Operational Technology Defense Console – Virtual Appliance 1.4

Quick Setup Guide
(for Windows Hyper-V)

2021-08-15

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

Table of Contents 3
Chapter 1 4
ODC Onboarding to Windows Hyper-V 4
Prerequisites 4
Deploying OT Defense Console 4
Accessing the ODC CLI 12
Getting the IP Address of the ODC Instance 12
[Optional] Configure the IP Address Settings 13
System Migration 14
Opening the Management Console 15
Appendix A 17
Terms and Acronyms 17

ODC Onboarding to Windows Hyper-V

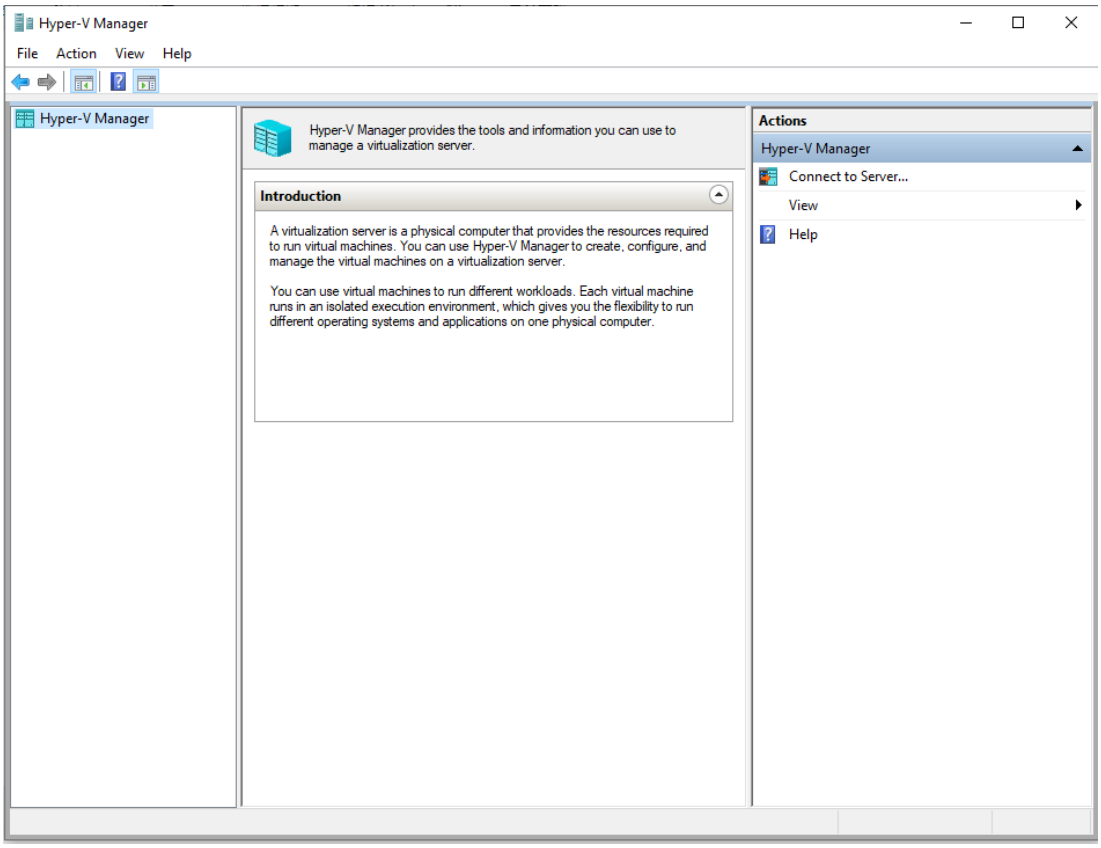
This chapter describes how to deploy OT Defense Console to a Hyper-V system.

Prerequisites

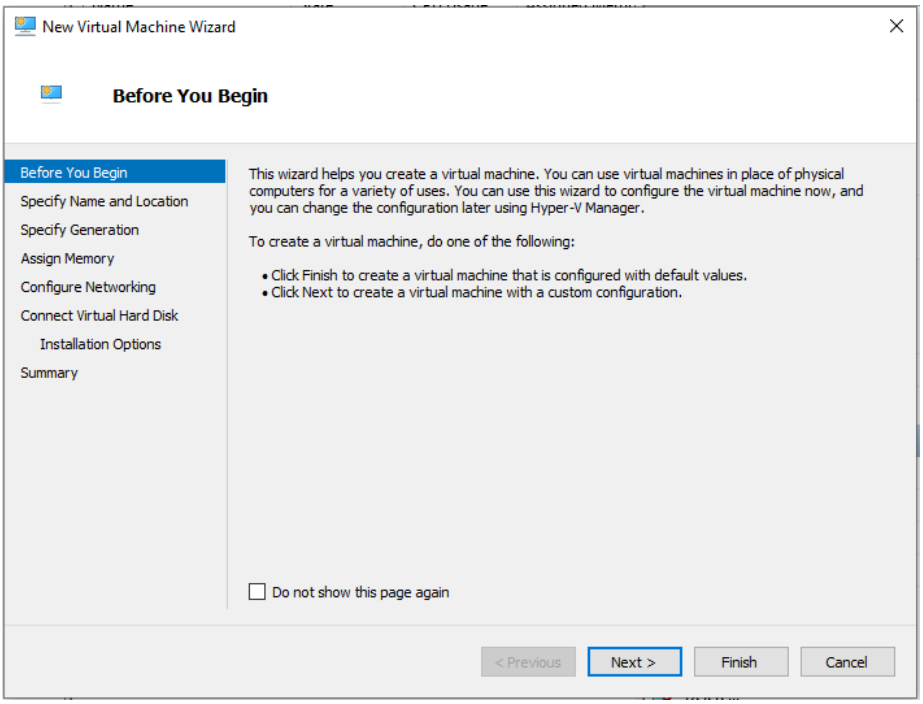
- The vhdx packages provided by Trend Micro must be available and accessible to Windows Hyper-V.
- The necessary networks have been properly created in Windows Hyper-V.
- Extra disk space (50GB or more)

Deploying OT Defense Console

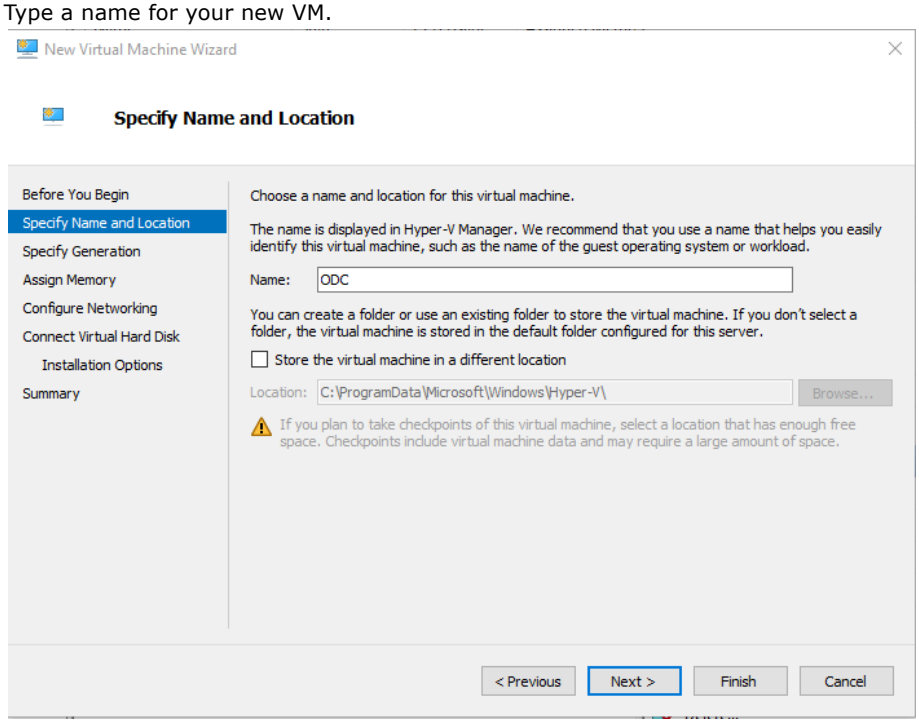
1. Launch Hyper-V manager.



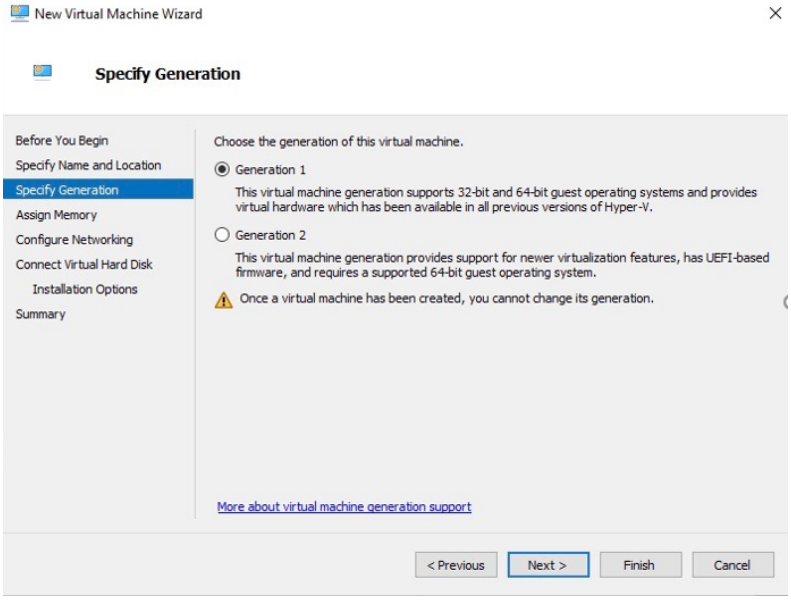
2. Under [Actions], click [New] and then click [Virtual Machine].



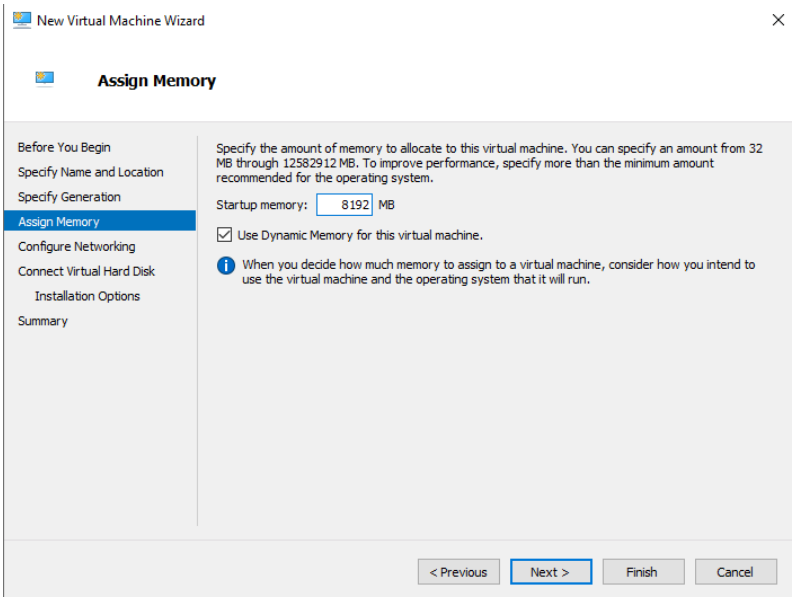
3. Type a name for your new VM.



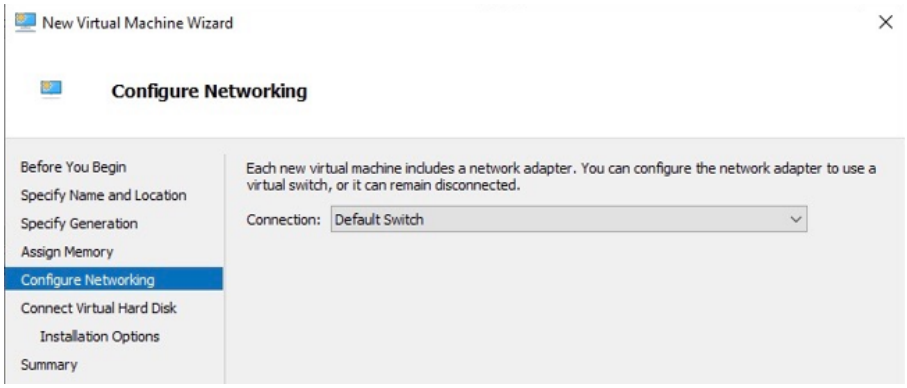
4. Specify the VM's Generation.



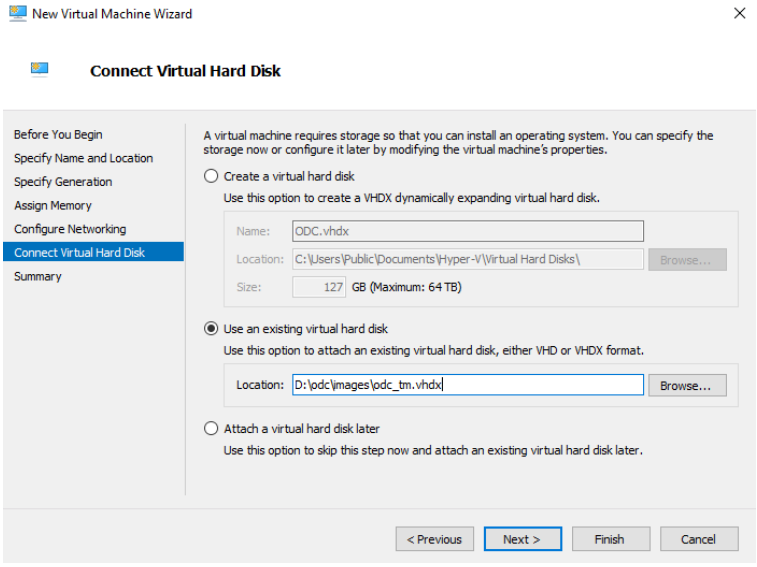
5. Allocate memory for the new VM.



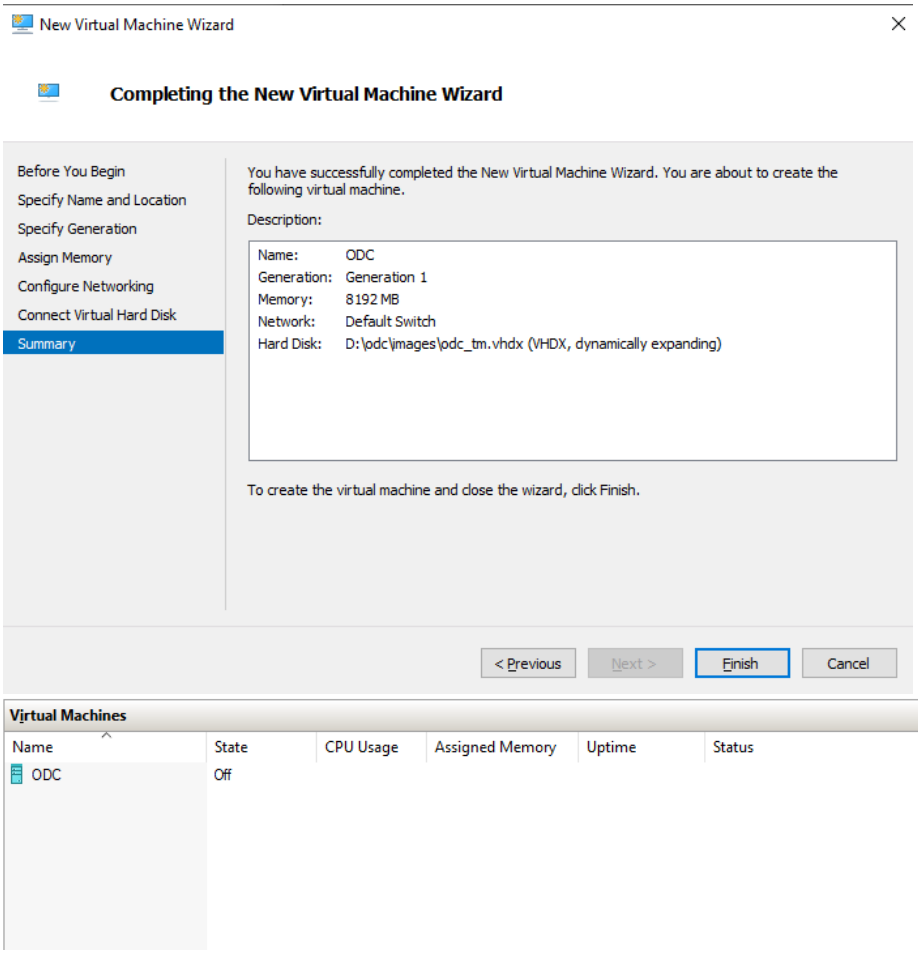
6. Configure the VM's networking settings.



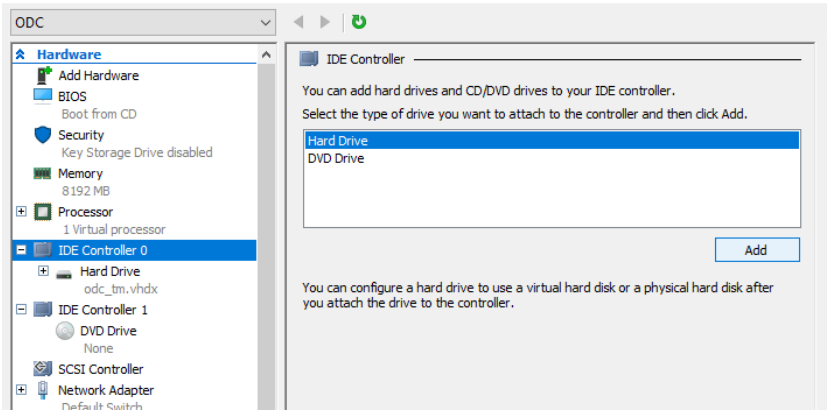
7. Select a virtual hard disk (choose the ODC vdhx package provided by Trend Micro).



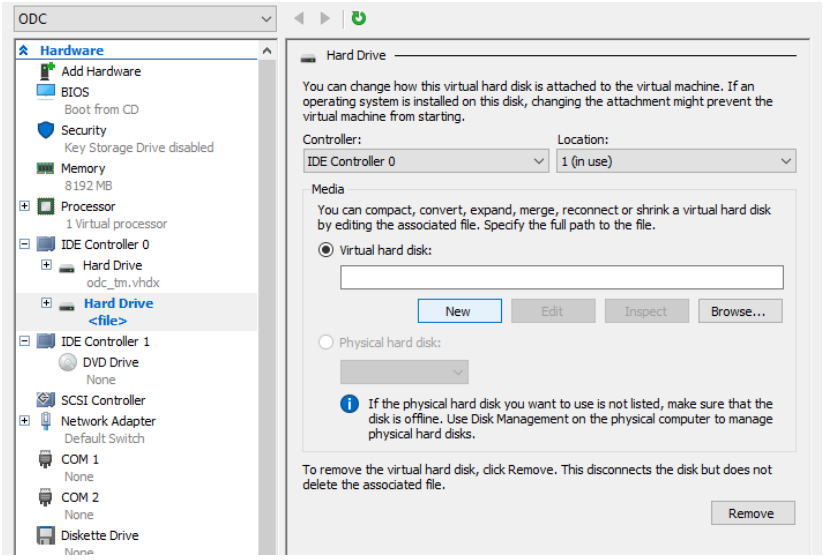
8. Check your settings then click [finish].



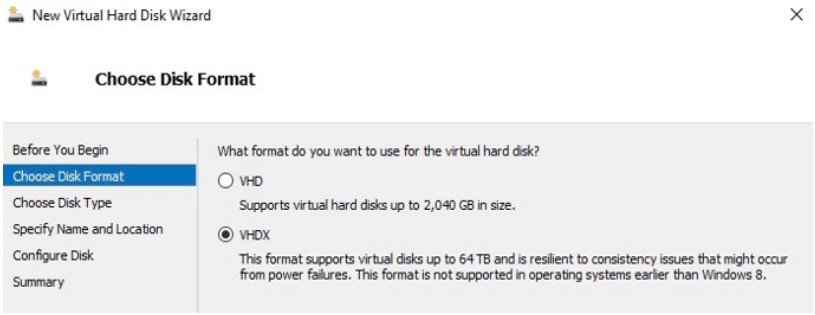
9. Add a new disk.
   a. Select [Hard Disk], then click [Add].



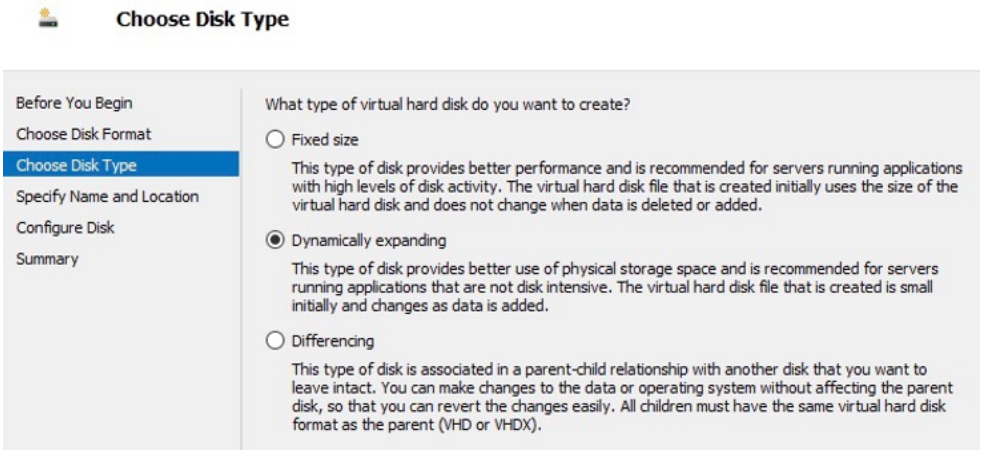
b. Click [New].



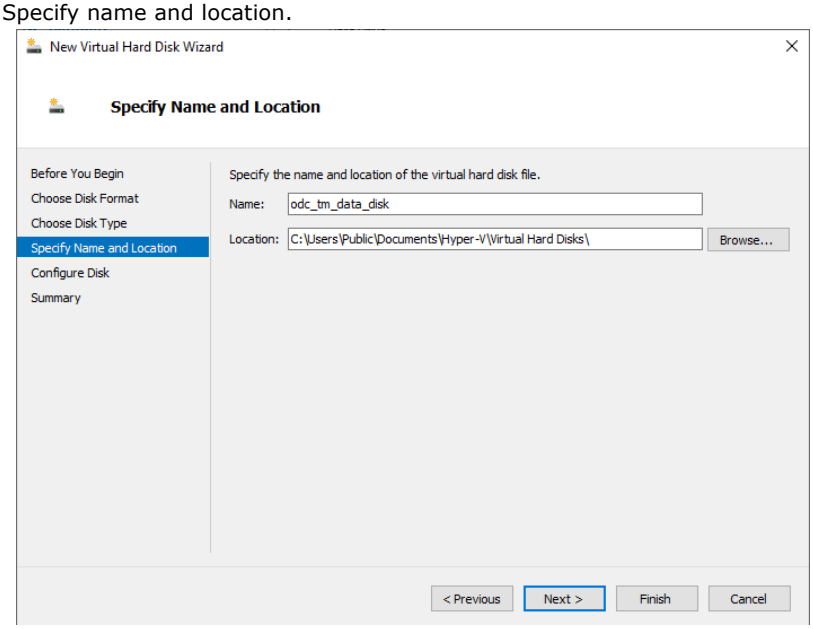
c. Choose the VHDX disk format.



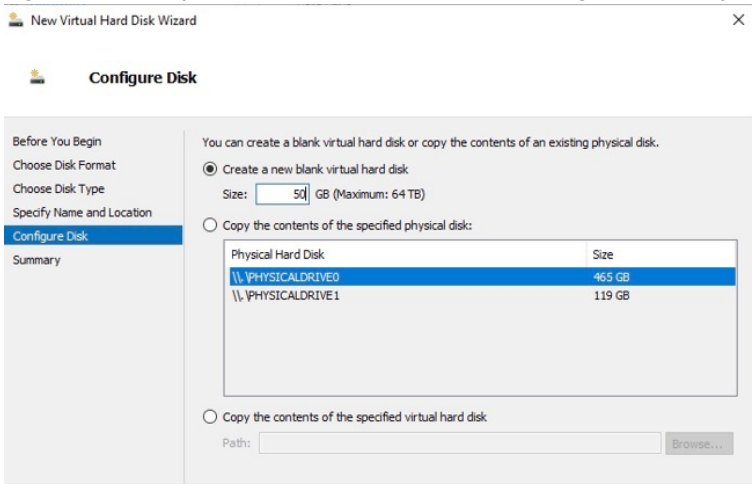
d. Choose the disk type [Dynamically expanding].



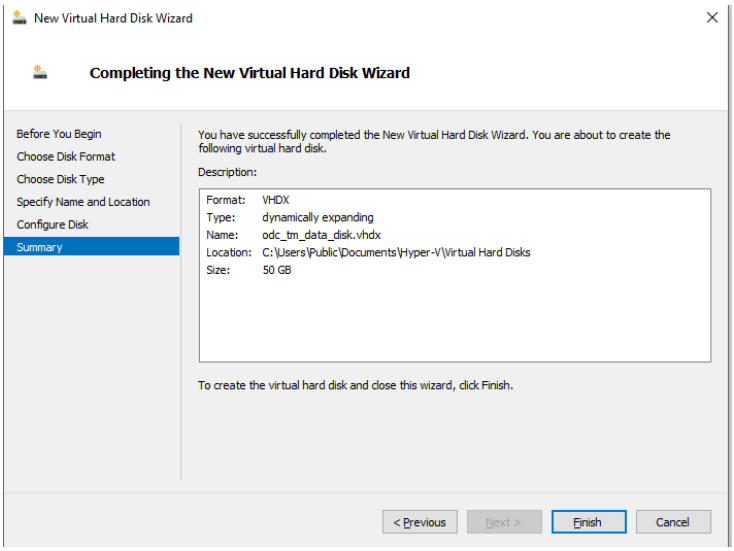
e. Specify name and location.



f. Configure disk size (ODC's disk size is based on the sizing table below).



g. Click [Finish].



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

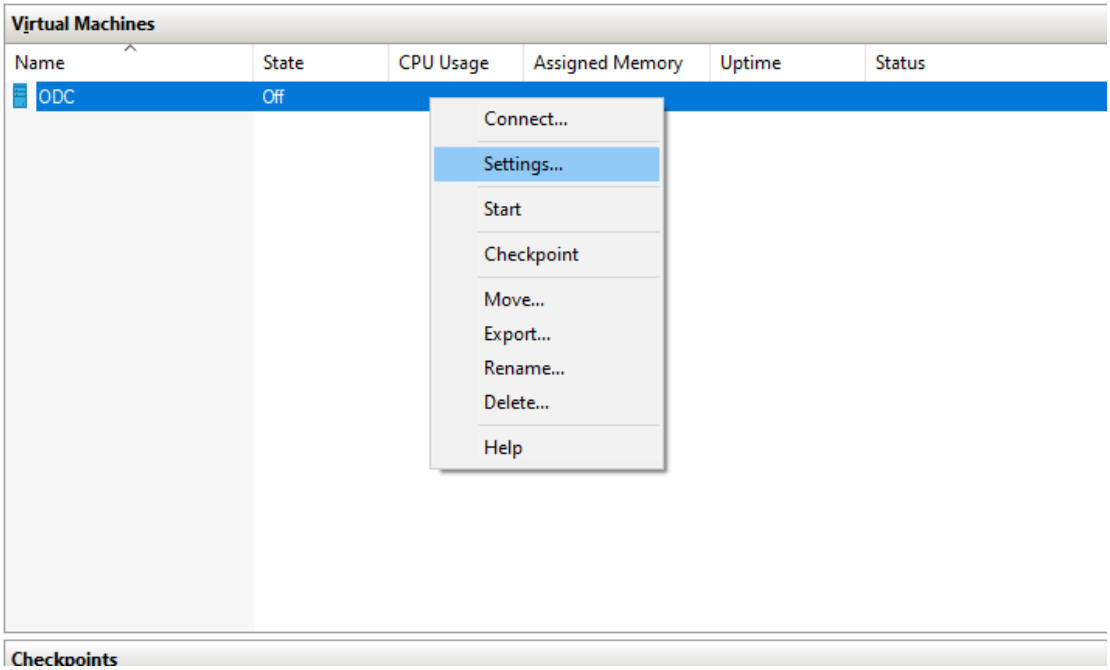
#of Logs	Disk
5,000,000	50 GB
10,000,000	150 GB
50,000,000	300 GB
100,000,000	500 GB

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.

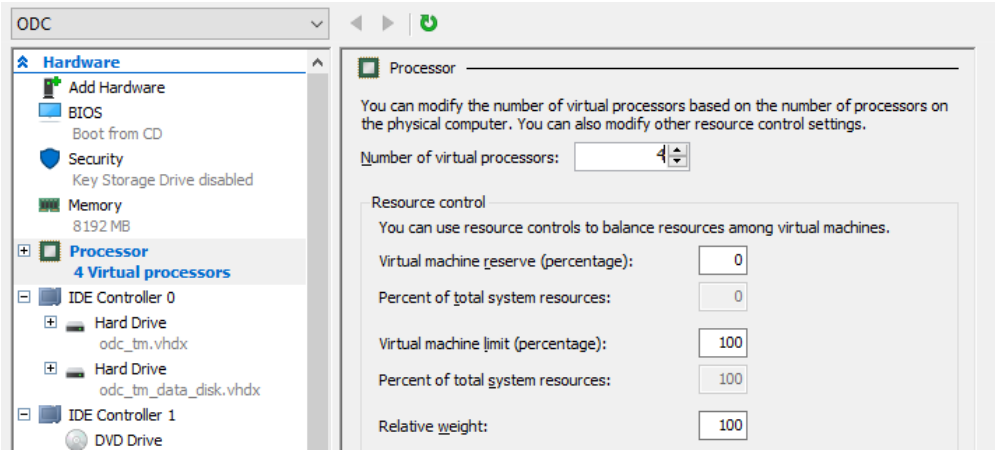
Note: The external disk is used to store the system configurations and event logs. You may attach the external disk of a terminated ODC instance here instead of adding a new disk if you want to migrate the previous configurations and logs to the new ODC instance.

10. **(Optional)** Adjust your ODC instance to use proper resource configurations based on the following sizing table or using default settings (8 CPU cores, 20 GB of memory).

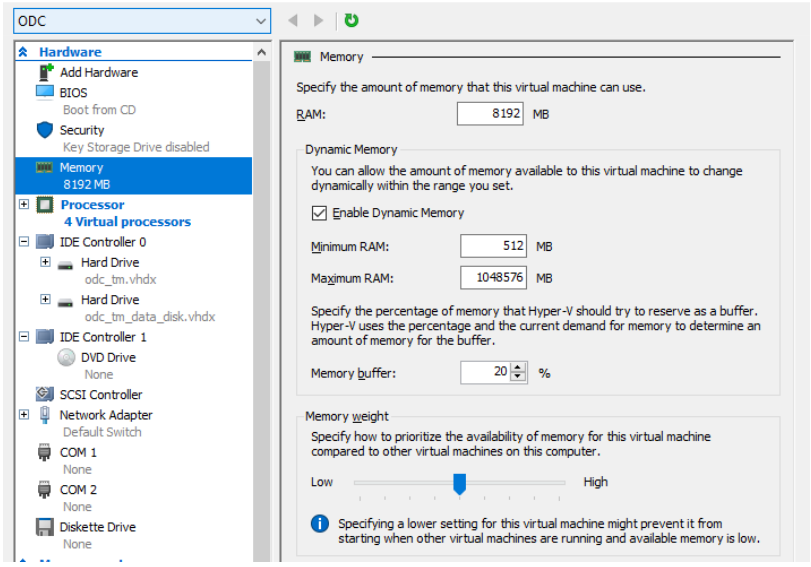
a. Shut down the instance of ODC and click [Settings].



b. Configure the number of CPU cores.



c. Configure the amount of memory.



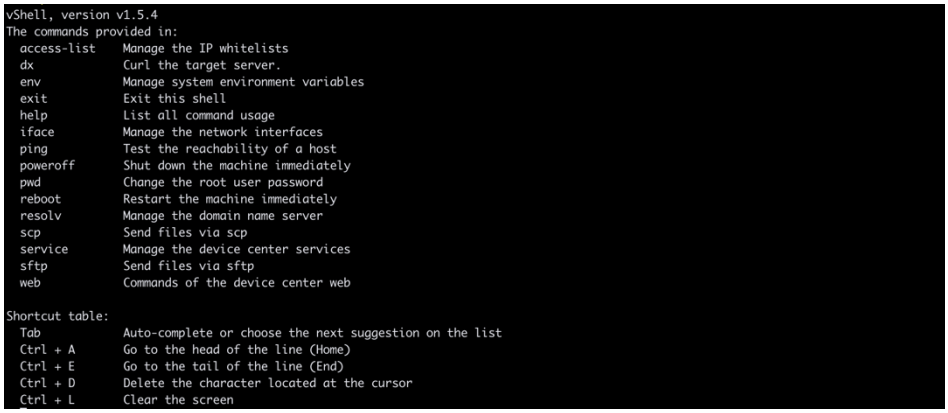
d. Boot the ODC instance.

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

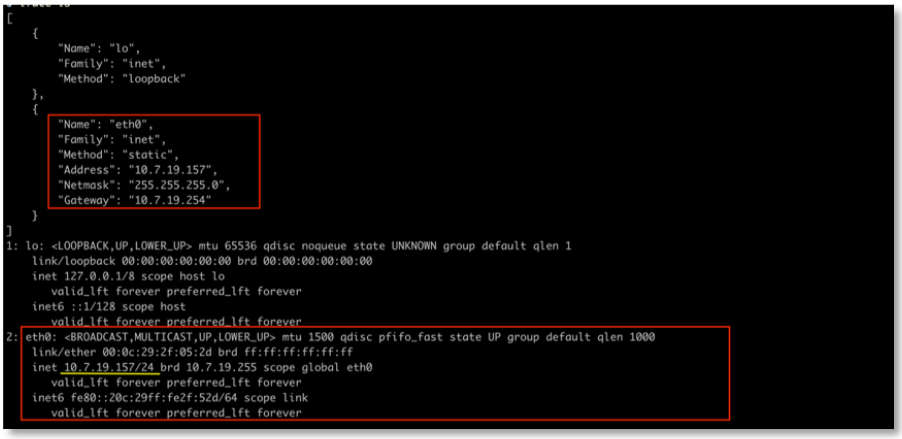
1. Open the ODC VM console.
2. Login with "root / txone"
3. After logging into the ODC, you may optionally type the "help" command to see a list of available commands on the instance.



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 10.7.19.187/24 with the Gateway IP address 10.7.19.190:

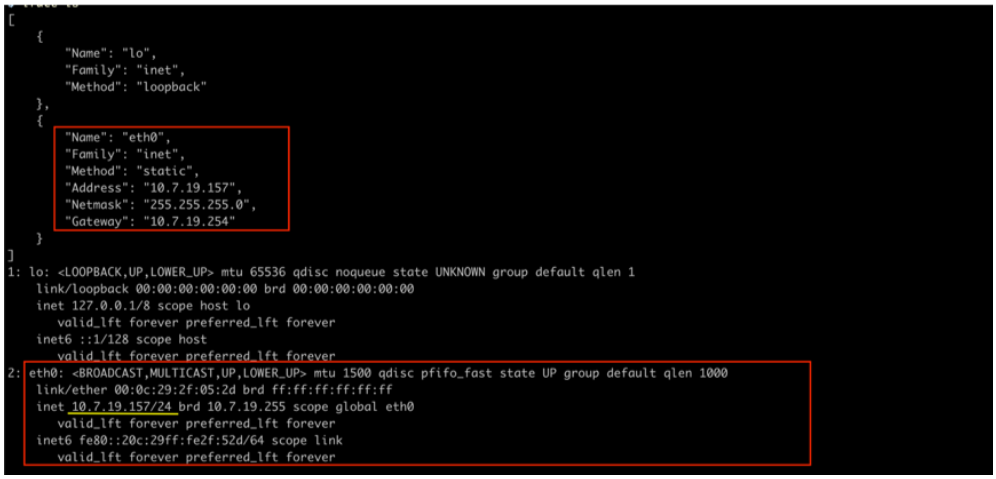
   ```
   $ iface update eth0 --method static --address 10.7.19.157  --netmask
   255.255.255.0 --gateway 10.7.19.254
   ```

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

   ```
   $ iface restart eth0
   ```

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

   ```
   $ iface ls
   ```

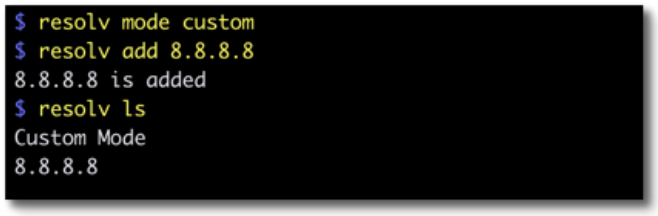


4. Use the "resolv add" command to add a DNS server and "resolv ls" to list the DNS servers you've added. For example, the following command adds "8.8.8.8" to the DNS server list.

