TREND MICRO | txOne networks

1.2 TXOne StellarOne™

Patch 1

Installation Guide (for Windows Hyper - V)

Unify your cyber security posture with one centralized console

TXOne Networks 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 theapplicable documentation, which are available from the TXOneNetworks website at:

http://docs.trendmicro.com/en-us/enterprise/txone-stellarenforce.aspx and

http://docs.trendmicro.com/en-us/enterprise/txone-stellarprotect.aspx

Document Part No.: SLEM19520/220624
Release Date: June 2022
Protected by U.S. Patent No.: Patents pending.

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 TXOne Online Help Center and/or the TXOne Knowledge Base.

TXOne always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any TXOne document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:
http://docs.trendmicro.com/en-us/survey.aspx

Privacy and Personal Data Collection Disclosure

Certain features available in TXOne products collect and send feedback regarding product usage and detection information to TXOne. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want TXOne to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that TXOne StellarOne collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by TXOne is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

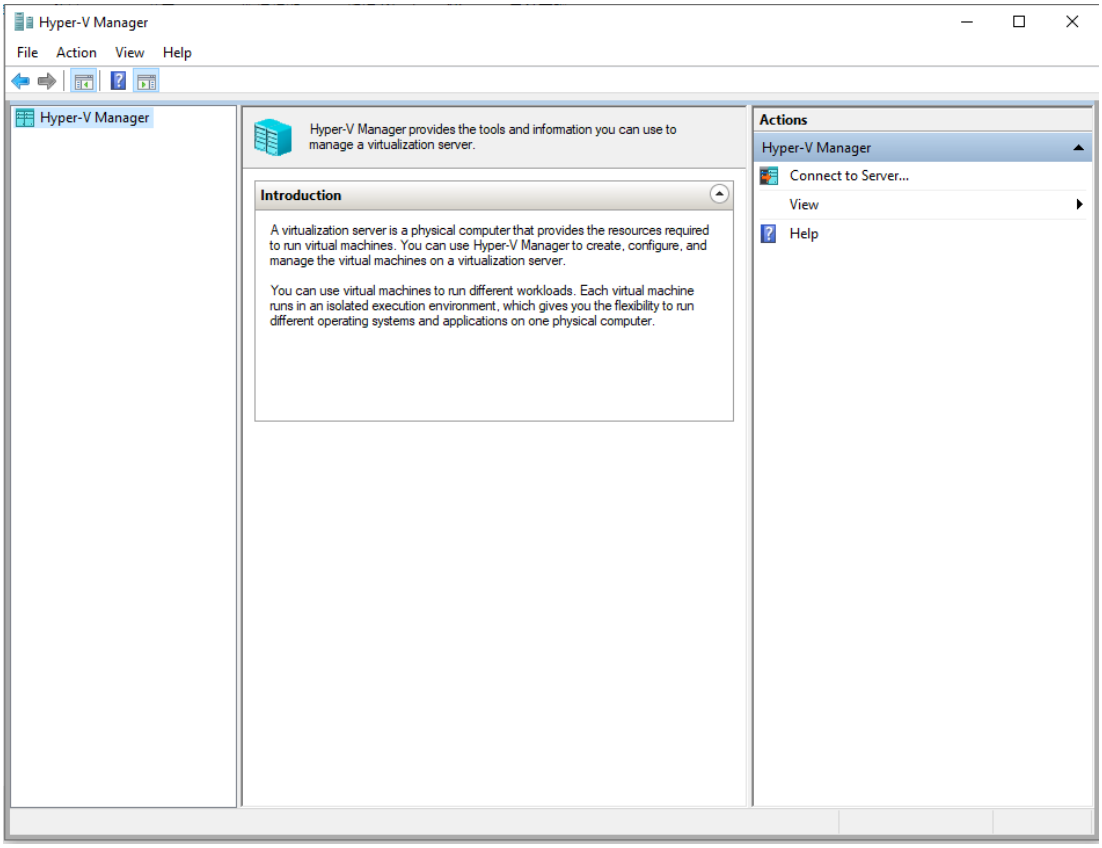
Table of Contents

StellarOne Onboarding to Windows Hyper-V

This chapter describes how to deploy Stellar One to a Hyper-V system.

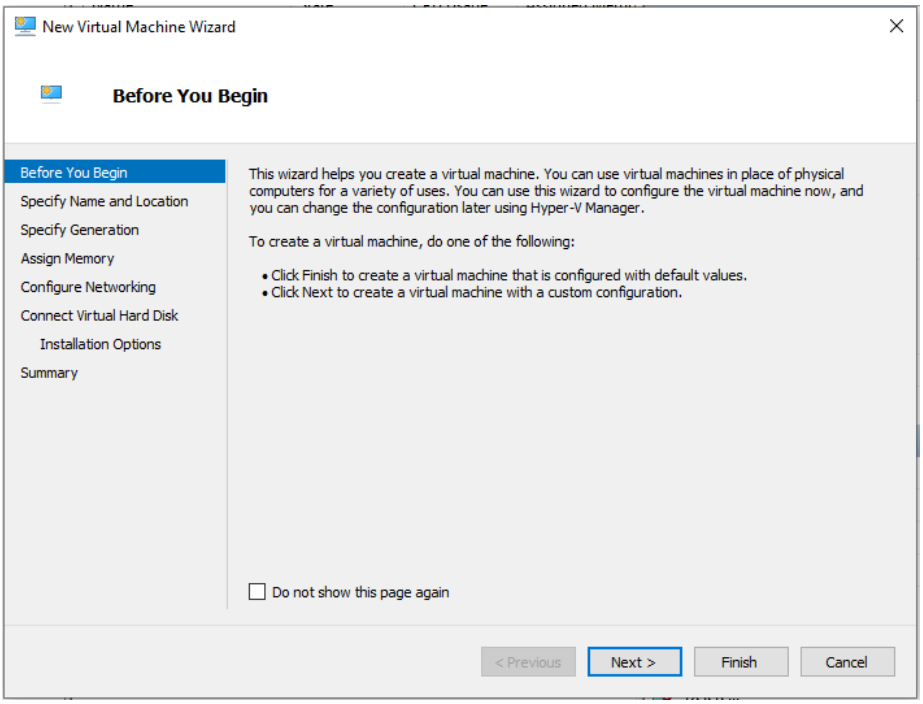
Prerequisites

- 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)

