Operational Technology Defense Console – Virtual Appliance 1.0.0

Quick Setup Guide
(for KVM)

2020-02-14

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 KVM

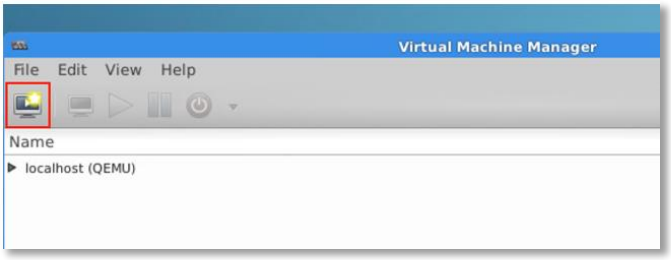
This chapter describes how to deploy OT Defense Console to a KVM.

Prerequisites

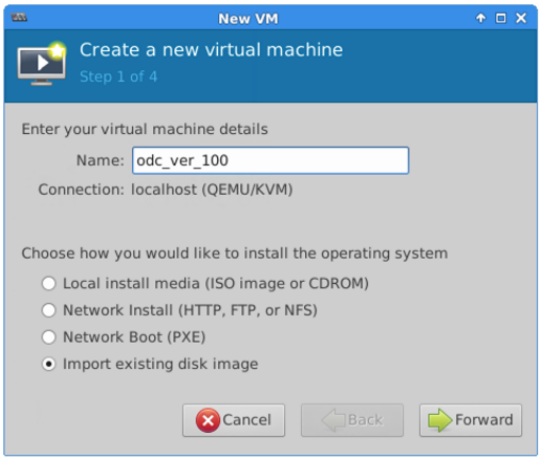
- The qcow2 packages provided by Trend Micro must be available and accessible to KVM 2.0.0.
- The necessary networks have been properly created in KVM.
- An extra disk (with more than 50GB free)

Deploying OT Defense Console

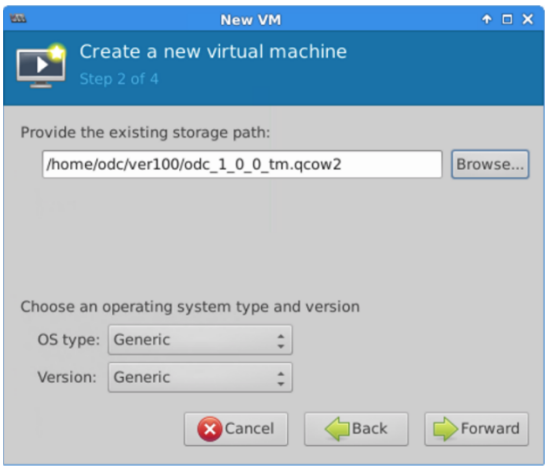
1. Open Virtual Machine Manager.



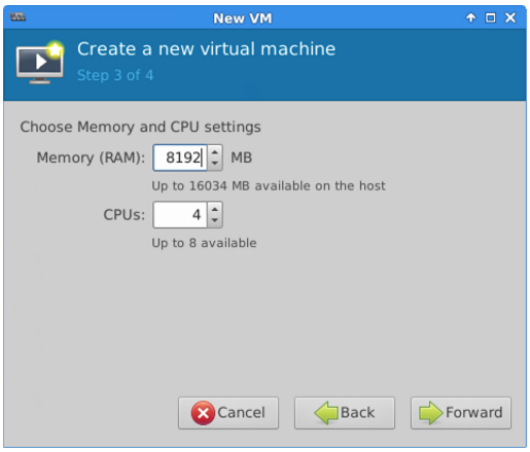
2. Click the [Create a new virtual machine] icon at the left top corner.
3. Input a virtual machine name, and select [Import existing disk image].



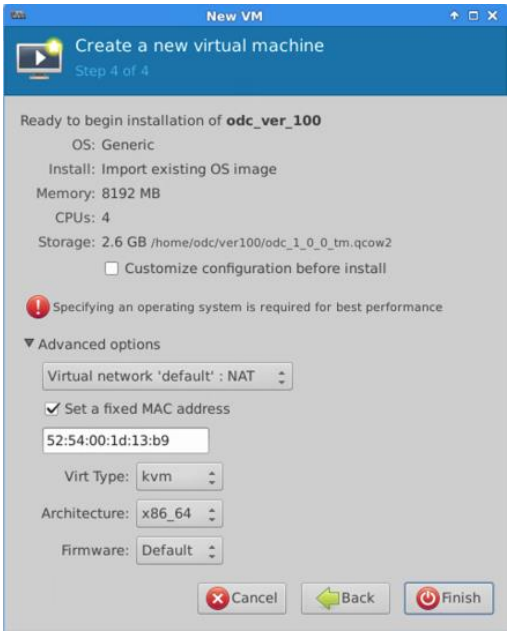
4. Click [Browse] and choose an ODC vm image.



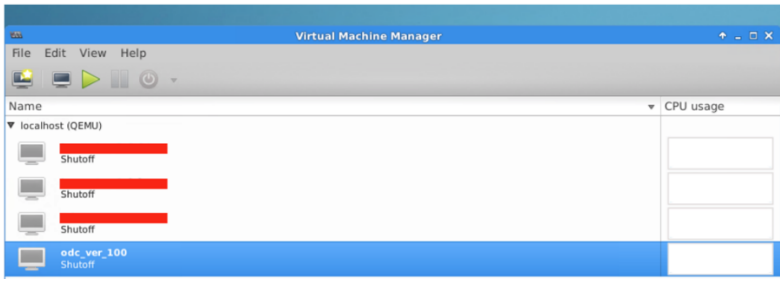
5. Adjust memory allotment and number of CPU cores.



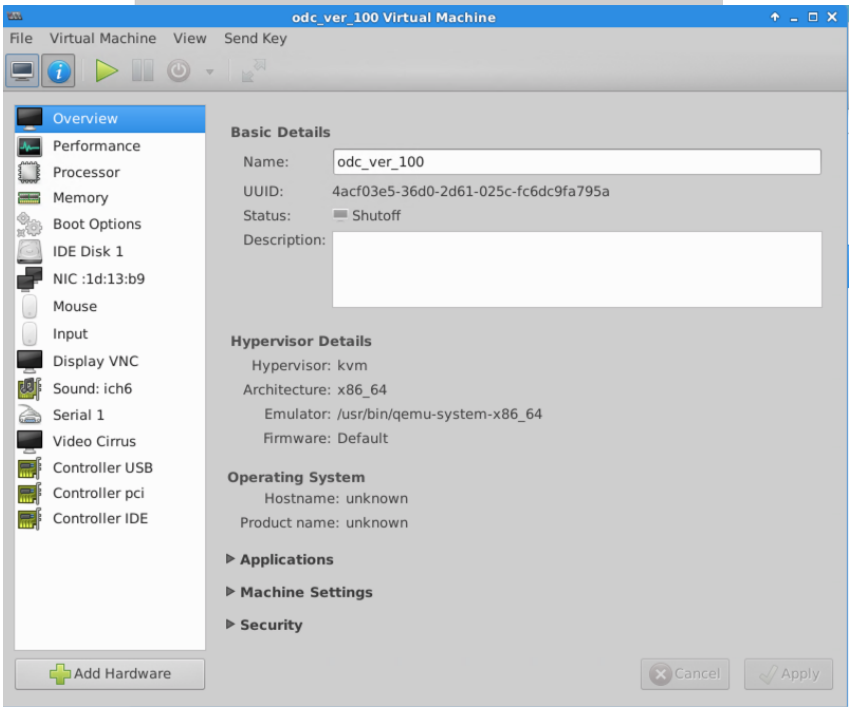
6. Click [Finish].



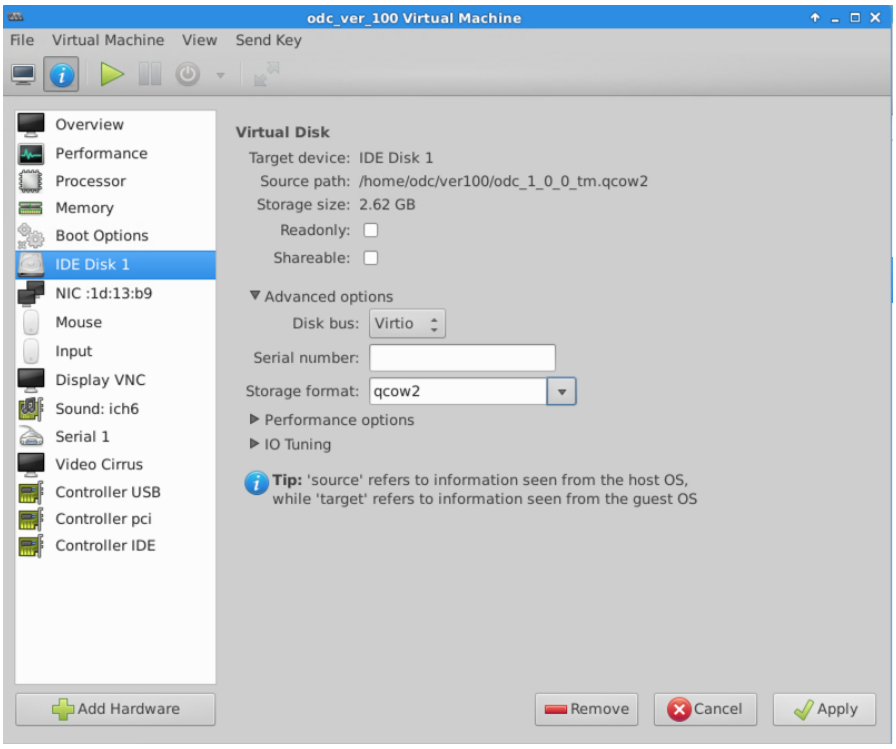
7. The new VM will be shown in the virtual machine list.



8. Click the selected VM and click [Show virtual hardware details].



9. At the bottom left corner, click [Add Hardware]. First, select existing disk, then adjust disk settings. Under [Disk bus] options, choose [Virtio]. Under [Storage format] options, select [qcow2].



10. Add a new disk. We can create a new disk image or select other existing storage.

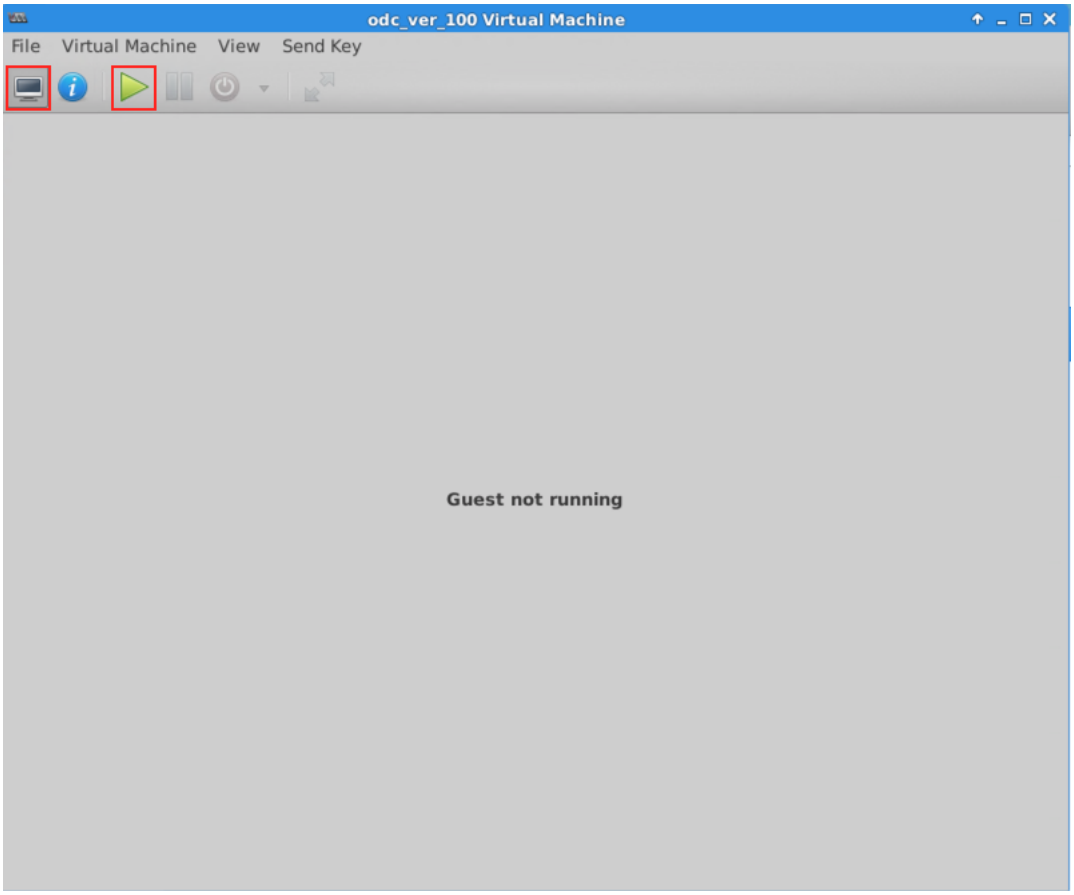
We can decide the external disk size depending on the number of logs to be stored, as shown on the suggestion table below.

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

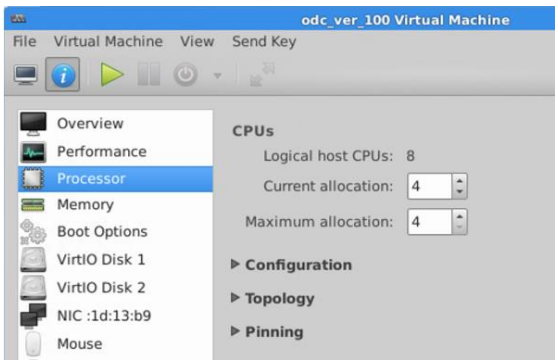
Note: The ODC requires one external disk and the minimum size of the external disk must be above 50GB, otherwise the ODC will not finish initialization and will not complete the boot process.

Note: The 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.

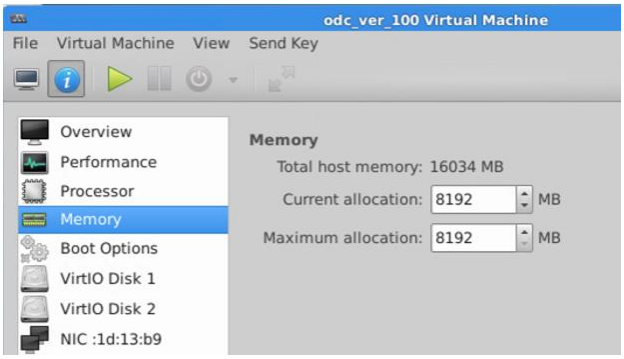
11. Now, the ODC instance will boot.



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



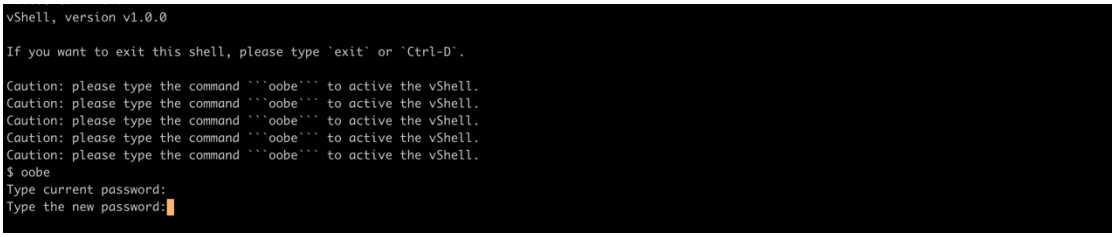
d. Boot the ODC instance.

Sizing Table

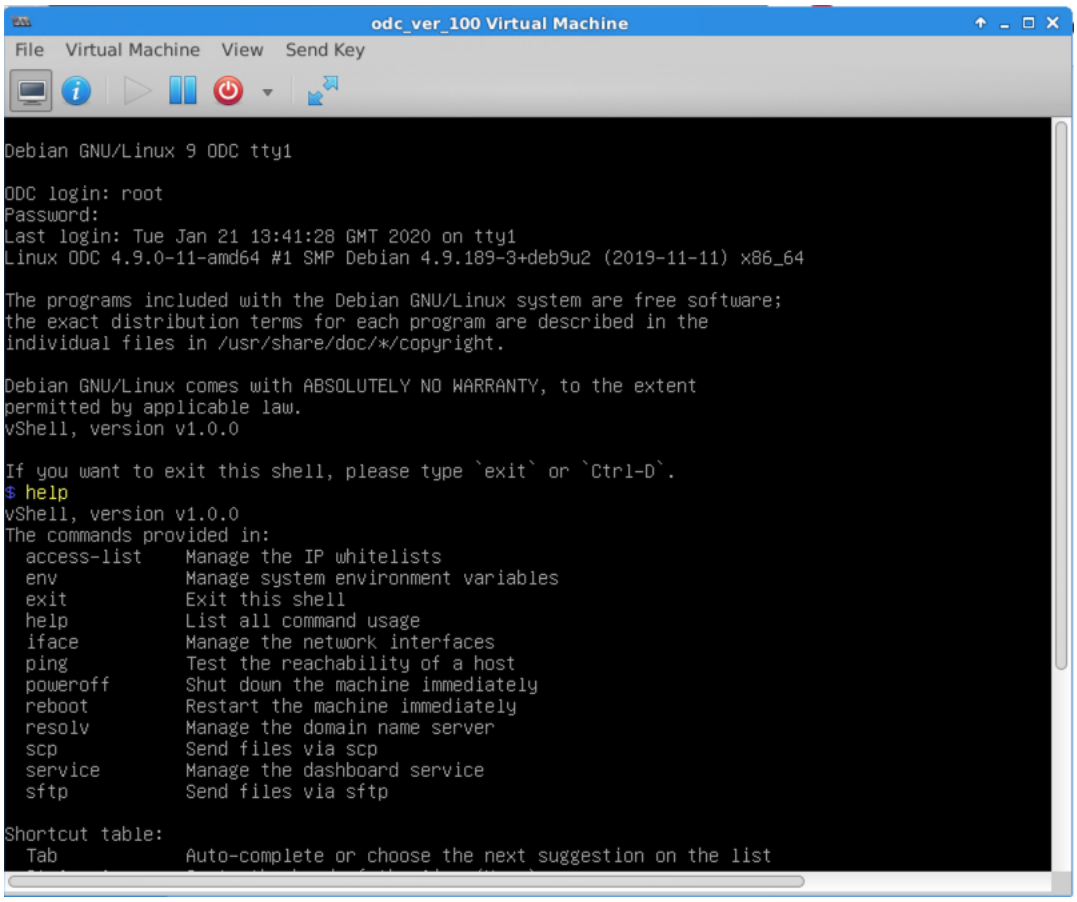
Nodes	CPU	Memory
50	4 cores	8 GB
100	4 cores	16 GB
150	6 cores	16 GB
200	8 cores	16 GB

Accessing the ODC CLI

1. Open the ODC VM console.
2. Login 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



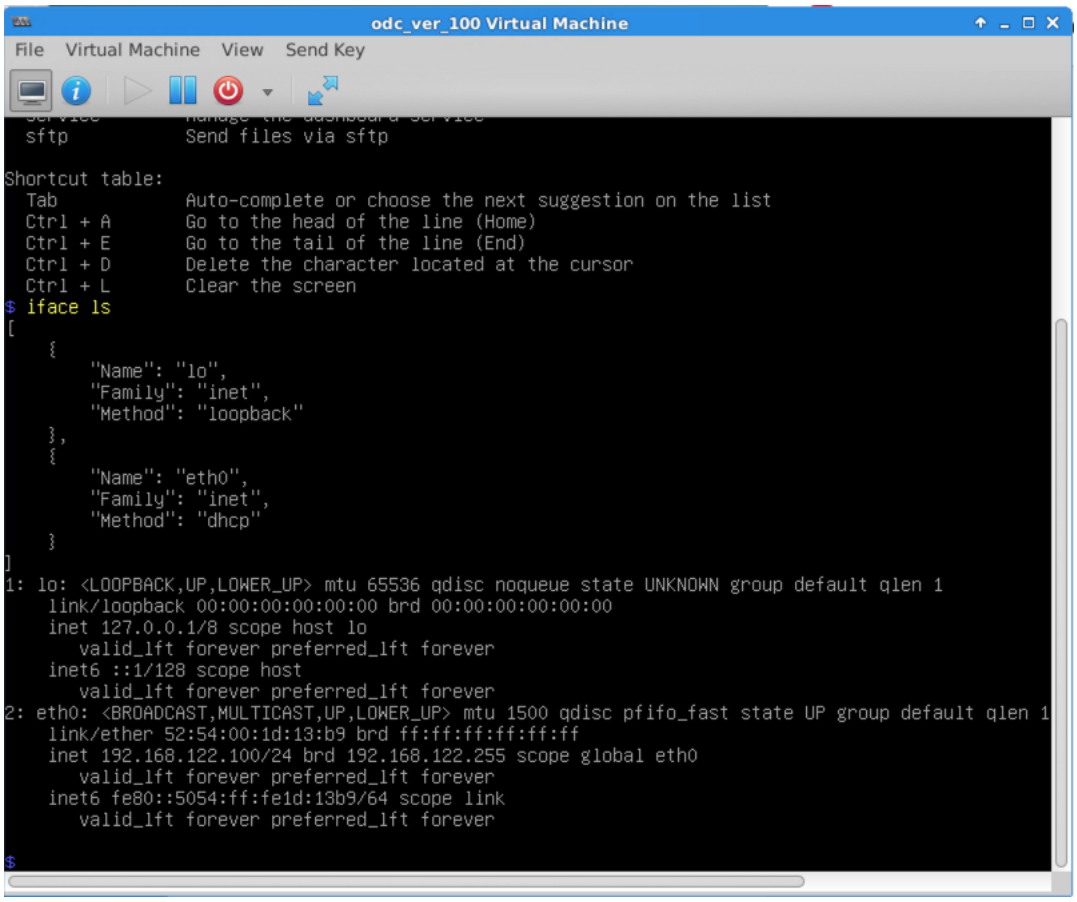
4. After logging into the ODC, you may optionally type the "help" command to see a list of available commands on the instance.



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:

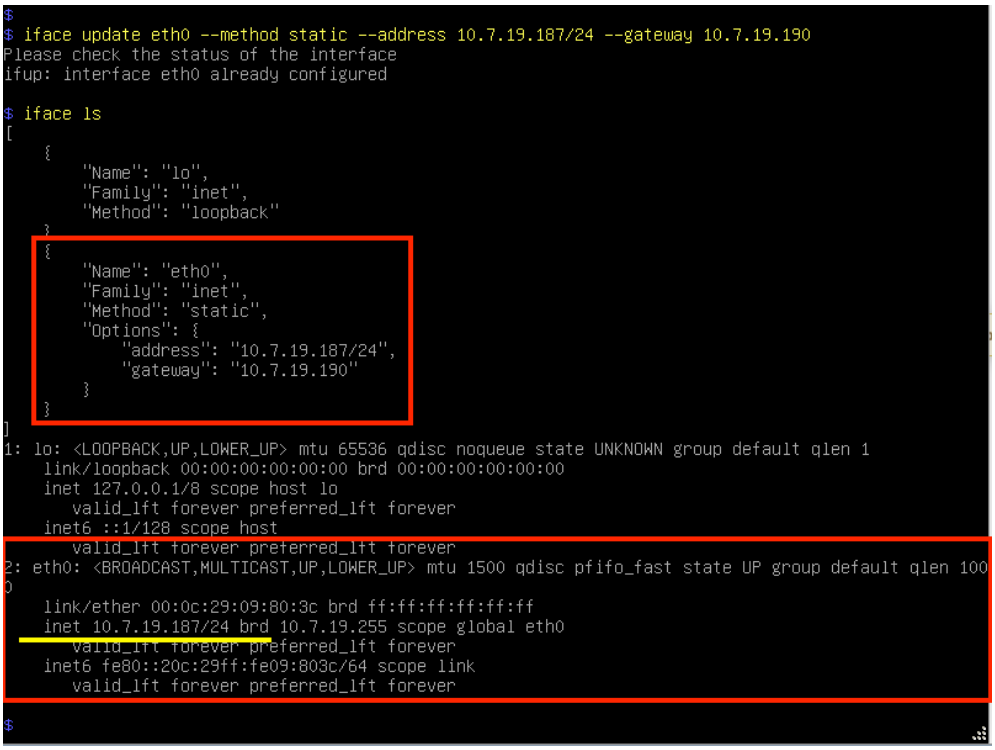
   ```
   $ iface update eth0 --method static --address 10.7.19.187 -netmask
   255.255.255.0 --gateway 10.7.19.190
   ```

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

   ```
   $ iface restart eth0
   ```

3. Input 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 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 login credentials (user name and password).

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

- User ID: `admin`
- Password: `txone`

3. Click Log On.
   If this is your first login, the Login Information Setup frame will appear.

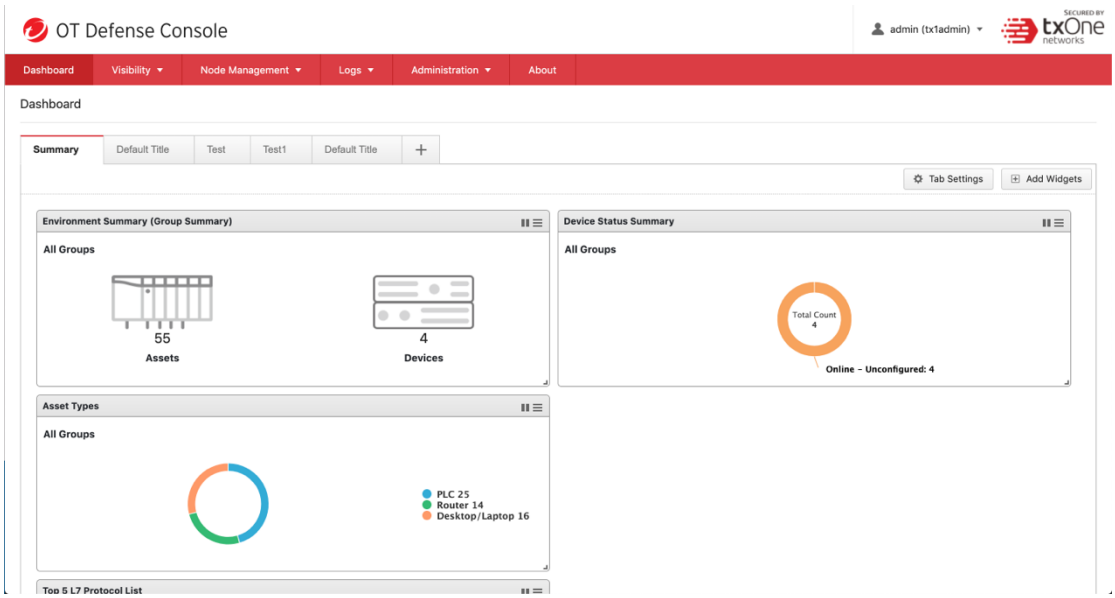
Note: You must change the default login name and password at first login before you can access the management console.

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

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.



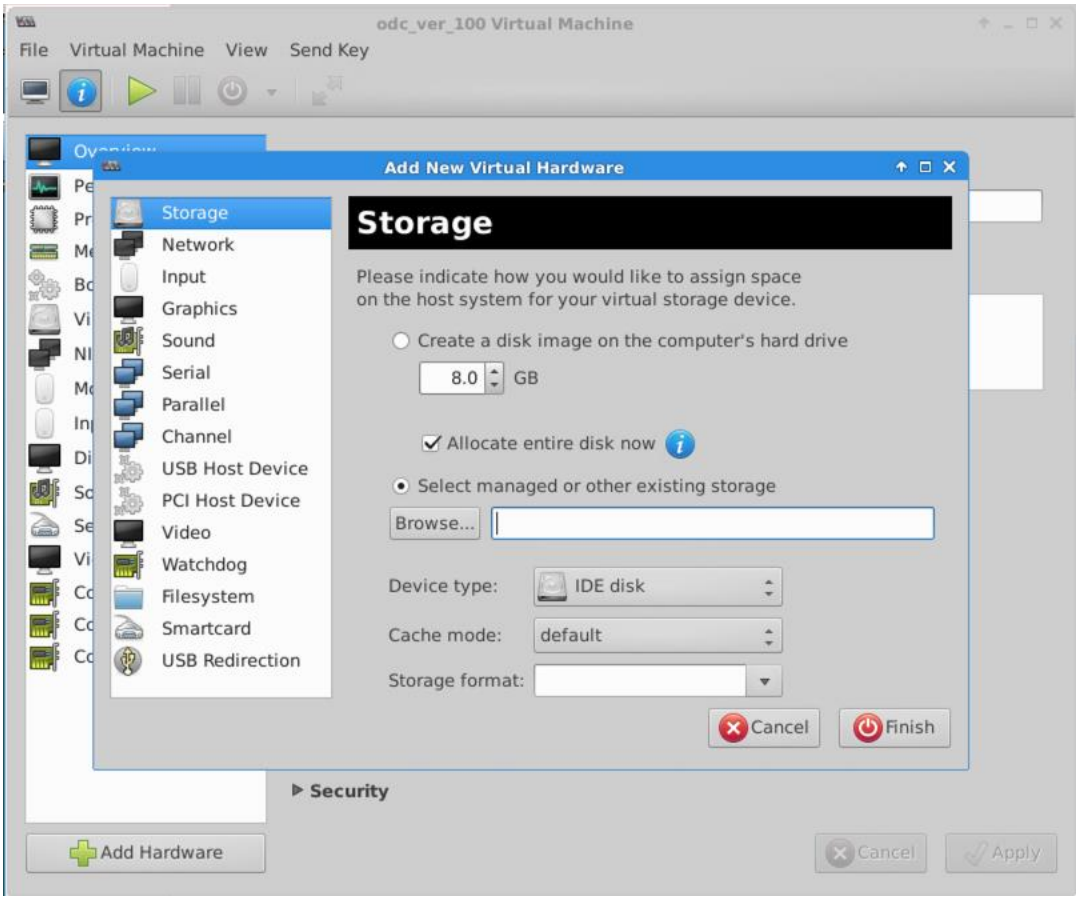
System Migration

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 settings from the old ODC such as its 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 on page 4*)
2. Power off the old ODC
3. Click [Browser] 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.



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