txOne networks | Keep the Operation Running

TXOne StellarOne

3.0 Service Pack 1

Installation Guide

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 the applicable documentation, which are available at:

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

TXOne Networks, StellarOne, StellarProtect, and StellarProtect (Legacy Mode) are trademarks or registered trademarks of TXOne Networks Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2023. TXOne Networks Incorporated. All rights reserved.

Document Part No.: APEM39830/230913

Release Date: September 2023

Protected by U.S. Patent No.: Patents pending.

Privacy and Personal Data Collection Disclosure

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

The following link outlines the types of data that TXOne Networks, StellarOne, StellarProtect, and StellarProtect (Legacy Mode) collect 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 Networks is subject to the conditions stated in the TXOne Networks Privacy Notice:

https://www.txone.com/privacy-policy/

Table of Contents

Preface

Preface v
About the Documentation v
Audience vi
Document Conventions vi
Terminology vii

Chapter 1: Introduction

About TXOne Stellar 1-2
Key Features and Benefits 1-3
What's New 1-5

Chapter 2: Installation Planning

System Requirements 2-2
Hardware Requirements 2-2
Hardware Requirements for VMware System 2-3
Hardware Requirements for Hyper-V System 2-5
Deciding an Instance Type for StellarOne on AWS EC2 Platform 2-7
Planning Network Bandwidth for Agent Deployment 2-9
Ports and FQDN Used 2-10
Supported Agent Versions 2-12

Chapter 3: Installation

StellarOne Installation Flow 3-2
StellarOne Onboarding to VMware ESXi 3-2
Prerequisites 3-2
Deploying StellarOne on the VMware ESXi 3-2

StellarOne Onboarding to Windows Hyper-V 3-12
Prerequisites 3-12
Deploying StellarOne to a Hyper-V System 3-12
StellarOne Onboarding to AWS EC2 3-29
Prerequisites 3-29
Deploying StellarOne on AWS EC2 3-30
Accessing StellarOne via SSH 3-37
Associating the Elastic IP Address with an Instance . 3-39
Opening StellarOne Management Console 3-43
Getting the License File 3-46
OT Intelligent Trust 3-48

Chapter 4: Configuring StellarOne via Command Line Interface (CLI)

Using the StellarOne Command Line Interface (CLI) 4-2
Configuring the IP Address via CLI 4-3
Configuring the Advertise Address via CLI 4-6
Modifying Communication Ports via CLI 4-9
Changing Language Settings via CLI 4-11
Managing Docker Network via CLI 4-13
Reseting Administrator's Password via CLI 4-13

Chapter 5: Upgrade

Supported Upgrade Paths 5-2
Upgrade Methods 5-3
Firmware Upgrade 5-3
Mount Upgrade (VMware) 5-4
Mount Upgrade (Hyper-V) 5-7

Chapter 6: Getting Help and Troubleshooting

Troubleshooting Resources 6-2
Self-Diagnosis 6-2
Resolving Low Disk Space Issues 6-2
Using the Support Portal 6-3
Threat Encyclopedia 6-4
Contacting Trend Micro and TXOne 6-5
Speeding Up the Support Call 6-6
Sending Suspicious Content to Trend Micro 6-6
Email Reputation Services 6-6
File Reputation Services 6-6
Web Reputation Services 6-7
Other Resources 6-7
Download Center 6-7

Index

Index IN-1

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.

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

Preface

This Installation Guide introduces TXOne StellarOne™ and guides administrators through installation and deployment.

Topics in this chapter include:

- *About the Documentation on page v*
- *Audience on page vi*
- *Document Conventions on page vi*
- *Terminology on page vii*

About the Documentation

TXOne StellarOne™ documentation includes the following:

Documentation	Description
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the other documents.
Installation Guide	A PDF document that discusses requirements and procedures for installing StellarOne
Administrator's Guide	A PDF document that discusses StellarOne agent installation, getting started information, and server and agent management
Online Help	HTML files that provide "how to's", usage advice, and field-specific information
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following websites: https://kb.txone.com/ http://success.trendmicro.com

Audience

TXOne StellarOne™ documentation is intended for administrators responsible for StellarOne management, including agent installation. These users are expected to have advanced networking and server management knowledge.

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes
Tip	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations

Convention	Description
WARNING!	Critical actions and configuration options

Terminology

The following table provides the official terminology used throughout the TXOne StellarOne™ documentation:

Terminology	Description
server	The StellarOne console server program
server endpoint	The host where the StellarOne server is installed
agents	The host running the StellarProtect program
managed agents managed endpoints	The hosts running the StellarProtect program that are known to the StellarOne server program
target endpoints	The hosts where the StellarOne managed agents will be installed
Administrator (or StellarOne administrator)	The person managing the StellarOne server
StellarOne (management) console	The user interface for configuring and managing StellarOne settings and the agents managed by StellarOne
CLI	Command Line Interface
license activation	Includes the type of StellarOne server installation and the allowed period of usage that you can use the application

Terminology	Description

agent installation folder	The folder on the host that contains the StellarProtect agent files. If you accept the default settings during installation, you will find the installation folder at one of the following locations:
	`C:\Program Files\TXOne\StellarProtect`
	`C:\Program Files\TXOne\StellarProtect (Legacy Mode)`

Chapter 1

Introduction

This section introduces TXOne StellarOne™ and provides an overview of its features.

Topics in this chapter include:

- *About TXOne Stellar on page 1-2*
- *Key Features and Benefits on page 1-3*
- *What's New on page 1-5*

About TXOne Stellar

TXOne Stellar provides a context-focused security solution for OT endpoints and cyber-physical systems (CPS), aiming to defend operation stability with continuous detection and response aligned to the specific requirements of the OT domain.

TXOne Stellar platform is composed of the centralized management console server and unified agents apt for legacy OT devices and modern cyber-physical systems.

- StellarOne™ , designed to streamline administration of the agents installed on modernized systems and legacy systems, along with its intuitive centralized management, consistent policy enforcement, and action-oriented alerts that empower security teams of all sizes and skill levels to successfully mature their organization's security posture.
- StellarProtect™ / StellarProtect (Legacy Mode), using the single-agent design that delivers seamless asset-centric protection and ensures coverage for modern CPS and legacy OT devices throughout their entire asset lifecycle. The lightweight unified agent simplifies security by combining CPS Detection and Response (CPSDR), threat prevention, operations lockdown, and device control.
    - CPSDR: Embodied within the advanced Operations Behavior Anomaly Detection feature, which establishes a unique baseline fingerprint of each agent-device during practicable operating states and performs fingerprint deviation analysis by means of an expansive industrial application repository and ransomware detection engine to defend against unexpected changes that may impact stability.

      Moreover, TXOne Stellar brings the contextualization of security into an operation-led view to allow both the operation and security teams to achieve their goals without needing to compromise. To illustrate, if a device suddenly tried to start launching different applications, it would be blocked from doing so.

      From the operation view, this may be an unplanned auto-update that, if run, would take the device offline to reboot. From a security

view, this could be an attempt to access an encryption library that is about to be used to execute ransomware. By applying the operation context, both security and operation-initiated changes can be detected, and appropriate responses are taken.

In both cases, CPSDR stopped the event before it could occur. The security team followed up and resolved the ransomware infection in a different part of the environment. The operation team scheduled the required update for during an upcoming planned maintenance window.

- Multi-Method Threat Prevention: Provides advanced threat scan on the basis of ICS root of trust and operations-focused machine learning to secure the agent-devices against known and unknown malware threats without compromising operational availability.
- Operations Lockdown: For fixed-function and devices with limited patching availability,operations lockdown enforcement prohibits unauthorized changes, including alterations to registry and function parameters.
- Trusted Peripheral Control: Unauthorized access from external sources, such as USB devices, is configurable and controlled to reduce physical access threats.

Leveraging an expansive ICS application and certificate library and exclusive ransomware detection engine, TXOne Stellar maintains CPS operational integrity through behavioral anomaly detection and eliminates configuration drift for legacy and fixed-use assets with device lockdown. Security teams can confidently deliver detection and response outcomes across the OT terrain, with TXOne Stellar effectively secure organization's security posture while maintaining its business operations stability.

Key Features and Benefits

The TXOne StellarOne™ management console provides following features and benefits.

TABLE 1-1. Features and Benefits

FEATURE	BENEFIT
Cyber-Physical System Detection and Response (CPSDR)	The CPSDR requires a deep understanding of what the expected behaviors for each device are. Embodied within the advanced Operations Behavior Anomaly Detection feature, which primarily defends against unexpected changes that may impact operational stability by comparing daily operation processes and behaviors with a unique baseline of each agent-device and performing comprehensive behavioral analysis not only via identifying baseline deviation but also using TXOne Networks' exclusive industrial application repository and ransomware detection engine.
Dashboard	The Dashboard provides an overview of the CPS situational awareness and deployment status at the centralized control level, along with the montiored agent events and StellarOne console's system status. Administrators can check deployed agent status easily, have quick access to the detected events for further investigation or actions if needed, and can generate security reports (Legacy Mode only) related to specific agent activity for specified periods.

Feature	Benefit
Centralized Agent Management	StellarOne allows administrators to perform the following tasks: • Monitor StellarProtect/StellarProtect (Legacy Mode) agent status • Examine connection status • View configurations • Collect agent logs on-demand or by policy (Legacy Mode only) • Turn agent Application Lockdown on or off • Enable or disable agent Device Control • Configure agent Maintenance Mode settings • Update agent components • Initialize the Approved List • Deploy agent patches • Add trusted files and USB devices • Export agents' information • Import/Export agents' configuration settings or Approved List (Legacy Mode only)
Centralized Event Management	On endpoints protected by StellarProtect/StellarProtect (Legacy Mode) agents, administrators can monitor status and events, as well as respond when files are blocked from running. StellarOne provides event management features that let administrators quickly know about and take action on the blocked-file events.
Server Event Auditing	Operations performed by StellarOne web console accounts are logged. StellarOne records an operating log for each account, tracking who logs on, who deletes event logs, and more.

What's New

TXOne StellarOne™ 3.0 Service Pack 1 provides following new features and enhancements.

TABLE 1-2. What's New in TXOne StellarOne™ 3.0 Service Pack 1

FEATURE	BENEFIT
New widgets for monitoring Cyber-Physical System Detection and Response (CPSDR)	The new widgets for CPSDR on the Dashboard provide an overview of the CPS situational awareness and deployment status at the centralized control level, by consolidating the anamolies and unexpected behaviors collected from each individual agent into the quantifying indicators of the potentail threats and baseline deviations, along with the up-to-date Operations Behavior Anomaly Detection deployment status of all the managed devices. Moreover, the widgets provide more clarity and quick access to the detected events, prompting users to take actions to defend against unexpected changes that may impact stability.
Disk space management	By means of the newly designed widgets displaying details about the disk usage of the 1st and 2nd HDD for StellarOne, the low disk space alerts based on a variety of usage thresholds, and the accompanied unavailable features list addressing such problems, you can manage your available disk space to ensure optimal performance for the StellarOne server.
Script Behavior functionality for StellarProtect (Legacy Mode)	The Script Behavior functionality complements the Operations Behavior Anomaly Detection feature for StellarProtect (Legacy Mode), providing a solid protection against script-based or fileless attacks.
Application Behavior functionality enhancements for StellarProtect (Legacy Mode)	The enhancements of the Application Behavior functionality for StellarProtect (Legacy Mode) implement effective application security.
API enhancements	The API now supports querying for the last components update time as well as enabling functions such as Scan Now and Maintenance Mode.
Last components update timestamp available on the GUI	The last components update timestamp for each agent can be viewed on the Agents list and the General Info page, allowing you to filter or export relevant data for specific agents or purly check the data at the single agent level.

Chapter 2

Installation Planning

This chapter shows how to plan for TXOne StellarOne installation.

Topics in this chapter include:

- *System Requirements on page 2-2*
- *Hardware Requirements on page 2-2*
- *Planning Network Bandwidth for Agent Deployment on page 2-9*
- *Ports and FQDN Used on page 2-10*

System Requirements

TXOne StellarOne™ is packaged in an Open Virtual Appliance (OVA) or Virtual Hard Disk v2 (VHDX) format. The above-mentioned package files respectively apply to different hypervisors.

Supported Hypervisors (OVA file)

- VMware ESXi 6.5 or above
- VMware Workstation 16 Pro or above

Supported Hypervisors (VHDX file)

- Windows Server 2019, Hyper-V Manager Windows 10 or above

Note

For StellarOne deployed from AMI on a AWS EC2 instance, refer to *Deciding an Instance Type for StellarOne on AWS EC2 Platform on page 2-7* for more details.

Supported Browser

- Google Chrome 87 or above
- Microsoft Edge 79 or above
- Mozilla Firefox 78 or above

Minimum Supported Resolution

- 1366x768

Hardware Requirements

Hardware requirements vary depending on the number of agents and logs that will be configured and retained. Please refer to the sections below for determining the optimal number of agents that your StellarOne server deployment can manage on different platforms.

Hardware Requirements for VMware System

See the following tables for determining the optimal number of agents that your StellarOne server deployment can manage on the VMware system.

TABLE 2-1. Sizing Table for VMware

MAX. NO. OF AGENTS	MIN NO. OF VCORES	MEMORY SIZE	1ST HDD SPACE	2ND HDD SPACE (RECOMMENDED)	2ND HDD SPACE REQUIRED WHEN OPERATIONS BEHAVIOR ANOMALY DETECTION ENABLED
30,000	8	32 GB	25 GB	100 GB	475 GB
20,000	8	16 GB		100 GB	350 GB
15,000	4	16 GB		50 GB	250 GB
10,000	4	16 GB		50 GB	175 GB
5,000	4	12 GB		50 GB	125 GB
1,000	4	12 GB		50 GB	70 GB
500	4	12 GB		50 GB	60 GB

Important

Ensure that you meet the 2nd disk storage requirement listed above for using the advanced Operations Behavior Anomaly Detection feature in StellarOne 3.0.

The external disk space varies depending on the number of logs planned to be stored, as shown in the table below.

TABLE 2-2. No. of Logs versus Disk Space

NO. OF LOGS	DISK SPACE
300,000,000	500 GB
180,000,000	300 GB
90,000,000	150 GB
60,000,000	100 GB
30,000,000	50GB

To determine the ideal specifications for your exernal HDD, please refer to the following formula:

[Output log numbers for a single agent per day] x [Log storage period in days] x [Total number of agents]

Example: External HDD size for 20,000 agents

- Output log numbers for a single agent per day: 100 events
- Log storage period in days: 30 days
- Total number of agents: 20,000 agents

Total number of logs:

100 x 30 x 20000 = 60,000,000 Logs

In this case, it would be required to prepare 100 GB for storage space.

Note

1. The StellarOne requires one external disk with at least 50 GB minimum space for initialization and booting process.
2. The external disk is used to store the system configurations and event logs. You may reuse the external disk of a terminated StellarOne instance if you want to migrate the previous configurations and logs to a new StellarOne instance.
3. Please also take the network bandwidth into consideration when planning for agent deployment. Refer to *Planning Network Bandwidth for Agent Deployment on page 2-9* for more details.

Hardware Requirements for Hyper-V System

See the following tables for determining the optimal number of agents that your StellarOne server deployment can manage on the Hyper-V system.

TABLE 2-3. Sizing Table for Hyper-V

MAX. NO. OF AGENTS	MIN. NO. OF CPU	MEMORY SIZE	1ST HDD SPACE	2ND HDD SPACE (RECOMMENDED)	2ND HDD SPACE REQUIRED WHEN OPERATIONS BEHAVIOR ANOMALY DETECTION ENABLED
30,000	10	24 GB	25 GB	100 GB	475 GB
20,000	8	16 GB		100 GB	350 GB
15,000	8	16 GB		50 GB	250 GB
10,000	8	16 GB		50 GB	175 GB
5,000	8	16 GB		50 GB	125 GB
1,000	4	16 GB		50 GB	70 GB

Max. No. of Agents	Min. No. of CPU	Memory Size	1st HDD Space	2nd HDD Space (Recommended)	2nd HDD Space required when Operations Behavior Anomaly Detection enabled
500	4	8 GB		50 GB	60 GB

Important

Ensure that you meet the 2nd disk storage requirement listed above for using the advanced Operations Behavior Anomaly Detection feature in StellarOne 3.0.

Table 2-4. No. of Logs versus Disk Space

No. of Logs	Disk Space
300,000,000	500 GB
180,000,000	300 GB
90,000,000	150 GB
60,000,000	100 GB
30,000,000	50GB

Note

1. The StellarOne requires one external disk with at least 50 GB minimum space for initialization and booting process.
2. The external disk is used to store the system configurations and event logs. You may reuse the external disk of a terminated StellarOne instance if you want to migrate the previous configurations and logs to a new StellarOne instance.
3. Please also take the network bandwidth into consideration when planning for agent deployment. Refer to *Planning Network Bandwidth for Agent Deployment on page 2-9* for more details.

Deciding an Instance Type for StellarOne on AWS EC2 Platform

Refer to the tables below for determining the optimal number of agents that your StellarOne server deployment can manage on the AWS EC2 platform.

Note

Please refer to Amazon EC2 Instance Types for specifications of the instance types.

TABLE 2-5. Sizing Table for AWS EC2

MAX. NO. OF AGENTS	MIN. NO. OF CPU	MEMORY SIZE	1ST HDD SPACE	2ND HDD SPACE (RECOMMENDED)	2ND HDD SPACE REQUIRED WHEN OPERATIONS BEHAVIOR ANOMALY DETECTION ENABLED
30,000	10	24 GB	25 GB	100 GB	475 GB
20,000	8	16 GB		100 GB	350 GB

Max. No. of Agents	Min. No. of CPU	Memory Size	1st HDD Space	2nd HDD Space (Recommended)	2nd HDD Space required when Operations Behavior Anomaly Detection enabled
15,000	8	16 GB		50 GB	250 GB
10,000	8	16 GB		50 GB	175 GB
5,000	8	16 GB		50 GB	125 GB
1,000	4	16 GB		50 GB	70 GB
500	4	8 GB		50 GB	60 GB

Table 2-6. No. of Logs versus Disk Space

No. of Logs	Disk Space
300,000,000	500 GB
180,000,000	300 GB
90,000,000	150 GB
60,000,000	100 GB
30,000,000	50GB

Note

1. The StellarOne requires one external disk with at least 50 GB minimum space for initialization and booting process.
2. The external disk is used to store the system configurations and event logs. You may reuse the external disk of a terminated StellarOne instance if you want to migrate the previous configurations and logs to a new StellarOne instance.
3. Please also take the network bandwidth into consideration when planning for agent deployment. Refer to *Planning Network Bandwidth for Agent Deployment on page 2-9* for more details.