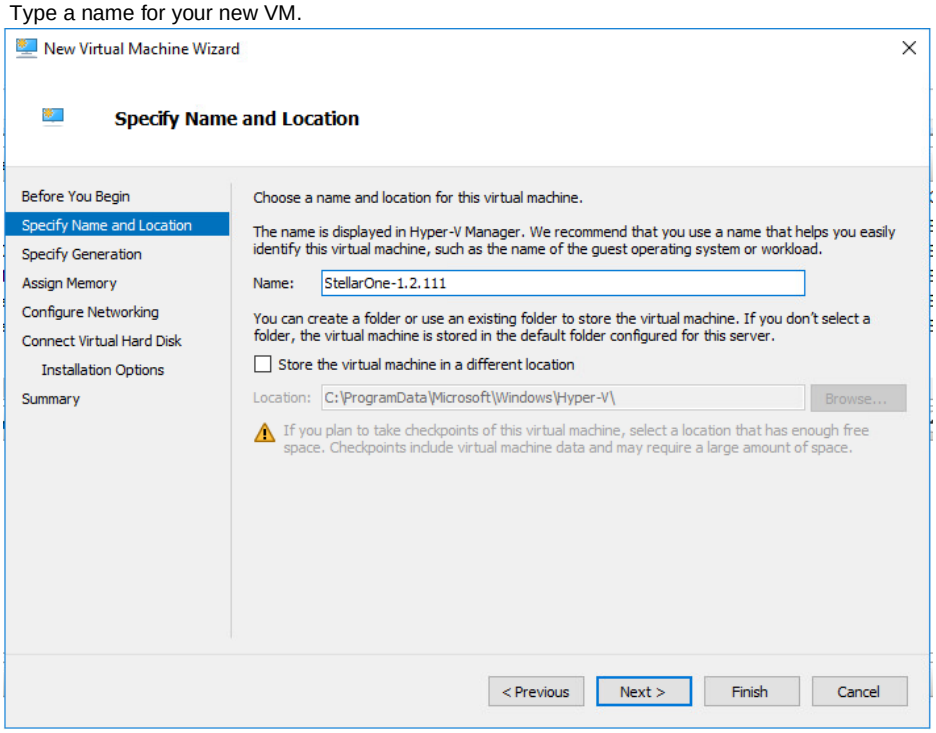


Deploying Stellar One Console

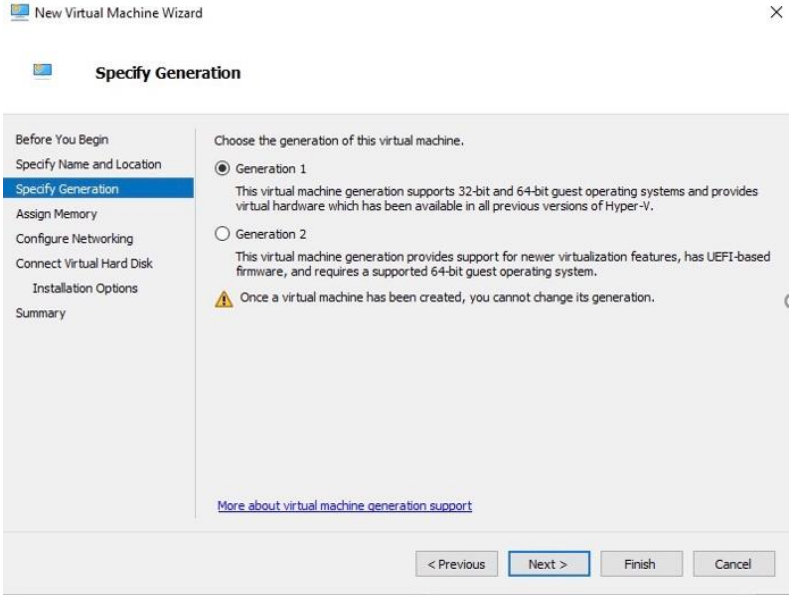
1. Launch Hyper-V manager.
2. Under [Actions], click [New] and then click [Virtual Machine].



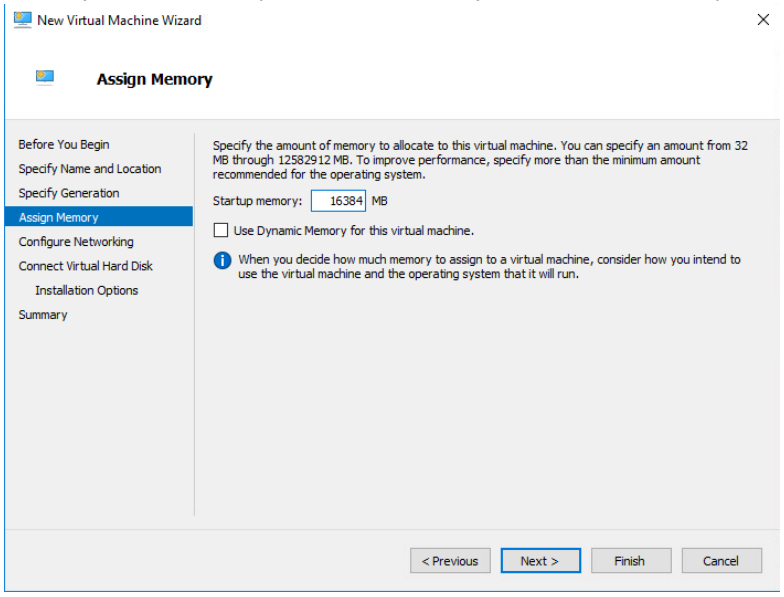
3. Type a name for your new VM.



