empow Platform

installation guide

Table of Contents

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.

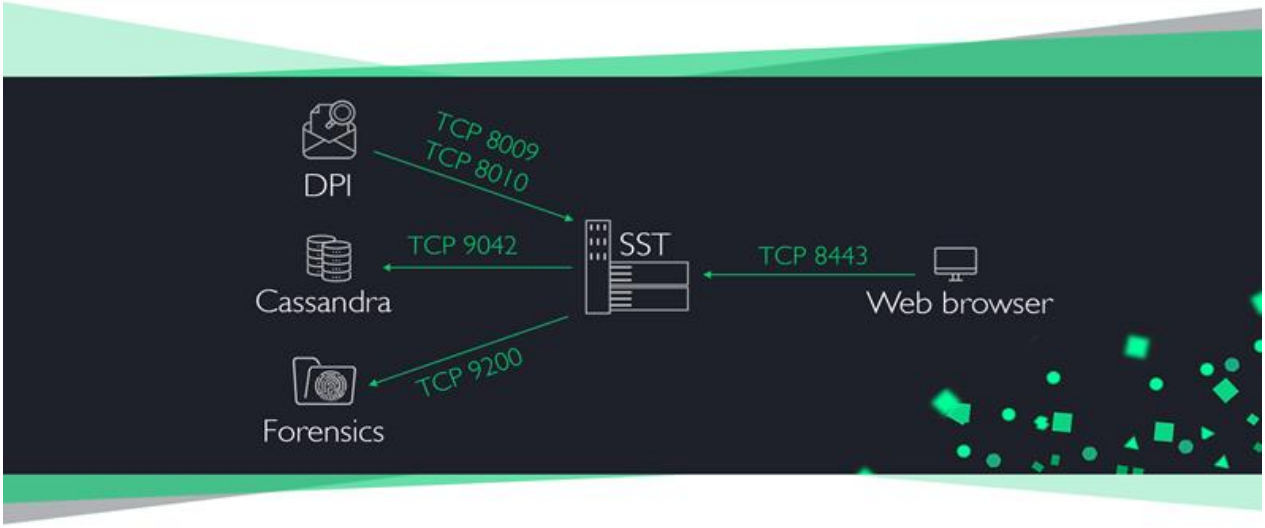
- empow Cassandra server
    - CPU cores 4
    - Memory 4GB
    - Disk Space 500GB
- empow Forensics server
    - CPU cores 4
    - Memory 4GB
    - Disk Space 100GB
- empow (SST) Security Stack
    - CPU cores 4
    - Memory 4GB
    - Disk Space 110GB
- DPI Server
    - CPU cores 4 (6 for full-scale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

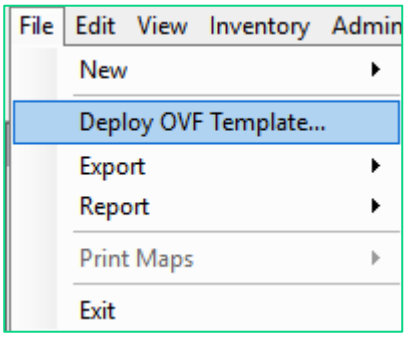
Summary

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

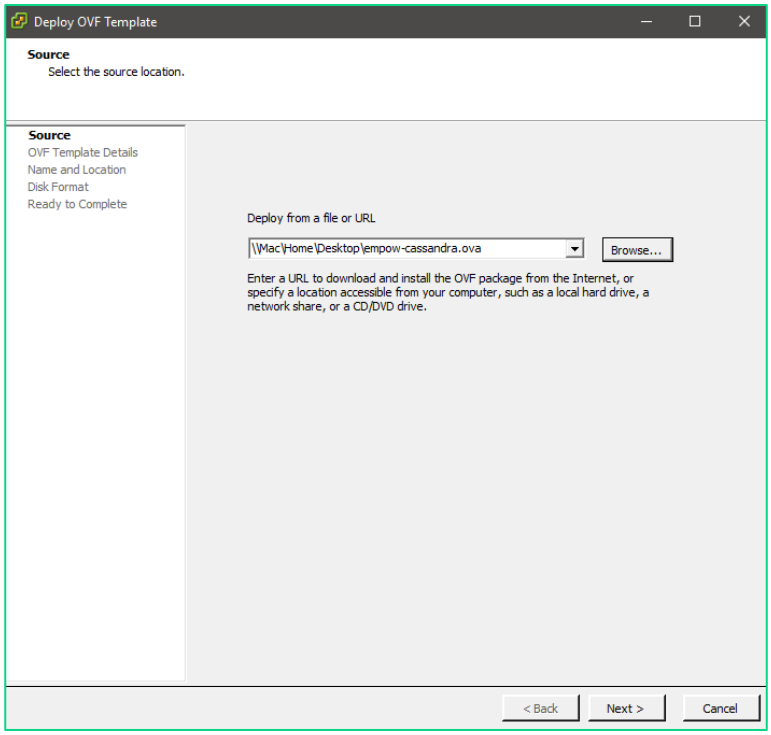
Apache Cassandra server

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

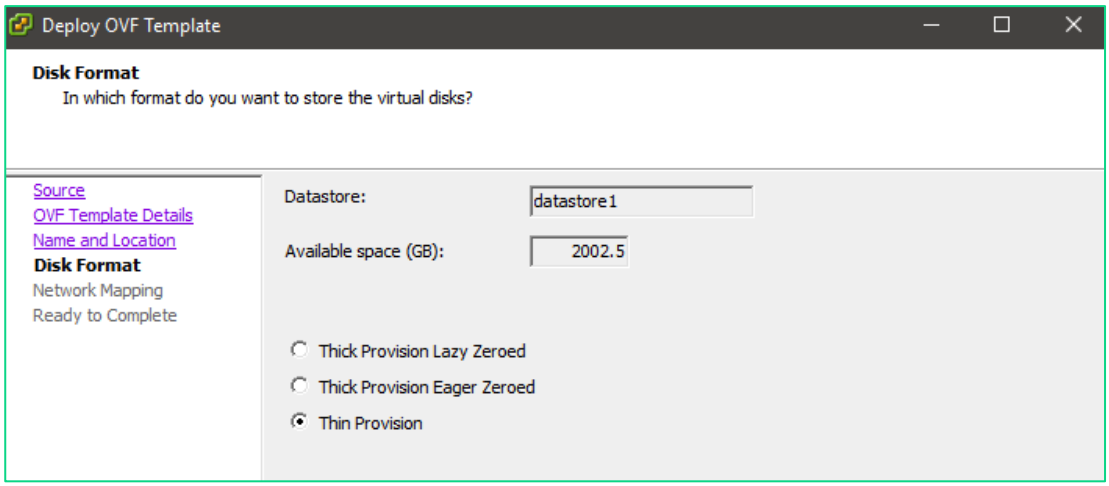
This option pre-allocates space for your disk. It is not subject to fragmentation, since it is pre-allocated, and is easier to track capacity utilization.

- Thick Provision Eager Zeroed

This option also pre-allocates the space, and then zeroes. This takes more time, but increases the net-new write performance of the virtual disk. The benefit of this may be marginal, since you enjoy the benefit only once. It does not improve the speed for subsequent overwrites.

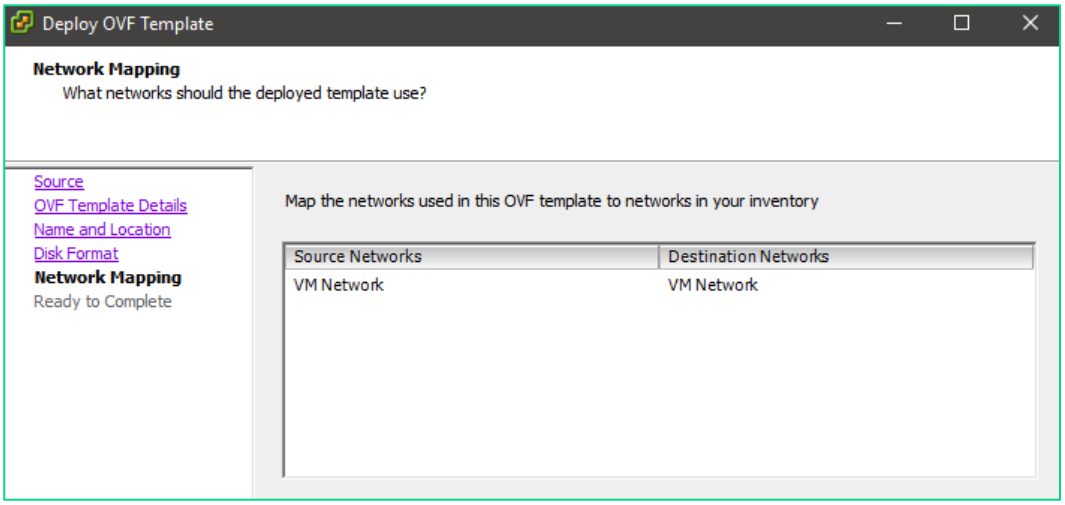
- Thin Provision

This option allocates storage on demand, instead of fixing it at the beginning. This is a good option for controlling costs, and for scaling the storage over time. You need to monitor disk utilization, to avoid overcommitting your storage to more than it can hold. In addition, since allocation is done on the fly, there may be performance hit on initial writes (as the storage allocation is scaled up) that wouldn't be encountered with the thick disk options. This is because newly allocated data blocks have to first be zeroed before being used, to ensure the space is empty.



