Operational Technology Defense Console – Virtual Appliance 1.2

Quick Setup Guide

(for VMware ESXi and Workstation)

2020-10-08

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/en-us/home.aspx

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Table of Contents

ODC Onboarding to VMware ESXi

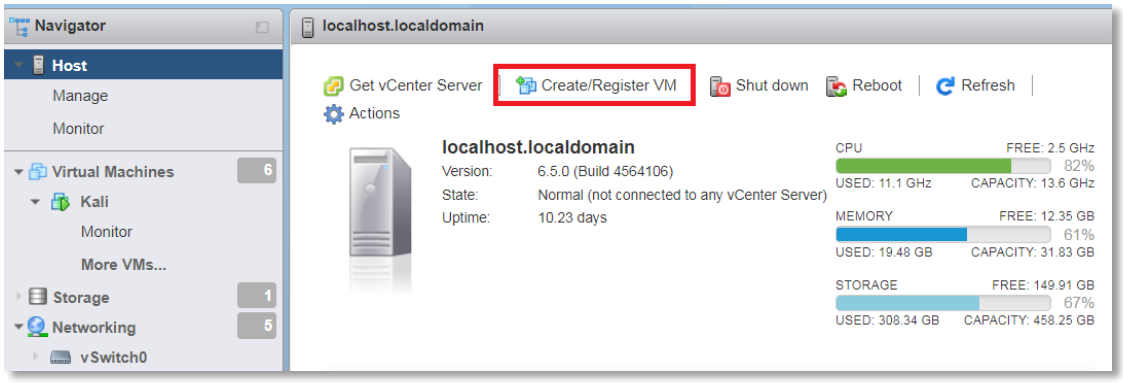
This chapter describes how to deploy OT Defense Console to a VMware ESXi system.

Prerequisites

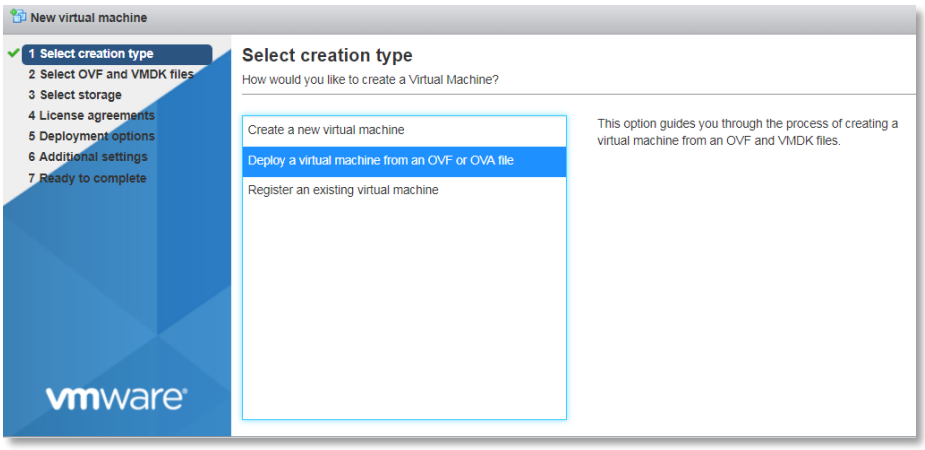
- The OVA packages provided by Trend Micro must be available and accessible to VMware ESXi.
- ESXi version 6 or above with the required specifications.
- The necessary networks have been properly created in ESXi.

Deploying OT Defense Console

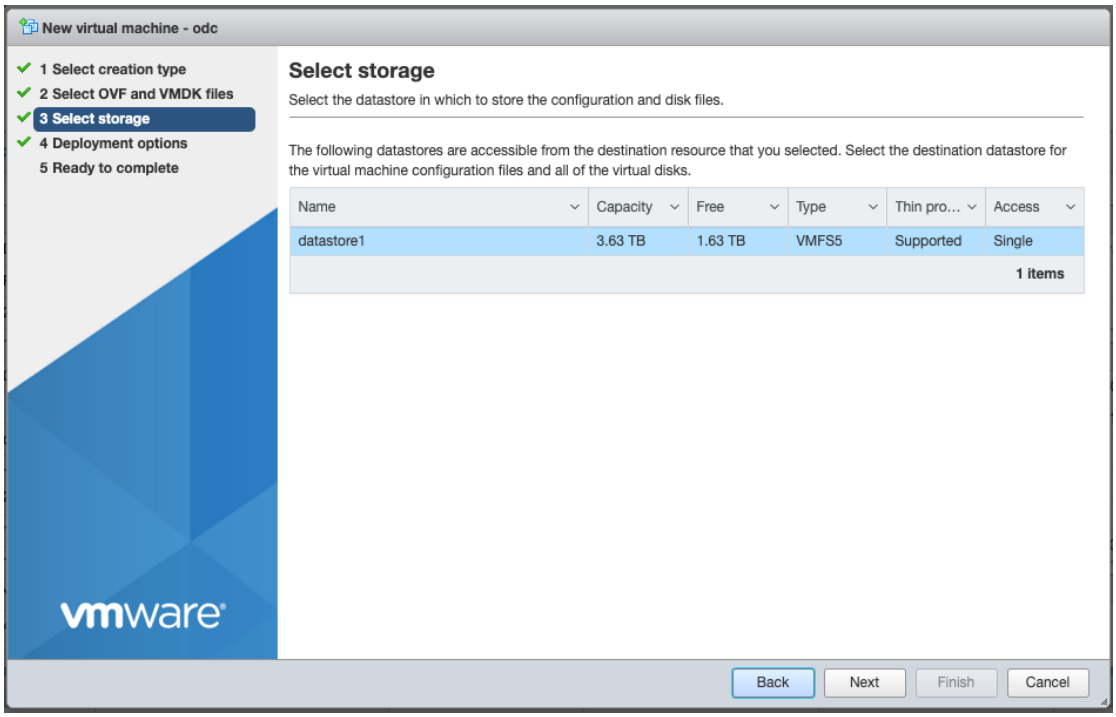
1. Log in to the VMware vSphere web client.
2. Under [Navigator], click [Host] and then click [Create/Register VM].



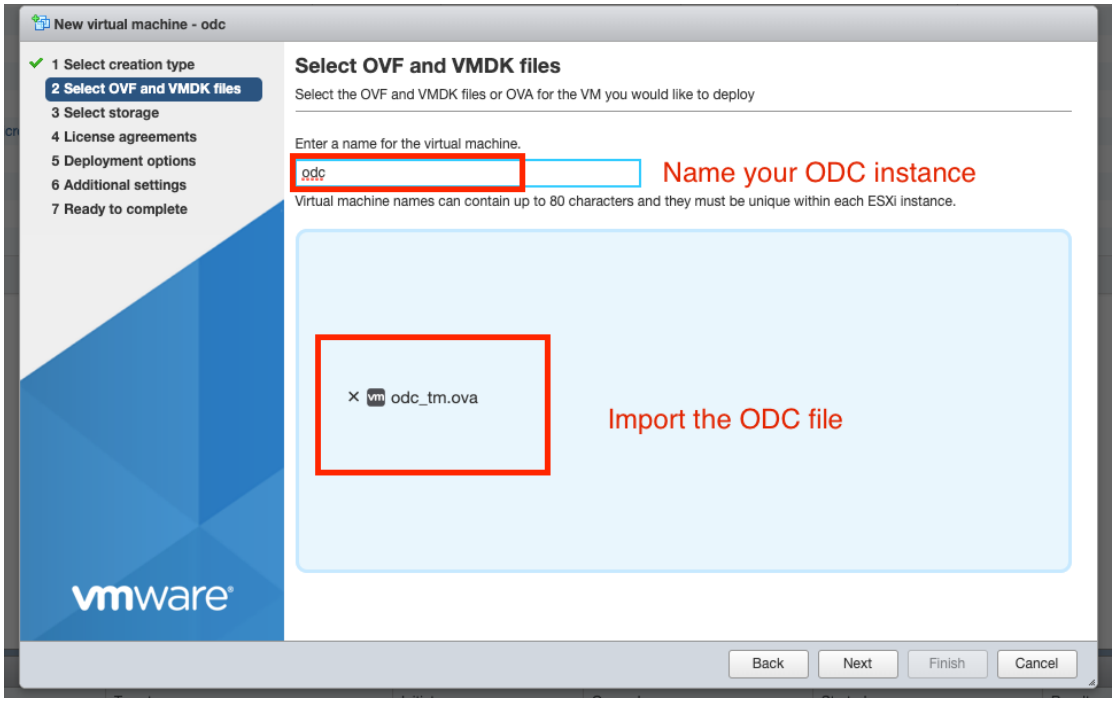
3. Select [Deploy a virtual machine from an OVF or OVA file].



