elastifile
Cross-Cloud Data Fabric

Elastifile 2.5.1
Dedicated Storage Mode (DSM)

Installation Guide

March 2018

Document Revision: 0.2

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 Elastifile 2.5.1 systems based on Dedicated Storage Mode (DSM).

For deploying the Elastifile system in a HyperConverged Infrastructure (HCI) for VMware environment, see the *Elastifile HyperConverged Infrastructure (HCI) for VMware Installation Guide*.

For deploying the Elastifile system in a HyperConverged Infrastructure (HCI) for KVM environment, see the *Elastifile HyperConverged Infrastructure (HCI) for KVM Installation Guide*.

1.2 Installation Overview

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

- Elastifile Management System (EMS) - the Elastifile management machine that controls the Elastifile system.
- Controller - a server acting as an Elastifile controller node.
- Client - a machine using Elastifile storage services.

The EMS and controller entities should not be used as clients or 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 Elastifile 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 Elastifile).
   - (optional) deploying a secondary EMS on an additional VM or physical server (see Section 7 - Installing the Secondary EMS (Optional)).

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

Elastifile'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. Elastifile uses the VLAN to isolate its internal IP scheme.

The network switch should meet the following port configuration requirements:

- 10GbE full duplex - mandatory
- MTU=9000 - highly recommended
- Dedicated VLAN (trunk mode) - highly recommended

- Elastifile recommends using two 10GbE switches. The minimum configuration is one 10GBe switch (one switch for each Elastifile network).
- For tested switches, see Appendix A.1 - Tested Switches.

2.2.2 NICs

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

- 10GbE for the data network
- 1GbE for the client network

- For tested NICs, see Appendix A.2 - Tested NICs.

2.3 Storage

- Priority-1 Devices:
  - NVMe SSD
  - PCI SSD
- Priority-2 Devices:
  - Single device in RAID 0 group with disabled read/write caching

For tested SSDs, see Appendix A.3 - Tested SSDs.

2.4 Host Resources

2.4.1 EMS Hardware Requirements

Each EMS requires the following resources:

- CPU: Minimum 4 virtual or physical cores.
- RAM: Minimum 8GB
- SSD: Minimum 64GB.

2.4.2 Controller Hardware Requirements

Each Elastifile controller requires:

- CPU: Dual socket, 6 physical cores.
- RAM: Minimum 128GB RAM (DDR4 or higher).
- SSD: Boot device with minimum 100GB.

2.4.3 Replication Service Machine Hardware Requirements (optional)

Each replication service machine requires:

- CPU: Dual socket, 4 physical cores.
- RAM: Minimum 16GB RAM.
- SSD: Boot device with minimum 32GB.

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 Elastifile, 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 Elastifile, and to let Elastifile control the drivers properly.

3.1.2 Servers

3.1.2.1 EMS Hosts

1. Make sure you have access to two VMs or servers that comply with the requirements described in Section 2 - Hardware Requirements

3.1.2.2 Controller Servers

- Each controller server must comply with the requirements described in in Section 2 - Hardware Requirements
- Each server should be able to boot from a 64GB bootable SSD.

3.1.3 Storage Devices

- EMS image store - 64GB on one of the available datastores accessible within the host running EMS VM.
- Elastifile data devices - between one to six dedicated local SSD or flash memory devices. It is highly recommended that the SSD devices will be accessed directly and not through a RAID controller (see Section 2.3 - Storage).

3.1.4 NICs

Make sure each server includes at least two 10GbE ports for the data network (for LAB deployments, only one NIC port is required), and one 1GbE port for the client network.

The network and IP requirements are as follows:

- Four independent subnets/VLAN are required:
  - MGMT for EMS public interface
  - Client for client traffic
  - DATA1 for Elastifile controller interconnect
  - DATA2 for Elastifile controller interconnect
- EMS (for each EMS server installed)
  - 1 IP for EMS public interface (static or DHCP)
    - DNS entry recommended for public IP
  - 2 IPs for data interconnect (1 per NIC, 2 NICs required)
- Controller - each controller requires:
  - 2 IPs for data interconnect (1 per NIC, 2 NICs required)
  - Client network for client connections:
    - For Layer 2 networks, define one client VIP.
    - For Layer 3 networks, define 20 client VIPs.

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 Elastifile designated data ports:

1. Make sure the port is synced to 10GbE speed - mandatory.
2. Configure MTU 9000 - highly recommended.
3. Make sure the designated VLAN is tagged and enabled for the port (trunk mode) - highly recommended.

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 Elastifile 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 Elastifile system, you can install the optional secondary EMS (see Section 7 - Installing the Secondary EMS (Optional)).

Before you start installing the EMS, request the EMS LiveCD from Elastifile.

4.1 Installing the Primary EMS

- The EMS script must be run from a Linux machine with at least 10GB of free space.
- The file names and IP addresses in the following scripts are just examples.
- The term "eManage" in the installation script refers to the EMS machine.

1. On the server or VM that will serve as the EMS, boot into the EMS LiveCD using the following credentials:
   - User: root
   - Password: 123456
2. Obtain or assign the machine's IP as follows:
   - If you will be using DHCP, run:

     ip a

     and note the machine's IP.
   - If you will be using a static IP, assign it as follows:

     ```
     ip addr add <IP/Mask> dev <Interface name>
     ```

     and note the IP you assigned.