Planning Network Bandwidth for Agent Deployment

Please take network bandwidth into consideration when planning for agent deployment. See below as an example of calculating the bandwidth required to support the number of agents planned to deploy.

Basic concept:

Total available bandwitdth / Deployment task size = How many agents can be deployed at one task

Currently, there are 3 types of StellarOne deployment tasks:

- Incremental Pattern Update: works for agent pattern version no less than server version for two weeks, which requires about less than 5 MB
- Full Pattern Update: works for agent pattern version that's already exceeded two-week duration compared to server/update source, which requires about 80 MB
- Agent Remote Patch: update with the remote agent deployment upgrade package, which requires about 70 MB

The following tables illustrate the number of agents to be deployed on condition that the deployment takes 5 minutes and requires 50% of network

bandwidth, as well as the recommended policy refresh interval regarding the number of agents managed.

Table 2-7. Agent Deployment Plan

Total Bandwidth / Deployment Task	No. of Agents Deployed			
	10 Mbps	100 Mbps	1000 Mbps	10 Gbps
Incremental Pattern Update	38	375	3750	37500
Full Pattern Update	2	23	234	2344
Agent Remote Patch	3	27	268	2679

Table 2-8. Policy Refresh Interval vs No. of Agents Managed

Policy Refresh Interval	No. of Agents Managed
5 minutes	5000
10 minutes	10000
20 minutes	20000
60 minutes	60000

Ports and FQDN Used

The following table shows the ports used by the StellarOne server. Please keep them opened in your firewall settings for StellarOne's use.

TABLE 2-9. Ports and FQDN Used

FROM	TO	OPEN PORT	FQDN	FUNCTION
StellarProtect	StellarOne	9443, 8000, 443	-	StellarOne's listening port for StellarProtect
StellarProtect (Legacy Mode)	StellarOne	8000, 443	-	StellarOne's listening port for StellarProtect (Legacy Mode)
StellarOne	StellarProtect	14336	-	StellarProtect's listening port
StellarOne	StellarProtect (Legacy Mode)	14336	-	StellarProtect (Legacy Mode)'s listening port
StellarOne	License (PR) Server	443	`odc.cs.txone-networks.com`	StellarOne connects to global server port for license verification and renewal through HTTPS
Browser	StellarOne Web	443	-	StellarOne's listening port for web access through HTTPS
StellarOne	Active Update Server	443	https://ttau.cs.txone.com/protect https://ttau.cs.txone.com/enforce	StellarOne connects to global server port for the Stellar Active Update through HTTPs

Note

The following ports are reserved for StellarOne private service usage and are not allowed to use for other purposes.

TABLE 2-10. StellarOne Occupied Ports

STELLARONE OCCUPIED PORT	PORT
StellarProtect (Legacy Mode) Default Port	8000
StellarProtect Default Port	9443, 8000
SSH	22
NTP	123
Web	443
StellarOne Internal Service	25
	7590
	8888
	8889
	8999
	9091

Supported Agent Versions

The following table indicates the StellarOne supported agent versions.

WARNING!

- Before upgrading, please check the table below to identify the StellarOne supported agent versions.
- Please upgrade the StellarOne server first before you upgrade the agents.

TABLE 2-11. Supported Agent Version

SERVER VERSION	AGENTS VERSION		
STELLARONE	STELLARPROTECT	STELLARPROTECT (LEGACY MODE)	STELLARENFORCE
3.0 Service Pack 1	3.0 Service Pack 1 and earlier versions	3.0 Service Pack 1 and earlier versions	N/A
3.0	3.0 and earlier versions	3.0 and earlier versions	N/A
2.2	2.2 and earlier versions	1.5 and earlier versions	N/A
2.1	2.1and earlier versions	1.4 and earlier versions	N/A
2.0	2.0 and earlier versions	1.3 and earlier versions	1.3 and earlier versions
1.2	1.2 and earlier versions	N/A	1.2 and earlier versions
1.1	1.1 and earlier version	N/A	1.1 and earlier version
1.0	1.0	N/A	1.0

Important

Please try to keep or upgrade the managed agents in or to the corresponding StellarOne major release version as indicated in the table above. Though StellarOne provides backward compatibility to support agents with earlier version, new features or enhanced functionality should not be applicable on some agents with earlier versions.

Note

The StellarEnforce was renamed StellarProtect (Legacy Mode) upon the release of version 1.3.

Chapter 3

Installation

This chapter guides you through TXOne StellarOne installation. StellarOne is packaged in an Open Virtual Appliance (OVA) or Virtual Hard Disk v2 (VHDX) format and supports 4 types of platforms: VMware ESXi, VMware Workstation, Windows Hyper-V systems, and AWS EC2.

Topics in this chapter include:

- *StellarOne Installation Flow on page 3-2*
- *StellarOne Onboarding to VMware ESXi on page 3-2*
- *StellarOne Onboarding to Windows Hyper-V on page 3-12*
- *StellarOne Onboarding to AWS EC2 on page 3-29*
- *Opening StellarOne Management Console on page 3-43*

StellarOne Installation Flow

Installing StellarOne web console requires performing the following steps:

Procedure

1. Deploy a StellarOne instance on VMware ESXi or Workstation, Windows Hyper-V, or AWS EC2 platform.
2. Add an external hard disk with at least 50 GB of space to the StellarOne instance.
3. Log on StellarOne web console to set up the administrator's account.
4. Log on StellarOne web console to activate the product license and set time properties.
5. Configure settings such as IP address and communication ports.

StellarOne Onboarding to VMware ESXi

This section describes how to deploy StellarOne to a VMware ESXi system.

Prerequisites

- The OVA packages provided by TXOne must be available and accessible to VMwareESXi.
- VMware ESXi 6.5 or above is required.
- The necessary networks have been properly created for ESXi.
- An external disk with at least 50 GB.

Deploying StellarOne on the VMware ESXi

The following section describes the procedures of deploying StellarOne from an OVA file to the VMware ESXi system.

Procedure

1. Log into the VMware vSphere web client.
2. Under **Navigator**, click **Host** > **Create/Register VM**.

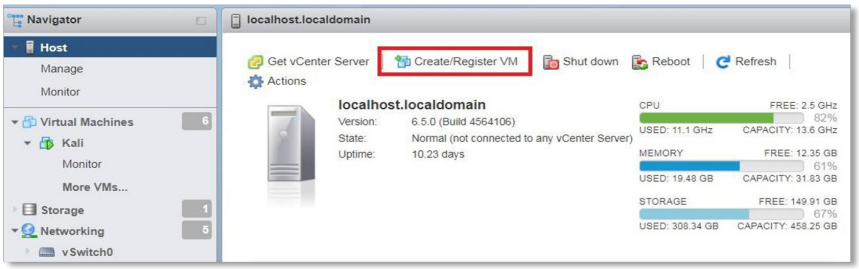


FIGURE 3-1. Navigator

3. In **Select creation type**, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.

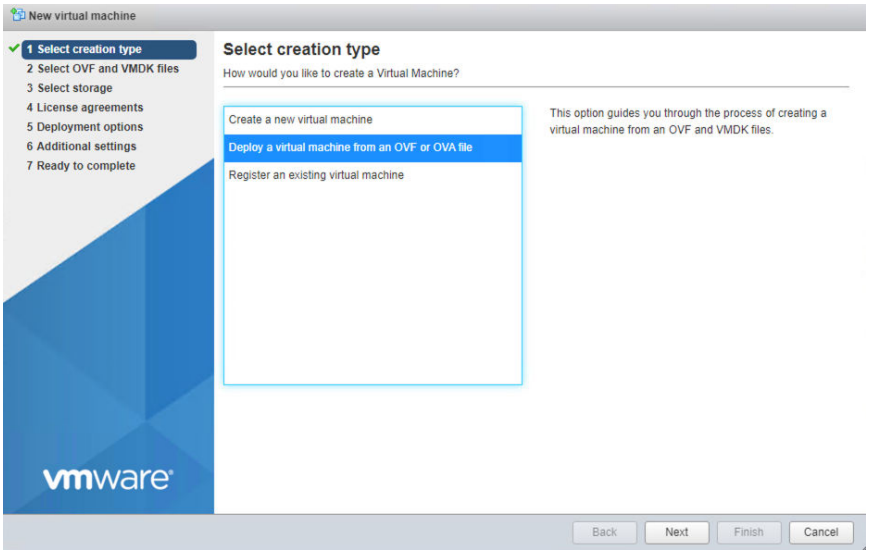


FIGURE 3-2. Select creation type

4. Specify a name for your new StellarOne instance and select the StellarOne disk image to upload.

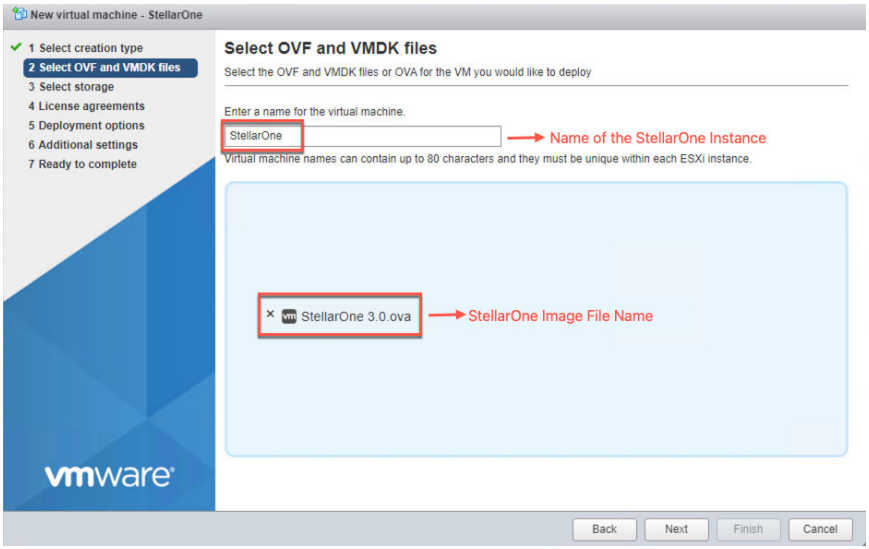


FIGURE 3-3. Select OVF and VMDK files

5. Choose a strorage location for the StellarOne instance and click **Next**.

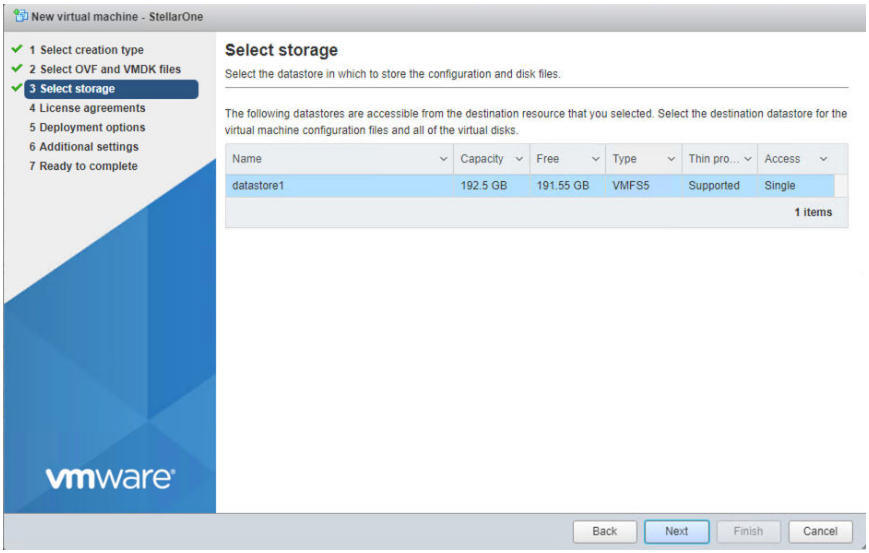


FIGURE 3-4. Select storage

6. Select deployment options and click **Next**.

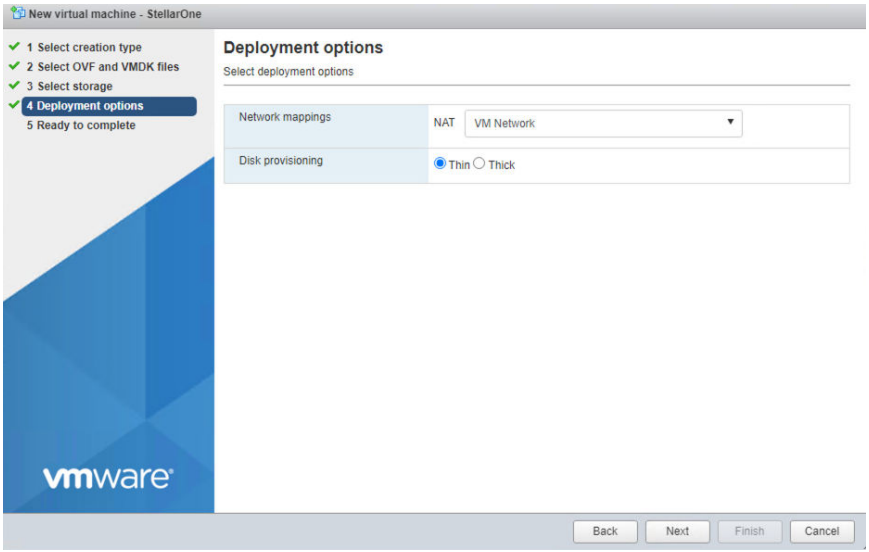


FIGURE 3-5. Deployment options

7. When you see **Ready to complete**, click **Finish** to start the deployment.

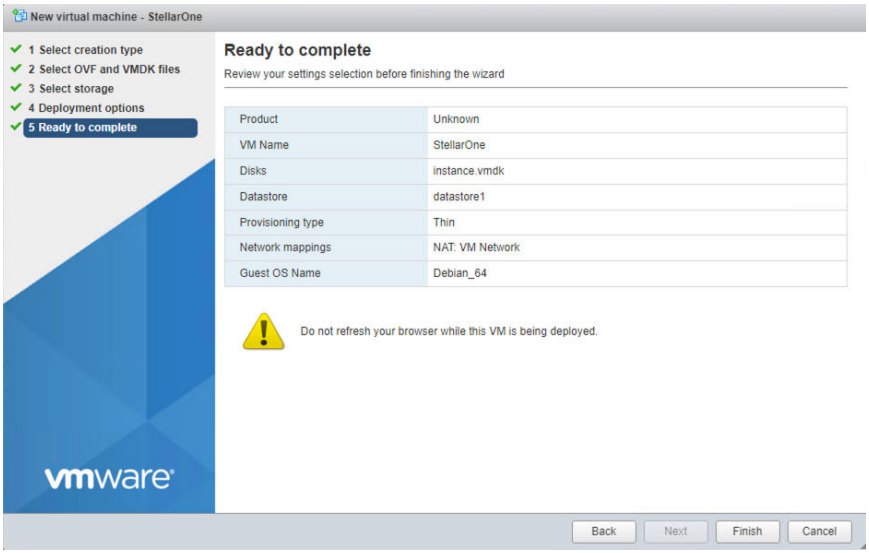


FIGURE 3-6. Ready to complete

8. Under the **Recent Tasks** pane, you will see a progress bar indicating the StellarOne image is being uploaded. Please wait until the upload is finished.

9. Add an external disk with at least 50 GB of capacity to the StellarOne instance.

   a. Close the StellarOne instance if it is open.

   b. The external disk capacity is determined by the number of logs to be stored, as shown in the table below.

NO. OF LOGS	DISK CAPACITY
90,000,000	150 GB
60,000,000	100 GB
30,000,000	50 GB

   To determine the ideal specifications for your external HDD, refer to the following formula:

[Output log numbers for a singel agent per day] x [Log storage period in days] x [Total number of agents]

For example, to calcuate the external HDD capacity required for 20,000 agents on the assumption that:

- Output log number for a single agent per day: 100 events
- Log storage period in days: 30 days
- Total number of agents: 20,000 agents

The total number of logs: 100 x 30 x 20,000 = 60,000,000 logs

In this case, it is requred to prepare an external disk with capacity of 100 GB for storage space.

c. Follow the procedures to add the external disk: **Actions** > **Edit settings** > **Add hard disk** > **New hard disk**

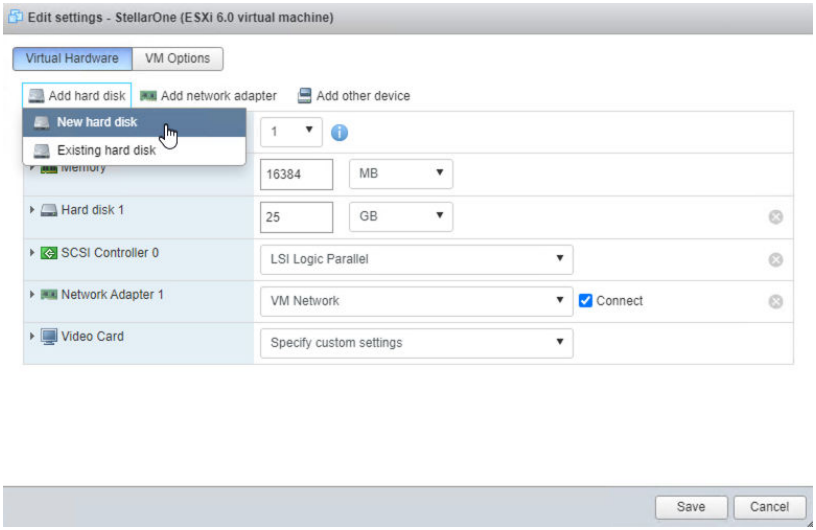


FIGURE 3-7. Edit settings - New hard disk

d. Set the new hard disk space to 50 GB.