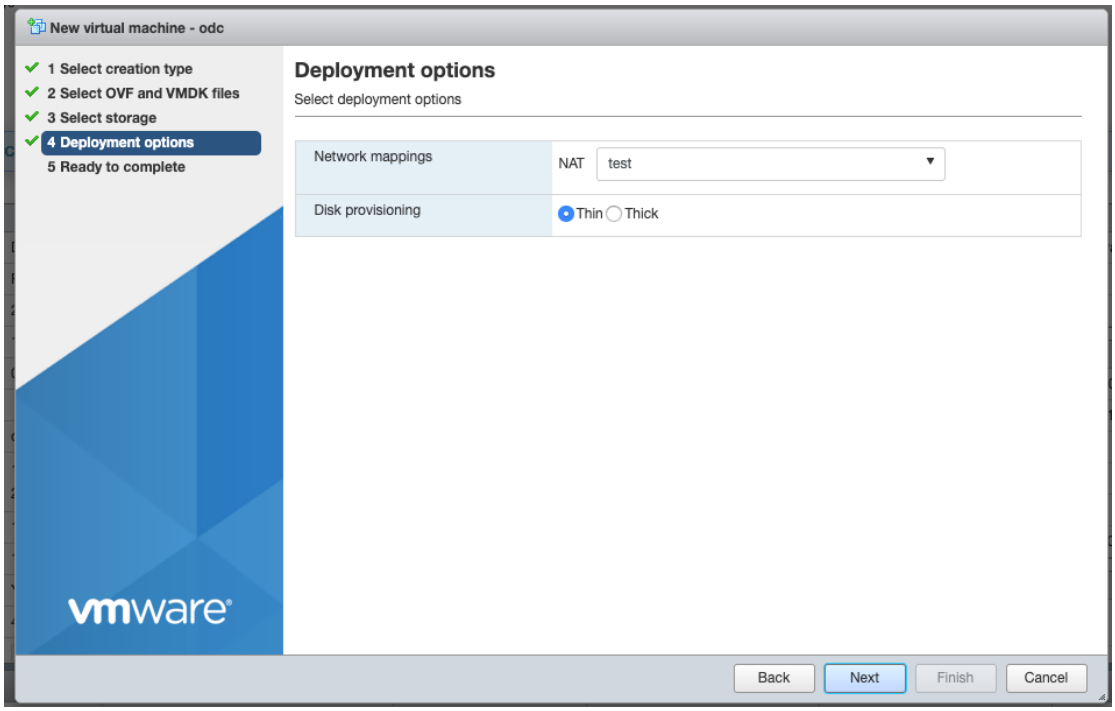
4. Input a name for your ODC and then select an ODC image to upload.



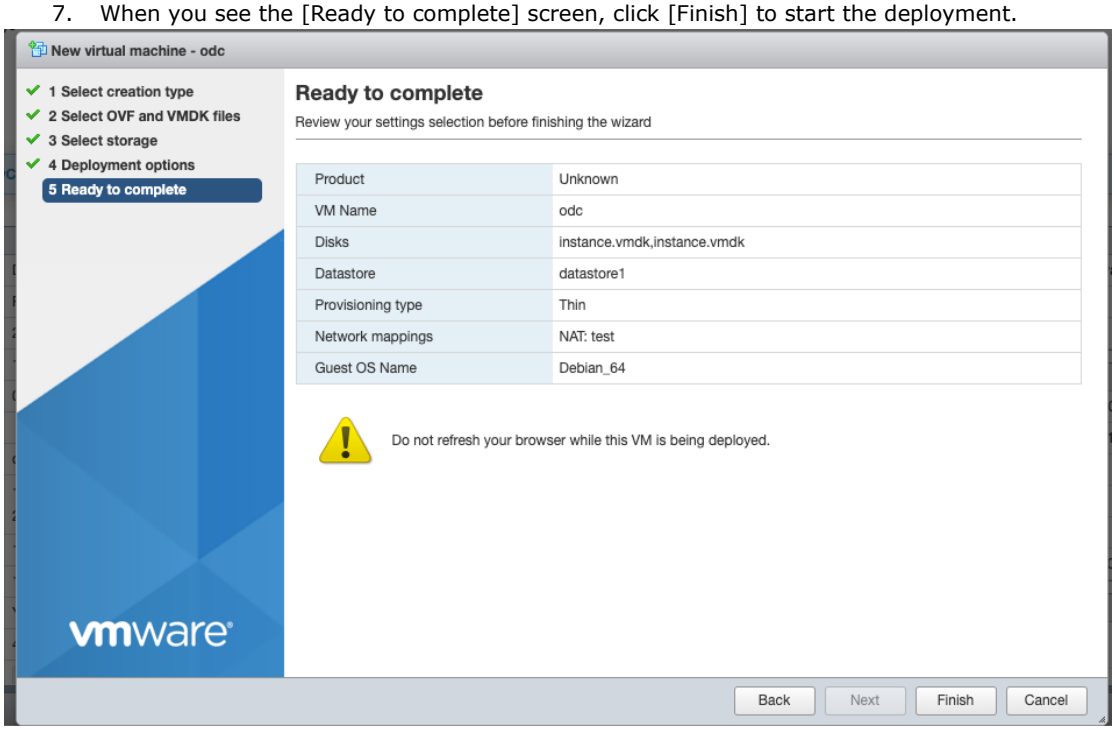
5. Choose a storage location for the ODC virtual machine.



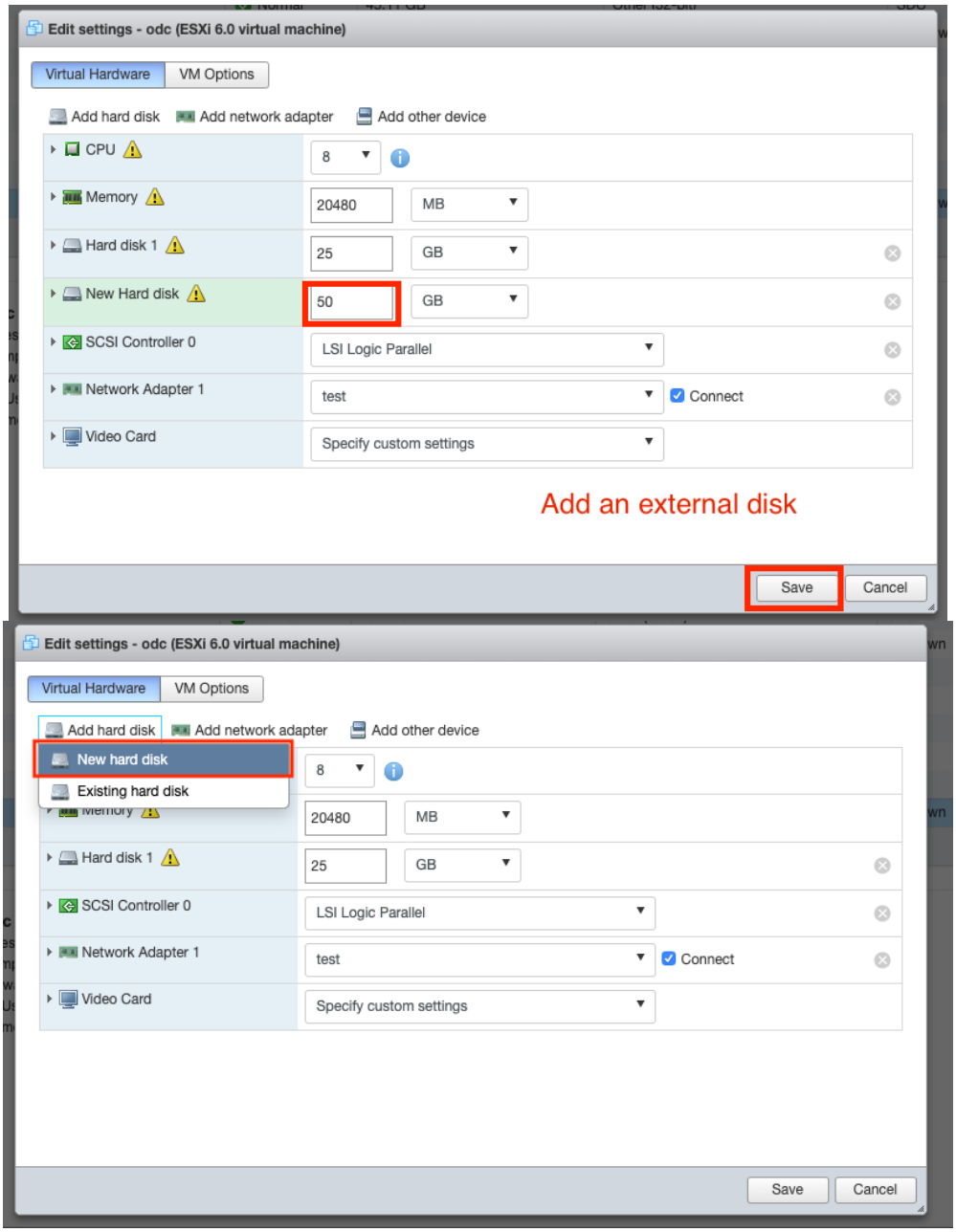
6. Select deployment options.