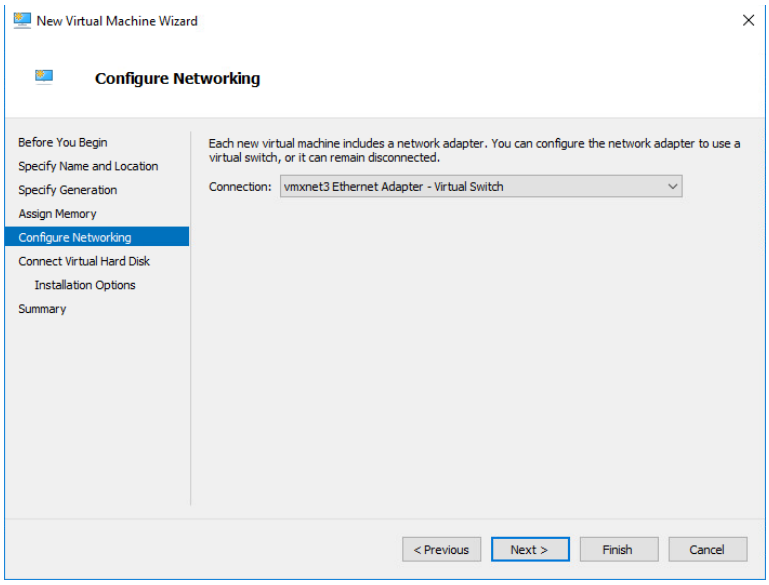
4. Specify the VM's Generation. Current StellarOne only support Hyper-V Generation 1.



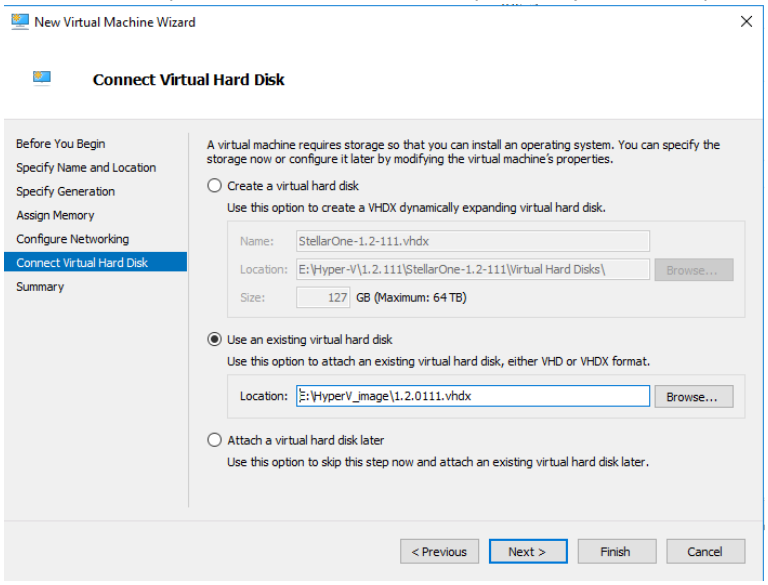
5. Allocate memory for the new VM. (StellarOne min Memory need 16GB = 16384MB)



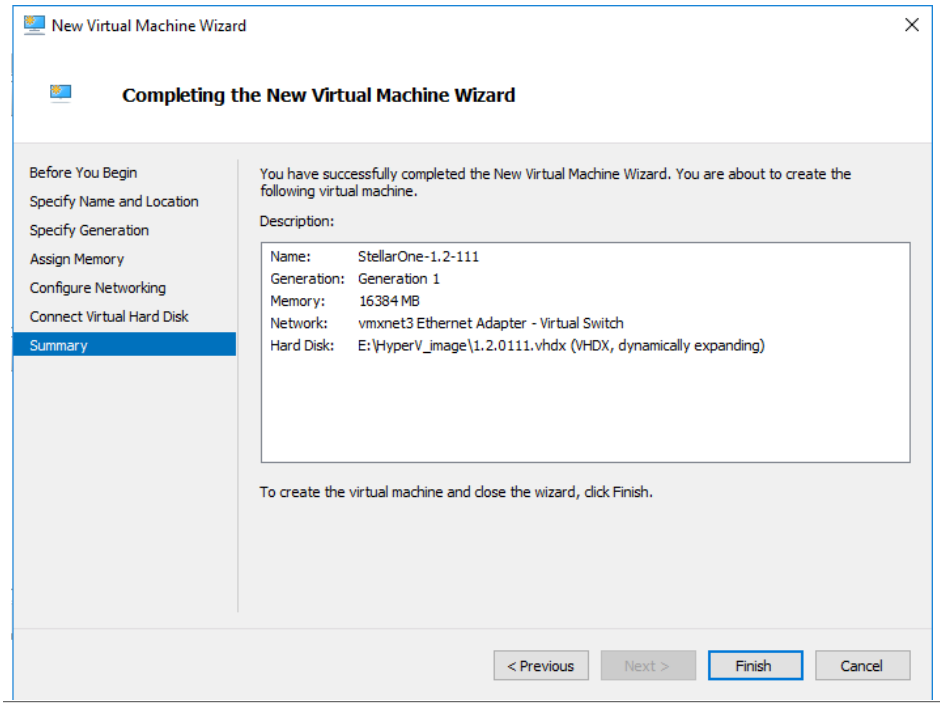
6. Configure the VM's networking settings.