     For example:

     ```
     ip addr add 192.168.0.86/24 dev eno1
     ```
3. Run ebp.sh.
   DHCP example: `./ebp.sh -d /dev/sda -t dhcp`
   Static example: `./ebp.sh -d /dev/sda -t static`
4. Wait for image copy to finish and the machine to reboot.
5. Determine the MAC addresses which will be used for the Elastifile data networks by running:
   `ip a`

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
```

```
valid_lft forever preferred_lft forever
2: eno33559296: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
link/ether 00:50:56:96:a8:db brd ff:ff:ff:ff:ff:ff
3: eno50338560: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
link/ether 00:50:56:96:f4:31 brd ff:ff:ff:ff:ff:ff
4: eno67109888: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
link/ether 00:50:56:96:40:01 brd ff:ff:ff:ff:ff:ff
```

6. Configure the Elastifile data network NICs by running the following command:
   `epa-cli nic set <MAC> <MTU> -s <static_ip_address>,<MASK>,1,1,1,<VLAN_ID>`

Elastifile recommends configuring the EMS data NIC with an IP address that ends with 101 (x.x.x.101).

Example:

```
root@localhost.localdomain ~# epa-cli nic set 00:50:56:96:f4:31 9000 -s
23.0.0.101,255.255.0.0,1,1,1,0
{
"errstr": "",
"status": 0
}
root@localhost.localdomain ~#
root@localhost.localdomain ~# epa-cli nic set 00:50:56:96:40:01 9000 -s
10.23.0.101,255.255.0.0,1,1,1,0
{
"errstr": "",
"status": 0
}
```

7. Run the installation script:

```
# ./install emanage.sh
```

8. Enter the relevant information for each question:

```
******************************
Select EMS Role (Primary/Secondary)
[1] Primary
[2] Secondary
1
You chose Primary, are you sure? [Y/n]
******************************
Select Management Network IP Type (DHCP/Static)
[1] DHCP
[2] Static
```

- If you selected DHCP, the following questions appear:

```
1
You chose DHCP, are you sure? [Y/n]
******************************
```

For EMS physical IP address, enter the IP you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter EMS physical IP address: 10.11.111.195
You chose 10.11.111.195, are you sure? [Y/n]
******************************
```

For EMS Virtual IP address network mask, enter the mask you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter EMS physical network mask: 255.255.0.0
You chose 255.255.0.0, are you sure? [Y/n]
```

```
******************************
```

For EMS Virtual IP address, enter the VIP you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter the EMS Virtual IP address: 10.11.209.5
You chose 10.11.209.5, are you sure? [Y/n]
```

- If you selected Static, the following questions appear:

```
2
You chose Static, are you sure? [Y/n]
******************************
```

For EMS physical IP address, enter the IP address you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter EMS physical IP address: 10.11.175.29
You chose 10.11.175.29, are you sure? [Y/n]
******************************
```

For EMS physical network mask, enter the mask you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter EMS physical network mask: 255.255.0.0
You chose 255.255.0.0, are you sure? [Y/n]

******************************
```

For Static IP Management Network Gateway, enter the gateway IP you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter Static IP Management Network Gateway: 10.11.0.1
You chose 10.11.0.1, are you sure? [Y/n]
******************************
Select do you want to add name server
[1] No
[2] Yes
2
You chose Yes, are you sure? [Y/n]
******************************
Enter local domain name (default empty): [None]
You chose None, are you sure? [Y/n]
local domain name (default empty): None
******************************
Enter list of name servers IP address, separated with comma: 10.11.0.21,10.12.0.21
You chose 10.11.0.21,10.12.0.21, are you sure? [Y/n]
list of name servers IP address, separated with comma: 10.11.0.21,10.12.0.21
******************************
Enter domain search list for host-name lookup (default empty), separated with comma: [None]
us.mycompany.com,lab.us.mycompany.com,build.us.mycompany.com
You chose us.mycompany.com,lab.us.mycompany.com,build.us.mycompany.com, are you sure? [Y/n]
domain search list for host-name lookup (default empty), separated with comma:
us.mycompany.com,lab.us.mycompany.com,build.us.mycompany.com
******************************
```

For EMS Virtual IP address, enter the VIP you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter the EMS Virtual IP address: 10.11.209.5
You chose 10.11.209.5, are you sure? [Y/n]
```

The installation process continues as follows:

```
*****************************
Setting up external network
The EMS virtual IP is 10.11.209.5
The EMS IP is 10.11.111.195

*****************************
```

9. Enter the Common Name (CN) for the host associated with the SSL certificate.

```
Enter commonName separated by comma (default empty): ems.mydomain.com
```

10. The installation finishes:

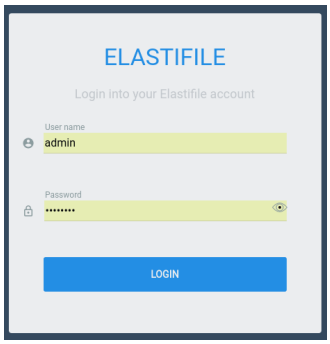
```
you can reuse the parameters by running the install script with @emanage_install_args_20170603-
104209
*****************************

EMS deployed successfully
```

After installing the EMS, you can log in to the Elastifile Management Console.

