Cisco Stealthwatch

Virtual Edition (with Data Store) Appliance Installation Guide 7.3.2

Table of Contents

Introduction

Overview

Use this guide to install the following Cisco Stealthwatch Enterprise Virtual Edition (VE) appliances:

- Stealthwatch Management Console (SMC) VE
- Stealthwatch Flow Collector VE
- Stealthwatch Data Node VE
  - If you plan on deploying Data Nodes as part of a Data Store, review the Data Store Virtual Edition Deployment and Configuration Guide before you begin for full instructions on deploying the Data Store, including proper order of appliance installation. Use this guide only as a reference for virtual appliance installation.
- Stealthwatch Flow Sensor VE
- Stealthwatch UDP Director VE

For more information about Stealthwatch, refer to the following online resources:

- **Overview:** https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
- **Appliances:** https://www.cisco.com/c/en/us/products/security/stealthwatch/datasheet-listing.html
- **Release Notes:** For details, refer to the Release Notes.
- **Hardware Installation Guides:** To install Stealthwatch x2xx series hardware, download the guides from https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html.
- **Data Node and Data Store Installation:** If you plan on deploying Data Nodes as part of a Data Store, review the Data Store Virtual Edition Deployment and Configuration Guide before you begin for complete instructions on deploying the Data Store, including proper order of appliance installation.

Audience

The intended audience for this guide includes network administrators and other personnel who are responsible for installing and configuring Stealthwatch products.

If you are configuring virtual appliances, we assume you have basic familiarity with VMware or KVM.

If you prefer to work with a professional installer, please contact your local Cisco Partner or Cisco Stealthwatch Support.

Terminology

This guide uses the term “**appliance**” for any Stealthwatch product, including virtual products such as the Stealthwatch Flow Sensor Virtual Edition (VE).

A "**cluster**" is your group of Stealthwatch appliances that are managed by the Stealthwatch Management Console (SMC).

Abbreviations

The following abbreviations may appear in this guide:

Abbreviations	Definition
DNS	Domain Name System (Service or Server)
dvPort	Distributed Virtual Port
ESX	Enterprise Server X
GB	Gigabyte
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	International Standards Organization
IT	Information Technology
KVM	Kernel-based Virtual Machine
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
SMC	Stealthwatch Management Console

Abbreviations	Definition
TB	Terabyte
UUID	Universally Unique Identifier
VDS	vNetwork Distributed Switch
VE	Virtual Edition
VLAN	Virtual Local Area Network
VM	Virtual Machine

Before You Begin

Before you begin, review this guide to understand the process as well as the preparation, time, and resources you'll need to plan for the installation.

Installation and Configuration Order

Before you install your virtual appliances, please note the required order for installing and configuring Stealthwatch.

1. **Review Data Store Overview:** Review the Data Store Virtual Edition Deployment Overview to understand basic prerequisite information for deploying Stealthwatch with a Data Store.
2. **Install Virtual Appliances:** Use the Data Store Virtual Edition Deployment and Configuration Guide for full instructions on deploying Stealthwatch Virtual Edition (VE) with a Data Store, including proper order of appliance deployment. Use this Virtual Edition (with Data Store) Appliance Installation Guide as reference for the virtual appliance installation.
3. **Configure Stealthwatch:** After you deploy your SMC VE, Data Nodes VE, and Flow Collectors VE, configure that appliance using the Stealthwatch System Configuration Guide v7.3.2 and the Data Store Virtual Edition Deployment and Configuration Guide.

   Note the following:

   - **Configuration Order:** Make sure you configure the appliances in order.
   - **Certificates:** Appliances are installed with a unique, self-signed appliance identity certificate.
   - **Central Management:** Use the primary SMC/Central Manager to manage your appliances and change configuration settings.

⚠ After you install your appliances, you will configure Stealthwatch using the Stealthwatch System Configuration Guide v7.3.2. This step is critical for the successful configuration and communication of your system.

4. **Configure Data Store Initialization and Retention:** After the SMC VE, Data Nodes VE, and Flow Collectors VE are deployed and configured in Stealthwatch, use the Data Store Virtual Edition Deployment and Configuration Guide to

initialize the Data Store and configure flow interface statistics data retention. The guide also includes Data Store maintenance information.

First Time Setup

As part of the **4. Configuring your Environment using First Time Setup** in this guide, you will configure your environment for a Data Store deployment. You can also choose to enable SAL On Prem.

> ⚠ After you make these selections in First Time Setup, you cannot change the configuration. If you select the wrong choice, deploy a new virtual appliance or RFD your virtual appliance.

Data Store

When you configure Stealthwatch with a Data Store in the First Time Setup, it is important to follow the instructions and note the following:

- **SMC and Flow Collectors:** You need to deploy the Data Store on your SMCs and Flow Collectors.
- **Guide:** Use the Data Store Virtual Edition Deployment and Configuration Guide for full instructions on deploying Stealthwatch with a Data Store, including proper order of appliance deployment, initializing the Data Store, and configuring data retention.

Security Analytics and Logging (OP)

You can choose to enable Security Analytics and Logging On Prem and use your Stealthwatch deployment to store Firepower event information. Note that this disables NetFlow collection on your Flow Collector.

- **SMC and Flow Collectors:** If you enable Security Analytics and Logging on your SMC, you must enable SAL on the Flow Collector.
- **Guide:** Refer to the Security Analytics and Logging: Firepower Event Integration Guide for more information.
- **App Requirement:** If you configure Security Analytics and Logging On Prem, install the Security Analytics and Logging On Prem App on your Stealthwatch Management Console.

Installation Methods

You can use a VMware environment or KVM (Kernel-based Virtual Machine) for the virtual appliance installation.

⚠ Before you start the installation, review the compatibility information and resource requirements.

Use the following table to choose an installation method. Also, make sure you review the compatibility and resource requirements before you start the installation.

Method	Installation Instructions (for reference)	Installation File	Details
VMware vCenter	**3a. Installing a Virtual Appliance using VMware vCenter (ISO)**	ISO	Installing your virtual appliances using VMware vCenter.
VMware ESXi Stand-Alone Server	**3b. Installing a Virtual Appliance on an ESXi Stand-Alone Server (ISO)**	ISO	Installing your virtual appliances on an ESXi stand-alone host server.
KVM and Virtual Machine Manager	**3c. Installing a Virtual Appliance on a KVM Host (ISO)**	ISO	Installing your virtual appliances using KVM and Virtual Machine Manager.

Compatibility

Whether you plan to install your virtual appliances in a VMware environment or KVM (Kernel-based Virtual Machine), make sure you review the following compatibility information:

General Requirements for All Appliances

Requirement	Description
Dedicated Resources	All appliances require the allocation of dedicated resources and cannot be shared with other appliances or hosts.
No Live Migration	Appliances do not support vMotion due to the possibility of corruption.
Network Adapter	All appliances require at least 1 network adapter. Flow Sensors can be configured with additional adapters to support additional throughput. Data Nodes require a second network adapter for communication with other Data Nodes as part of the Data Store.
Storage Controller	When configuring the ISO in VMware, select the `LSI Logic SAS` **SCSI Controller** type.
Storage Provisioning	Assign Thick Provisioned Lazy Zeroed storage provisioning when deploying virtual appliances.

VMware

- **Compatibility:** VMware v6.5, v6.7, v7.0.
- **Operating System:** Debian 10 64-bit.
- **ISO Deployment:** We validated VMware v6.5 using update 2 and the vSphere flash-based web client. There may be issues using other clients from vSphere. You can use the ESXi 6.5 update 2 HTML5 client, but you may encounter system time-outs.
- **Live migration:** We do not support host to host live migration (for example, with vMotion).
- **Snapshots:** Virtual machine snapshots are not supported.

⚠ Do not install VMware Tools on a Stealthwatch virtual appliance because it will override the custom version already installed. Doing so would render the virtual appliance inoperable and require reinstallation.

KVM

- **Compatibility:** You can use any compatible Linux distribution.
- **KVM Host Versions:** There are several methods used to install a virtual machine on a KVM host. We tested KVM and validated performance using the following components:
    - libvirt 3.0.0 - 6.5.0
    - qemu-KVM 2.8.0 - 5.0.0
    - Open vSwitch 2.6.1 - 2.13.0
    - Linux Kernel 4.4.38 - 5.4.55
- **Operating System:** Debian 10 64-bit.
- **Virtualization Host**: For minimum requirements and best performance, review the **Resource Requirements** section and see the hardware specification sheet for your appliance at Cisco.com.

ⓘ The system performance is determined by the host environment. Your performance may vary.

Downloading Software

Use Cisco Software Central to download virtual appliance (VE) installation files, patches, and software update files. Log in to your Cisco Smart Account at https://software.cisco.com or contact your administrator. Refer to **2. Downloading VE Installation Files** for instructions.

TLS

Stealthwatch requires v1.2.

Third Party Applications

Stealthwatch does not support installing third party applications on appliances.

Browsers

- **Compatible Browsers:** Stealthwatch supports the latest version of Chrome, Firefox, and Edge.
- **Microsoft Edge:** There may be a file size limitation with Microsoft Edge. We do not recommend using Microsoft Edge to install the VE ISO files.

Host Name

A unique host name is required for each appliance. We cannot configure an appliance with the same host name as another appliance. Also, make sure each appliance host name meets the Internet standard requirements for Internet hosts.

Domain Name

A fully qualified domain name is required for each appliance. We cannot install an appliance with an empty domain.

NTP Server

- **Configuration:** At least 1 NTP server is required for each appliance.
- **Problematic NTP:** Remove the 130.126.24.53 NTP server if it is in your list of servers. This server is known to be problematic and it is no longer supported in our default list of NTP servers.

Time Zone

All Stealthwatch appliances use Coordinated Universal Time (UTC).

- **Virtual Host Server:** Make sure your virtual host server is set to the correct time.

> ⚠ Make sure the time setting on the virtual host server (where you will be installing the virtual appliances) is set to the correct time. Otherwise, the appliances may not be able to boot up.

Resource Requirements

This section provides the resource requirements for the virtual appliances. Use the tables provided in this section to record settings you will need to install and configure the Stealthwatch VE appliances.

- Stealthwatch Management Console (SMC)
- Flow Collector
- Data Node
- Flow Sensor
- UDP Director
- Data Storage

Make sure you reserve the required resources for your system. This step is critical for system performance.

⚠ If you choose to deploy Cisco Stealthwatch appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.

Stealthwatch Management Console VE

To determine the minimum resource allocations for the Stealthwatch Management Console VE, you should determine the number of concurrent users expected to log in to the SMC.

Refer to the following specifications to determine your resource allocations.

Stealthwatch Management Console

Concurrent Users*	**Required Reserved Memory**	**Required Reserved CPUs**	**Minimum Storage Space**
up to 9	32 GB	4	125 GB
10 or more	64 GB	8	200 GB

*Concurrent users include scheduled reports and people using the SMC client at the same time.

Flow Collector VE

Because the Data Nodes within a Data Store will store flows instead of the Flow Collectors, the resource requirements are different depending on whether you deploy a Data Store.

Flow Collector with a Data Store

Flows per second	Interfaces	Exporters	Required Reserved Memory	Required Reserved CPUs	Required Minimum Data Storage
Up to 50,000	Up to 65535	Up to 2048	32 GB	6	200 GB
Up to 120,000	Up to 65535	Up to 4096	70 GB	8	200 GB

Data Node VE

> If you plan on deploying Data Nodes as part of a Data Store, review the Data Store Installation and Configuration Guide before you begin for full instructions on initializing the Data Store, including proper order of appliance deployment.

To determine your resource requirements for the Data Node VE, you should determine the flows per second expected on the network. This also affects the resource requirements for your Flow Collectors VE. Refer to **Flow Collector VE** for more information on resource requirements.

You can deploy only 3 Data Nodes VE to your network. You cannot deploy additional Data Nodes VE.

If you deploy a Data Store VE with 3 Data Nodes VE, we recommend that for each Data Node, calculate the storage allocation as follows:

```
[[(daily average FPS/1,000) x 1.6 x days] / number of Data
Nodes
```

- Determine your `daily average (FPS)`
- Divide this number by `1,000` FPS
- Multiply this number by `1.6` GB of storage for one day's worth of storage
- Multiply this number by the number of `days` you want to store the flows for total Data Store storage
- Divide this number by the `number of Data Nodes` in your Data Store for storage per Data Node

For example, if your system:

- has `50,000 daily average (FPS)`
- will store flows for `90 days`, and
- you have `3 Data Nodes`

calculate per Data Node as follows:

```
[(50,000/1,000) x 1.6 x 90] / 3 = 2400 GB (2.4 TB) per Data
Node
```

- `daily average FPS = 50,000`
- `50,000 daily average FPS / 1,000= 50`
- `50 x 1.6 GB = 80 GB for one day's worth of storage`

- `80 GB x 90 days per Data Store = 7200 GB per Data Store`
- `7200 GB / 3 Data Nodes = 2400 GB (2.4 TB) per Data Node`

Refer to the following specifications to determine your resource requirements:

Flows per second	Required Reserved Memory	Required Reserved CPUs	Required Minimum Data Storage for 30 days
Up to 50,000	32 GB per Data Node VE	6 per Data Node VE	• 800 GB per Data Node • 2.4 TB total across 3 Data Nodes
Up to 120,000	32 GB per Data Node VE	12 per Data Node VE	• 1.92 TB per Data Node • 5.76 TB total across 3 Data Nodes
Up to 220,000	64 GB per Data Node VE	16 per Data Node VE	• 3.52 TB per Data Node • 10.56 TB total across 3 Data Nodes

Flow Sensor VE

Stealthwatch offers various types of Flow Sensor VEs depending upon the number of NICs for the Flow Sensor VE.

- **Cache:** The Flow Cache Size column indicates the maximum number of active flows that the Flow Sensor can process at the same time. The cache adjusts with the amount of reserved memory, and flows are flushed every 60 seconds. Use the Flow Cache Size to calculate the amount of memory needed for the amount of traffic being monitored.
- **Requirements:** Your environment may require more resources depending on a number of variables, such as average packet size, burst rate, and other network and host conditions.

NICs - monitoring ports	**Required Reserved CPUs**	**Required Minimum Reserved Memory**	**Estimated Throughput**	**Flow Cache Size** (maximum number of concurrent flows)
1 x 1 Gbps	2	4 GB	850 Mbps	32,766
2 x 1 Gbps	4	8 GB	1,850 Mbps Interfaces configured as PCI pass-through (igb/ixgbe compliant or e1000e compliant)	65,537
4 x 1 Gbps	8	16 GB	3,700 Mbps Interfaces configured as PCI pass-through (igb/ixgbe compliant or e1000e compliant)	131,073
1 x 10 Gbps*	12	24 GB	8 Gbps	~512,000

NICs - monitoring ports	**Required Reserved CPUs**	**Required Minimum Reserved Memory**	**Estimated Throughput**	**Flow Cache Size** (maximum number of concurrent flows)
			Interfaces configured as PCI pass-through (Intel ixgbe/i40e compliant)	
2 x 10 Gbps*	22	40 GB	16 Gbps Interfaces configured as PCI pass-through (Intel ixgbe/i40e compliant)	~1,000,000

*For 10 Gbps throughput, configure all CPUs in 1 socket. For each additional 10 Gbps NIC, add 10 vCPUs and 16 GB of RAM.

Optional: One or more 10G NICs may be used on the physical VM host.

These figures are based on tests with Cisco UCS C220 M4, which contains the following:

- **Processors:** 2 Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40 GHz, 2 sockets, 12 cores per socket
- **Memory:** 128 GB
- **Storage:** 800 GB
- **ESXi:** VMware vSphere 6.7.0
- **Monitoring Interfaces:** PCI pass-through with 1 Gbps and 10 Gbps interfaces

Flow Sensor VE Network Environments

Before installing the Flow Sensor VE, make sure you know the type of network environment you have. This guide covers all types of network environments that a Flow Sensor VE can monitor.

Compatibility: Stealthwatch supports a VDS environment, but it does not support VMware Distributed Resource Scheduler (VM-DRS).

Virtual Network Environments: The Flow Sensor VE monitors the following types of virtual network environments:

- A network with virtual local area network (VLAN) trunking
- Discrete VLANs where one or more VLANs are prohibited from attaching packet monitoring devices (for example, due to local policy)
- Private VLANs
- Hypervisor hosts rather than VLANs

Integration: For integration information, review **Stealthwatch Flow Sensor**.

Flow Sensor VE Traffic

The Flow Sensor will process traffic with the following Ethertypes:

Ethertype	Protocol
0x8000	Normal IPv4
0x86dd	Normal IPv6
0x8909	SXP
0x8100	VLAN
0x88a8 0x9100 0x9200 0x9300	VLAN QnQ
0x8847	MLPS unicast
0x8848	MLPS multicast

ⓘ The Flow Sensor saves the top-level MPLS label or VLAN ID and exports it. It bypasses the other labels when it is processing packets.

UDP Director VE

The UDP Director VE requires that the virtual machine meets the following specifications:

Required Reserved CPU	Required Reserved Memory	Minimum Data Storage	Maximum FPS Rate
2	4 GB	60 GB	10,000

Data Storage

The appliance data storage expands automatically when the appliance reboots. Also, you may want to expand the appliance resource allocations to improve performance. Use the following information to allocate storage for each appliance.

> Make sure you reserve the required resources for your system. This step is critical for system performance.
>
> ⚠ If you choose to deploy Cisco Stealthwatch appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.

- **Expansion Calculation:** The virtual appliance uses approximately 75% of the server for data storage, leaving 25% for the operating system and cache. Therefore, always expand the data storage to 40% more than the desired amount.
- **FPS Calculation:** Allocate a minimum of 1 GB of data storage for every 1,000 flows per second (FPS) your system averages daily multiplied by the number of days you want to store the flows. For example, if your system averages 2,000 FPS and you want to store flows for 30 days, allocate a minimum of 60 GB (2 X 30) of data storage space.
- **Syslog:** If the External Event processing (syslog) feature is used, more memory and processing resources are required.
- **Data Storage:** Use the following table to determine the data storage required for each appliance.
- **Restart:** If you increase the virtual machine memory using another method on your Hypervisor host, restart the appliance after you have saved your changes.

Stealthwatch VE Model	Required Minimum Data Storage	Maximum Addressable Storage/ Hardware Equivalent
Stealthwatch Management Console VE	125 GB	5.6 TB
Flow Collector NetFlow or sFlow VE	200 GB	n/a, depends on Data Store
Data Node VE	See Data Node VE Resource Requirements for more information	See Data Node VE Resource Requirements for more information
Flow Sensor	60 GB	n/a
UDP Director	60 GB	n/a

1. Configuring your Firewall and Ports

Overview

Before you can install your virtual appliance, complete the following procedures to prepare your network:

1. **Placing the Appliances**
2. **Configuring Your Firewall for Communications**
3. **Stealthwatch Flow Sensor**

Placing the Appliances

Review the placement information for each appliance you are installing.

- Stealthwatch Management Console (SMC)
- Flow Collector
- Flow Sensor
- UDP Director
- Data Node

Stealthwatch Management Console

As the management device, install the Stealthwatch Management Console at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of Stealthwatch Management Consoles, we recommend installing the primary and the secondary consoles in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

When you place a Flow Collector outside a firewall, we recommend that you turn off the setting **Accept traffic from any exporter**.

Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated web-based management systems that facilitate either centralized or remote management and administration.

The Flow Sensor VE appliance is most effective when placed at critical segments of your corporate network as follows:

- **Inside your firewall** to monitor traffic and determine if a firewall breach has occurred
- **Outside your firewall,** monitoring traffic flow to analyze who is threatening your firewall
- **At sensitive segments of your network,** offering protection from disgruntled employees or hackers with root access
- **At remote office locations** that constitute vulnerable network extensions
- **On your business network for protocol use management** (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Important Considerations for Integration

The Stealthwatch Flow Sensor VE is versatile enough to integrate with a wide variety of network topologies, technologies, and components. Before you install a Flow Sensor VE, you must make several decisions about your network and how you want to monitor it. It is important to review the following:

- Analyze your network's topology and your specific monitoring needs.
- Connect a Flow Sensor so that it receives network transmissions to and from the monitored network, and, if desired, receives interior network transmissions as well.
- For optimum performance when using the Flow Sensor to monitor physical network traffic, configure your Flow Sensor VE with direct access to the underlying physical host’s NICs (such as using an igb or e1000e compliant PCI pass-through).

The following sections explain how to integrate a Stealthwatch Flow Sensor VE appliance into your network using the following Ethernet network devices:

- **TAPs**
- **SPAN Ports**

While not all network configurations can be discussed here, the examples may help you determine the best setup for your monitoring needs. These examples provide physical network scenarios, and the virtual host can be configured in a similar way.

TAPs

When a Test Access Port (TAP) is placed in line with a network connection, it repeats the connection on a separate port or ports. For example, an Ethernet TAP placed in line with an Ethernet cable will repeat each direction of transmission on separate ports. Therefore, use of a TAP is the most reliable way to use the Flow Sensor. The type of TAP you use depends on your network.

> Review the Stealthwatch System Configuration Guide v7.3.2 for Flow Sensor configuration requirements.

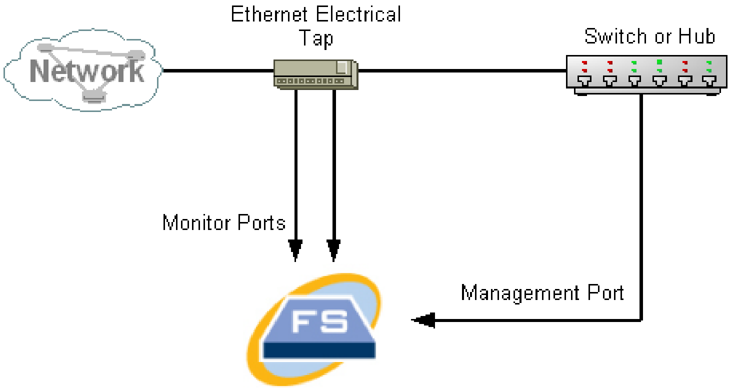
This section explains the following ways to use TAPs:

- **Using Electrical TAPs**
- **Using Optical TAPs**
- **Using TAPs Outside Your Firewall**
- **Placing the Flow Sensor VE Inside Your Firewall**

In a network using TAPs, the Flow Sensor VE can capture performance monitoring data only if it is connected to an aggregating TAP that is capturing both inbound and outbound traffic. If the Flow Sensor VE is connected to a unidirectional TAP that is capturing only one direction of traffic on each port, then the Flow Sensor VE will not capture performance monitoring data.

Using Electrical TAPs

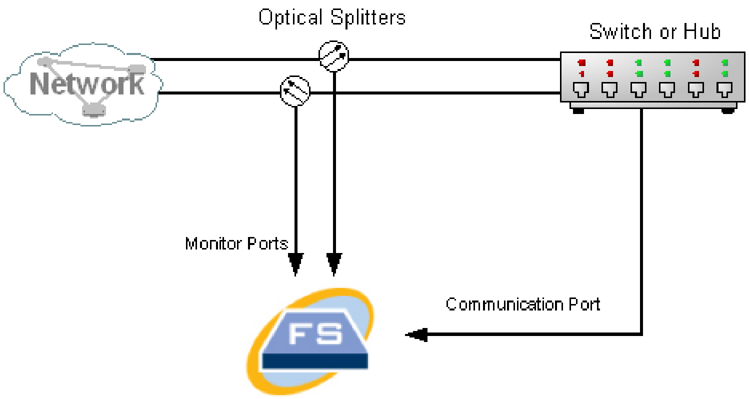
The following illustration shows the Stealthwatch Flow Sensor VE connected to an Ethernet electrical TAP. To achieve this configuration, connect the two TAP ports to the Flow Sensor VE Monitor Ports 1 and 2, as shown.



Using Optical TAPs

Two splitters are required for fiber-optic-based systems. You can place a fiber-optic cable splitter in line with each direction of transmission and use it to repeat the optical signal for one direction of transmission.

The following illustration shows the Flow Sensor connected to a fiber-optic-based network. To achieve this configuration, connect the outputs of the optical splitters to the Flow Sensor VE Monitor Ports 1 and 2, as shown.



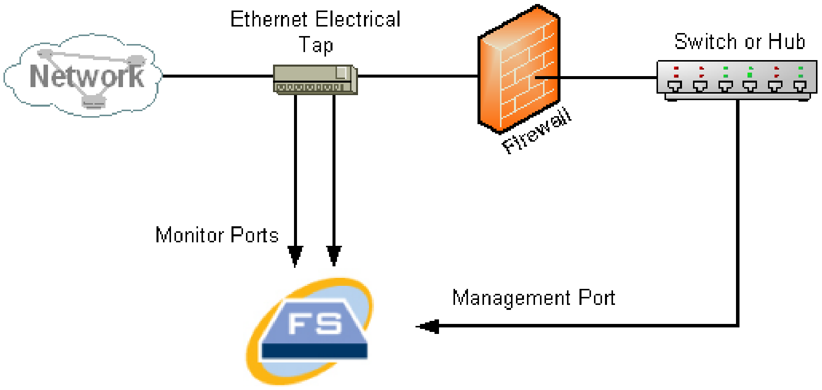
If the connection between the monitored networks is an optical connection, then the Stealthwatch Flow Sensor VE appliance is connected to two optical splitters. The management port is connected to either the switch of the monitored network or to another switch or hub.

Using TAPs Outside Your Firewall

To have the Flow Sensor VE monitor traffic between your firewall and other networks, connect the Stealthwatch management port to a switch or port outside of the firewall.

> ⚠ Use a TAP for this connection so that failure of the device does not bring down your entire network.

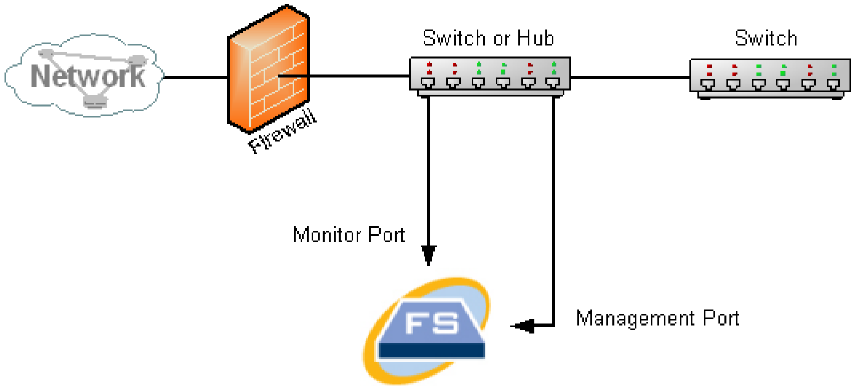
The following illustration shows an example of this configuration using an Ethernet electrical TAP. The management port must be connected to the switch or hub of the monitored network. This setup is similar to the setup that monitors traffic to and from your network.



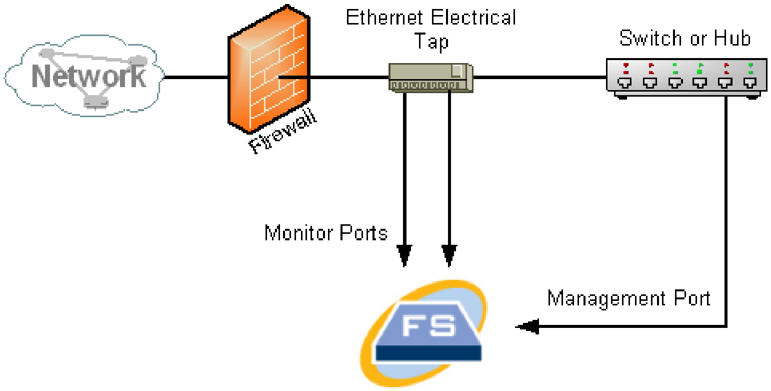
If your firewall is performing network address translation (NAT), you can observe only the addresses that are on the firewall.

Placing the Flow Sensor VE Inside Your Firewall

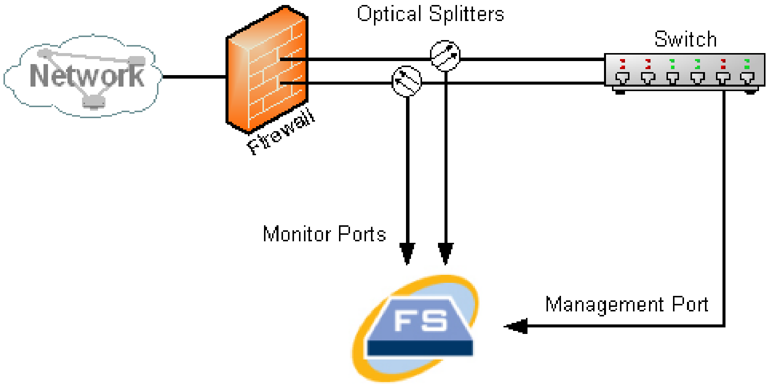
To monitor traffic between internal networks and a firewall, the Flow Sensor VE must be able to access all traffic between the firewall and the internal networks. You can accomplish this by configuring a mirror port that mirrors the connection to the firewall on the main switch. Make sure that the Flow Sensor VE Monitor Port 1 is connected to the mirror port, as shown in the following illustration:



To monitor traffic inside your firewall by using a TAP, insert the TAP or optical splitter between your firewall and the main switch or hub. A TAP configuration is shown below.



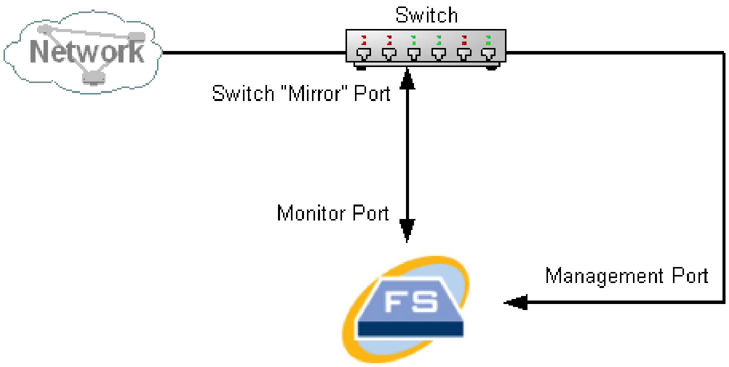
An optical splitter configuration is shown below.



SPAN Ports

You can also connect the Flow Sensor VE to a switch. However, because a switch does not repeat all traffic on each port, the Flow Sensor VE will not perform properly unless the switch can repeat packets transmitted to and from one or more switch ports. This type of switch port is sometimes called a mirror port or Switch Port Analyzer (SPAN).

The following illustration shows how you can achieve this configuration by connecting your network to the Stealthwatch Flow Sensor VE through the management port.



In this configuration, you must configure a switch port (also called a mirror port), to repeat all traffic to and from the host of interest to the mirror port. The Flow Sensor VE Monitor Port 1 must be connected to this mirror port. This allows the Flow Sensor to monitor traffic to and from the network of interest and to other networks. In this instance, a network may be made up of some or all of the hosts connected to the switch.

A common way of configuring networks on a switch is to zone them into virtual local area networks (VLANs), which are logical rather that physical connections of hosts. If the mirror port is configured to mirror all ports on a VLAN or switch, the Flow Sensor VE can monitor all traffic to, from, and within the network of interest, as well as other networks.

- **Configuration:** Review the Stealthwatch System Configuration Guide v7.3.2 for Flow Sensor configuration requirements.
- **Documentation:** In all cases, make sure you consult your switch manufacturer's documentation to determine how to configure the switch mirror port and what traffic will be repeated to the mirror port.

Stealthwatch UDP Director

The only requirement for the placement of the Stealthwatch UDP Director is that it has an unobstructed communication path to the rest of your Stealthwatch appliances.

> ⚠ If you are deploying the UDP Director in an environment where Cisco's ACI is being utilized and Unicast Reverse Path Forwarding (uRPF) or **Limit IP learning to subnet** is enabled, the local network may block the forwarded traffic leaving the UDP Director. You need to spoof the UDP traffic as part of the forwarding rules so tools collecting the log data are able to know the original source of traffic.
>
> To ensure a successful operation of the UDP Director in this case, deploy your UDP Director on a portion of your network where you can disable uRPF or **Limit IP learning to subnet** (typically internally). You can place the UDP Director in an L3 out (no IP learning). If on 4.0+, you can disable endpoint learning on a per VRF basis.

Stealthwatch Data Node

As a repository for flow data collected by Flow Collectors, and as the centralized repository against which a Stealthwatch Management Console runs queries, install your Data Nodes at a location on your network that is accessible by all of your Flow Collectors and your Stealthwatch Management Console. See the Data Store Virtual Edition Deployment and Configuration Guide for more information.

Configuring Your Firewall for Communications

In order for the appliances to communicate properly, you should configure the network so that firewalls or access control lists do not block the required connections. Use the information provided in this section to configure your network so that the appliances can communicate through the network.

Open Ports

Stealthwatch Management Console (SMC), Flow Collector, Data Nodes, Flow Sensor, and UDP Director

Consult with your network administrator to ensure that the following ports are open and have unrestricted access:

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 5222
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

In addition, if you deploy Data Nodes to your network, ensure that the following ports are open and have unrestricted access:

- TCP 5433
- TCP 5444
- TCP 9450

Communication Ports and Protocols

The following table shows how the ports are used in Stealthwatch:

From (Client)	To (Server)	Port	Protocol
Admin User PC	All appliances	TCP/443	HTTPS
All appliances	Network time source	UDP/123	NTP
Active Directory	SMC	TCP/389, UDP/389	LDAP
Cisco ISE	SMC	TCP/443	HTTPS
Cisco ISE	SMC	TCP/5222	XMPP
External log sources	SMC	UDP/514	SYSLOG
Flow Collector	SMC	TCP/443	HTTPS
UDP Director	Flow Collector - sFlow	UDP/6343	sFlow
UDP Director	Flow Collector - NetFlow	UDP/2055*	NetFlow
UDP Director	3rd Party event management systems	UDP/514	SYSLOG
Flow Sensor	SMC	TCP/443	HTTPS
Flow Sensor	Flow Collector - NetFlow	UDP/2055	NetFlow
Identity	SMC	TCP/2393	SSL
NetFlow Exporters	Flow Collector - NetFlow	UDP/2055*	NetFlow
sFlow Exporters	Flow Collector - sFlow	UDP/6343*	sFlow
SMC	Cisco ISE	TCP/443	HTTPS

From (Client)	To (Server)	Port	Protocol
SMC	Cisco ISE	TCP/5222	XMPP
SMC	DNS	UDP/53	DNS
SMC	Flow Collector	TCP/443	HTTPS
SMC	Flow Sensor	TCP/443	HTTPS
SMC	Identity	TCP/2393	SSL
SMC	Flow Exporters	UDP/161	SNMP
SMC	LDAP	TCP/636	TLS
User PC	SMC	TCP/443	HTTPS

*This is the default port, but any UDP port could be configured on the exporter.

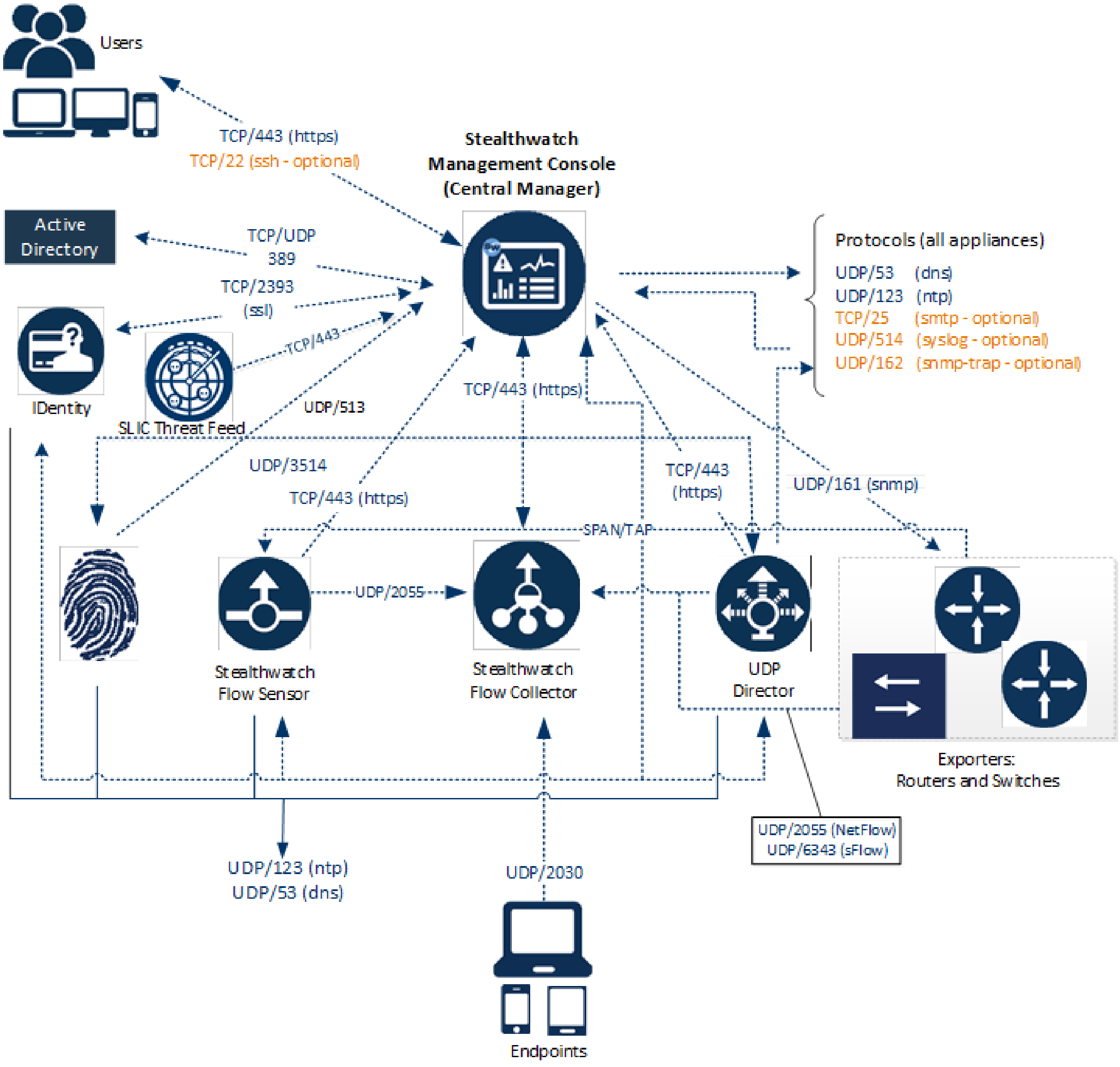
Optional Communication Ports

The following table is for optional configurations determined by your network needs:

From (Client)	To (Server)	Port	Protocol
All appliances	User PC	TCP/22	SSH
SMC	3rd Party event management systems	UDP/162	SNMP-trap
SMC	3rd Party event management systems	UDP/514	SYSLOG
SMC	Email gateway	TCP/25	SMTP
SMC	Threat Intelligence Feed	TCP/443	SSL
User PC	All appliances	TCP/22	SSH

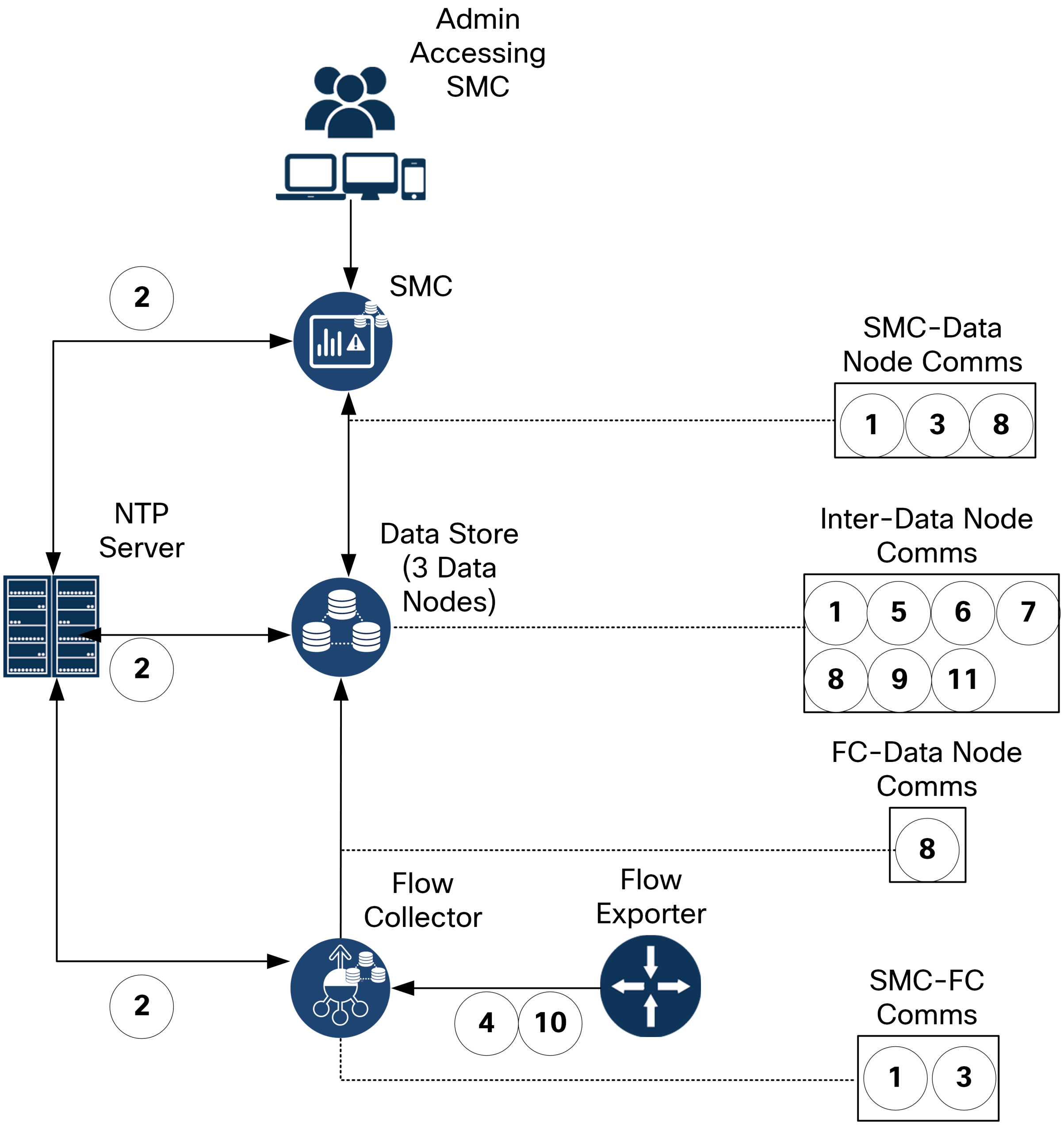
Stealthwatch Deployment Example

The following diagram shows the various connections used by Stealthwatch. Some of these ports are optional.



Stealthwatch Deployment with Data Store Example

The following diagram shows an example Stealthwatch architecture with a Data Store deployed. See the table for the ports associated with each callout.



The following lists the communication ports to open on your firewall to deploy the Data Store.

#	From (Client)	To (Server)	Port	Protocol or Purpose
1	SMC	Flow Collectors and Data Nodes	22/TCP	SSH, required to initialize Data Store database
1	Data Nodes	all other Data Nodes	22/TCP	SSH, required to initialize Data Store database and for database administration tasks
2	SMC, Flow Collectors, and Data Nodes	NTP server	123/UDP	NTP, required for time synchronization
2	NTP server	SMC, Flow Collectors, and Data Nodes	123/UDP	NTP, required for time synchronization
3	SMC	Flow Collectors and Data Nodes	443/TCP	HTTPS, required for secure communications between appliances
3	Flow Collectors	SMC	443/TCP	HTTPS, required for secure communications between appliances
3	Data Nodes	SMC	443/TCP	HTTPS, required for secure communications between appliances
4	NetFlow Exporters	Flow Collectors - NetFlow	2055/UDP	NetFlow ingestion
5	Data Nodes	all other Data Nodes	4803/TCP	inter-Data Node messaging service
6	Data Nodes	all other Data Nodes	4803/UDP	inter-Data Node messaging service

7	Data Nodes	all other Data Nodes	4804/UDP	inter-Data Node messaging service
8	SMC, Flow Collectors, and Data Nodes	Data Nodes	5433/TCP	Vertica client connections
9	Data Node	all other Data Node	5433/UDP	Vertica messaging service monitoring
10	sFlow Exporters	Flow Collectors - sFlow	6343/UDP	sFlow ingestion
11	Data Nodes	all other Data Nodes	6543/UDP	inter-Data Node messaging service

See the Data Store Virtual Edition Deployment and Configuration Guide for more information on Data Store communication ports.

2. Downloading VE Installation Files

Use the following instructions to download the ISO files for your virtual appliance installation. Refer to **Installation Files** to determine the file type.

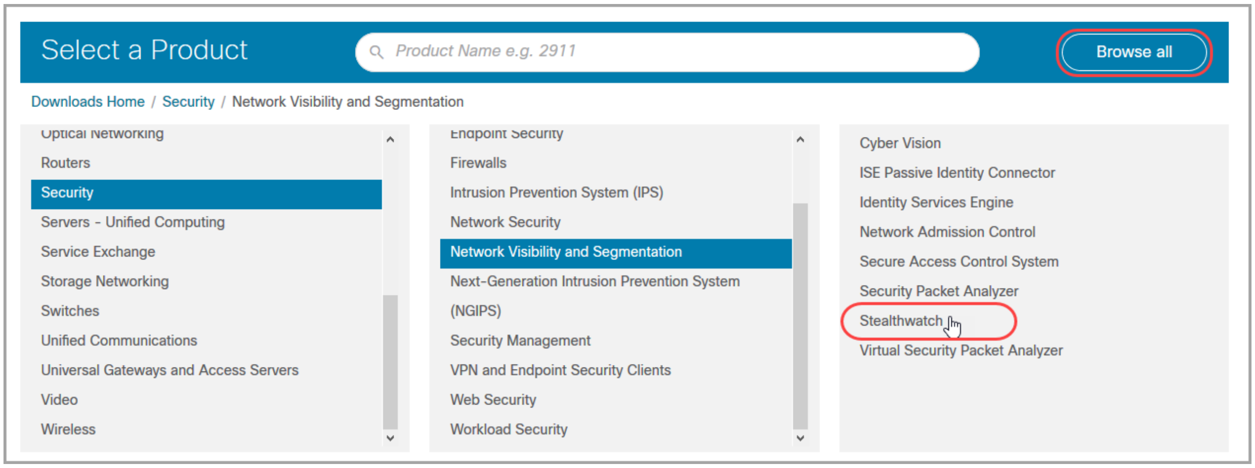
Installation Files

Virtual Machine	Appliance Installation File	Details
3a. VMware vCenter	ISO	Installing your virtual appliances using VMware vCenter.
3b. VMware ESXi Stand-Alone Server	ISO	Installing your virtual appliances on an ESXi stand-alone host server.
3c. KVM and Virtual Machine Manager	ISO	Installing your virtual appliances using KVM and Virtual Machine Manager.

1. Log in to Cisco Software Central

1. Log in to Cisco Software Central at https://software.cisco.com.
2. In the **Download and manage** > **Download and Upgrade** section, select **Access downloads**.
3. Scroll down until you see the **Select a Product** field.
4. You can access Stealthwatch files in two ways:

    - **Search by Name:** Type **Stealthwatch** in the **Select a Product field**. Press Enter.
    - **Search by Menu:** Click Browse All. Select **Security** > **Network Visibility and Segmentation** > **Stealthwatch**.


Select a Product
Product Name e.g. 2911
Browse all
Downloads Home / Security / Network Visibility and Segmentation
Optical Networking
Routers
Security
Servers - Unified Computing
Service Exchange
Storage Networking
Switches
Unified Communications
Universal Gateways and Access Servers
Video
Wireless
Endpoint Security
Firewalls
Intrusion Prevention System (IPS)
Network Security
Network Visibility and Segmentation
Next-Generation Intrusion Prevention System (NGIPS)
Security Management
VPN and Endpoint Security Clients
Web Security
Workload Security
Cyber Vision
ISE Passive Identity Connector
Identity Services Engine
Network Admission Control
Secure Access Control System
Security Packet Analyzer
Stealthwatch
Virtual Security Packet Analyzer

2. Download Files

1. Select an appliance type.

    - Stealthwatch Management Console Virtual Appliance
    - Stealthwatch Flow Collector Virtual Appliance
    - Stealthwatch Data Node Virtual Appliance
    - Stealthwatch Flow Sensor Virtual Appliance
    - Stealthwatch UDP Director Virtual Appliance

2. Select **Stealthwatch System Software**.
3. In the Latest Release column, select **7.3.2** (or the version of 7.3.x that you are installing).
4. **Download:** Locate the ISO installation file. Click the **Download** icon or **Add to Cart** icon.
5. Repeat these instructions to download the files for each appliance type.

3a. Installing a Virtual Appliance using VMware vCenter (ISO)

Overview

Use the following instructions to install your virtual appliances using **VMware vCenter**.

> ⓘ If you plan on deploying Data Nodes as part of a Data Store, review the Data Store Virtual Edition Deployment and Configuration Guide before you begin for full instructions on initializing the Data Store, including proper order of appliance deployment.

To use an alternative method, refer to the following:

- **VMware ESXi Stand-Alone Server:** Use **3b. Installing a Virtual Appliance on an ESXi Stand-Alone Server (ISO)**.
- **KVM:** Use **3c. Installing a Virtual Appliance on a KVM Host (ISO)**.

Before You Begin

Before you begin the installation, complete the following preparation procedures:

1. **Compatibility:** Review the compatibility requirements in **Compatibility**.
2. **Resource Requirements:** Review the **Resource Requirements** section to determine the required allocations for the appliance. You can use a resource pool or alternative method to allocate resources.
3. **Firewall:** Configure your firewall for communications. Refer to **1. Configuring your Firewall and Ports**.
4. **Files:** Download the appliance ISO files. Refer to **2. Downloading VE Installation Files** for instructions.
5. **Time:** Confirm the time set on the hypervisor host in your VMware environment (where you will be installing the virtual appliance) shows the correct time. Otherwise, the virtual appliances may not be able to boot up.

> ⚠ Do not install an untrusted physical or virtual machine on the same physical cluster/system as your Stealthwatch appliances.

⚠ Do not install VMware Tools on a Stealthwatch virtual appliance because it will override the custom version already installed. Doing so would render the virtual appliance inoperable and require reinstallation.

Installing a Virtual Appliance Using vCenter (ISO)

If you have VMware vCenter (or similar), use the following instructions to install a virtual appliance using the ISO.

Process Overview

Installing a virtual appliance involves completing the following procedures, which are covered in this chapter:

1. Logging in to the VMware Web Client

2a. Configuring the Flow Sensor to Monitor Traffic

2b. Configuring an Isolated LAN for inter-Data Node Communications

3. Installing the Virtual Appliance

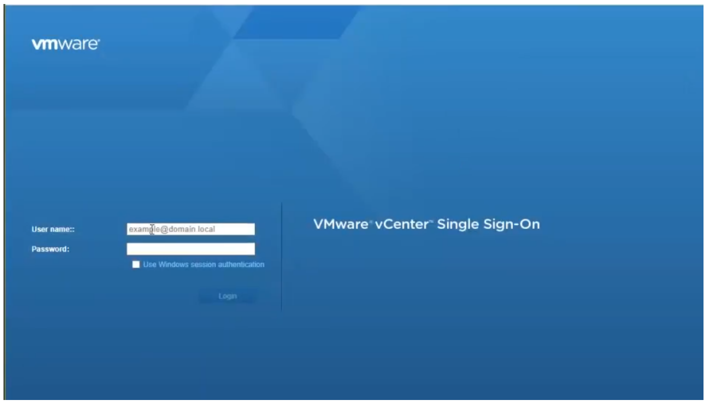
4. Defining Additional Monitoring Ports (Flow Sensors only)

1. Logging in to the VMware Web Client

To install the virtual appliance, log in to the VMware Web Client.

> Some of the menus and graphics may vary from the information shown here. Please refer to your VMware guide for details related to the software.

1. Log in to your VMware Web Client.


vmware
User name::
example@domain.local
Password:
□ Use Windows session authentication
Login
VMware vCenter Single Sign-On

2. You have the following options:

   Flow Sensors: If the appliance is a Flow Sensor, go to **2a. Configuring the Flow Sensor to Monitor Traffic**.

Data Nodes: If you are deploying Data Nodes, go to Configuring an Isolated LAN for inter-Data Node Communications.

All Other Appliances: If the appliance is not a Flow Sensor, go to **3. Installing the Virtual Appliance**.

2a. Configuring the Flow Sensor to Monitor Traffic

The Flow Sensor VE has the ability to provide visibility into VMware environments, generating flow data for areas that are not flow-enabled. As a virtual appliance installed inside each hypervisor host, the Flow Sensor VE passively captures Ethernet frames from the host vSwitch, and it observes and creates flow records containing valuable session statistics that pertain to conversational pairs, bit rates, and packet rates. For details, refer to **Flow Sensor VE** and **Stealthwatch Flow Sensor**.

Use the following instructions to configure the Flow Sensor VE to monitor traffic on a vSwitch as follows:

- **Monitoring a vSwitch with Multiple Hosts**
- **Monitoring a vSwitch with a Single Host**

Monitoring External Traffic with PCI Pass-Through

You can also configure your Flow Sensor VE for direct network monitoring using a compliant PCI pass-through.

- **Requirements:** igb/ixgbe compliant or e1000e compliant PCI pass-through.
- **Resource Information:** Refer to **Flow Sensor VE**.
- **Integration:** Refer to **1. Configuring your Firewall and Ports**.
- **Instructions:** To add PCI network interfaces to the Flow Sensor VE, refer to your VMware documentation.

Monitoring a vSwitch with Multiple Hosts

Use the instructions in this section to use the Flow Sensor VE to monitor traffic on a Distributed vSwitch that spans multiple VM hosts or clusters.

This section applies only to VDS networks. If your network is in a non-VDS environment, go to **Monitoring a vSwitch with a Single Host**.

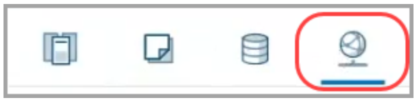
Configuration Requirements

This configuration has the following requirements:

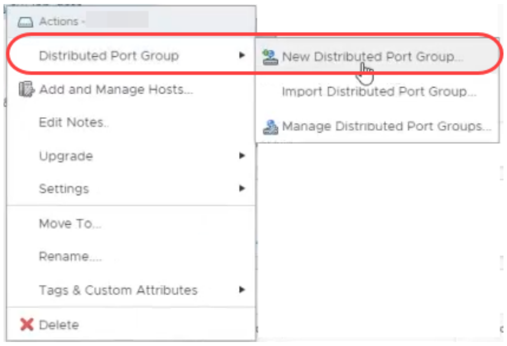
- **Distributed Virtual Port (dvPort):** Add a dvPort group with the correct VLAN settings for each VDS that the Flow Sensor VE will monitor. If the Flow Sensor VE monitors both VLAN and non-VLAN traffic on the network, you need to create two dvPort groups, one for each type.
- **VLAN Identifier:** If your environment uses a VLAN (other than VLAN trunking or a private VLAN), you need the VLAN identifier to complete this procedure.
- **Promiscuous Mode:** Enabled.
- **Promiscuous Port:** Configured to the vSwitch.

Complete the following steps to configure the network using a VDS:

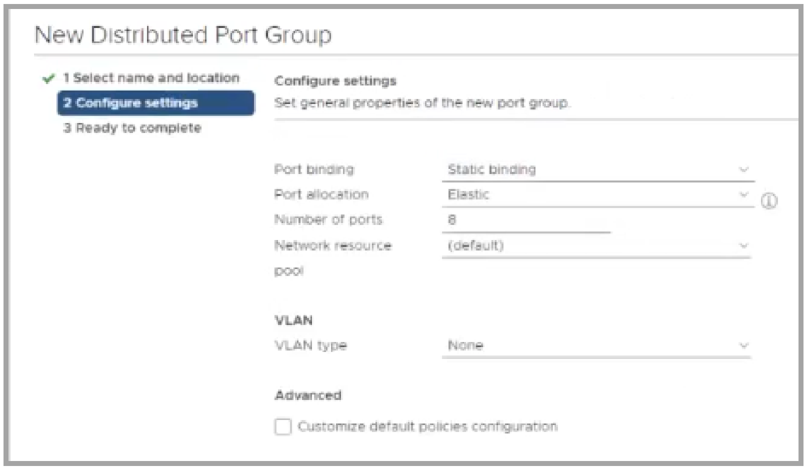
1. Click the **Networking** icon.



2. In the Networking tree, right-click the VDS.
3. Select **Distributed Port Group** > **New Distributed Port Group**.



4. Use the **New Distributed Port Group** dialog box to to configure the port group, including the specifications in the following steps.
5. **Select Name and Location:** In the **Name** field, enter a name to identify this dvPort group.
6. **Configure Settings:** In the **Number of Ports** field, enter the number of Flow Sensor VEs in your cluster of hosts.



New Distributed Port Group

- ✓ 1 Select name and location
- 2 Configure settings
- 3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding	Static binding
Port allocation	Elastic
Number of ports	8
Network resource pool	(default)

VLAN

VLAN type	None

Advanced

□ Customize default policies configuration

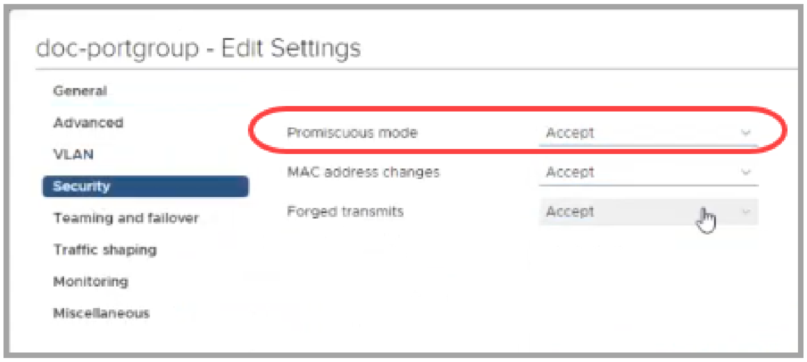
7. Click the **VLAN type** drop-down list.

   - If your environment doesn't use a VLAN, select **None**.
   - If your environment uses a VLAN, select the VLAN type. Configure it as follows:

VLAN Type	Detail
VLAN	In the **VLAN ID** field, enter the number (between 1 and 4094) that matches the identifier.
VLAN Trunking	In the **VLAN trunk range** field, enter **0-4094** to monitor all VLAN traffic.
Private VLAN	Select **Promiscuous** from the drop-down list.

8. **Ready to Complete:** Review the configuration settings. Click **Finish**.

9. In the Networking tree, right-click the new dvPort group. Select **Edit Settings**.
10. Select **Security**.
11. Click the **Promiscuous Mode** drop-down list. Select **Accept**.



doc-portgroup - Edit Settings

Promiscuous mode: Accept

MAC address changes: Accept

Forged transmits: Accept

12. Click **OK** to close the dialog box.
13. Does the Flow Sensor VE monitor both VLAN and non-VLAN network traffic?
    - If yes, repeat the steps in this section **Monitoring a vSwitch with Multiple Hosts**.
    - If no, continue to the next step.
14. Is there another VDS in the VMware environment that the Flow Sensor VE will monitor?
    - If yes, repeat the steps in this section **Monitoring a vSwitch with Multiple Hosts** for the next VDS.
    - If no, go to Configuring an Isolated LAN for inter-Data Node Communications if you are deploying Data Nodes, or **3. Installing the Virtual Appliance** if you are not.

Monitoring a vSwitch with a Single Host

Use the instructions in this section to use the Flow Sensor VE to monitor traffic on a vSwitch with a single host.

> This section applies only to non-VDS networks. If your network uses a VDS, go to **Monitoring a vSwitch with Multiple Hosts**.

Configuration Requirements

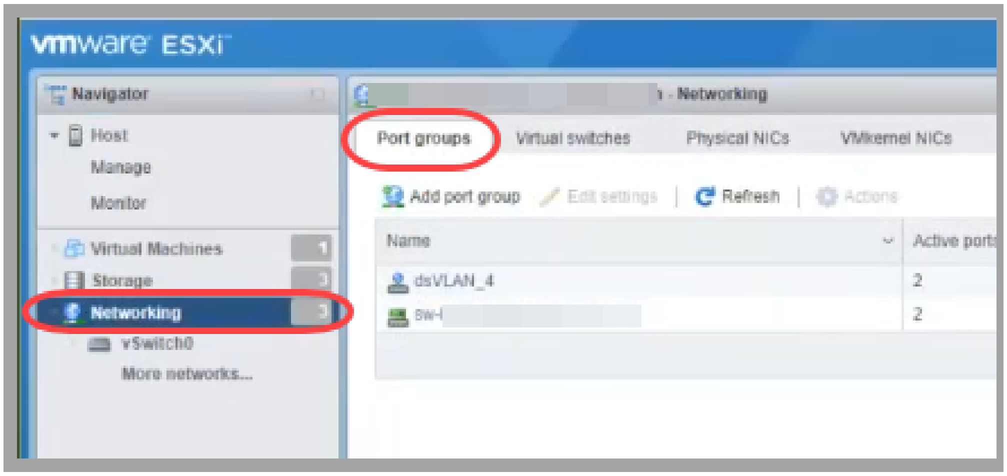
This configuration has the following requirements:

- **Promiscuous Port Group:** Add a promiscuous port group for each virtual switch that the Flow Sensor VE will be monitoring.
- **Promiscuous Mode:** Enabled.
- **Promiscuous Port:** Configured to the vSwitch.

Configure the Port Group to Promiscuous Mode

Use the following instructions to add a port group, or edit a port group, and set it to Promiscuous.

1. Log in to your VMware ESXi host environment.
2. Click **Networking**.



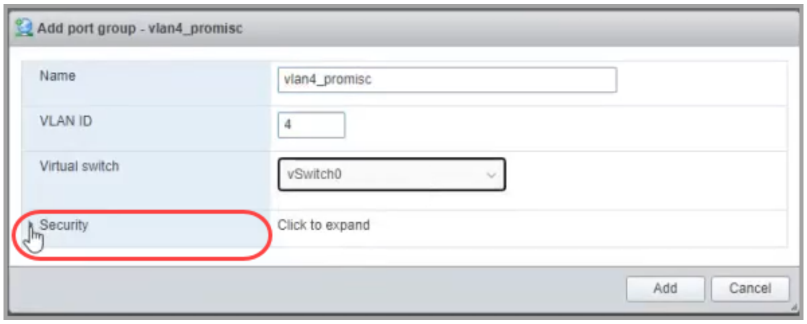
3. Select the **Port groups** tab.
4. You can create a new port group or edit a port group.

- **Create Port Group:** Click **Add port group**.
- **Edit Port Group:** Select the port group. Click **Edit Settings**.

5. Use the dialog box to configure the port group. Configure the VLAN ID or VLAN Trunking:

VLAN Type	Detail
VLAN ID	Use VLAN ID to specify a single VLAN. In the **VLAN ID** field, enter the number (between 1 and 4094) that matches the identifier.
VLAN Trunking	Use VLAN Trunking to monitor all VLAN traffic. The range defaults to 0-4095.

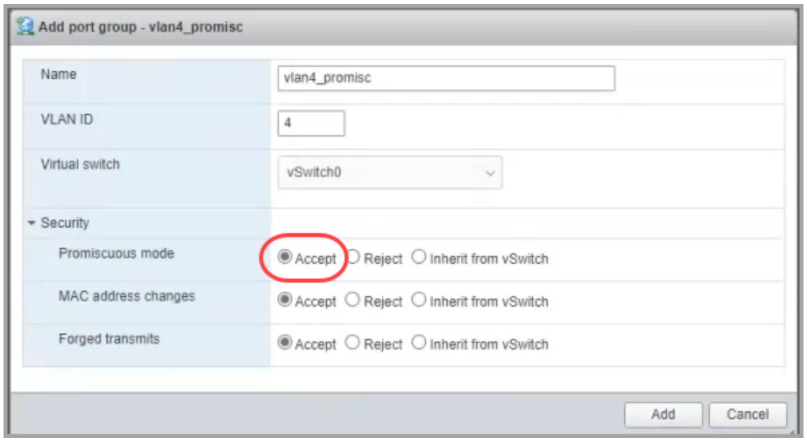
6. Click the **Security** arrow.



Add port group - vlan4_promisc

Name	vlan4_promisc
VLAN ID	4
Virtual switch	vSwitch0
Security	Click to expand

7. **Promiscuous Mode:** Choose **Accept**.



Add port group - vlan4_promisc

Name	vlan4_promisc
VLAN ID	4
Virtual switch	vSwitch0
Security	
Promiscuous mode	● Accept ○ Reject ○ Inherit from vSwitch
MAC address changes	● Accept ○ Reject ○ Inherit from vSwitch
Forged transmits	● Accept ○ Reject ○ Inherit from vSwitch

8. Will the Flow Sensor VE be monitoring another virtual switch in this VMware environment?

    - If yes, go back to **2a. Configuring the Flow Sensor to Monitor Traffic**, and repeat all the steps for the next virtual switch.
    - If no, go to Configuring an Isolated LAN for inter-Data Node Communications if you are deploying Data Nodes, or **3. Installing the Virtual Appliance** if you are not.

2b. Configuring an Isolated LAN for inter-Data Node Communications

If you are deploying Data Nodes VE to your network, configure an isolated LAN with a virtual switch so that the Data Nodes can communicate with each other over **eth1** for inter-Data Node communication.

> We recommend that you deploy all of your Data Nodes VE on the same ESXi host. If you plan on deploying your Data Nodes VE on separate ESXi hosts, contact Cisco Professional Services for assistance in configuring the isolated LAN.

To configure a vSphere Standard Switch:

1. Log into your VMware host environment.
2. From the VMware Host Client inventory, right-click **Networking** and click **Add standard vSwitch**.
3. Enter a vSwitch name.
4. Click **Create virtual switch**.
5. Do **NOT** configure physical network cards as uplinks.
6. Select the **Cisco Discovery Protocol**.
7. Click **Add**.
8. Go to **3. Installing the Virtual Appliance**.

> To configure a vSphere Distributed Switch:

1. Log into your VMware host environment.
2. From the menu, select **Networking**.
3. Right-click a data center and select **Distributed Switch > New Distributed Switch**.
4. Enter a name, then click **Next**.
5. Select a distributed switch version based on your ESXi version, then click **Next**. For example, if you have ESXI 7.0 or later deployed, select `7.0.0`.
6. For **Number of uplinks**, select `0`. Do **NOT** configure physical network cards as uplinks.
7. Select **Create a default port group** and enter a **Port group name**.
8. Click **Next**.

9. Click **Finish**.
10. Go to **3. Installing the Virtual Appliance**.

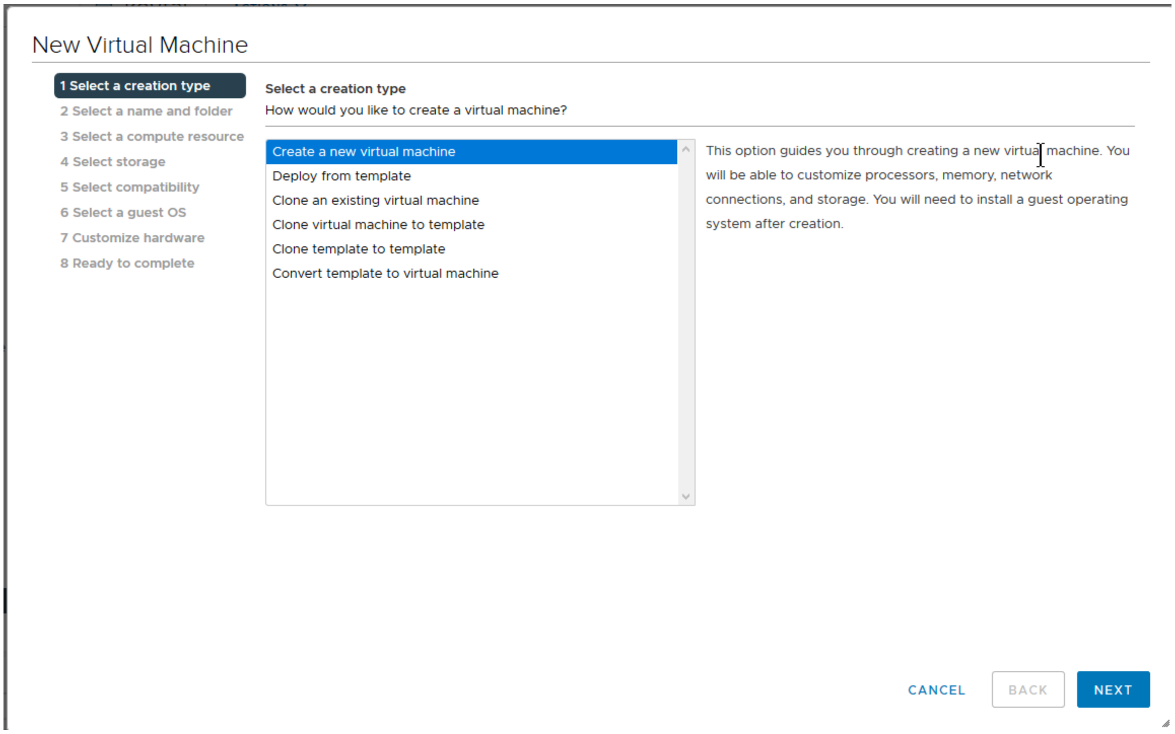
3. Installing the Virtual Appliance

Use the following instructions to install a virtual appliance on your hypervisor host and define the virtual appliance management and monitoring ports.

> Some of the menus and graphics may vary from the information shown here. Please refer to your VMware guide for details related to the software.

1. Locate the virtual appliance software file (ISO) that you downloaded from Cisco Software Central.
2. Make the ISO available in vCenter. You have the following options:
    - Upload the ISO to a vCenter datastore.
    - Add the ISO to a content library.
    - Keep the ISO on your local workstation, and configure the deployment to reference that file.

    See the VMware documentation for more information.
3. From the vCenter UI, select **Menu > Hosts and Clusters**.
4. In the navigation pane, right click a cluster or host and select **New Virtual Machine...** to access the New Virtual Machine wizard.
5. From the Select a creation type window, select **Create a new virtual machine**, then click **Next**.



New Virtual Machine

1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete

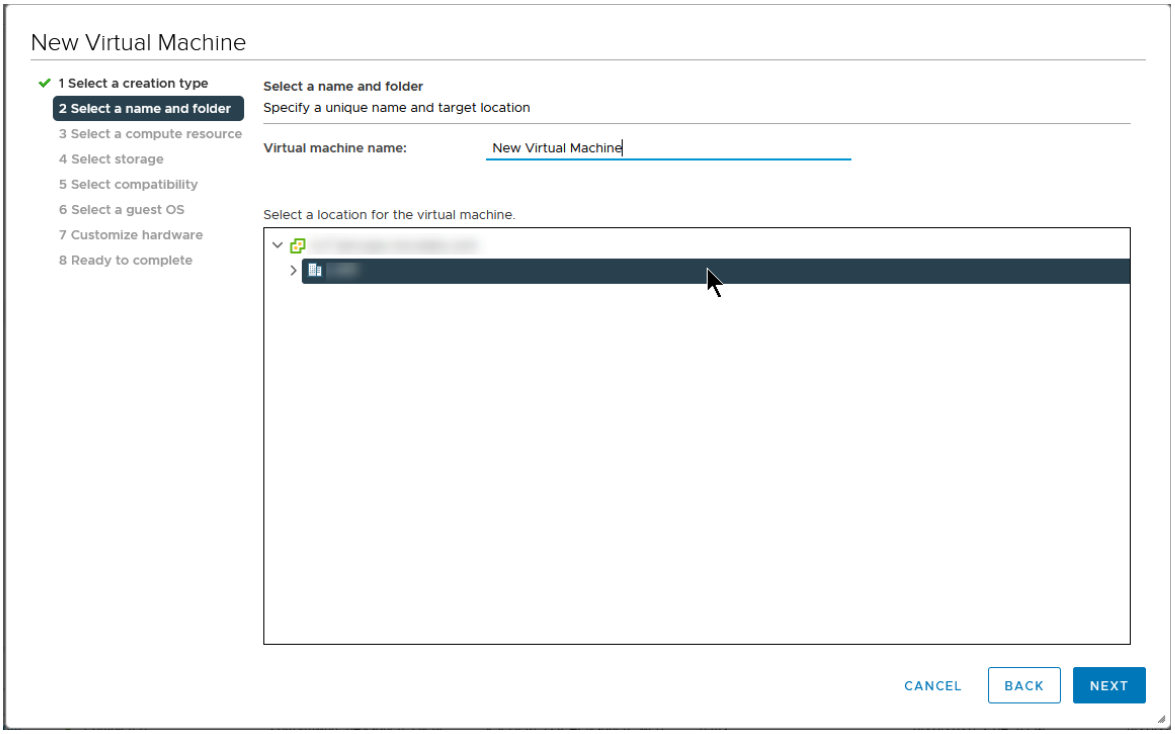
Select a creation type

How would you like to create a virtual machine?

Create a new virtual machine
Deploy from template
Clone an existing virtual machine
Clone virtual machine to template
Clone template to template
Convert template to virtual machine

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

6. From the Select a name and folder window, enter a **Virtual machine name**, **select a location for the virtual machine**, then click **Next**.



New Virtual Machine

Select a name and folder

Specify a unique name and target location

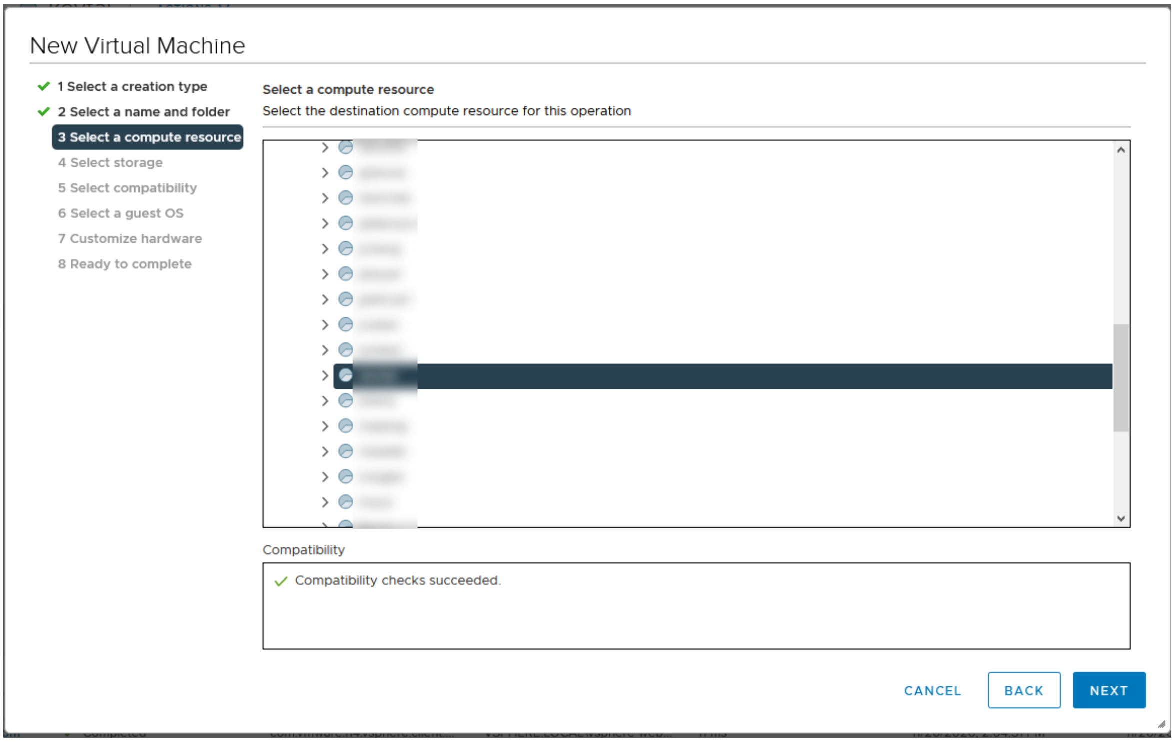
Virtual machine name: New Virtual Machine

Select a location for the virtual machine.

[redacted]

[redacted]

7. From the Select a compute resource window, select a cluster, host, resource pool, or vApp to which you will deploy the appliance, then click **Next**.



New Virtual Machine

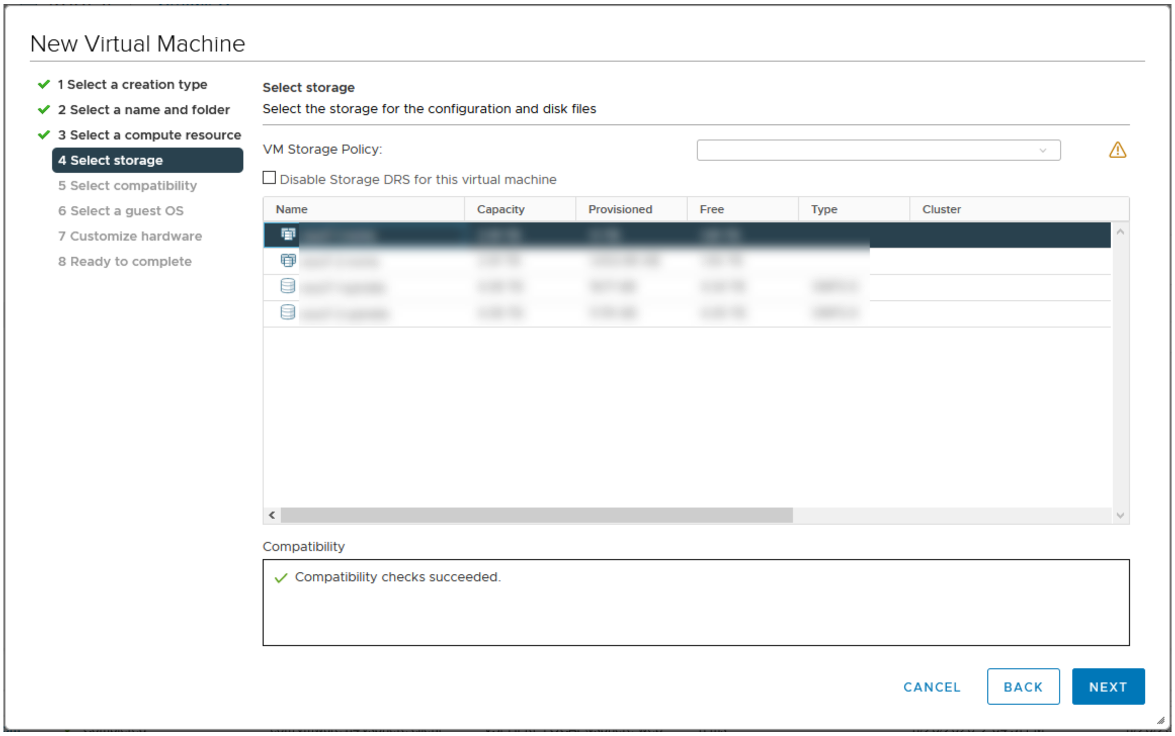
Select a compute resource

Select the destination compute resource for this operation

Compatibility

✓ Compatibility checks succeeded.

8. From the Select storage window, select a **VM Storage Policy** from the drop-down, then select a storage location, then click **Next**.



New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Select storage

Select the storage for the configuration and disk files

VM Storage Policy: ⚠

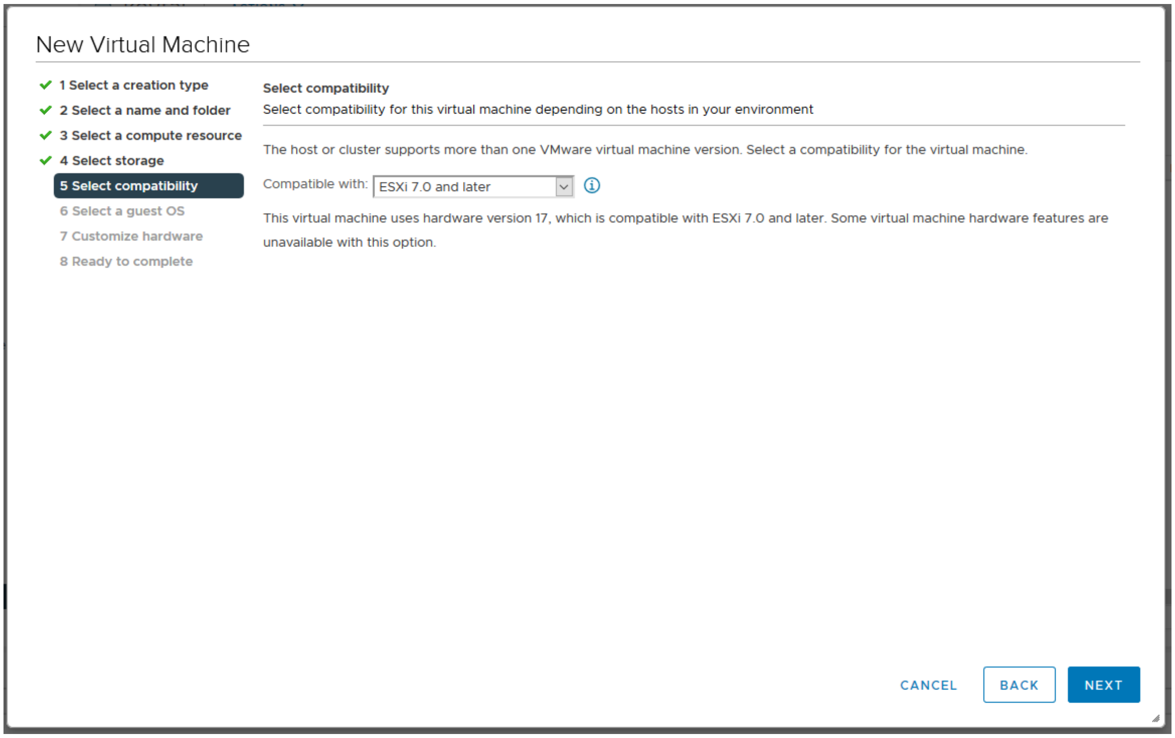
☐ Disable Storage DRS for this virtual machine

Name	Capacity	Provisioned	Free	Type	Cluster
[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	

Compatibility

✓ Compatibility checks succeeded.

9. From the Select compatibility window, select a virtual machine version from the **Compatible with** drop-down, based on your current deployed ESXi version. For example, the following screenshot shows **ESXi 7.0 and later** because ESXi 7.0 is deployed. Click **Next**.



New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Select compatibility

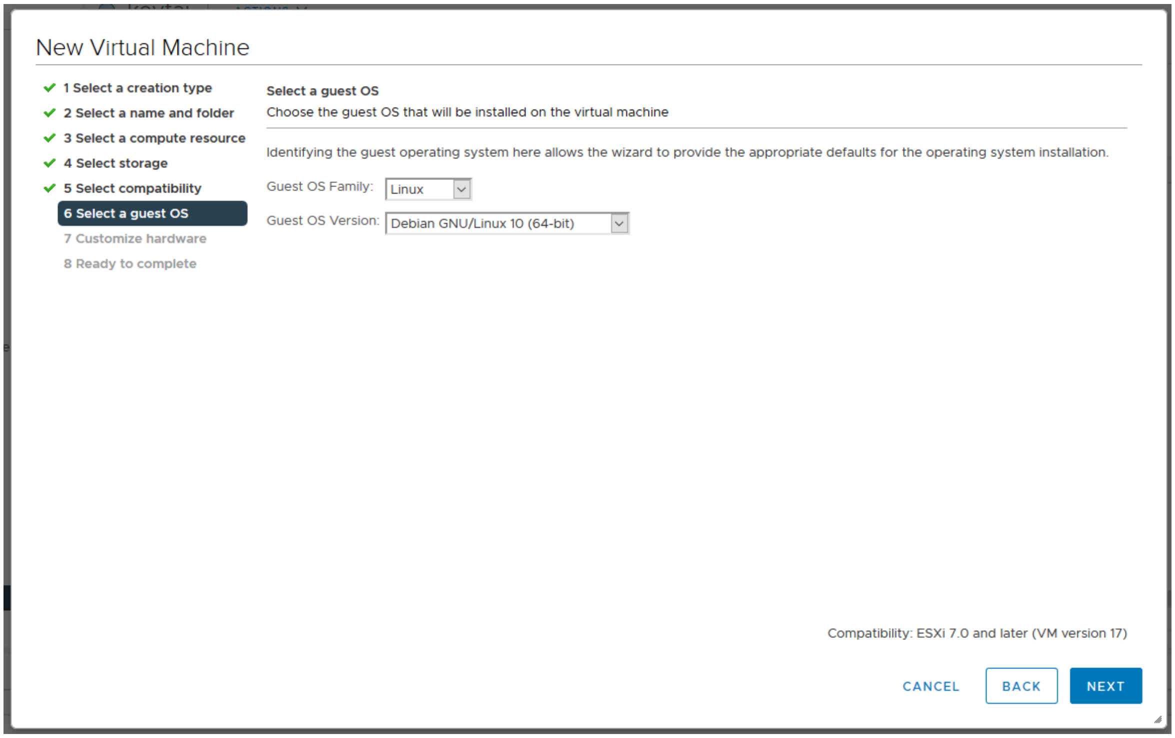
Select compatibility for this virtual machine depending on the hosts in your environment

The host or cluster supports more than one VMware virtual machine version. Select a compatibility for the virtual machine.

Compatible with: ESXi 7.0 and later

This virtual machine uses hardware version 17, which is compatible with ESXi 7.0 and later. Some virtual machine hardware features are unavailable with this option.

10. From the Select a guest OS screen, select the **Linux Guest OS Family** and the **Debian GNU/Linux 10 (64-bit) Guest OS Version.** Click **Next.**



New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Select a guest OS

Choose the guest OS that will be installed on the virtual machine

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

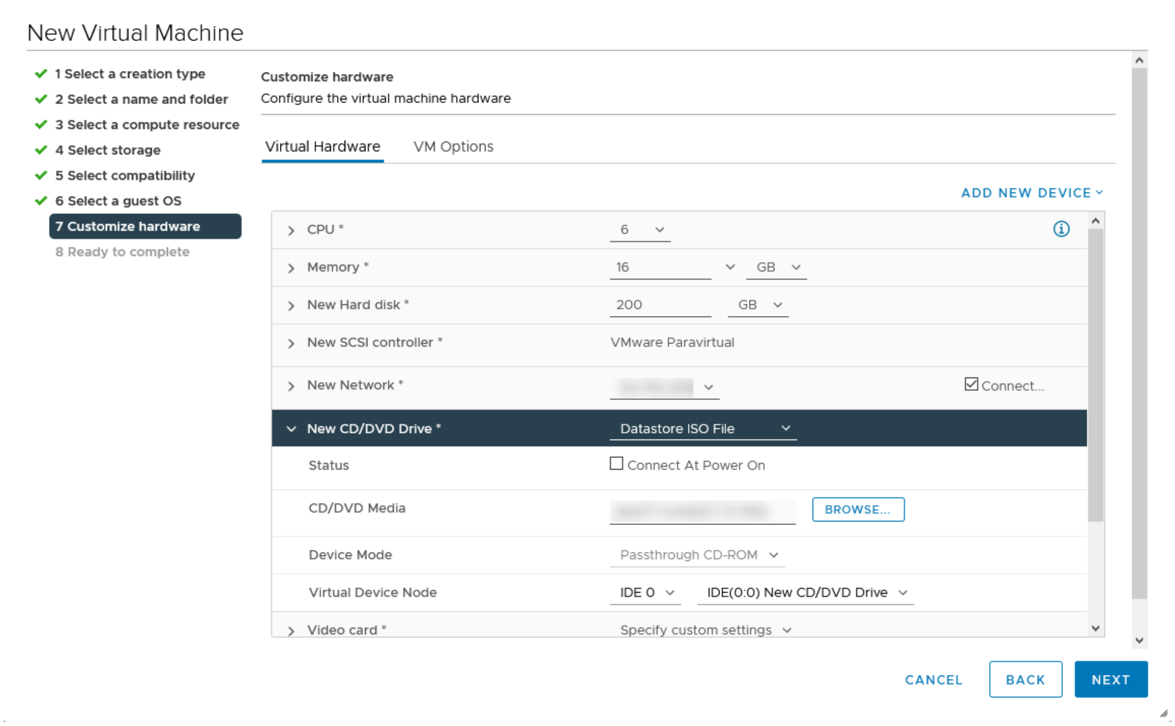
Guest OS Family: Linux

Guest OS Version: Debian GNU/Linux 10 (64-bit)

Compatibility: ESXi 7.0 and later (VM version 17)

11. From the Customize hardware window, configure the virtual hardware. Refer to **Resource Requirements** for specific recommendations for your appliance type.

> ⚠ This step is critical for system performance. If you choose to deploy Cisco Stealthwatch appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.



New Virtual Machine

Customize hardware
Configure the virtual machine hardware

CPU * 6
Memory * 16 GB
New Hard disk * 200 GB
New SCSI controller * VMware Paravirtual
New Network * [redacted] ☑ Connect...
New CD/DVD Drive * Datastore ISO File
Status □ Connect At Power On
CD/DVD Media [redacted] BROWSE...
Device Mode Passthrough CD-ROM
Virtual Device Node IDE 0 IDE(0:0) New CD/DVD Drive
Video card * Specify custom settings

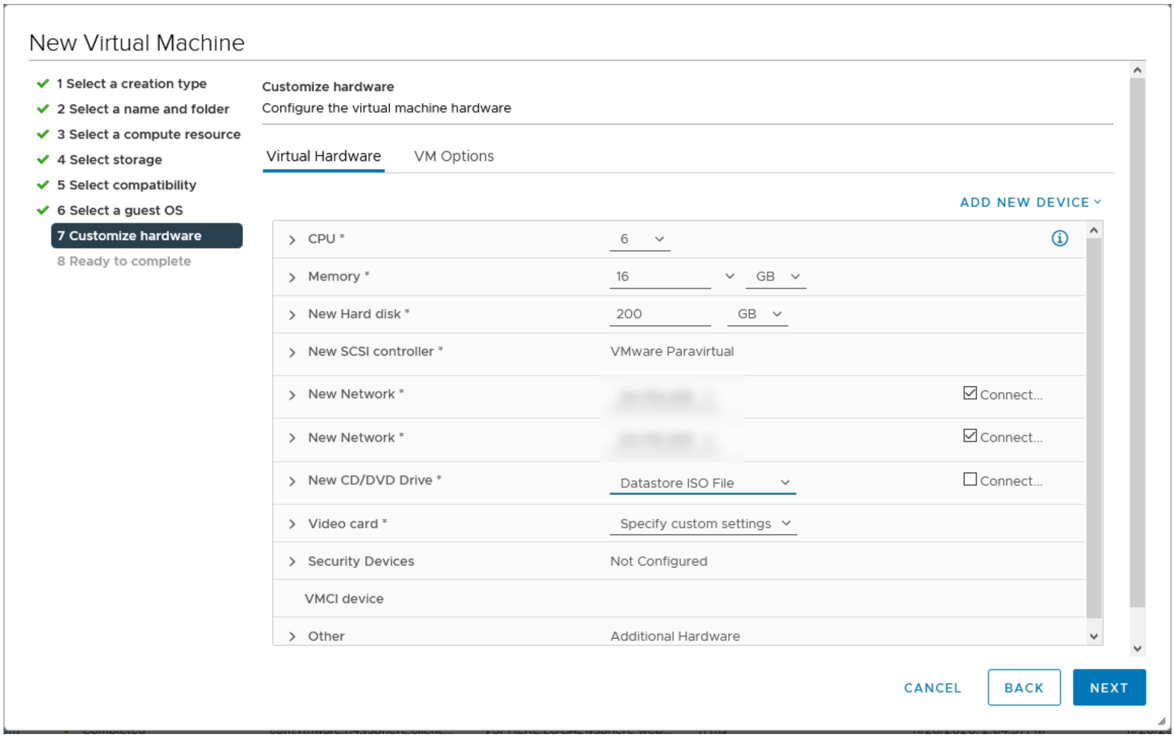
In addition to the resource requirements, select the following settings:

- Click **New Hard disk** to expand the configuration options. Select **Thick Provision Lazy Zeroed** from the **Disk Provisioning** drop-down.
- In the **New CD/DVD Drive** field, select an ISO location based on where you have stored the ISO. Click **New CD/DVD Drive** to expand the configuration options. Check **Connect At Power On**.
- Click **New SCSI controller** to expand the configuration options. Select **LSI Logic SAS** from the **Change Type** drop-down. If you do not select **LSI Logic SAS**, your virtual appliance may fail to properly deploy.

- **If the appliance is a Flow Sensor,** and you are configuring 10 Gbps throughput for the NIC, click **CPU** to expand the configuration options. Configure all **Cores per Socket** so all CPUs are in one socket.

12. If you are deploying a Data Node virtual appliance, also add a second network adaptor. Click **Add New Device**, then select **Network Adaptor**. For the first network adaptor, select a switch that will allow the Data Node VE to communicate on a public network with other appliances. For the second network adaptor, select the switch that you created in Configuring an Isolated LAN for inter-Data Node Communications that will allow the Data Node VE to communicate on a private network with other Data Nodes.

    Ensure that you properly assign the network adaptors and virtual switches for every Data Node in your deployment as you deploy each Data Node.



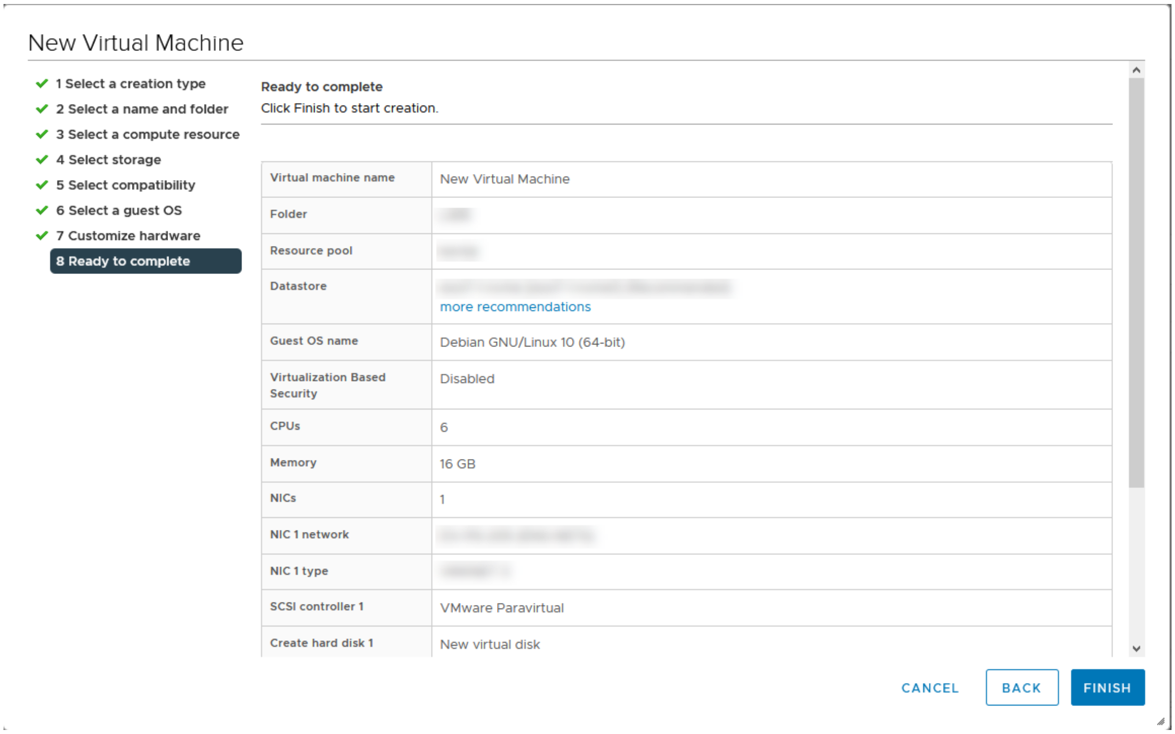
New Virtual Machine

✓ 1 Select a creation type
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Select storage
✓ 5 Select compatibility
✓ 6 Select a guest OS
7 Customize hardware
8 Ready to complete

Customize hardware
Configure the virtual machine hardware

CPU *	6	
Memory *	16 GB	
New Hard disk *	200 GB	
New SCSI controller *	VMware Paravirtual	
New Network *	[redacted]	☑ Connect...
New Network *	[redacted]	☑ Connect...
New CD/DVD Drive *	Datastore ISO File	□ Connect...
Video card *	Specify custom settings	
Security Devices	Not Configured	
VMCI device		
Other	Additional Hardware	

13. From the Ready to complete window, review your settings, then click **Finish**.



New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- ✓ 6 Select a guest OS
- ✓ 7 Customize hardware
- 8 Ready to complete

Ready to complete

Click Finish to start creation.

Virtual machine name	New Virtual Machine
Folder	[redacted]
Resource pool	[redacted]
Datastore	[redacted] more recommendations
Guest OS name	Debian GNU/Linux 10 (64-bit)
Virtualization Based Security	Disabled
CPUs	6
Memory	16 GB
NICs	1
NIC 1 network	[redacted]
NIC 1 type	[redacted]
SCSI controller 1	VMware Paravirtual
Create hard disk 1	New virtual disk

14. The deployment starts in the background. Monitor the deployment progress in the **Recent Tasks** section. Make sure the deployment is completed and shown in the Inventory tree before you go to the next steps.
15. **Flow Sensors:** If the appliance is a Flow Sensor and will be monitoring more than one virtual switch in the VMware environment, or more than one VDS in a cluster, continue with the next section **4. Defining Additional Monitoring Ports (Flow Sensors only)**.
16. Repeat all of the procedures in **3a. Installing a Virtual Appliance using VMware vCenter (ISO)** for the next virtual appliance in your system.

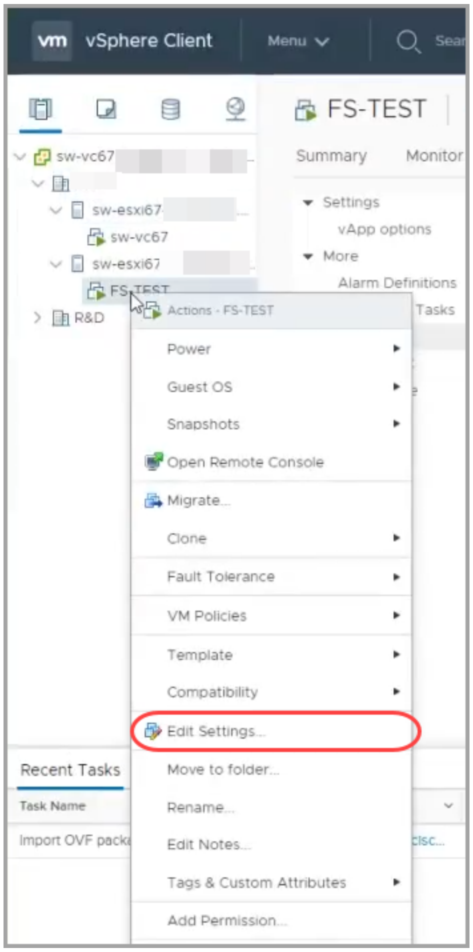
    If you have completed installing all virtual appliances in your system, go to **4. Configuring your Environment using First Time Setup**.

4. Defining Additional Monitoring Ports (Flow Sensors only)

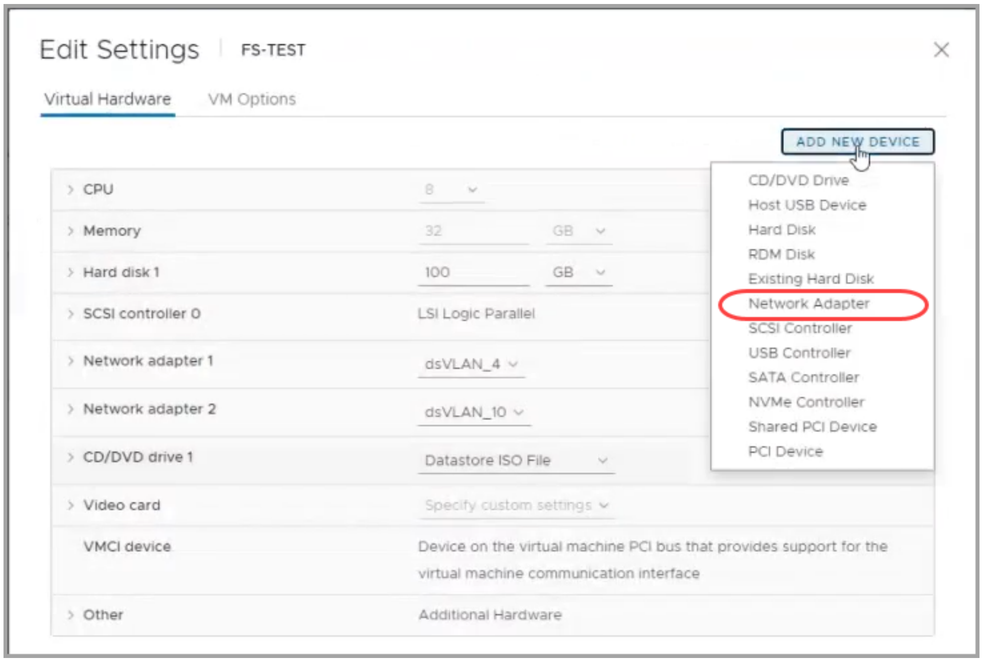
This procedure is required if the Flow Sensor VE will be monitoring more than one virtual switch in a VMware environment or more than one VDS in a cluster. If this is not the monitoring configuration for your Flow Sensor, go to **4. Configuring your Environment using First Time Setup**.

To add Flow Sensor VE monitoring ports, complete the following steps:

1. In the Inventory tree, right-click the Flow Sensor VE. Select **Edit Settings**.



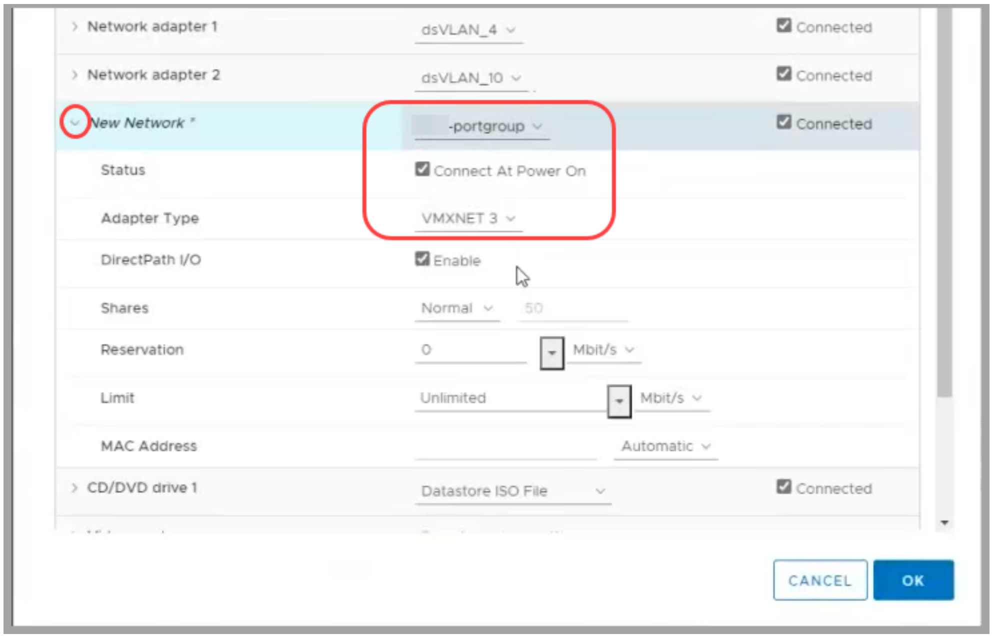
2. Use the **Edit Settings** dialog box to configure the following specified settings.
3. Click **Add New Device**. Select **Network Adapter**.



CPU: 8
Memory: 32 GB
Hard disk 1: 100 GB
SCSI controller 0: LSI Logic Parallel
Network adapter 1: dsVLAN_4
Network adapter 2: dsVLAN_10
CD/DVD drive 1: Datastore ISO File
Video card: Specify custom settings
VMCI device: Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other: Additional Hardware

4. Locate the new network adapter. Click the arrow to expand the menu, and configure the following:

   - **New Network:** Select an unassigned promiscuous port group.
   - **Adapter Type:** Select **VMXNET 3**.
   - **Status:** Check the **Connect at Power On** check box.



Network adapter 1: dsVLAN_4 ☑ Connected
Network adapter 2: dsVLAN_10 ☑ Connected
New Network *: -portgroup ☑ Connected
Status: ☑ Connect At Power On
Adapter Type: VMXNET 3
DirectPath I/O: ☑ Enable
Shares: Normal 50
Reservation: 0 Mbit/s
Limit: Unlimited Mbit/s
MAC Address: Automatic
CD/DVD drive 1: Datastore ISO File ☑ Connected

5. After reviewing the settings, click **OK**.
6. Repeat this procedure to add another Ethernet adapter as needed.

   If you have added all Ethernet adapters, go to to **4. Configuring your Environment using First Time Setup**.

3b. Installing a Virtual Appliance on an ESXi Stand-Alone Server (ISO)

Overview

Use the following instructions to install your virtual appliances using a **VMware environment with an ESXi Stand-alone server**.

> ℹ If you plan on deploying Data Nodes as part of a Data Store, review the Data Store Installation and Configuration Guide before you begin for full instructions on initializing the Data Store, including proper order of appliance deployment.

To use an alternative method, refer to the following:

- **VMware vCenter:** Use **3a. Installing a Virtual Appliance using VMware vCenter (ISO)** .
- **KVM:** Use **3c. Installing a Virtual Appliance on a KVM Host (ISO)**.

Before You Begin

Before you begin the installation, complete the following preparation procedures:

1. **Compatibility:** Review the compatibility requirements in **Compatibility**.
2. **Resource Requirements:** Review the Resource Requirements section to determine the required allocations for the appliance. You can use a resource pool or alternative method to allocate resources.
3. **Firewall:** Configure your firewall for communications. Refer to **1. Configuring your Firewall and Ports**.
4. **Files:** Download the appliance ISO files. Refer to **2. Downloading VE Installation Files** for instructions.
5. **Time:** Confirm the time set on the hypervisor host in your VMware environment (where you will be installing the virtual appliance) shows the correct time. Otherwise, the virtual appliances may not be able to boot up.

> ⚠ Do not install an untrusted physical or virtual machine on the same physical cluster/system as your Stealthwatch appliances.

⚠ Do not install VMware Tools on a Stealthwatch virtual appliance because it will override the custom version already installed. Doing so would render the virtual appliance inoperable and require reinstallation.

Installing a Virtual Appliance on an ESXi Stand-Alone Server (ISO)

Use the following instructions to install your virtual appliances using a **VMware environment with an ESXi Stand-alone server**.

Process Overview

Installing a virtual appliance involves completing the following procedures, which are covered in this chapter:

1. Logging in to the VMware Web Client

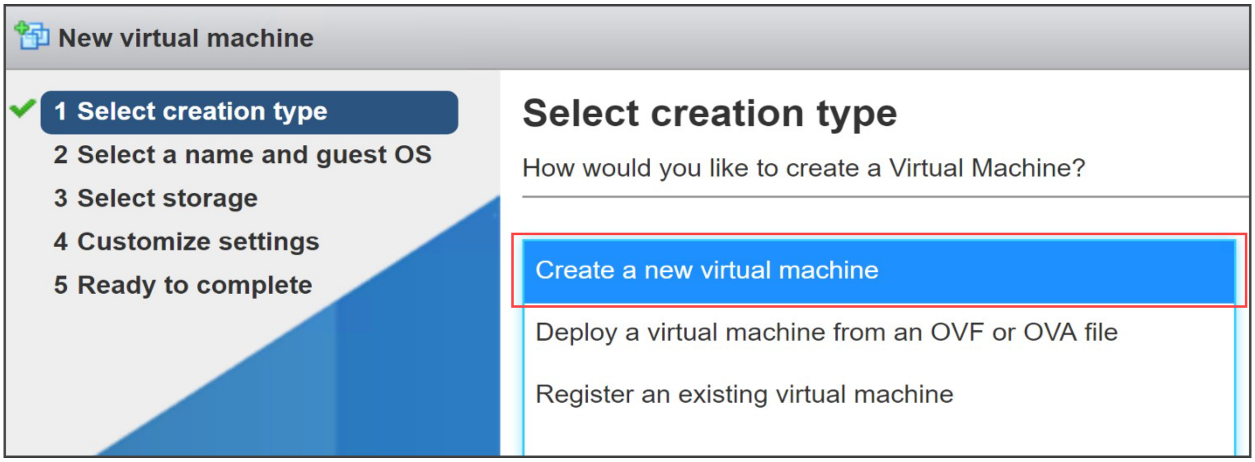
2. Booting from the ISO

Flow Sensors: If the appliance is a Flow Sensor, review **Stealthwatch Flow Sensor** to understand the additional configuration steps required.

1. Logging in to the VMware Web Client

Some of the menus and graphics may vary from the information shown here. Please refer to your VMware guide for details related to the software.

1. Log in to the VMware Web Client.
2. Click **Create/Register a Virtual Machine**.
3. Use the **New Virtual Machine** dialog box to configure the appliance as specified in the following steps.
4. **Select Creation Type:** Select **Create a New Virtual Machine**.



New virtual machine

✓ 1 Select creation type
2 Select a name and guest OS
3 Select storage
4 Customize settings
5 Ready to complete

Select creation type

How would you like to create a Virtual Machine?

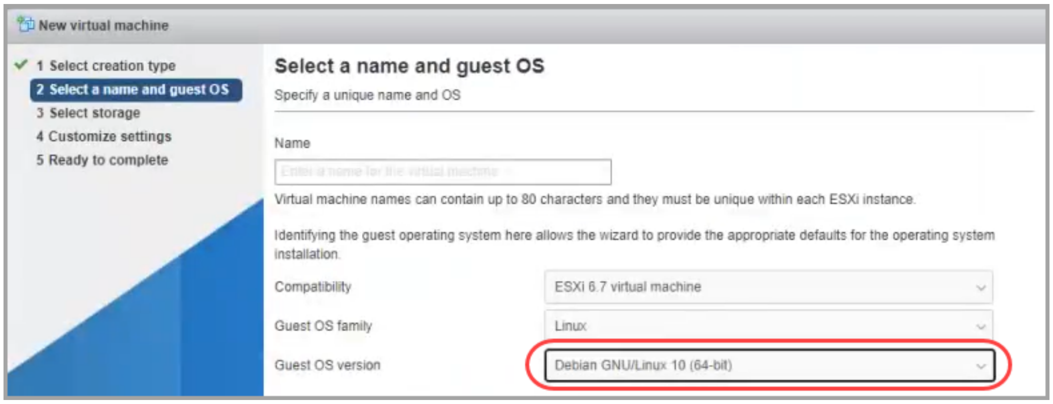
Create a new virtual machine

Deploy a virtual machine from an OVF or OVA file

Register an existing virtual machine

5. **Select a Name and Guest OS:** Enter or select the following:

   - **Name:** Enter a name for the appliance so you can identify it easily.
   - **Compatibility:** Select the version you are using (v6.5 or v6.7).
   - **Guest OS family:** Linux.
   - **Guest OS version:** Select **Debian GNU/Linux 10 64-bit**.



New virtual machine

✓ 1 Select creation type
2 Select a name and guest OS
3 Select storage
4 Customize settings
5 Ready to complete

Select a name and guest OS

Specify a unique name and OS

Name

Enter a name for the virtual machine

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

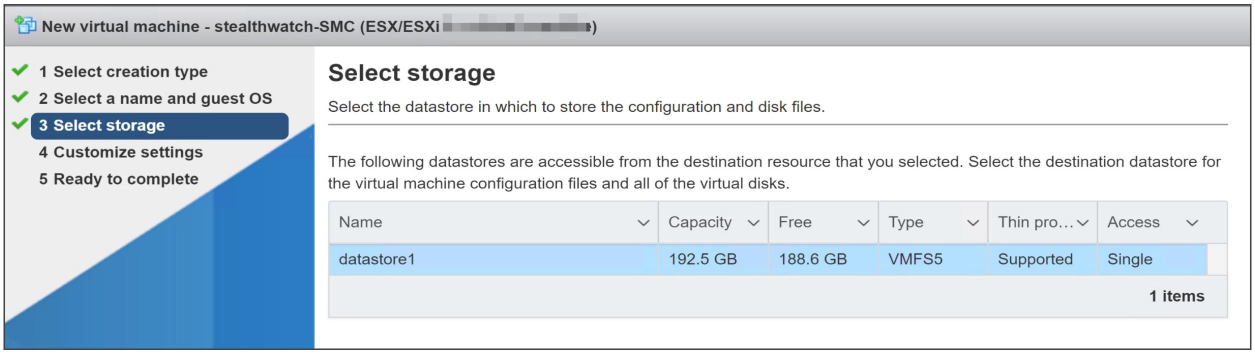
Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility: ESXi 6.7 virtual machine

Guest OS family: Linux

Guest OS version: Debian GNU/Linux 10 (64-bit)

6. **Select Storage:** Select an accessible datastore. Review Resource Requirements to confirm you have enough space.



New virtual machine - stealthwatch-SMC (ESX/ESXi [redacted])

✓ 1 Select creation type
✓ 2 Select a name and guest OS
✓ 3 Select storage
4 Customize settings
5 Ready to complete

Select storage

Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	192.5 GB	188.6 GB	VMFS5	Supported	Single

1 items

Review Resource Requirements to allocate sufficient resources. This step is critical for system performance.

⚠ If you choose to deploy Cisco Stealthwatch appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.

7. **Customize Settings:** Enter or select your appliance requirements (refer to Resource Requirements for details).

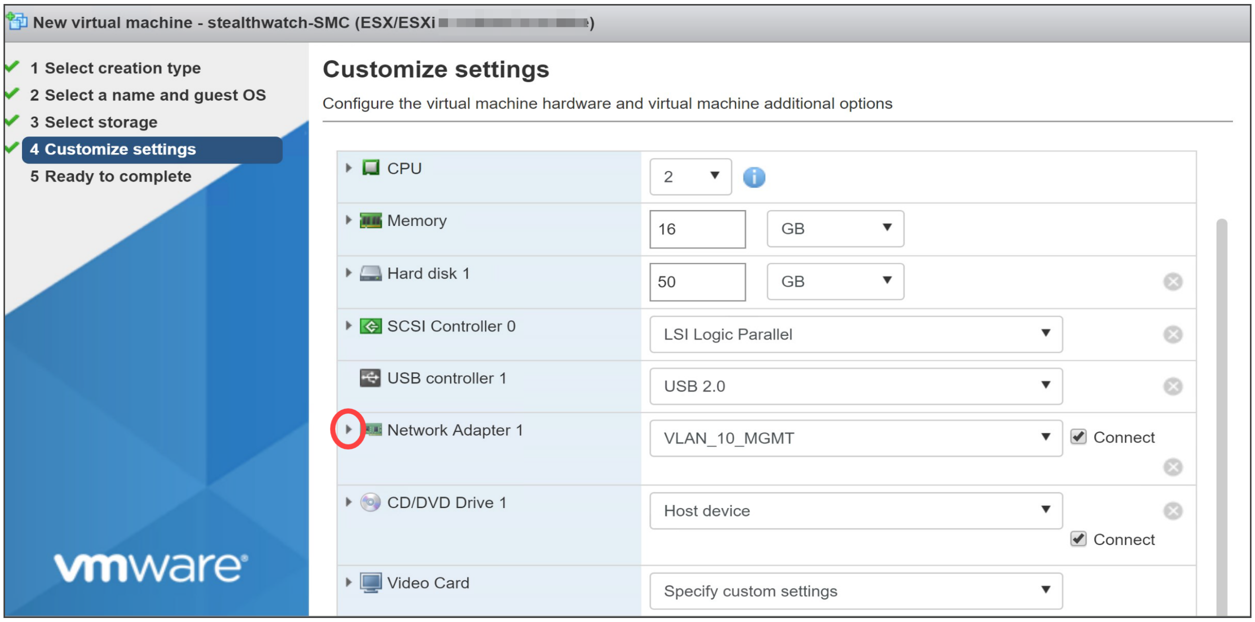
   Make sure you select the following:

   - **SCSI Controller:** LSI Logic SAS
   - **Network Adapter:** Confirm the management address for the appliance.
   - **Hard Disk:** Thick Provisioning Lazy Zeroed

     If the appliance is a Flow Sensor, you can click **Add Network Adapter** to add another management or sensing interface. Refer to **Stealthwatch Flow Sensor** for details.

     If the appliance is a Flow Sensor, and you are configuring 10 Gbps throughput for the NIC, click **CPU** to expand the configuration options. Configure all all CPUs in one socket.

     If the appliance is a Data Node, you must add another network interface to allow inter-Data Node communications. Click **Add Network Adapter**. For the first network adaptor, select a switch that will allow the Data Node VE to communicate on a public network with other appliances. For the second network adaptor, select the switch that you created in Configuring an Isolated LAN for inter-Data Node Communications that will allow the Data Node VE to communicate on a private network with other Data Nodes.



New virtual machine - stealthwatch-SMC (ESX/ESXi [redacted])

✓ 1 Select creation type
✓ 2 Select a name and guest OS
✓ 3 Select storage
✓ 4 Customize settings
5 Ready to complete

Customize settings

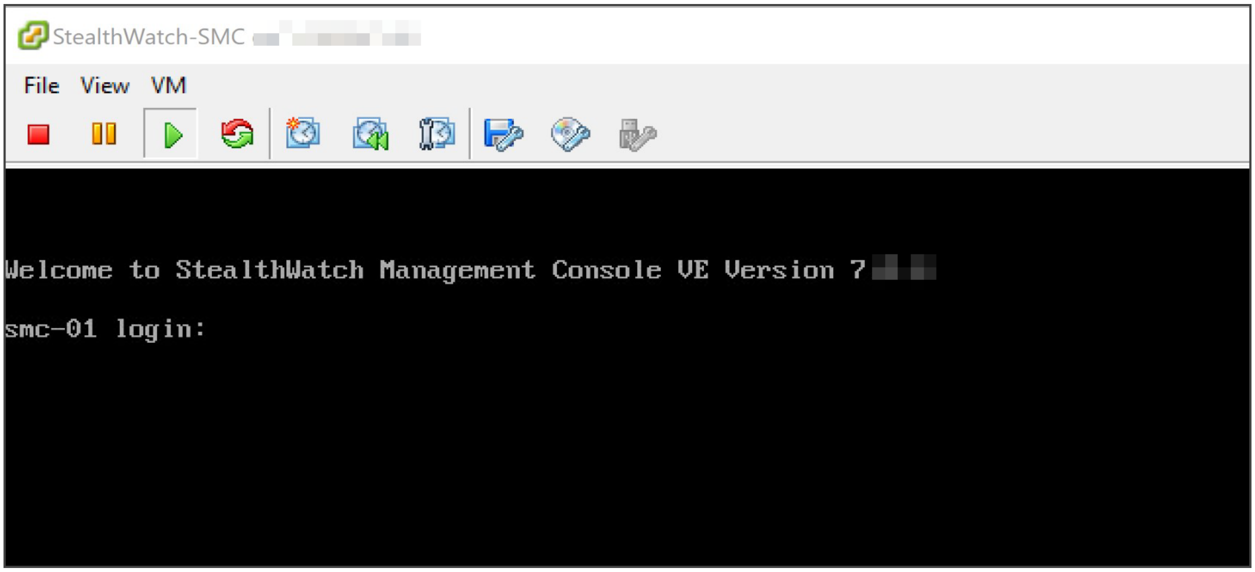
Configure the virtual machine hardware and virtual machine additional options

CPU	2
Memory	16 GB
Hard disk 1	50 GB
SCSI Controller 0	LSI Logic Parallel
USB controller 1	USB 2.0
Network Adapter 1	VLAN_10_MGMT ☑ Connect
CD/DVD Drive 1	Host device ☑ Connect
Video Card	Specify custom settings

8. Click the arrow next to Network Adapter.
9. For the Adapter Type, select **VMXnet3**.
10. Review your configuration settings and confirm they are correct.
11. Click **Finish**. A virtual machine container is created.

2. Booting from the ISO

1. Open the VMware console.
2. Connect the ISO to the new virtual machine. Refer to the VMware guide for details.
3. Boot the virtual machine from the ISO. It runs the installer and reboots automatically.
4. Once the installation and reboot are completed, you will see the login prompt.



```
Welcome to StealthWatch Management Console VE Version 7[redacted]

smc-01 login:
```

5. Disconnect the ISO from the virtual machine.
6. Repeat all of the procedures in **3b. Installing a Virtual Appliance on an ESXi Stand-Alone Server (ISO)** for the next virtual appliance.
7. **Flow Sensors:** If the appliance is a Flow Sensor, review **Stealthwatch Flow Sensor** and finish the setup using the previous sections of this manual:
    - **2a. Configuring the Flow Sensor to Monitor Traffic** (use Monitoring a vSwitch with a Single Host)
    - If the Flow Sensor will be monitoring more than one virtual switch in the VMware environment, or more than one VDS in a cluster, go to **4. Defining Additional Monitoring Ports (Flow Sensors only)**.
8. If you have completed installing all virtual appliances in your system, go to **4. Configuring your Environment using First Time Setup**.

3c. Installing a Virtual Appliance on a KVM Host (ISO)

Overview

Use the following instructions to install your virtual appliances using **KVM and Virtual Machine Manager**.

> ⓘ If you plan on deploying Data Nodes as part of a Data Store, review the Data Store Installation and Configuration Guide before you begin for full instructions on initializing the Data Store, including proper order of appliance deployment.

To use an alternative method, refer to the following:

- **VMware vCenter:** Use **3a. Installing a Virtual Appliance using VMware vCenter (ISO)** .
- **VMware ESXi Stand-Alone Server:** Use **3b. Installing a Virtual Appliance on an ESXi Stand-Alone Server (ISO)**.

Before You Begin

Before you begin the installation, make sure you've completed the following procedures:

1. **Compatibility:** Review the compatibility requirements in **Compatibility**.
2. **Resource Requirements:** Review the Resource Requirements section to determine the required allocations for the appliance. You can use a resource pool or alternative method to allocate resources.
3. **Firewall:** Configure your firewall for communications. Refer to **1. Configuring your Firewall and Ports**.
4. **Files:** Download the appliance ISO files and copy them to a folder on the KVM host.We use the following folder in the example provided in this section: var/lib/libvirt/image. Refer to **2. Downloading VE Installation Files** for instructions.
5. **Time:** Confirm the time set on the hypervisor host in your VMware environment (where you will be installing the virtual appliance) shows the correct time. Otherwise, the virtual appliances may not be able to boot up.

⚠ Do not install an untrusted physical or virtual machine on the same physical cluster/system as your Stealthwatch appliances.

Installing a Virtual Appliance on a KVM Host (ISO)

If you have a KVM host, use the following instructions to install a virtual appliance using the ISO.

Process Overview

Installing a virtual appliance involves completing the following procedures, which are covered in this chapter:

Configuring an isolated LAN for Data Nodes

1. Installing a Virtual Appliance on a KVM Host

2. Adding NIC (Data Node, Flow Sensor) and Promiscuous Port Monitoring on an Open vSwitch (Flow Sensors Only)

Configuring an isolated LAN for Data Nodes

If you are deploying Data Nodes VE to your network, configure an isolated LAN with a virtual switch so that the Data Nodes can communicate with each other over **eth1** for inter-Data Node communication. See your virtual switch's documentation for more information on creating an isolated LAN.

> ⓘ We recommend that you deploy all of your Data Nodes VE on the same ESXi host. If you plan on deploying your Data Nodes VE on separate ESXi hosts, contact Cisco Professional Services for assistance in configuring the isolated LAN.

1. Installing a Virtual Appliance on a KVM Host

There are several methods to install a virtual machine on a KVM host using a ISO file. The following steps give one example for installing a virtual Stealthwatch Management Console (SMC) through a GUI tool called Virtual Machine Manager running on a Ubuntu box. You can use any compatible Linux distribution. For compatibility details, refer to **Compatibility**.

Monitoring Traffic

The Flow Sensor VE has the ability to provide visibility into KVM environments, generating flow data for areas that are not flow-enabled. As a virtual appliance installed inside each KVM host, the Flow Sensor VE passively captures Ethernet frames from traffic it observes and creates flow records containing valuable session statistics that pertain to conversational pairs, bit rates, and packet rates. For details, refer to **Stealthwatch Flow Sensor**: Integrating the Flow Sensor VE into your network.

Configuration Requirements

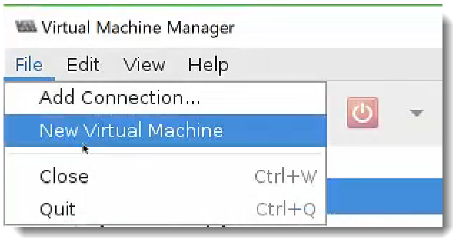
This configuration has the following requirements:

- **Promiscuous Mode:** Enabled.
- **Promiscuous Port:** Configured to an open vSwitch.

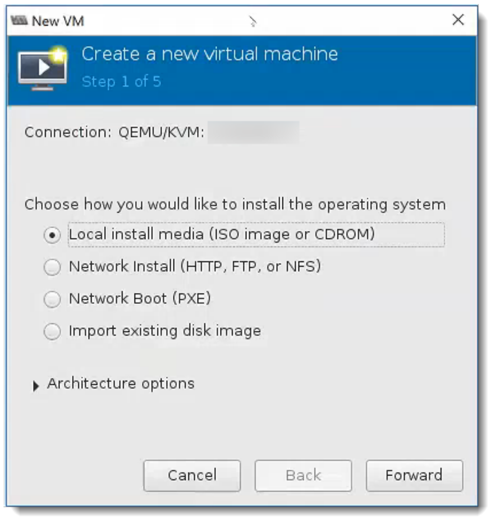
Installing a Virtual Appliance on a KVM Host

To install a virtual appliance, and enable the Flow Sensor VE to monitor traffic, complete the following steps:

1. Use Virtual Machine Manager to connect to the KVM Host and configure the appliance as specified in the following steps.
2. Click **File > New Virtual Machine**.



3. Select **Local install media (ISO image or CDROM)**. Click **Forward**.



New VM

Create a new virtual machine

Step 1 of 5

Connection: QEMU/KVM: [redacted]

Choose how you would like to install the operating system

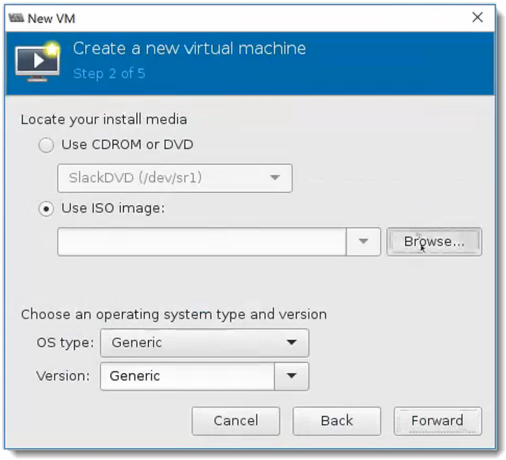
● Local install media (ISO image or CDROM)

○ Network Install (HTTP, FTP, or NFS)

○ Network Boot (PXE)

○ Import existing disk image

4. Click **Use ISO image**.
5. Click **Browse**. Select the appliance image.



New VM

Create a new virtual machine

Step 2 of 5

Locate your install media

○ Use CDROM or DVD

SlackDVD (/dev/sr1)

● Use ISO image:

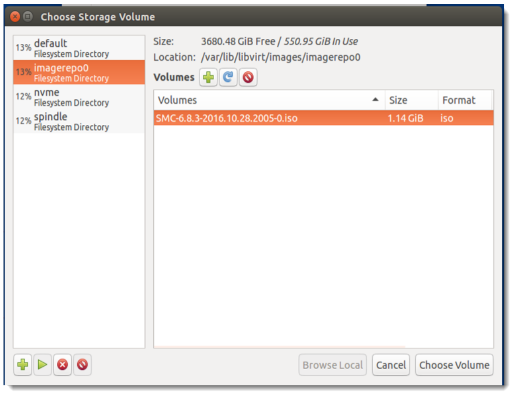
Choose an operating system type and version

OS type: Generic

Version: Generic

6. Select the ISO file. Click **Choose Volume**.

   Confirm the ISO file is accessible by the KVM Host.



Choose Storage Volume

13%	default Filesystem Directory
13%	imagerepo0 Filesystem Directory
12%	nvme Filesystem Directory
12%	spindle Filesystem Directory

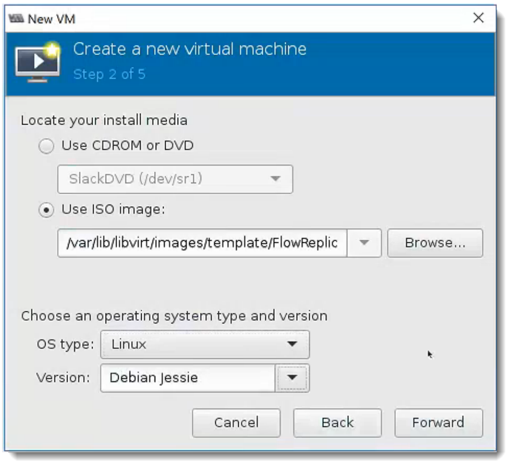
Size: 3680.48 GiB Free / *550.95 GiB In Use*

Location: /var/lib/libvirt/images/imagerepo0

Volumes

Volumes	Size	Format
SMC-6.8.3-2016.10.28.2005-0.iso	1.14 GiB	iso

7. Under Choose an operating system type and version, select **Linux** from the OS type drop-down list.
8. From the Version drop-down list, select **Debian Jessie**. Click **Forward**.



Locate your install media

○ Use CDROM or DVD

SlackDVD (/dev/sr1)

● Use ISO image:

/var/lib/libvirt/images/template/FlowReplic

Choose an operating system type and version

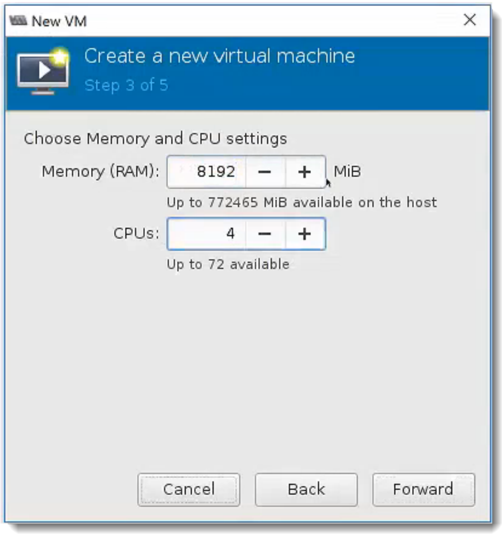
OS type: Linux

Version: Debian Jessie

9. Increase the Memory (RAM) and CPUs to the amount shown in the **Resource Requirements** section.

Review Resource Requirements to allocate sufficient resources. This step is critical for system performance.

⚠ If you choose to deploy Cisco Stealthwatch appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.



Choose Memory and CPU settings

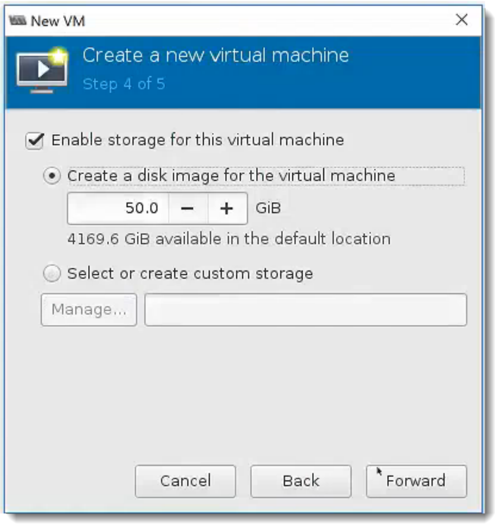
Memory (RAM): 8192 MiB

Up to 772465 MiB available on the host

CPUs: 4

Up to 72 available

10. Select **Create a disk image for the virtual machine**.
11. Enter the data storage amount shown for the appliance in **Resource Requirements** section. Click **Forward**.



☑ Enable storage for this virtual machine

● Create a disk image for the virtual machine

50.0 GiB

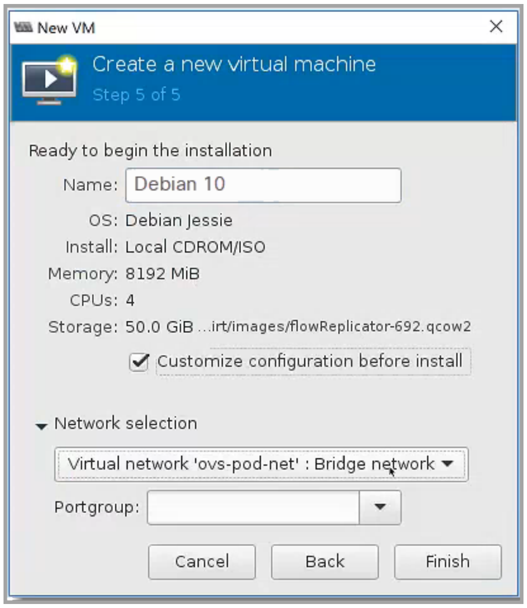
4169.6 GiB available in the default location

○ Select or create custom storage

Review Resource Requirements to allocate sufficient resources. This step is critical for system performance.

⚠ If you choose to deploy Cisco Stealthwatch appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.

12. Assign a Name for the virtual machine. This will be the display name, so use a name that will help you find it later.
13. Check the **Customize configuration before install** check box.
14. In the **Network selection** drop-down box, select the applicable network and port group for installation. If this is a Data Node, select a network and port group that will allow the Data Node to communicate on a public network with other appliances.



New VM

Create a new virtual machine
Step 5 of 5

Ready to begin the installation

Name: Debian 10

OS: Debian Jessie
Install: Local CDROM/ISO
Memory: 8192 MiB
CPUs: 4
Storage: 50.0 GiB ...irt/images/flowReplicator-692.qcow2

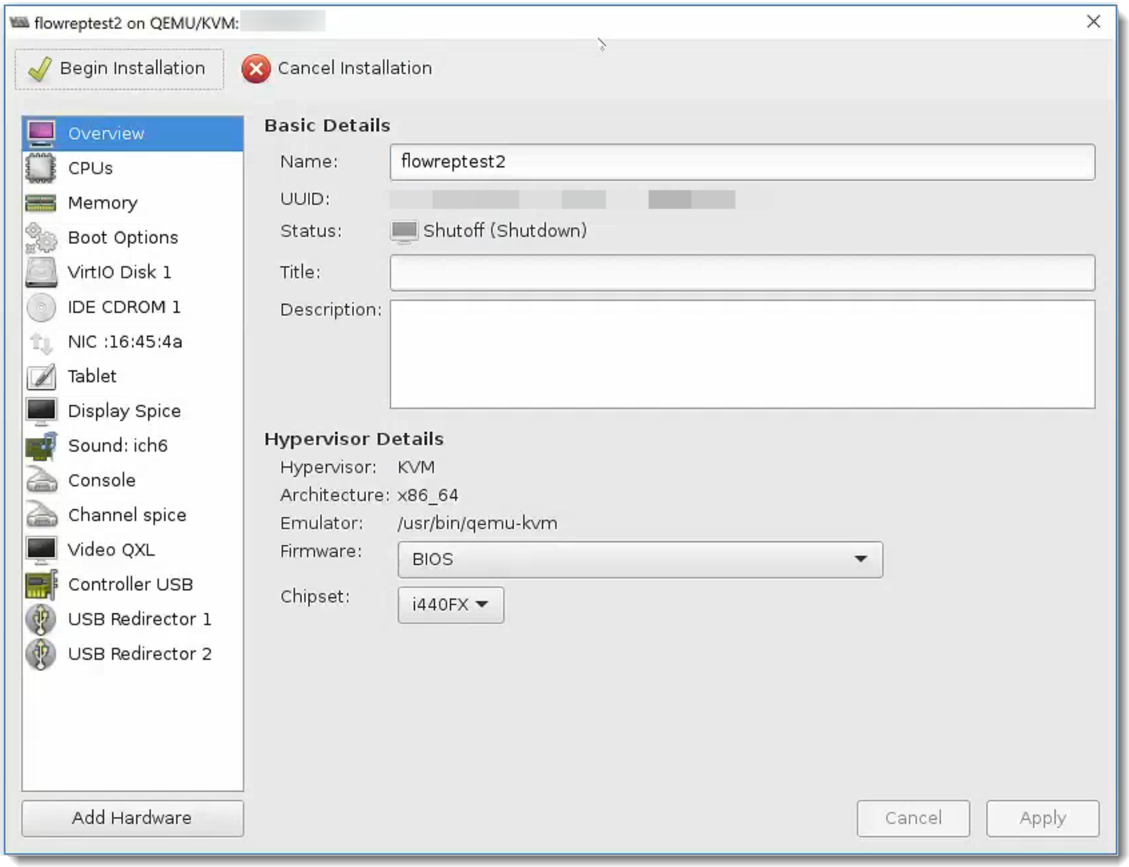
☑ Customize configuration before install

Network selection

Virtual network 'ovs-pod-net' : Bridge network

Portgroup:

15. Click **Finish**. The configuration menu opens.



flowreptest2 on QEMU/KVM: [redacted]

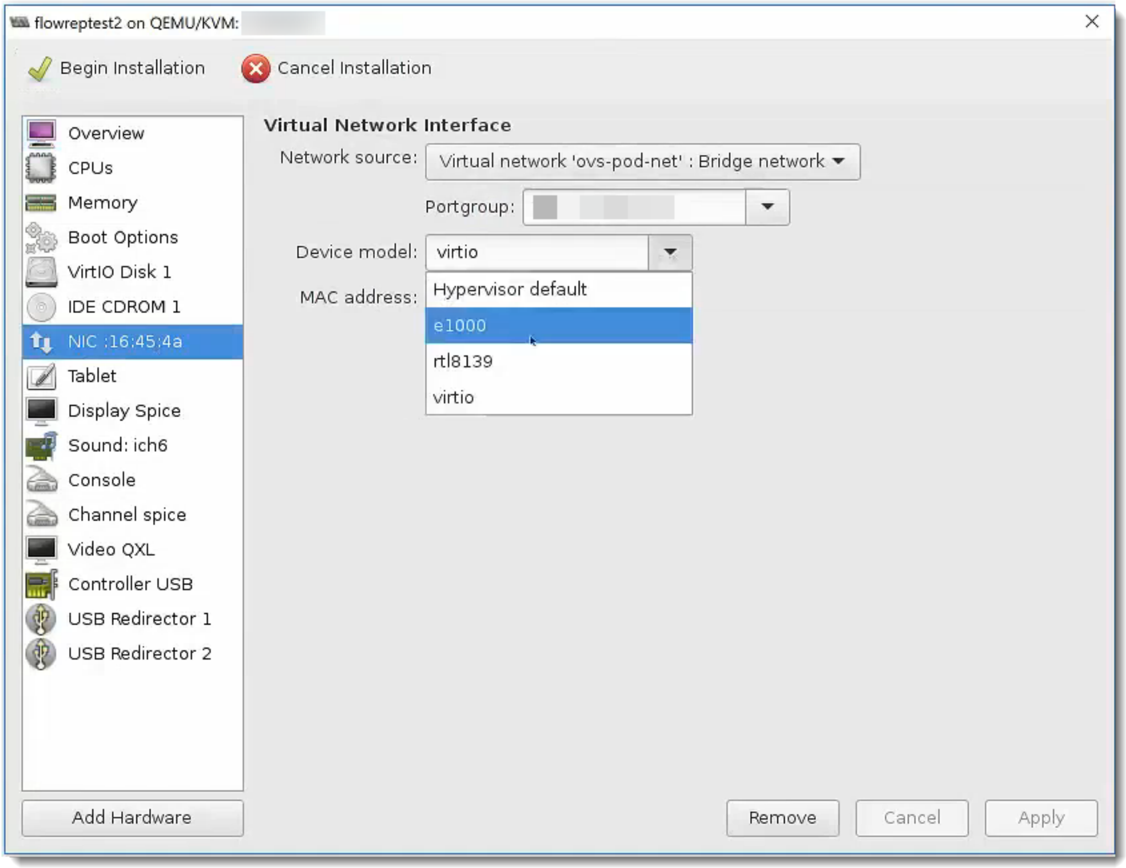
Basic Details

Name: flowreptest2
UUID: [redacted]
Status: Shutoff (Shutdown)
Title:
Description:

Hypervisor Details

Hypervisor: KVM
Architecture: x86_64
Emulator: /usr/bin/qemu-kvm
Firmware: BIOS
Chipset: i440FX

16. In the navigation pane, select **NIC**.
17. Under Virtual Network Interface, select **e1000** in the Device model drop-down box. Click **Apply.**



flowreptest2 on QEMU/KVM: [redacted]

Virtual Network Interface

Network source: Virtual network 'ovs-pod-net' : Bridge network

Portgroup: [redacted]

Device model: virtio

MAC address:

18. Click **VirtIO Disk 1**.
19. In the Advanced Options drop-down list, select **SCSI** in the Disk bus drop-down box. Click **Apply**.
20. Do you need to add additional NICS for monitoring ports on the Flow Sensor VE, or to enable inter-Data Node communications on a Data Node VE?

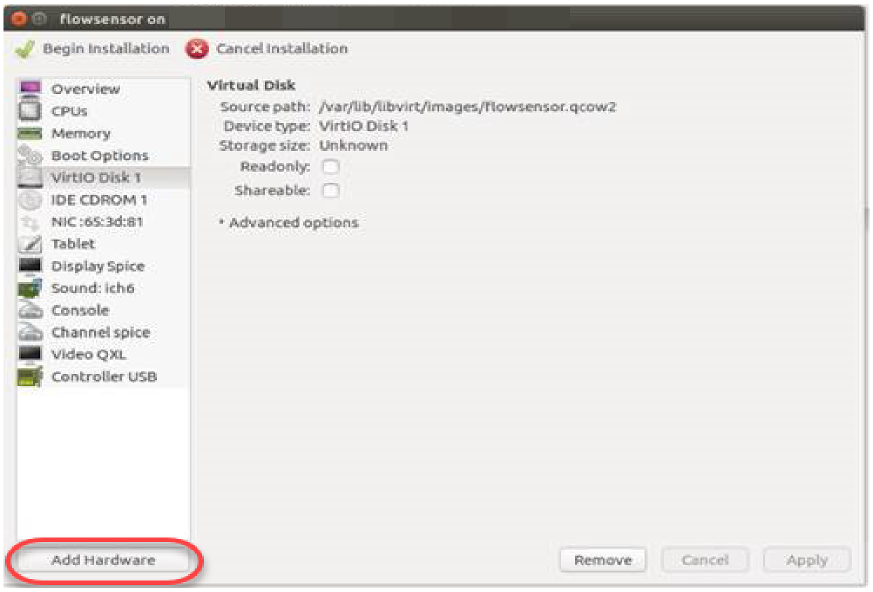
    - If yes, go to **2. Adding NIC (Data Node, Flow Sensor) and Promiscuous Port Monitoring on an Open vSwitch (Flow Sensors Only)**.
    - If no, go to the next step.

21. Click **Begin Installation**.
22. Go to **4. Configuring your Environment using First Time Setup**.

2. Adding NIC (Data Node, Flow Sensor) and Promiscuous Port Monitoring on an Open vSwitch (Flow Sensors Only)

To add additional NICs for the Flow Sensor VE monitoring ports or Data Node VE and to complete the installation, complete the following steps:

1. In the Configuration Menu, click **Add Hardware**. The Add New Virtual Hardware dialog box displays.

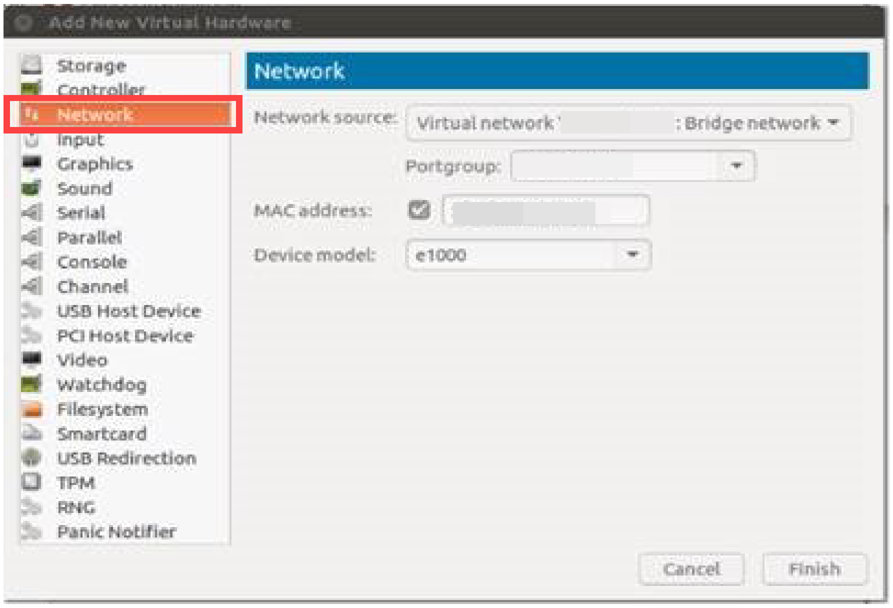


Virtual Disk

Source path: /var/lib/libvirt/images/flowsensor.qcow2
Device type: VirtIO Disk 1
Storage size: Unknown
Readonly: □
Shareable: □

▸ Advanced options

2. In the left navigation pane, click **Network**.



Network

Network source: Virtual network '[redacted] : Bridge network

Portgroup: [redacted]

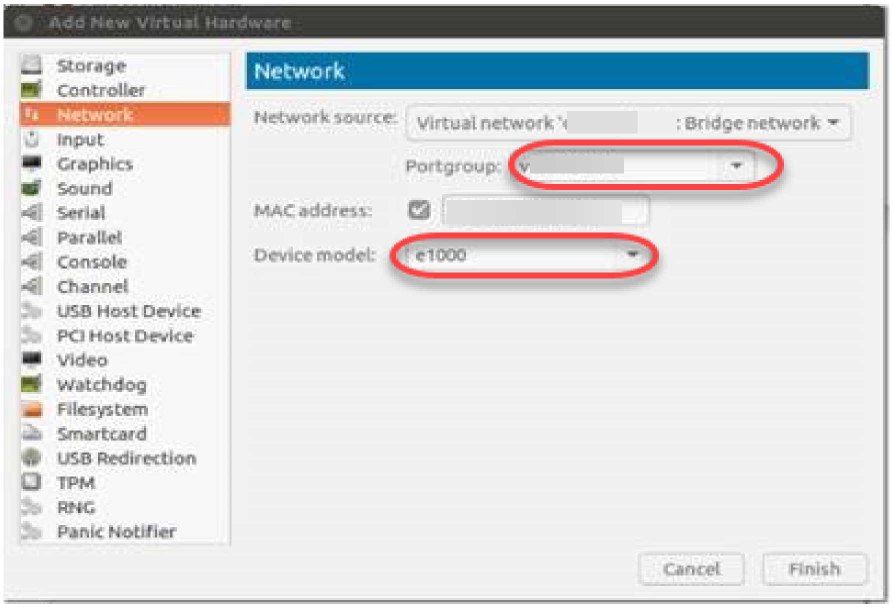
MAC address: ☑ [redacted]

Device model: e1000

3. If this is a Flow Sensor, click the Portgroup drop-down list to select an unassigned promiscuous port group you want to monitor.

   Click the Device Model drop-down list to select **e1000**.

   If this is a Data Node, select a network source that will allow for inter-Data Node communication on an isolated LAN, using the configuration that you created in **Configuring an isolated LAN for Data Nodes**.



Network

Network source: Virtual network '[redacted] : Bridge network

Portgroup: v[redacted]

MAC address: ☑ [redacted]

Device model: e1000

4. Click **Finish**.
5. If you need to add another monitoring port, repeat these instructions.
6. After you have added all monitoring ports, click **Begin Installation**.

4. Configuring your Environment using First Time Setup

After you install the Stealthwatch VE appliances using VMware or KVM, you are ready to configure the basic virtual environment for them.

Select the procedure for your appliance:

- **Configuring a Stealthwatch Management Console or Flow Collector**
- **Configuring a Data Node**
- **Configuring a Flow Sensor or UDP Director**

Configuring a Stealthwatch Management Console or Flow Collector

1. Connect to your Hypervisor host (virtual machine host).
2. In the Hypervisor host, locate your virtual machine.
3. Confirm the virtual machine is powered on.

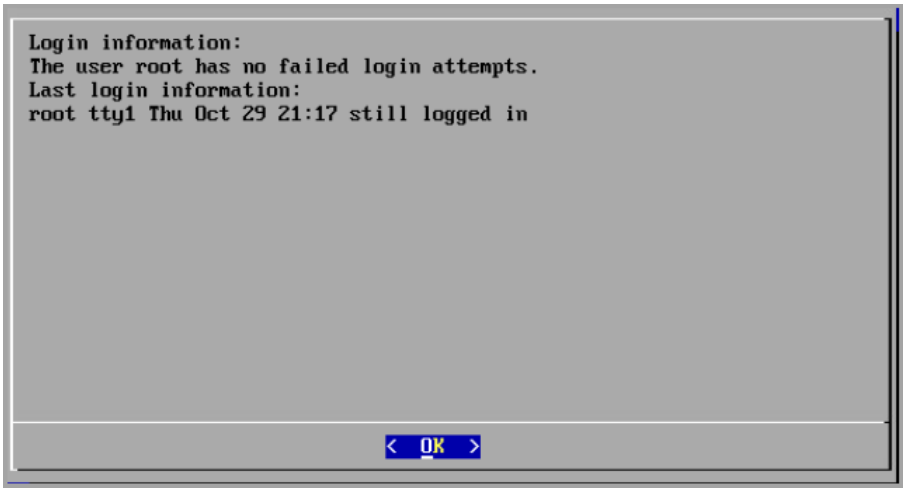
   If the virtual machine does not power on, and you receive an error message about insufficient available memory, do one of the following:

   - **Resources:** Increase the available resources on the system where the appliance is installed. Refer to **Resource Requirements** section for details.
   - **VMware Environment:** Increase the memory reservation limit for the appliance and its resource pool.

> Review **Resource Requirements** to allocate sufficient resources. This step is critical for system performance.
>
> ⚠ If you choose to deploy Cisco Stealthwatch appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.

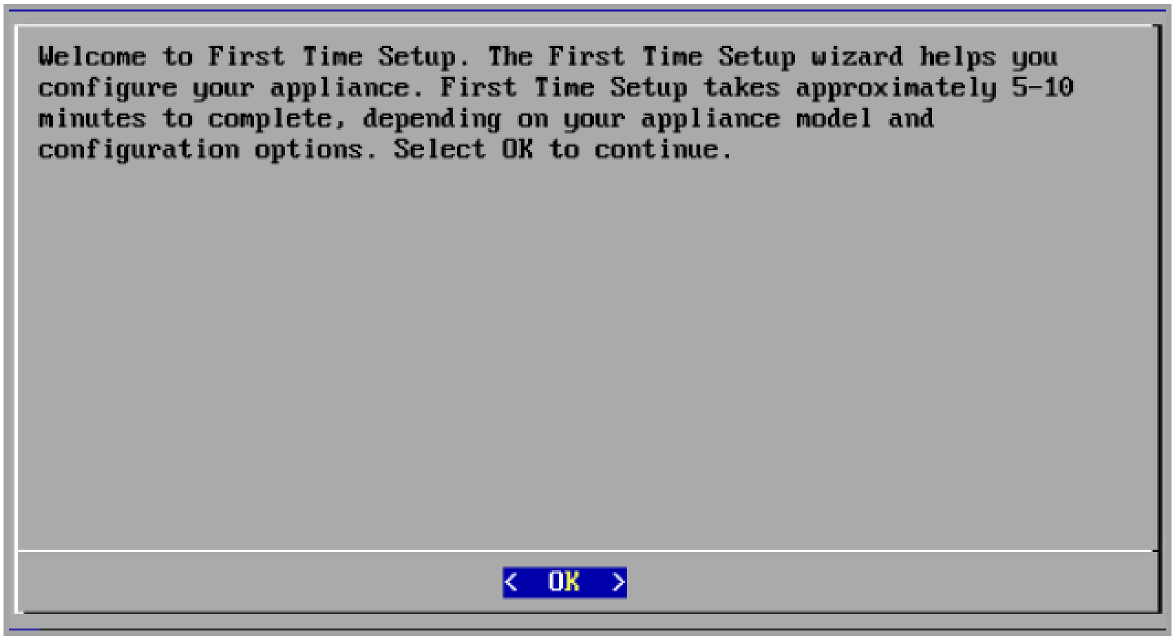
4. Access the virtual machine console. Allow the virtual appliance to finish booting up.

5. Log in through the console.
   - **Login:** root
   - **Default Password:** lan1cope
   - You will change the default password when you configure the system.
6. At the command prompt, type `SystemConfig`. Press Enter.
7. Review the failed login attempts information. Select **OK** to continue.



```
Login information:
The user root has no failed login attempts.
Last login information:
root tty1 Thu Oct 29 21:17 still logged in
```

8. Review the First Time Setup introduction. Select **OK** to continue.

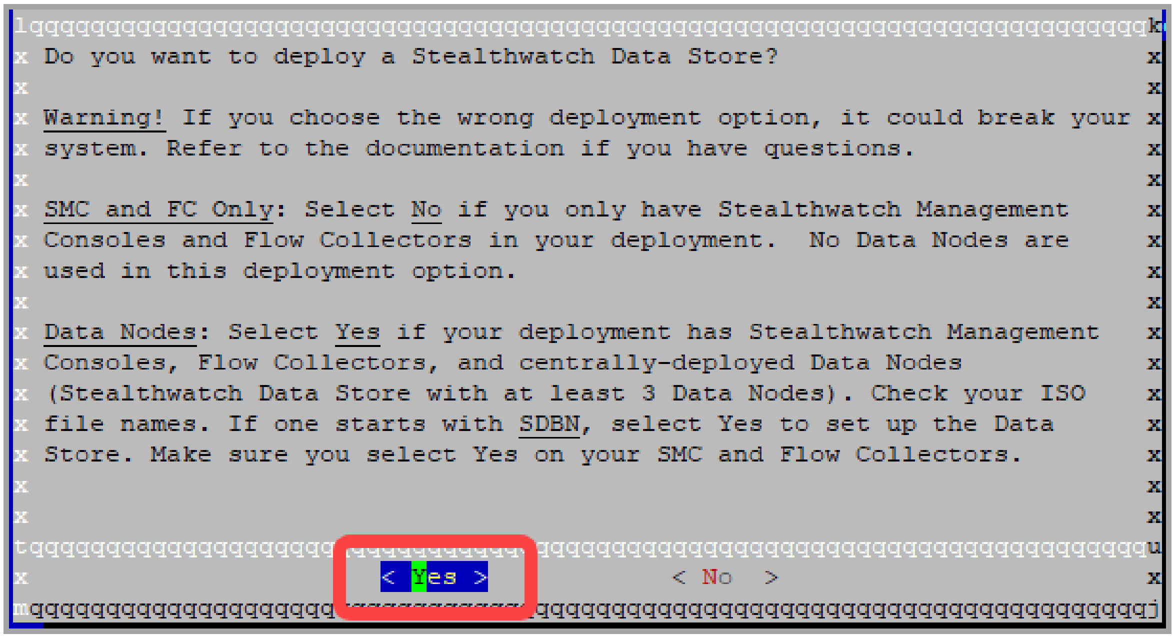


Welcome to First Time Setup. The First Time Setup wizard helps you configure your appliance. First Time Setup takes approximately 5-10 minutes to complete, depending on your appliance model and configuration options. Select OK to continue.

9. **Do you want to deploy a Data Store?** Select **Yes**.

   SMC and Flow Collectors: Make sure you select **Yes** on your SMCs and Flow Collectors.

> After you choose to configure your SMC or Flow Collector for use with Data Store, you cannot change this configuration. Select Yes **only if** you plan to deploy a Data Store to your network.
>
> If you select the wrong choice, deploy a new virtual appliance or RFD your virtual appliance.



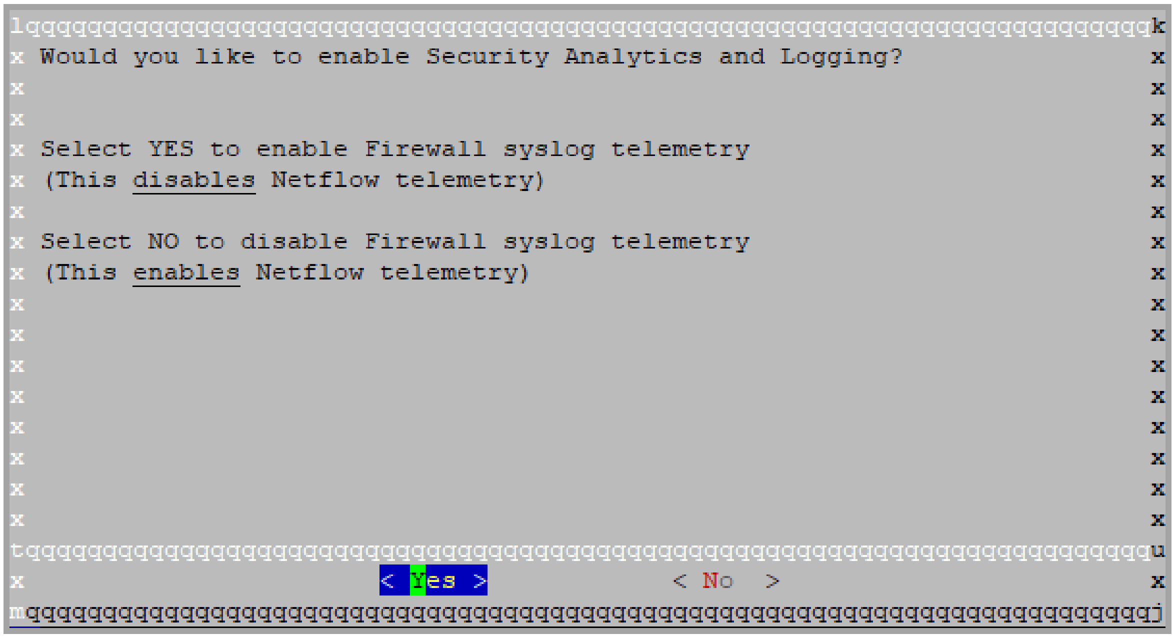
```
Do you want to deploy a Stealthwatch Data Store?

Warning! If you choose the wrong deployment option, it could break your
system. Refer to the documentation if you have questions.

SMC and FC Only: Select No if you only have Stealthwatch Management
Consoles and Flow Collectors in your deployment.  No Data Nodes are
used in this deployment option.

Data Nodes: Select Yes if your deployment has Stealthwatch Management
Consoles, Flow Collectors, and centrally-deployed Data Nodes
(Stealthwatch Data Store with at least 3 Data Nodes). Check your ISO
file names. If one starts with SDBN, select Yes to set up the Data
Store. Make sure you select Yes on your SMC and Flow Collectors.
```

10. **Do you want to enable Security Analytics and Logging?** Select **Yes** or **No**.

    More Information: If you enable Security Analytics and Logging (OP), you will use your Stealthwatch deployment to store Firepower event information. Note that this disables NetFlow collection on your Flow Collector.

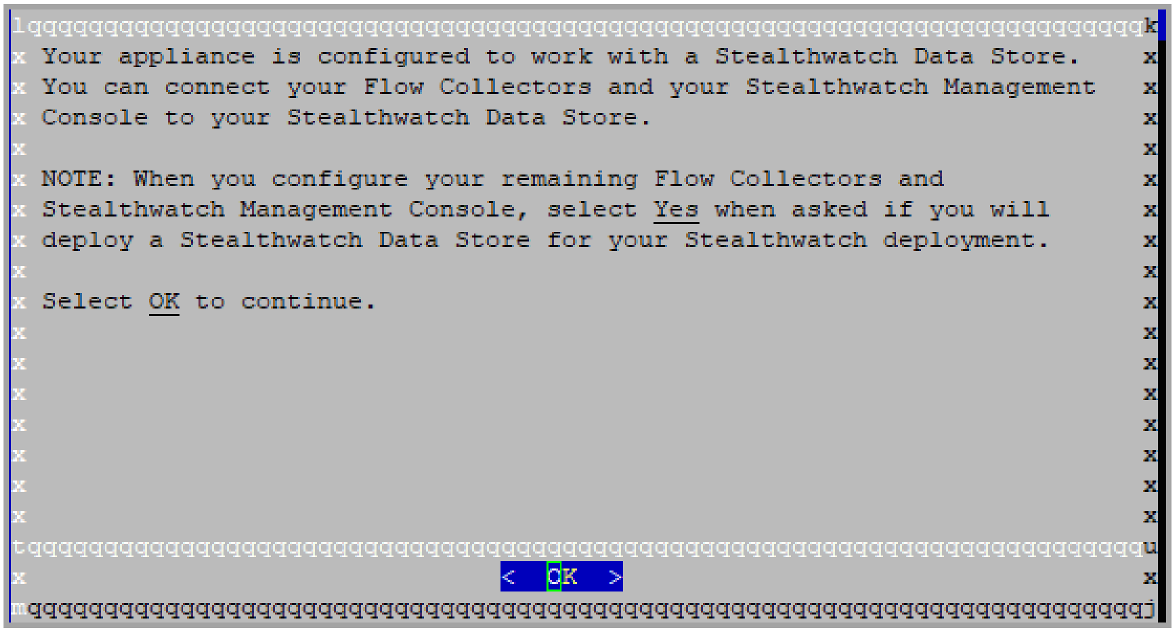
    - **SMC and Flow Collectors:** If you enable Security Analytics and Logging on your SMC, you must enable SAL on the Flow Collector.
    - **Guide:** Refer to the Security Analytics and Logging: Firepower Event Integration Guide for more information.
    - **App Requirement:** If you configure Security Analytics and Logging On Prem, install the Security Analytics and Logging On Prem app on your Stealthwatch Management Console.

> ⚠ After you choose to configure your SMC or Flow Collector for use with Security Analytics and Logging On Prem, you cannot change this configuration. Select Yes **only if** you plan to use Stealthwatch for Security Analytics and Logging On Prem to store your Firepower event information.
>
> If you select the wrong choice, deploy a new virtual appliance or RFD your virtual appliance.



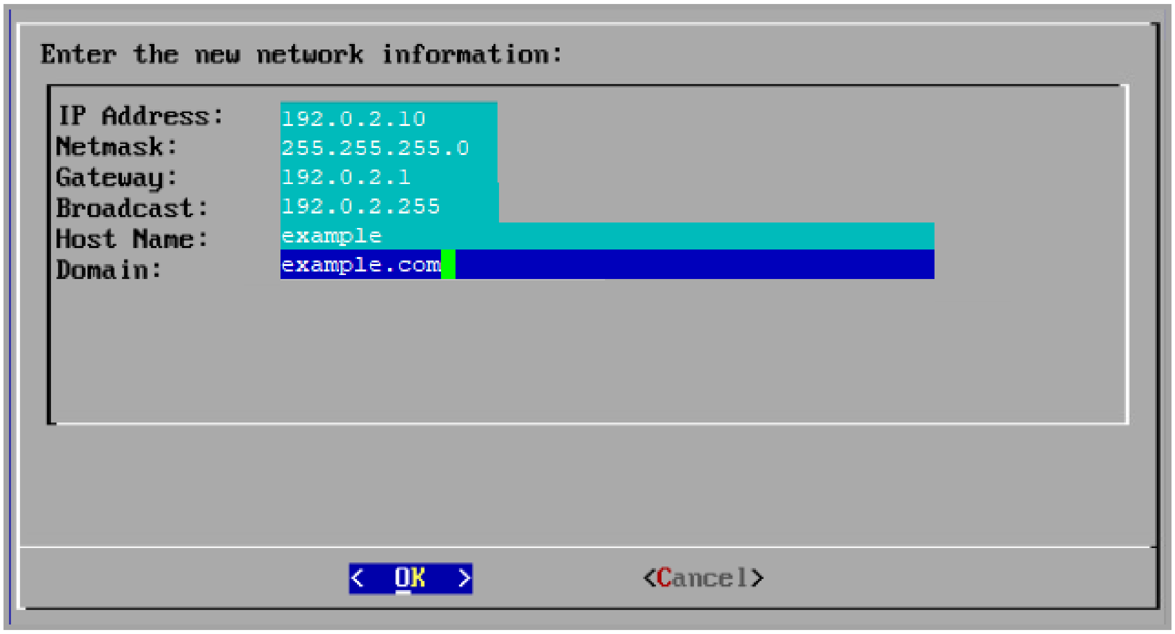
```
 Would you like to enable Security Analytics and Logging?


 Select YES to enable Firewall syslog telemetry
 (This disables Netflow telemetry)

 Select NO to disable Firewall syslog telemetry
 (This enables Netflow telemetry)

                         < Yes >                  < No  >
```

11. Select **OK** to confirm your selection.



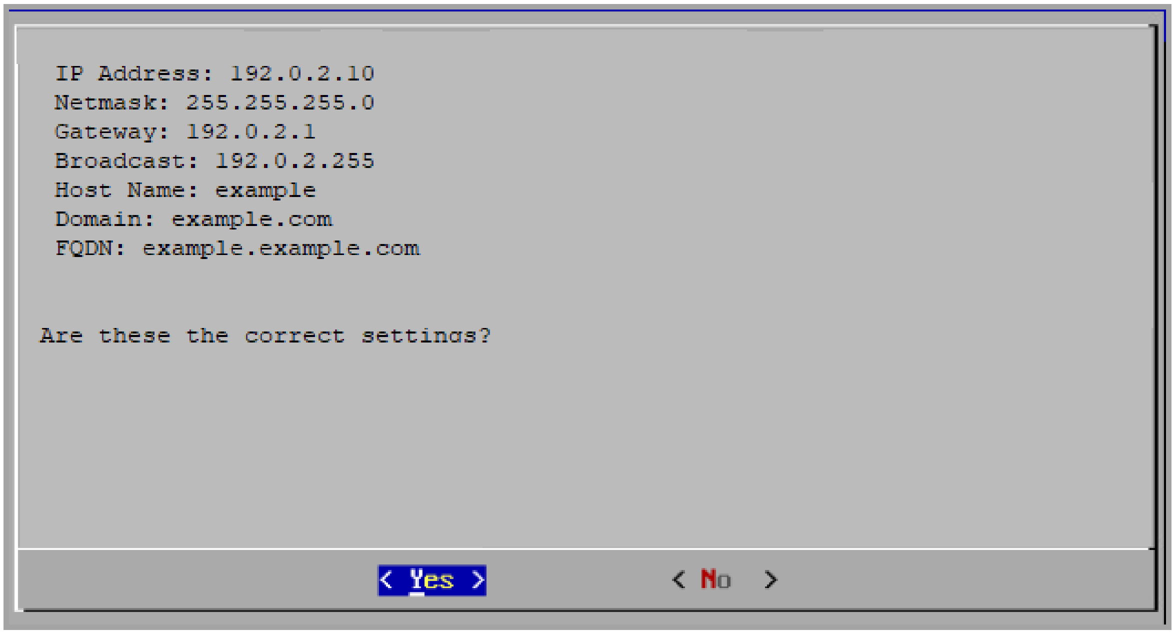
```
Your appliance is configured to work with a Stealthwatch Data Store.
You can connect your Flow Collectors and your Stealthwatch Management
Console to your Stealthwatch Data Store.

NOTE: When you configure your remaining Flow Collectors and
Stealthwatch Management Console, select Yes when asked if you will
deploy a Stealthwatch Data Store for your Stealthwatch deployment.

Select OK to continue.
```

12. Enter the management interface **IP Address**, **Netmask**, **Gateway**, **Broadcast**, **Host Name**, and **Domain**, then select **OK** to continue.



```
Enter the new network information:

 IP Address:    192.0.2.10
 Netmask:       255.255.255.0
 Gateway:       192.0.2.1
 Broadcast:     192.0.2.255
 Host Name:     example
 Domain:        example.com
```

13. Confirm your settings. Select **Yes** to continue.



```
  IP Address: 192.0.2.10
  Netmask: 255.255.255.0
  Gateway: 192.0.2.1
  Broadcast: 192.0.2.255
  Host Name: example
  Domain: example.com
  FQDN: example.example.com


 Are these the correct settings?
```

14. Select **OK** to confirm your selection. Follow the on-screen prompts to finish the virtual environment and restart the appliance.

15. Press **Ctrl + Alt** to exit the console.

16. Repeat all the steps in **4. Configuring your Environment using First Time Setup** for the next SMC or Flow Collector in your system.

    If you've configured all SMCs and Flow Collectors in First Time Setup, go to **Configuring a Data Node**.

Configuring a Data Node

1. Connect to your Hypervisor host (virtual machine host).
2. In the Hypervisor host, locate your virtual machine.
3. Confirm the virtual machine is powered on.

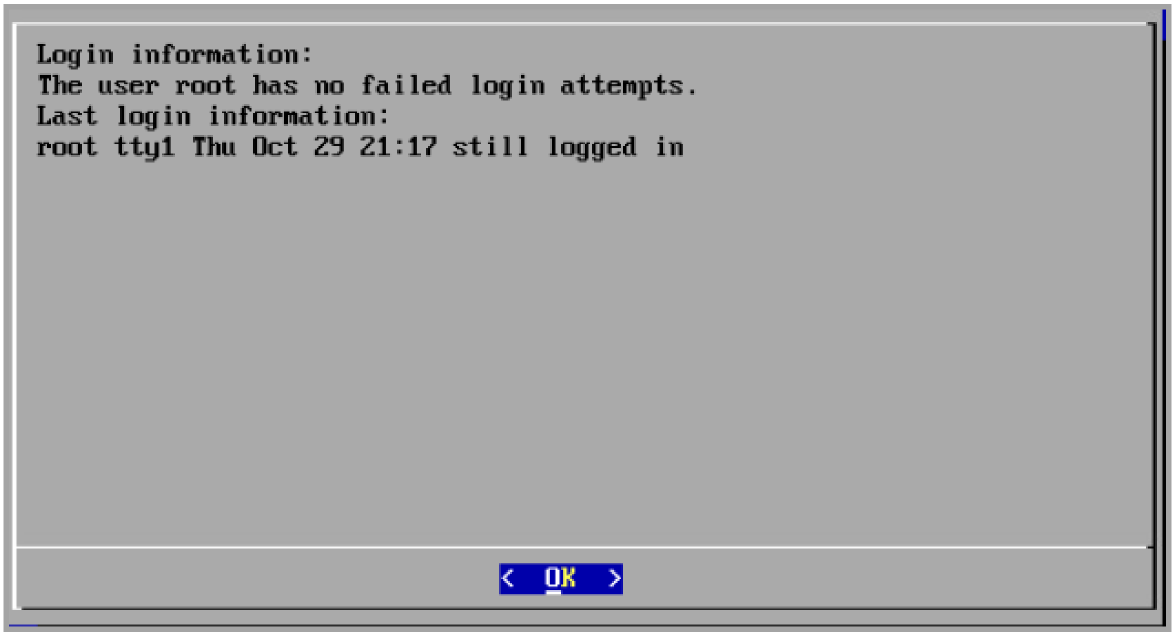
    If the virtual machine does not power on, and you receive an error message about insufficient available memory, do one of the following:

    - **Resources:** Increase the available resources on the system where the appliance is installed. Refer to **Resource Requirements** section for details.
    - **VMware Environment:** Increase the memory reservation limit for the appliance and its resource pool.

Review **Resource Requirements** to allocate sufficient resources. This step is critical for system performance.

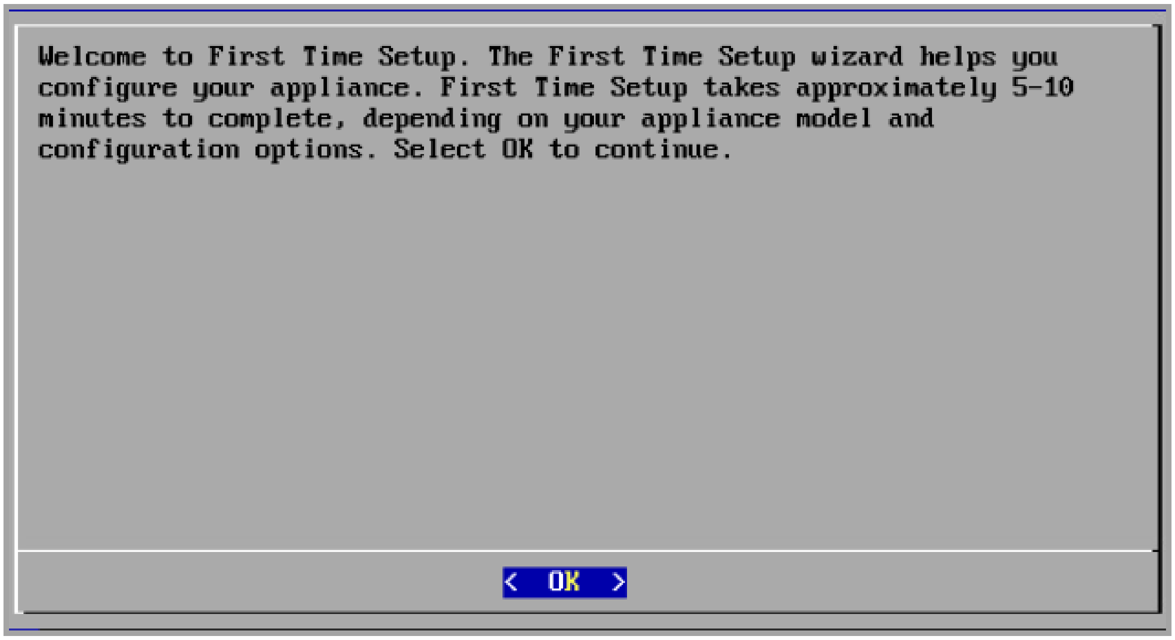
⚠ If you choose to deploy Cisco Stealthwatch appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.

4. Access the virtual machine console. Allow the virtual appliance to finish booting up.
5. Log in through the console.
    - **Login:** root
    - **Default Password:** lan1cope
    - You will change the default password when you configure the system.
6. At the command prompt, type `SystemConfig`. Press Enter.
7. Review the failed login attempts information. Select **OK** to continue.



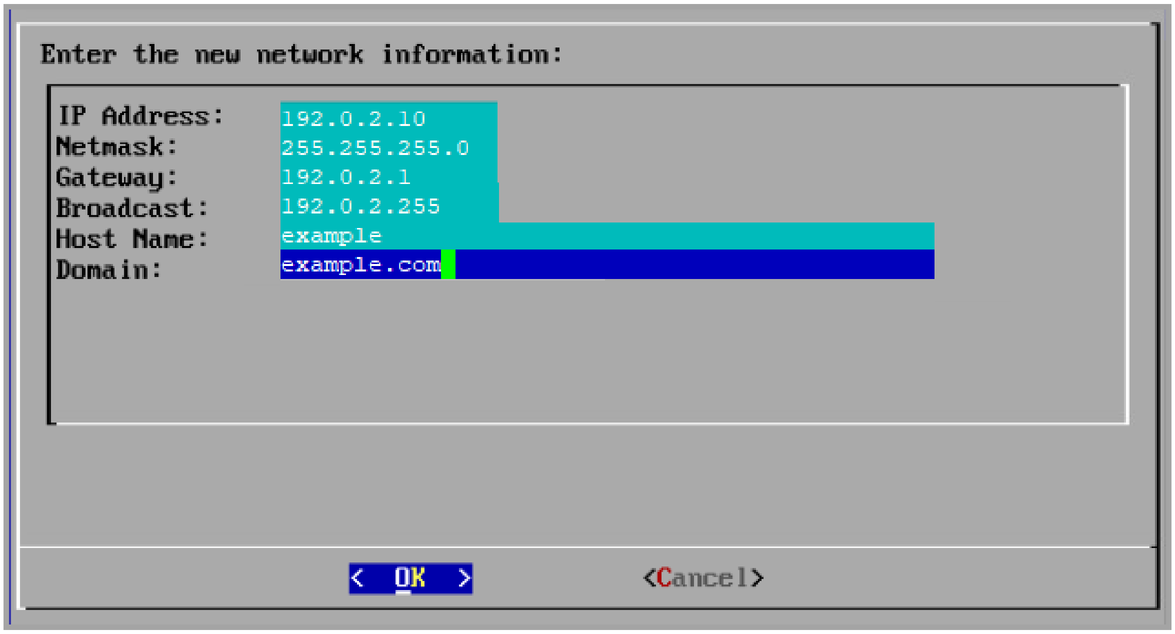
```
Login information:
The user root has no failed login attempts.
Last login information:
root tty1 Thu Oct 29 21:17 still logged in
```

8. Review the First Time Setup introduction. Select **OK** to continue.



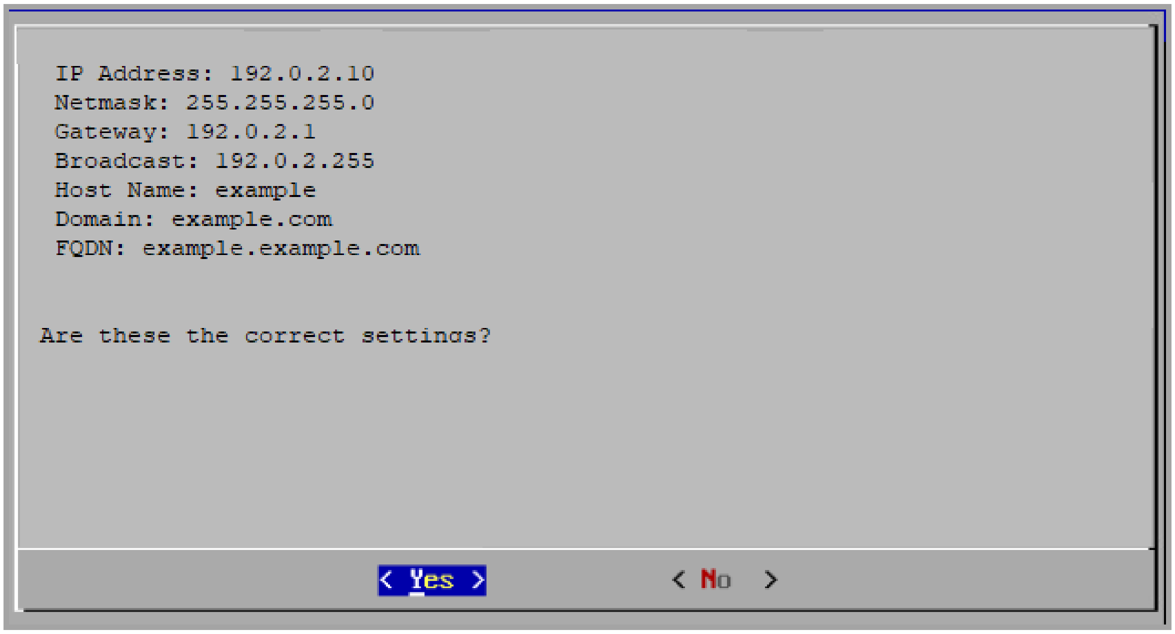
```
Welcome to First Time Setup. The First Time Setup wizard helps you
configure your appliance. First Time Setup takes approximately 5-10
minutes to complete, depending on your appliance model and
configuration options. Select OK to continue.
```

9. Enter the management interface **IP Address**, **Netmask**, **Gateway**, **Broadcast**, **Host Name**, and **Domain**, then select **OK** to continue.



```
Enter the new network information:

IP Address:      192.0.2.10
Netmask:         255.255.255.0
Gateway:         192.0.2.1
Broadcast:       192.0.2.255
Host Name:       example
Domain:          example.com
```

10. Confirm your settings. Select **Yes** to continue.

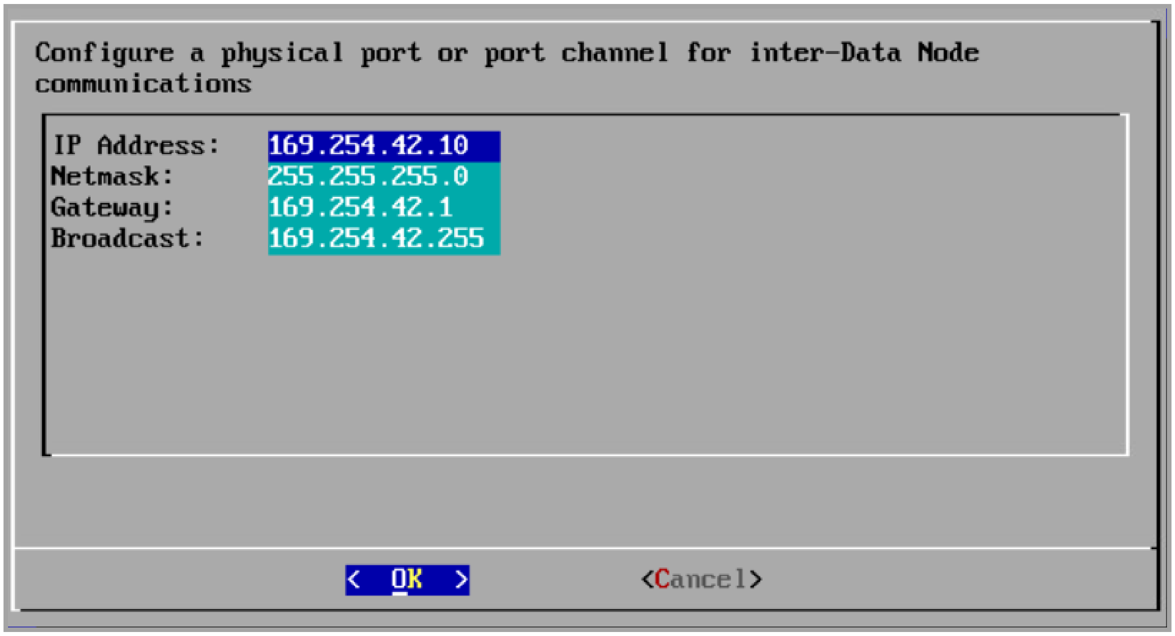


```
  IP Address: 192.0.2.10
  Netmask: 255.255.255.0
  Gateway: 192.0.2.1
  Broadcast: 192.0.2.255
  Host Name: example
  Domain: example.com
  FQDN: example.example.com


 Are these the correct settings?
```

11. Select **OK** to confirm your selection. Follow the on-screen prompts.

12. **Configure a physical port or port channel for inter-Data Node communications.** Enter the following:

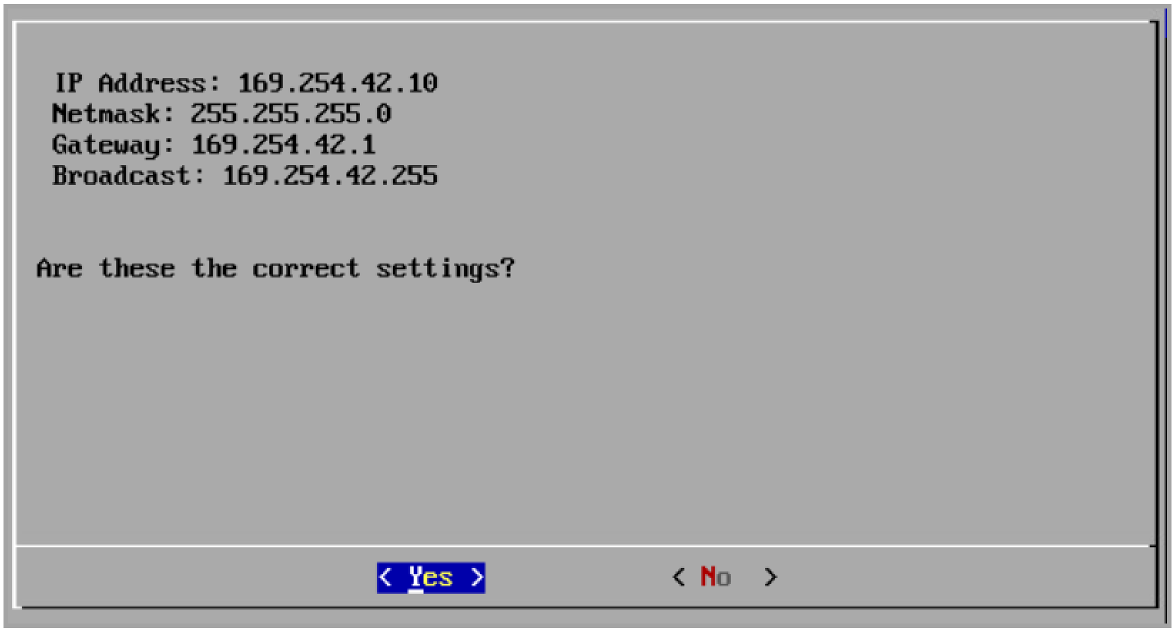
    - **IP Address:** `eth1` interface for inter-Data Node communications with a non-routable **IP Address** from the 169.254.42.0/24 CIDR block, between 169.254.42.2 and 169.254.42.254. For ease of maintenance, select sequential IP addresses (such as 169.254.42.10, 169.254.42.20, and 169.254.42.30).
    - **Netmask**: 255.255.255.0
    - **Gateway**: 169.254.42.1
    - **Broadcast**: 169.254.42.255



```
Configure a physical port or port channel for inter-Data Node
communications

IP Address:     169.254.42.10
Netmask:        255.255.255.0
Gateway:        169.254.42.1
Broadcast:      169.254.42.255
```

13. Select **OK** to continue.

14. Confirm your settings. Select **Yes** to continue.



```
IP Address: 169.254.42.10
Netmask: 255.255.255.0
Gateway: 169.254.42.1
Broadcast: 169.254.42.255


Are these the correct settings?
```

15. Follow the on-screen prompts to finish the virtual environment and restart the appliance.

16. Press **Ctrl + Alt** to exit the console.

17. Repeat all the steps in **Configuring a Data Node** for the next Data Node in your system.

    - If you've configured all Data Nodes in First Time Setup, go to **Configuring a Flow Sensor or UDP Director**.
    - If you've configured all your virtual appliances in First Time Setup, go to **5. Configuring your Stealthwatch System**.

Configuring a Flow Sensor or UDP Director

1. Connect to your Hypervisor host (virtual machine host).
2. In the Hypervisor host, locate your virtual machine.
3. Confirm the virtual machine is powered on.

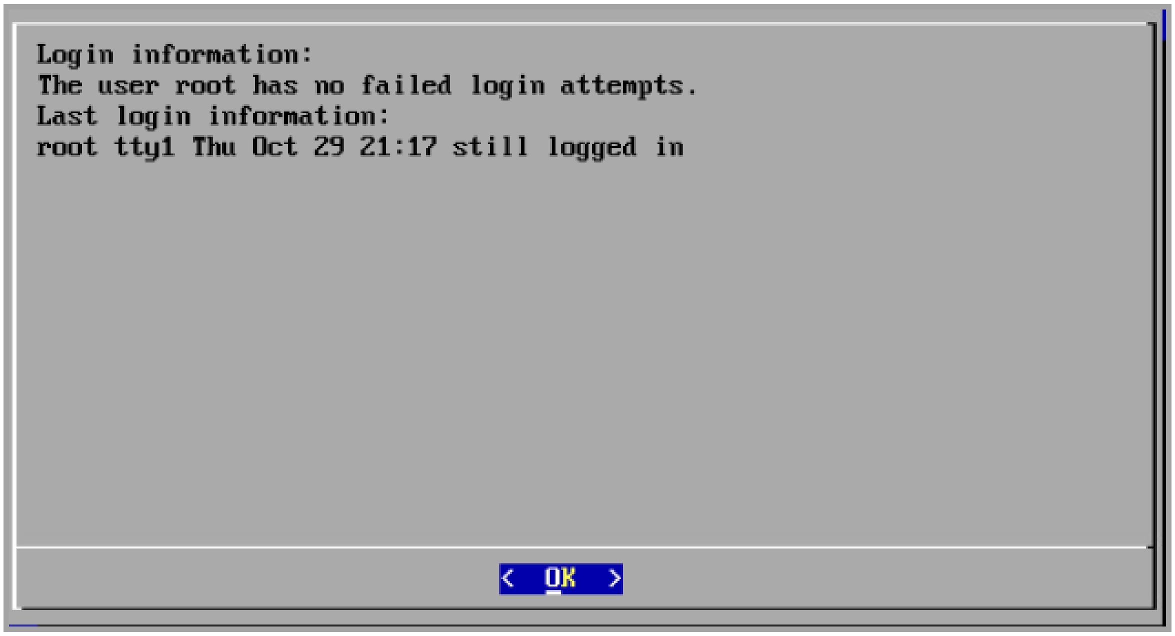
   If the virtual machine does not power on, and you receive an error message about insufficient available memory, do one of the following:

   - **Resources:** Increase the available resources on the system where the appliance is installed. Refer to **Resource Requirements** section for details.
   - **VMware Environment:** Increase the memory reservation limit for the appliance and its resource pool.

> Review **Resource Requirements** to allocate sufficient resources. This step is critical for system performance.
>
> ⚠ If you choose to deploy Cisco Stealthwatch appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.

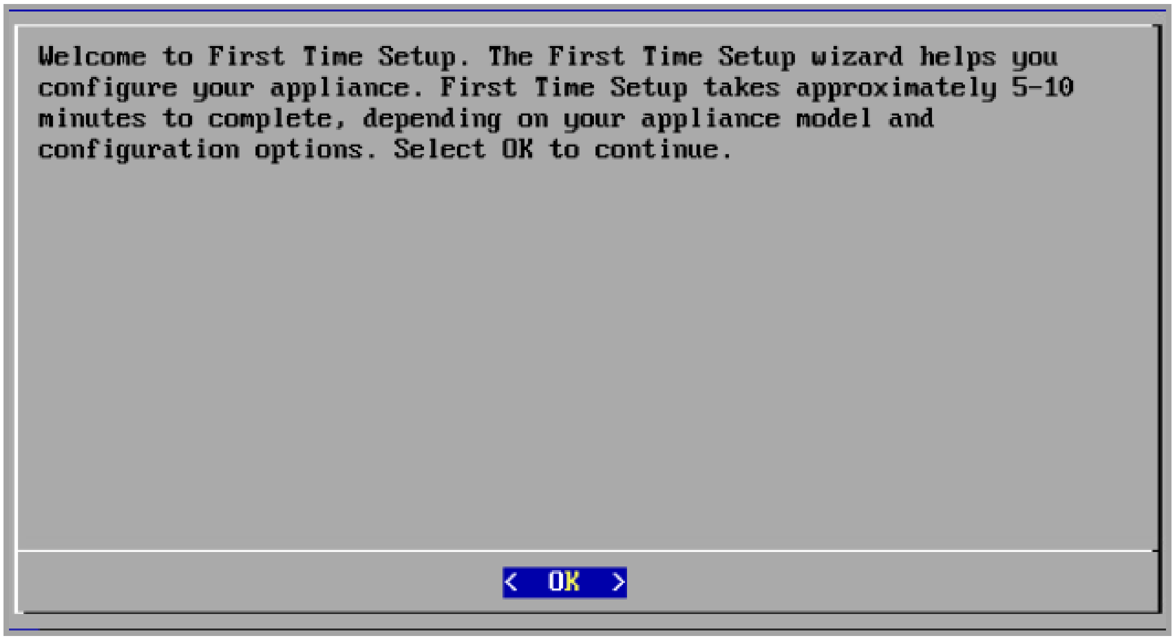
4. Access the virtual machine console. Allow the virtual appliance to finish booting up.
5. Log in through the console.
   - **Login:** root
   - **Default Password:** lan1cope
   - You will change the default password when you configure the system.
6. At the command prompt, type `SystemConfig`. Press Enter.

7. Review the failed login attempts information. Select **OK** to continue.



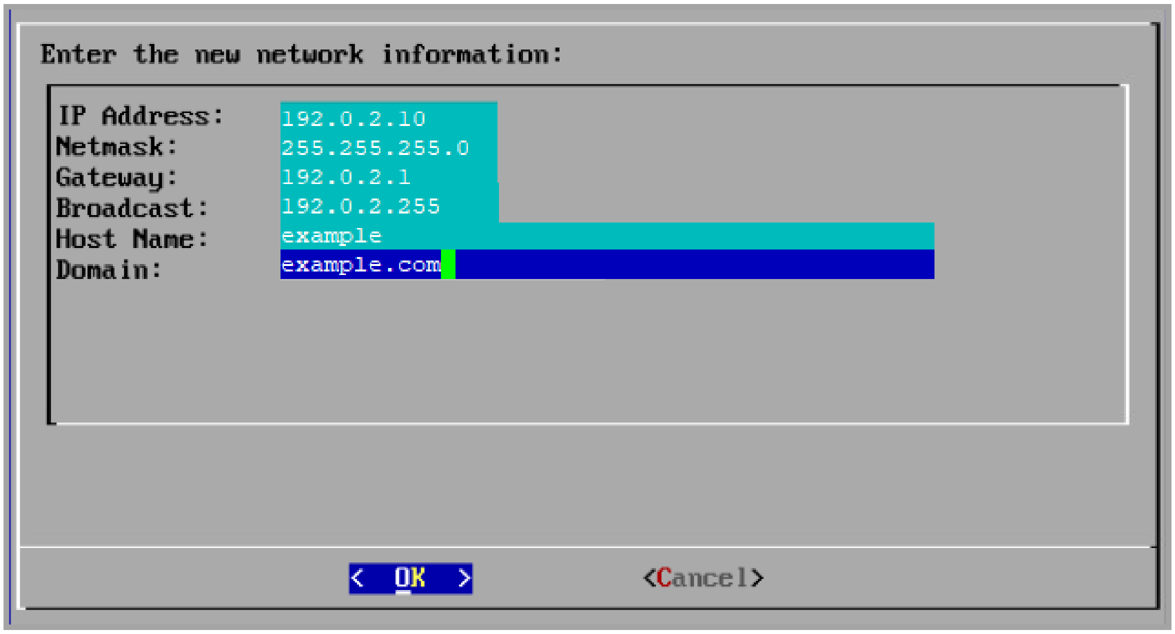
```
Login information:
The user root has no failed login attempts.
Last login information:
root tty1 Thu Oct 29 21:17 still logged in
```

8. Review the First Time Setup introduction. Select **OK** to continue.



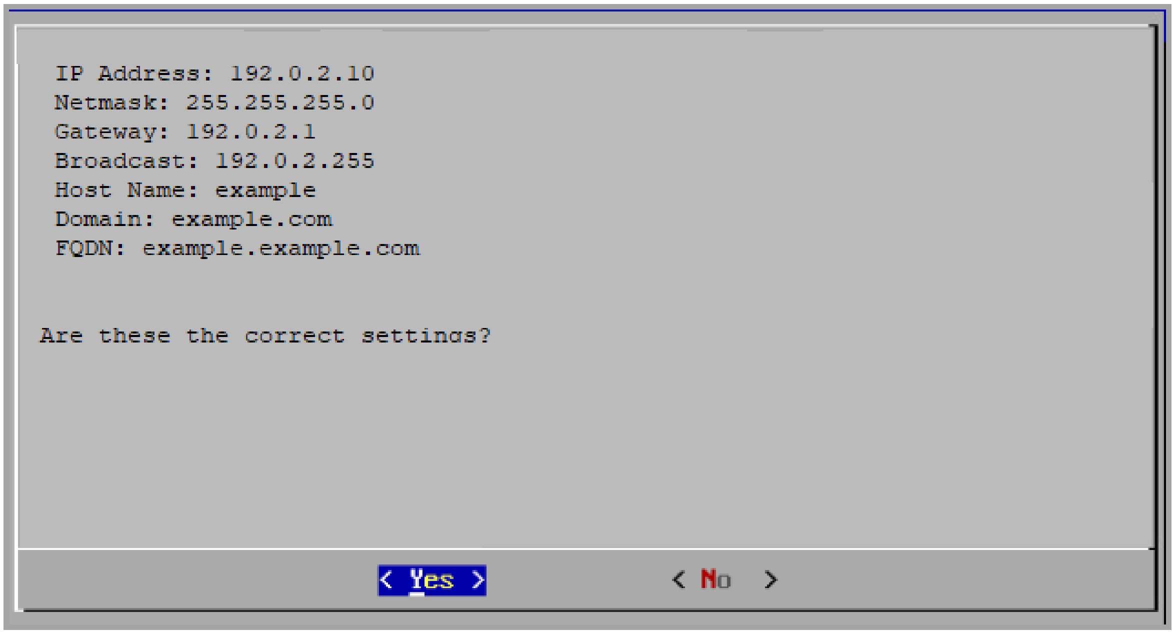
```
Welcome to First Time Setup. The First Time Setup wizard helps you
configure your appliance. First Time Setup takes approximately 5-10
minutes to complete, depending on your appliance model and
configuration options. Select OK to continue.
```

9. Enter the management interface **IP Address**, **Netmask**, **Gateway**, **Broadcast**, **Host Name**, and **Domain**, then select **OK** to continue.



```
Enter the new network information:

 IP Address:      192.0.2.10
 Netmask:         255.255.255.0
 Gateway:         192.0.2.1
 Broadcast:       192.0.2.255
 Host Name:       example
 Domain:          example.com
```

10. Confirm your settings. Select **Yes** to continue.



```
  IP Address: 192.0.2.10
  Netmask: 255.255.255.0
  Gateway: 192.0.2.1
  Broadcast: 192.0.2.255
  Host Name: example
  Domain: example.com
  FQDN: example.example.com


 Are these the correct settings?
```

11. Select **OK** to confirm your selection. Follow the on-screen prompts to finish the virtual environment and restart the appliance.

12. Press **Ctrl + Alt** to exit the console.

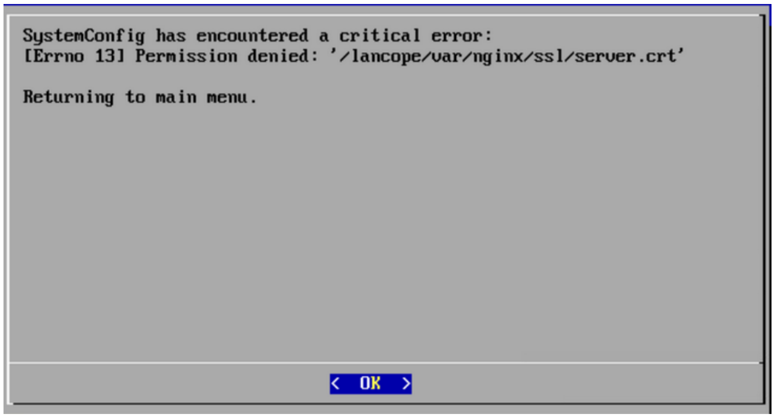
13. Repeat all the steps in **4. Configuring your Environment using First Time Setup** for the next virtual appliance in your system.

If you've configured all your virtual appliances in First Time Setup, go to **5. Configuring your Stealthwatch System**.

Troubleshooting

Certificate Error

If your VM environment usage is high, there may be a timing error and some events occur out of order. If you receive the following error that permission is denied due to a certificate error **(.crt)**, do the following:



```
SystemConfig has encountered a critical error:
[Errno 13] Permission denied: '/lancope/var/nginx/ssl/server.crt'

Returning to main menu.
```

1. Log in to the appliance console as **sysadmin**. The default password is lan1cope.

   You will change the default password when you configure the system. For more information, refer to the Stealthwatch System Configuration Guide.

2. Run the following command:

   ```
   /lancope/admin/plugins/update/.98-FIX-SECRET-PERMS.sh
   ```

3. Run `SystemConfig`.
4. Return to **4. Configuring your Environment using First Time Setup** (starting at step 5) and complete all steps in the section. If you cannot access the appliance, please contact Cisco Stealthwatch Support.

Accessing the Appliance

If you cannot access the appliance after it restarts, do the following:

1. Log in as root.
2. Run the following commands and confirm the docker containers and services are up and running:

- `docker ps`
- `systemctl list-units --failed`
- `systemd-analyze critical chain`

3. Once all docker containers and services are up and running, try the login again. If you cannot access the appliance, please contact Cisco Stealthwatch Support.

5. Configuring your Stealthwatch System

As you deploy your SMC VE, Data Nodes VE, and Flow Collectors VE, configure that appliance using the Stealthwatch System Configuration Guide v7.3.2 and note the following:

- **Certificates:** Appliances are installed with a unique, self-signed appliance identity certificate.
- **Central Management:** Use the primary SMC/Central Manager to manage your appliances and change configuration settings.

Make sure that each appliance is Up in Central Management before continuing to the next appliance. After the SMC VE, Data Nodes VE, and Flow Collectors VE are deployed and configured in Stealthwatch, use the Data Store Virtual Edition Deployment and Configuration Guide to initialize the Data Store and configure flow interface statistics data retention.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Stealthwatch Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Copyright Information