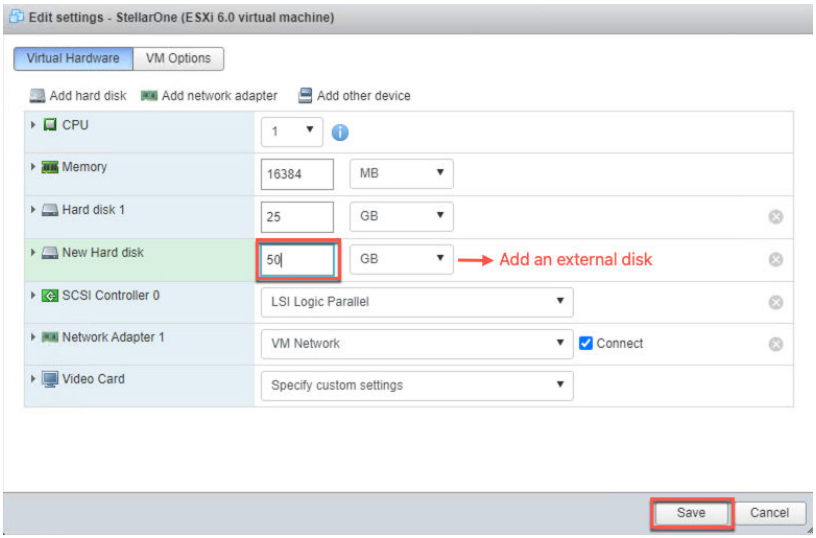


FIGURE 3-8. Edit settings - New hard disk capacity

a. If you need to increase the number of logs StellarOne can store, follow the procedures.

1. Shut down StellarOne
2. Increase the external disk capacity to fit the maximum log requirements
3. Restart the StellarOne instance. After that, the storage space available for StellarOne log files will be expanded.

b. If you wan to migrate the existing StellarOne settings to the newly launched virtual machine, see *System Migration on page 5-4*.

Note

a. StellarOne requires one external disk with minimum capacity of 50GB; otherwise, StellarOne will not finish initialization and will not complete the boot process.

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

10. Turn on the virtual machine.

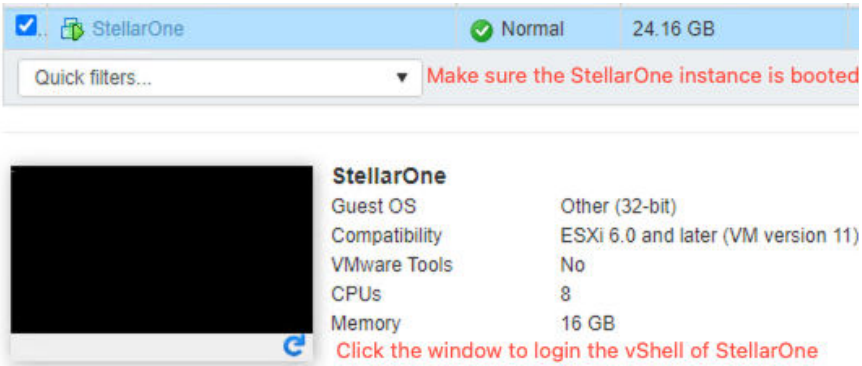


FIGURE 3-9. VM turned on

11. (Optional) Adjust your StellarOne instance to use the proper resource configurations based on the default setting of 8 CPU cores and 16 GB Memory.

a. Shut down the StellarOne instance and click **Actions** > **Edit settings**. The **Edit settings** window appears.

b. Configure the number of CPU cores.

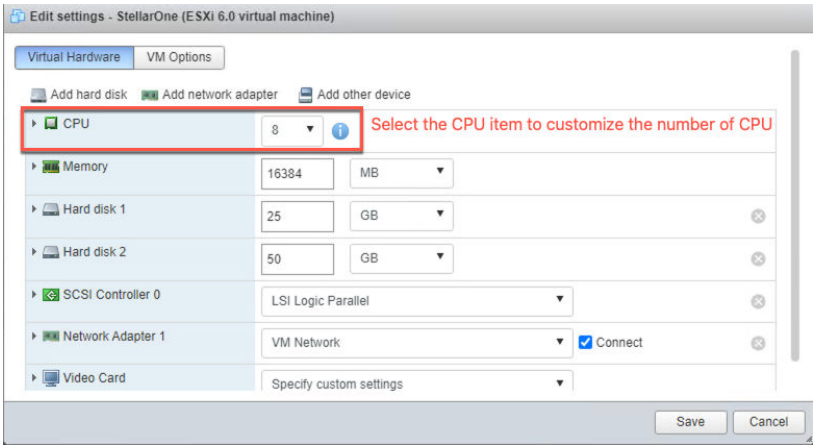


FIGURE 3-10. Select number of CPU

c. Configure the amount of Memory.

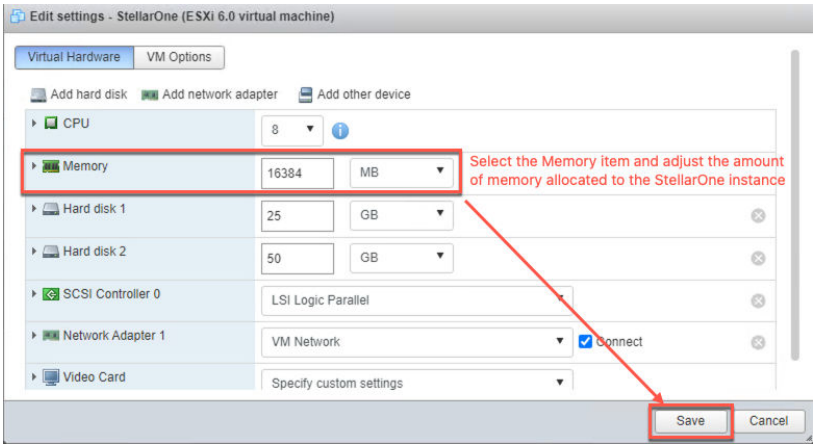


FIGURE 3-11. Configure Memory

Note

See the *Hardware Requirements for VMware System on page 2-3* for the CPU and memory requirements for agent deployment and corresponding StellarOne configuration and resource allocation.

d. Boot the StellarOne instance.

StellarOne Onboarding to Windows Hyper-V

This section describes how to deploy StellarOne to the Windows Hyper-V system.

Prerequisites

- The VHDX packages provided by TXOne must be available and accessible to Windows Hyper-V.
- Windows Server 2019, Hyper-V Manager Windows 10 or above.
- The necessary networks have been properly created for Windows Hyper-V.
- An external disk with at least 50 GB.

Deploying StellarOne to a Hyper-V System

The following section describes the procedures of deploying StellarOne from a VHDX File to a Hyper-V system.

Procedure

1. Launch **Hyper-V Manager**

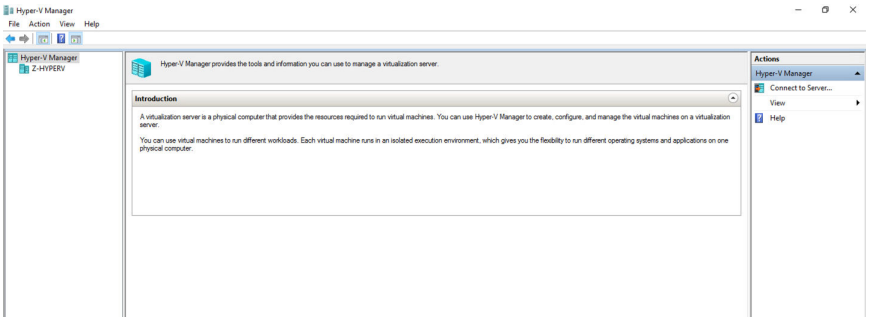


FIGURE 3-12. Hyper-V Manager

2. Under **Actions**, click **New** > **Virtual Machine**.
3. The **New Virtual Machine Wizard** appears, click **Next**.

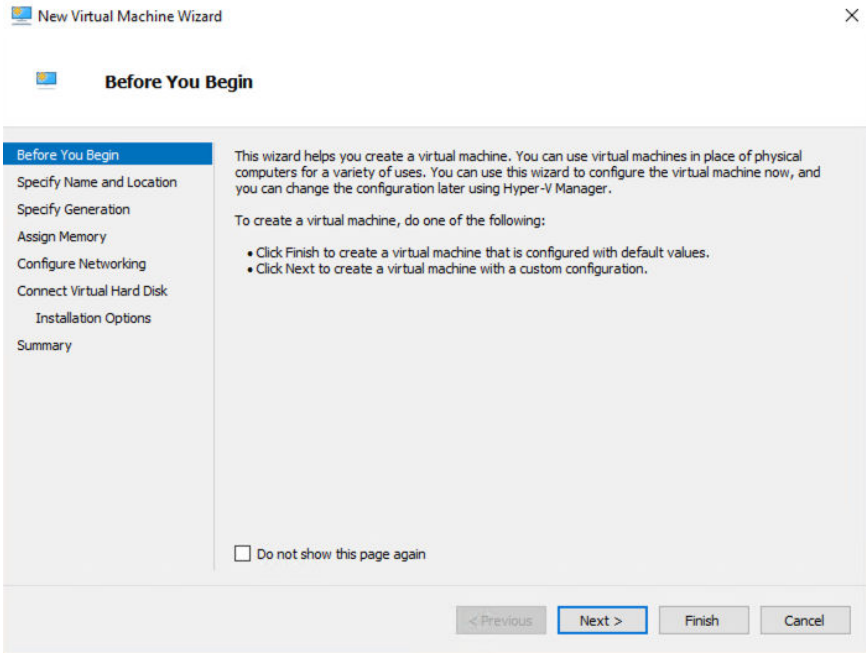


FIGURE 3-13. New Virtual Machine Wizard: Before You Begin

4. In **Specify Name and Location**, type a name for your new virtual machine and click **Next**.

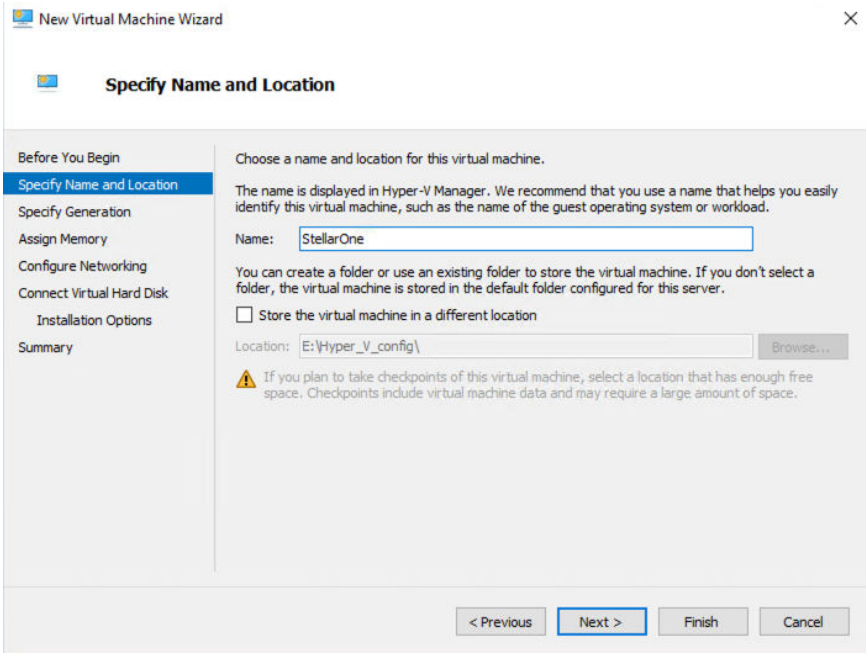


FIGURE 3-14. New Virtual Machine Wizard: Specify Name and Location

5. In **Specify Generation**, select **Generation 1**.

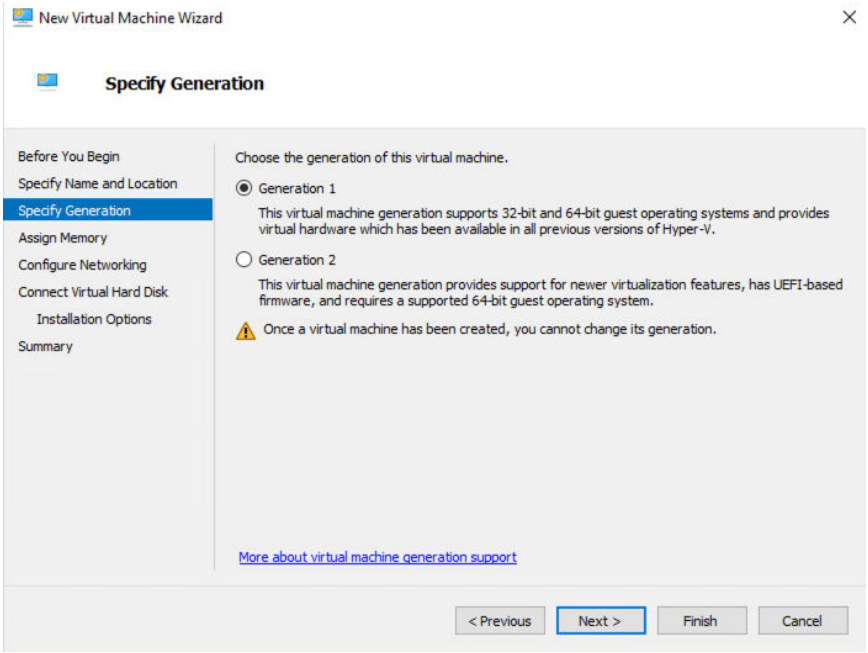


FIGURE 3-15. New Virtual Machine Wizard: Specify Generation

6. In **Assign Memory**, allocate memory for the new virtual machine and click **Next**.

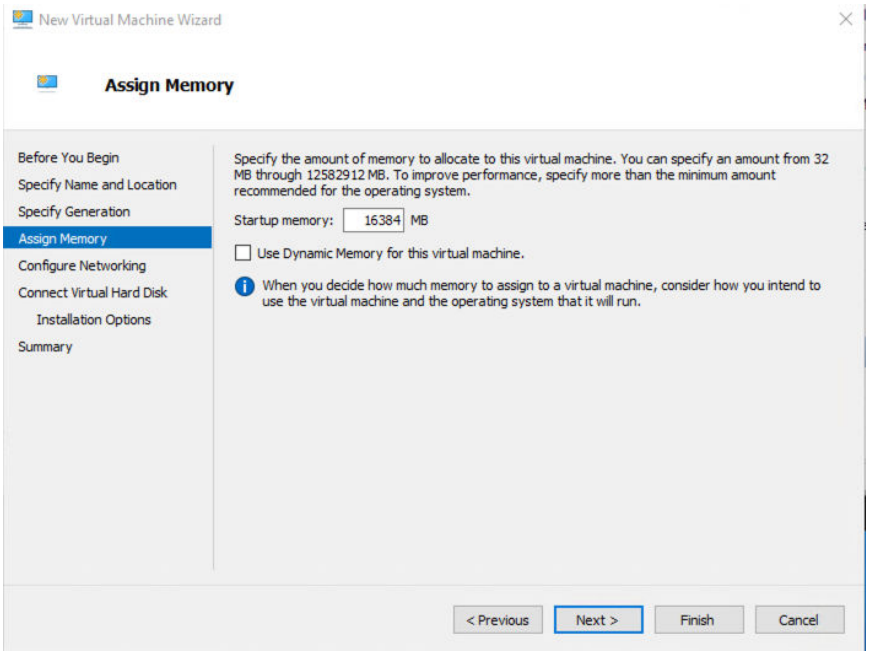


FIGURE 3-16. Assign Memory for Virtual Machine

Note

For further agent deployment and configurations, it is recommended to at least meet the hardware requirements: 8 CPU cores and 16 GB Memory.

7. Configure the network settings for the new virtual machine, and then click **Next**.

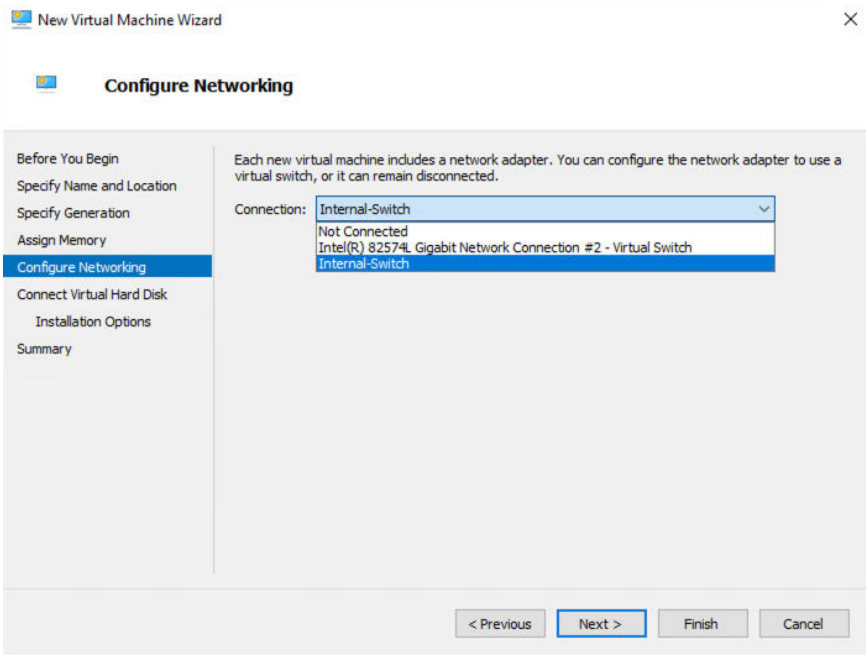


FIGURE 3-17. Configure Networking for Virtual Machine

8. Select a virtual hard disk (the StellarOne `.vhdx` file) and click **Next**.

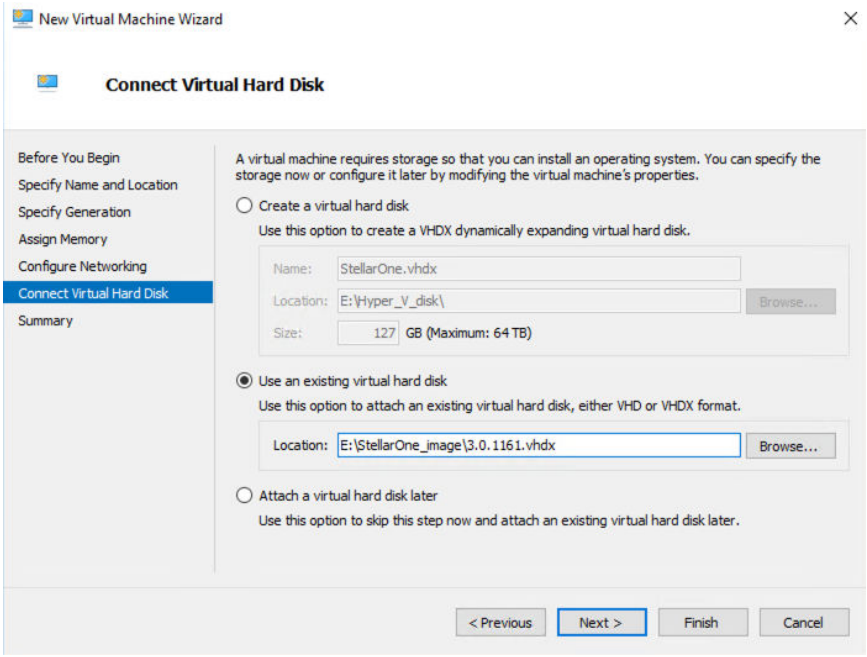


FIGURE 3-18. Connect Virtual Hard Disk

9. Check your settings and click **Finish**.

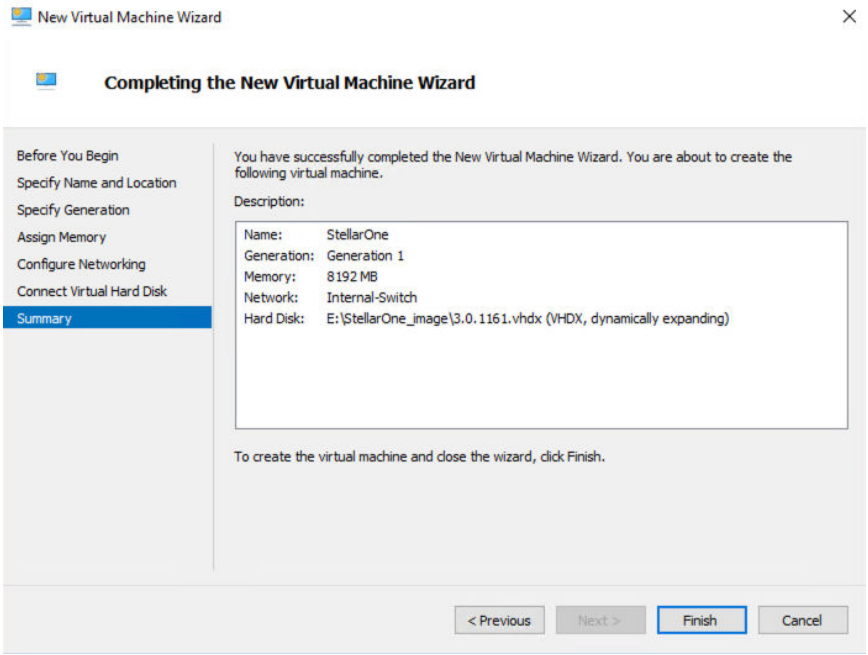


FIGURE 3-19. Completing the New VM Wizard

10. Add a new disk for the StellarOne virtual machine.

Note

Make sure the previous StellarOne instance is turned off.

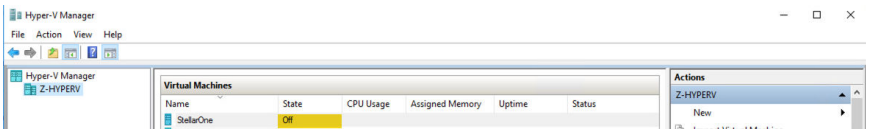


FIGURE 3-20. State of StellarOne instance is off

a. Select the StellarOne virtual machine and right click to select **Settings** from the context menu.

b. Select **Hard Drive** from the **IDE Contoller 0** item and click **Add**.

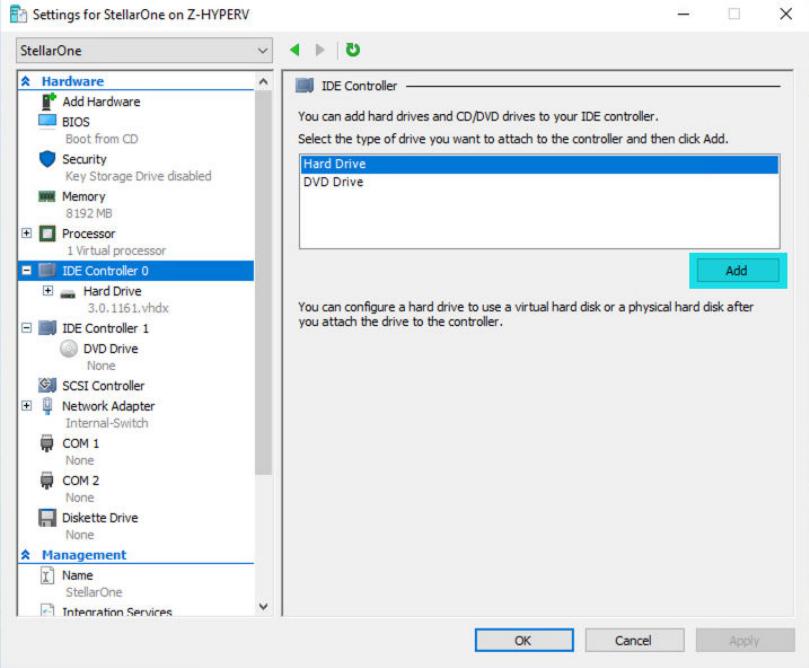


FIGURE 3-21. Settings for StellarOne - 1

c. Click **New**.

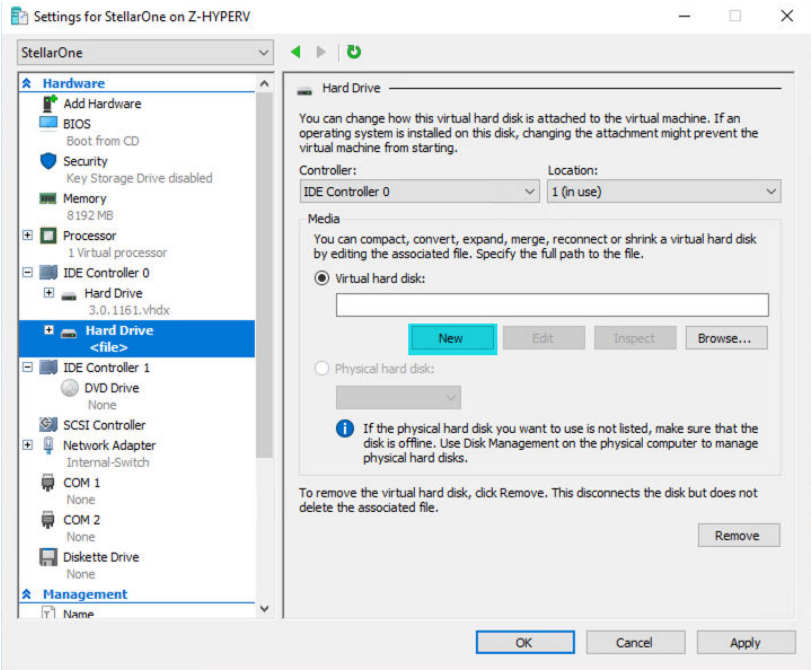


FIGURE 3-22. Settings for StellarOne - 2

d. The **New Virtual Hard Disk Wizard** appears. Click **Next**.

e. In **Choose Disk Format**, select **VHDX** as the disk format and click **Next**.

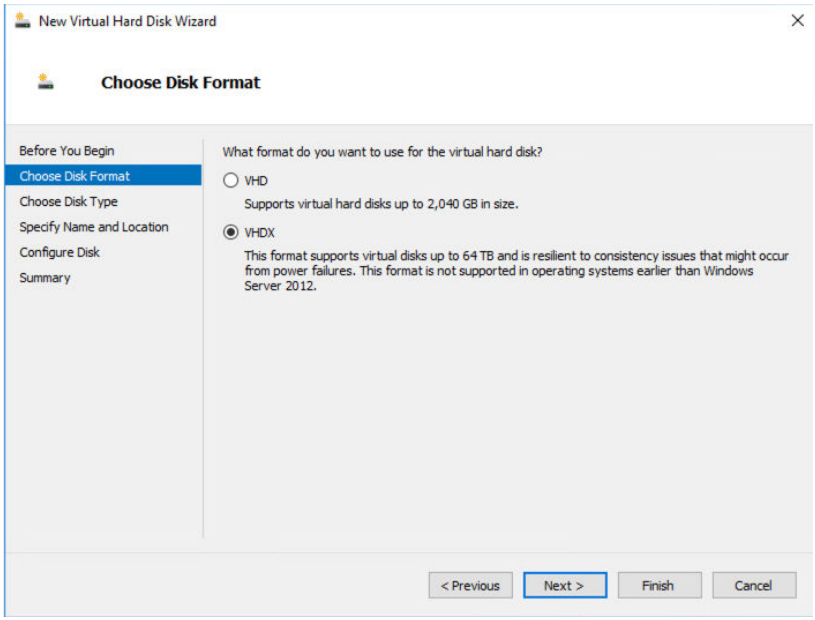


FIGURE 3-23. Choose Disk Format

f. In **Choose Disk Type**, select **Dynamically expanding** as the disk type and click **Next**.

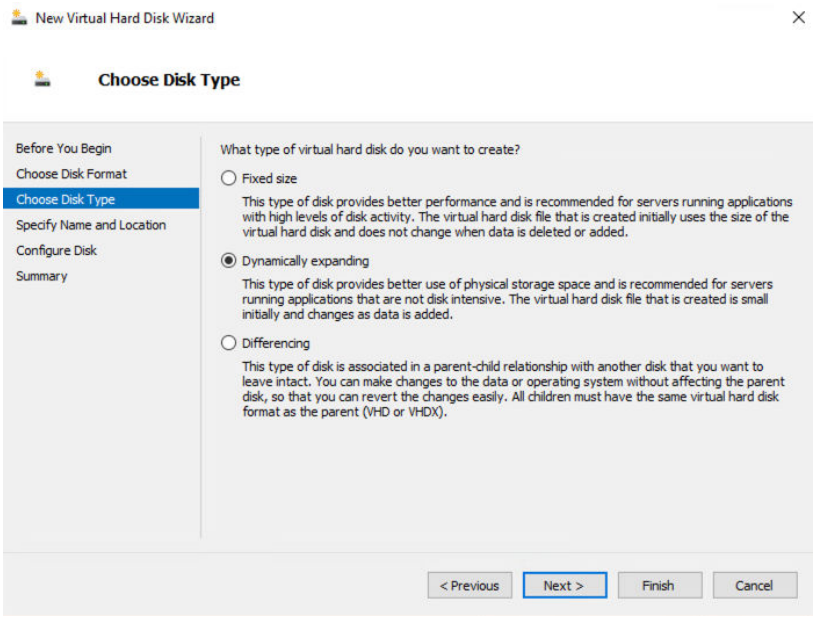


FIGURE 3-24. Choose Disk Type

g. Specify the name and location of the virtual hard disk file.

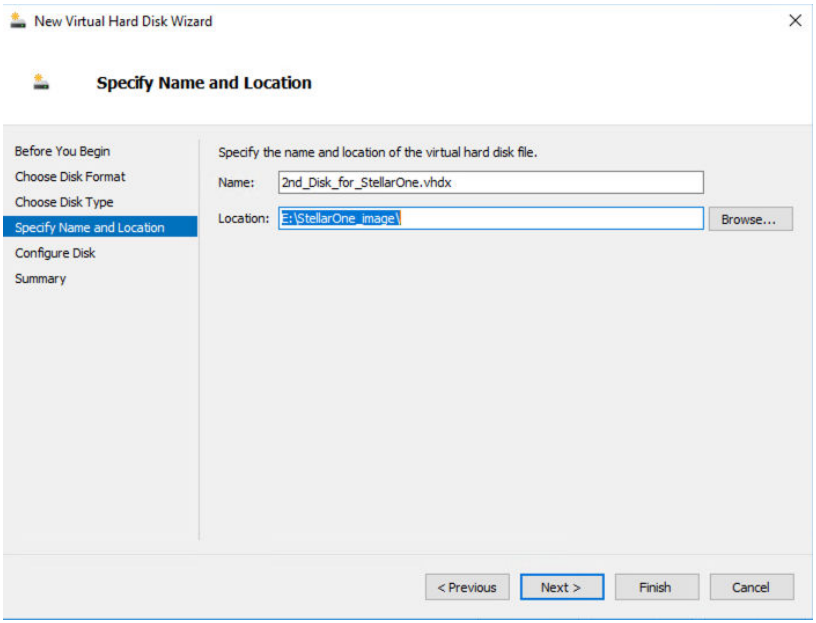


FIGURE 3-25. Specify Name and Location

h. Configure disk size.

Note

See *Sizing Table for Hyper-V System on page 2-5* for the recommended 2nd disk size for StellarOne.

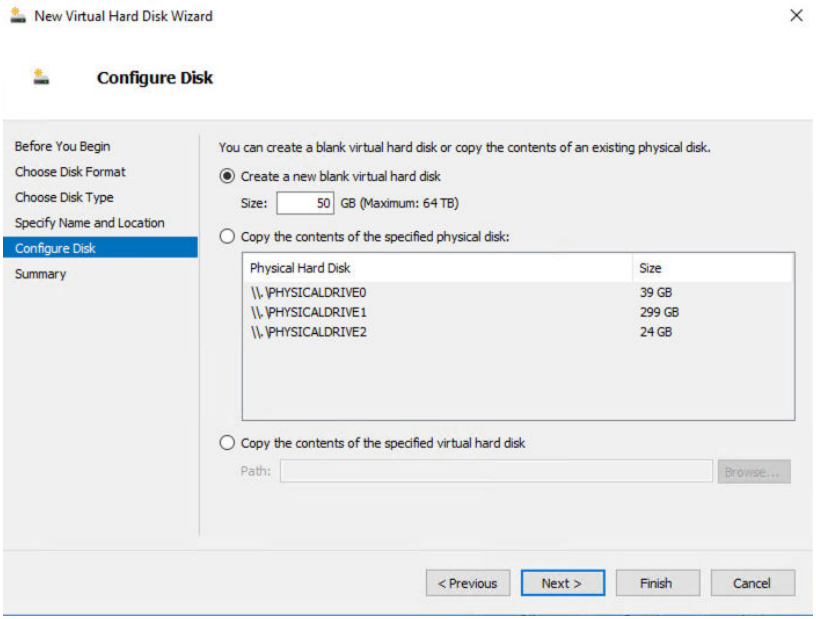


FIGURE 3-26. Configure Disk for StellarOne

i. Click **Next** to check your settings.

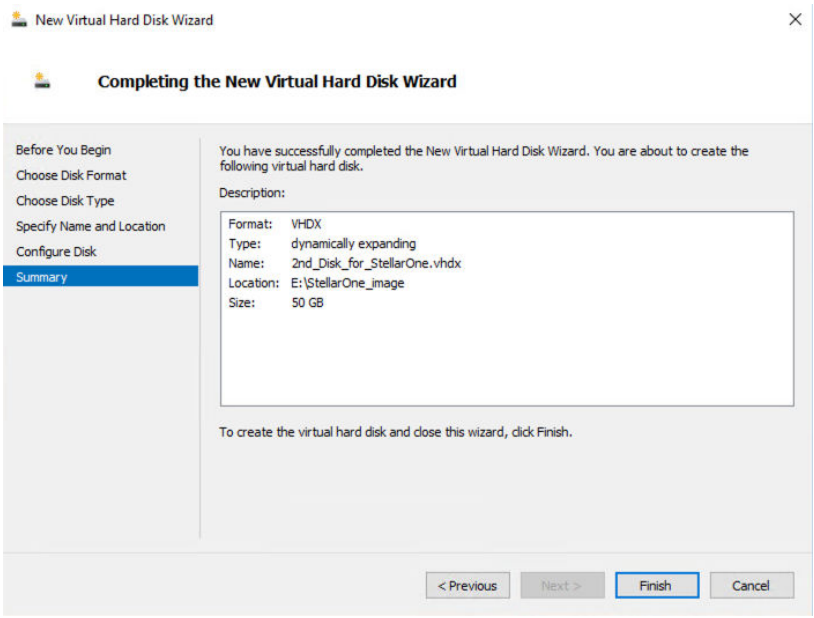


FIGURE 3-27. Completing the New Virtual Hard Disk Wizard

j. Click **Finish** to complete the settings.

11. (Optional) See *Hardware Requirements for Hyper-V System on page 2-5* for the CPU and memory requirements for agent deployment and corresponding StellarOne configuration and resource allocation. It is recommended to at least meet the hardware requirements (4 CPU cores, 16 GB Memory).

a. Shut down the StellarOne instance. Select and right click the instance, and then click **Settings**.

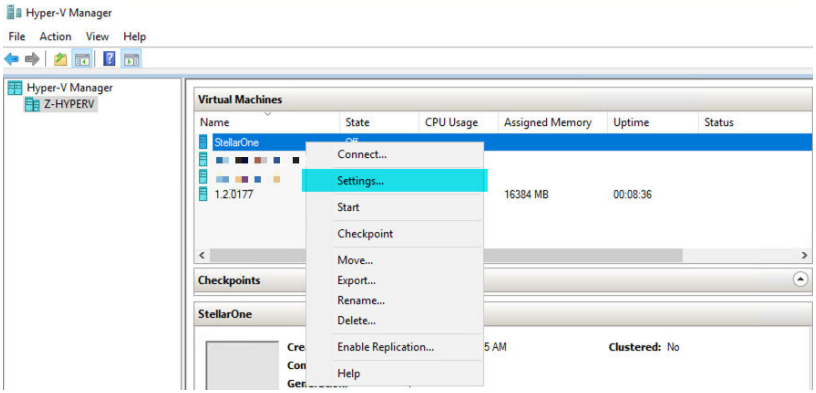


FIGURE 3-28. Configure the settings of StellarOne instance

b. In **Processor**, configure the number of virtual processors and the associated resource control settings. Click **OK** to complete the settings.

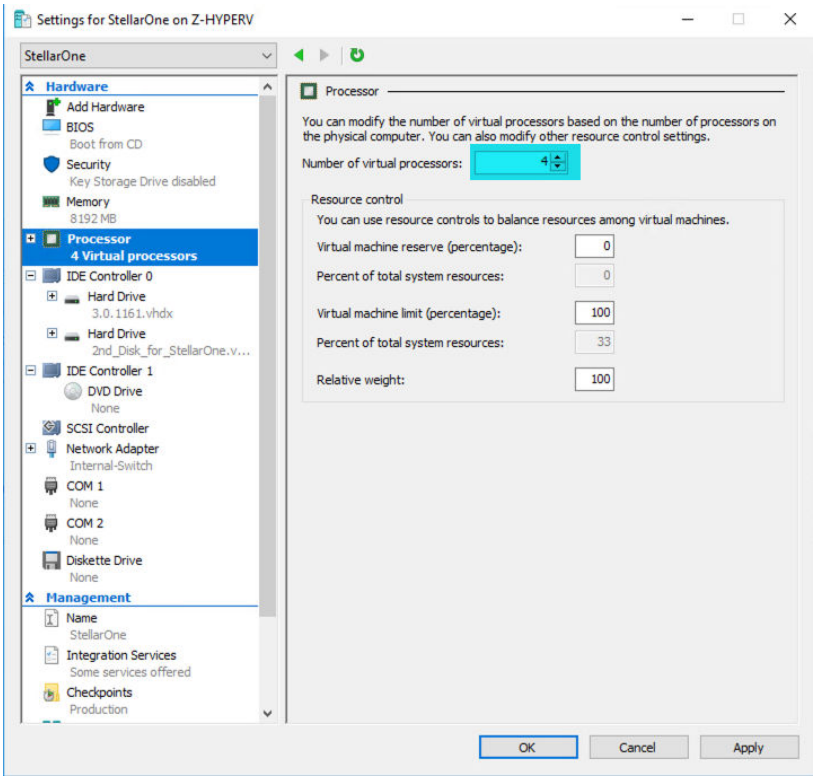


FIGURE 3-29. Configure the processor settings of StellarOne instance

c. In the **Memory** section, specify the amount of memory that the StellarOne instance can use.

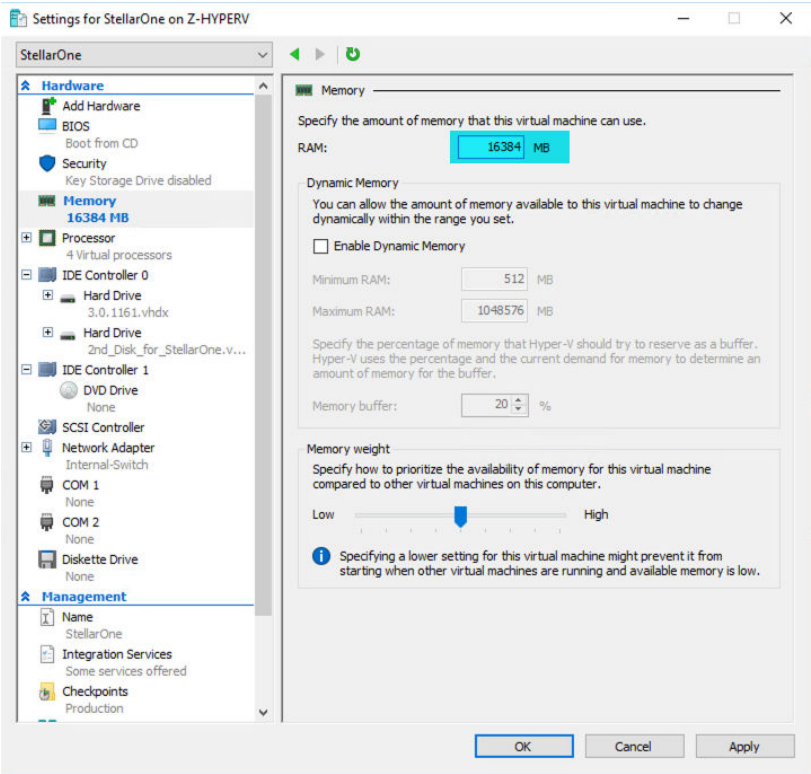


FIGURE 3-30. Configure the memory settings of StellarOne instance

d. Boot the StellarOne instance.

StellarOne Onboarding to AWS EC2

This section describes how to deploy StellarOne on the AWS EC2 platform.

Prerequisites

- An AWS account is required
- StellarOne for AWS supports only BYOL (Bring Your Own License)

- An external disk (EBS) with at least 50 GB.

Note

Please contact your support provider for the BYOL license.

Deploying StellarOne on AWS EC2

Below section details procedures of deploying StellarOne from BYOL AMI on the AWS EC2 platform.

Procedure

1. Go to the **AWS Markeplace** homepage.
2. Enter the search string such as TXOne or StellarOne in the search bar and then run the search.
3. Click the search result and read the product information carefully before proceeding to the subscription process.
4. After accepting the terms and conditions for using StellarOne, choose the **Fulfillment option**, **Software version**, and **Region** to launch StellarOne.
5. Select **Launch through EC2** as the launch action.

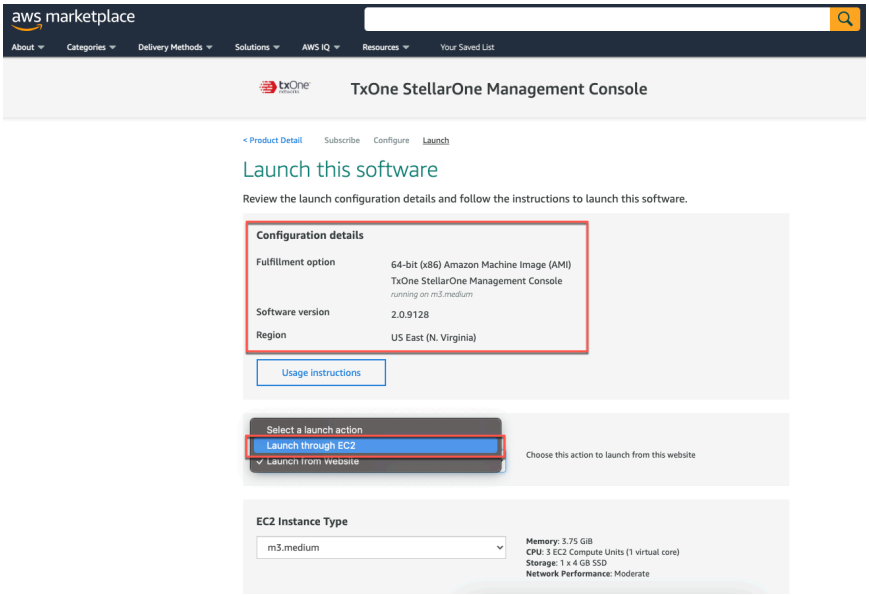


FIGURE 3-31. Select a Launch Action

6. Log on the AWS EC2 console.
7. Go to **Images** > **AMIs**.
8. Select the region you chose in step 4.
9. Find the target AMI from the list of **AMI ID**.
10. Select the target AMI and click **Launch Instance from AMI**.
11. Select a supported instance type.

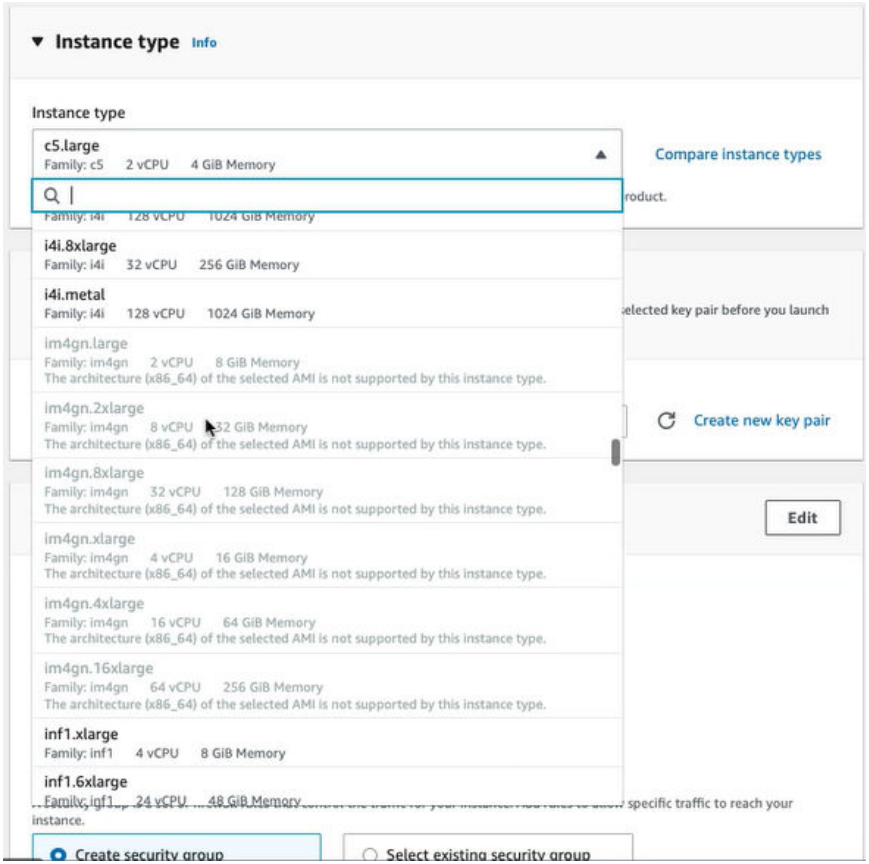


FIGURE 3-32. Select an Instance Type

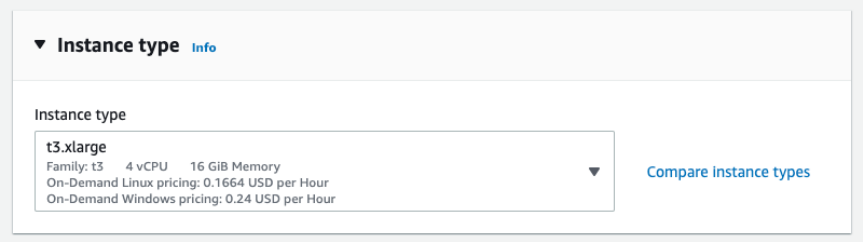


FIGURE 3-33. Information of the Selected Insance Type

Note

- The instance types that do not meet StellarOne's deployment requirements will be unavailable for selection.
- Refer to *Deciding an Instance Type for StellarOne on AWS EC2 Platform on page 2-7* for determining which instance type to use.

12. Configure the instance settings:
    a. Select or create the **Key pair (login)**

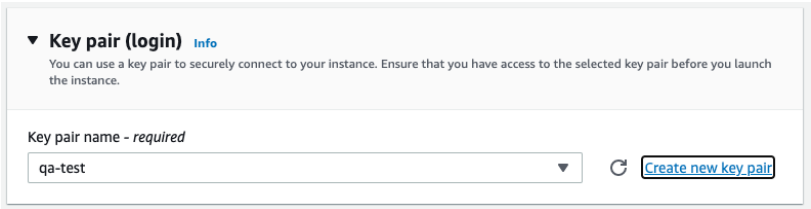


FIGURE 3-34. Key pair (login)

    b. Configure the **Network settings**:
        - Be sure to create security group for allowing specific data exchanges to access your instance. It is required to enable the **HTTPS traffic from the Internet** to allow StellarOne to manage endpoints on the network.

- (Optional) If you have the need for SSH login, you can also enable the **Allow SSH traffic from** and select **Anywhere** or specify the IP address.

Note

Refer to *Ports and FQDN Used on page 2-10* for configuring the ports that should have access to StellarOne.

- Be sure to grant 8000 or 9443, the dedicated port for StellarProtect or StellarProtect (Legacy Mode), access to your instance.
- For security reasons, it is recommended to allow 443 or 22, the web port or SSH port for StellarOne, to be accessible from trusted IP address.

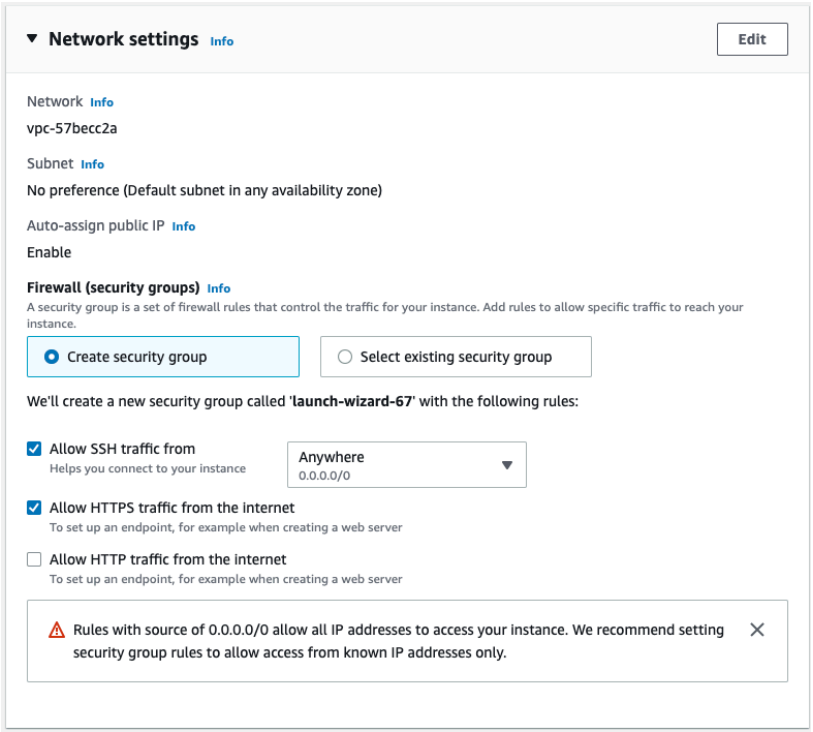


FIGURE 3-35. Network settings

c. Add an EBS with at least 50 GB of space to the StellarOne instance in **Configure storage**.

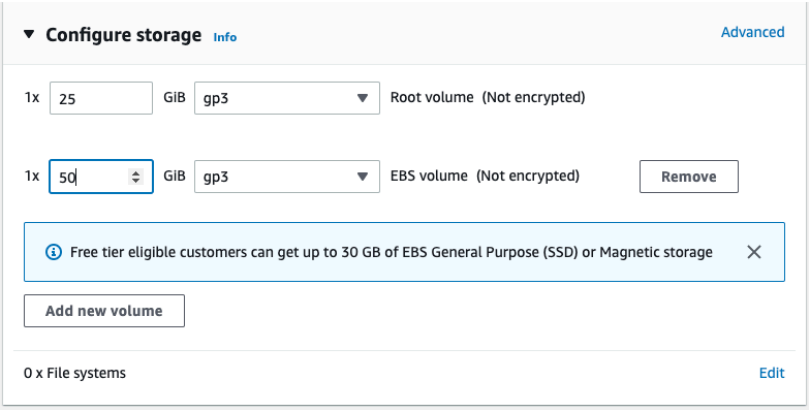


FIGURE 3-36. Configure Storage

d. Click **Launch Instance**.

Note

It may take 5 to 10 minutes to complete the deployment.

13. Find the StellarOne instance and copy its assigned IP address.

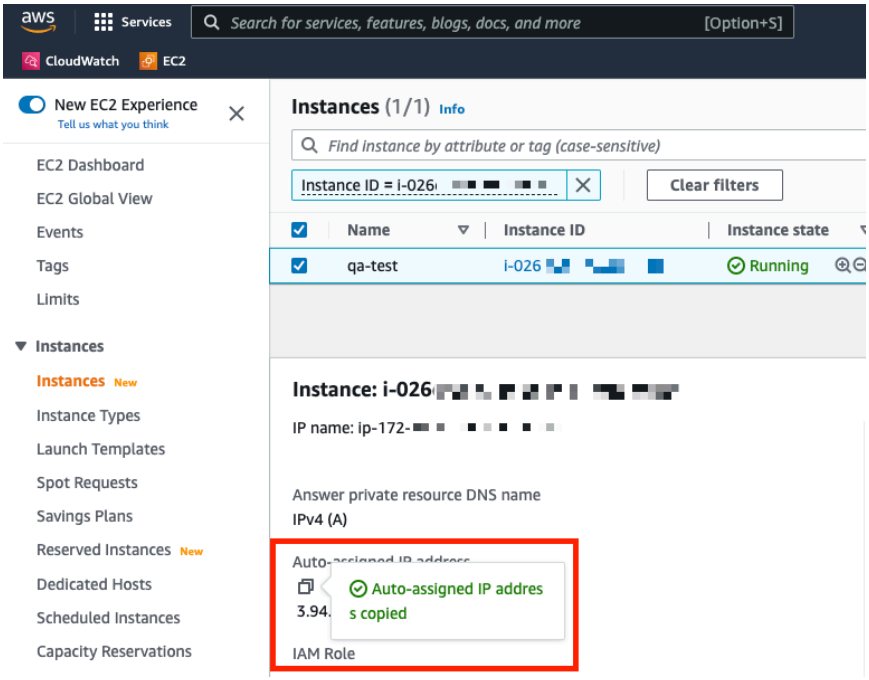


FIGURE 3-37. Auto-assigned IP address

Note

The auto-assigned IP address may change if the instance has been rebooted. Please refer to *Associating the Elastic IP Address with an Instance on page 3-39* for assigning a static IPv4 address to your instance.

14. Refer to *Opening StellarOne Management Console on page 3-43* for logging on StellarOne via a web browser, or *Accessing StellarOne via SSH on page 3-37* for accessing StellarOne via SSH.

Accessing StellarOne via SSH

This section describes how to access StellarOne via SSh.

Procedure

1. Find the StellarOne instance on the AWS EC2 and copy its auto-assigned IP address.

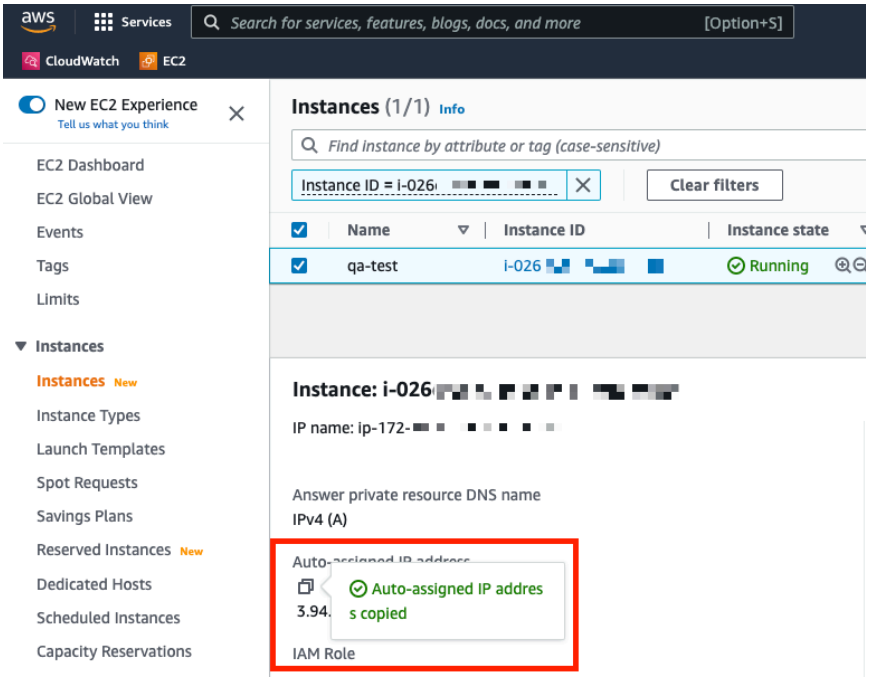


FIGURE 3-38. Auto-assigned IP address

2. Open the SSH terminal on your device and run the following command:
`ssh -i <private key>.pem admin@<auto-assigned IP address>`

Note

The auto-assigned IP address may change if the instance has been rebooted. Please refer to *Associating the Elastic IP Address with an Instance on page 3-39* for assigning a static IPv4 address to your instance.

Important

- Ensure that you use `admin` as the SSH login username.
- If you access StellarOne via SSH, it is not required to go through the OOBE process and change password.

3. Check if the service of StellarOne instance is activated and runnning.

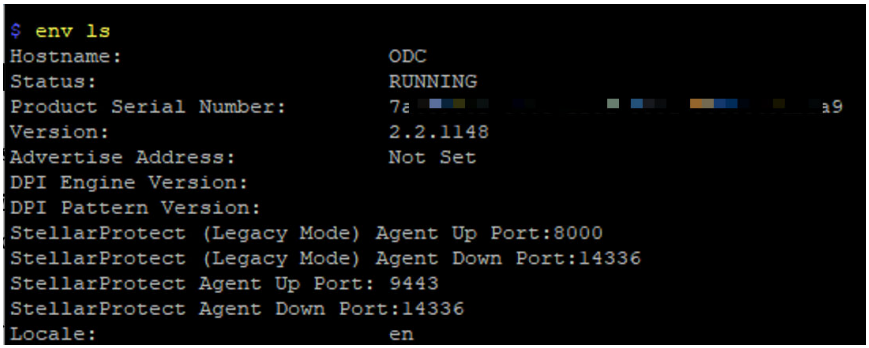


FIGURE 3-39. Check Service Status via SSH

Associating the Elastic IP Address with an Instance

The following section describes how to assign the Elastic IP addrdss to your StellarOne instance deployed from the AMI on AWS EC2 platform.

Note

The Elastic IP address is a static IPv4 address designed for dynamic cloud computing, and is allocated to your AWS account.

Procedure

1. Log on the AWS EC2 console and go to **Network & Security** > **Elastic IPs**.
2. Select the Elastic IP address to associate and choose **Actions** > **Associate Elastic IP address**.

3. For **Resource type**, select **Instance**.
4. Choose the target instance.

Note

You can search for a specific instance by typing relevant strings in the search bar.

5. (Optional) For **Private IP address**, specify a private IP address with which to associate the Elastic IP address.
6. Click **Associate**.

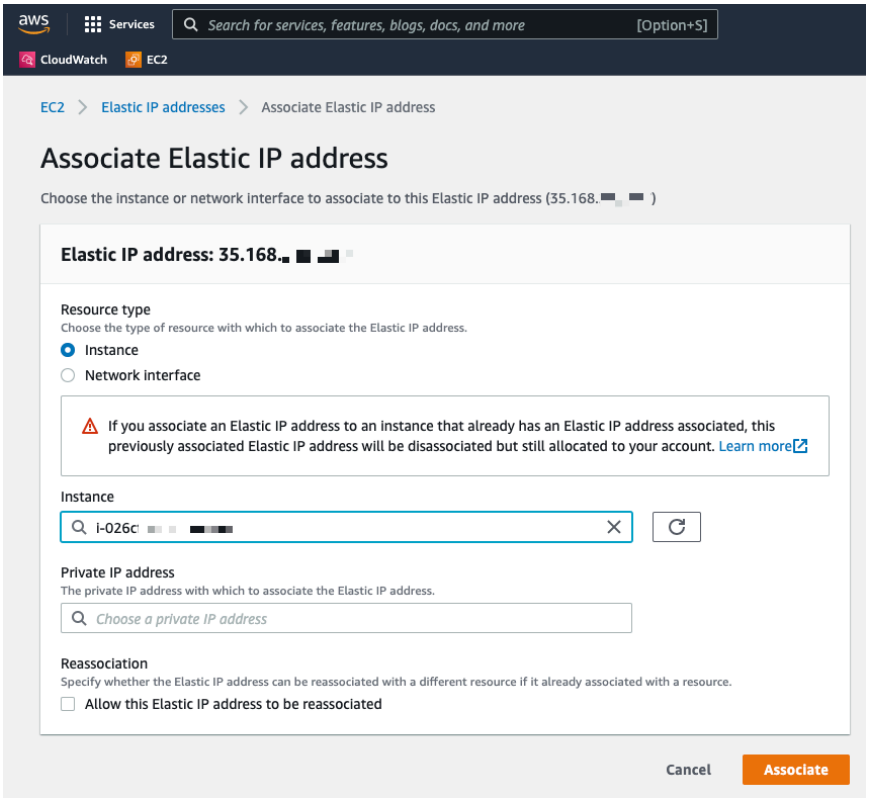


FIGURE 3-40. Associate the Elastic IP Address with an Instance

7. A message appears indicating the Elastic IP address has been associated to the target instance.

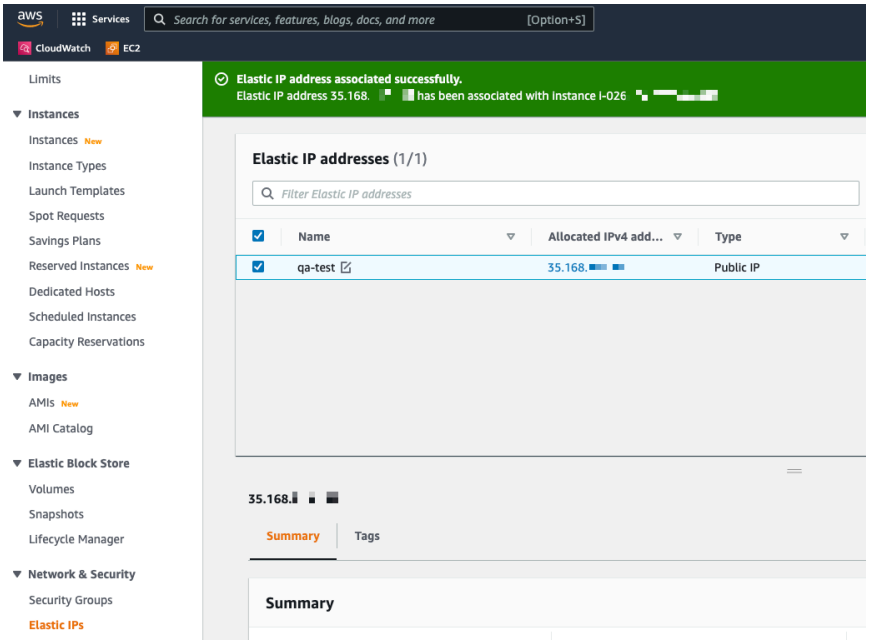


FIGURE 3-41. Associate Elastic IP Address

8. You can use the Elastic IP address to log on StellarOne via a web browser or via SSH now.

9. (Optional) Choose one of the methods below to access StellarOne via SSH with the Elastic IP address:

   - Replace the advertise address with the Elastic IP address by typing:

     ```
     env advertise <the elastic IP address>
     ```

   - Replace the advertise address with the Elastic Load Balancer address by typing:

     ```
     env advertise <the ELB address>
     ```

Opening StellarOne Management Console

Procedure

1. In a web browser, type the address of the StellarOne in the following format: `https://<targetserver IP address>`. The log on screen appears.
2. Enter your credentials (user ID and password).

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

   - User ID: `admin`
   - Password: `txone`
3. Click **Log On**.
4. If this is the first time the StellarOne instance being logged on, follow below procedures to complete the initial settings.

   a. The **Login Information Setup** window appears and prompts you to change password. Confirm your password settings by:

      - specifying your new password in the **New Password** text field.
      - specifying the password again in the **Confirm Password** text field.

      Note

      - For StellarOne 1.2 or above, the default login name is always `admin` and can not be changed by the user.
      - For StellarOne 1.0/1.1, in addition to changing the password, the user is also required to change the default login name in this step. The new login name can not be `admin`, `administrator`, `auditor` or `root`.

   b. Click **Confirm**. You will be automatically logged out. The **Log On** screen will appear again.

c. Log on again using your new credentials. The **License Activation** window appears.

d. Choose one of the ways to activate the license based on your license data and network environment:

- **License Key**

  1. Click **License Key**.
  2. Specify your license key in the text field.

  Note

  - The license key that contains more than 30 characters can be used for online or offline license activation.
  - The license key that contains less than 30 characters can only be used for online license activation.

    The license key with less than 30 characters can be used to download the license file, which can be used for offline license activation.

- **License File**:

  1. Click **License File**.
  2. Select the license file (a `.txt` file) to import.

  Note

  - The license file can be used for license activation if the StellarOne has no Internet connection.
  - If you don't have the license file on hand, see *Getting the License File on page 3-46*. A license file with less than 30 characters is required for downloading a license file.

e. Click **Apply**.

Note

A full license can not be converted to a trial license.

f. A success message appears. The license information also appears at the bottom of the **License Activation** window. Check if it matches the license data provided by your support provider.

g. Click **Continue**.

h. The **End User License Agreement and TXOne OT Intelligent Trust** window appears. Click the links to read the documents carefully and click the checkboxes to proceed to next step.

Note

It is recommended to enable **TXOne OT Intelligent Trust** to enhance security deployment. See *OT Intelligent Trust on page 3-48* for more details.

i. Specify the time settings such as the **Date and Time** as well as the **Time Zone**, and then click **Continue**.

j. The StellarOne console is ready for use now.

Note

After the initial settings are completed, the StellarOne allows various user accounts to log on remotely via a web browser.

5. (Optional) You can change your password by clicking the ID icon at the top right corner of the screen, and then selecting **Change Password**.

6. (Optional) For security reasons, you can manually log off by clicking the ID icon at the top right corner of the screen.

   a. A pop-up **Log Off** window appears. Click **Yes** to log out of StellarOne.

Note

You will be automatically logged off the console if no operations are performed within 30 minutes.

Getting the License File

Depending on the license data available from your support provider, you may need a license file to activate license for StellarOne.

Note

The license file can be used for license activation if the StellarOne has no Internet connection.

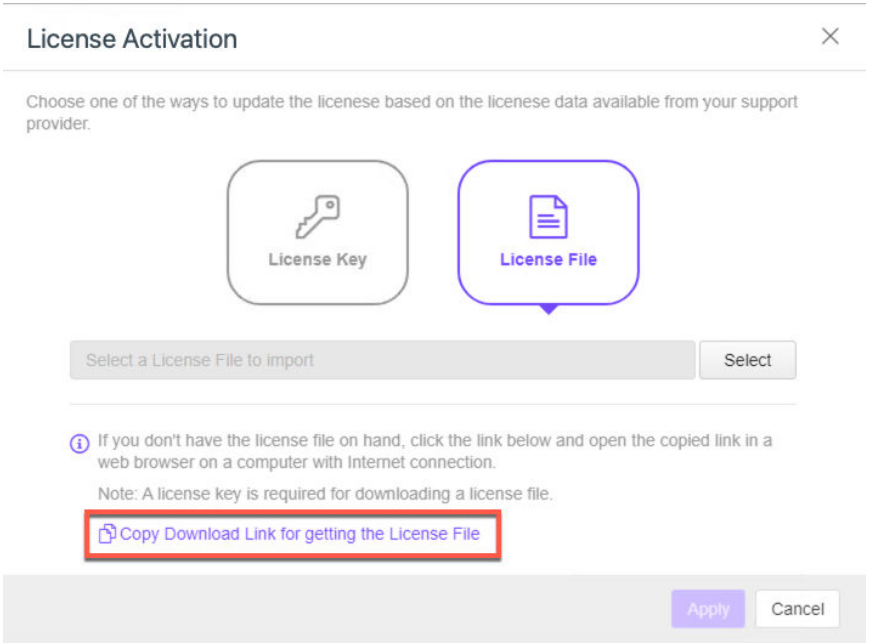
Procedure

1. Go to **Administration** > **License**
2. Click the **New License Key / File** button.
3. The **New License** window appears.
4. When you log on StellarOne using your new credentials after the **Login Information Setup** procedure, the **License Activation** window appears.
5. Click **License File**.
6. Click **Copy Download Link for getting the License File** at the bottom of the **License ActivationNew License** window.

Important

A license key is required for downloading a license file.

FIGURE 3-42. Copy Download Link for License File



7. **The Download Link has been copied** toast message appears.
8. Open the copied link in a web browser on a computer with Internet connection.
9. You will be directed to the TXOne **License File Management** screen. Specify your license key in the **License Key** field, and then click **Download**.

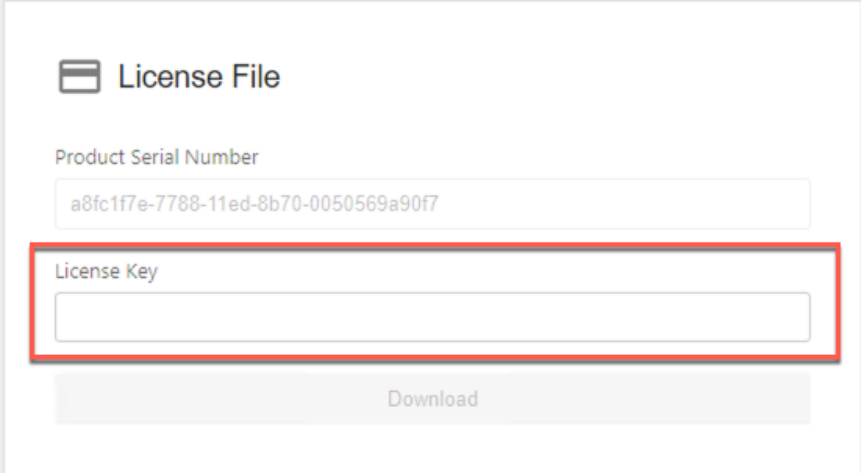


FIGURE 3-43. TXOne License File Management

10. A pop-up window appears showing the license information. Read it carefully and click **Yes** for downloading the license file.

> **Tip**
> You can send the license file to StellarOne that has no Internet connection via the internal secured network or a trusted portable device.

OT Intelligent Trust

When enabled, TXOne OT Intelligent Trust shares anonymous threat information with the Smart Protection Network, allowing TXOne to rapidly indentify and address new threats. You can disable TXOne OT Intelligent Trust anytime on this console.

Chapter 4

Configuring StellarOne via Command Line Interface (CLI)

This chapter describes how to configure some settings for StellarOne via command line interface (CLI).

Topics in this chapter include:

- *Using the StellarOne Command Line Interface (CLI) on page 4-2*
- *Configuring the IP Address via CLI on page 4-3*
- *Modifying Communication Ports via CLI on page 4-9*
    - *Configuring the Advertise Address via CLI on page 4-6*
- *Changing Language Settings via CLI on page 4-11*
- *Managing Docker Network via CLI on page 4-13*
- *Reseting Administrator's Password via CLI on page 4-13*

Using the StellarOne Command Line Interface (CLI)

The following section describes how to log on StellarOne and get a list of available commands via command line interface (CLI).

Procedure

1. Open the StellarOne VM console.
2. Log on by tying `root` as the user name, `txone` as the password.

   Note

   If the StellarOne instance is deployed from AMI on AWS EC2 platform, type `admin` as the user name and no password is needed.