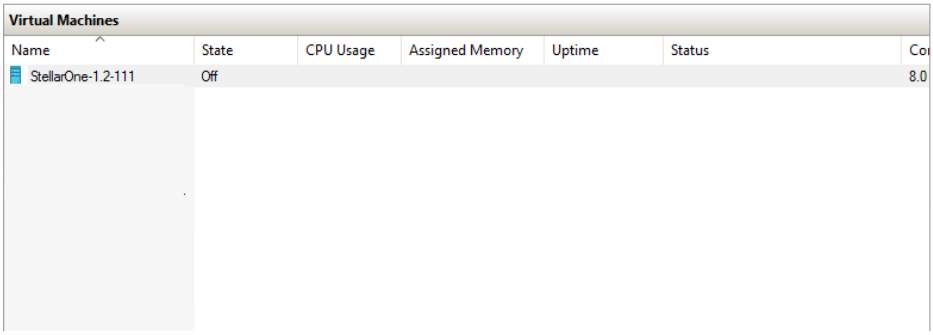


7. Select a virtual hard disk (choose the StellarOne vhdx file provided by Trend Micro).

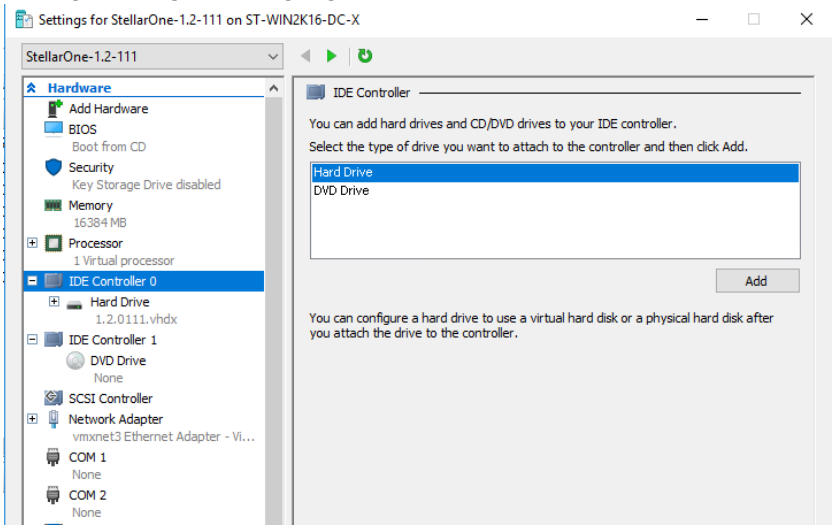


8. Check your settings then click [finish].

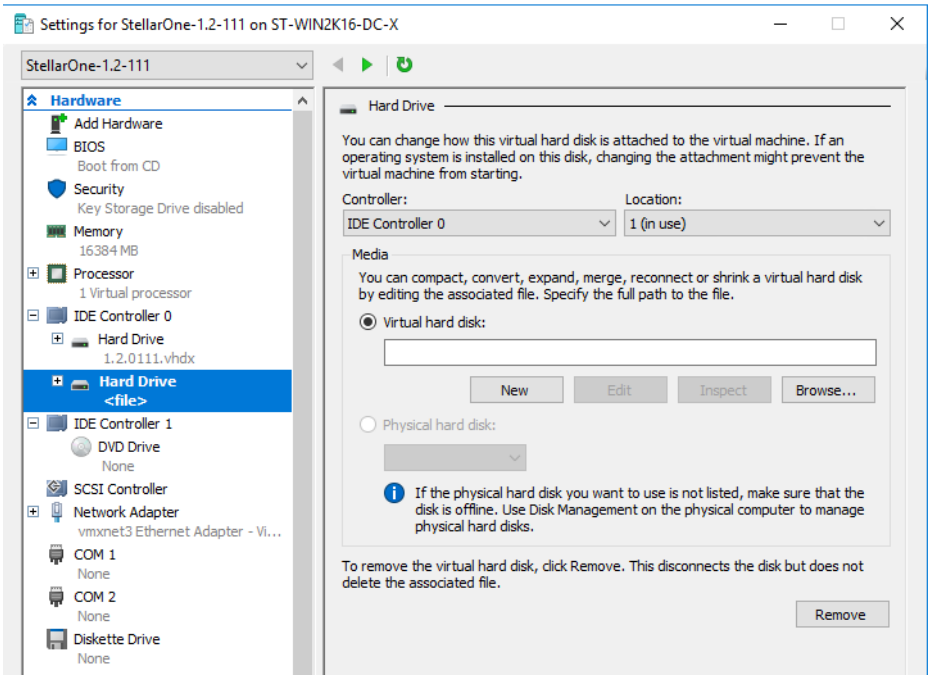




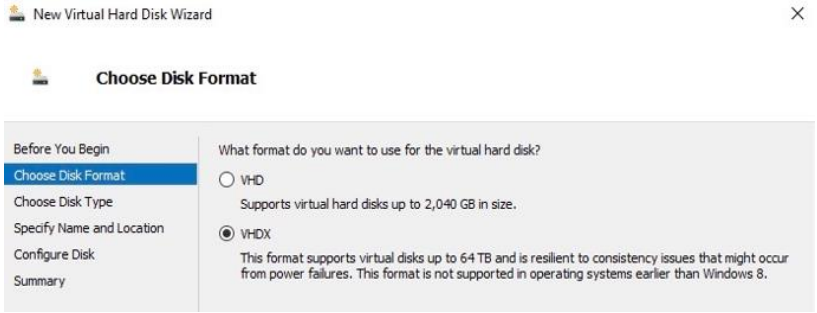
9. Add a new disk.
   a. Select Virtual machine, Right click menu select [Settings].
   b. Select [Hard Disk], then click [Add].