5. Logging in to Elastifile

To log in to the Elastifile system:

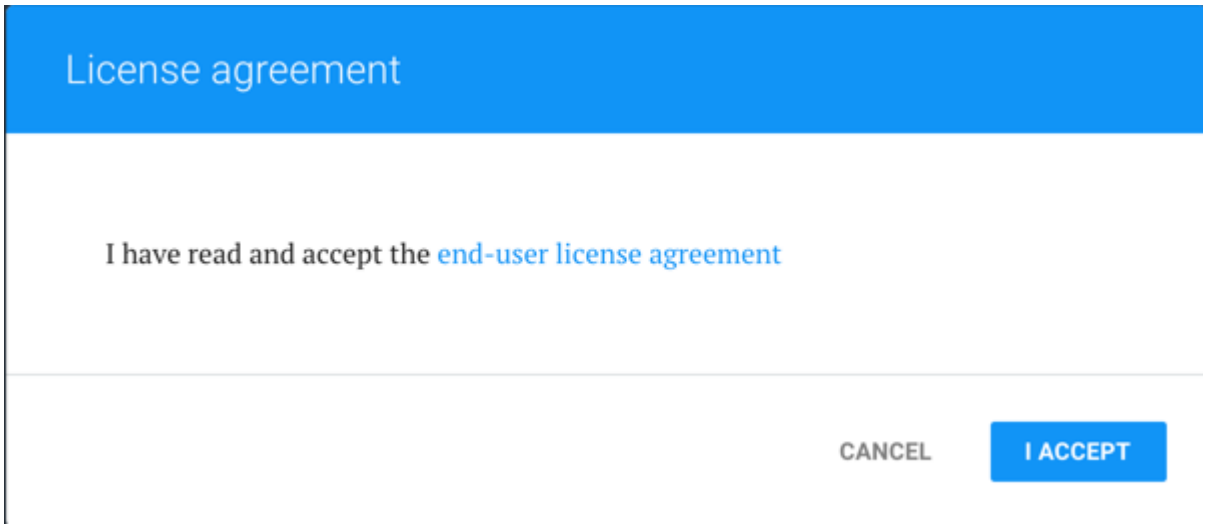
1. In your browser, enter the Elastifile Management URL (IP address or DNS name you set during installation of the primary EMS) and press Enter. The login window appears:



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 Elastifile system entities (nodes and optional secondary EMS).

6. Deploying Elastifile

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

6.1 Setting Up the Elastifile System

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

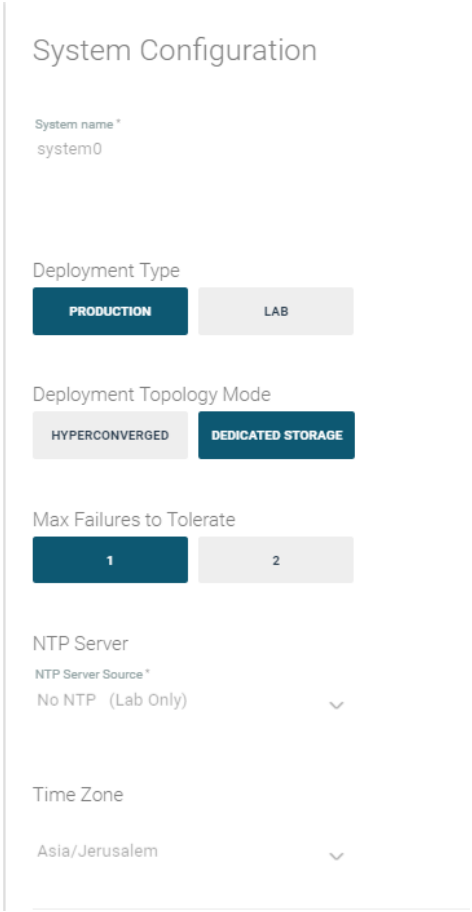
The wizard consists of the following main steps:

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 one of the following options: • **PRODUCTION** - select this option if you require high availability and performance. This option enforces minimum requirements as specified in Section 2 - Hardware Requirements and Section 3 - Preparing the Environment for Installation. • **LAB** - select this option if your setup is less than optimal, for example if you don't have network redundancy.
Deployment Topology Mode	Select **DEDICATED STORAGE**.
Max Failures to Tolerate	Select the number of servers that can fail without putting the Elastifile 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.

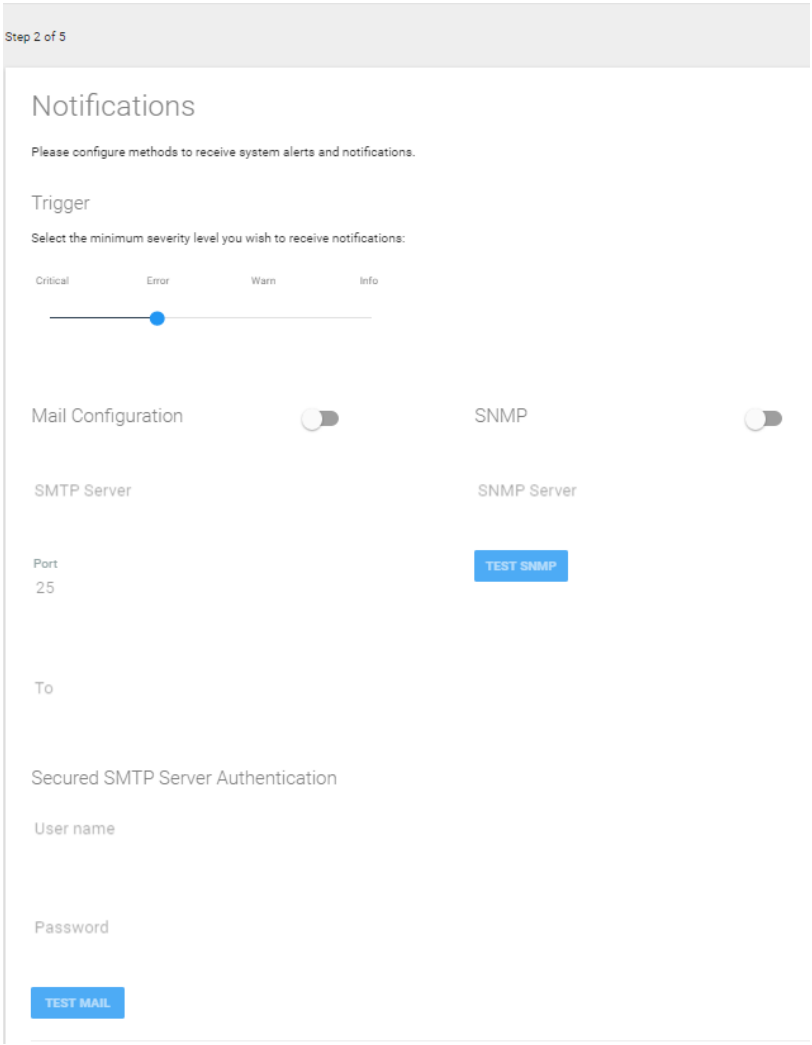
Details	Description
NTP Server	Select the time source to synchronize time settings in all system servers. Select one of the following options: • **Manual** - provide the IP address or DNS name of NTP server(s). Multiple NTP servers should be comma-separated. • **Google** - use Google's NTP servers. • **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 Elastifile 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:



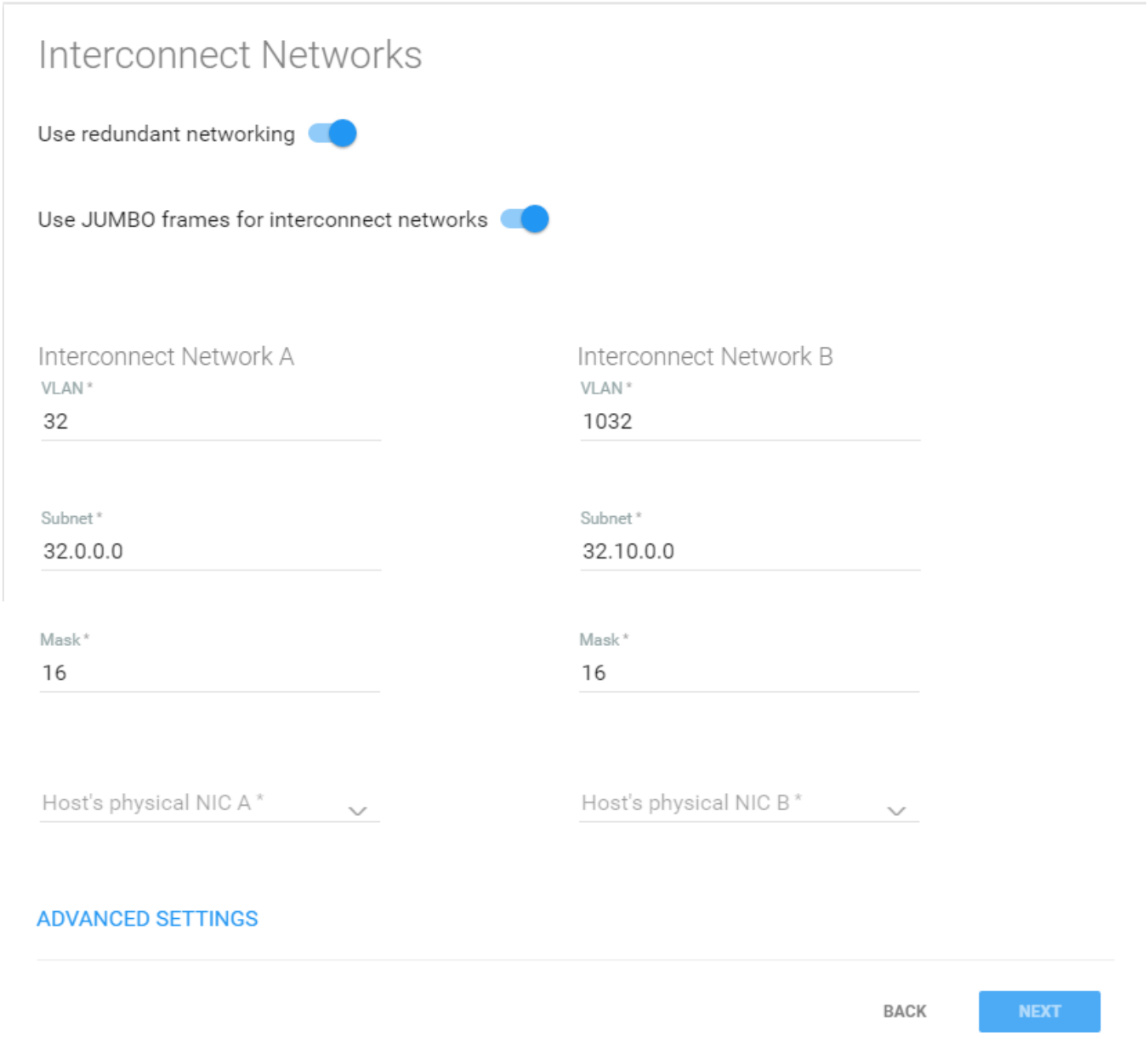
Details	Description
Trigger	Move the **Trigger** slider to your required minimum notification severity level: **Critical**, **Error**, **Warn** or **Info**.
Mail Configuration	To receive notifications via email: 1. Move the **Mail Configuration** slider to the right. 2. In **SMTP Server**, enter your 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 Elastifile, as explained in the following figure and table:



Details	Description
Use redundant net-working	If in "Step 1 - General System Configuration" on page 1 you selected the following Deployment type: • Lab mode - the **redundant networking** toggle is automatically set to on. • Production mode - the **redundant networking** is not displayed. • On (default option) - Data Network A and B are both available. Enter the **VLAN**, **Subnet** (IP), **Mask** for both networks. For **Host's Physical NIC**, select the EMS server's NIC that is connected to the respective network (A and/or B). • Off - only Data Network A fields are available. Enter the **VLAN**, **Subnet** (IP), **Mask**. For **Host's Physical NIC**, select the EMS server's NIC that is connected to network A .
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 Elastifile.

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 Elastifile 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 the Elastifile system through the wizard, the Management Console is in System view. You can now install Elastifile controllers and register them with the EMS. The Elastifile system must contains at least three controllers.

To install the controller, you will need to obtain (from Elastifile customer support) the Controller LiveCD.

To install a controller on a server:

1. Boot the server using a boot device with the Controller LiveCD.
2. When requested, use the following credentials:
   - user=root
   - password=123456
3. On the server, run:
   ```
   $ ./ebp.sh -d <device> -t none -e <EMS ip> [-a <admin password>]
   ```
   Writing the iso image file to /dev/sda (or any other system device) requires approximately 10 minutes.

   Example:

   ```
   ./ebp.sh -d /dev/sda -t none -e 10.11.209.29 -a admin abc123
   ```

   The server reboots.

If the server does not reboot, use RMM to perform a cold reboot.

4. Determine the MAC addresses which will be used for the Elastifile data networks by running:
   ```
   ip a
   ```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
```

```
2: eno33559296: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
link/ether 00:50:56:96:45:23 brd ff:ff:ff:ff:ff:ff
3: eno50338560: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
link/ether 00:50:56:96:e6:79 brd ff:ff:ff:ff:ff:ff
4: eno67109888: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
link/ether 00:50:56:96:22:4a brd ff:ff:ff:ff:ff:ff
```

5. Configure the Elastifile data network NICs by running the following command:
   `epa-cli nic set <MAC> <MTU> -s <static_ip_address>,<MASK>,1,1,1,<VLAN_ID>`

Example:

```
root@localhost.localdomain ~# epa-cli nic set 00:50:56:96:e6:79 9000 -s
23.0.0.11,255.255.0.0,1,1,1,0
{
"errstr": "",
"status": 0
}
root@localhost.localdomain ~#
root@localhost.localdomain ~# epa-cli nic set 00:50:56:96:22:4a 9000 -s
10.23.0.11,255.255.0.0,1,1,1,0
{
"errstr": "",
"status": 0
}
```

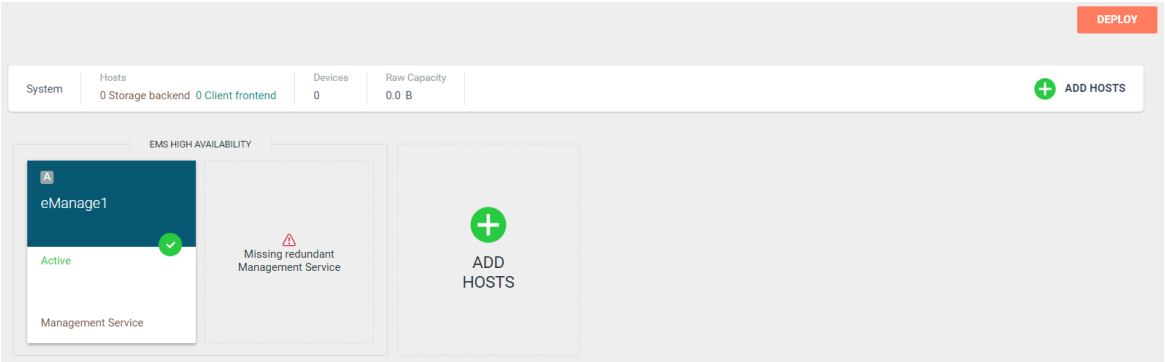
6. Register each controller with the EMS using one of the Elastifile data networks:
   `epa-cli sys register-physical-host --user USER --password PASSWORD --emanage-ip EMANAGE_IP --host-ip HOST_IP`

For each server on which you want to install the controller, repeat the above procedure To install a controller on a server:.

6.3 Adding Hosts

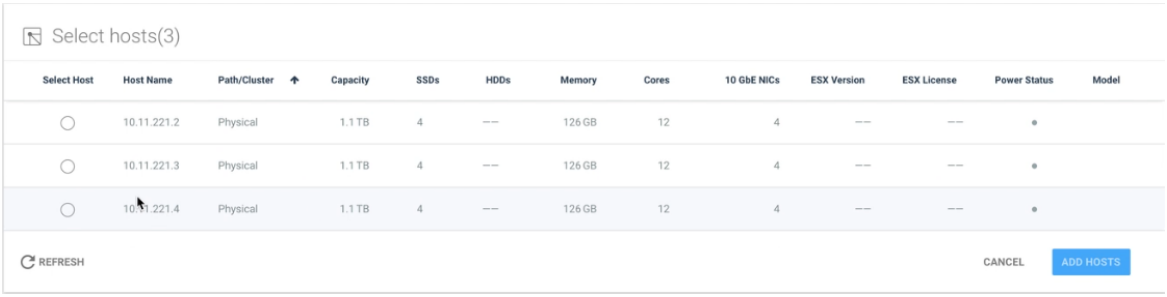
To add servers that will be used by the Elastifile system:

1. Click **ADD HOSTS**.

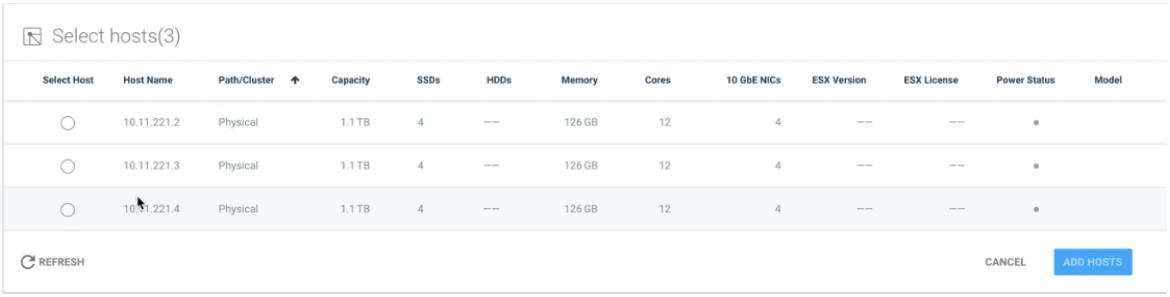


elastifile

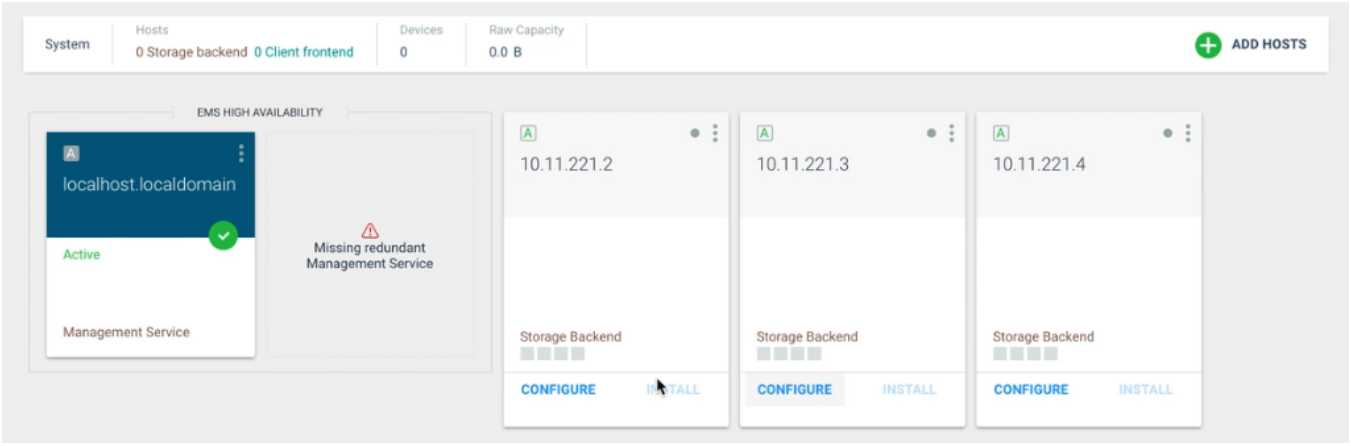
2. Select the servers to add:



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

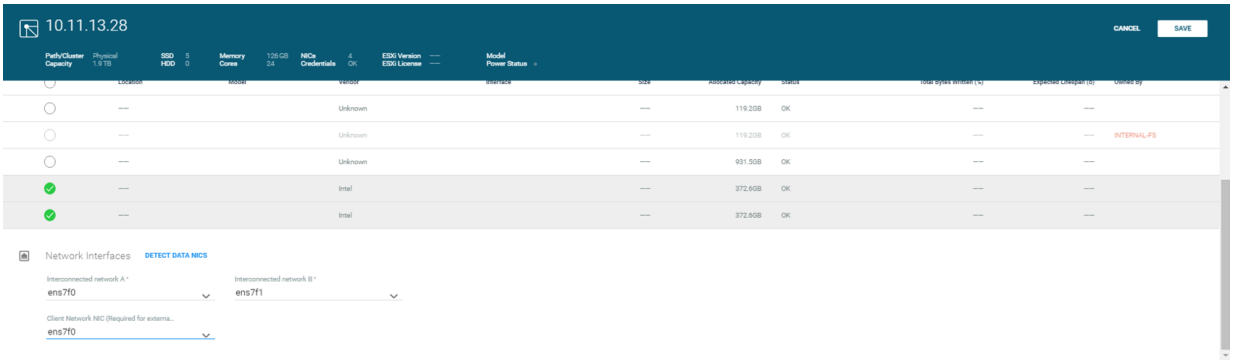


4. The System View window appears displaying the servers you selected.



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

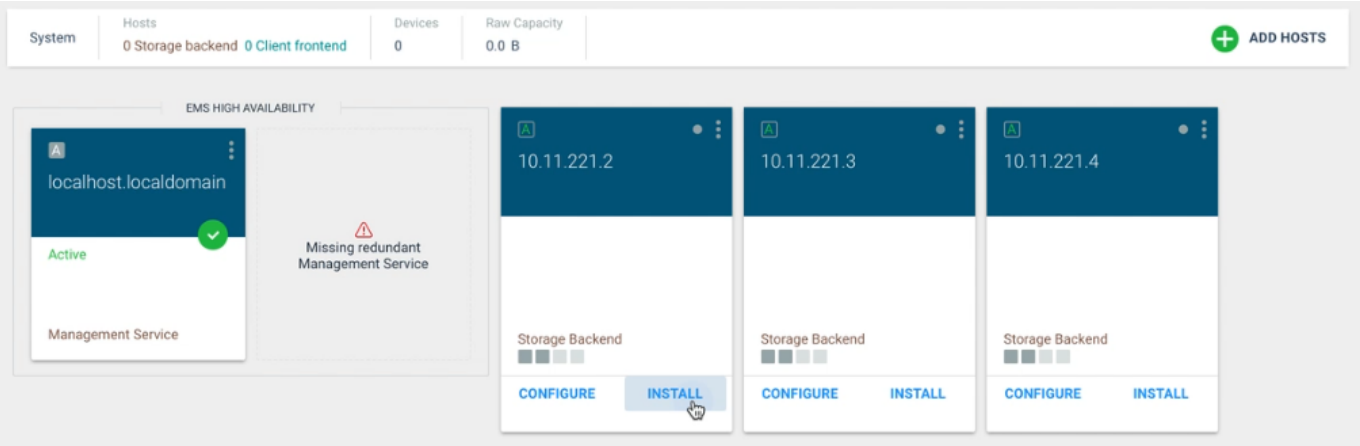
6. Configure the server as described below:



elastifile

Details	Description
Storage Devices	Select the storage devices that will be part of the Elastifile 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 server you are configuring , click **Detect Data NICS**. The Elastifile system automatically selects the NICs connected to the data networks . Select a different NIC if required. 2. If your hardware supports SR-IOV, toggle the **SR-IOV** on.

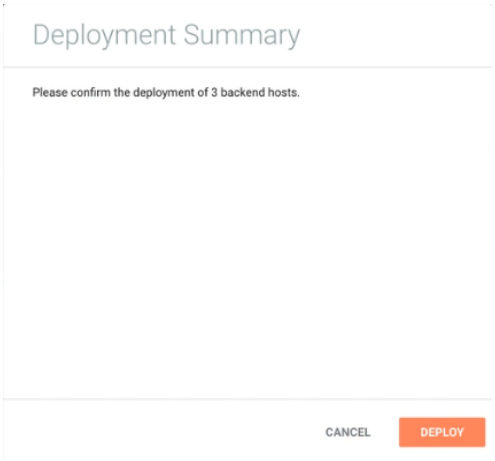
3. Click **SAVE**. The **INSTALL** button becomes active.



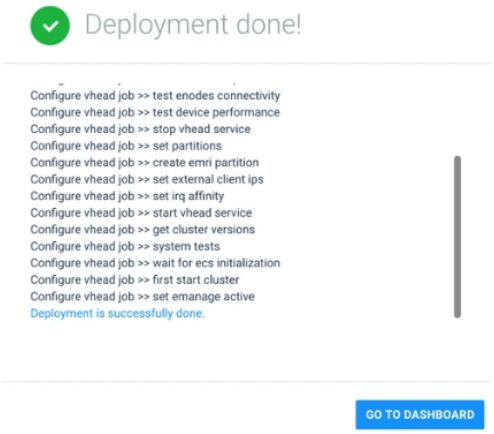
4. Click **INSTALL**. After a few seconds, a progress bar appears on the server.

You can configure and install several servers in parallel.

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



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



7. Installing the Secondary EMS (Optional)

- The EMS script must be run from a Linux machine with at least 10GB of free space.
- The file names and IP addresses in the following scripts are just examples.
- The term "eManage" in the installation script refers to the EMS machine.

1. On the server or VM that will serve as the EMS, boot into the EMS LiveCD using the following credentials:
   - User: root
   - Password: 123456
2. Obtain or assign the machine's IP as follows:
   - If you will be using DHCP, run:

   ip a

   and note the machine's IP.

   - If you will be using a static IP, assign it as follows:

   ```
   ip addr add <IP/Mask> dev <Interface name>
   ```

   and note the IP you assigned.

   For example:

   ```
   ip addr add 192.168.0.86/24 dev eno1
   ```
3. Run ebp.sh.
   DHCP example: ./ebp.sh -d /dev/sda -t dhcp
   Static example: ./ebp.sh -d /dev/sda -t static
4. Wait for image copy to finish and the machine to reboot
5. Run the installation script:

```
# ./install emanage.sh
```

6. Enter the relevant information for each question:

```
******************************
Select Installation mode (vCenter/physical)
[1] physical
[2] vCenter
1
You chose physical, are you sure? [Y/n]
******************************
Select EMS Role (Primary/Secondary)
[1] Primary
[2] Secondary
2
You chose Secondary, are you sure? [Y/n]
******************************
Enter Primary EMS physical IP address: 10.11.111.195
You chose 10.11.111.195, are you sure? [Y/n]
******************************
Enter Primary EMS username: admin
You chose admin, are you sure? [Y/n]
******************************
```

```
Enter Primary EMS password:
******************************
Select Management Network IP Type (DHCP/Static)
[1] DHCP
[2] Static
```

- If you selected DHCP, the following questions appear:

```
1
You chose DHCP, are you sure? [Y/n]
******************************
```

For EMS physical IP address, enter the IP you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter EMS physical IP address: 10.11.113.29
You chose 10.11.113.29, are you sure? [Y/n]
******************************
```

For EMS physical network mask, enter the mask you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter EMS physical network mask: 255.255.0.0
You chose 255.255.0.0, are you sure? [Y/n]
```

- If you selected Static, the following questions appear:

```
2
You chose Static, are you sure? [Y/n]
******************************
```

For EMS physical IP address, enter the IP address you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter EMS physical IP address: 10.11.175.29
You chose 10.11.175.29, are you sure? [Y/n]
******************************
```

For EMS physical network mask, enter the mask you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter EMS physical network mask: 255.255.0.0
You chose 255.255.0.0, are you sure? [Y/n]

******************************
```

For Static IP Management Network Gateway, enter the gateway IP you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter Static IP Management Network Gateway: 10.11.0.1
You chose 10.11.0.1, are you sure? [Y/n]
******************************
Select do you want to add name server
[1] No
[2] Yes
2
You chose Yes, are you sure? [Y/n]
******************************
Enter local domain name (default empty): [None]
You chose None, are you sure? [Y/n]
local domain name (default empty): None
******************************
```

```
Enter list of name servers IP address, separated with comma: 10.11.0.21,10.12.0.21
You chose 10.11.0.21,10.12.0.21, are you sure? [Y/n]
list of name servers IP address, separated with comma: 10.11.0.21,10.12.0.21
******************************
Enter domain search list for host-name lookup (default empty), separated with comma: [None]
us.mycompany.com,lab.us.mycompany.com,build.us.mycompany.com
You chose us.mycompany.com,lab.us.mycompany.com,build.us.mycompany.com, are you sure? [Y/n]
domain search list for host-name lookup (default empty), separated with comma:
us.mycompany.com,lab.us.mycompany.com,build.us.mycompany.com
******************************
```

For EMS Virtual IP address, enter the VIP you previously obtained from your IT department (as specified in the *DSM Site Preparation Guide*).

```
Enter the EMS Virtual IP address: 10.11.209.5
You chose 10.11.209.5, are you sure? [Y/n]
```

The installation process continues as follows:

```
******************************
Setting up external network
The EMS IP is 10.11.113.29
The EMS virtual IP is 10.11.209.5
******************************
Updating Secondary EMS with primary IP
******************************
Updating Primary EMS with secondary IP
Do you want to detect data networks [Y/n] Y
******************************
Trying to detect data networks
******************************
Select Secondary EMS Data1 network
[1] eno16777984
[2] eno33557248 [DetectedAsNic1]
[3] eno50336512 [DetectedAsNic2]
2
You chose eno33557248 [DetectedAsNic1], are you sure? [Y/n]
******************************
Select Secondary EMS Data2 network
[1] eno16777984
[2] eno33557248 [DetectedAsNic1]
[3] eno50336512 [DetectedAsNic2]
3
You chose eno50336512 [DetectedAsNic2], are you sure? [Y/n]
******************************
Update host 10.11.111.195 with chosen data networks
```

7. Enter the Common Name (CN) for the host associated with the SSL certificate.

```
Enter commonName separated by comma (default empty): ems.mydomain.com
```

8. The installation finishes:

```
you can reuse the parameters by running the install script with @emanage_install_args_20170603-
114644
******************************
EMS deployed successfully
```

After installing the EMS, you can log in to the Elastifile Management Console.

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. Tested Hardware List

The following list contains specific hardware models that have been tested to work with Elastifile.

A.1 Tested Switches

Brand	Model	Firmware
Mellanox	SX1012	SX_PPC_M460EX SX_3.3.5006
Brocade	NetXtreme II BCM 57810	

A.2 Tested NICs

Brand	Model	Firmware
Intel	82599EB	
Brocade	NetXtreme II BCM 57810	
Mellanox	MT27630	

A.3 Tested SSDs

Brand	Model	Firmware
Intel	82599EB	
	SATA/SAS based S3500/S3610	
Micron	P400 SSD, 400GB	
	P410m SSD, 400GB	
	P420m Enterprise PCIe SSD, 700GB	
	M500DC SATA SSD	
Samsung	XS1715 NVMe 400GB	
	850 PRO	
	SSD HDD Enterprise SM843T 2.5" 7mm 240GB MZ-7WD2400/003	
Sandisk	CloudSpeed Ultra SATA SSDs 400GB	