C:\Users\serge\AppData\Local\Microsoft\Windows\INetCache\Content.Word\VERTICAL_BORDER.JPG

empow Platform

quick setup guide



Table of Contents

[Introduction 3](#_Toc526328620)

[Overview of the empow platform 3](#_Toc526328621)

[System Components 3](#_Toc526328622)

[System Requirements 3](#_Toc526328623)

[Connectivity Map 5](#_Toc526328624)

[Installation procedure 6](#_Toc526328625)

[Summary 6](#_Toc526328626)

[Apache Cassandra server 6](#_Toc526328627)

[Forensics Server 12](#_Toc526328628)

[Security Stack (SST) Server 16](#_Toc526328629)

[DPI Server 19](#_Toc526328630)

[Start the application 20](#_Toc526328631)

[Success example 21](#_Toc526328632)

[Failure example 21](#_Toc526328633)

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 three 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

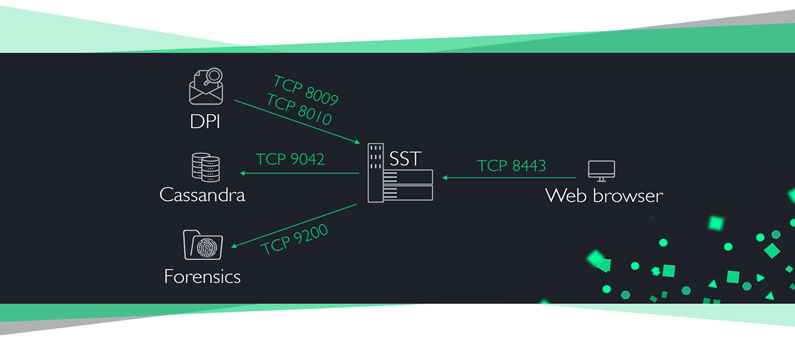
Virtualization platform

* + 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 |
| 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

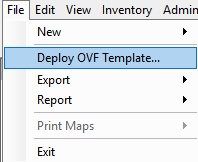
Summary

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

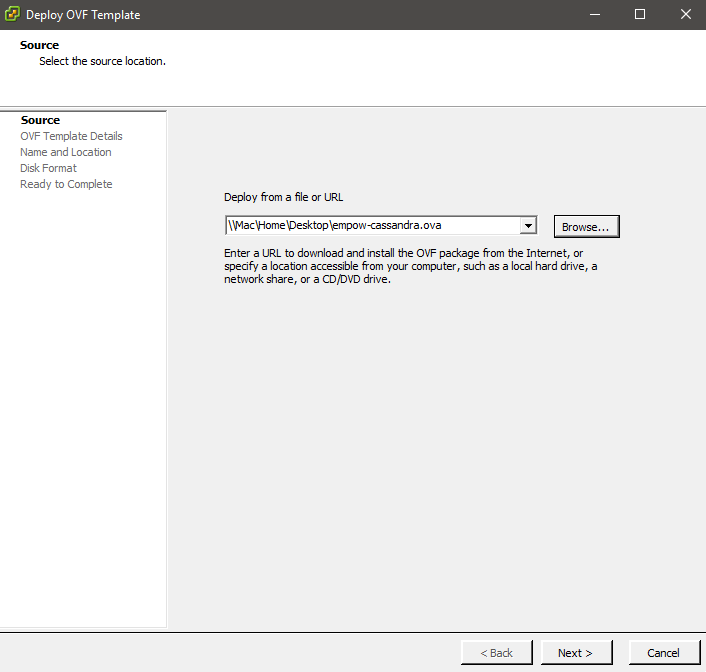
Apache Cassandra server

Deploy the image using the vSphere client

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



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



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

* Thick Provision Lazy Zeroed

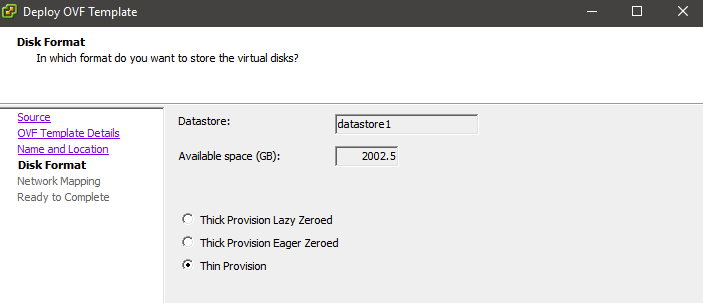
If you want to pre-allocate the space for your disk, one option is to make a thick lazy zeroed disk. It won’t be subject to fragmentation since it pre-allocates all the space so no other files will get in the middle (which causes fragmentation), and it’s easier to track capacity utilization.

* Thick Provision Eager Zeroed

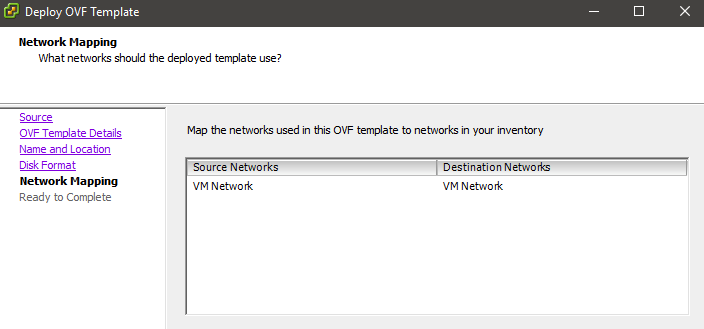
When provisioning a thick eager zeroed disk, VMware pre-allocates the space and then zeroes it all out ahead of time. In other words, this takes a while — just to increase the net-new write performance of your virtual disk. We don’t frequently see the benefit in this since you only enjoy this perk only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

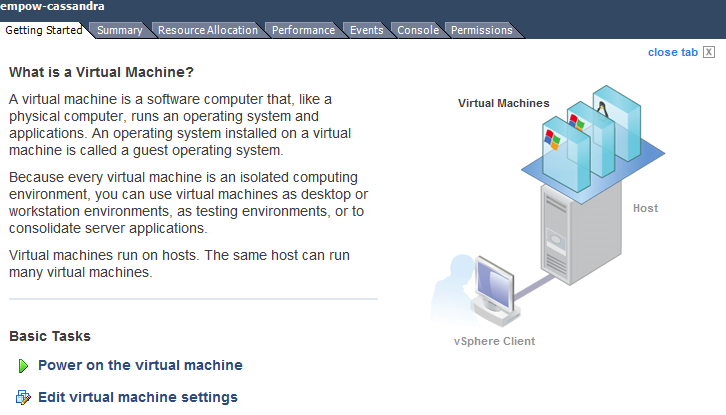


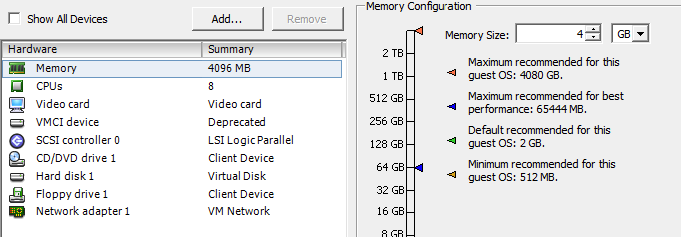
1. Assign the machine to the management network.



1. 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.





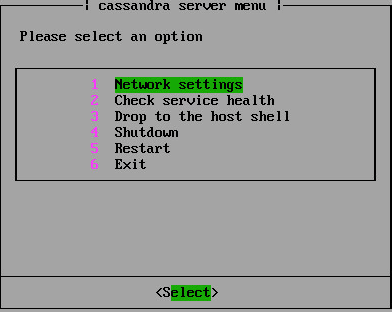
Initial configuration

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

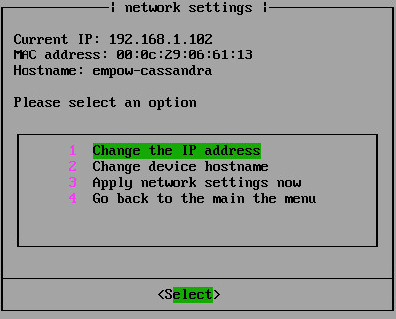
Use the following credentials to log in:

Username: admin

Password: empow



1. 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.

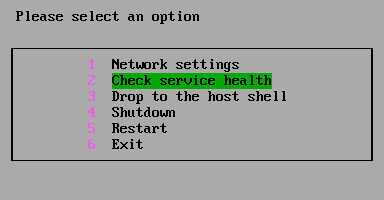
*Note: for system stability, it is mandatory to assign a static IP address or bind the received address on the DHCP server side*

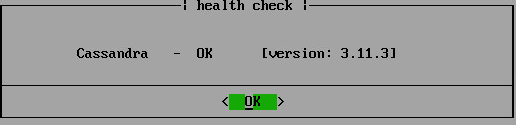
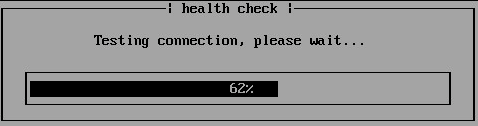
Change the hostname to use the following convention – *customer\_name-service*

e.g. customer\_x-cassandra.

Note: the hostname will change only after rebooting the machine

1. 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.

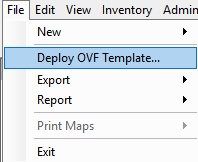




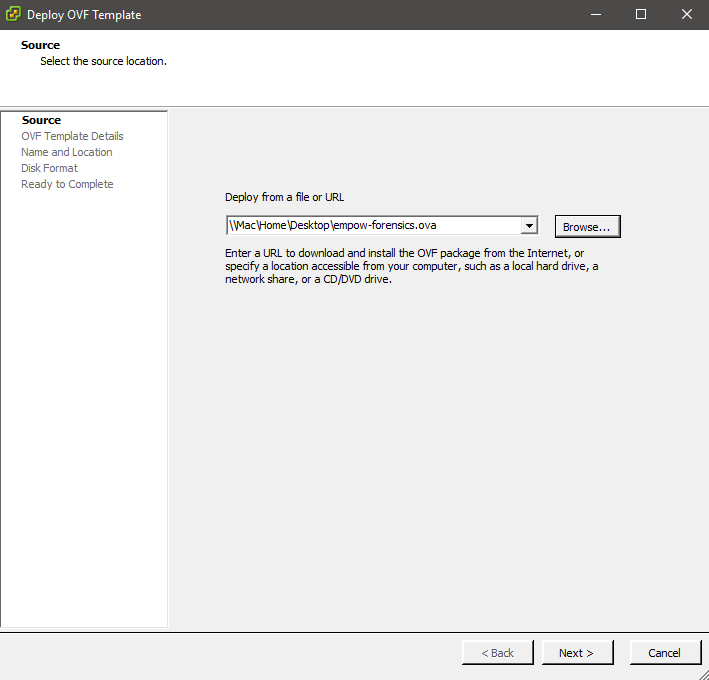
Forensics Server

Deploy the image using vSphere client

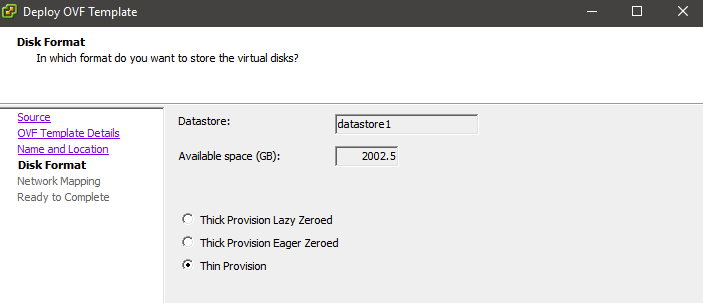
1. In the vSphere client, navigate to **File > Deploy OVF template…**



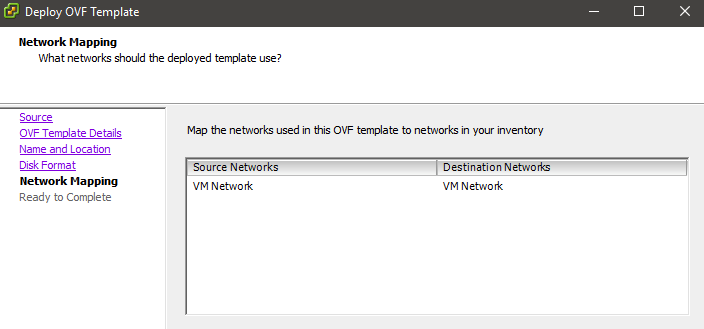
1. Enter the empow-forensics.ova file location.



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

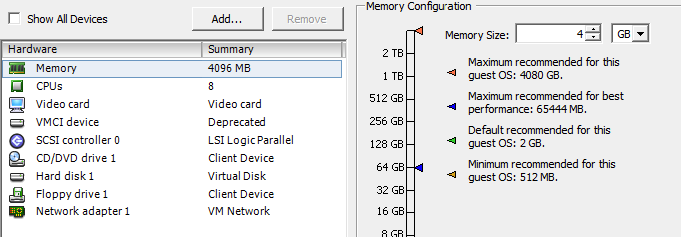


1. Assign the machine to the management network.



1. 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.



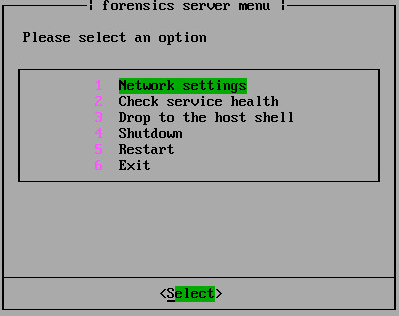
Initial configuration

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

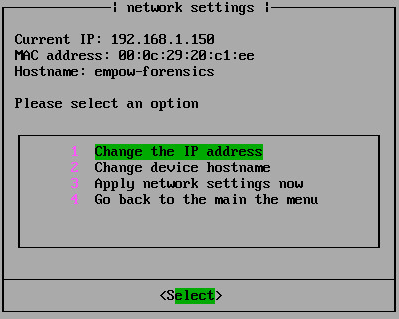
Use the following credentials to log in:

Username: admin

Password: empow



1. 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.

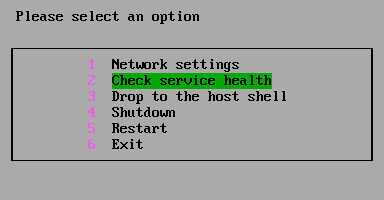
Note: for system stability, it is mandatory to assign a static IP address or bind the received address on the DHCP server side.

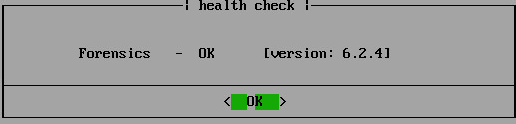
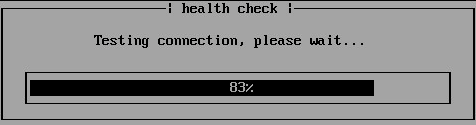
Change the hostname to use the following convention – *customer\_name-service*

e.g. customer\_x-forensics.

Note: the hostname will change only after rebooting the machine

1. 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.

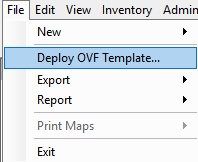




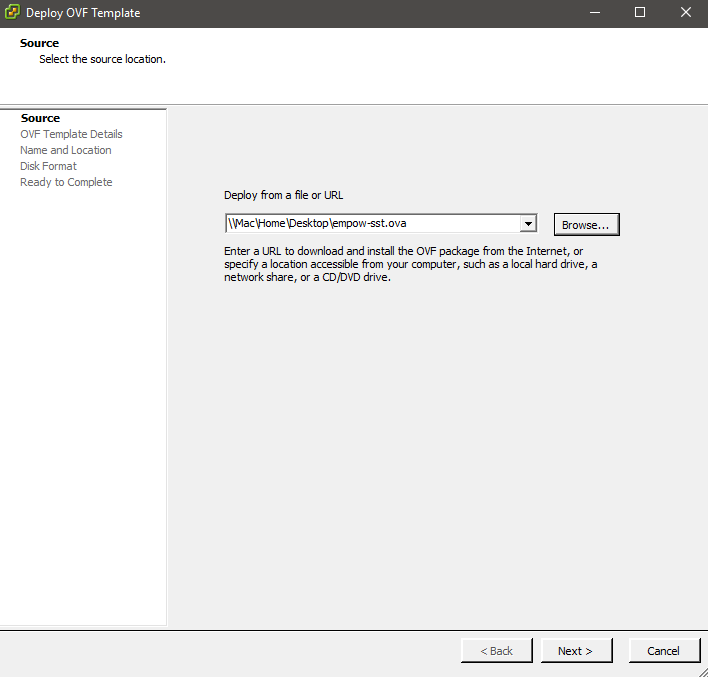
Security Stack (SST) Server

Deploy the image using vSphere client

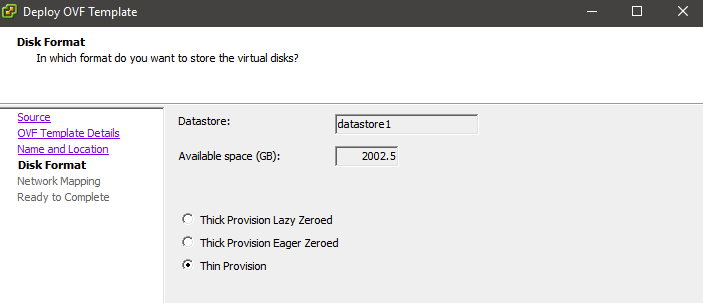
1. In the vSphere client, navigate to **File > Deploy OVF template…**



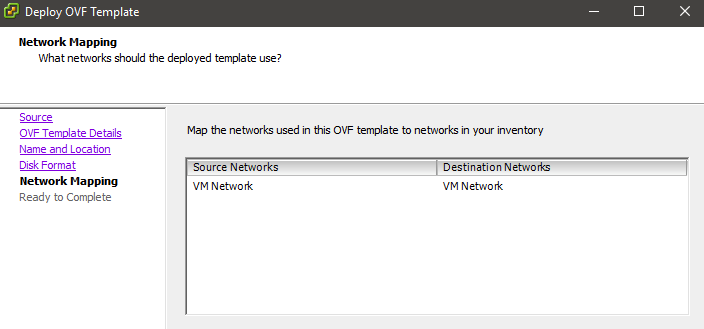
1. Enter the empow-sst.ova file location.



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

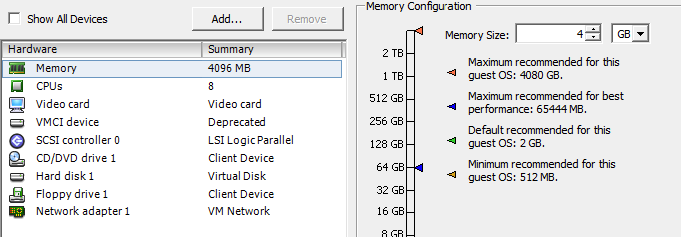


1. Assign the machine to the management network.



1. 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.



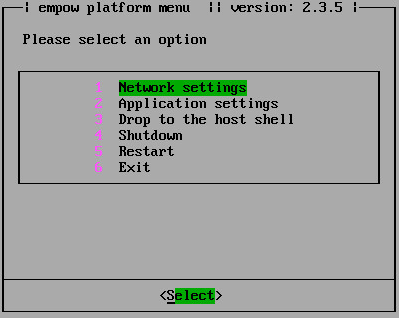
Initial configuration

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

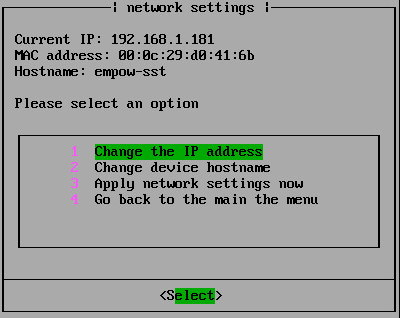
Use the following credentials to log in:

Username: admin

Password: empow



1. 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.

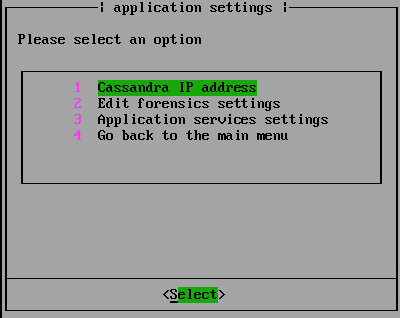
Note: for system stability, it is mandatory to assign a static IP address or bind the received address on the DHCP server side.

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.



1. Configure Cassandra IP address

Enter the IP address assigned to the Cassandra server.

1. Edit forensics settings

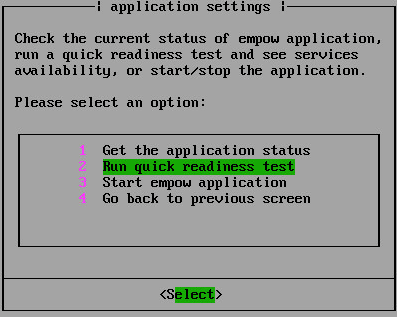
Change the status of the Forensics service and enter the IP address.

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

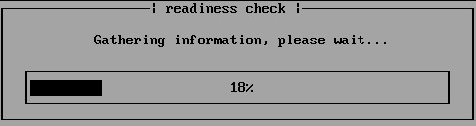
DPI Server

Start the application

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



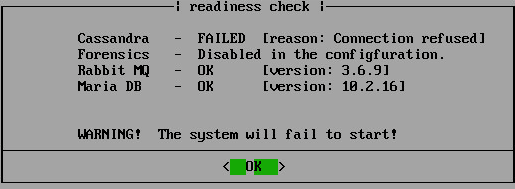
1. Choose the run quick readiness test option to get the sanity test results.



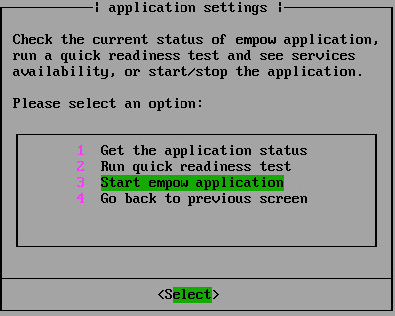
Success example



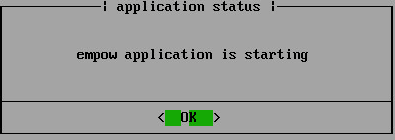
Failure example



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



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



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*

Use the following credentials to log in:

Username: admin

Password: empow