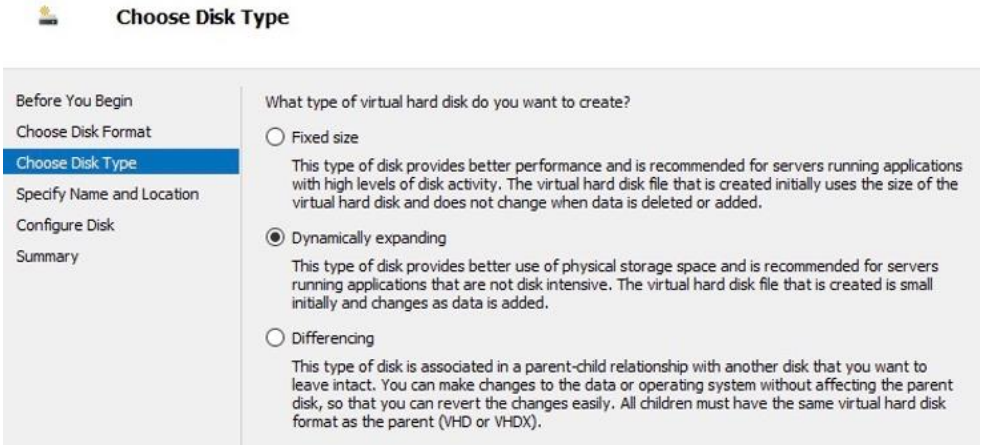
   c. Click [New].



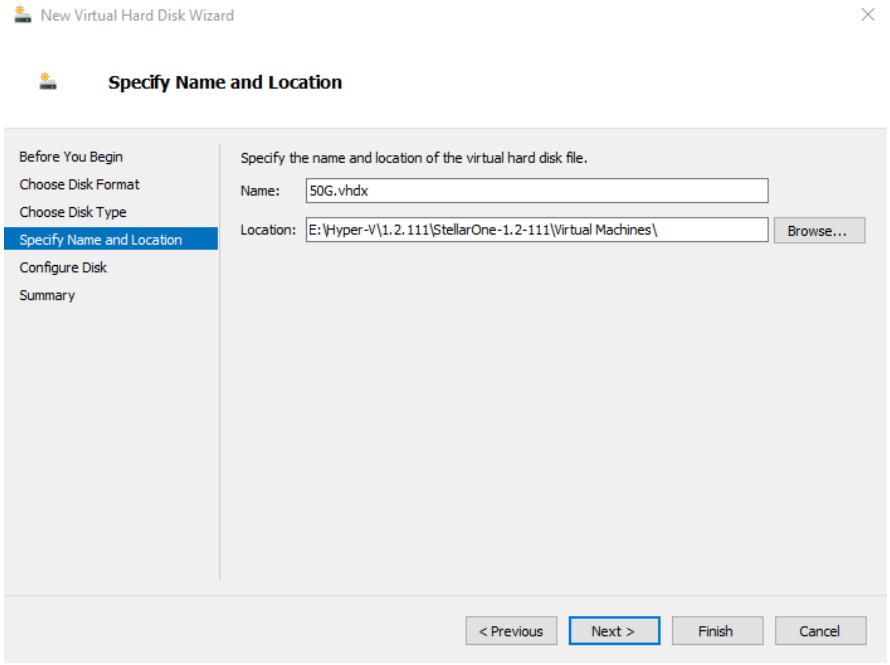
d. Choose the VHDX disk format.



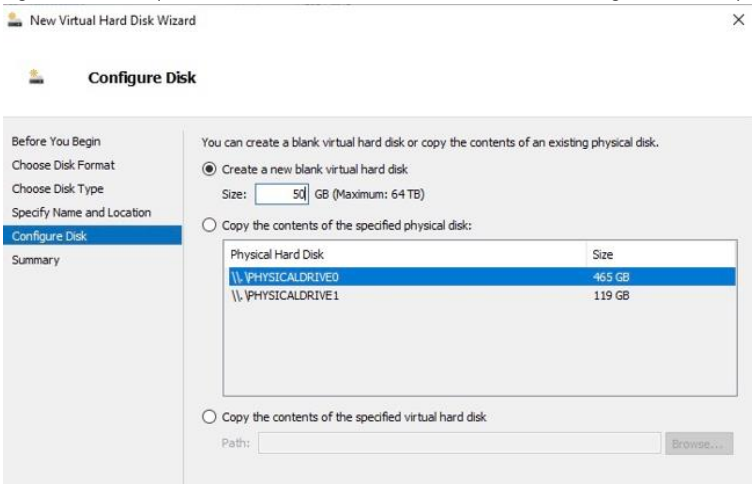
e. Choose the disk type [Dynamically expanding].