   ```
   $ 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
   ```

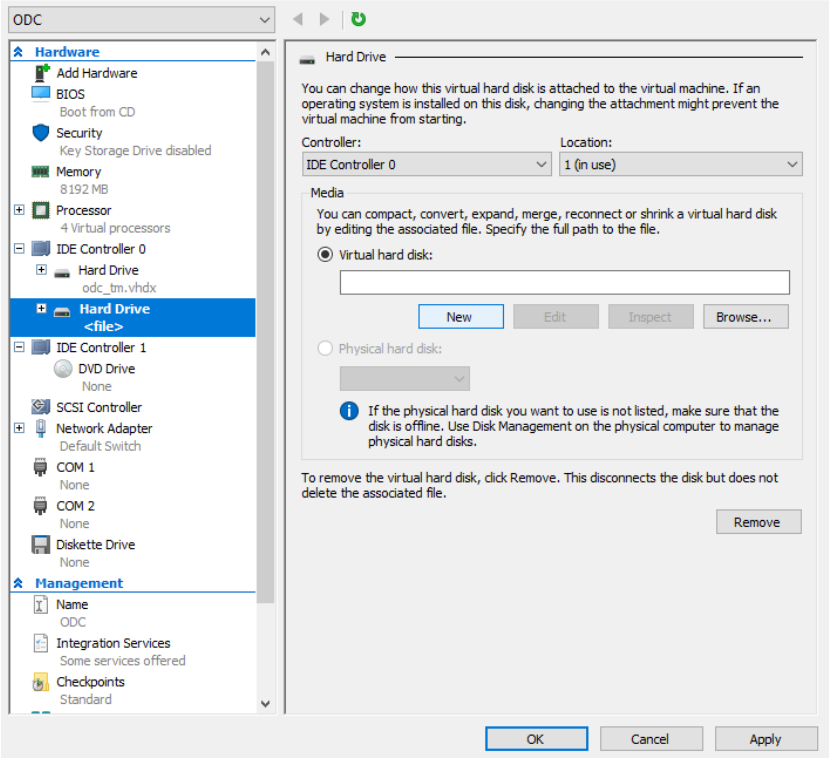
System Migration

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 can include:

- The UUID of the old ODC
- The pattern and firmware downloaded by the old ODC
- The system configurations of 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 Deploying OT Defense Console)
2. Power off the old ODC
3. Click [Browse] and choose an existing disk
4. Attach the external disk of the old ODC to the new ODC
5. The old ODC's information will be migrated into the new ODC



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 on 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.

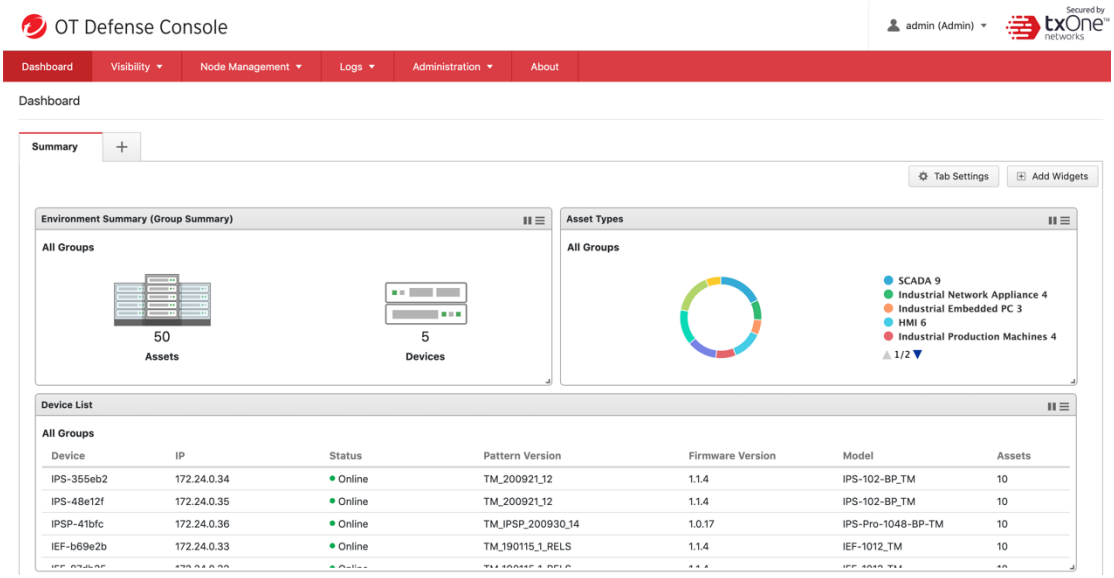
Note: You must change the default login name and password at first log on before you can access the management console.

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.



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