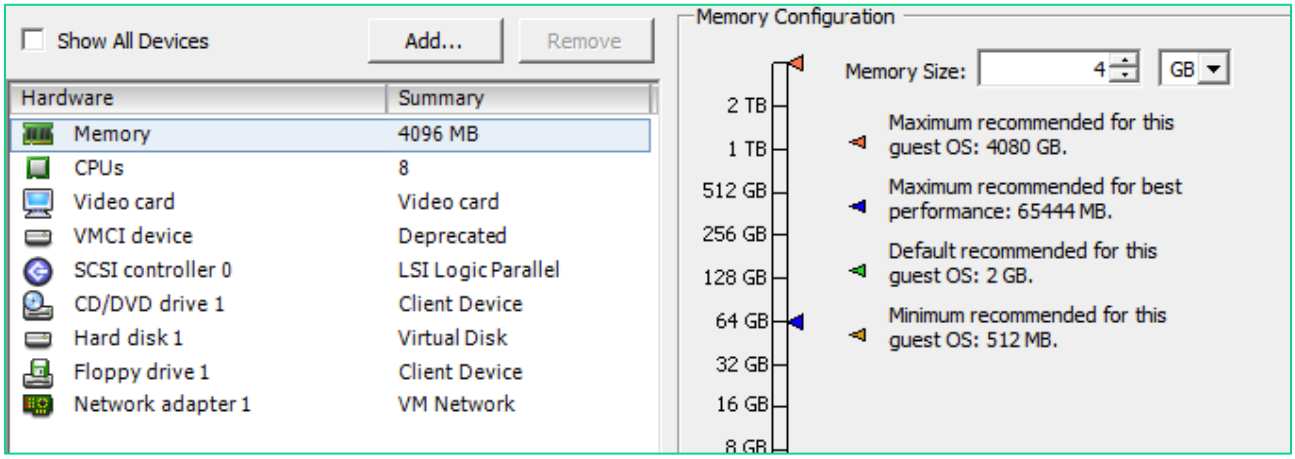
We recommend the *Thick provision Lazy Zeroed* option, for all servers.

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 500GBytes hard disk.



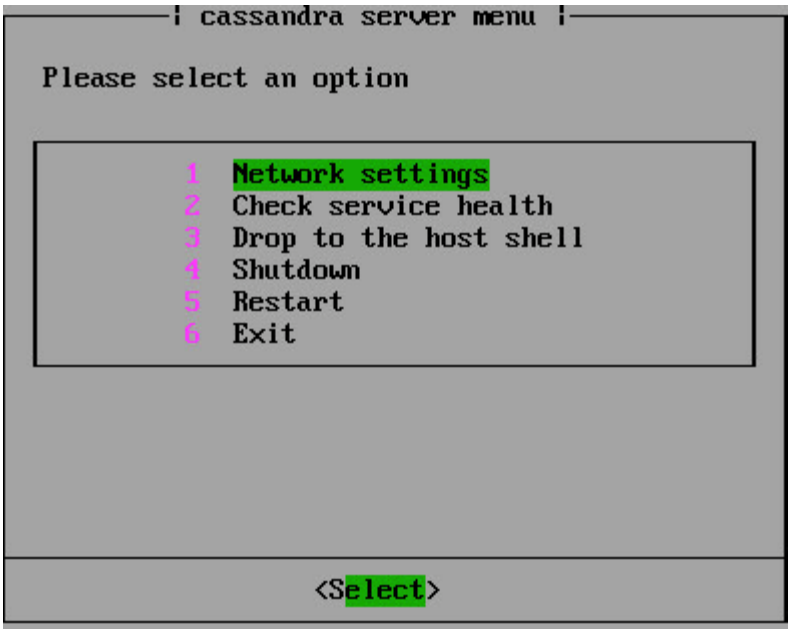
Initial configuration

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

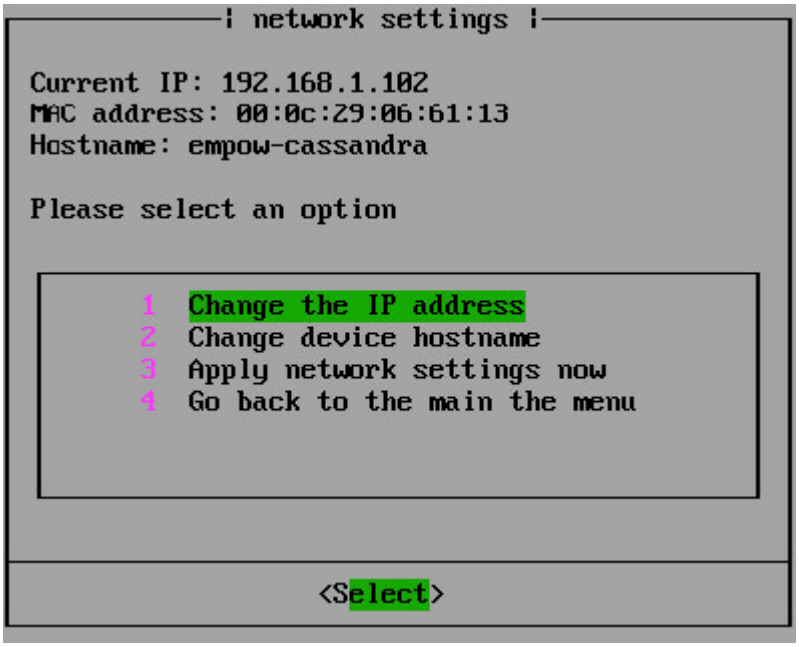
   Use these credentials to log in:

   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.

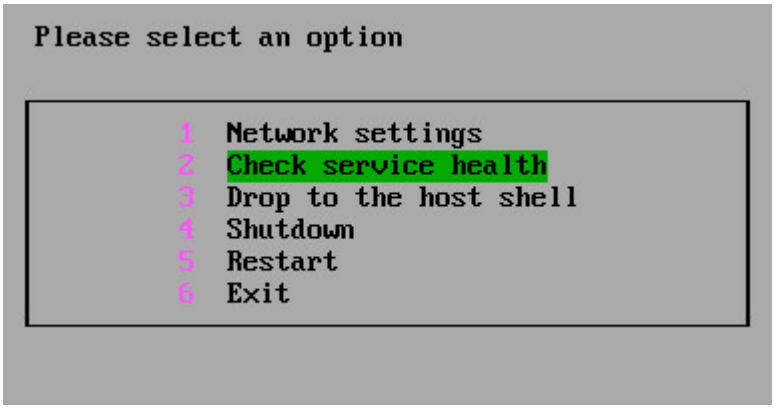
Note: for system stability, it is mandatory to assign a static IP address, or bind the received address on the DHCP server side

Change the hostname to use the following convention – *customer_name-service*

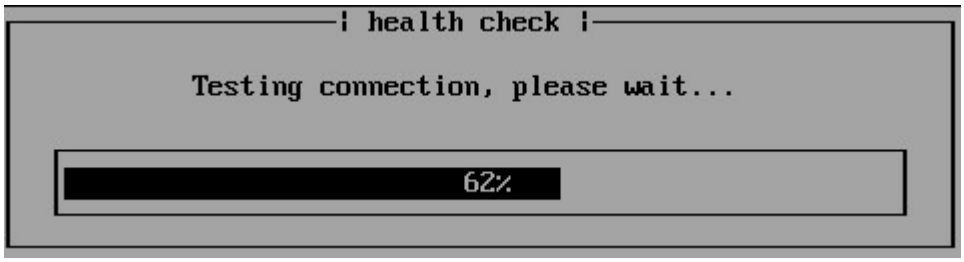
e.g. customer_x-cassandra.

Note: the hostname will change only after the machine is rebooted

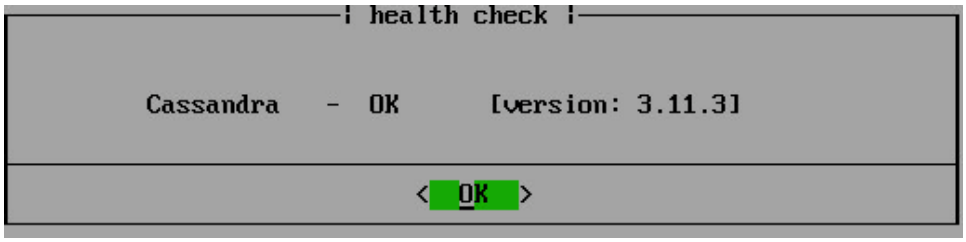
3. In the main menu, select **Check service health** to validate that Cassandra is up and running. If there is a problem, the reason should appear.



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



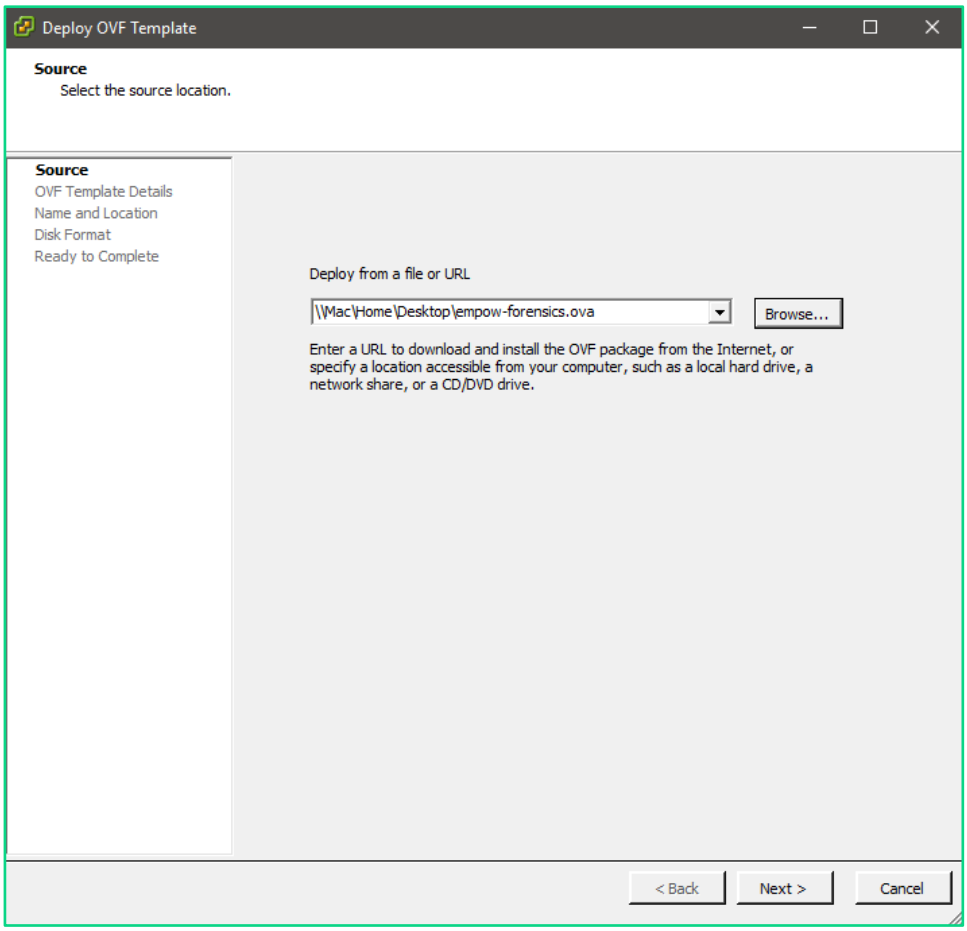
When completed, the result will be shown:



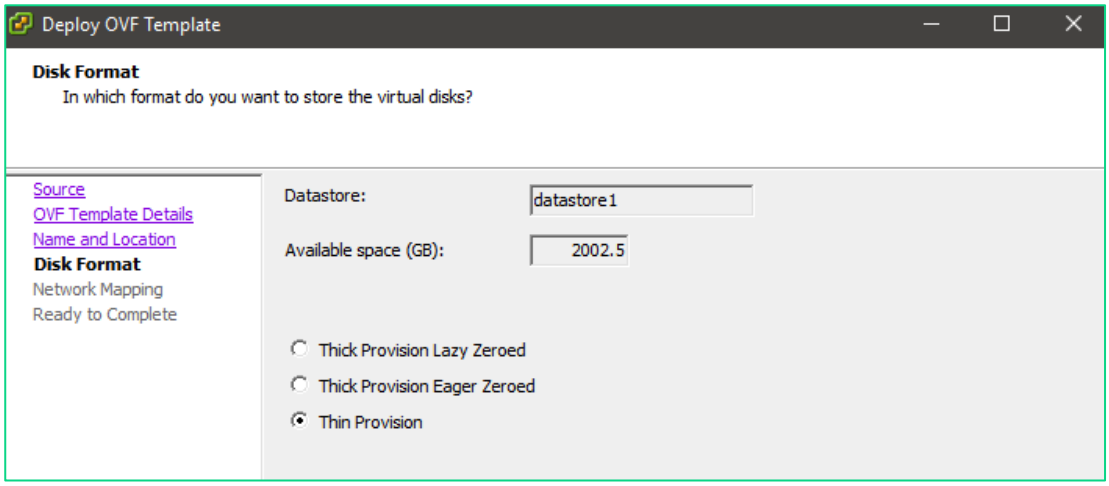
Forensics Server

Deploy the image using the vSphere client

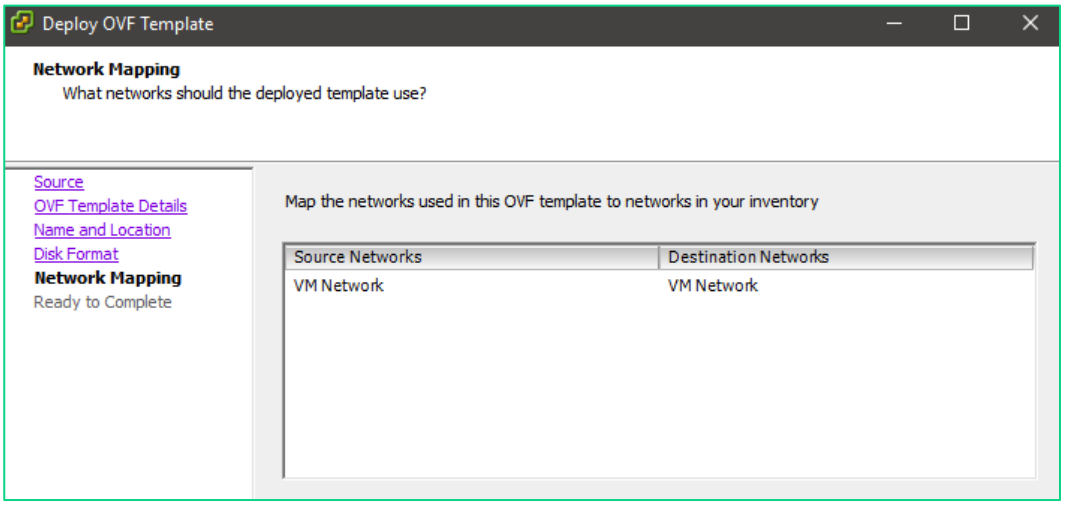
1. In the vSphere client, navigate to **File > Deploy OVF Template...**
2. Enter the empow-forensics.ova file location.



3. Choose a storage provisioning method from the same options as for the Cassandra server (in the previous section). We recommend the *Thick provision Lazy Zeroed* option.

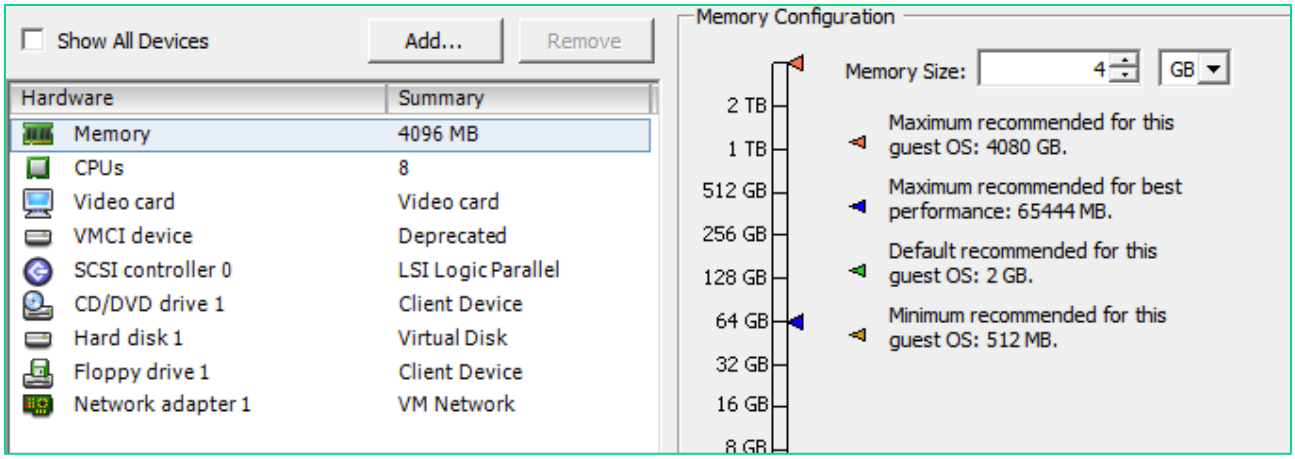


4. Assign the machine to the management network.



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.



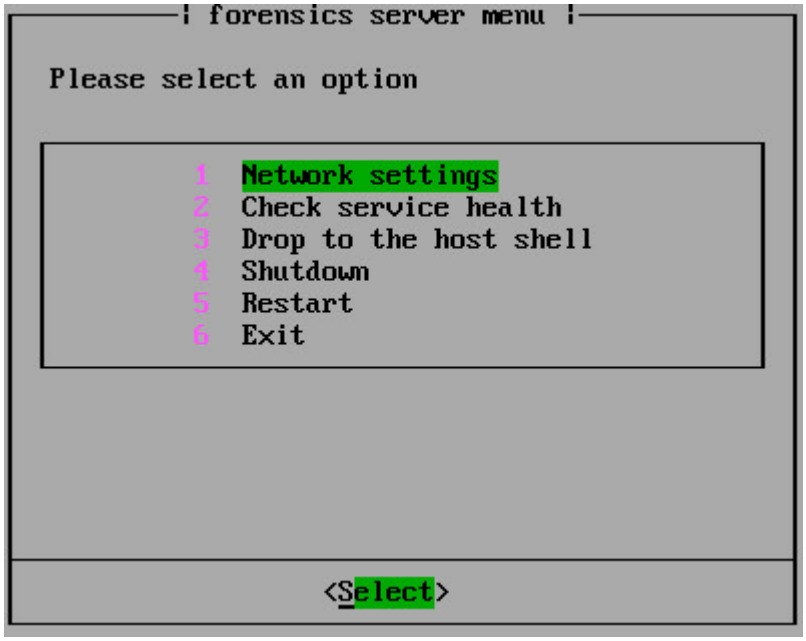
Initial configuration

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

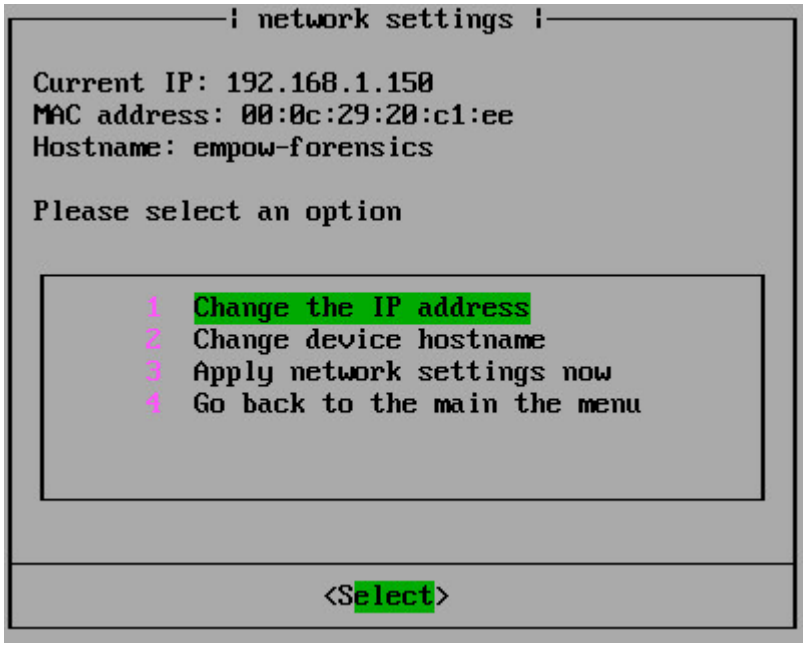
   Use these credentials to log in:

   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.

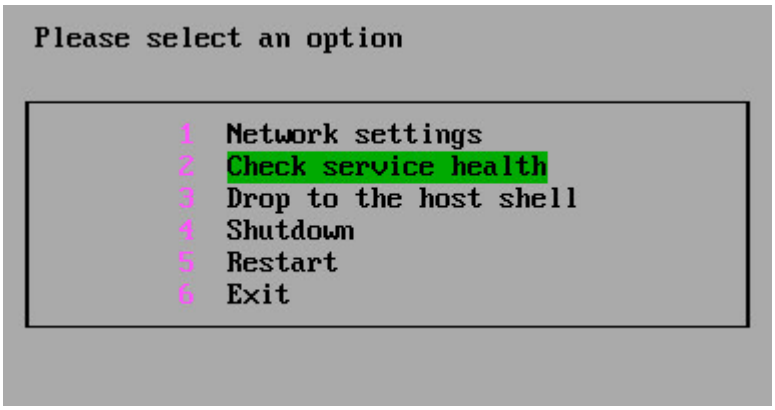
Note: for system stability, it is mandatory to assign a static IP address, or bind the received address on the DHCP server side.

Change the hostname to use the following convention – *customer_name-service*

e.g. customer_x-forensics.

Note: the hostname will change only after the machine is rebooted

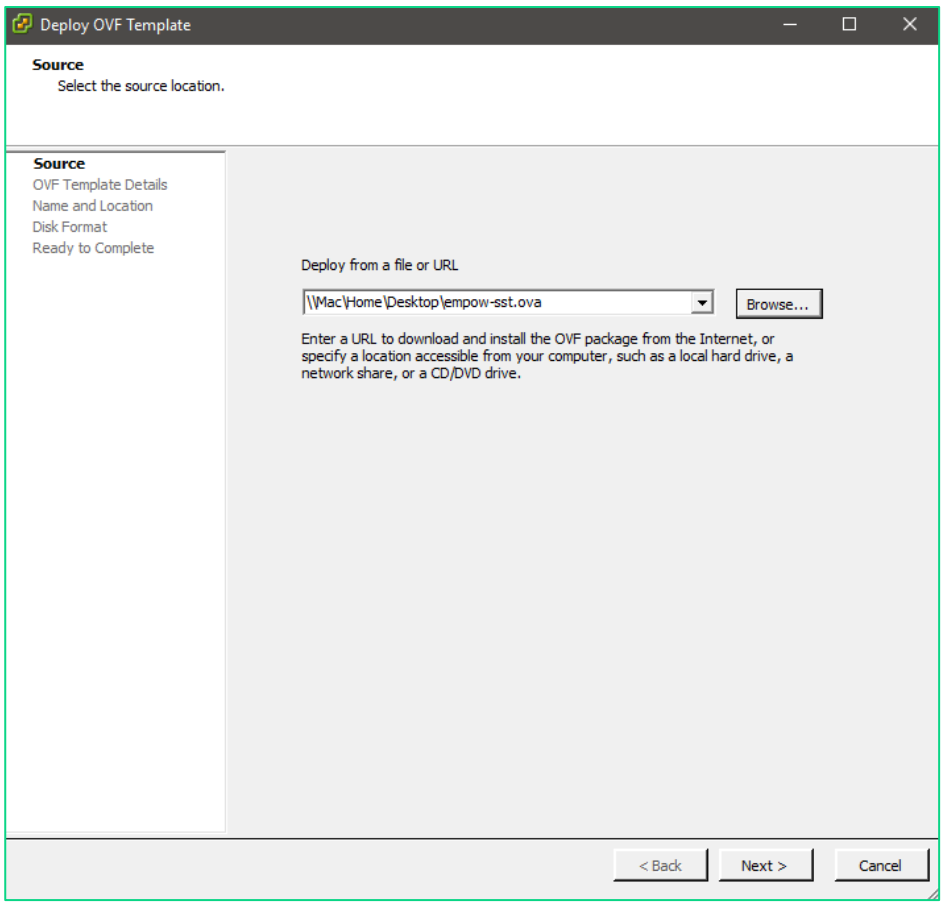
3. In the main menu, select **Check service health** to verify that Elasticsearch is up and running. If there is a problem the reason should appear.



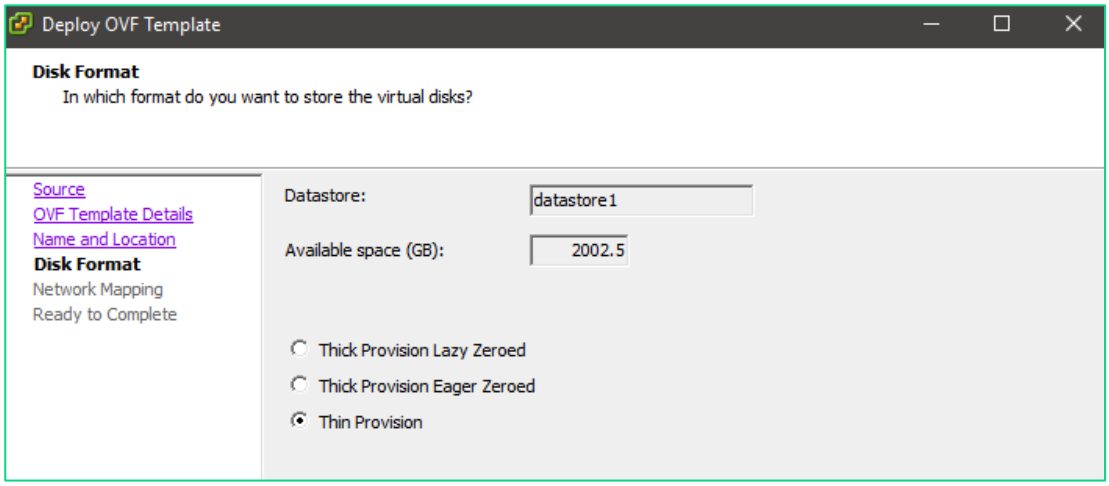
Security Stack (SST) Server

Deploy the image using vSphere client

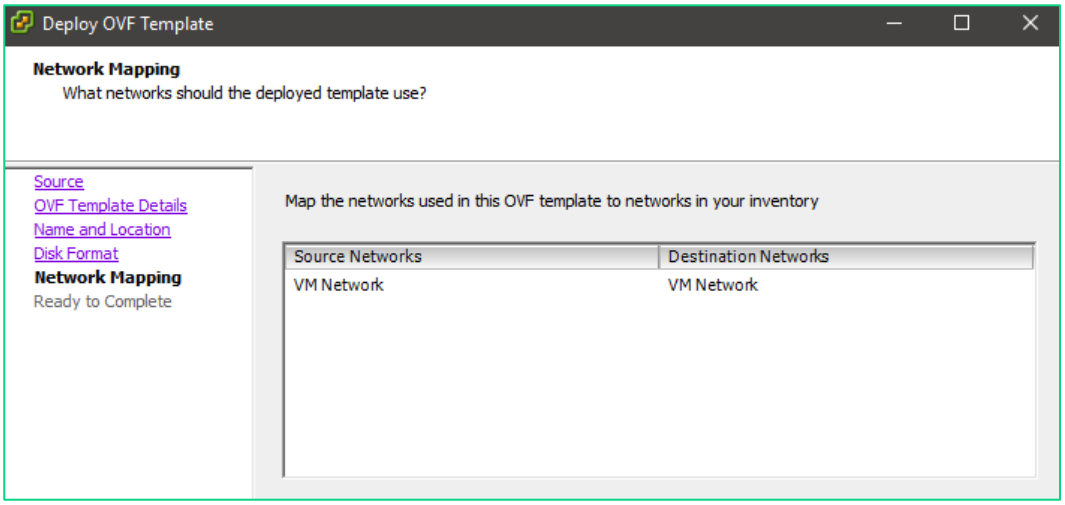
1. In the vSphere client, navigate to **File > Deploy OVF Template...**
2. Enter the empow-sst.ova file location.



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

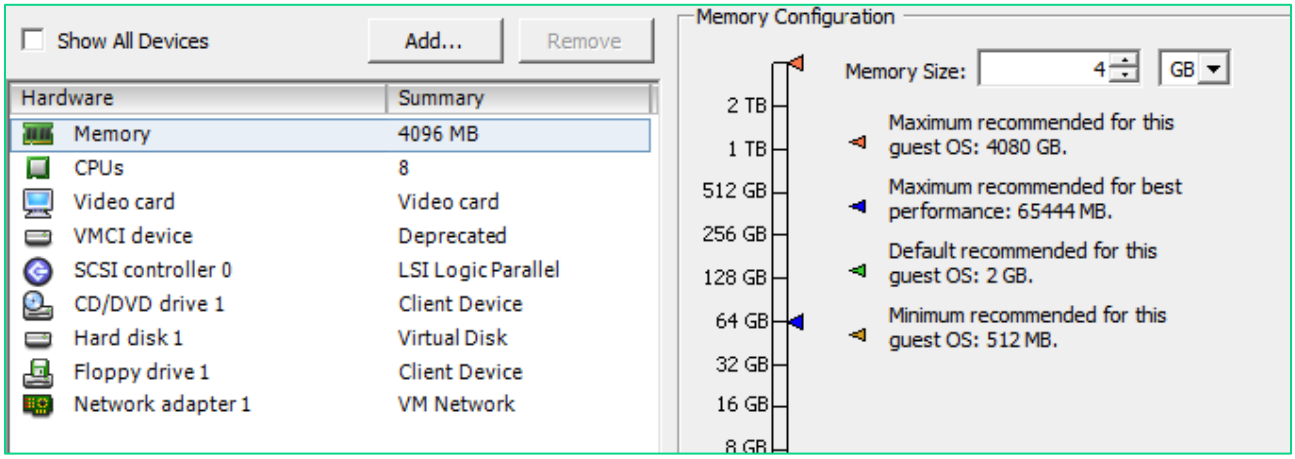


4. Assign the machine to the management network.



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.



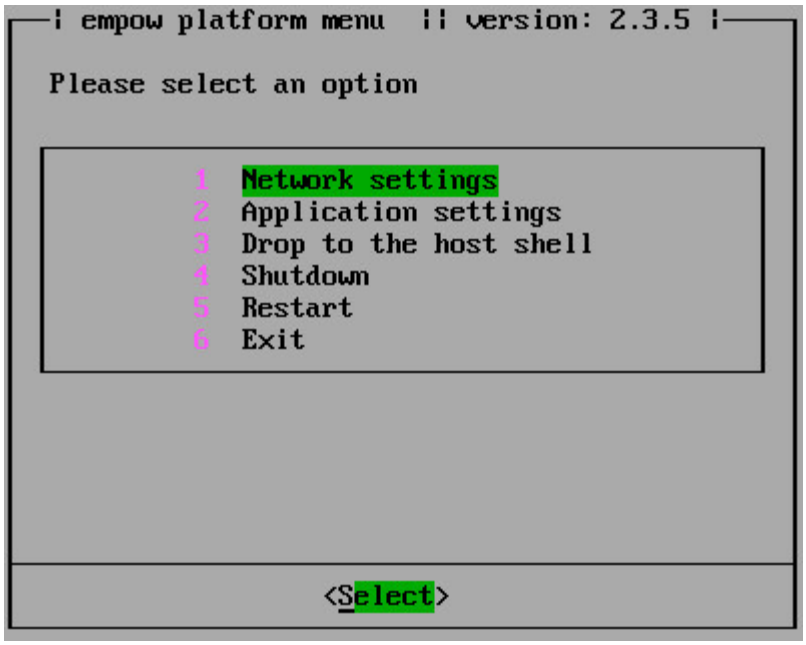
Initial configuration

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

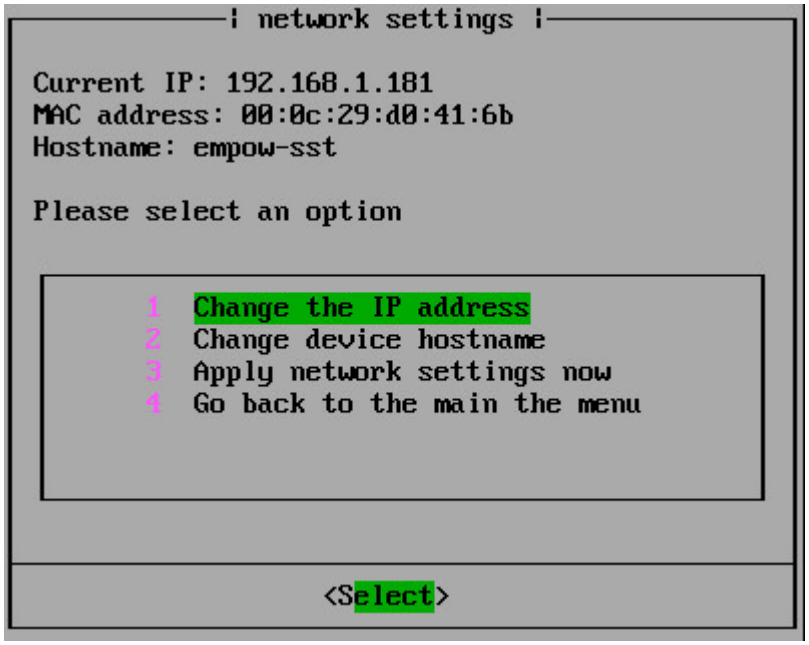
   Use these credentials to log in:

   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.

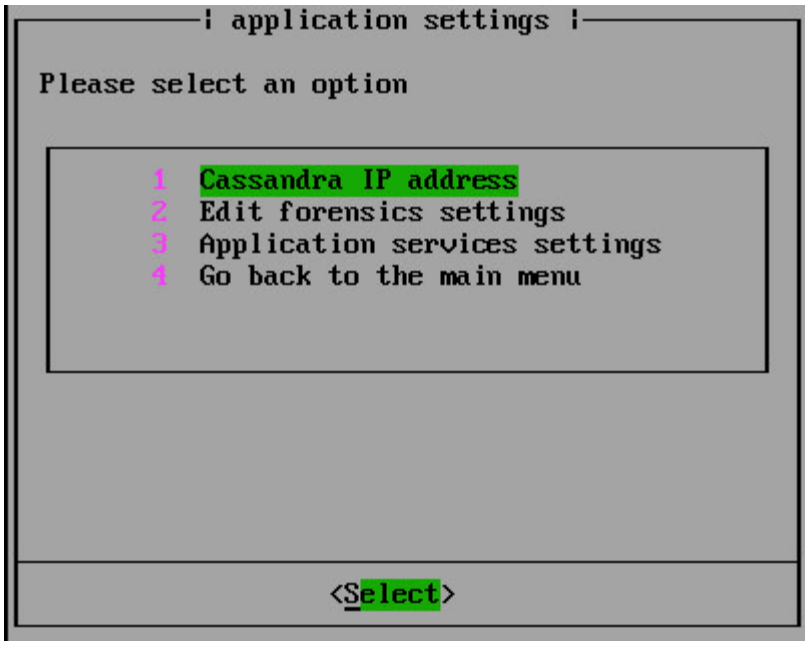
Note: for system stability, it is mandatory to assign a static IP address, or bind the received address on the DHCP server side.

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.

Return to the main menu and select application settings to configure mandatory settings begore starting the application.



3. Configure Cassandra IP address

   Enter the IP address assigned to the Cassandra server.

4. Edit forensics settings

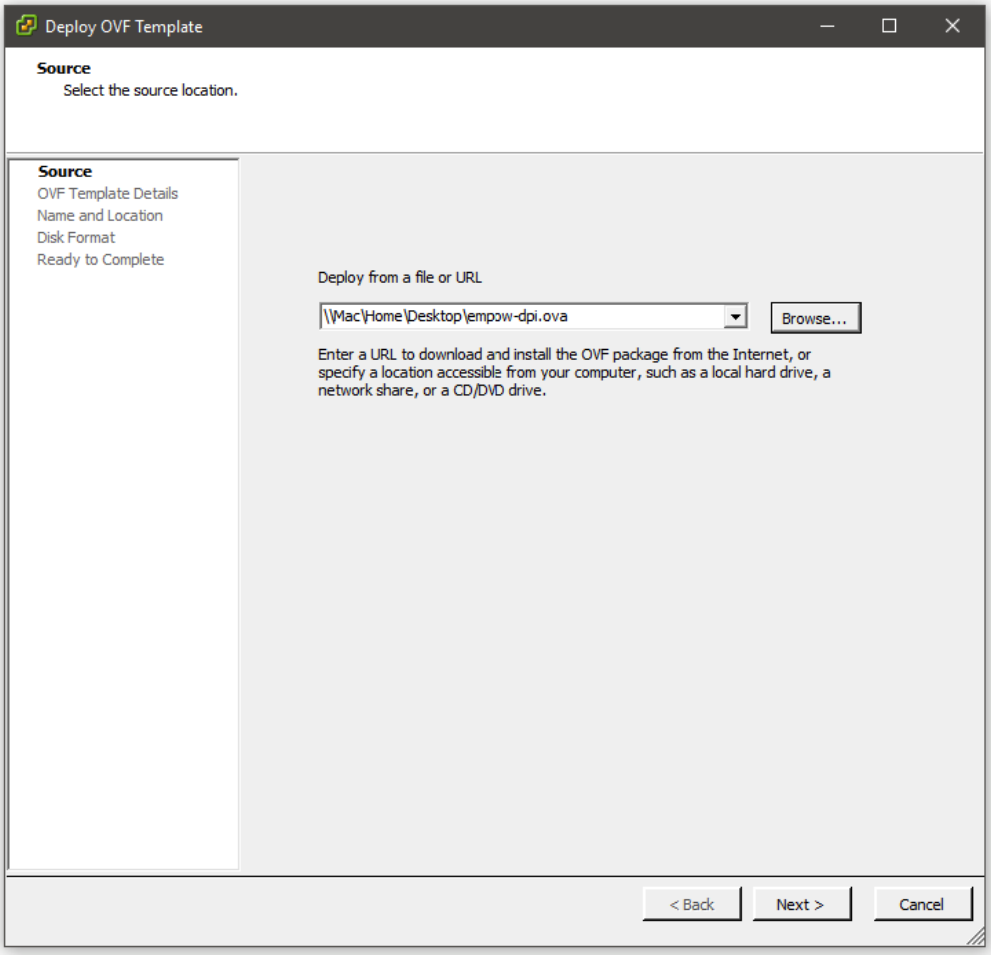
   Change the status of the Forensics service and enter the IP address.

Note: set the service to OFF if the Forensics service is not being used.

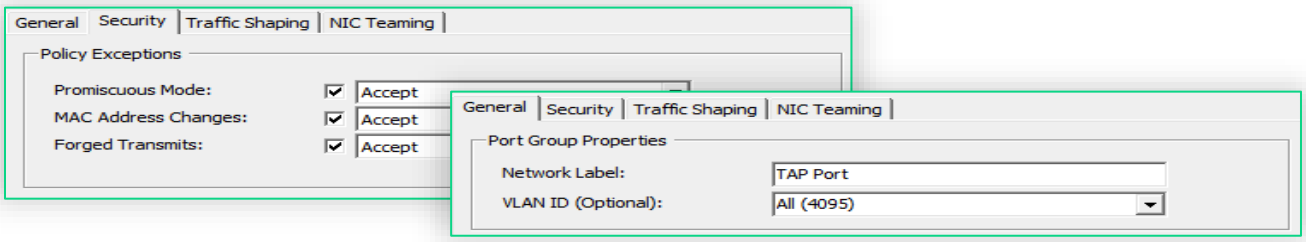
DPI Server

Deploy the server using the vSphere client

1. In the vSphere client, navigate to **File > Deploy OVF Template**…
2. Enter the empow-dpi-universal.ova file location.



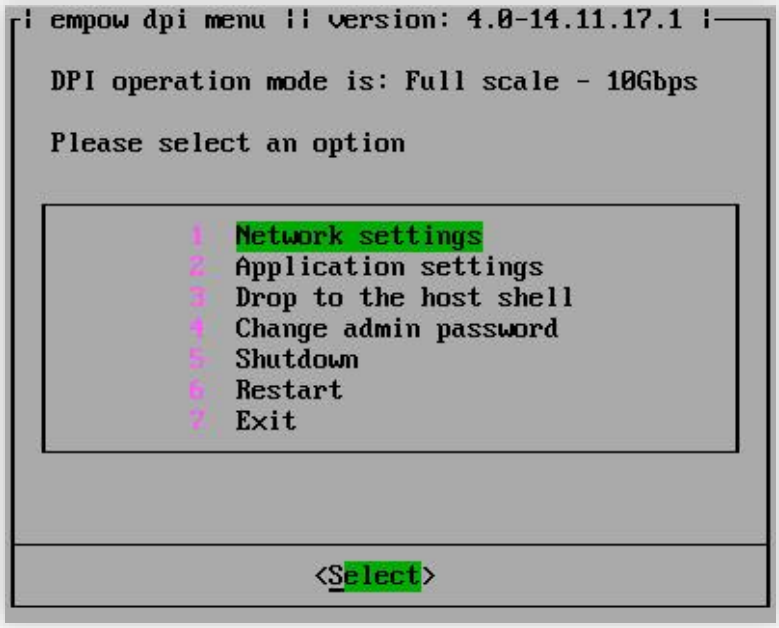
3. Choose a storage provisioning method, as for the Cassandra and SST servers.
4. Configure the VMware vSwitch to allow all VLAN IDs, and to enable promiscuous mode, in order to deliver all the mirrored traffic it receives to the empow DPI server.



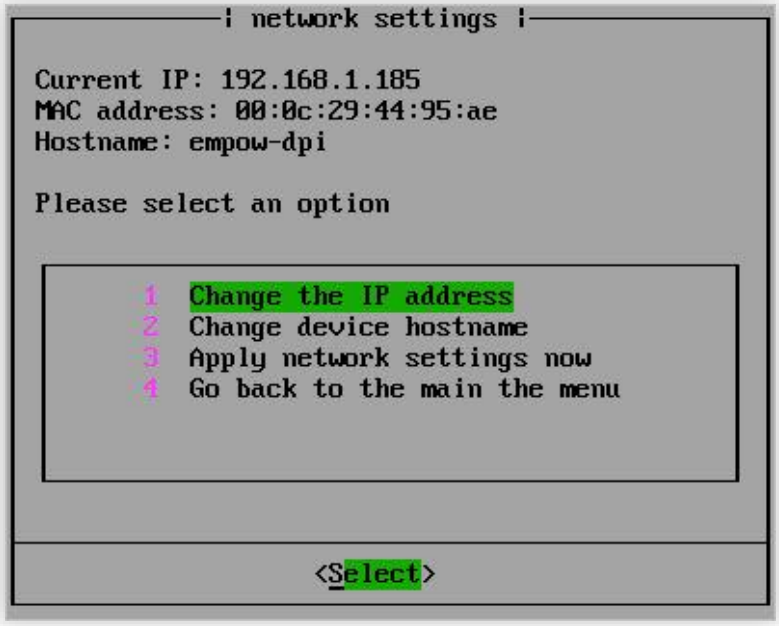
Initial configuration

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

   Use these credentials to log in:
   Username: admin
   Password: empow



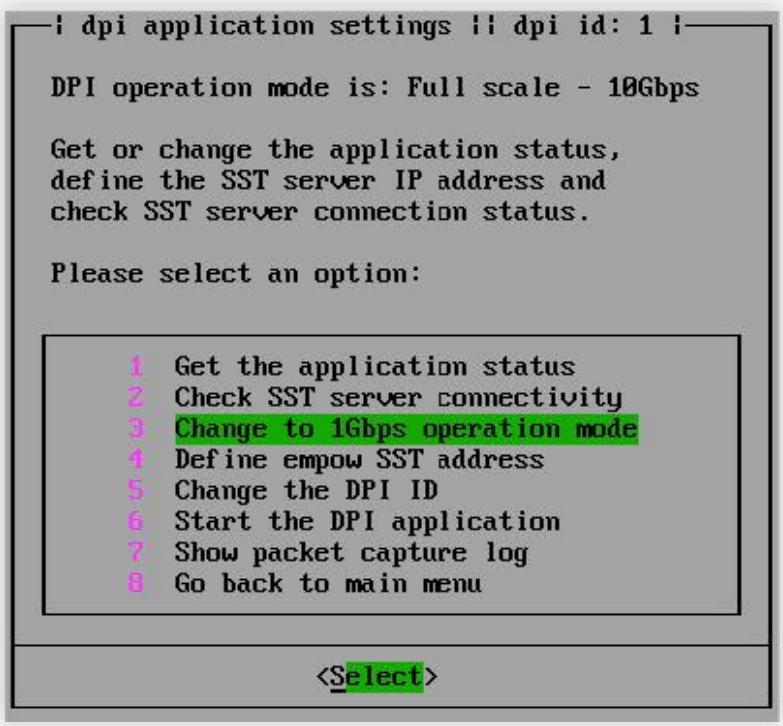
2. Enter the network settings to configure the IP address and assign a hostname.



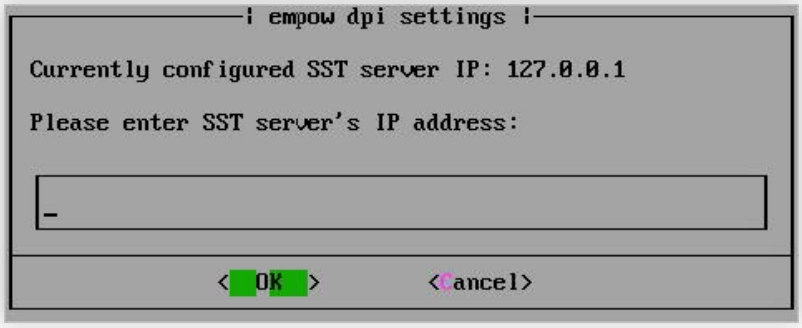
Application configuration

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.

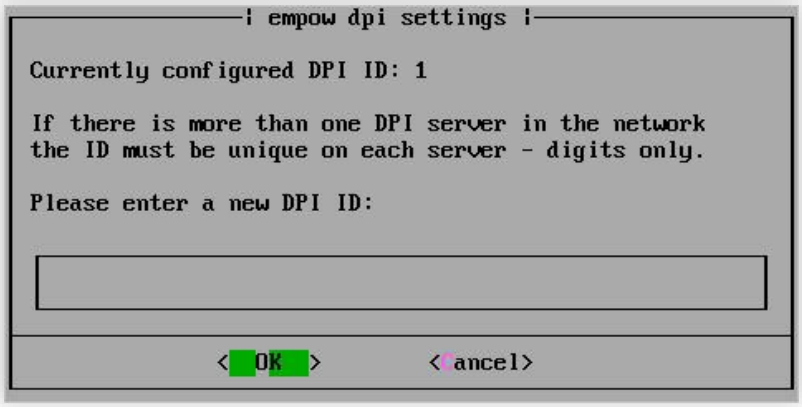


2. In the application menu, select option 4 (“Define empow SST address”) to set the empow Security Stack server IP address.

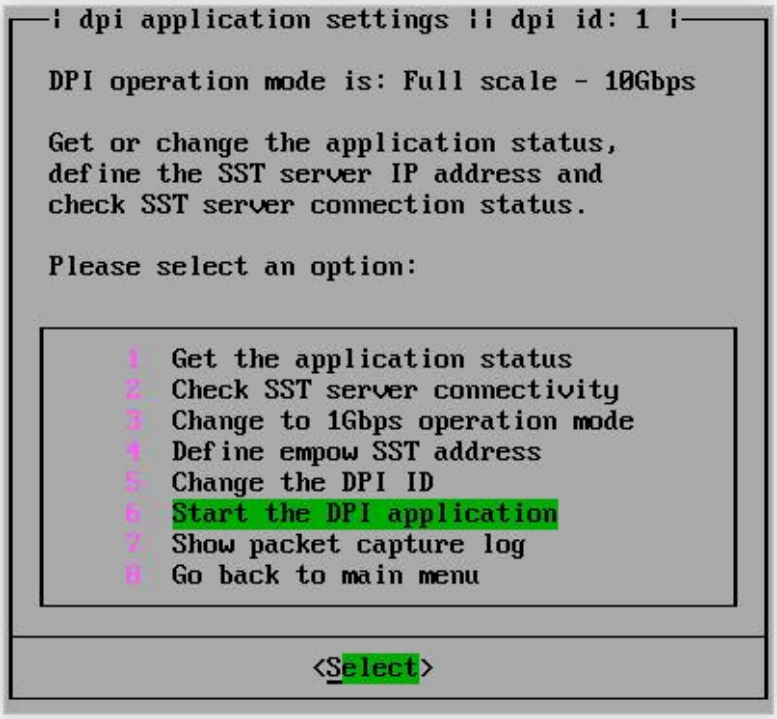


3. If another empow DPI is already deployed, the DPI ID for this server must also be changed. Select option 5 (“Change the DPI ID”) to set a new DPI ID. The default value is 1.

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



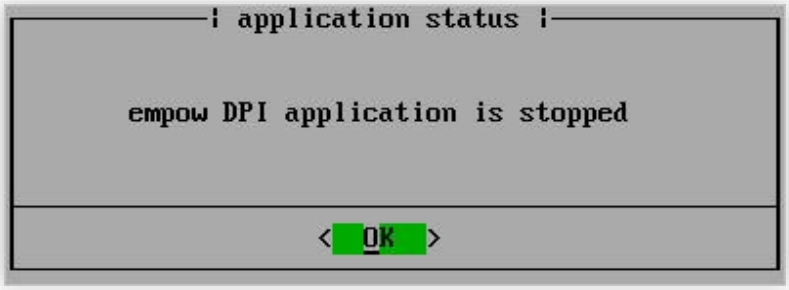
4. Select option 6 (“Start the DPI application”) to start the server.



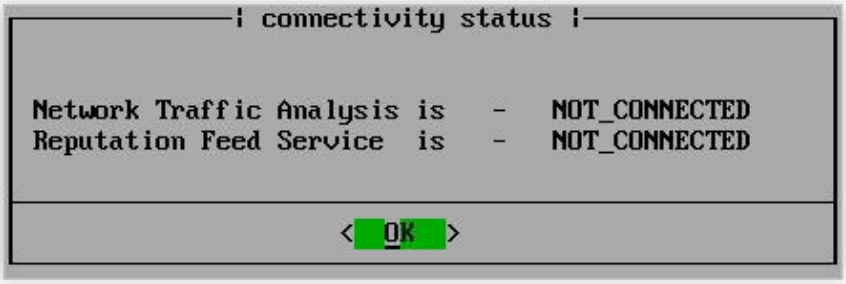
Validation

Check the 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.



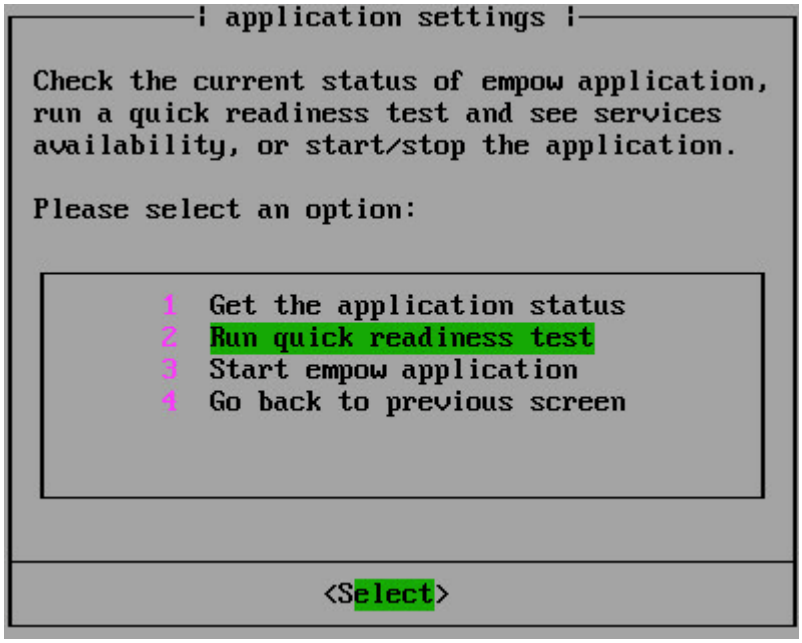
Note: the status will show CONNECTED or NOT_CONNECTED based on the current real time status.

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.

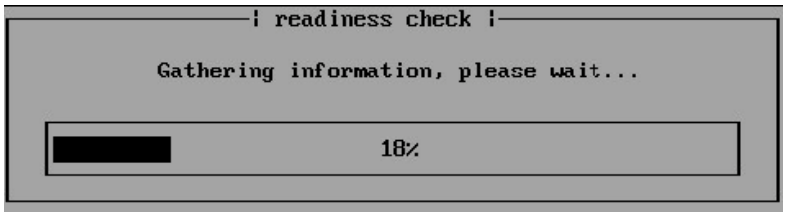
Note: this option can be used for troubleshooting, or to validate that the mirrored traffic arrives at the capturing port.

Start the application

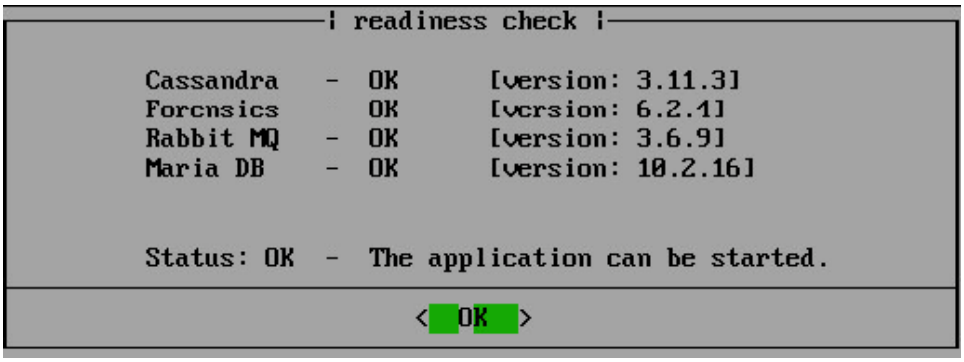
1. Select application services settings to perform quick sanity test and start the empow application.



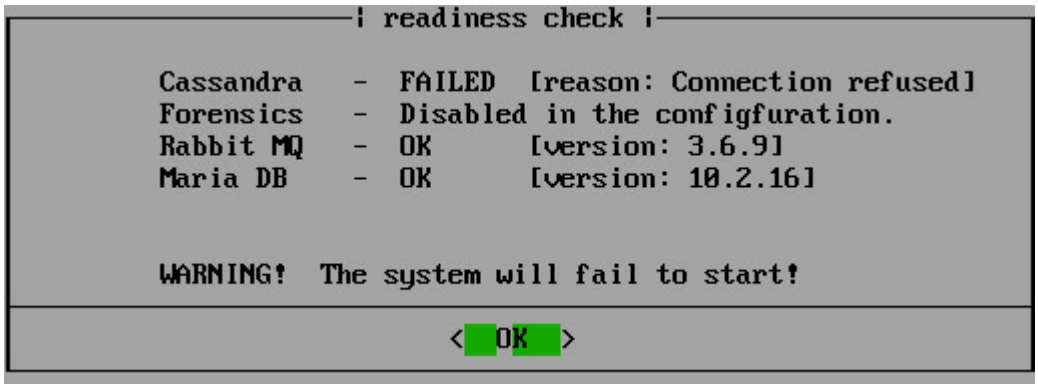
2. Choose the run quick readiness test option to get the sanity test results.



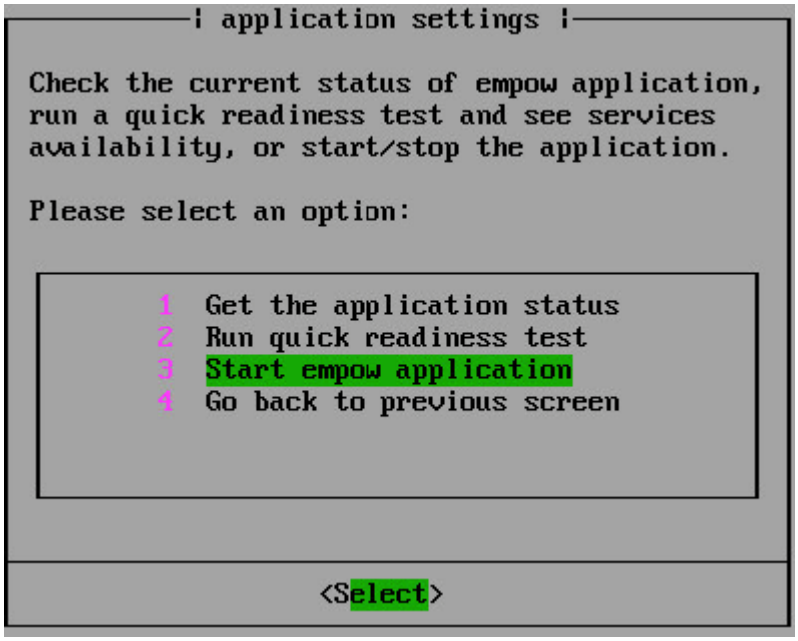
This will be displayed for a successful result:



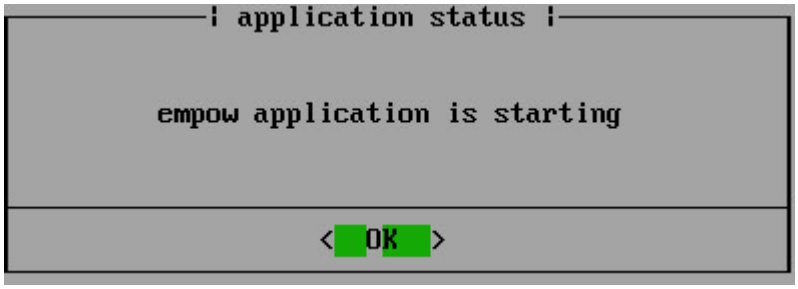
This will be displayed if the readiness test fails:



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



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



Note: press OK, and select option 1 ("Get the application status") every few seconds, to manually refresh the screen, as it does not refresh itself.

When the application status switches to available, open the web management interface at *https://EMPOW_SST_IP_ADDRESS:8443*

Use these credentials to log in:

Username: admin

Password: empow