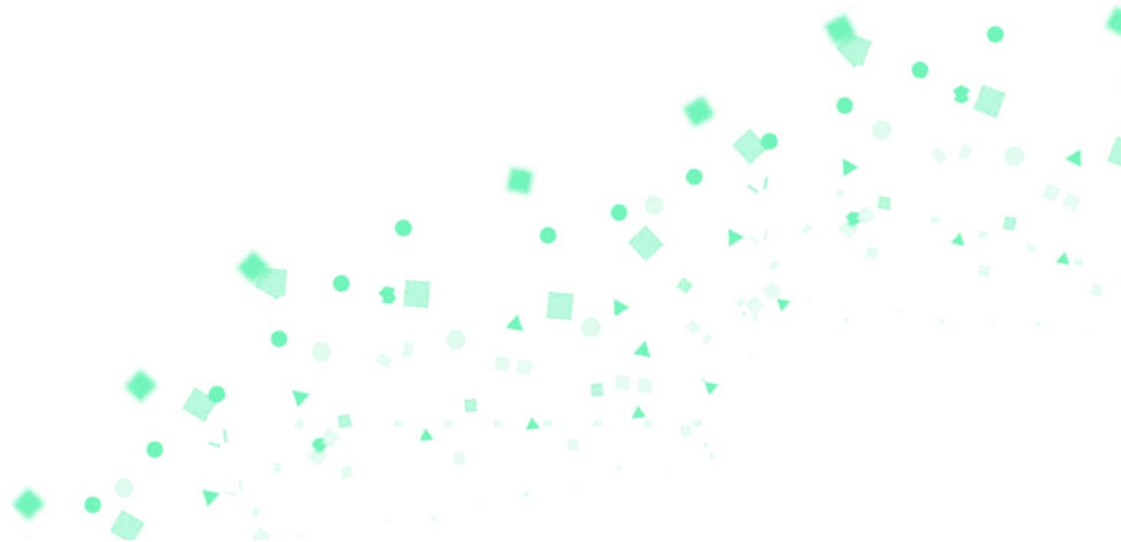




# empow Platform

quick setup guide



# Table of Contents

<b>Introduction .....</b>	<b>3</b>
Overview of the empow platform .....	3
System Components .....	3
System Requirements .....	3
Connectivity Map .....	4
<b>Installation procedure .....</b>	<b>5</b>
Summary .....	5
Apache Cassandra server .....	5
Forensics Server .....	10
Security Stack (SST) Server .....	14
DPI Server .....	18
<b>Start the application .....</b>	<b>24</b>
Success example .....	24
Failure example .....	25

# Introduction

## Overview of the empow platform

This document describes the installation procedure for the empow platform on VMware ESXi and the configuration steps required for launching the empow Security Stack (SST).

The platform is deployed on VMs from distribution OVAs.

## System Components

**Apache Cassandra server** – this is the database server for the platform, based on Apache Cassandra

**Forensics Server** – this server is used for Forensic searches; it is an optional component in the platform

**Security Stack (SST)** -this is the main platform server

**DPI server** – Deep Packet Inspection server

## System Requirements

The minimum system requirements are listed below. These will allow the system to boot for testing purposes, but will not be sufficient to operate in a production environment.

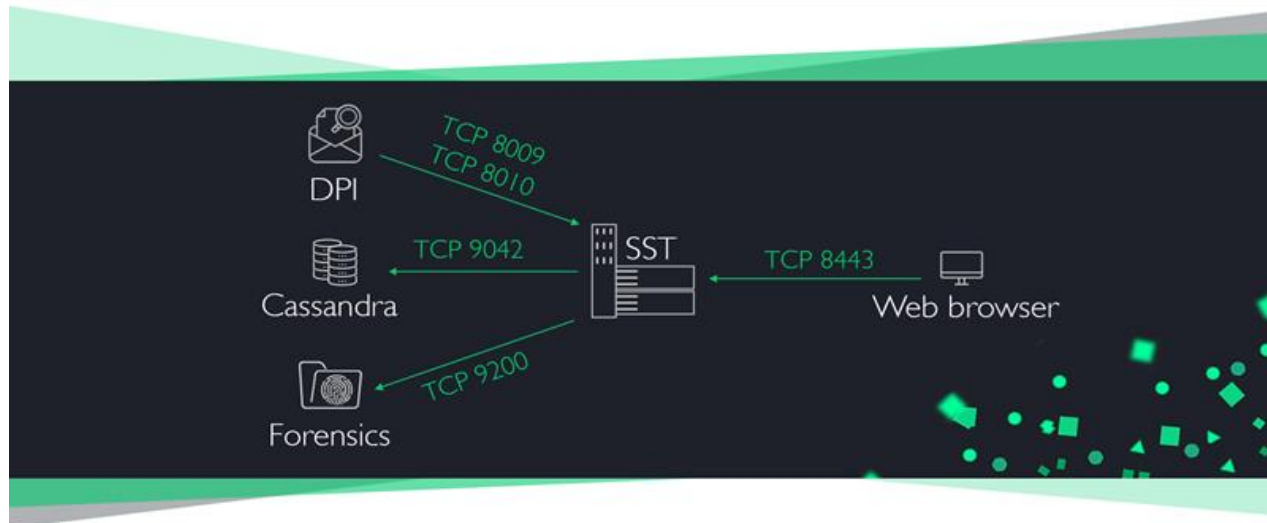
- empow Cassandra server
  - CPU cores 4
  - Memory 4GB
  - Disk Space 500GB
- empow Forensics server
  - CPU cores 4
  - Memory 4GB
  - Disk Space 100GB
- empow (SST) Security Stack
  - CPU cores 4
  - Memory 4GB
  - Disk Space 110GB
- DPI Server
  - CPU cores 6
  - Memory 12GB
  - Disk Space 50GB
- Virtualization platform

- VMware ESXi 6.0.0 or higher
- vSphere client 6.0.0 or higher

## Connectivity Map

The Security Stack (SST) server communicates with the Cassandra, Forensics, and DPI servers; the user accesses the Security Stack server using a web browser.

The figure below shows the communication ports.



SSH access is required to all empow servers, for support and troubleshooting purposes.

## Default communication ports table

Communication direction		Protocol & Port		Use
SST	→ Cassandra	TCP	9042	DB Queries
SST	→ Forensics	TCP	9200	DB Queries
SST	→ Empow cloud	TCP	443	Reports and classification
SST	→ smtp.gmail.com	TCP	587	Monitoring system alerts
DPI	→ SST	TCP	8009	NTA
DPI	→ SST	TCP	8010	Reputation
User	→ SST	TCP	8443	Web management
User	→ Empow cloud	TCP	443	Reports access
User	→ All empow machines	TCP	22	CLI access

# Installation procedure

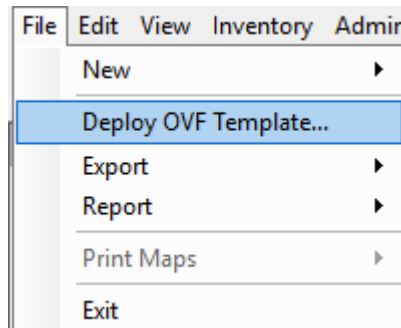
## Summary

The empow platform is installed on three VMs, using the vSphere client and the distribution OVA files.

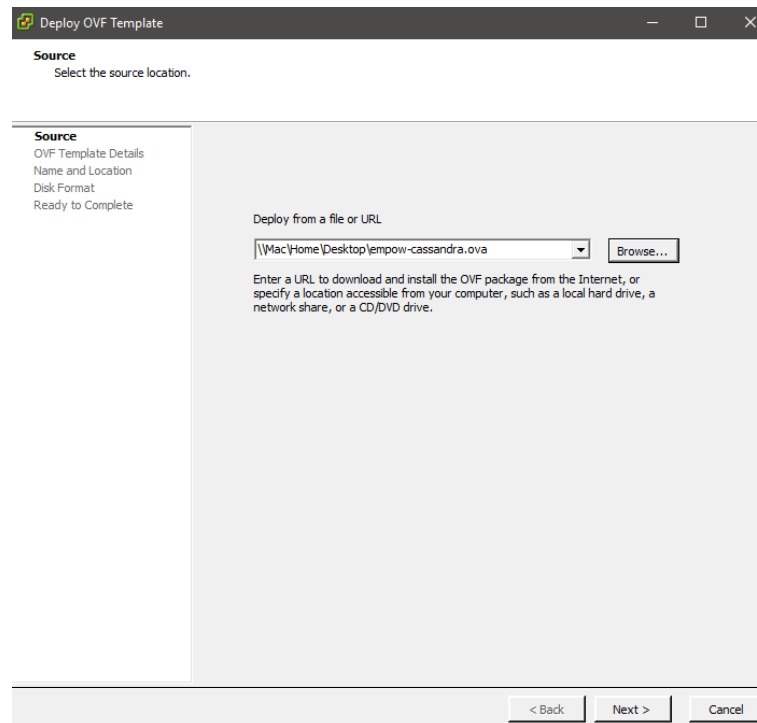
## Apache Cassandra server

### Deploy the image using the vSphere client

1. On the vSphere client, navigate to **File > Deploy OVF template...**



2. Enter the empow-cassandra.ova file location.



3. Choose a storage provisioning method from the following options:

- Thick Provision Lazy Zeroed

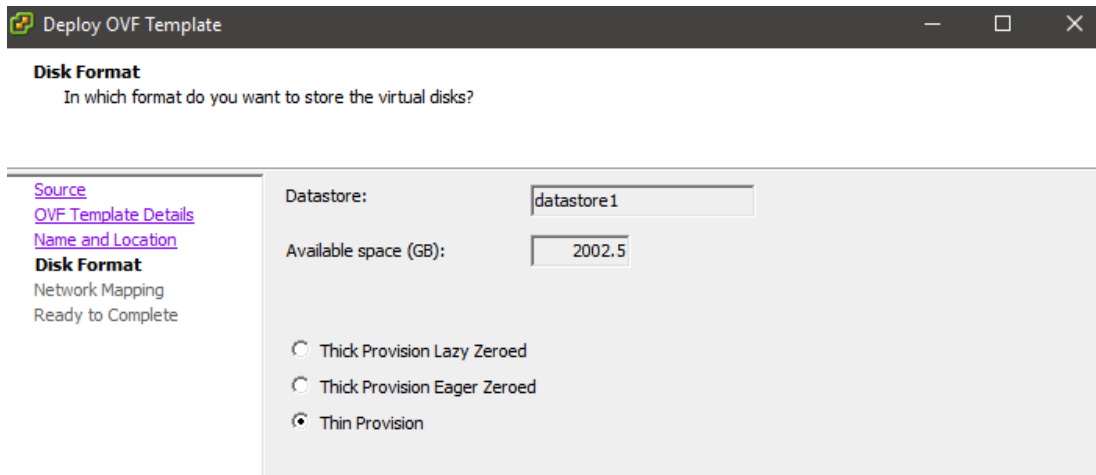
If you want to pre-allocate the space for your disk, one option is to make a thick lazy zeroed disk. It won't be subject to fragmentation since it pre-allocates all the space so no other files will get in the middle (which causes fragmentation), and it's easier to track capacity utilization.

- Thick Provision Eager Zeroed

When provisioning a thick eager zeroed disk, VMware pre-allocates the space and then zeroes it all out ahead of time. In other words, this takes a while — just to increase the net-new write performance of your virtual disk. We don't frequently see the benefit in this since you only enjoy this perk only one time. It doesn't improve the speed of any of the innumerable subsequent overwrites.

- Thin Provision

This type of virtual disk allows you to allocate storage on demand, instead of deciding ahead of time how much space it's going to take up. This is a good option if you want to control costs and scale out your storage over time. However, you need to pay closer attention to your disk size so you don't overprovision and overcommit your storage to more than it can hold. Additionally, since it's allocating on the fly, you might take some performance hits on initial writes that you wouldn't encounter if you were to utilize one of its thick disk brethren options. This is because as new data space is allocated, the blocks have to first be zeroed to ensure the space is empty before the actual data is written.



The screenshot shows a window titled "Deploy OVF Template" with a sidebar on the left containing links: "Source", "OVF Template Details", "Name and Location", "Disk Format" (which is highlighted), "Network Mapping", and "Ready to Complete". The main area of the window is titled "Disk Format" with the subtitle "In which format do you want to store the virtual disks?". It contains two input fields: "Datastore:" with the value "datastore1" and "Available space (GB):" with the value "2002.5". Below these fields are three radio button options: "Thick Provision Lazy Zeroed", "Thick Provision Eager Zeroed", and "Thin Provision" (which is selected).

We recommend the Thick provision Lazy Zeroed option, for all servers.

4. Assign the machine to the management network.

Deploy OVF Template

Source

OVF Template Details

Name and Location

Disk Format

Network Mapping

Ready to Complete

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
VM Network	VM Network

- After the image is uploaded, edit the virtual machine settings to adjust the amount of memory and the number of CPU cores, based on the sizing calculator results, and add additional disk to expand the memory, if required.

The image comes with a 500GBytes hard disk.

empow-cassandra

Getting Started

Summary

Resource Allocation

Performance

Events

Console

Permissions

close tab X

What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

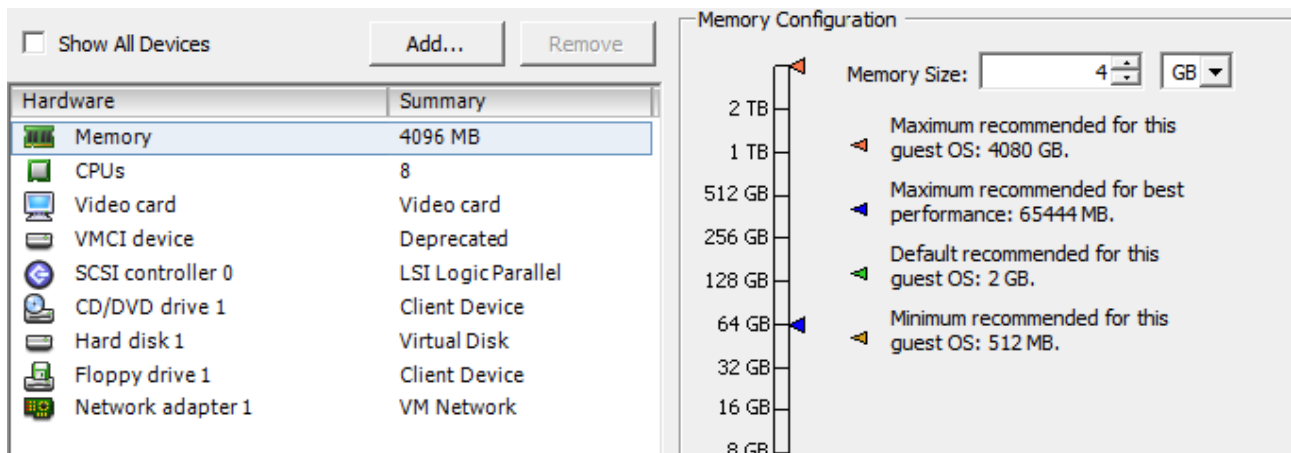
Power on the virtual machine

Edit virtual machine settings

Virtual Machines

Host

vSphere Client



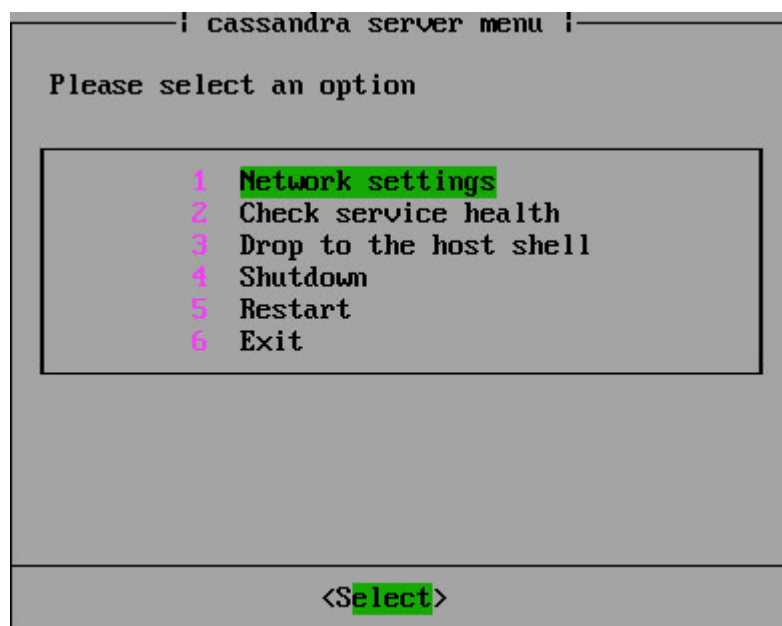
## Initial configuration

1. Launch the virtual machine, open the console and wait for the login prompt.

Use the following credentials to log in:

Username: admin

Password: empow



2. Enter the network settings to configure the IP address and assign a hostname



```

      | network settings |
Current IP: 192.168.1.102
MAC address: 00:0c:29:06:61:13
Hostname: empow-cassandra

Please select an option

1 Change the IP address
2 Change device hostname
3 Apply network settings now
4 Go back to the main the menu

<Select>

```

If the network has DHCP service, the server will receive an IP address.

*Note: for system stability, it is mandatory to assign a static IP address or bind the received address on the DHCP server side*

Change the hostname to use the following convention – *customer\_name-service*

e.g. customer\_x-cassandra.

*Note: the hostname will change only after rebooting the machine*

3. In the main menu, select **Check service health** to validate that Cassandra is up and running. If there is a problem, the reason should appear.

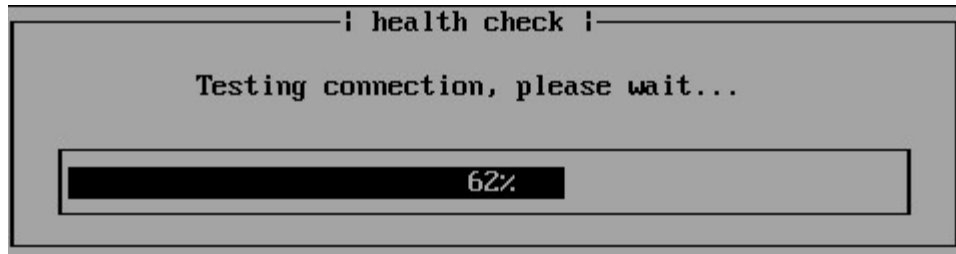
```

Please select an option

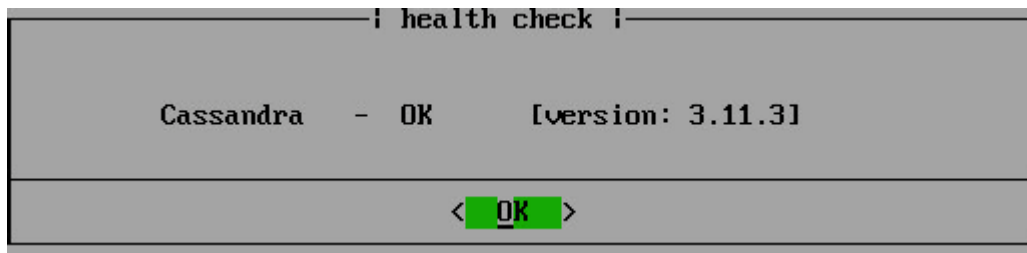
1 Network settings
2 Check service health
3 Drop to the host shell
4 Shutdown
5 Restart
6 Exit

```

While the test is in progress, this will be shown:



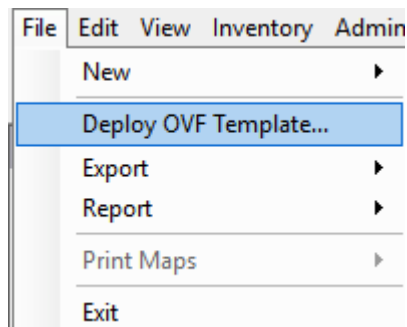
When completed, the result will be shown:



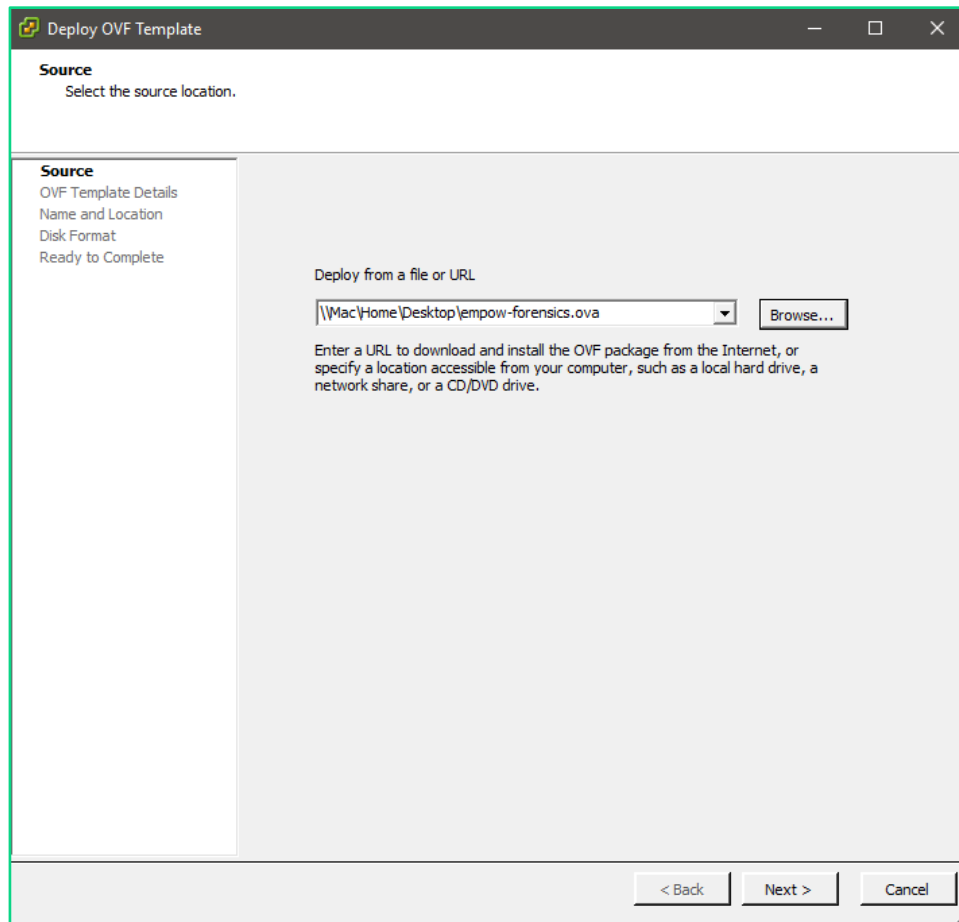
## Forensics Server

### Deploy the image using vSphere client

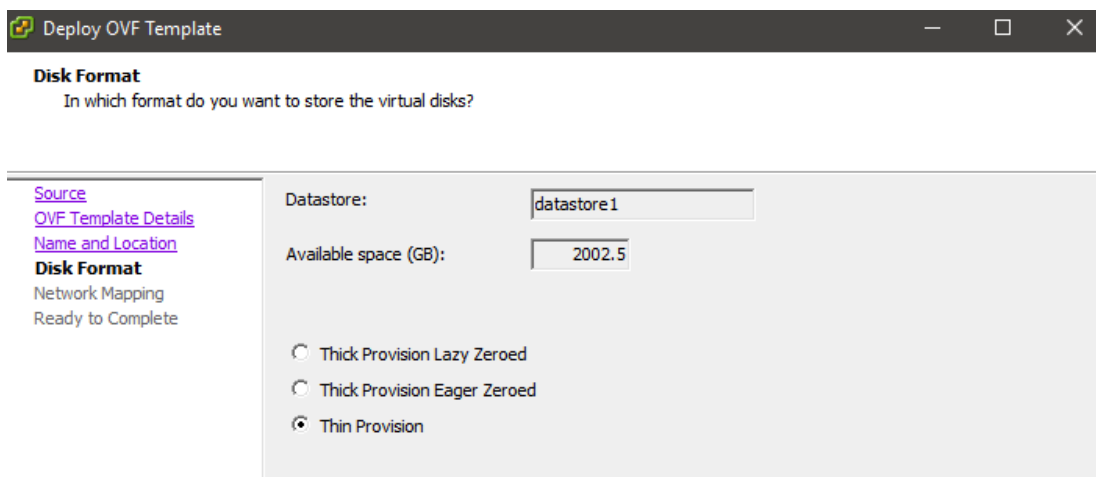
1. In the vSphere client, navigate to **File > Deploy OVF template...**



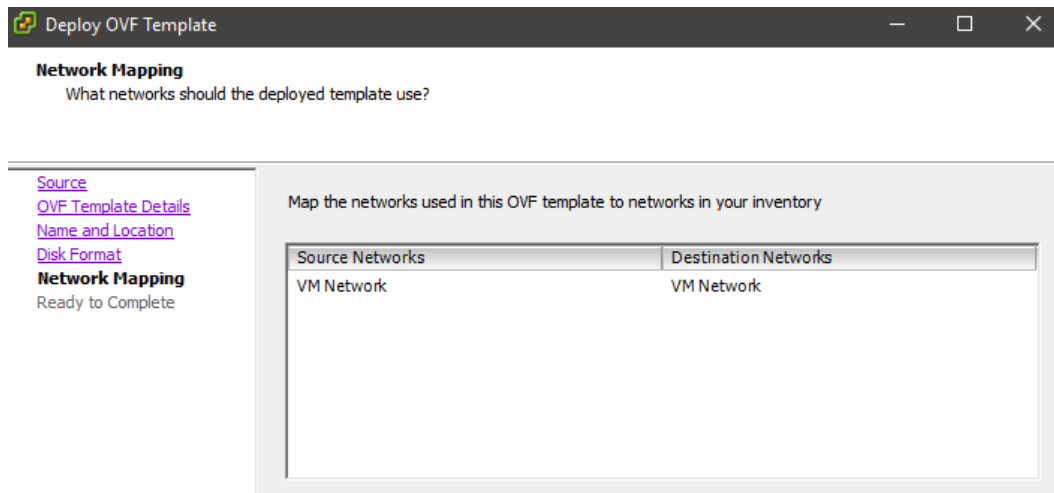
2. Enter the empow-forensics.ova file location.



3. Choose a storage provisioning method from the same options as for the Cassandra server (in the previous section).

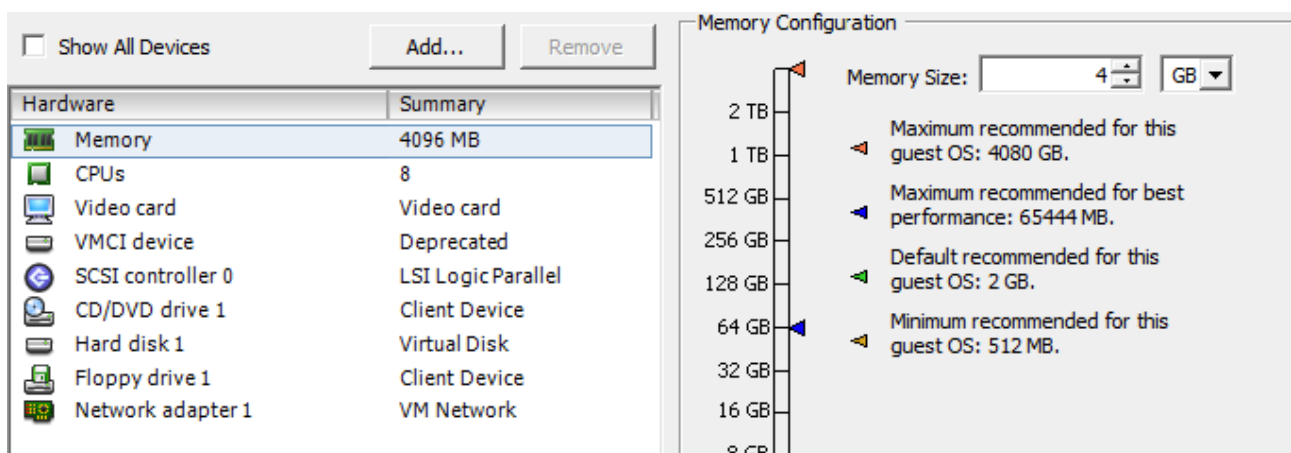


4. Assign the machine to the management network.



5. After the image is uploaded, edit the virtual machine settings to adjust the amount of memory and the number of CPU cores, based on the sizing calculator results, and add additional disk to expand the memory, if required.

The image comes with a 100GBytes hard disk.



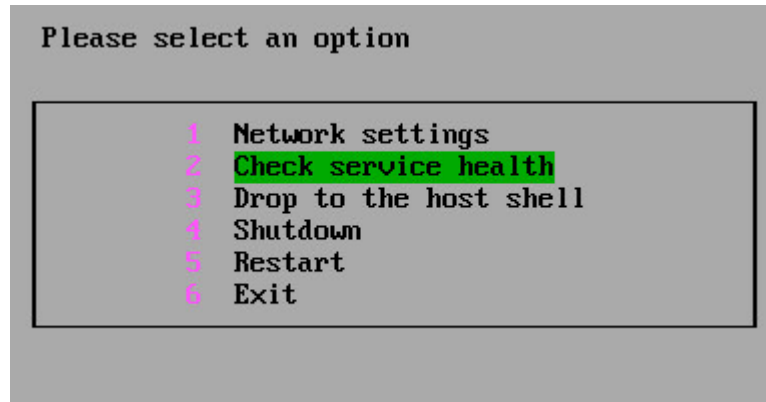
## Initial configuration

1. Launch the virtual machine, open console and wait for the login prompt.

Use the following credentials to log in:

Username: admin  
Password: empow

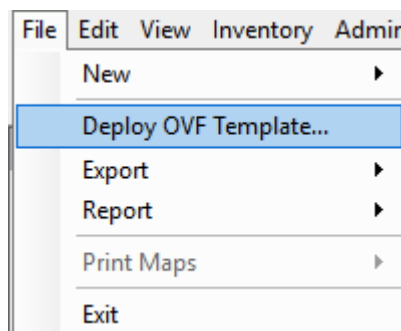




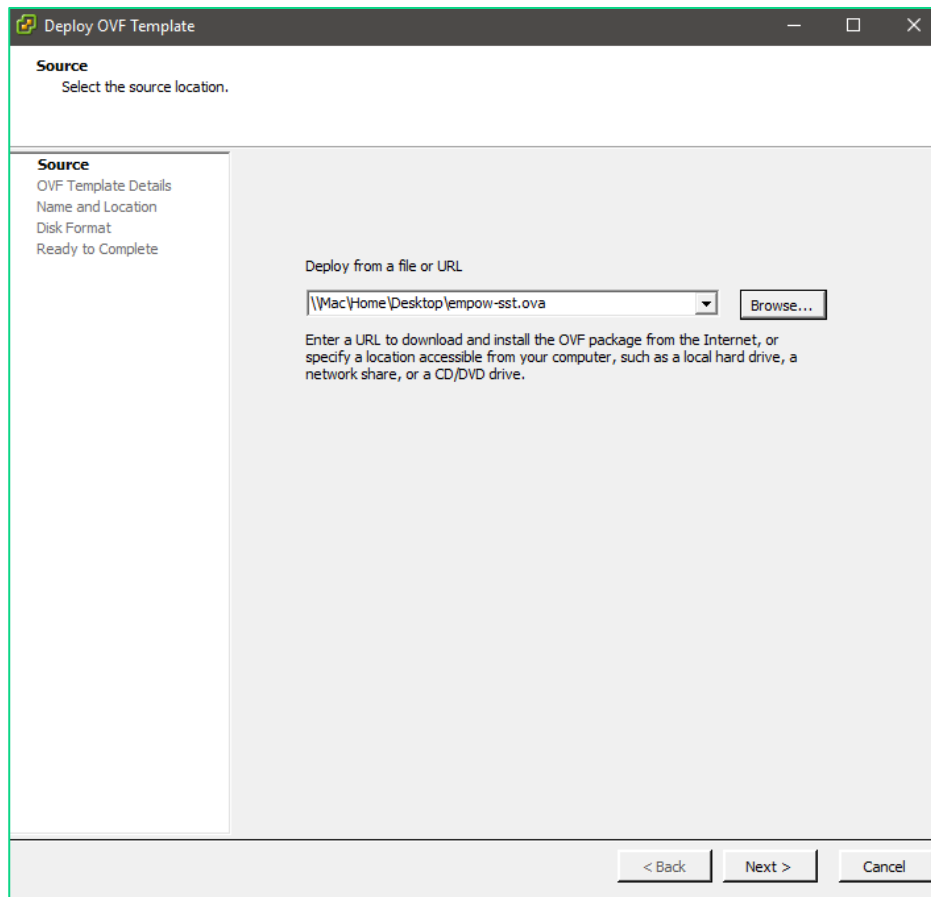
## Security Stack (SST) Server

### Deploy the image using vSphere client

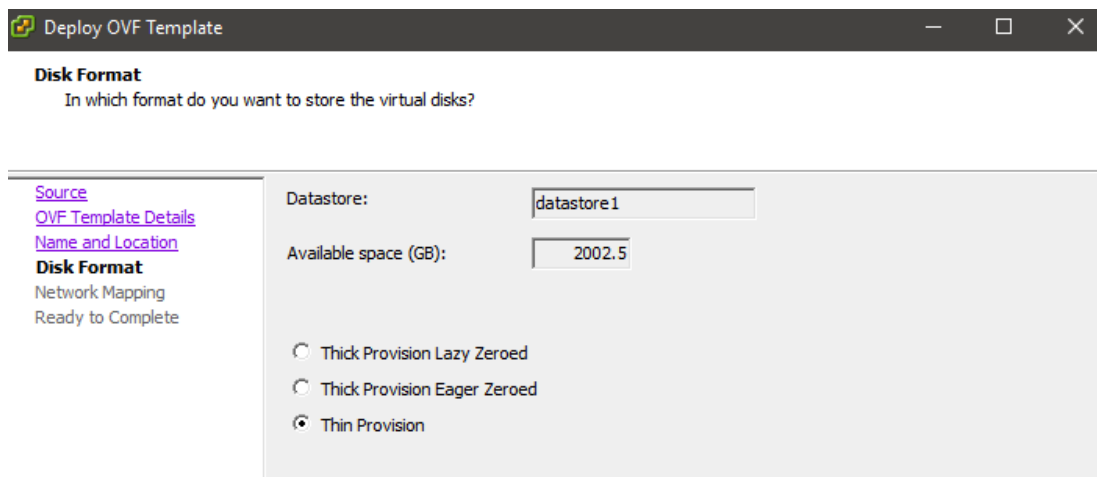
1. In the vSphere client, navigate to **File > Deploy OVF template...**



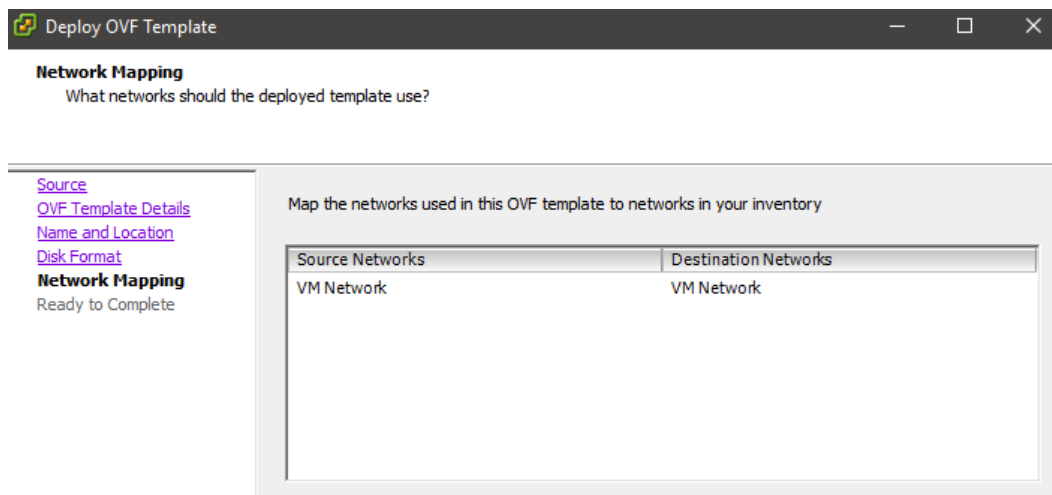
2. Enter the empow-sst.ova file location.



3. Choose a storage provisioning method, as for the Cassandra and Forensics servers.

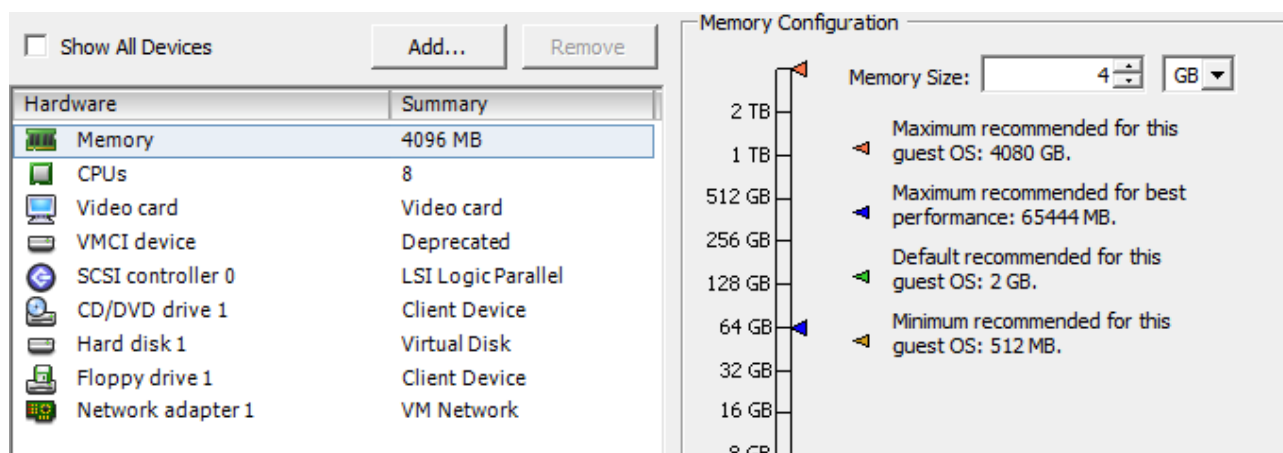


4. Assign the machine to the management network.



5. After the image is uploaded, edit virtual machine settings to adjust the amount of memory and the number of CPU cores, based on the sizing calculator results, and add additional disk to expand the memory, if required.

The image comes with a 110GBytes hard disk.



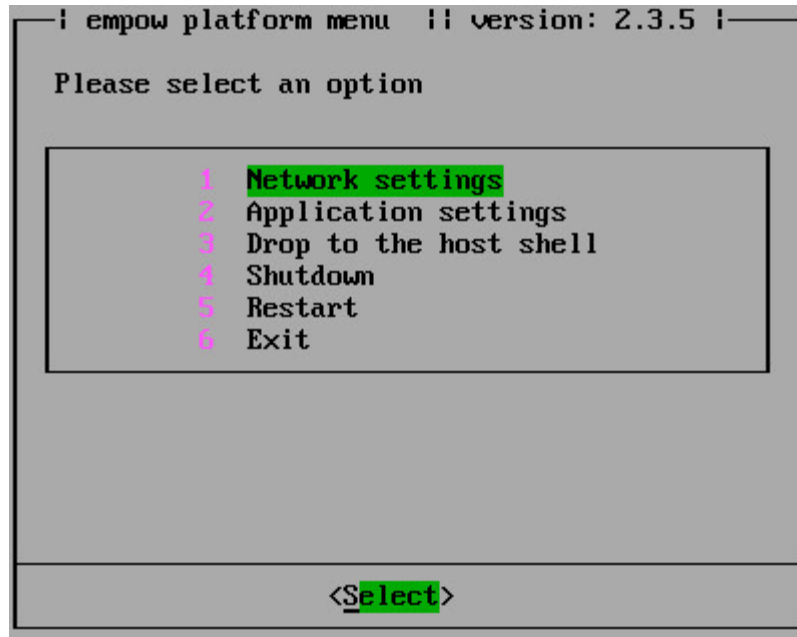
## Initial configuration

1. Launch the virtual machine, open console and wait for the login prompt.

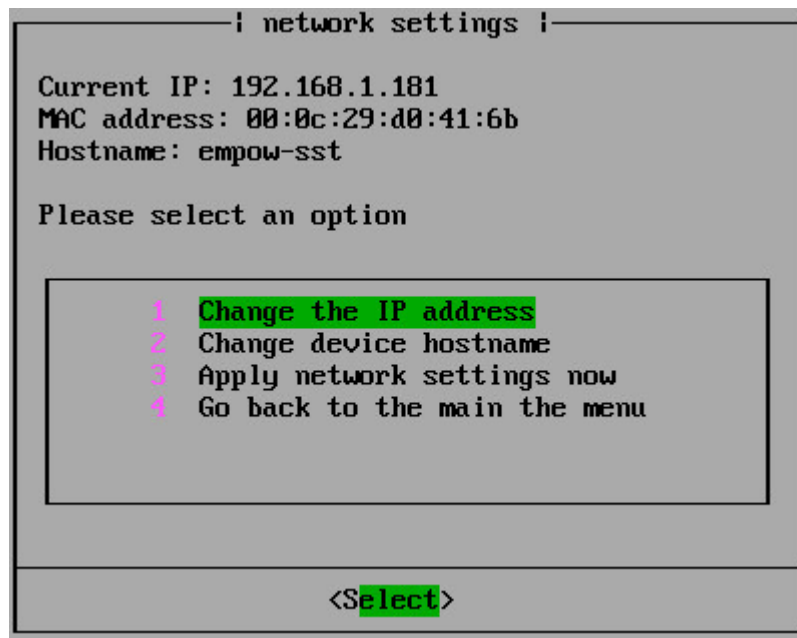
Use the following credentials to log in:

Username: admin  
Password: empow





2. Enter the network settings to configure the IP address and assign a hostname.



If the network has DHCP service, the server will receive an IP address.

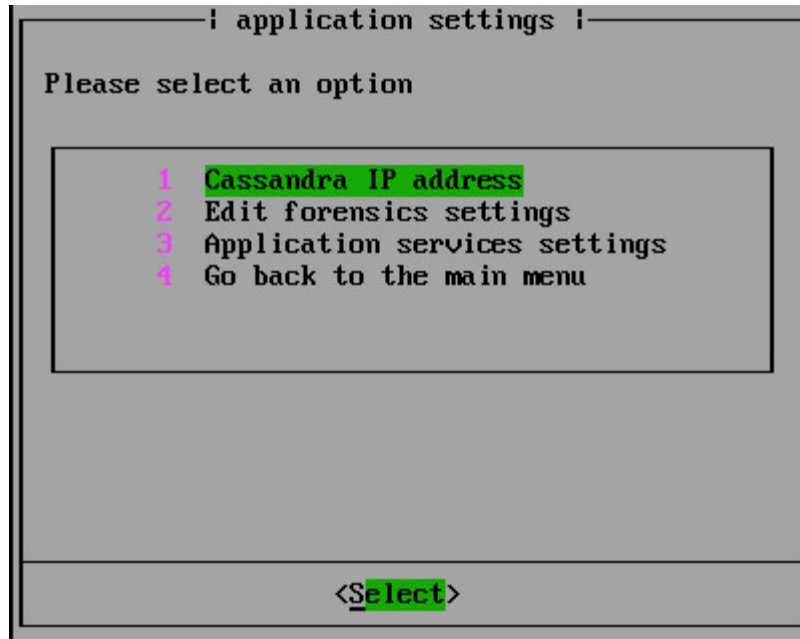
*Note: for system stability, it is mandatory to assign a static IP address or bind the received address on the DHCP server side.*

Change the hostname to use the following convention – *customer\_name-service*

e.g. customer\_x-sst.

*Note: the hostname will change only after rebooting the machine.*

Go back to the main menu and select application settings to configure mandatory setting prior starting the application.



### 3. Configure Cassandra IP address

Enter the IP address assigned to the Cassandra server.

### 4. Edit forensics settings

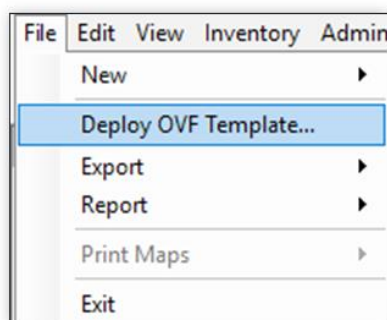
Change the status of the Forensics service and enter the IP address.

*Note: ensure that the service is set to OFF if the Forensics service is not going to be used.*

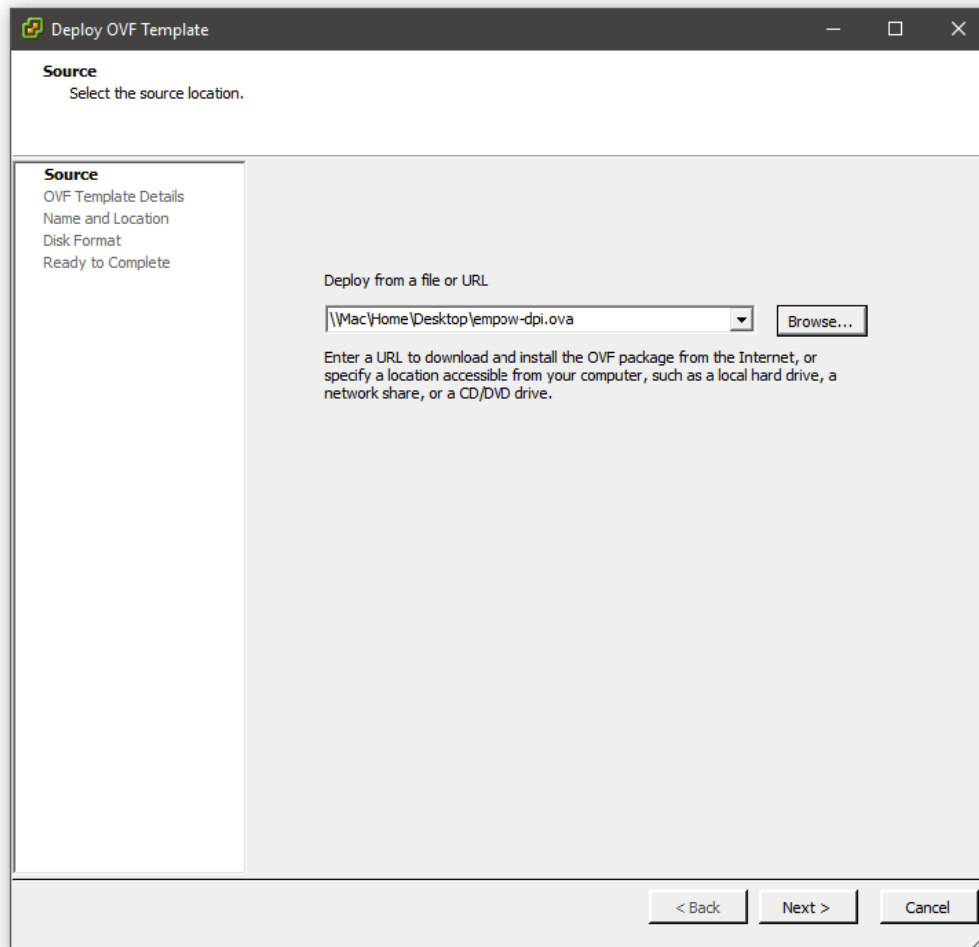
## DPI Server

### Deploy the server

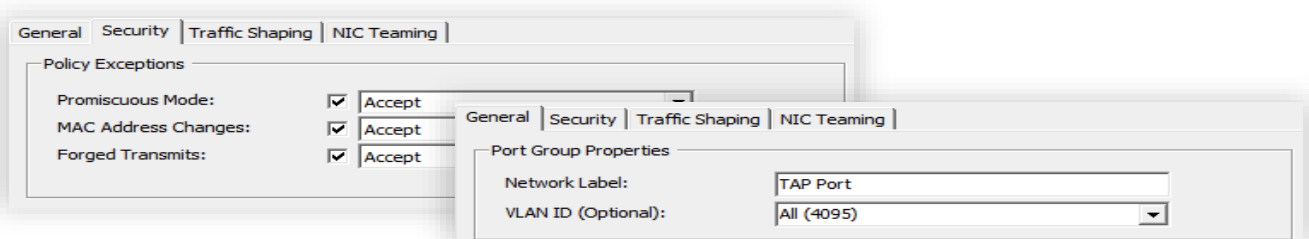
1. In the vSphere client, navigate to **File > Deploy OVF template...**



2. Enter the empow-dpi-universal.ova file location.



3. Choose a storage provisioning method, as for the Cassandra and SST servers.
4. Configure the VMware vSwitch to allow all VLAN IDs and have promiscuous mode enabled, in order to deliver all the mirrored traffic it receives to the empow DPI server.

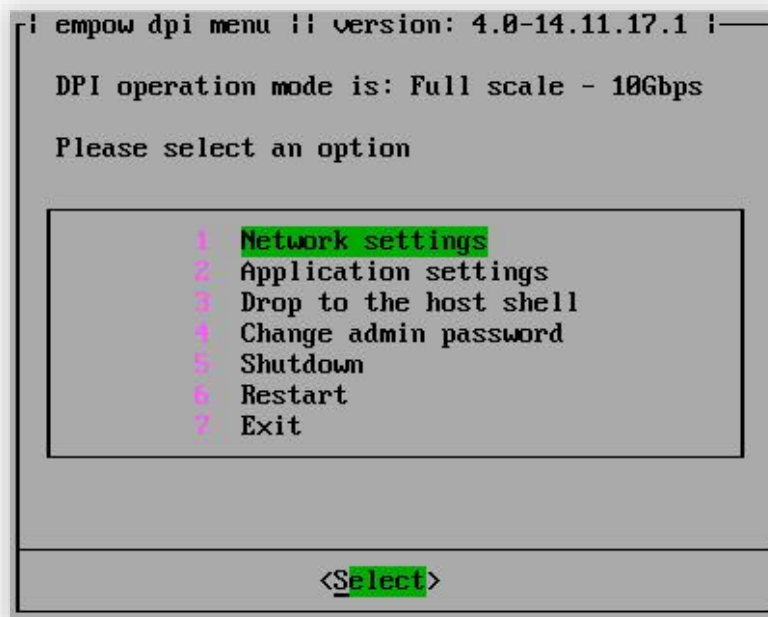


## Initial configuration

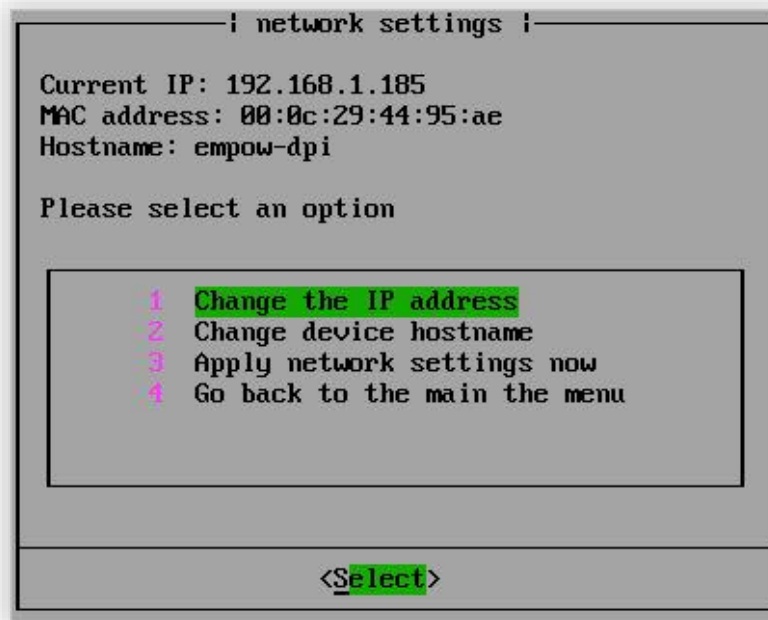
1. Launch the virtual machine, open the console and wait for the login prompt.

Use the following credentials to log in:

Username: admin  
Password: empow



2. Enter the network settings to configure the IP address and assign a hostname.



## Application configuration

1. The server boots in a “full scale” operating mode by default. Choose option 3 (“Change to 1Gbps operation mode”) in the application menu to set the operation mode to small scale – up to 1Gbps.

*Note: Changing the operation will reboot the system. A warning message will be displayed.*

```

! dpi application settings !! dpi id: 1 !
DPI operation mode is: Full scale - 10Gbps

Get or change the application status,
define the SST server IP address and
check SST server connection status.

Please select an option:

1 Get the application status
2 Check SST server connectivity
3 Change to 1Gbps operation mode
4 Define empow SST address
5 Change the DPI ID
6 Start the DPI application
7 Show packet capture log
8 Go back to main menu

<Select>

```

2. In the application menu, select option 4 ("Define empow SST address") to set the empow Security Stack server IP address.

```

! empow dpi settings !
Currently configured SST server IP: 127.0.0.1
Please enter SST server's IP address:

-

<OK> <Cancel>

```

3. If another empow DPI is already deployed, the DPI ID for this server must also be changed. Select option 5 ("Change the DPI ID") to set a new DPI ID. The default value is 1.

*Note: the ID allows the Security Stack server to differentiate between different DPI servers, and must be a numeric value.*

```

      | empow dpi settings |
      |
      | Currently configured DPI ID: 1
      |
      | If there is more than one DPI server in the network
      | the ID must be unique on each server - digits only.
      |
      | Please enter a new DPI ID:
      |
      | 
      |
      | < OK >      < cancel >
  
```

4. Select option 6 ("Start the DPI application") to start the server.

```

      | dpi application settings || dpi id: 1 |
      |
      | DPI operation mode is: Full scale - 10Gbps
      |
      | Get or change the application status,
      | define the SST server IP address and
      | check SST server connection status.
      |
      | Please select an option:
      |
      | 1 Get the application status
      | 2 Check SST server connectivity
      | 3 Change to 1Gbps operation mode
      | 4 Define empow SST address
      | 5 Change the DPI ID
      | 6 Start the DPI application
      | 7 Show packet capture log
      | 8 Go back to main menu
      |
      | < Select >
  
```

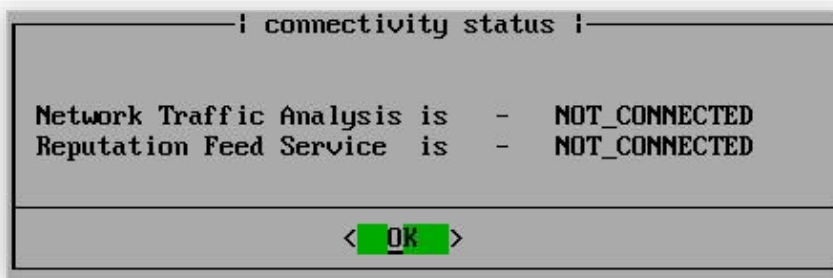
## Validation

Check service and connectivity status of the server.

1. Select option 1 ("Get the application status") to check the current status.



2. Select option 3 ("Check SST server connectivity") to check the connectivity status between the empow DPI and the empow Security Stack (SST) servers.



*Note: the status will show CONNECTED or NOT\_CONNECTED based on the current real time status.*

3. When the application is running, select option 7 ("Show packet capture log") to preview layer 4 traffic details, source and destination IP addresses, ports, and protocols.

*Note: this option can be used for troubleshooting, or to validate that the mirrored traffic arrives at the capturing port.*

# Start the application

1. Select application services settings to perform quick sanity test and start the empow application.

```
— ! application settings ! —

Check the current status of empow application,
run a quick readiness test and see services
availability, or start/stop the application.

Please select an option:

1 Get the application status
2 Run quick readiness test
3 Start empow application
4 Go back to previous screen

<Select>
```

2. Choose the run quick readiness test option to get the sanity test results.

```
— ! readiness check ! —

Gathering information, please wait...

[Progress Bar] 18%
```

## Success example

```
— ! readiness check ! —

Cassandra - OK [version: 3.11.3]
Forensics - OK [version: 6.2.4]
Rabbit MQ - OK [version: 3.6.9]
Maria DB - OK [version: 10.2.16]

Status: OK - The application can be started.

< OK >
```



## Failure example

! readiness check !

Cassandra	-	FAILED	[reason: Connection refused]
Forensics	-	Disabled	in the configuration.
Rabbit MQ	-	OK	[version: 3.6.9]
Maria DB	-	OK	[version: 10.2.16]

**WARNING!** The system will fail to start!

< **OK** >

If the readiness test is successful, select **Start empow application**.

! application settings !

Check the current status of empow application, run a quick readiness test and see services availability, or start/stop the application.

Please select an option:

1 Get the application status

2 Run quick readiness test

3 **Start empow application**

4 Go back to previous screen

< **Select** >

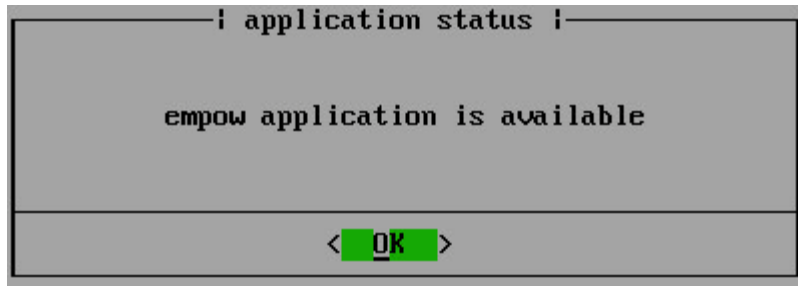
3. Check the application status, by selecting the first option.

! application status !

**empow application is starting**

< **OK** >

*Note: the screen will not refresh by itself, make sure to refresh it manually every few seconds, by pressing OK and selecting the get the current application status.*

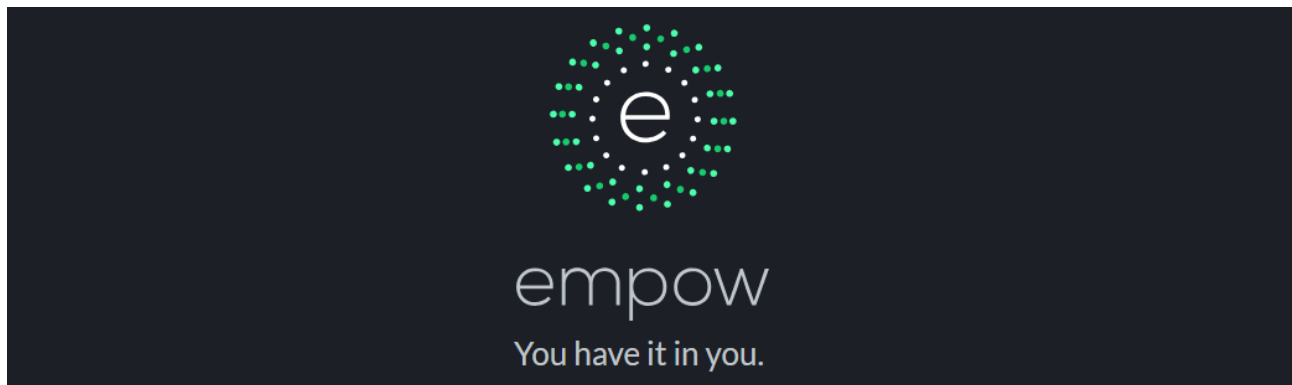


When the application status switches to available, access the web management interface at [https://EMPOW\\_SST\\_IP\\_ADDRESS:8443](https://EMPOW_SST_IP_ADDRESS:8443)


Use the following credentials to log in:


Username: admin

Password: empow



## LOGIN

 admin

 .....

SIGN IN