3. After logging on the StellarOne console, type `help` command for a list of available commands.

```
$ help
vShell, version
The commands provided in:
  access-list     Manage the IP whitelists
  dx              Connection test for 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
  ssh             SSH to a device
  service         Manage the StellarOne service
  sftp            Send files via sftp
  web             Commands of the web management console
  stellar         Commands of the Stellar products
  locale          Locale setting
  network         Manage network for the StellarOne service

Shortcut table:
  Tab             Auto-complete or switch among options available
  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
$
```

FIGURE 4-1. Command list

Configuring the IP Address via CLI

The following section describes procedures of configuring the IP address settings for StellarOne instance via CLI.

Procedure

1. Type `iface ls` to get the IP address of the StellarOne instance.

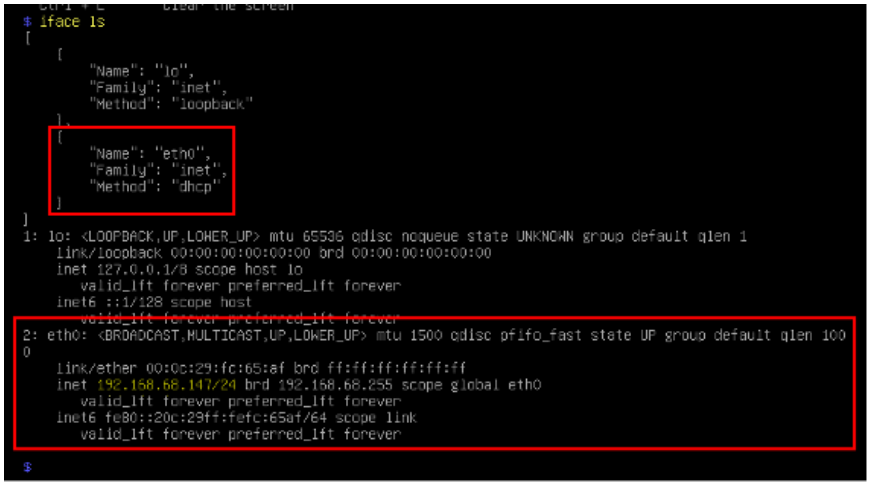


FIGURE 4-2. Getting the IP Address of StellarOne

2. Type `iface update` command for updating the settings of current 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
   ```

3. Check if the network interface settings are correct, and then type the following command to execute the change.

   ```
   iface restart eth0
   ```

4. Type following command again for viewing the new network interface settings.

   ```
   iface ls
   ```

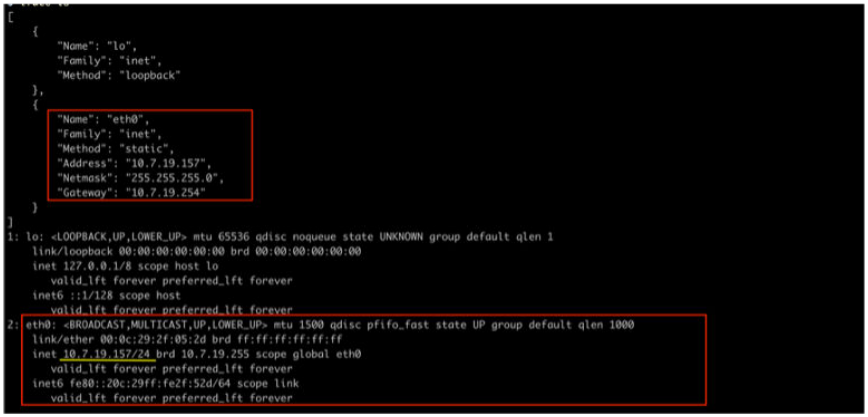


FIGURE 4-3. Viewing New Network Settings

5. Use the `resolv add` command to add a DNS server and `resolv ls` to view the DNS server list. For example, the following command adds `8.8.8.8` to the DNS server list

   ```
   resolv mode custom
   ```

   ```
   resolv add 8.8.8.8
   ```

6. Type following command to view the DNS server settings

   ```
   resolv ls
   ```

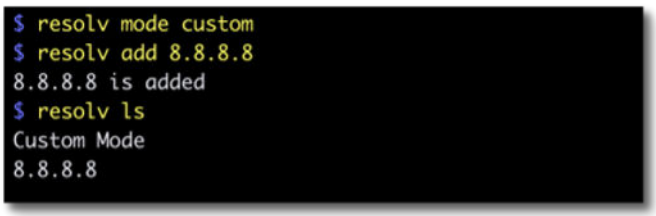


FIGURE 4-4. Viewing DNS Server Settings

7. Type following command to reboot the VM.

   ```
   reboot
   ```

Configuring the Advertise Address via CLI

The following section describes how to configure the IP address or FQDN as the StellarOne advertise address via CLI.

Procedure

1. Type `help` command for a list of available commands.
2. Type `env` and find the `advertise-addr` command.

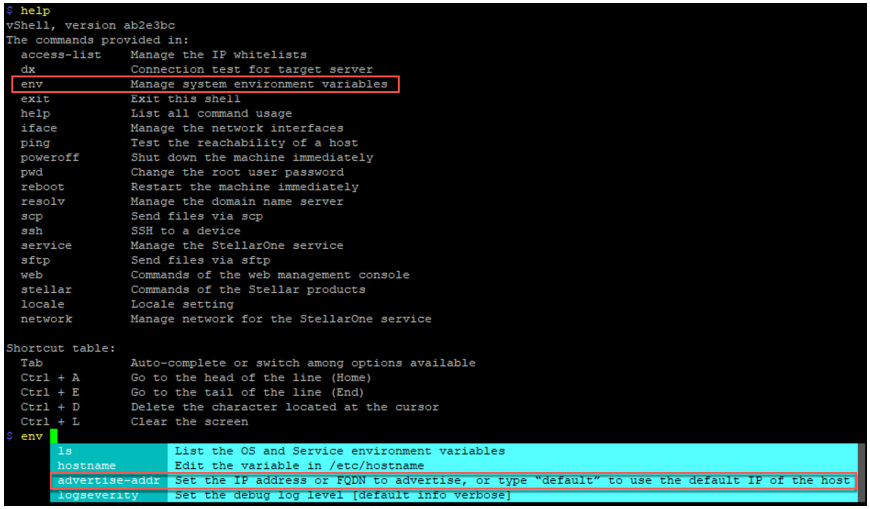


FIGURE 4-5. The advertise-addr command

3. Specify the advertise address for StellarOne after the `advertise-addr` command. The following example uses the FQDN as the advertise address:

```
env advertise-addr S1.txone.com
```

Note

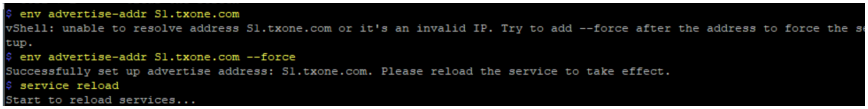
You can choose to specify the IP address, FQDN, or type `default` to use the default IP address for StellarOne.

4. (Optional) If the specified advertise address can not be resolved, type the `--force` command after it to force the setup:

   ```
   env advertise-addr S1.txone.com --force
   ```

5. Reload the StellarOne web console by typing:

   ```
   service reload
   ```



6. Type the following command to check the advertise address settings.

   ```
   env ls
   ```

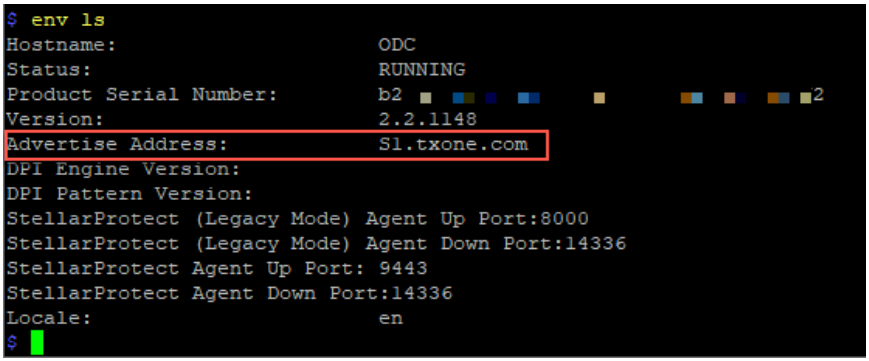


FIGURE 4-6. Checking Advertise Address Settings

7. After the setup, the agent installer package and the SAML SSO (Single Sign-On) metadata file downloaded from StellarOne should contain the configured advertise address, allowing the quick deployment for the agents to communicate with StellarOne or SSO login via the advertise address.

- See the examples below as the agent's config files (`StellarSetup.ini`) that contain the configured advertise address.

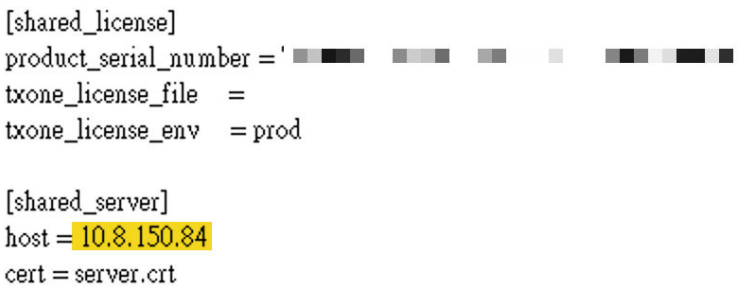


FIGURE 4-7. Use IP address as the advertise address in `StellarSetup.ini`

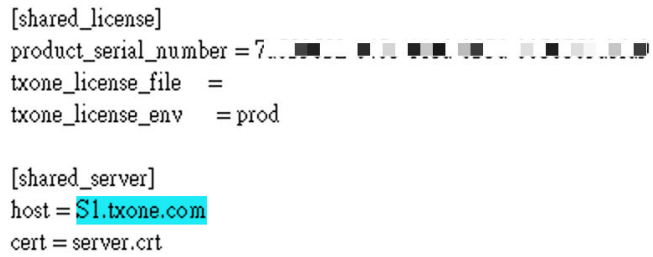


FIGURE 4-8. Use FQDN as the advertise address in `StellarSetup.ini`

- See the example below as the SAML SSO metada files tha contatin the configured advertise address.

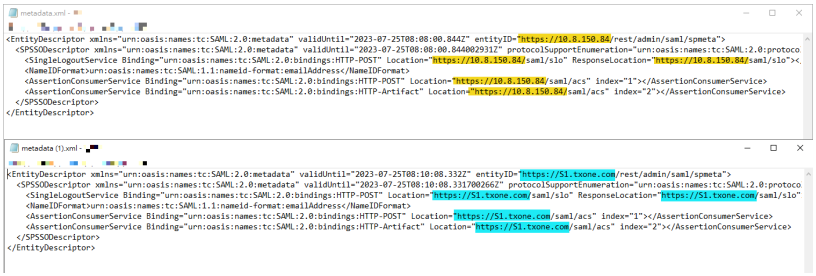


FIGURE 4-9. Use IP address or FQDN as the advertise address in SAML SSO metadata file

Modifying Communication Ports via CLI

Below section describes how to modify the communication ports for StellarOne instance via CLI.

Procedure

1. Type `env ls` command for the list of current communication ports.

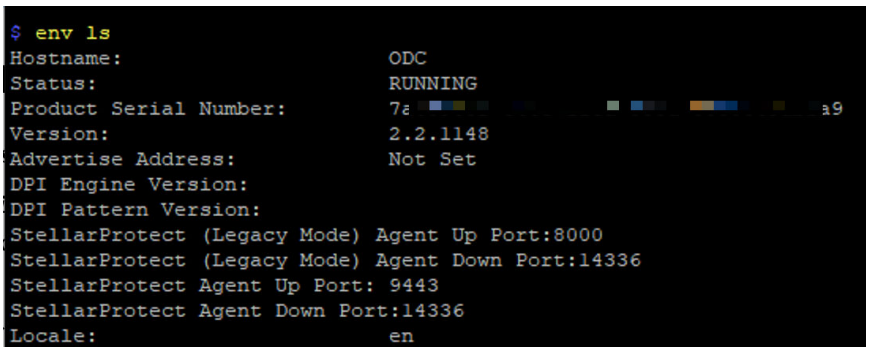


FIGURE 4-10. List of Current Communication Ports

2. Type `stellar` command for available agents to appear for selection.

FIGURE 4-11. Available Agents for Selection

3. Select one of the agents to edit its communication port.

FIGURE 4-12. Select the Agent for Editing Communication Port

4. Input the valid value for <up-port> and <down-port>.
   - <up-port>: Port for receiving data from agents.
   - <down-port>: Port for sending command to agents

Note

Make sure not to use StellarOne's service port. Please refer to **Table 2-7. StellarOne Occupied Ports** in *Ports and FQDN Used on page 2-10*.

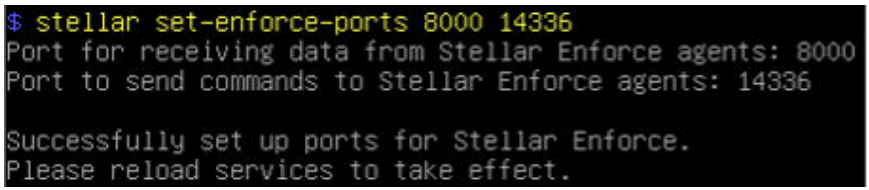


FIGURE 4-13. Agent's Communication Ports

5. Reboot.

Important

Please note the previously installed package does not contain the new port setting. Be sure to do either of the following actions after changing the commuication ports for StellarOne via CLI.

- Download the agent's installer package containing the new port setting from StellarOne, and install it on the agent.
- Modify the port setting accordingly in the `StellarSetup.ini` file in the agent's existing installer package, and reinstall it on the agent.

Changing Language Settings via CLI

Below section describes how to change language settings for StellarOne via CLI. The default language for StellarOne web console is English. You can change the language to Japanese following below procedures.

Procedure

1. Type `locale ja` command to switch the language to Japanese.
2. Reload the StellarOne web console

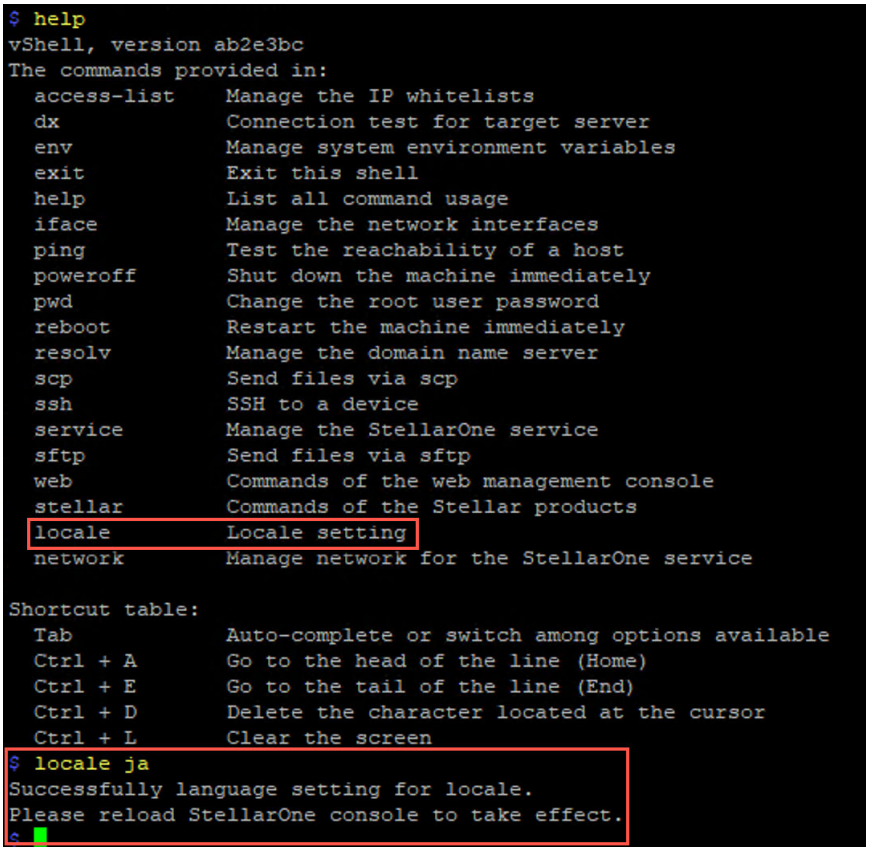


FIGURE 4-14. Reload StellarOne console

3. Type `env ls` command to check current language settings.

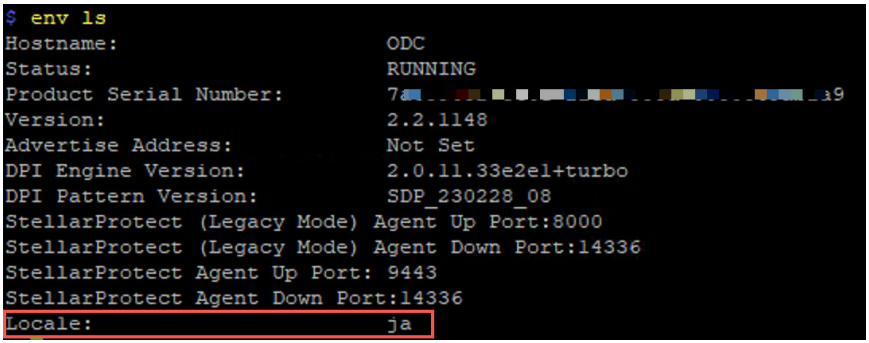


FIGURE 4-15. Check Language Settings

Managing Docker Network via CLI

The following section describes how to manage docker network on vShell for StellarOne via CLI.

Procedure

1. If `169.254.0.0/16` IP range is used in your network setting, please type `network internal-service-update <New IP>` command to set a new IP address for converting IP/16 subnet mask for docker daemon.
2. If you want to restore docker daemon back to the default-address-pools (`169.254.0.0/16`), type `network internal-service-reset` command.
3. Type `network internal-service-list` command to display the address pools of docker daemon configuration.

Reseting Administrator's Password via CLI

The following section describes how to reset administrator's password for StellarOne via CLI.

Procedure

1. Type `web reset admin` command to reset administrator's password.
2. The `reset OK!` message appears. The administrator's password has been reset.
3. Use the default credentials (user ID: `admin` / password: `txone`) to log on the StellarOne web console.

   Note

   For StellarOne 1.0/1.1, the default login name (user ID) is required to be changed by users. Be sure to use the changed default login name for accessing StellarOne 1.0 or 1.1.

4. The **Login Information Setup** window appears and prompts you to change password. Confirm your password settings by:
   a. specifying your new password in the **New Password** text field.
   b. specifying the password again in the **Confirm Password** text field.
5. Click **Confirm**. You will be automatically logged out. The **Log On** screen will appear again.
6. Log on again using your new credentials.

Chapter 5

Upgrade

This chapter describes the supported upgrade paths and methods for TXOne StellarOne.

Topics in this chapter include:

- *Supported Upgrade Paths on page 5-2*
- *Upgrade Methods on page 5-3*

Supported Upgrade Paths

The following table illustrates the supported upgrade paths for StellarOne installed in VMware or Windows Hyper-V system.

TABLE 5-1. Supported Upgrade Paths

PLATFORM	CURRENT VERSION	SUPPORTED TARGET UPGRADE VERSION	FIRMWARE UPGRADE*	MOUNT UPGRADE
VMWare Hyper-V	2.2	3.0 / 3.0 Service Pack 1	√	√
	2.1	2.2 / 3.0 / 3.0 Service Pack 1	√	√
	2.0	2.1 / 2.2 / 3.0 / 3.0 Service Pack 1	√	√
	1.2 Patch 1	2.0 / 2.1 / 2.2	N/A	√
	1.2	2.0 / 2.1	N/A	√
	1.2	1.2 Patch 1	√	√
VMWare	1.1	1.2 / 1.2 Patch 1	√	√
	1.0	1.1	N/A	√

Important

- Though StellarOne 3.0 requires more external disk capacity to use the advanced Operations Behavior Anomaly Detection feature, ensure you upgrade StellarOne to 3.0 before increasing the 2nd disk space for optimizing the disk usage.
- The 2nd disk space requirement for StellarOne varies depending on new features enabled in the latest verison. Check the Sizing Table in S1IG to ensure the storage requirement is fulfilled.
- Do not use firmware upgrade to update StellarOne 1.0, 1.2, or 1.2 Patch1 to a newer version (except for upgrading 1.2 to 1.2 patch 1). Use mount upgrade instead, which requires importing a new virtual image (`.ova` or `.vhdx` file) to a new instance and then mounting the 2nd external disk from the previous StellarOne instance. See *Mount Upgrade (VMware) on page 5-4* or *Mount Upgrade (Hyper-V) on page 5-7* for more details.
- StellarOne 1.2 patch1 equals to StellarOne1.2.2114
- TXOne Networks recommends always using firmware upgrade to update StellarOne if both upgrade options are available.

Upgrade Methods

This section describes two methods to upgrade StellarOne installed in VMware or Windows Hyper-Vsystem.

Topics in this section include:

- *Firmware Upgrade on page 5-3*
- *Mount Upgrade (VMware) on page 5-4*
- *Mount Upgrade (Hyper-V) on page 5-7*

Firmware Upgrade

This section describes how to perform firmware upgrade via the StellarOne web console.

Procedure

1. Download the `.acf` upgrade patch file (e.g., `TXOne-S1-acus.fw-3.x.xxxx.acf`) from the Download Center.
2. Log on the StellarOne web console and go to **Administration** > **Fimware**.
3. Click **Import** and select the `.acf` file downloaded in *Step 1*, and then click **Apply**.
4. Wait until the following window appears and read the upgrade notice carefully.

FIGURE 5-1. Firmware Install

Note

Before executing the firmware upgrade, please create a back up of the VM files first.

5. Click **Install Now** to start the upgrade.

Mount Upgrade (VMware)

This section describes how to perform mount upgrade for StellarOne on VMware ESXi system. The mount upgrade is performed by attaching the external disk of previous StellarOne instance to the StellarOne instance running new firmware version. The previously configured settings will be transferred to the new StellarOne instance, including:

- The UUID

- The pattern and firmware
- The agent list, policy settings, and StellarOne certificates
- The system configuration, including license, account information, security policies, and proxy/SSO settings
- Security event logs

Important

- Before executing a mount upgrade, please create a back up of the VM files first.
- StellarOne 2.0 ONLY supports mount upgrade from version 1.2 or 1.2 Patch 1. Make sure you upgrade StellarOne 1.1 to 1.2 or 1.2 Patch 1 before upgrading to 2.0.
- StellarOne 1.1 ONLY supports mount upgrade from version 1.0.

Procedure

1. Launch the new StellarOne instance. See *Deploying StellarOne on the VMware ESXi on page 3-2* for detailed instructions.
2. Close the previous StellarOne instance.

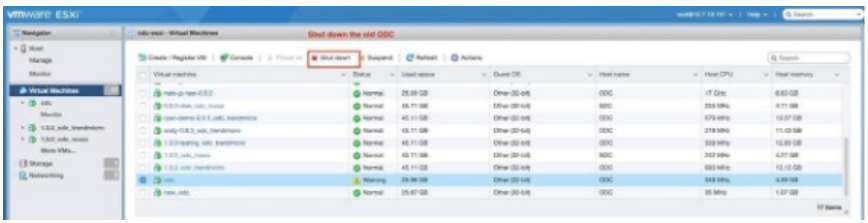


FIGURE 5-2. Shut Down the Previous VM

3. Attach the external disk of the existing StellarOne instance to the new StellarOne instance.

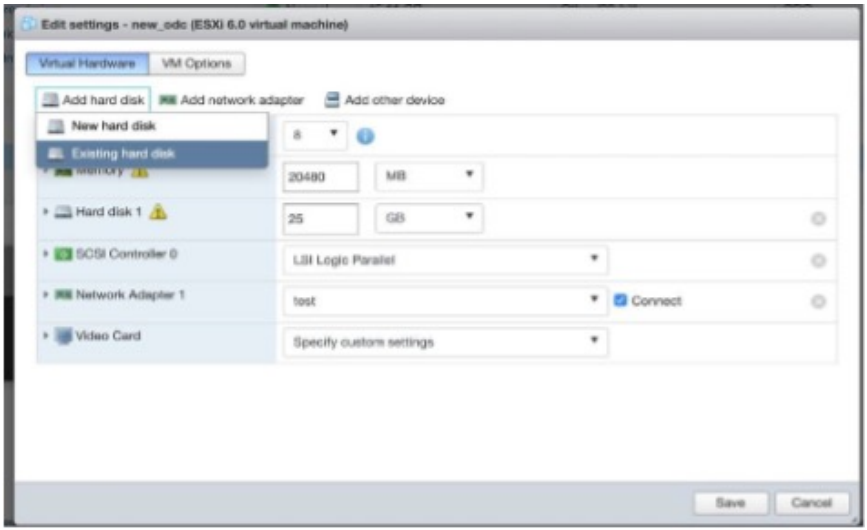


FIGURE 5-3. Select Existing (Previous) Hard Disk

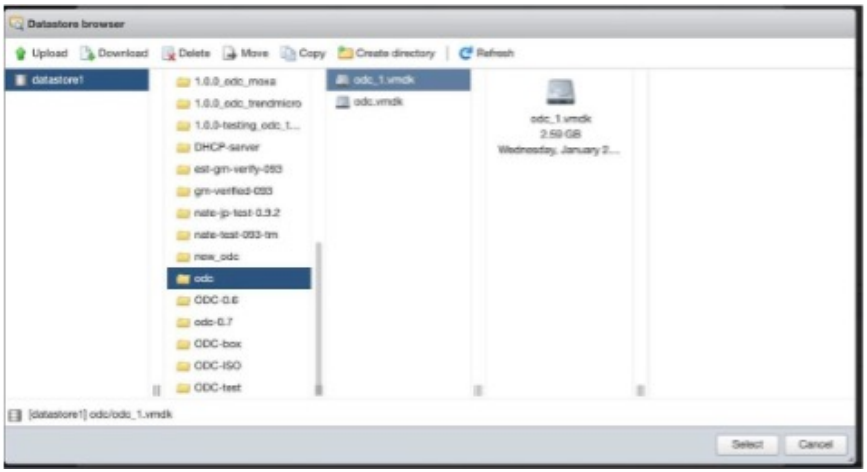


FIGURE 5-4. Attach to New VM

4. The data of the previous StellarOne instance will be migrated to new StellarOne instance.

5. The IP address of the new StellarOne instance must be the same as that of the previous StellarOne instance. If not, manually configure the IP address so the new StellarOne instance and agents can be connected to each other. Next time when the agents synchronize their status with the server, they will connect to the new StellarOne. By default, the agents synchronize with the server every 20 minutes.
6. If the proxy or scan component update source has already been defined in the previous StellarOne instance, please define it again via the web GUI of the new StellarOne instance.
7. If you want to change the language setting to Japanese for the new StellarOne instance, see *Changing Language Settings via CLI on page 4-11*.

Mount Upgrade (Hyper-V)

This section describes how to perform mount upgrade for StellarOne in Windows Hyper-V system. The mount upgrade is performed by attaching the external disk of previous StellarOne instance to the StellarOne instance running new firmware version. The previously configured settings will be transferred to the new StellarOne instance, including:

- The UUID
- The pattern and firmware
- The agent list, policy settings, and StellarOne certificates
- The system configuration, including license, account information, security policies, and proxy/SSO settings
- Security event logs

Important

- Before executing a mount upgrade, please create a back up of the VM files first.
- StellarOne 2.0 ONLY supports mount upgrade from version 1.2 or 1.2 Patch 1.

Procedure

1. Launch the new StellarOne instance. See *Deploying StellarOne to a Hyper-V System on page 3-12* for deployment details.
2. Close the previous StellarOne instance.
3. Click **Browse** and choose the existing disk.
4. Attach the external disk of previous StellarOne to the new StellarOne instance.

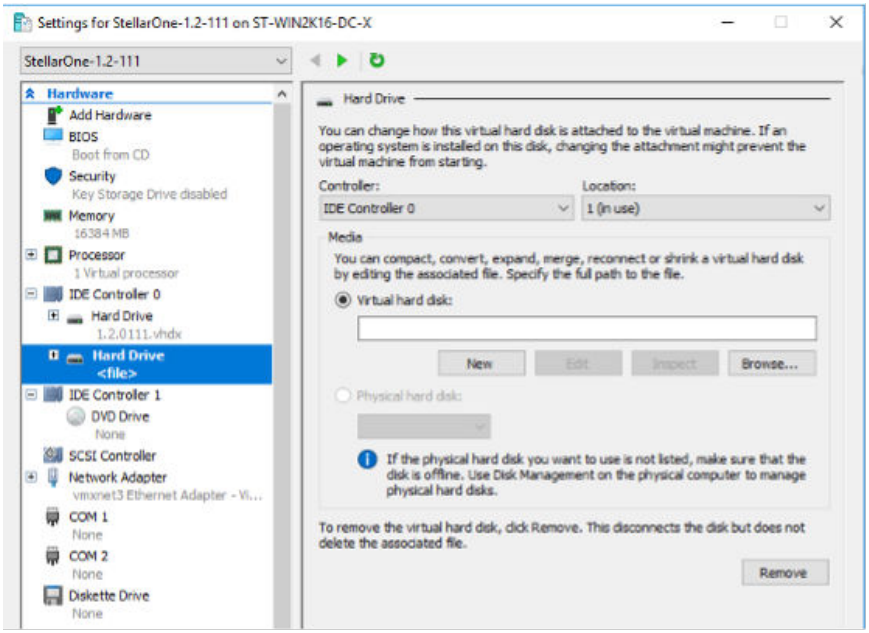


FIGURE 5-5. Shut Down the Previous VM

5. The data of the previous StellarOne instance will be migrated to new StellarOne instance.
6. The IP address of the new StellarOne instance must be the same as that of the previous StellarOne instance. If not, manually configure the IP address so the new StellarOne instance and agents can be connected to

each other. Next time when the agents synchronize their status with the server, they will connect to the new StellarOne. By default, the agents synchronize with the server every 20 minutes.

7. If the proxy or scan component update source has already been defined in the previous StellarOne instance, please define it again via the web GUI of the new StellarOne instance.

8. If you want to change the language setting to Japanese for the new StellarOne instance, see *Changing Language Settings via CLI on page 4-11*.

Chapter 6

Getting Help and Troubleshooting

Support for TXOne Networks products is provided mutually by TXOne Networks and Trend Micro. All technical support goes through TXone and Trend Micro engineers.

Learn about the following topics:

- *Troubleshooting Resources on page 6-2*
- *Contacting Trend Micro and TXOne on page 6-5*
- *Sending Suspicious Content to Trend Micro on page 6-6*
- *Other Resources on page 6-7*

Troubleshooting Resources

Before contacting technical support, consider troubleshooting with TXOne Networks StellarOne and visiting the followingTrend Micro online resources.

Self-Diagnosis

Identify and troubleshoot low disk space issues with StellarOne.

- *Resolving Low Disk Space Issues on page 6-2*

Resolving Low Disk Space Issues

To keep you informed of your disk usage, and any potential issues that may arise, StellarOne displays banners or modal windows at certain disk usage thresholds. When encountering such errors, you can check the following table for the features affected and take actions as suggested in the **Workaround** column.

However, the most efficient way to get rid of low disk space error caused by the 2nd HDD is to add more space to the drive or partition. Follow the procedures:

1. Go to **Dashboard** to check the Disk Usage widgets.
2. Check the following table for the features that will become unavailable at certain usage thresholds.
3. Extend the drive or partition which is running out of space.

Note

- If you take snapshots for the StellarOne virtual machine, ensure the snapshot files be consolidated before extending the partition space.
- Contact your support provider if you need to fix the low disk space error caused by the 1st HDD.

TABLE 6-1. Unavailable Features List due to Low Disk Space

UNAVAILABLE FEATURES	MENU PATH	DESCRIPTION	USAGE THRESHOLD	WORKAROUND
Firmware upgrade	**Administration** > **Update** > **Firmware**	Unable to import the StellarOne firmware for upgrade	• 1st HDD disk space less than 3 GB • 2nd HDD disk space on System partition less than 3 GB	Free up the 2nd HDD disk space on System partition by: • Deleting unused patch files • Purging unwanted agent debug logs
Agent patch file import	**Administration** > **Downloads/ Updates** > **Agent**	Unable to import Agent patch files	• 2nd HDD disk usage on System partition less than 20% • 2nd HDD disk usage on Database partition less than 20%	
Agent debug tool collection	StellarOne debug page (for SEG purpose)	Unable to collect the debug logs for StellarProtect or StellarProtect (Legacy Mode)		
Debug log level selection		Unable to select the **Info** or **Verbose** log level. Only the **Warn (Default)** level logs can be collected.		
Server debug tool collection		Unable to collect the debug logs for the StellarOne server		

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to https://success.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

   Tip

   To submit a support case online, visit the following URL:

   https://success.trendmicro.com/smb-new-request

   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro and TXOne combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware and https://www.encyclopedia.txone.com/ to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information

- Weekly malware reports

Contacting Trend Micro and TXOne

In the United States, Trend Micro and TXOne representatives are available by below contact information:

TABLE 6-2. Trend Micro Contact Information

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	https://www.trendmicro.com
Email address	support@trendmicro.com

TABLE 6-3. TXOne Contact Information

Address	TXOne Networks, Incorporated 222 West Las Colinas Boulevard, Suite 1650 Irving, TX 75039 U.S.A
Website	https://www.txone.com
Email address	support@txone.com

- Worldwide support offices:

  https://www.trendmicro.com/us/about-us/contact/index.html

  https://www.txone.com/contact/

- Trend Micro product documentation:

  https://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

https://success.trendmicro.com/solution/1059565

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

https://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, TXOne Networks may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

https://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Index

A

agent deployment plan, 2-9
- No. of Agents Deployed, 2-10
- Total Bandwidth / Deployment Task, 2-10

C

command line interface, 4-2
- change language settings, 4-11
- configure advertise address, 4-6
- configure IP address, 4-3
- manage docker network, 4-13
- modify communication ports, 4-9
- reset administrator's password, 4-13

F

Firmware upgrade, 5-3

H

hardware requirements for AWS EC2, 2-7
hardware requirements for Hyper-V, 2-5
- 1st HDD Space, 2-7, 2-8
- 2nd HDD Space, 2-7, 2-8
- Disk Space, 2-6, 2-8
- Max. No. of Agents, 2-7, 2-8
- memory size, 2-7, 2-8
- Min. No. of CPU, 2-7, 2-8
- No. of Logs, 2-6, 2-8

hardware requirements for VMware, 2-3
- Disk Space, 2-4
- No. of Logs, 2-4

I

installation, 3-29
- Deploy on AWS EC2, 3-30

Installation, 3-2, 3-12
- Deploy on Hyper-V, 3-12
- Deploy on VMware ESXi, 3-2

Installation flow, 3-2

M

Mount upgrade
- Hyper-V, 5-7
- VMware, 5-4

P

Ports and FQDN, 2-10
- FQDN, 2-11
- function, 2-11
- open port, 2-11

R

reference table
- Agent Remote Patch, 2-10
- Full Pattern Update, 2-10
- Incremental Pattern Update, 2-10

requirements, 2-2

S

StellarOne Occupied Ports, 2-12
- NTP, 2-12
- SSH, 2-12
- StellarOne internal service, 2-12
- StellarProtect (Legacy Mode) default port, 2-12

StellarProtect default port, 2-12
Web, 2-12
support
resolve issues faster, 6-6
Supported agent version, 2-12
system requirements, 2-2

U

Upgrade paths, 5-2

TXONE NETWORKS INCORPORATED

222 West Las Colinas Boulevard, Suite 1650
Irving, TX 75039 U.S.A
Email: support@txone.com
www.txone.com

Item Code: APEM39830/230913