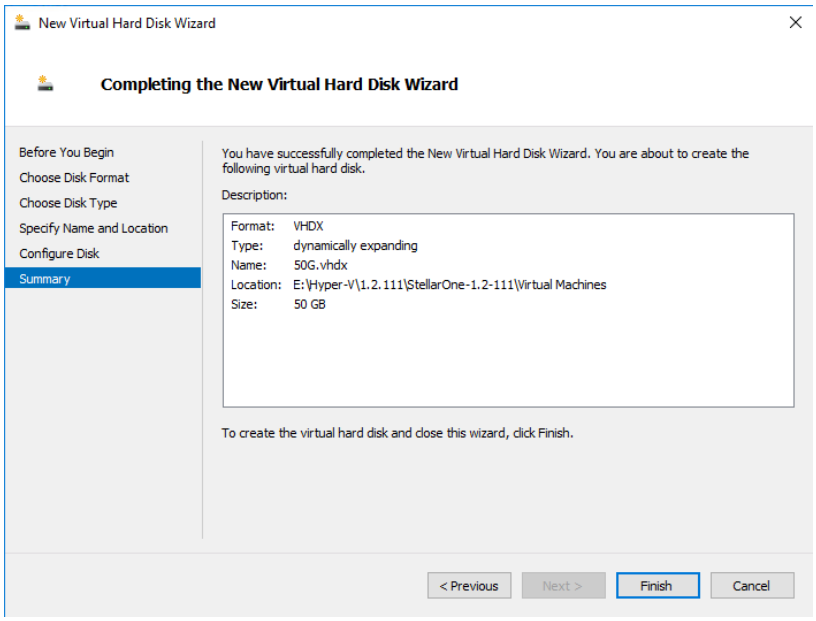
f. Specify name and location.



g. Configure disk size (STELLAR ONE's disk size is based on the sizing table below).



h. 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.

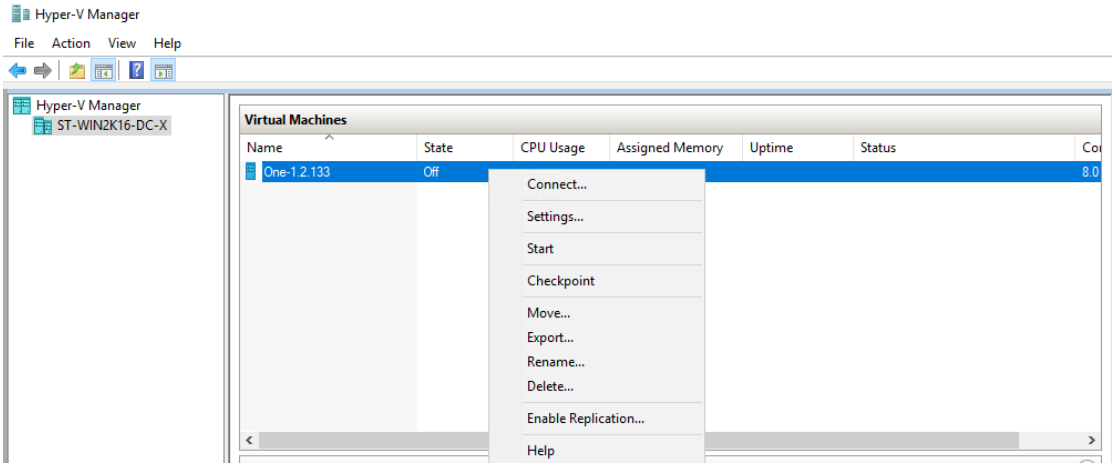
#of Logs	Disk
5,000,000	50 GB
10,000,000	150 GB
50,000,000	300 GB
100,000,000	500 GB

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

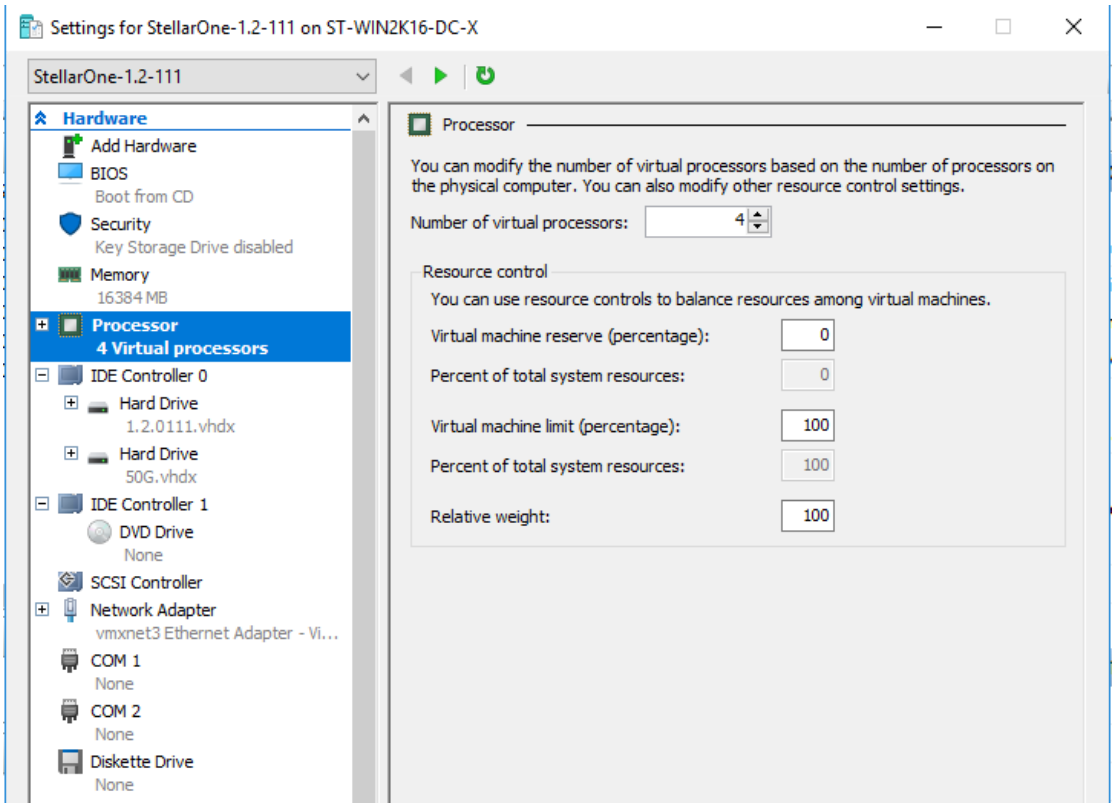
Note: The external disk is used to store the system configurations and event logs. You may attach the external disk of a terminated STELLAR ONE instance here instead of adding a new disk if you want to migrate the previous configurations and logs to the new Stellar One instance.