7. When you see the [Ready to complete] screen, click [Finish] to start the deployment.



8. Under the [Recent tasks] pane, you will see a progress bar indicating that the ODC image is being uploaded. Please wait until the upload is finished.
9. Add an external disk with at least 50 GB space to the ODC instance.
   a. Power off the ODC instance if it is powered on.
   b. Add the external disk by the following steps: [Actions] → [Edit settings] → [Add hard disk] → [Save].



c. The external disk size can be decided depending on the number of logs to be stored, as shown on the suggestion table below.

#of Logs	Disk
10,000,000	50 GB
50,000,000	150 GB
100,000,000	300 GB

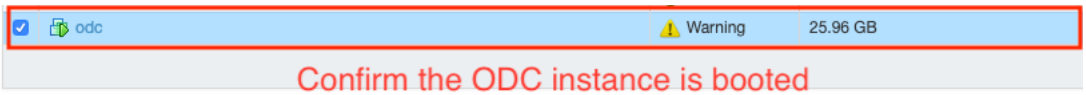
d. If ODC needs to increase the number of the logs to be stored, the steps are (1) power off the ODC, (2) enlarge the external disk size to fit the maximum log requirement, and (3) power on the ODC instance. After that, ODC will enlarge the storage available for log files.

e. If we want to migrate the existing ODC setting to the newly launched VM, please refer to *System Migration on page 21*.

Note: The ODC requires one external disk and the minimum size of the external disk must be above 50GB, otherwise the ODC will not finish initialization and will not complete the boot process.

Note: The external disk is used to store the system configurations and event logs. You may attach the external disk of a terminated ODC instance here instead of adding a new disk if you want to migrate the previous configurations and logs to the new ODC instance.

10. Power on the VM.



Confirm the ODC instance is booted

odc

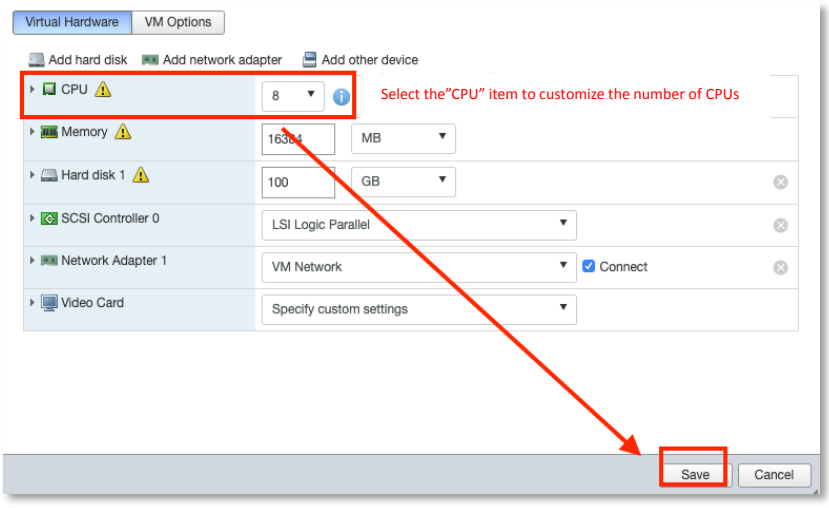
Guest OS	Other (32-bit)
Compatibility	ESXi 6.0 and later (VM version 11)
VMware Tools	Yes
CPUs	8
Memory	20 GB

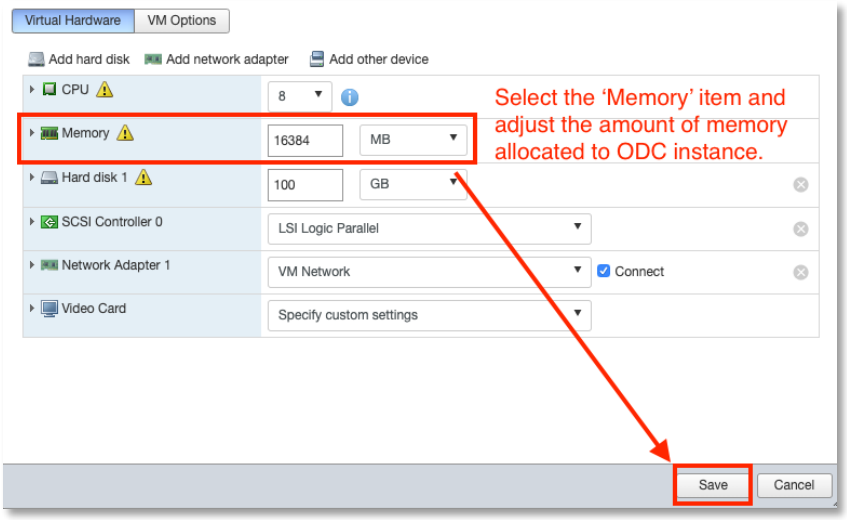
Click the window to log into the vShell of ODC

11. **(Optional)** Adjust your ODC instance to use proper resource configurations based on the following sizing table or using the default settings (8 core CPU, 16 GB memory).
    a. Shut down the instance of ODC and click [Edit].
    The [Edit settings] window will appear.
    b. Configure the number of CPU cores.
    c. Configure the amount of memory.
    d. Boot the ODC instance.

Sizing Table

Nodes	CPU	Memory
50	4 cores	16 GB
100	4 cores	16 GB
150	6 cores	32 GB
200	8 cores	32 GB





Accessing the ODC CLI

1. Open the ODC VM console.
2. Log in with "root / txone"
3. Change the default password
    a. Type oobe
    b. Change the default password
    c. Re-log in to the ODC with your new password

```
If you want to exit this shell, please type `exit` or `Ctrl-D`.

Caution: please type the command ```oobe``` to active the vShell.
Caution: please type the command ```oobe``` to active the vShell.
Caution: please type the command ```oobe``` to active the vShell.
Caution: please type the command ```oobe``` to active the vShell.
Caution: please type the command ```oobe``` to active the vShell.
$ oobe
Type current password:
Type the new password:
```

4. After re-logging in to ODC, you may optionally type the "help" command to see a list of available commands for the instance.

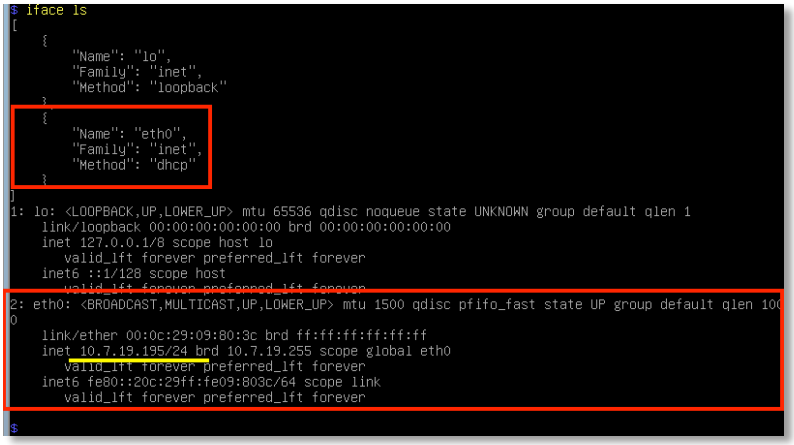
```
vShell, version v1.5.4
The commands provided in:
  access-list    Manage the IP whitelists
  dx             Curl the target server.
  env            Manage system environment variables
  exit           Exit this shell
  help           List all command usage
  iface          Manage the network interfaces
  ping           Test the reachability of a host
  poweroff       Shut down the machine immediately
  pwd            Change the root user password
  reboot         Restart the machine immediately
  resolv         Manage the domain name server
  scp            Send files via scp
  service        Manage the device center services
  sftp           Send files via sftp
  web            Commands of the device center web

Shortcut table:
  Tab            Auto-complete or choose the next suggestion on the list
  Ctrl + A       Go to the head of the line (Home)
  Ctrl + E       Go to the tail of the line (End)
  Ctrl + D       Delete the character located at the cursor
  Ctrl + L       Clear the screen
```

Getting the IP Address of the ODC Instance

1. Type the following command to get the IP address of the ODC Instance

   ```
   $ iface ls
   ```



[Optional] Configure the IP Address Settings

You can choose to configure the IP address manually.

1. Use the "iface update" command to update the settings of an existing network interface. For example, the following command sets the interface "eth0" to a static IP address 10.7.19.157/24 with the Gateway IP address 10.7.19.254:

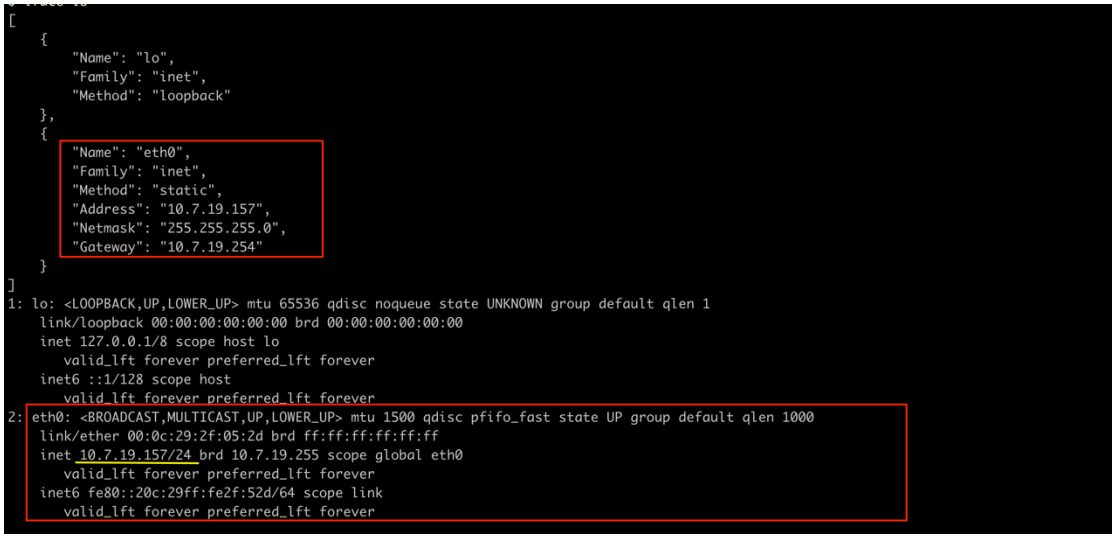
   ```
   $ iface update eth0 --method static --address 10.7.19.157  --netmask
   255.255.255.0 --gateway 10.7.19.254
   ```

2. Confirm the network interface settings are correct and execute the following command to bring the new settings into effect:

   ```
   $ iface restart eth0
   ```

3. Execute the following command to view the network interface settings:

   ```
   $ iface ls
   ```

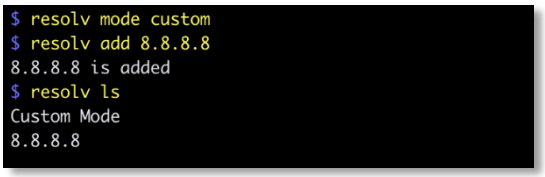


4. Use the "resolv add" command to add a DNS server and "resolv ls" to list the DNS servers you've added. For example, the following command adds "8.8.8.8" to the DNS server list.

```
$ resolv mode custom
$ resolv add 8.8.8.8
```

5. Type the following command to view the DNS server settings.

```
$ resolv ls
```



6. Execute the following command to reboot the VM:

```
$ reboot
```

Opening the Management Console

OT Defense Console provides a built-in management console that you can use to configure and manage the product. View the management console using a web browser.

Note: View the management console using Google Chrome version 63 or later; Firefox version 53 or later; Safari version 10.1 or later; or Edge version 15 or later.

Procedure

1. In a web browser, type the address of the OT Defense Console in the following format:

   `https://<target server IP address or FQDN>`

   The login screen will appear.
2. Enter your credentials (user name and password).

   Use the default administrator credentials when logging in for the first time:

   - User name: `admin`
   - Password: `txone`
3. Click Log On.

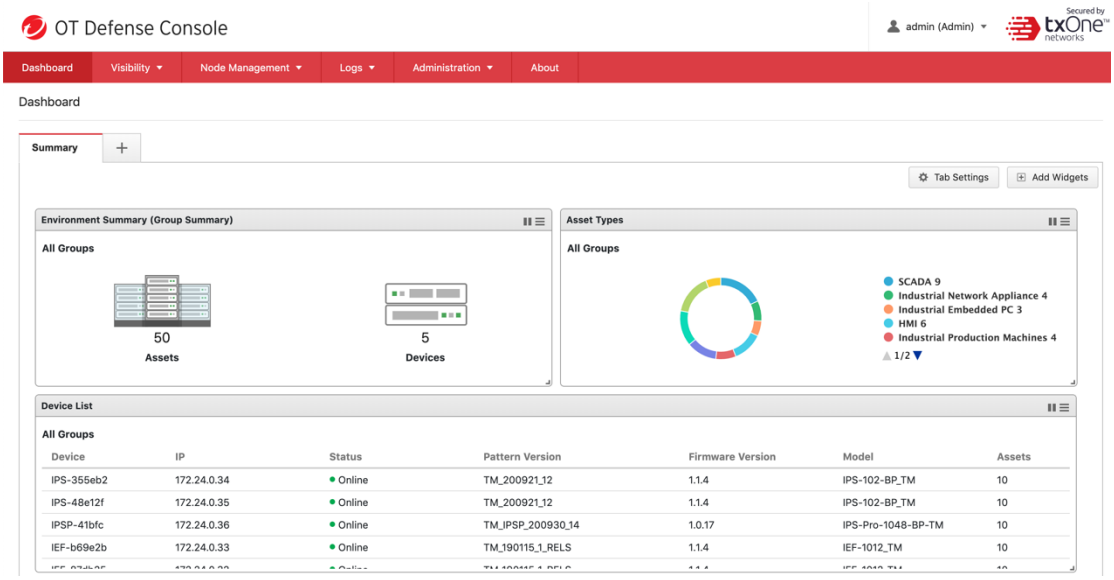
   If this is your first log on, the Login Information Setup frame will appear.

Note: You must change the default login name and password at first log on before you can access the management console.

Note: New login name can not be "root", "admin", "administrator" or "auditor" (case-insensititive).

   a. Confirm your password settings.
      - New Login Name
      - New Password
      - Retype Password
   b. Click Confirm.

      You will be automatically logged out of the system. The Log On screen will appear again.
   c. Log on again using your new credentials.



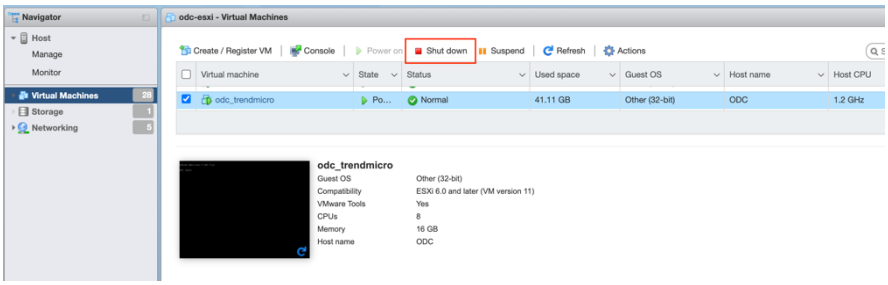
System Migration

When a new version of ODC is released, we can migrate the settings of the old ODC by attaching the external disk of the old ODC to the new ODC VM. The migration of settings includes:

- The UUID of the old ODC
- The pattern and firmware downloaded by the old ODC
- The system configuration set from the old ODC including its license, accounting information, security policies, and so on
- The security event logs stored by old ODC

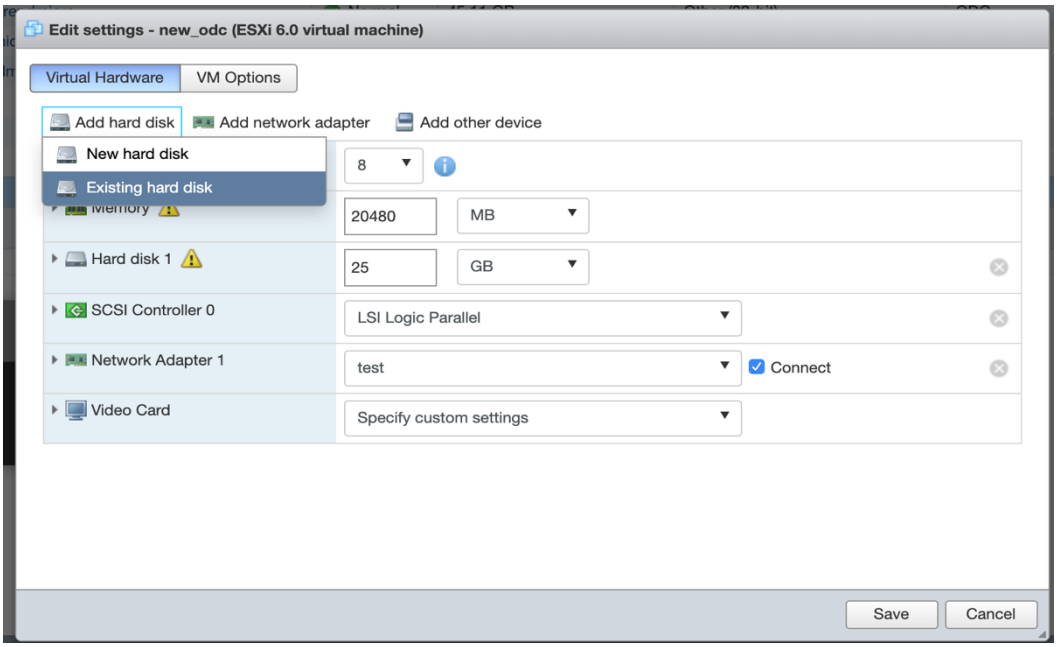
Procedure

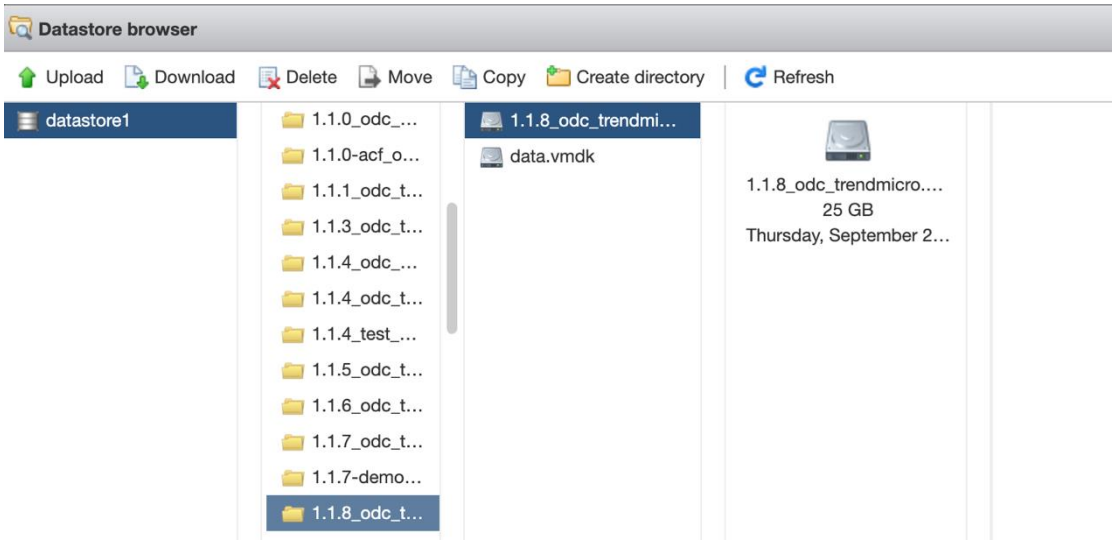
1. Launch the new instance of ODC (refer to section "Deploying OT Defense Console")
2. Power off the old ODC



3. Attach the external disk of the old ODC to the new ODC.

4. The old ODC's information will be migrated into the new ODC.





Installing ODC on a VMware Workstation

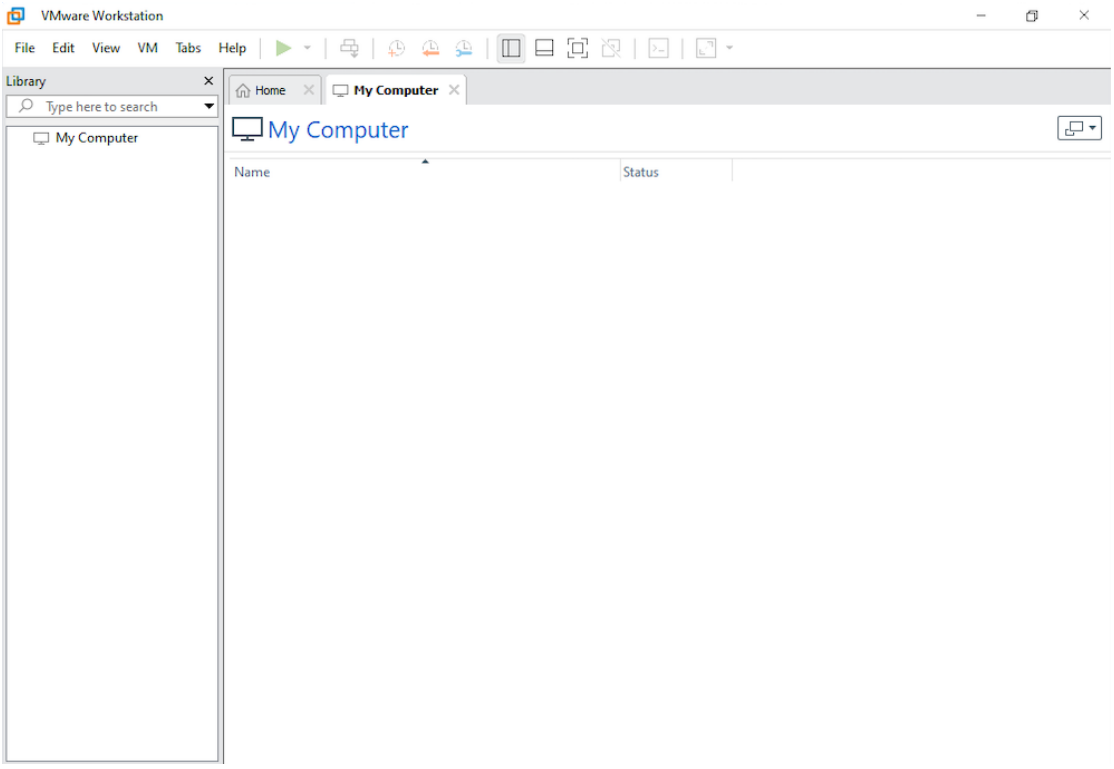
This chapter describes how to deploy OT Defense Console to a VMware Workstation system.

Prerequisites

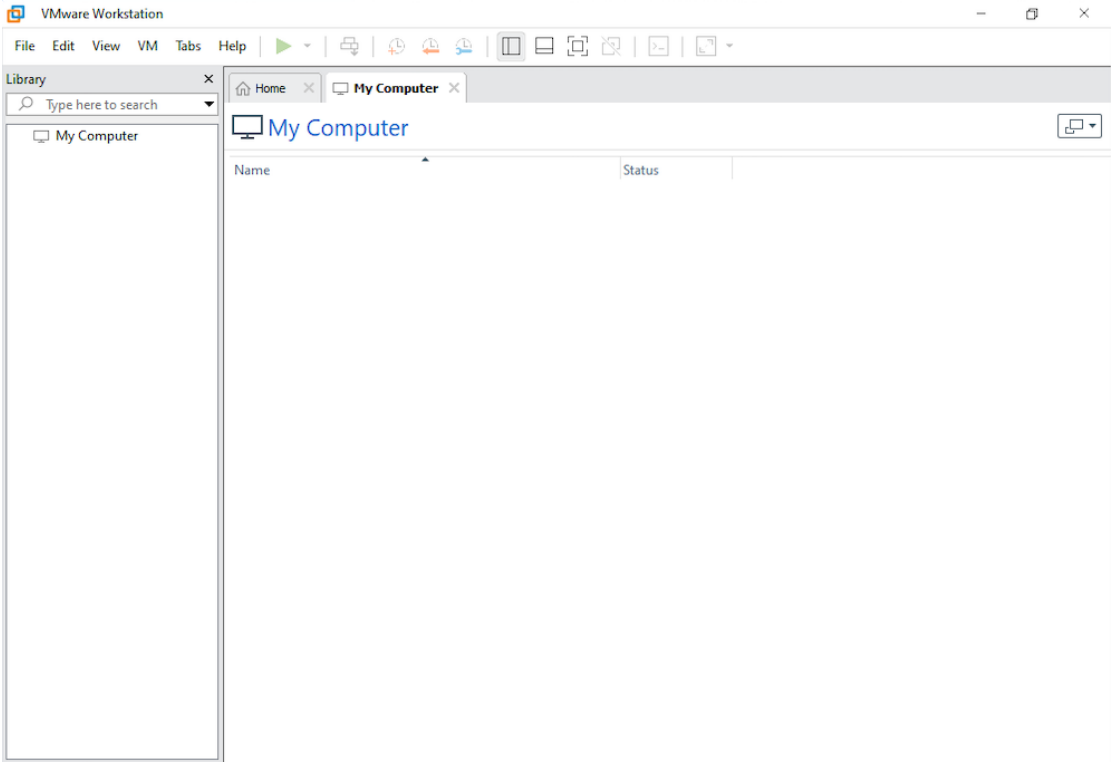
- The OVA packages provided by Trend Micro must be available and accessible to the VMware Workstation.
- VMware workstation 14 or later is required.

Deploying OT Defense Console

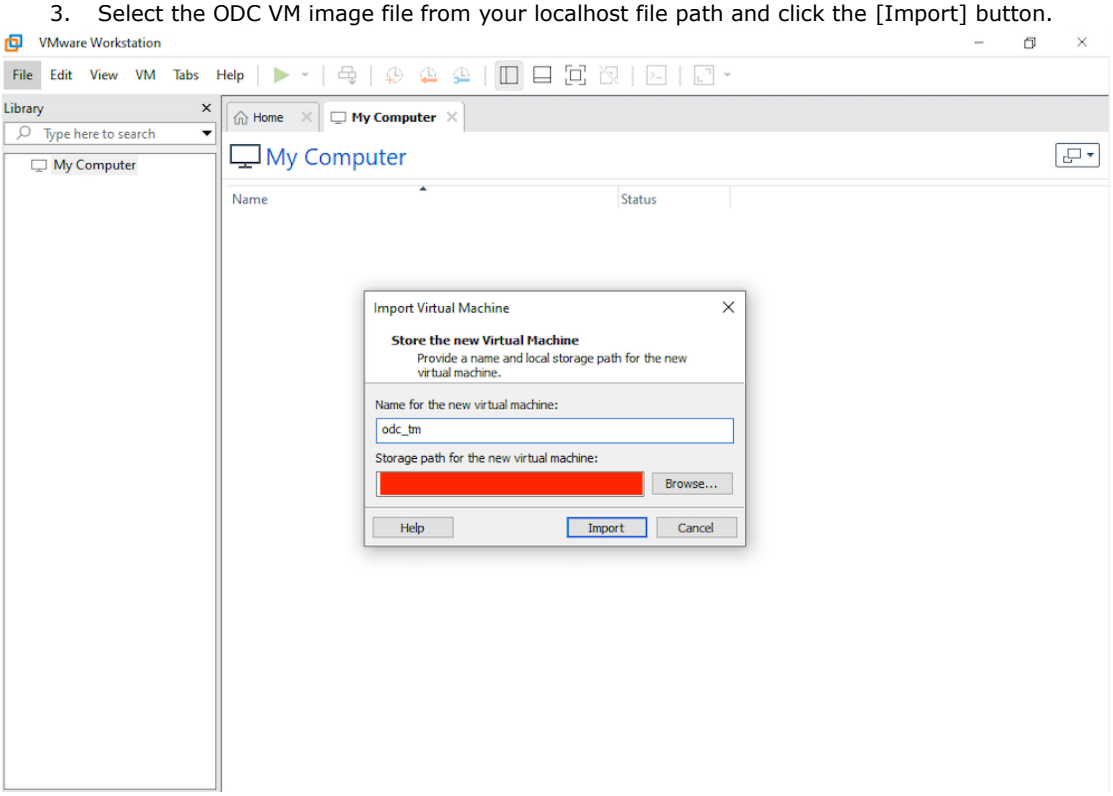
1. Start the VMware Workstation and click [File] on the menu bar.



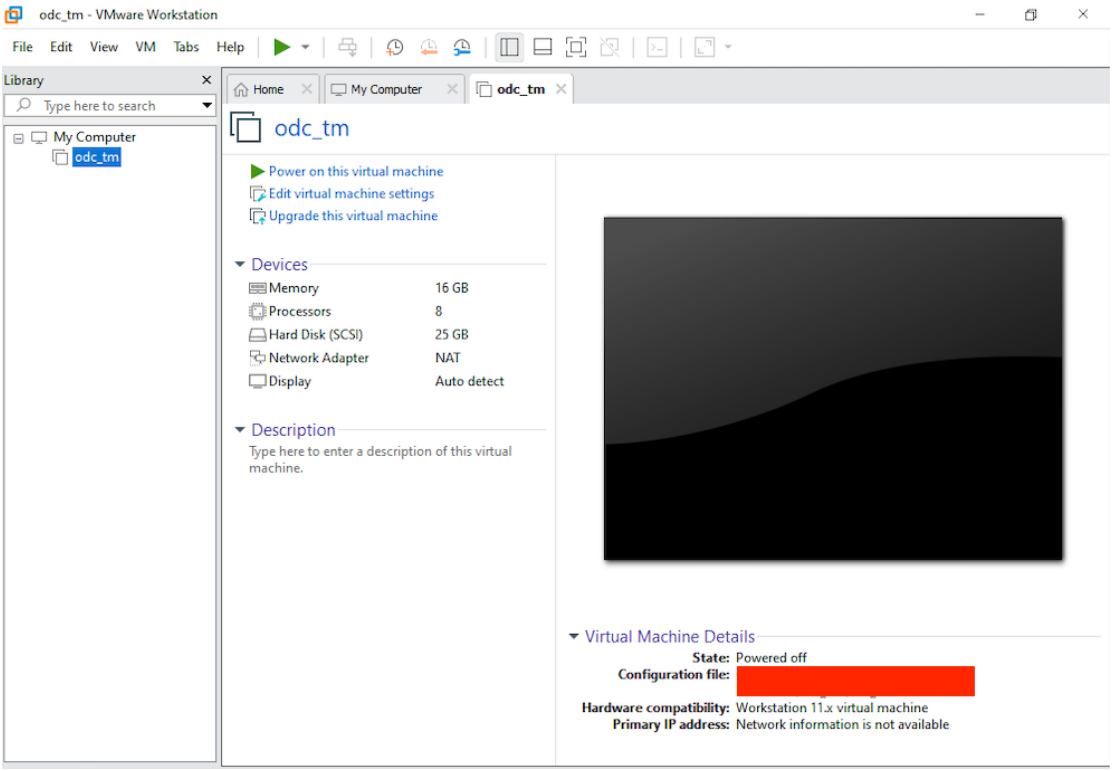
2. Select [Open] to import the ODC VM image file (*.ova).



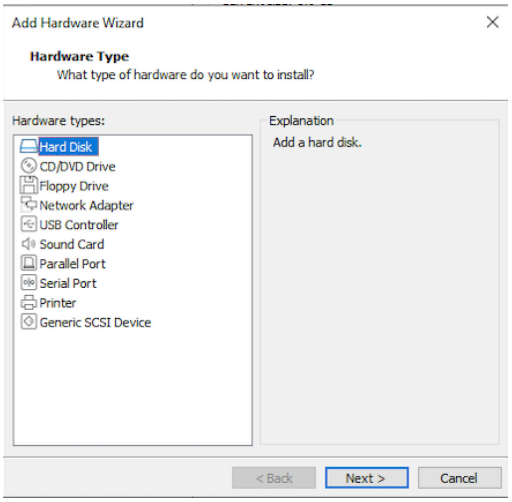
3. Select the ODC VM image file from your localhost file path and click the [Import] button.



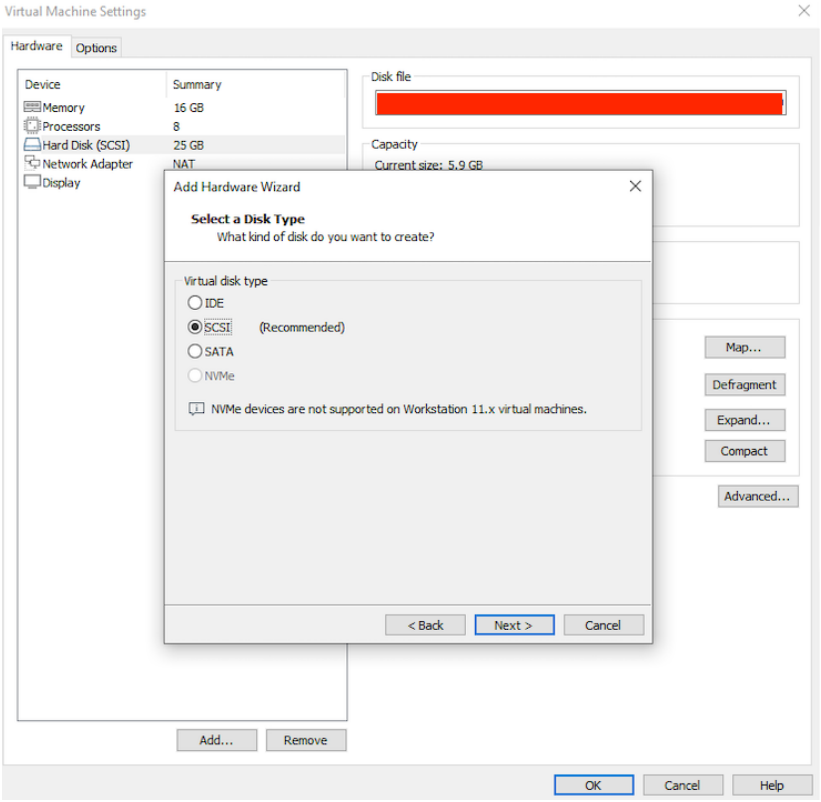
4. Check the detailed VM information of the imported ODC VM.



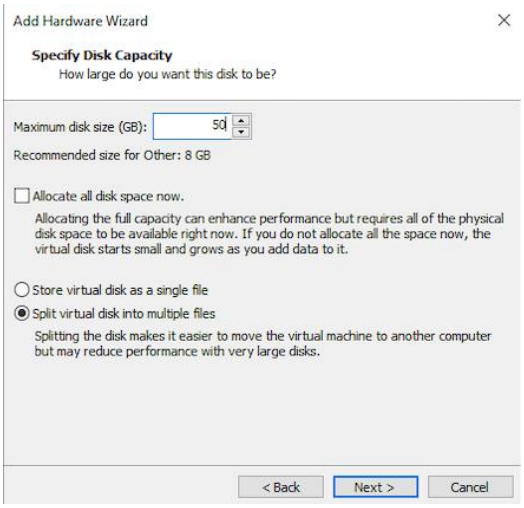
5. Add an extra disk.
   a. Click [Edit virtual machine settings].
   b. Click [Add], then choose [Hard Disk].



   c. Select Disk type.



d. Select Disk size.



e. Select path to store the disk.

f. Click [OK].

6. **(Optional)** Adjust your ODC instance to use proper resource configurations based on the following sizing table or using default settings (8 CPU cores, 16 GB of memory).

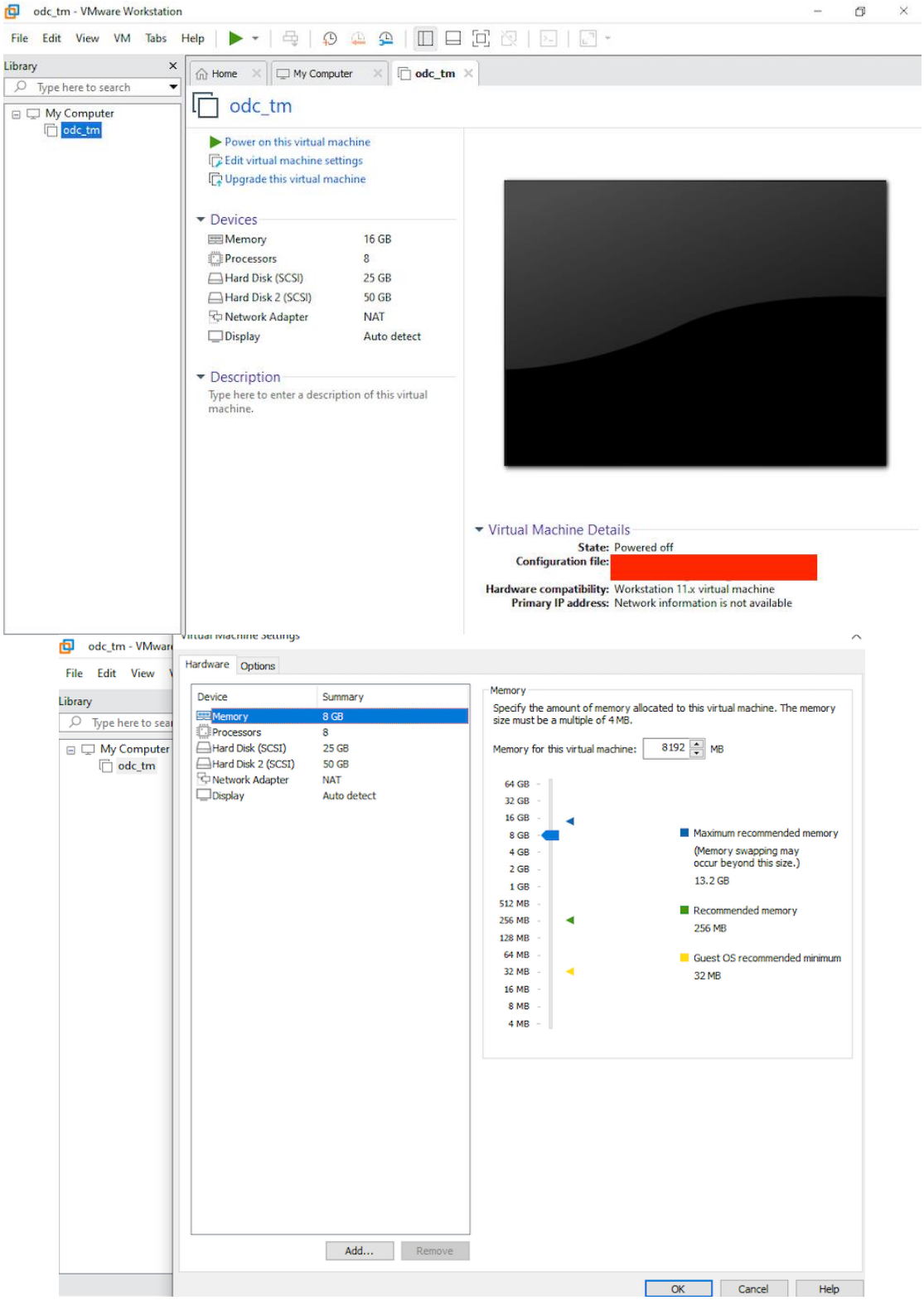
Sizing Table

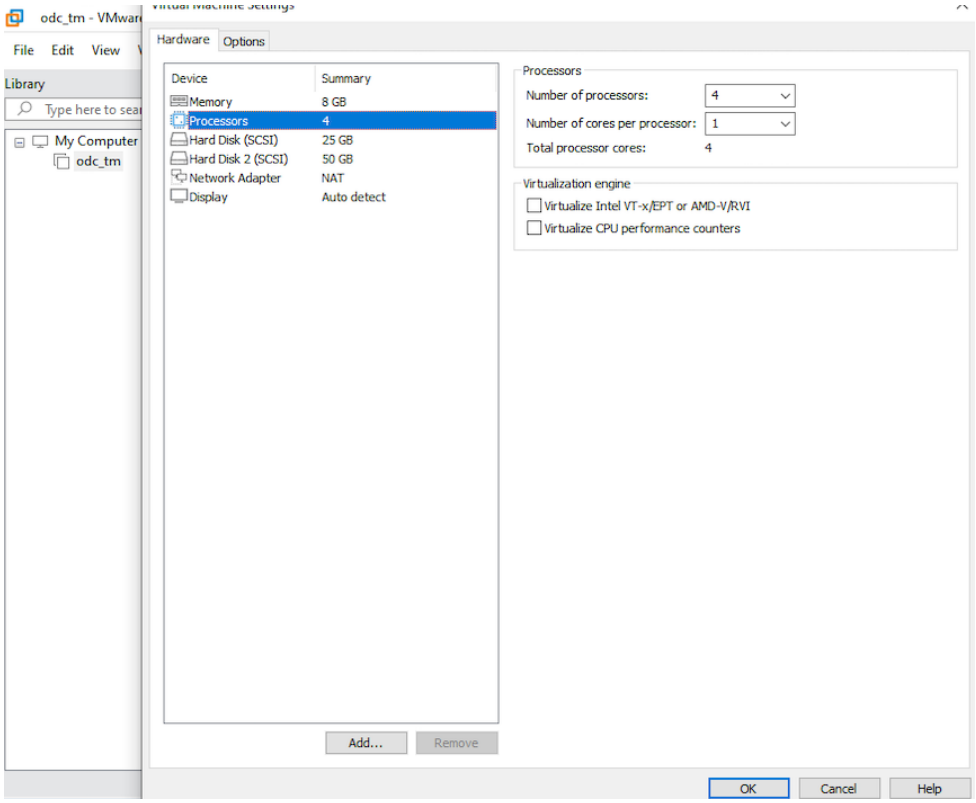
Nodes	CPU	Memory
50	4 cores	16 GB
100	4 cores	16 GB
150	6 cores	32 GB
200	8 cores	32 GB

a. Click [Edit virtual machine settings].

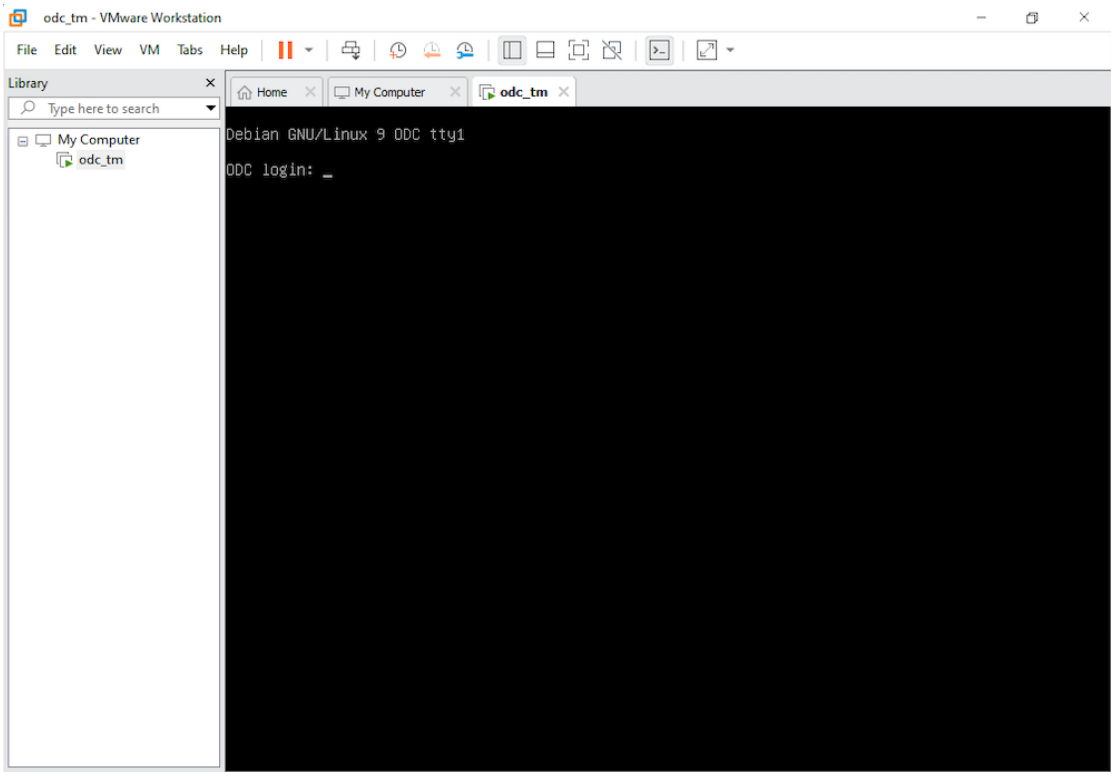
b. Configure the amount of memory.

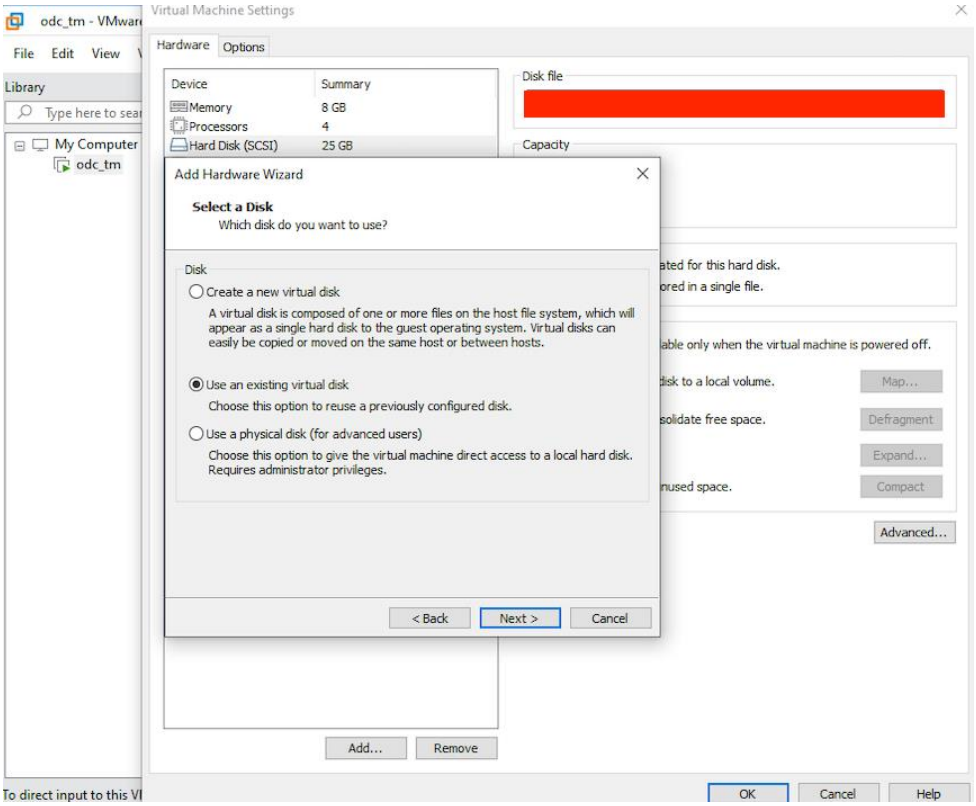
c. Configure the number of CPU cores.





7. **(Optional)** Change the network adapter setting from 'NAT' to 'Bridged'.
   a. Right click the ODC VM icon and select [Settings].
   b. Select [Network Adapter] and change the default setting from [NAT] to [Bridged] if necessary.
8. Boot the ODC VM, and the ODC instance will start.





System Migration

When a new version of ODC is released, we can migrate the setting of the old ODC by attaching the external disk of the old ODC to the new ODC VM. The migration of settings can include:

- The UUID of the old ODC
- The pattern and firmware downloaded by the old ODC
- The system configuration set by the old ODC including license, accounting information, security policies, and so on.
- The security event logs stored by the old ODC

Procedure

1. Launch the new ODC instance (refer to section "Deploying OT Defense Console")
2. Power off the old ODC
3. Attach the external disk of the old ODC to the new ODC.
4. A window will come up where you can select which settings and data will be migrated into the new ODC, and after your confirmation the old ODC's selected information will be migrated into the new ODC.

Configuring the ODC system

Please check the following sections for directions on configuring your ODC system:

- *Accessing the ODC CLI on page 9*
-

Terms and Acronyms

The following table lists the terms and acronyms used in this document.

Term/Acronym	Definition
EWS	Engineering Workstation
HMI	Human-Machine Interface
ICS	Industrial Control System
IT	Informational Technology
ODC	Operational Technology Defense Console
OT	Operational Technology
OT Defense Console	Operational Technology Defense Console
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition