Keep the Operation Running



TXOne StellarOne 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.: APEM39733/230619

Release Date: July 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 Hardware Requirements for Hyper-V System Deciding an Instance Type for StellarOne on AWS EC2	2-3 2-5
Platform	2-7
Planning Network Bandwidth for Agent Deployment	2-9
Ports and FQDN Used 2	2-10
Supported Agent Versions 2	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 4-0
Modifying Communication Ports via CLI 4-9
Changing Language Settings via CLI 4-12
Managing Docker Network via CLI 4-13
Reseting Administrator's Password via CLI 4-13

Chapter 5: Upgrade

ii

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

iii

Chapter 6: Technical Support

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

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 <u>docs@txone-networks.com</u>.



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

vi

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.

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
Г р Тір	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations

TABLE 1. Document Conventions

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

viii

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

1 - 1

Introduction

This section introduces TXOne Stellar One ${}^{\rm TM}$ 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

1-2

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 menagement 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 web console dashboard provides summarized information about monitored agents. Administrators can check deployed agent status easily, and can
	generate security reports (Legacy Mode only) related to specific agent activity for specified periods.
	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
Controlized Agent	Enable or disable agent Device Control
Management	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)

1-4

FEATURE	BENEFIT
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 provides following new features and enhancements.

FEATURE	Benefit
Cyber-Physical System Detection and Response (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 exclusive ransomware detection engine to defend against unexpected changes that may impact stability. Since every agent continuously analyzes its host device to establish and maintain a unique baseline fingerprint, in real-time, unexpected behaviors and deviations from this fingerprint can be detected at the individual agent level and then secondarily at the centralized control level to inform wider instability issues and prompt preventative actions to be taken.
Scan components displayed on the General Info for StellarProtect (Legacy Mode)	You can view the details of the scan components for the StellarProtect (Legacy Mode) agent on the General Info page now.
Add File Information in the exported event data	The exported event logs now contain the File Information details.

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

1-5

Chapter 2

2-1

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



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

Note

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

Minimum Supported Resolution

• 1366x768

2-2

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 (Recommend ED)	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.

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

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

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.



- 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.

Max. No. of Agents	Min. No. of CPU	Memory Size	1ST HDD Space	2ND HDD Space (Recommen ded)	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

TABLE 2-3. Sizing Table for Hyper-V

Max. No. of Agents	Min. No. of CPU	Memory Size	1ST HDD Space	2ND HDD Space (Recommen ded)	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

2-6



- 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.



Please refer to <u>Amazon EC2 Instance Types</u> 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 (Recommen ded)	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

2-7

Max. No. of Agents	Min. No. of CPU	Memory Size	1ST HDD Space	2ND HDD Space (Recommen ded)	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

<u>2-8</u>



- 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 I	Deploy	ment Plan
------------	---------	--------	-----------

TOTAL	No. of Agents Deployed				
BANDWIDTH / DEPLOYMEN T TASK	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.

FROM	То	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

TABLE 2-9. Ports and FQDN Used

2-11



Note

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

	TABLE 2-	10. Ste	llarOne (Occupie	ed 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.



SERVER VERSION	Agents Version			
STELLARONE	STELLARPROTECT	StellarProtect (Legacy Mode)	STELLARENFORCE	
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	

TABLE 2-11. Supported Agent Version



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

2-1

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

3-2

- 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.

Navigator	localhost.localdomain			
Manage	Get vCenter Server	1 Create/Register VM 🛛 🔂 Shut down	Reboot C	Refresh
	S Iocalm Version: State: Uptime:	ost. Jocaldomain 6.5.0 (Build 4564106) Normal (not connected to any vCenter Server) 10.23 days	CPU USED: 11.1 GHz MEMORY USED: 19.48 GB STORAGE USED: 308.34 GB	FREE: 2.5 GHz 82% CAPACITY: 13.6 GHz FREE: 12.35 GB 61% CAPACITY: 31.83 GB FREE: 149.91 GB 67% CAPACITY: 458.25 GB

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.

🔁 New virtual machine - StellarOne	
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 4 License agreements 5 Deployment options 6 Additional settings 7 Ready to complete 	Select OVF and VMDK files Select the OVF and VMDK files or OVA for the VM you would like to deploy Enter a name for the virtual machine. StellarOne Name of the StellarOne Instance Virtual machine names can contain up to 80 characters and they must be unique within each ESX instance.
	×
vm ware ⁻	
	Back Next Finish Cancel

FIGURE 3-3. Select OVF and VMDK files

3-4

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


FIGURE 3-4. Select storage

6. Select deployment options and click Next.



1 Select creation type	Deployment options						
2 Select OVF and VMDK files 3 Select storage	Select deployment options						
4 Deployment options 5 Ready to complete	Network mappings	NAT	VM Network			•	
	Disk provisioning	🖲 Th	n O Thick				

FIGURE 3-5. Deployment options

3-6

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

2 Select OVF and VMDK files	Ready to complete Review your settings selection b	efore finishing the wizard
4 Deployment options	Product	Unknown
5 Ready to complete	VM Name	StellarOne
	Disks	instance.vmdk
	Datastore	datastore1
	Provisioning type	Thin
	Network mappings	NAT: VM Network
	Guest OS Name	Debian_64
	Do not refresh y	our browser while this VM is being deployed.

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

Virtual Hardware VM Options)			
🔜 Add hard disk 🛤 Add netwo	rk adapter 🛛 🔚 Ad	dd other device		
New hard disk	1 1	0		
Existing hard disk				
* and memory	16384	MB 🔻		
Hard disk 1	25	GB 🔻		C
SCSI Controller 0	LSI Logic	Parallel	•	C
Network Adapter 1	VM Netwo	rk	▼ Connect	¢
Video Card	Specify cu	stom settinas	•	

Save Cancel

FIGURE 3-7. Edit settings - New hard disk

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

CPU	1 •	0			
Memory	16384	MB	•		
Hard disk 1	25	GB	•		6
Rew Hard disk	50	GB	▼ —→ Add a	an external disk	¢
SCSI Controller 0	LSI Logic	Parallel		•	C
Network Adapter 1	VM Netwo	ork		▼ Connect	C
Video Card	Specify cu	istom settings		•	

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*.



- 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.

🗹. 🗄 StellarOne		Norma	24.16 GB
Quick filters	٠	Make sure the	StellarOne instance is booted
	StellarO	ne	a
	Guest OS		Other (32-bit)
	Compatib	ility	ESXi 6.0 and later (VM version 11)
	VMware T	ools	No
	CPUs		8
	Memory		16 GB
	Click the	e window to loc	in the vShell of StellarOne

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.

Firtual Hardware VM Options				
🔜 Add hard disk 🛛 🛤 Add netw	ork adapter 🛛 📒 Ad	d other device		
CPU	8 🔻	Select the CPU i	tem to customize the nu	mber of CPU
Memory	16384	мв 🔻		
Hard disk 1	25	GB 🔻		0
Hard disk 2	50	GB 🔻		0
SCSI Controller 0	LSI Logic F	Parallel	•	0
Network Adapter 1	VM Netwo	rk	▼ Connect	0
Video Card	Specify cu	stom settings	•	

FIGURE 3-10. Select number of CPU

c. Configure the amount of Memory.

Add hard disk 🛤 Add netwo	rk adapter 🛛 💻 Ad	dd other device		
CPU	8 •	0		
Memory	16384	MB	Select the Memory item a of memory allocated to the	nd adjust the amoun e StellarOne instanc
▶ 🛄 Hard disk 1	25	GB	•	۵
Hard disk 2	50	GB	•	0
SCSI Controller 0	LSI Logic	Parallel		0
Network Adapter 1	VM Netwo	ork	▼ Sonnect	0
Video Card	Specify cu	istom settings	•	

FIGURE 3-11. Configure Memory



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

Hyper-V Manager		-	× c
🗢 🔿 🚾 🖬 📩			
Hyper-V Manager	Hyper-V Manager provides the tools and information you can use to manage a vitualization server.	Actions	
		Hyper-V Manager	*
	Introduction	View	•
	A virtualization server is a physical computer that provides the resources required to run virtual machines. You can use Hyper-V Manager to create, configure, and manage the virtual machines on a virtualization server.	Help	
	You can use what insphrens to un offerent wolkloads. Each virtual nuclines curs in an isolated execution environment, which gives you the finability to un offerent operating systems and applications on one physical computer.		

FIGURE 3-12. Hyper-V Manager

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

Before You Begin	This wizard helps you create a virtual machine. You can use virtual machines in place of physical
Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	computers for a variety of uses. Fou can use this wizard to configure the virtual machine how, and you can change the configuration later using Hyper-V Manager. To create a virtual machine, do one of the following: • Click Finish to create a virtual machine that is configured with default values. • Click Next to create a virtual machine with a custom configuration.
	Do not show this page again

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.

🖳 New Virtual Machine Wiz	ard >
💴 Specify Gen	eration
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	 Choose the generation of this virtual machine. Generation 1 This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V. Generation 2 This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system. Image: Once a virtual machine has been created, you cannot change its generation. More about virtual machine generation support
	< Previous Next > Finish Cancel

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

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

Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Specify the amoun MB through 12582 recommended for 1 Startup memory: Use Dynamic M When you dee use the virtua	t of memory y 12 MB. To in the operating 16384 Memory for th ide how muc machine an	to allocate to thin prove performa system. IB is virtual machin h memory to ass d the operating s	s virtual n nce, sper e. sign to a v system th	nachine. You cify more thar /irtual machini at it will run.	can specify an an the minimum am a, consider how y	rount from 32
--	--	--	---	--	--	--	---------------

FIGURE 3-16. Assign Memory for Virtual Machine



lor furth or aga

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**.

Each new virtual m virtual switch, or it	achine includes can remain dis	s a network adapt connected.	er. You can conf	igure the network a	adapter to us
Connection: Inte	nal-Switch				~
Not	Connected	-hit Maturali Car		of Costale	
Inter	nal-Switch	abit NetWork Con	necuon #2 - virt	ual Switch	
	Each new virtual m virtual switch, or it Connection: Inter Not (Inter Inter	Each new virtual machine include: virtual switch, or it can remain dis Connection: Internal-Switch Not Connected Inte(R) 82574. Gir Internal-Switch	Each new virtual machine includes a network adapt virtual switch, or it can remain disconnected. Connection: Internal-Switch Not Connected Inte(R) 82574. Gigabit Network Con Internal-Switch	Each new virtual machine includes a network adapter. You can conf virtual switch, or it can remain disconnected. Connection: Internal-Switch Not Connected Intel(R) 82574. Gigabit Network Connection #2 - Virt Internal-Switch	Each new virtual machine includes a network adapter. You can configure the network a virtual switch, or it can remain disconnected. Connection: Internal-Switch Not Connected Intel(R) 82574. Ggabit Network Connection #2 - Virtual Switch Internal-Switch

FIGURE 3-17. Configure Networking for Virtual Machine

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



efore You Begin pecify Name and Location pecify Generation ussign Memory	A virtual machine storage now or o O Create a virt Use this optic	e requires storage so that you can install an operating s configure it later by modifying the virtual machine's proj ual hard disk on to create a VHDX dynamically expanding virtual hard	system. You can specify the perties. d disk.
Configure Networking	Name:	StellarOne.vhdx	
onnect Virtual Hard Disk	Location:	E:\Hyper_V_disk\	Browse
ummary	Size:	127 GB (Maximum: 64 TB)	
	Use an existi Use this optic	ng virtual hard disk on to attach an existing virtual hard disk, either VHD or	VHDX format.
	Location:	E:\StellarOne_image\3.0.1161.vhdx	Browse
	O Attach a virt	ual hard disk later	

FIGURE 3-18. Connect Virtual Hard Disk

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

Before You Begin Specify Name and Location	You have successfully completed the New Virtual Machine Wizard. You are about to create following virtual machine.	e the
Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk	Name: StellarOne Generation: Generation 1 Memory: 8192 MB Network: Internal-Switch	
Summary	Hard Disk: E:\StellarOne_image\3.0.1161.vhdx (VHDX, dynamically expanding)	
	To create the virtual machine and close the wizard, click Finish.	

FIGURE 3-19. Completing the New VM Wizard

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



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.

 New Virtual Hard Disk Wi Choose Disk 	card k Format
Before You Begin Choose Disk Format Choose Disk Type Specify Name and Location Configure Disk Summary	What format do you want to use for the virtual hard disk? VHD Supports virtual hard disks up to 2,040 GB in size. VHDX This format supports virtual disks up to 64 TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012.
	< Previous Next > Finish Cancel

FIGURE 3-23. Choose Disk Format

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

🛓 Choose Disl	сТуре
Before You Begin Choose Disk Format Choose Disk Type	What type of virtual hard disk do you want to create? Fixed size This type of disk provides better performance and is recommended for servers running applicat with high levels of disk activity. The virtual hard disk file that is created initially uses the size of
Configure Disk Summary	 Dynamically expanding This type of disk provides better use of physical storage space and is recommended for server running applications that are not disk intensive. The virtual hard disk file that is created is small initially and changes as data is added. Differencing This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the part disk, so that you can revert the changes easily. All children must have the same virtual hard dis format as the parent (VHD or VHDX).

FIGURE 3-24. Choose Disk Type

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

🛓 New Virtual Hard Disk V	Vizard		>
🚢 Specify Na	ame and Loo	tion	
Before You Begin Choose Disk Format	Specify t Name:	name and location of the virtual hard disk file. 2nd_Disk_for_StellarOne.vhdx	
Specify Name and Location	Location:	E:\StellarOne_image\	Browse
Configure Disk			

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.

Before You Begin Choose Disk Format Choose Disk Type Specify Name and Location	You can create a blank virtual hard disk or copy the con Create a new blank virtual hard disk Size: 50 GB (Maximum: 64 TB) Copy the contents of the specified physical disk:	itents of an existing physical disk.
conngure olsk. Summary	Physical Hard Disk (\PHYSICALORIVE0 \\PHYSICALDRIVE1 \\PHYSICALDRIVE2	Size 39 GB 299 GB 24 GB
	Copy the contents of the specified virtual hard disk	Destances

FIGURE 3-26. Configure Disk for StellarOne

i. Click Next to check your settings.



 New Virtual Hard Disk Wi Completing 	the New Virtual Hard Disk Wizard	×
Before You Begin Choose Disk Format Choose Disk Type Speofy Name and Location Configure Disk Summary	You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk. Description: Format: VHDX Type: dynamically expanding Name: 2nd_Disk_for_StellarOne.vhdx Location: E:\StellarOne_image Size: S0 GB To create the virtual hard disk and dose this wizard, dick Finish.	
	< Previous Next > Finish Cancel	

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**.

Hyper-V Manager File Action View Help						
Hyper-V Manager	Virtual Machines					
	Name	State	CPU Usage	Assigned Memory	Uptime	Status
	StellarOne	Connect				
	1.2.0177	Settings		16384 MB	00:08:36	
		Start				
		Checkpoint				
	<	Move				>
	Checkpoints	Export				\odot
	StellarOne	Rename Delete				
	Cre	Enable Replica	ation	5 AM	Clustered: No	
	Con Gen	Help				

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.

Stell	larOne	~	. ▲ . ►	Ü					
* 1	Hardware	^	D P	rocessor -					
1	Add Hardware								
E	BIOS		You ca	an modify ti	he number of	t virtual proces	sors based on the	e number of p	rocessors o
	Boot from CD		uie pi	ryaicai comp		ar diso mouny (ourier resource c	ond of accords	•
	Security Key Storage Drive disabled		Numb	er of virtual	processors:		4		
	Memory		Res	ource contro	ol				
_	8192 MB		You	u can use re	esource contr	rols to balance	resources amon	g virtual machi	ines.
•	Processor		Virt	tual machine	e reserve (pe	rcentage):	0		
	4 Virtual processors								
•	IDE Controller 0		Per	cent of tota	al system res	ources:	0		
	🗈 👝 Hard Drive								
	3.0.1161.vhdx		Virt	tual machine	e limit (percer	ntage):	100		
	 Hard Drive 2nd_Disk_for_StellarOne.v 	2	Per	cent of tota	al system res	ources:	33		
	IDE Controller 1		Pal	ative weigh			100		
	OVD Drive			auve weigh					
10	None								
-	SCSI Controller								
+	Vetwork Adapter								
2	Internal-Switch								
1	None								
1	COM 2								
2	None								
1	Diskette Drive								
	None								
* 1	Management								
1	Name StellarOne								
-	Integration Services								
	Some services offered								
0	Checkpoints								
	Production	~							

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.



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.

aws n	narketnlar	م				0
About	Catanorias =	Dalivary Mathoda 📼	Solutions = AWS IO =	Pasources w Vour Stand List		
About +	Categories +	Delivery Methous +		TxOne StellarOne Mar	nagement Console	
			Launch this	s software		
			Review the launch cor	nfiguration details and follow the	instructions to launch this software.	
			Configuration deta	ails 64-bit (x86) Amazon Machin TxOne StellarOne Managem	e Image (AMI) ent Console	
			Software version Region	running on m3.medium 2.0.9128 US East (N. Virginia)		
			Usage instruction	ons		
			Select a launch act Launch through EC ✓ Launch from Webs	tion C2	Choose this action to launch from this website	
			EC2 Instance Type	*	Memory: 3.75 GiB CPU: 3 EC2 Compate Units (1 virtual core) Storage 1: 4 x 68 S50 Network Performance: Moderate	

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.

stance type	
c5.large Family: c5 2 vCPU 4 GiB Memory	Compare instance types
٩١	roduct.
Family: 141 128 VCPU 1024 GIB Memory	
i 4i.8xlarge Family: i4i 32 vCPU 256 GiB Memory	
i 4i.metal Family: i4i 128 vCPU 1024 GIB Memory	elected key pair before you launch
im4gn.large Family: im4gn 2 vCPU 8 GiB Memory The architecture (x86_64) of the selected AMI is not supported by this instance type.	
im4gn.2xlarge Family: im4gn 8 vCPU \$32 GiB Memory The architecture (x86_64) of the selected AMI is not supported by this instance type.	C Create new key pair
im4gn.8xlarge Family: im4gn 32 vCPU 128 GiB Memory The architecture (x86_64) of the selected AMI is not supported by this instance type.	Edit
im4gn.xlarge Family: im4gn 4 vCPU 16 GiB Memory The architecture (x86_64) of the selected AMI is not supported by this instance type.	
im4gn.4xlarge Family: im4gn 16 vCPU 64 GiB Memory The architecture (x86_64) of the selected AMI is not supported by this instance type.	
im4gn. 16xlarge Family: im4gn 64 vCPU 256 GiB Memory The architecture (x86_64) of the selected AMI is not supported by this instance type.	
inf1.xlarge Family: inf1 4 yCPU 8 GiB Memory	

FIGURE 3-32. Select an Instance Type

Instance type Info				
nstance type				
AT the second				
t5.xlarge				
T3.Xlarge Family: t3 4 vCPU 16 GiB Memory	-	Compare instance types		
t3.xtarge Family: t3 4 vCPU 16 GiB Memory On-Demand Linux pricing: 0.1664 USD per Hour	•	Compare instance types		

FIGURE 3-33. Information of the Selected Insance Type



- 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.



A 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.

Network Info vpc-57becc2a Subnet Info No preference (Default subnet in any availability zone) Auto-assign public IP Info Enable Firewall (security groups) Info A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance. C Create security group Select existing security group We'll create a new security group called 'launch-wizard-67' with the following rules: Allow SSH traffic from Helips you connect to your instance Anywhere 0.0.0/0 Anywhere C Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server	Network settings Info			Edit
vpc-57becc2a Subnet info No preference (Default subnet in any availability zone) Auto-assign public IP info Enable Firewall (security groups) info A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance. Image: Create security group Select existing security group Image: Create security group called 'launch-wizard-67' with the following rules: Image: Allow SSH traffic from Heinternet To set up an endpoint, for example when creating a web server Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server	Network Info			
Subnet Info No preference (Default subnet in any availability zone) Auto-assign public IP Info Enable Firewall (security groups) Info A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance. C Create security group Select existing security group We'll create a new security group called 'launch-wizard-67' with the following rules: Allow SSH traffic from Helps you connect to your instance Anywhere 0.0.0.0/0 Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server To set up an endpoint, for example when creating a web server	/pc-57becc2a			
No preference (Default subnet in any availability zone) Auto-assign public IP info Enable Firewall (security groups) info A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance. Create security group Select existing security group We'll create a new security group Called 'launch-wizard-67' with the following rules: Allow SSH traffic from Helps you connect to your instance Anywhere 0.0.0.0/0 Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server Cost up an endpoint, for example when creating a web server	Subnet Info			
Auto-assign public IP Info Enable Firewall (security groups) Info A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance. Create security group We'll create a new security group called 'launch-wizard-67' with the following rules: Allow SSH traffic from Helps you connect to your instance O.0.0.0/0 Anywhere 0.0.0.0/0 Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server Coset up an endpoint, for example when creating a web server	No preference (Default subnet in any av	ailability zone)		
Enable Firewall (security groups) info A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance. Cereate security group Select existing security group We'll create a new security group called 'launch-wizard-67' with the following rules: Allow SSH traffic from Helps you connect to your instance Anywhere 0.0.0.0/0 Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server To set up an endpoint, for example when creating a web server	Auto-assign public IP Info			
Firewall (security groups) Info A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance. Create security group Select existing security group We'll create a new security group called 'launch-wizard-67' with the following rules: Allow SSH traffic from Heinternet To set up an endpoint, for example when creating a web server Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server	Enable			
Helps you connect to your instance 0.0.0.0/0 Image: Constant of the internet 0.0.0.0.0/0 Image: Constant of the interne 0.0.0.0.0/0	Create security group We'll create a new security group called Allow SSH traffic from	Select existin	ng security group	
 Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server 	Helps you connect to your instance	0.0.0/0	•	
i o set up an enopoint, tor example when creating a web server	 Allow HTTPS traffic from the internet To set up an endpoint, for example when c Allow HTTP traffic from the internet 	rt reating a web server		
	To set up an endpoint, for example when c	reating a web server		
▲ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting × security group rules to allow access from known IP addresses only.	▲ Rules with source of 0.0.0.0/0 all security group rules to allow acce	ow all IP addresses to a ess from known IP addre	ccess your instance. We recomn esses only.	nend setting $ imes$

FIGURE 3-35. Network settings

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

Configure s	torage Info	Advanced
1x 25	GiB gp3 Root volume (Not encrypted)	
1x 50 \$	GiB gp3 w EBS volume (Not encrypted) Rem	ove
(i) Free tier el	gible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic stor	age $ imes$
Add new volu	me	
0 x File systems		Edit

FIGURE 3-36. Configure Storage

d. Click Launch Instance.



3-36

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

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

WS III Services Q Search for services, features, blogs, docs, and more [Option+S]		
점 CloudWatch 🧧 EC2		
New EC2 Experience X Tell us what you think	Instances (1/1) Info Q. Find instance by attribute or tag (case-sensitive) Instance ID = I-025 Instance ID = I-025	
EC2 Dashboard EC2 Global View		
Events	✓ Name ▼ Instance ID Instance state Name	
Tags	🗹 qa-test i-026 💶 💶 🥥 Running 🔍 🖸	
Limits		
▼ Instances		
Instances New	Instance: i-026	
Instance Types	IP name: in-172-	
Launch Templates		
Spot Requests	Answer private resource DNS name	
Savings Plans	IPv4 (A)	
Reserved Instances New	Auto-scianod IP address	
Dedicated Hosts	□ O Auto-assigned IP addres	
Scheduled Instances	3.94. s copied	
Capacity Reservations	IAM Role	

FIGURE 3-37. Auto-assigned IP address



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

 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.

\$ env ls	
Hostname:	ODC
Status:	RUNNING
Product Serial Number:	7ē 📕 a9
Version:	2.2.1148
Advertise Address:	Not Set
DPI Engine Version:	
DPI Pattern Version:	
StellarProtect (Legacy Mode)	Agent Up Port:8000
StellarProtect (Legacy Mode)	Agent Down Port:14336
StellarProtect Agent Up Port:	9443
StellarProtect Agent Down Por	t:14336
Locale:	en

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.

P 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.
| aws Services | Q Search for services, features, blogs, docs, and more [Option | on+S] |
|--|--|---------------------------------------|
| 점 CloudWatch 🛛 🙋 EC2 | 2 | |
| EC2 > Elastic IP a | addresses > Associate Elastic IP address | |
| Associate | Elastic IP address | |
| Choose the instance | e or network interface to associate to this Elastic IP address (35.168. \blacksquare) | |
| Elastic IP ad | dress: 35.168. | |
| Resource type
Choose the type of
Instance | resource with which to associate the Elastic IP address. | |
| ▲ If you ass
previous | sociate an Elastic IP address to an instance that already has an Elastic IP address
ly associated Elastic IP address will be disassociated but still allocated to your ac | associated, this
count. Learn more |
| Instance | | |
| Q, i-026c' ≡ | × (| 3 |
| Private IP addres | 55
ess with which to associate the Elastic IP address. | |
| Q Choose a p | rivate IP address | |
| Reassociation
Specify whether th
Allow this El | e Elastic IP address can be reassociated with a different resource if it already associated with astic IP address to be reassociated | a resource. |
| | c | ancel 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.

aws services Q Searc	th for services, features, blogs, docs, and more [Option+S]	
점 CloudWatch 🔗 EC2		
Limits	Elastic IP address associated successfully. Elastic IP address 35.168. Elastic IP address 35.168.	
▼ Instances		
Instances New		
Instance Types	Elastic IP addresses (1/1)	
Launch Templates	Q Filter Elastic IP addresses	
Spot Requests		
Savings Plans	☑ Name ▽ Allocated IPv4 add ▽ Type ▽	
Reserved Instances New	☑ qa-test 🗹 35.168.■■ Public IP	
Dedicated Hosts		
Scheduled Instances		
Capacity Reservations		
▼ Images		
AMIS New		
AMI Catalog		
Elastic Block Store		
Volumes		
Snanshots	35.168.	
Lifecycle Manager	Summary Tags	
an augura i tantigur		
Network & Security		
Security Groups	Summary	
Elastic IPs		

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.



- 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.

3-43

- **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.



- 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.



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.
- Click Continue. g.
- 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.



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

- (Optional) You can change your password by clicking the ID icon at the 5. top right corner of the screen, and then selecting Change Password.
- (Optional) For security reasons, you can manually log off by clicking the 6. ID icon at the top right corner of the screen.
 - A pop-up **Log Off** window appears. Click **Yes** to log out of StellarOne. a.



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

available from your support
Select
open the copied link in a

- 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**.

Product Serial N	umber		
a8fc1f7e-7788	-11ed-8b70-0050	569a90f7	
License Key			
License Key			

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.



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

4-1

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

4-2

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



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.

<pre>\$ help</pre>	
vShell, version	
The commands pro	vided 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 if ace 1s to get the IP address of the StellarOne instance.



FIGURE 4-2. Getting the IP Address of StellarOne

2. Type if ace 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

4-4



FIGURE 4-3. Viewing New Network Settings

5. Use the resolv add command to add a DNS server and resolv 1s 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:



💡 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

\$ env ls	
Hostname:	ODC
Status:	RUNNING
Product Serial Number:	b2 1 1 1 1 1 1 1 1
Version:	2.2.1148
Advertise Address:	Sl.txone.com
DPI Engine Version:	
DPI Pattern Version:	
StellarProtect (Legacy Mode) A	Agent Up Port:8000
StellarProtect (Legacy Mode) #	Agent Down Port:14336
StellarProtect Agent Up Port:	9443
StellarProtect Agent Down Port	:14336
Locale:	en
\$	

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.

[shared_license]
product_serial_number ='
txone_license_file =
txone_license_env = prod
[shared_server]
host = 10.8.150.84
cert = server.crt



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.

\$ env ls	
Hostname:	ODC
Status:	RUNNING
Product Serial Number:	7a a9
Version:	2.2.1148
Advertise Address:	Not Set
DPI Engine Version:	
DPI Pattern Version:	
StellarProtect (Legacy Mode) A	Agent Up Port:8000
StellarProtect (Legacy Mode) A	Agent Down Port:14336
StellarProtect Agent Up Port:	9443
StellarProtect Agent Down Port	:14336
Locale:	en

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.

stellar set-enforce-ports set-enforce-ports Edit the communication ports for Stellar Enforce agents set-protect-ports Edit the communication ports for Stellar Protect agents

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*.

```
$ stellar set-enforce-ports 8000 14336
Port for receiving data from Stellar Enforce agents: 8000
Port to send commands to Stellar Enforce agents: 14336
Successfully set up ports for Stellar Enforce.
Please reload services to take effect.
```

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

\$ help	
vShell, version a	ab2e3bc
The commands prov	rided 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
\$ locale ja	
Successfully lang	guage setting for locale.
Please reload Ste	ellarOne console to take effect.
a	

FIGURE 4-14. Reload StellarOne console

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

\$ env ls	
Hostname:	ODC
Status:	RUNNING
Product Serial Number:	7an
Version:	2.2.1148
Advertise Address:	Not Set
DPI Engine Version:	2.0.11.33e2e1+turbo
DPI Pattern Version:	SDP_230228_08
StellarProtect (Legacy Mode) A	Agent Up Port:8000
StellarProtect (Legacy Mode) A	Agent Down Port:14336
StellarProtect Agent Up Port:	9443
StellarProtect Agent Down Port	:14336
Locale:	ja

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.



4-14

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

5-1

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.

PLATFORM	CURRENT VERSION	SUPPORTED TARGET UPGRADE VERSION	Firmware Upgrade*	MOUNT UPGRADE
VMWare	2.2	3.0	\checkmark	\checkmark
Hyper-V	2.1	2.2 / 3.0	\checkmark	\checkmark
	2.0	2.1/2.2/3.0	\checkmark	\checkmark
	1.2 Patch 1	2.0 / 2.1 / 2.2	N/A	\checkmark
	1.2	2.0/2.1	N/A	\checkmark
	1.2	1.2 Patch 1	\checkmark	\checkmark
VMWare	1.1	1.2 / 1.2 Patch 1	\checkmark	\checkmark
	1.0	1.1	N/A	\checkmark

TABLE 5-1. Supported Upgrade Paths



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-S1acus.fw-3.x.xxx.acf) from the <u>Download Center</u>.
- 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

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.

Resignant Di	adu-esal - Writael Machines	Shut down the old ODC					
Hoat Marage	States (Register 100 @Carante) Pro-		C'Astest @ Actes				(Q. Smith
Montor	What raching	v bate v	Used space -	Ouer DS	 Resinance 	- Heat CPU	~ Not namely
Writer Hachines	de nam-p-inam-63.2	Q lores	25.00-02	Other (SE-bit)	006	IT Die	6.61-05
() sec	C Buthhad on man	C Normal	45.TT 08	Citiver (201-bril)	800	225 1040	4.11 (08
Martin	C & rye-deno-233.odc.temprice	@ Hormal	45.11.08	Other (32-6/6	000	679.68%	18.57-08
B 120, ede, bundhalans	C Burdy-0.8.3, add, bendmann	@ hornal	45.11.08	DTer (21-64)	0000	278 104	11.03.08
(D 180,edc.main	A LED waters and Austiment	@ Normal	45.11.08	Other (02-048	000	332 MPW	12.89 0.0
Hore VMa.	C @ 120,08,000	@ Normal	48.11.08	Direc(22-14)	NDC .	242 1094	627.68
Storage III.	120.ok.medinan	O Normal	45.11/08	01#10.08	000	. 600 Millio	15.15.08
Notworking III	0 (0	A Noting	25.06.08	00w (82-6-8	000	348.10%	4.00'08
	C Bran at	G Normal	25.67.08	Other (82-64)	000	35 Mills	1.07.08

FIGURE 5-2. Shut Down the Previous VM

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

Execting hand disk 20480 MB Hand disk 1 25 GB E SCBI Controller 0 LBI Logic Parallel •	New hard disk	8 *	0			
Hard disk 1 🚵 25 GB 🔹	Existing hard disk	20480	MB			
El SCOI Controller 0 LBI Logio Parallel Katwork Adapter 1 tost Connect Connect	🔜 Hard disk 1 🧥	25	GB			0
Mill Network Adapter 1 tost Convect	SCSI Controller 0	LBI Logic P	haraitei	,		0
	INE Network Adapter 1	test			Connect	0
Video Card Specify outlons settings	Video Card	Specify out	storm settings			

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

datastore1 => 1.0.0, edc, mass => adc, 1 umdk => 1.0.0, edc, transmisso => adc, 1 umdk => adc, 1 umdk => 1.0,0, edc, transmisso => adc, 1 umdk => adc, 1 umdk => 0.00,0 transmisso => adc, 1 umdk => adc, 1 umdk => 0.00,0 transmisso => adc, 1 umdk >> adc, 1 umdk => 0.00,0 transmisso => adc, 1 umdk >> adc, 1 umdk => 0.00,0 transmisso => adc, 1 umdk >> adc, 1 umdk => 0.00,0 transmisso => adc, 1 umdk >> adc, 1 umdk => 0.00,0 transmisso => adc, 1 umdk >> adc, 1 umdk => adc, 1 umdk => adc, 1 umdk >> adc, 1 umdk => adc, 1 umdk => adc, 1 umdk >> adc, 1 umdk => adc, 0 umd, 1 umdk => adc, 1 umdk >> adc, 1 umdk => adc, 0 umd, 1 umdk => adc, 1 umdk >> adc, 1 umdk => adc, 0 umd, 1 umdk => adc, 1 umdk >> adc, 1 umdk => adc, 0 umd, 1 umdk => adc, 1 umdk >> adc, 1 umdk => adc, 0 umdk => adc, 1 umdk => adc, 1 umdk => adc, 0 umdk => adc, 1 umdk => adc, 1 umdk => adc, 0 umdk => adc, 1 umdk => adc, 1 umdk<	P Upload 🔓 Download	Delete 🔒 Move 🔝 Copy	Create directory	C Refresh		
i GOC-test	datastore1	1.0.0, edc, mass 1.0.0, edc, mass 1.0.0, edc, mendmicro 1.0.0-testing, edc, t DHCP-server ed:-gm-verthy-063 gm-verthy-063 mate-jp-test 0.3.2 nate-jp-test 0.3.2 nate-isst 033-tm reac_odc COC-0.0 GOC-0.0 GOC-0.0 GOC-best GOC-test GOC-test	B odc.smdk	edc, 1 umdk 2.99 GB Wednestey, January 2	-	

FIGURE 5-4. Attach to New VM

5-6

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.

Ste	ellarOne-1.2-111	✓ < ► Ø			
*	Hardware Add Hardware BIOS Boot from CD Security Key Storage Drive disabled	Hard Drive You can change how this vi operating system is installe virtual machine from startin Controller:	tual hard disk is I on this disk, cha g.	attached to the virtual anging the attachment of Location:	machine. If an night prevent the
	Memory 16384 MB	IDE Controller 0	×	1 (in use)	
•	Processor Virtual processor IDE Controller 0 H And Drive	You can compact, conve by editing the associated Virtual hard disk:	t, expand, merg file. Specify the	e, reconnect or shrink a full path to the file.	virtual hard dsk
	I L2.0111.vhdx	N	ew E	ist impect	Browse
-	IDE Controller 1	O Physical hard data	8		
•	SCSI Controller Network Adapter vmmet3 Ethernet Adapter - Vi	If the physical disk is offline. U physical hard disk	If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.		
	COM 1 None	To remove the virtual hard disk, click Remove. This disconnects the disk but do delete the associated file.			disk but does not
	Diskette Drive				Kemove

FIGURE 5-5. Shut Down the Previous VM

5-8

- **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

6-1

Technical Support

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 6-3
- Sending Suspicious Content to Trend Micro on page 6-4
- Other Resources on page 6-5

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

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.

6-2

Go to <u>https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware</u> and <u>https://www.encyclopedia.txone.com/</u> 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:

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 6-1. Trend Micro Contact Information

TABLE 6-2. 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

С

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

Н

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

М

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

Ρ

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

IN-1

StellarProtect default port, 2-12 Web, 2-12 support resolve issues faster, 6-4 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