10. **(Optional)** Adjust your STELLAR ONE instance to use proper resource configurations based on the following sizing table or at least using default settings (4 CPU cores, 16 GB of memory).

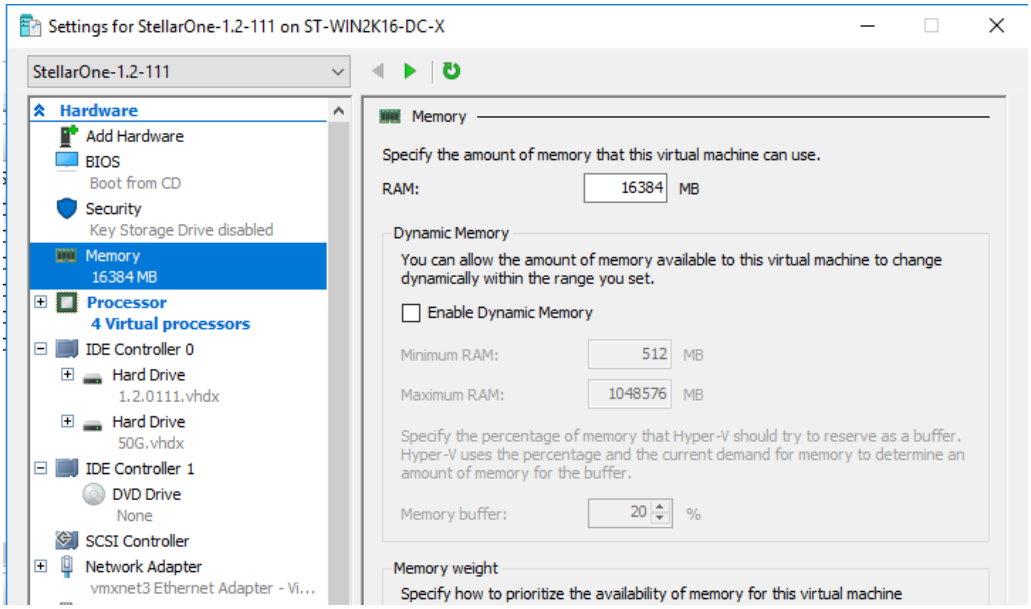
a. Shut down the instance of STELLAR ONE and click [Settings].



b. Configure the number of CPU cores



c. Configure the amount of memory.



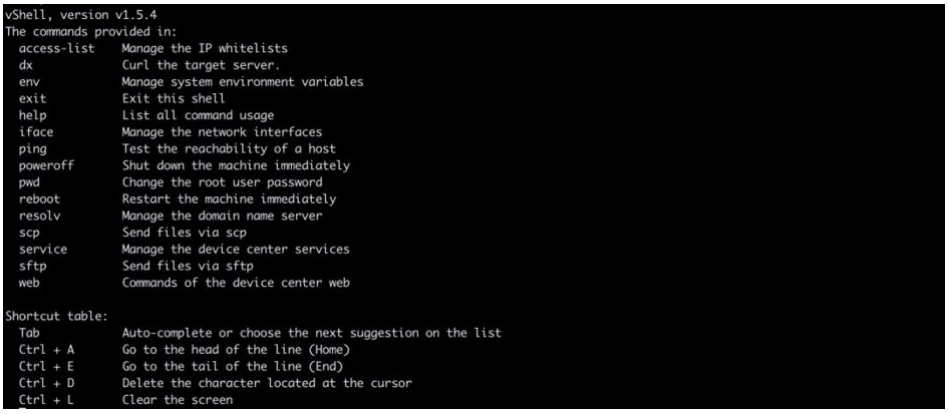
d. Boot the STELLAR ONE instance.

Sizing Table

Agents	CPU	Memory
500	4 cores	8 GB
1,000	4 cores	16 GB
5,000	8 cores	16 GB
10,00	8 cores	16 GB
15,000	8 cores	16 GB
20,000	8 cores	16 GB
30,000	10 cores	24 GB

Accessing the STELLAR ONE CLI

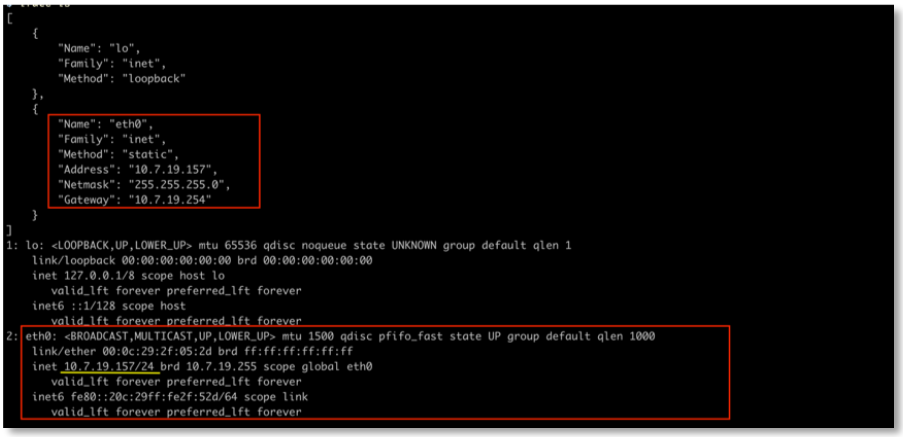
1. Open the STELLAR ONE VM console.
2. Login with “root / txone”
3. After logging into the STELLAR ONE, you may optionally type the “help” command to see a list of available commands on the instance.



