive system alerts and notifications through email and/or SNMP, as explained in the following figure and table:



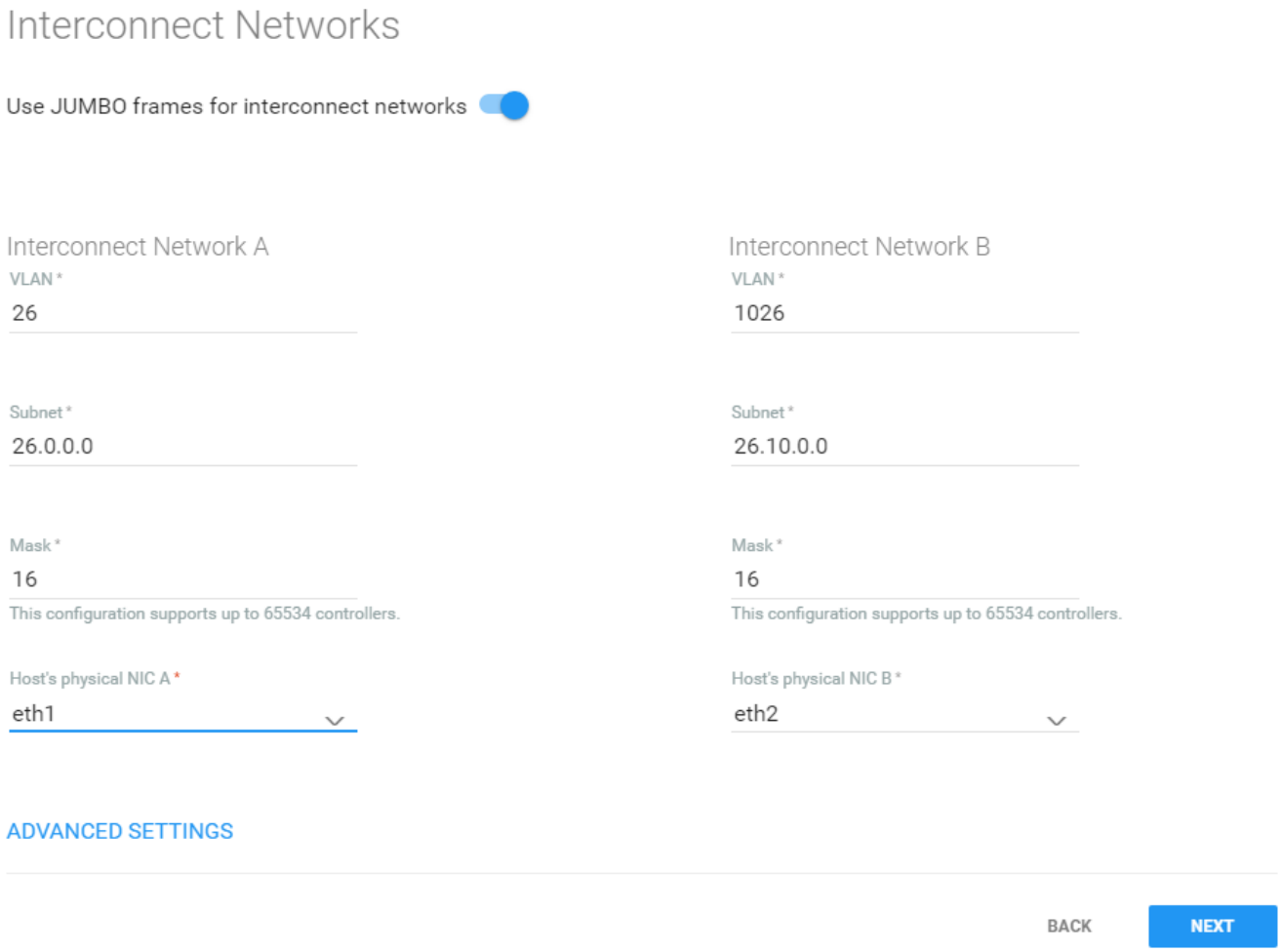
Details	Description
Trigger	Move the **Trigger** slider to your required minimum notification severity level: **Critical**, **Error**, **Warn** or **Info**.
Mail Configuration	To receive notifications via email: 1. Move the **Mail Configuration** slider to the right. 2. In **SMTP Server**, enter your SMTP server name. 3. In **Port**, enter your port number.  For Gmail, valid ports are 587 or 25. If these are unsuccessful, try port 465. 4. In **To**, enter the required email address. 5. In **Secured SMTP Server Authentication**, enter your user name. 6. In **Secured SMTP Server Authentication**, enter your password. 7. Click **TEST MAIL**, and verify that a test email was received by the user-defined email.
SNMP Configuration	To receive notifications via an SNMP server: 1. Move the **SNMP** slider to the right. 2. In **SNMP Server**, enter your SNMP server name. 3. Click **TEST** and verify that a test message was received as per the SNMP server configuration.

2. Click **NEXT**. The wizard saves the Notification parameters that you entered.

 The Next button remains disabled until all mandatory fields have been completed.

6.1.3 Interconnect Network Configuration

1. In this step of the wizard, define the interconnect networks to be used by ECFS, as explained in the following figure and table:



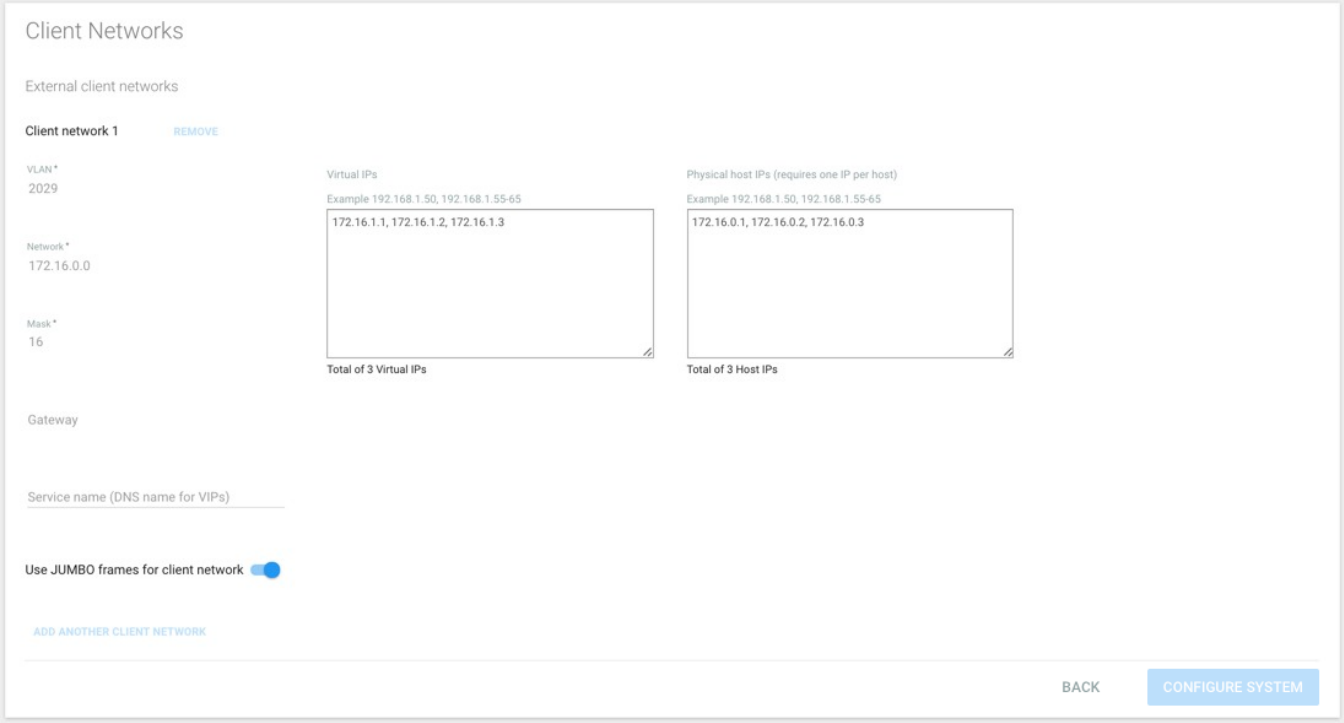
Details	Description
Use JUMBO frames for interconnect networks	On (default) - set to on if available data networks (A,B) support MTU 9000 (jumbo) frame.
ADVANCED SETTINGS	If you are requested to do so by Elastifile, click to open the Auxiliary Network configuration and configure as instructed by Elastifile.

Click **NEXT**. The wizard saves your interconnect network settings.

The Next button remains disabled until all mandatory fields have been completed.

6.1.4 Configuring the Client Network

In this step of the wizard, configure the client networks to be used by ECFS.



1. Enter the **VLAN**, **Network** (IP), and **Mask**.
2. In **Service name**, enter the client network DNS name.
3. Move the **Use JUMBO frames for client network** slider to the right if the client networks support the MTU 9000 (jumbo) frame.
4. **Virtual IP** is a list of Virtual IPs (VIPs) for effective load balancing. The number of VIPS required is determined as follows:
   - For Layer 2 networks, define one client VIP.
   - For Layer 3 networks, define 20 client VIPs.
5. In **Physical host IPs**, enter an IP for each physical node of the ECFS network.

Both VIPs and Physical host IPs must be in the range defined for the client network above.

6. Click **Configure System**. The wizard saves the network parameters that you entered.

6.2 Installing a Controller on Servers

After setting up ECFS through the wizard, you can install ECFS controllers. The ECFS must contain at least three controllers.

- Run the ECFS installer file on the same Linux machine you used for installing the primary EMS.
- The file names and IP addresses in the following scripts are just examples.

To install a controller on a server:

The VMs/physical servers for the EMS, controllers and replication agents must have Centos Minimal 7.4 (1708) pre- installed with partitioning configured as per Elastifile requirements as described in Appendix A - Configuring CentOS Partitions for ECFS.

1. On the server or VM that will serve as the controller, obtain machine's IP as follows:

   ip a

2. On the Linux machine, in the directory where the files were extracted, run:

```
./bin/elfs-install deploy enode --remote --host=<EMS IP> --user=root --password=<password> --ems-password=<password> --ems-host=<EMS host IP>
```

If the controller IPs are consecutive (such as 10.11.200.126, 10.11.200.127, 10.11.200.128), you can provide them as a range (such as 10.11.200.126-128).
Otherwise, run the installation one by one for each controller.

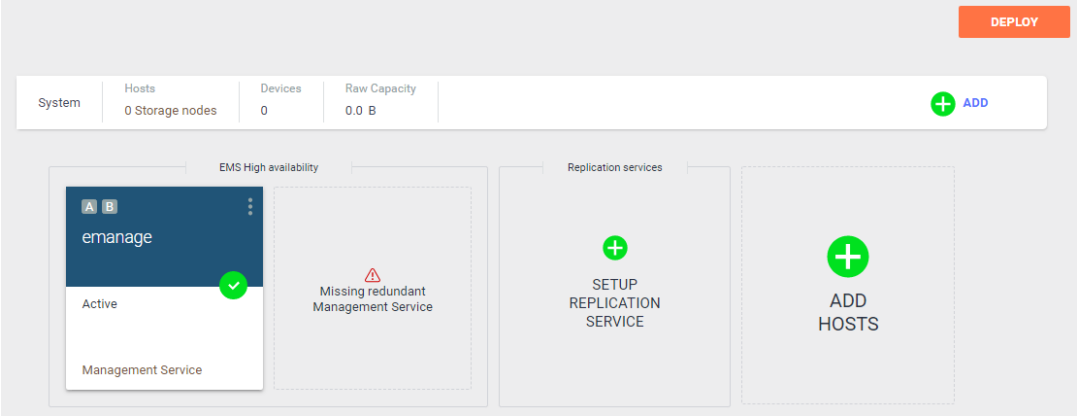
The following script is an example of an installation of three controllers with consecutive IPs:

```
# ./bin/elfs-install deploy enode --remote --host=10.11.221.2-4 --user=root --password=123456 --ems-password=changeme --ems-host=10.11.133.6

{'timestamp': 1529474955, 'message': 'Host 10.11.221.2: Configure installer repository', 'level': 'I'}
{'timestamp': 1529474955, 'message': 'Host 10.11.221.2: Install core system packages', 'level': 'I'}
{'timestamp': 1529475105, 'message': 'Host 10.11.221.2: Install system packages', 'level': 'I'}
{'timestamp': 1529475140, 'message': 'Host 10.11.221.2: Configure core system', 'level': 'I'}
{'timestamp': 1529475141, 'message': 'Host 10.11.221.2: Configure host', 'level': 'I'}
{'timestamp': 1529475141, 'message': 'Host 10.11.221.2: Starting service Elastifile Platform Agent', 'level': 'I'}
{'timestamp': 1529475142, 'message': 'Host 10.11.221.2: Register host with EMS', 'level': 'I'}
{'timestamp': 1529475143, 'message': 'Shutdown all network connection.', 'level': 'I'}
Disconnecting from 10.11.221.2... done.
{'timestamp': 1529474955, 'message': 'Host 10.11.221.3: Configure installer repository', 'level': 'I'}
{'timestamp': 1529474955, 'message': 'Host 10.11.221.3: Install core system packages', 'level': 'I'}
{'timestamp': 1529475105, 'message': 'Host 10.11.221.3: Install system packages', 'level': 'I'}
{'timestamp': 1529475140, 'message': 'Host 10.11.221.3: Configure core system', 'level': 'I'}
{'timestamp': 1529475141, 'message': 'Host 10.11.221.3: Configure host', 'level': 'I'}
{'timestamp': 1529475141, 'message': 'Host 10.11.221.3: Starting service Elastifile Platform Agent', 'level': 'I'}
{'timestamp': 1529475142, 'message': 'Host 10.11.221.3: Register host with EMS', 'level': 'I'}
{'timestamp': 1529475143, 'message': 'Shutdown all network connection.', 'level': 'I'}
Disconnecting from 10.11.221.3... done.
{'timestamp': 1529474955, 'message': 'Host 10.11.221.4: Configure installer repository', 'level': 'I'}
{'timestamp': 1529474955, 'message': 'Host 10.11.221.4: Install core system packages', 'level': 'I'}
{'timestamp': 1529475105, 'message': 'Host 10.11.221.4: Install system packages', 'level': 'I'}
{'timestamp': 1529475140, 'message': 'Host 10.11.221.4: Configure core system', 'level': 'I'}
{'timestamp': 1529475141, 'message': 'Host 10.11.221.4: Configure host', 'level': 'I'}
{'timestamp': 1529475141, 'message': 'Host 10.11.221.4: Starting service Elastifile Platform Agent', 'level': 'I'}
{'timestamp': 1529475142, 'message': 'Host 10.11.221.4: Register host with EMS', 'level': 'I'}
{'timestamp': 1529475143, 'message': 'Shutdown all network connection.', 'level': 'I'}
Disconnecting from 10.11.221.4... done.
```

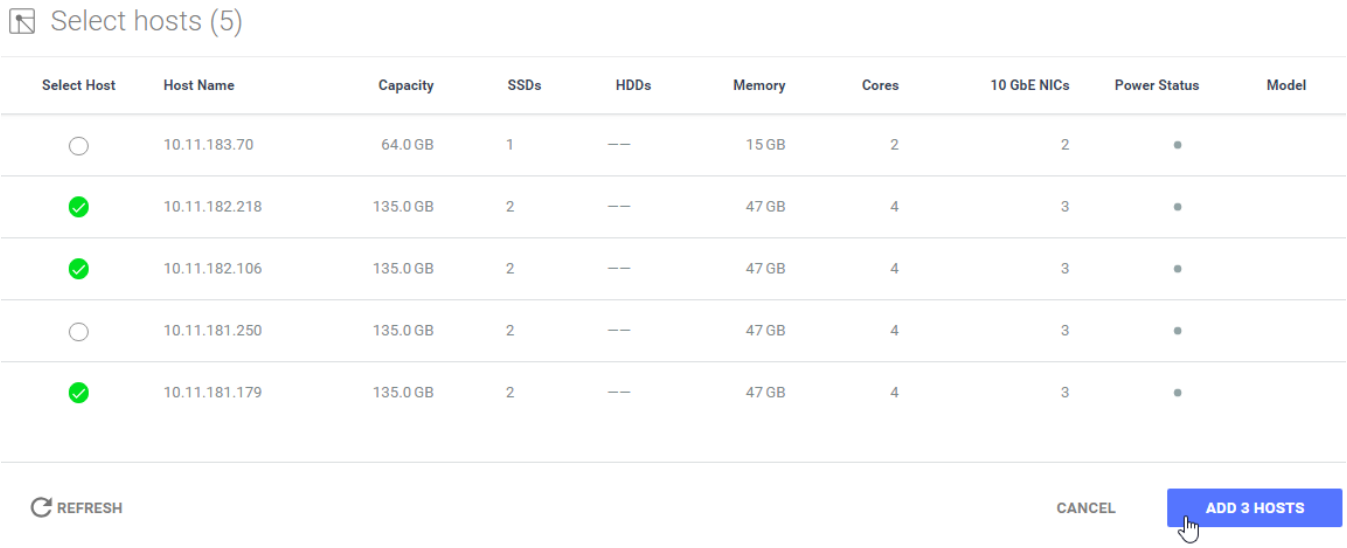
6.3 Adding Hosts

To add hosts that will be used by the ECFS system:

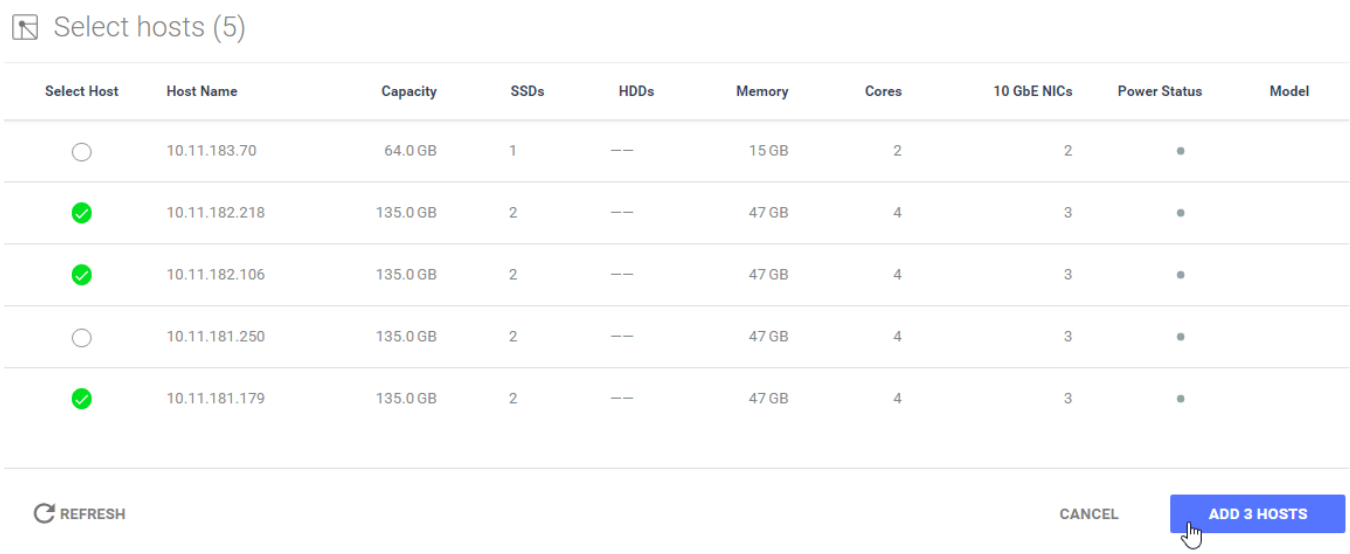
1. Click **ADD HOSTS**.



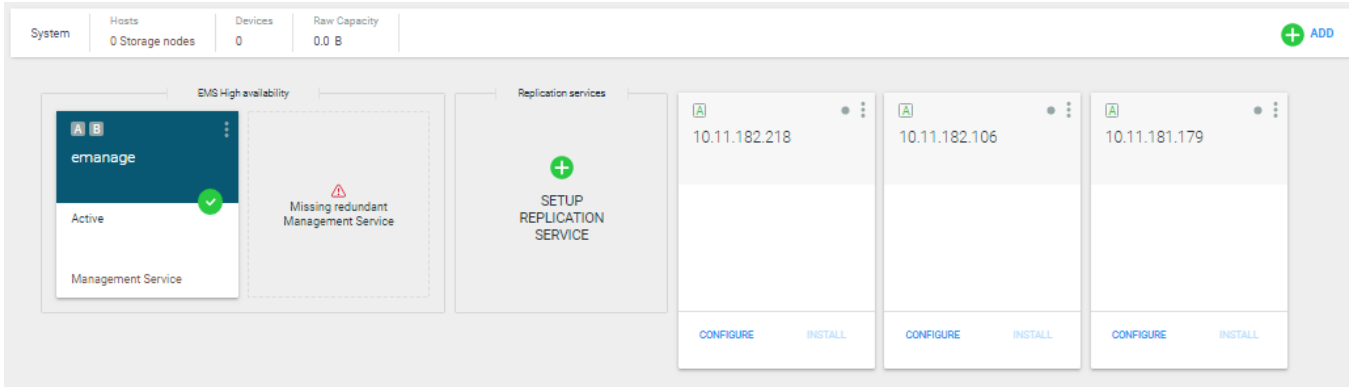
2. Select the hosts to add:



3. When you have selected all the hosts you want, click **ADD HOSTS**.

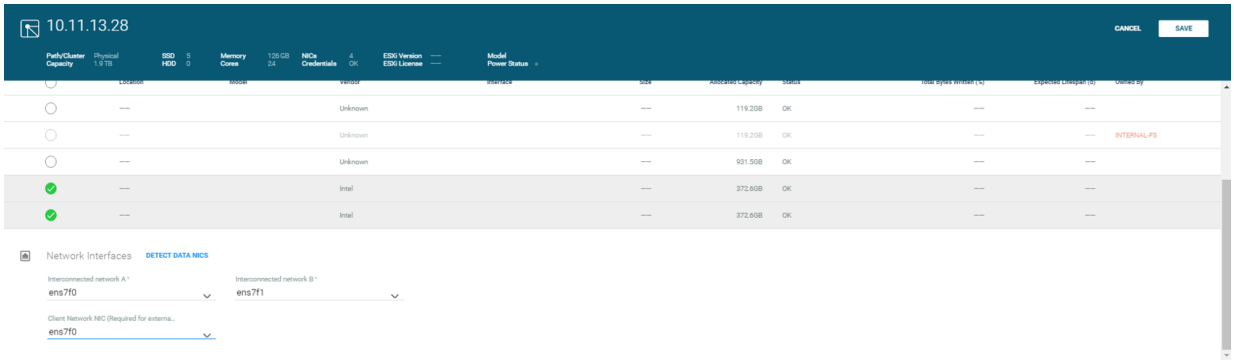


4. The System View window appears displaying the hosts you selected.



5. For each host, click **CONFIGURE**.

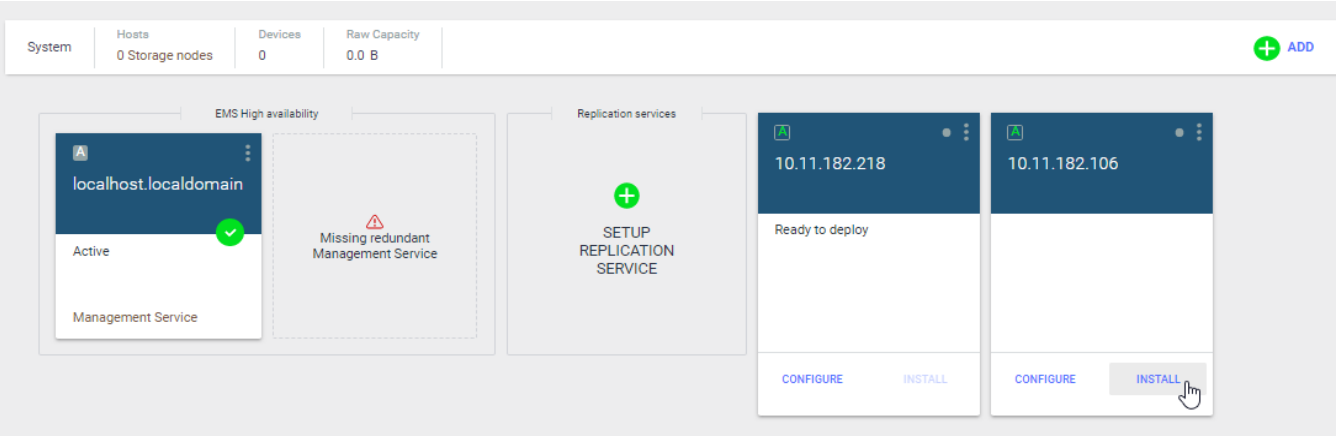
6. Configure the host as described below:



elastifile

Details	Description
Storage Devices	Select the storage devices that will be part of the ECFS system (select the first check box for all storage devices). You can only select **local** devices that are not owned by other services, as indicated in the **Owned By** column.
Network Interfaces	1. For the first host you are configuring , click **Detect Data NICS**. The ECFS system automatically selects the NICs connected to the data networks . Select a different NIC if required.

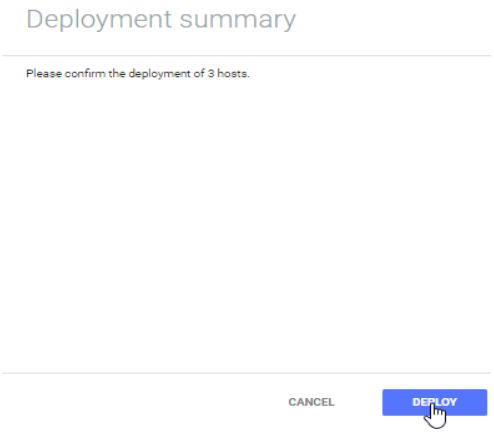
2. Click **SAVE**. The **INSTALL** button becomes active.



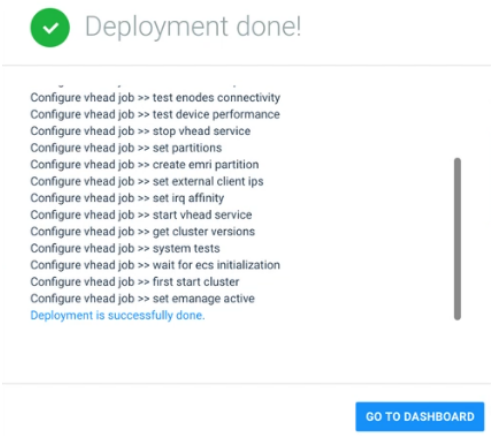
3. Click **INSTALL**. After a few seconds, a progress bar appears on the hosts.

You can configure and install several hosts in parallel.

4. The Deployment Summary window appears to confirm deployment. Click **DEPLOY**.



5. The hosts are deployed, and deployment progress is displayed in the Deployment Summary window. When deployment is successfully done, click **GO TO DASHBOARD**.



6.4 Installing a Replication Agent (Optional)

- Make sure the VM or physical server for the replication agent meet the requirements described in Section 3.1.2 - Servers.
- Run the ECFS installer file on the same Linux machine you used for installing the primary EMS and controllers.
- The file names and IP addresses in the following scripts are just examples.

To install a replication agent:

The VMs/physical servers for the EMS, controllers and replication agents must have Centos Minimal 7.4 (1708) pre- installed with partitioning configured as per Elastifile requirements as described in Appendix A - Configuring CentOS Partitions for ECFS.

1. On the server or VM that will serve as the controller, obtain machine's IP as follows:

   ip a

2. On the Linux machine, in the directory where the files were extracted, run:

```
./bin/elfs-install deploy ragent --remote --host=<EMS IP> --user=root --password=<password> --
ems-password=<password> --ems-host=<EMS host IP>
```

The following script is an example of an installation:

```
$ ./bin/elfs-install deploy ragent --remote --host=10.11.148.255 --user=root --password=123456 --
ems-password=changeme --ems-host=10.11.133.6

Host 10.11.148.255: Configure installer repository .
Host 10.11.148.255: Install core system packages
.....................................................................................
.....................................................
Host 10.11.148.255: Install system packages ..............................
Host 10.11.148.255: Configure core system .
Host 10.11.148.255: Configure host .
```

```
Host 10.11.148.255: Starting service Elastifile Platform Agent
Host 10.11.148.255: Register host with EMS .
Shutdown all network connection. ...Disconnecting from 10.11.148.255... done.
...
Done.
Elastifile Replication Agent deployment completed.
```

7. Installing the Secondary EMS

- Make sure the VM or physical server for the secondary EMS meet the requirements described in Section 3.1.2 - Servers.
- Run the ECFS installer file on the same Linux machine you used for installing the primary EMS and controllers.
- The file names and IP addresses in the following scripts are just examples.

To install the secondary EMS:

The VMs/physical servers for the EMS, controllers and replication agents must have Centos Minimal 7.4 (1708) pre- installed with partitioning configured as per Elastifile requirements as described in Appendix A - Configuring CentOS Partitions for ECFS.

1. On the server or VM that will serve as the secondary EMS, obtain machine's IP as follows:

   ip a

2. On the Linux machine, in the directory where the files were extracted, run:

```
./bin/elfs-install deploy ems --secondary --remote --host=<EMS IP> --user=root --
password=<password> --ems-password=<password> --ems-host=<EMS host IP> --vip=<VIP IP> --
netmask=255.255.0.0 --data-nics=<Data Networks>
```

The following script is an example of an installation:

```
$ ./bin/elfs-install deploy ems --secondary --remote --host=10.11.199.192 --user=root --
password=123456 --ems-password=changeme --ems-host=10.11.133.6 --vip=10.11.209.29 --
netmask=255.255.0.0 --data-nics=ens224,ens256
Configure installer repository .
Install core system packages .
Install EMS system packages .
Configure core system .
Configure EMS ............
Starting service Elastifile Platform Agent .....
Reconfigure networking .
Register EMS ........
Reboot system ..............................
Waiting for system to start ...
updating system object .......
Configure EMS VIP .
Configure EMS high availability ...
Register remote EMS on local ems ..................
Shutdown all network connection. ...Disconnecting from 10.11.199.192... done.
...
Done.
Elastifile secondary EMS deployment completed.
```

8. Loading Your SSL Certificate (Optional)

You can generate a certificate signing request (CSR) on the primary EMS for self-signing or signing by a Certificate Authority (CA). You then upload the CSR and the signed SSL certificate to the active EMS.

The optional secondary EMS should be installed before loading your SSL certificate.

To create a CSR:

1. Open an SSH connection to the active EMS.
2. After the connection has been established, run the following CLI command:

```
elfs-cli certificate create_csr
```

3. Copy the CLI command output to a text file and save the file.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIE1zCCAr8CAQAwZDEcMBoGA1UEChQTZWxhc3RpZmlsZV83ZVQxS3VhNTEVMBMG
A1UEAxMMMTAuMTEuMTgxLjUwMRYwFAYDVQQDEw0xMC4xMS4yMDkuMjI5MRUwEwYD
VQQDEwwxMC4xMS4xNzguNDcwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoIC
.
.
.
.
Y0lEV2vfHSLJwZK3xQer9VfO5J3t28JjTLmV5X/9v9s/cCvkD0jtn2cV9/lsBs/X
BriyeS6q9mT4jmbT2xesbPvDqXLz/Lu1eq08H93UZTA0OiwwWEaRaVXeBXk0aNcI
sTScn8VO93fTCJZbwsk5zB88b17SOYGNe7jMQa/+FqLp7LSjLiBaZsV5IA==
-----END CERTIFICATE REQUEST-----
```

4. Using the above CSR file, generate a certificate by self-signing or signing by a CA.
5. Copy the certificate to the active EMS (click **SYSTEM VIEW** to identify the active EMS).
6. Upload the CSR file and the certificate by running the following CLI command:

```
# elfs-cli certificate upload --csr <path-to-file/csr_filename> --cert <path-to-file\cert_
filename>
```

7. Restart the active EMS by running the following CLI command:

```
# systemctl restart emanage
```

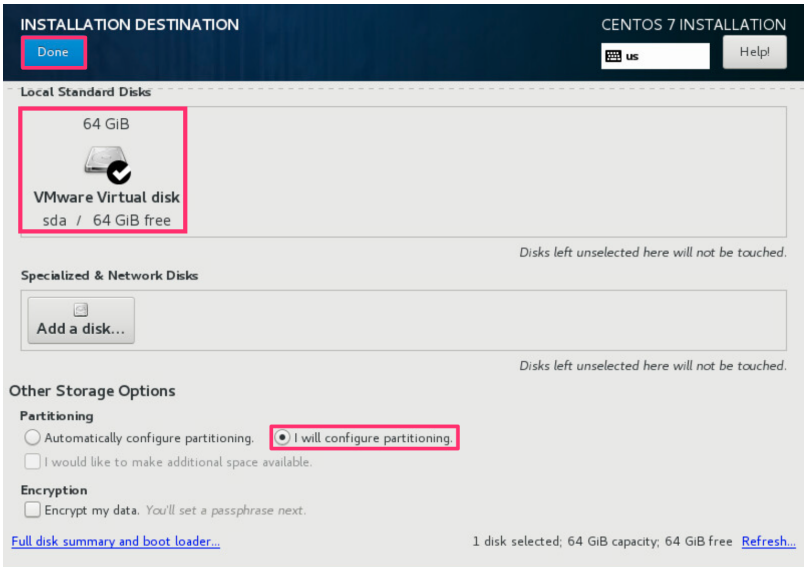
If a standby EMS is installed, the certificate will be automatically deployed to it.

Appendix A. Configuring CentOS Partitions for ECFS

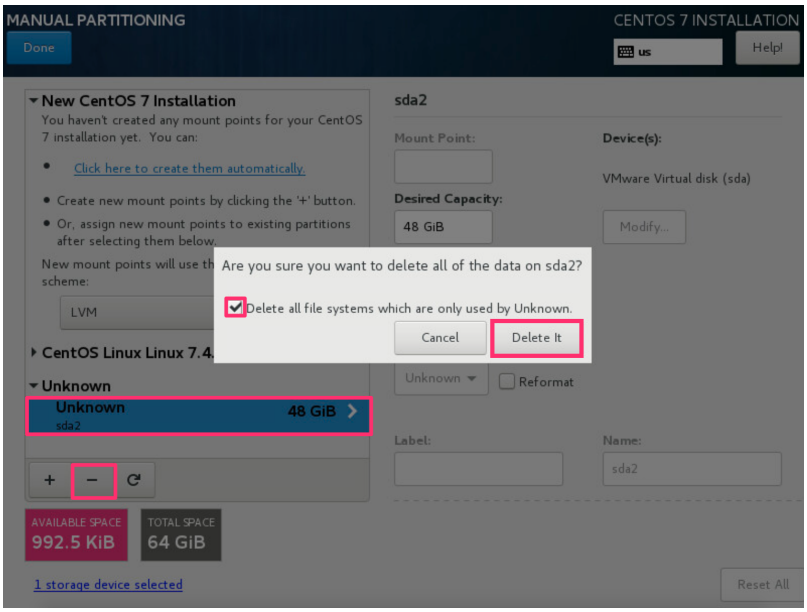
As part of the CentOS installation forECFS servers (EMS, controllers and Replication Agents), you must manually configure a partition for use by ECFS, including limiting the OS partition size for other ECFS software requirements.

1. In the CentOS wizard installation, click **INSTALLATION DESTINATION**.

2. Select the device on which to install the OS.
3. Under **Other Storage Options**, under **Partitioning**, select **I will configure partitioning**.
4. Click **Done**.

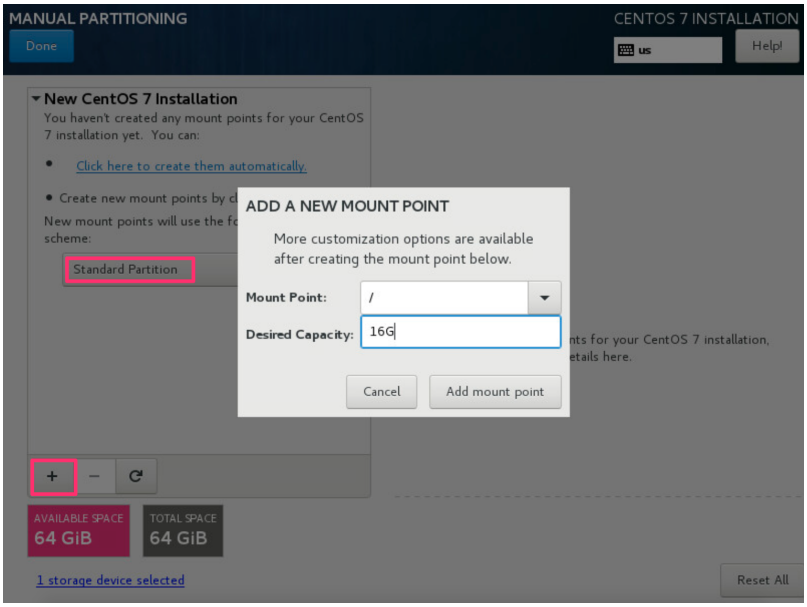


5. In the **MANUAL PARTITIONING** window, delete any predefined partitions on the device as follows:
   a. Select the partition to delete.
   b. Click **-**.
   c. In the confirmation window, select the check box.
   d. Click **Delete it**.
   e. Repeat this procedure for any other partitions.



elastifile

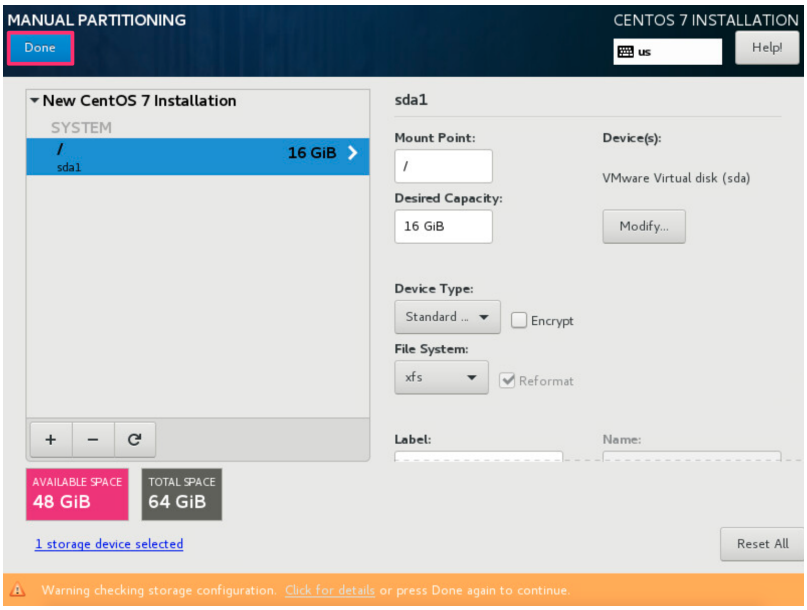
6. Under New CentOS 7 installation, select **Standard Partition**.
7. In Mount Point, select **/**.
8. In **Desired Capacity**, type the size according to the server function as follows:
   - EMS: 16G
   - Controllers and Replication Agents: 10G



The remaining disk space will be used by ECFS.

9. Click **Add mount point**.

10. Review the manual partition settings and click **Done**.
11. Ignore the no swap configured warning message and click **Done** again.



elastifile

12. Click **Accept changes**. The installation will proceed till completion.