Getting the IP Address of the STELLAR ONE Instance

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

   $ iface ls



[Optional] Configure the IP Address Settings

You can choose to configure the IP address manually.

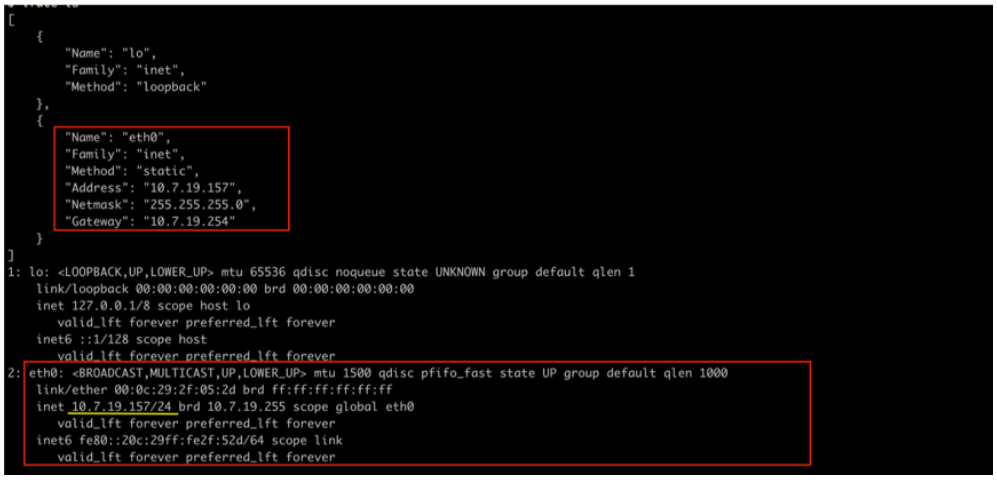
1. Use the “iface update” command to update the settings of an existing network interface. For example, the following command sets the interface “eth0” to a static IP address 10.7.19.187/24 with the Gateway IP address 10.7.19.190:

   $ 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:

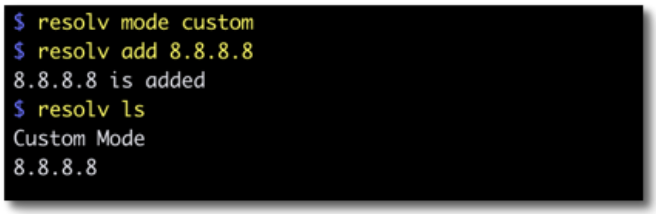
   $ iface restart eth0

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

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-insensitive).

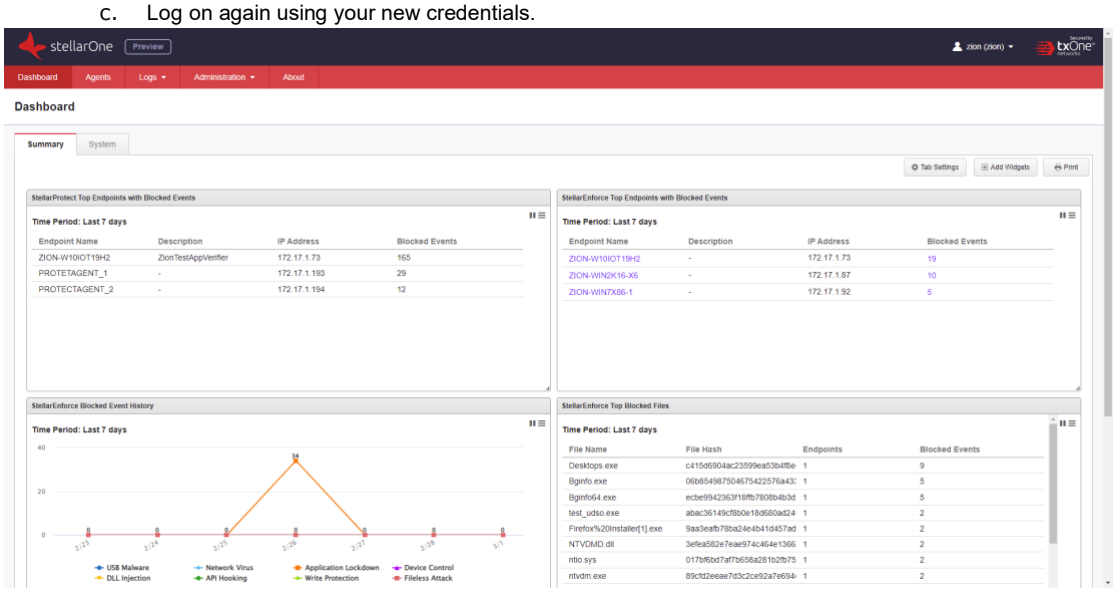
   a. Confirm your password settings.

      - 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.



Appendix A

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
STELLAR ONE	Operational Technology Defense Console
OT	Operational Technology
OT Defense Console	Operational Technology Defense Console
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition