UDP Director Virtual Edition
Installation and Configuration Guide
(for Stealthwatch System v6.10.1)
Copyrights and Trademarks

© 2019 Cisco Systems, Inc. All rights reserved.

NOTICE

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
CONTENTS

Contents .................................................................................................................................................. iii
Introduction .................................................................................................................................................. 1
  Overview .................................................................................................................................................... 1
  Audience ................................................................................................................................................... 1
  About the UDP Director VE .................................................................................................................. 1
  Before You Begin ...................................................................................................................................... 2
  Data Storage ........................................................................................................................................... 3
  How to Use This Guide ............................................................................................................................. 5
  Contacting Support .................................................................................................................................. 6
Installing a Virtual Appliance .................................................................................................................... 7
  Overview ................................................................................................................................................... 7
  Process Overview ....................................................................................................................................... 7
  Configuring Your Firewall for Communications ..................................................................................... 8
  Communication Ports ............................................................................................................................... 8
Installing a Virtual Appliance using VMware vSphere Client ..................................................................... 12
  Overview .................................................................................................................................................. 12
  Before You Begin ....................................................................................................................................... 12
  Process Overview ....................................................................................................................................... 12
  Logging in to the VMware vSphere Client ............................................................................................... 13
  Installing the Virtual Appliance ................................................................................................................ 13
Installing a Virtual Appliance on a KVM Host ........................................................................................... 22
  Overview ................................................................................................................................................... 22
  Before You Begin ....................................................................................................................................... 22
  Process Overview ....................................................................................................................................... 22
  Installing a Virtual Appliance on a KVM Host .......................................................................................... 22

© 2019 Cisco Systems, Inc. All Rights Reserved.
Configuring the Virtual Environment .................................................................................... 29
  Overview ............................................................................................................................ 29
  Configure the IP Addresses ............................................................................................... 29
  Change the Default User Passwords .................................................................................. 33
     Changing the sysadmin Password .................................................................................. 33
     Changing the root Password ........................................................................................ 35
Configuring a Virtual Appliance .......................................................................................... 39
  Overview ............................................................................................................................ 39
  Process Overview ............................................................................................................. 39
  Configuring the Individual Appliances .............................................................................. 39
  Configuring the UDP Director from the SMC .................................................................. 44
     Creating a Management Channel .................................................................................... 45
     Adding a UDP Director .................................................................................................. 45
     Configuring Forward Rules ............................................................................................ 46
  Configuration through the Appliance Admin Interface ..................................................... 48
     Log in to the Appliance Administration Interface ......................................................... 49
     Configure the System Time ............................................................................................ 51
     Configure the UDP Director VE Rules ......................................................................... 53
     Restart the Virtual Appliance ........................................................................................ 54
INTRODUCTION

Overview

This is an installation and configuration guide for the UDP Director VE in a network.

For Stealthwatch System physical appliances, see the Stealthwatch System Hardware Installation Guide and the Stealthwatch System Hardware Configuration Guide.

Read this chapter to learn more about this guide and how to contact Support, if needed. This chapter includes the following sections:

- Audience
- About the UDP Director VE
- Before You Begin
- How to Use This Guide
- Resource Requirements

Audience

The primary audience for this guide is administrators who need to install and configure Stealthwatch UDP Director VE appliances. This guide assumes the audience has a basic familiarity with VMware or KVM.

About the UDP Director VE

The UDP Director VE is a virtual appliance that serves as a central collector for flow data generated by flow-enabled devices.

The Stealthwatch UDP Director VE is a high-speed, high-performance UDP packet replicator. The UDP Director VE is very helpful in redistributing NetFlow, sFlow, syslog, or Simple Network Management Protocol (SNMP) traps to various collectors.

As it receives UDP packets from multiple sources, the UDP Director VE aggregates the information into a single data stream. It then modifies the packets to appear as though they came from the original source, and sends the data to multiple destinations. Network and security administrators define the rules by which aggregated information is collected and distributed, based on source IP, destination IP, and destination port.
Before You Begin

Use the information in this section to prepare for installing and configuring the Stealthwatch VE appliances. Note that the configuration is a two-part process using first the VMware vSphere client interface or KVM interface, and then the Appliance Administration (Admin) interface.

Compatibility

You can use VMware or KVM (Kernel-based Virtual Machine) for the virtual appliance installation. It is important to review the following compatibility information:

VMware

- **Compatibility**: VMware vSphere v5.5 or 6.0
- **VMware Upgrades**: Stealthwatch VE appliances that are running on older versions of VMware ESX are not compatible with ESX v5.5 or 6.0. If you upgrade VMware to ESX v5.5 or 6.0, delete your existing Stealthwatch VE appliances and reinstall them.
- **Live migration** (for example, with vMotion) from host to host is not supported.
- **Virtual machine snapshots** are not supported.

**CAUTION!** 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 Using 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
  - qemu-KVM 2.8.0
  - Open vSwitch 2.6.1
  - Linux Kernel 4.4.38

- **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.

  **Note**: The system performance is determined by the host environment. Your performance may vary.

Installation Order

It is important to install and configure your virtual appliances in the following order:
1. UDP Director
2. Flow Collector Database 5000 Console (if used)
3. All other Flow Collectors
4. All Flow Sensors
5. Cloud License Concentrator
6. Endpoint Concentrator
7. Secondary Stealthwatch Management Console
8. Primary Stealthwatch Management Console

If you do not follow this recommended order when you set up the Stealthwatch system, the system may not properly collect data from the appliances and you will have to set up each one separately.

**CAUTION!** Be sure the time setting on the virtual host server (where you will be installing the virtual appliances) reflects the correct time. Otherwise, the appliances may not be able to boot up.

**Downloading the VE Software**

Before you can complete the procedures in this guide, you must obtain the appliance installation file (OVF or ISO) from the Download and License Center. For instructions on downloading the file for each appliance, see the *Downloading and Licensing Stealthwatch Products* document in the Download and License Center or on Cisco.com.

**Registering and Licensing**

As part of the configuration process, you will register and license your Stealthwatch products. For instructions, see the *Downloading and Licensing Stealthwatch Products* document in the Download and License Center or on Cisco.com.

**Resource Requirements**

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

**Data Storage**

During installation, you will expand the available data storage on the server. Use the following information to allocate the correct amount of storage for each appliance.

- **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:** Cisco recommends allocating 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.

- **If the External Event processing (syslog) feature is used,** more memory and processing resources are required.

- **Minimum Data Storage:** Use the following table to determine the minimum data storage required for each appliance.

<table>
<thead>
<tr>
<th>Stealthwatch VE Model</th>
<th>Minimum Data Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stealthwatch Management Console VE</td>
<td>100 GB</td>
</tr>
<tr>
<td>Stealthwatch Management Console VE 2000</td>
<td>200 GB</td>
</tr>
<tr>
<td>Flow Collector NetFlow VE</td>
<td>200 GB</td>
</tr>
<tr>
<td>Flow Collector NetFlow VE 2000</td>
<td>600 GB</td>
</tr>
<tr>
<td>Flow Collector NetFlow VE 4000</td>
<td>1.5 TB</td>
</tr>
<tr>
<td>Flow Collector sFlow VE</td>
<td>100 GB</td>
</tr>
<tr>
<td>Flow Collector sFlow VE 2000</td>
<td>600 GB</td>
</tr>
<tr>
<td>Flow Collector sFlow VE 4000</td>
<td>1.5 TB</td>
</tr>
<tr>
<td>Flow Sensor</td>
<td>50 GB</td>
</tr>
<tr>
<td>UDP Director</td>
<td>50 GB</td>
</tr>
</tbody>
</table>

**UDP Director VE**

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

- 4 GB RAM
- **Data Storage:** see the Data Storage table.

**Note:** Cisco recommends thick provisioning although thin provisioning can be used if disk space is limited.
Information Needed for Console Access

<table>
<thead>
<tr>
<th>Setting</th>
<th>Hypervisor Server</th>
<th>UDP Director VE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login User Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
<td>(Default = 192.168.1.2)</td>
</tr>
<tr>
<td>Netmask IP Address</td>
<td></td>
<td>(Default = 255.255.255.0)</td>
</tr>
<tr>
<td>Gateway IP Address</td>
<td></td>
<td>(Default = 192.168.1.1)</td>
</tr>
</tbody>
</table>

Information Needed for the Appliance Admin Interface

<table>
<thead>
<tr>
<th>Setting</th>
<th>UDP Replicator VE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>(Default = 192.168.1.2)</td>
</tr>
<tr>
<td>Host Name</td>
<td></td>
</tr>
<tr>
<td>Network Domain Name</td>
<td></td>
</tr>
<tr>
<td>NTP Server IP Address(es)</td>
<td></td>
</tr>
<tr>
<td>DNS Server IP Address(es)</td>
<td></td>
</tr>
</tbody>
</table>

How to Use This Guide

In addition to this introduction, we have divided this guide into the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing a Virtual Appliance</td>
<td>How to prepare the virtual environment and install VE appliances</td>
</tr>
<tr>
<td>Configuring the Virtual Environment</td>
<td>How to set up the virtual environment for the appliances</td>
</tr>
<tr>
<td>Configuring a Virtual Appliance System</td>
<td>How to configure appliances to begin processing traffic data</td>
</tr>
</tbody>
</table>

Abbreviations

The following abbreviations may appear in this guide:
<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Domain Name System (Service or Server)</td>
</tr>
<tr>
<td>dvPort</td>
<td>Distributed Virtual Port</td>
</tr>
<tr>
<td>ESX</td>
<td>Enterprise Server X</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>KVM</td>
<td>Kernel-based Virtual Machine</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OVF</td>
<td>Open Virtualization Format</td>
</tr>
<tr>
<td>SMC</td>
<td>Stealthwatch Management Console</td>
</tr>
<tr>
<td>TB</td>
<td>Terabyte</td>
</tr>
<tr>
<td>UUID</td>
<td>Universally Unique Identifier</td>
</tr>
<tr>
<td>VDS</td>
<td>vNetwork Distributed Switch</td>
</tr>
<tr>
<td>VE</td>
<td>Virtual Edition</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
</tbody>
</table>

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 email: tac@cisco.com
  - For phone support: 1-800-553-2447 (U.S.)
INSTALLING A VIRTUAL APPLIANCE

Overview

This chapter describes how to install the virtual appliances.

For instructions on how to install a Stealthwatch physical appliance, see the Stealthwatch System v6.x Hardware Installation Guide.

Compatibility: You can use one of the following for the virtual edition installation. For compatibility details, see the Compatibility section of the Introduction.

- VMware vSphere Client v5.5 or 6.0
- KVM using any Linux distribution

Note: Confirm the time setting on the virtual host server (where you will be installing the virtual appliances) reflects the correct time. Otherwise, the appliances may not be able to boot up.

CAUTION! 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.

Process Overview

Installing a virtual appliance involves completing the following procedures, which we discuss in this chapter:

1. Configuring Your Firewall for Communications
2. Installing a Virtual Appliance using VMware vSphere Client or KVM.
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.

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

Communication Ports

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

<table>
<thead>
<tr>
<th>From (Client)</th>
<th>To (Server)</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin User PC</td>
<td>All appliances</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>All appliances</td>
<td>Network time source</td>
<td>UDP/123</td>
<td>NTP</td>
</tr>
<tr>
<td>Active Directory</td>
<td>SMC</td>
<td>TCP/389, UDP/389</td>
<td>LDAP</td>
</tr>
<tr>
<td>AnyConnect</td>
<td>Endpoint Concentrator</td>
<td>UDP/2055</td>
<td>NetFlow</td>
</tr>
</tbody>
</table>

© 2019 Cisco Systems, Inc. All Rights Reserved.
<table>
<thead>
<tr>
<th>From (Client)</th>
<th>To (Server)</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ISE</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Cisco ISE</td>
<td>SMC</td>
<td>TCP/5222</td>
<td>XMPP</td>
</tr>
<tr>
<td>Endpoint Concentrator</td>
<td>Flow Collector</td>
<td>UDP/2055</td>
<td>NetFlow</td>
</tr>
<tr>
<td>External log sources</td>
<td>SMC</td>
<td>UDP/514</td>
<td>SYSLOG</td>
</tr>
<tr>
<td>Flow Collector</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>SLIC</td>
<td>SMC</td>
<td>TCP/443 or proxied connection</td>
<td>HTTPS</td>
</tr>
<tr>
<td>UDP Director</td>
<td>Flow Collector - sFlow</td>
<td>UDP/6343</td>
<td>sFlow</td>
</tr>
<tr>
<td>UDP Director</td>
<td>Flow Collector - NetFlow</td>
<td>UDP/2055*</td>
<td>NetFlow</td>
</tr>
<tr>
<td>UDP Director</td>
<td>3rd Party event management systems</td>
<td>UDP/514</td>
<td>SYSLOG</td>
</tr>
<tr>
<td>Flow Sensor</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Identity</td>
<td>SMC</td>
<td>TCP/2393</td>
<td>SSL</td>
</tr>
<tr>
<td>NetFlow Exporters</td>
<td>Flow Collector - NetFlow</td>
<td>UDP/2055*</td>
<td>NetFlow</td>
</tr>
<tr>
<td>sFlow Exporters</td>
<td>Flow Collector - sFlow</td>
<td>UDP/6343*</td>
<td>sFlow</td>
</tr>
<tr>
<td>SMC</td>
<td>Cisco ISE</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>SMC</td>
<td>DNS</td>
<td>UDP/53</td>
<td>DNS</td>
</tr>
<tr>
<td>SMC</td>
<td>Flow Collector</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>From (Client)</td>
<td>To (Server)</td>
<td>Port</td>
<td>Protocol</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
<td>----------</td>
</tr>
<tr>
<td>SMC</td>
<td>Flow Sensor</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>SMC</td>
<td>Identity</td>
<td>TCP/2393</td>
<td>SSL</td>
</tr>
<tr>
<td>SMC</td>
<td>Flow Exporters</td>
<td>UDP/161</td>
<td>SNMP</td>
</tr>
<tr>
<td>SMC</td>
<td>Endpoint Concentrator</td>
<td>UDP.2055</td>
<td>HTTPS</td>
</tr>
<tr>
<td>User PC</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>From (Client)</th>
<th>To (Server)</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>All appliances</td>
<td>User PC</td>
<td>TCP/22</td>
<td>SSH</td>
</tr>
<tr>
<td>SMC</td>
<td>3rd Party event management systems</td>
<td>UDP/162</td>
<td>SNMP-trap</td>
</tr>
<tr>
<td>SMC</td>
<td>3rd Party event management systems</td>
<td>UDP/514</td>
<td>SYSLOG</td>
</tr>
<tr>
<td>SMC</td>
<td>Email gateway</td>
<td>TCP/25</td>
<td>SMTP</td>
</tr>
<tr>
<td>SMC</td>
<td>SLIC</td>
<td>TCP/443</td>
<td>SSL</td>
</tr>
<tr>
<td>User PC</td>
<td>All appliances</td>
<td>TCP/22</td>
<td>SSH</td>
</tr>
</tbody>
</table>

The following diagram shows the various connections used by the Stealthwatch System. The ports marked as *optional* may be used according to your own network needs.
Note: Go to the section that is applicable to your virtual appliance installation: VMware vSphere Client or KVM.
INSTALLING A VIRTUAL APPLIANCE USING VMWARE VSphere CLIENT

Overview

This chapter describes how to install the virtual appliances using VMware vsphere Client (v5.5 or 6.0).

Before You Begin

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

1. Download the OVF file from the Download and License Center. See the Downloading and Licensing Guide for instructions.
2. Review the Compatibility information in the Introduction.
3. Configure Your Firewall for Communications.
4. Review the Resource Requirements section to determine the proper allocations for the appliance. You can use a resource pool or alternative method to allocate resources.
5. Confirm the time set on the ESX server (where you will be installing the virtual appliance) reflects the correct time. Otherwise, the virtual appliances may not be able to boot up.

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

CAUTION! 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.

Process Overview

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

1. Logging in to the VMware vsphere Client
2. Installing the Virtual Appliance
Logging in to the VMware vSphere Client

To install the virtual appliance, you must first log in to the VMware vSphere Client (v5.5 or 6.0), by completing the following steps:

**Note:** Whether you are using the The VMware vSphere Client or Web Client interface, some of the graphics and commands may vary from the information shown here. Please see your VMware vSphere guide for details related to the software.

1. Launch the VMware vSphere Client software. The Login dialog opens.

2. Type the IP address of the ESX server and your login credentials.
3. Click **Login**. The Home page opens.

**Note:** The Web Client has two dialogs for the configuration: Select name and location and Configure settings.

Installing the Virtual Appliance

To install a virtual appliance on the ESX server and define the virtual appliance management and monitoring ports, complete the following steps:

1. Locate the virtual appliance software file (OVF.TGZ) that you downloaded from the Download and License Center.
2. Unzip or open the file, and then untar it.
   - To untar the file, select all the files in the folder and extract them.
   - Unzipping TGZ file is a two-step process, and the steps may vary depending on the software you use.
3. On the vSphere client menu, click **File > Deploy OVF Template**.
   **Web Client:** Right-click the host. Select **Deploy OVF Template**.
Note: The Web client OVF template wizard may vary from the images and instructions shown here, but the steps are similar. One example is the Web client uses Source Location instead of Source. The image below shows the steps on the left side for a OVF template ready to deploy:

The Deploy OVF Template wizard opens.
4. Click **Browse**. Navigate to select the virtual appliance OVF file.

5. Click **Next** to display the OVF Template Details page.

   **Web Client**: The 1.b. Review details page opens.
6. Click **Next**. Review the End User License Agreement.

**Web Client:** 1c. Accept EULAs.

7. After reviewing the information, click **Accept**. Click **Next**. The Name and Location page opens.

**Web Client:** 2a. The Name and Location page opens.
8. **Optional**: Change the name and location for the virtual appliance. This should be a unique name and will display in the Inventory tree. Click **Next**.

9. On the Storage page, select where you want to store the data files. Click **Next**.
10. On the Disk Format page, select **Thick Provision Lazy Zeroed** or **Thick Provision Eager Zeroed**. Click **Next**.
   - Use the Thin Provision format only if your disk space is limited.
   - For more information, see your VMware documentation.
11. On the Network Mapping page, select the networks for the virtual appliance. Click **Next**.

**Web Client:** The 2c. Setup Networks page opens.
12. On the Ready to Complete page, review the summary of settings. If they are correct, click Finish.
13. The deployment dialog box opens.

14. When the deployment is completed, click Close. The installed virtual appliance appears in the Inventory tree.

15. Have you completed all of the procedures in this chapter for all of the UDP Directors?
   - If yes, go to Configuring the Virtual Environment
   - If no, repeat all of the procedures in this chapter for the next virtual appliance.
INSTALLING A VIRTUAL APPLIANCE ON A KVM HOST

Overview

This chapter describes how to install the virtual appliances using KVM and Virtual Machine Manager.

Before You Begin

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

1. Download the ISO file from the Download and License Center and copy the image to a folder on the KVM host. In the example given below, the folder is var/lib/libvirt/image. See the Downloading and Licensing Guide for instructions.
2. Review the Compatibility information in the Introduction.
3. Configure Your Firewall for Communications.
4. Review the Resource Requirements section to determine the proper allocations for the appliance.
5. Confirm the time set on the virtual host server (where you will be installing the virtual appliance) reflects the correct time. Otherwise, the virtual appliances may not be able to boot up.

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

Process Overview

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

- Installing a Virtual Appliance on a KVM Host

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 SMC appliance through a GUI tool.
called Virtual Machine Manager running on a Ubuntu box. You can use any compatible Linux distribution. For compatibility details, see the Compatibility section of the Introduction.

To install a virtual appliance, complete the following steps:

1. Use Virtual Machine Manager to connect to the KVM Host.

2. Click File > New Virtual Machine.

3. Select Local install media (ISO image or CDROM), and then click Forward.

4. Click Use ISO image.

5. Click Browse. Select the appliance image.
6. Select the ISO file. Click **Choose Volume**.

   **Note:** Confirm the ISO file is accessible by the KVM Host.

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

10. Click Forward.
11. Select Create a disk image for the virtual machine.
12. Enter the data storage amount shown for the appliance in the Resource Requirements section. Click Forward.
13. Assign a Name for the virtual machine. This will be the display name, so use a name that will help you find it later.

14. Select the **Customize configuration before install** check box.

15. In the Network selection drop-down box, select the applicable network and port group for installation.

16. Click **Finish**. The configuration menu opens.
17. In the navigation pane, select NIC.
18. Under Virtual Network Interface, select e1000 in the Device model drop-down box. Click Apply.
19. Click **VirtIO Disk 1**.

20. In the Advanced Options drop-down list, select **SCSI** in the Disk bus drop-down box. Click **Apply**.

21. Click **Begin Installation**.

22. Go to **Configuring the Virtual Environment**.
CONFIGURING THE VIRTUAL ENVIRONMENT

Overview

After you install the Stealthwatch VE appliances, you are ready to configure the virtual environment for them. This process involves completing the following procedures as detailed in this chapter:

1. Configure the IP Addresses
2. Change the Default User Passwords

Configure the IP Addresses

To configure the IP addresses for a virtual appliance, complete the following steps:

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.

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

- Increase the available resources on the system where the appliance is installed. See the Resource Requirements section for details.
- **ESX server:** Increase the memory reservation limit for the appliance and its resource pool.

4. Access the virtual machine console.
5. Allow the virtual appliance to finish booting up. The virtual appliance Administrative IP Address page opens.
6. Click on the page. Enter the IP address for the virtual appliance.
7. Select OK, and then press Enter. The IP Netmask page opens with the default network mask IP address.

8. Do the following:
   - Accept the default value or enter a new one based on your environment.
   - Select OK and press Enter to continue.

The IP Broadcast Address page opens with the default broadcast IP address.
9. Do the following:
   - Accept the default value or enter a new one based on your environment.
   - Select OK and press Enter to continue.

The Gateway Address page opens with the default gateway server IP address.

10. Do the following:
    - Accept the default value or enter a new one based on your environment.
    - Select OK and press Enter to continue.

A page opens showing a summary of your entries.
11. Review the information. Are the settings correct?
   - If yes, go to the next step.
   - If no, go to step 13.

12. Press Enter. The system restart page opens.

13. Press Enter. The system restarts and implements the changes. On completion, a login prompt appears.

14. Select No and press Enter. The Administrative IP Address page opens. Repeat steps 5 through 10 to make any necessary changes. The system restart page opens.

15. Press Enter. The system restarts and implements the changes. On completion, a login prompt appears.
16. Press **Ctrl + Alt** to exit the console.
17. Go to **Change the Default User Passwords** next in this chapter.

**Change the Default User Passwords**

**Important:** To ensure that your network is secure, you must change the default password for the sysadmin and root users.

**Changing the sysadmin Password**

To change the sysadmin password, complete the following steps:

1. At the login page, do the following:
   
   a. Type **sysadmin** (case-sensitive), and then press **Enter**.
   b. When the password prompt appears, type **lan1cope**, and then press **Enter**.

2. On the System Configuration menu, select **Password** and press **Enter**.
Important: If you change the trusted hosts list from the defaults, you must make sure each Stealthwatch appliance is included in the trusted host list for every other Stealthwatch appliance in your deployment. Otherwise, the appliances will not be able to communicate with each other.

A prompt for the current password appears below the menu.

3. Type the current password, and then press Enter.
   The prompt for a new password appears.

4. Type the new password, and then press Enter.

Notes:
- The password must be between 8 and 30 alphanumeric characters in length with no spaces. You also may use the following special characters: $@%=?_;"}
Any password change must be different from the previous password by at least four characters.

5. Type the new password again, and then press Enter. A message appears indicating that the password was updated successfully.

6. Press Enter to return to the System Configuration Console menu.
7. Continue with the next section, “Changing the root Password.”

Changing the root Password

To change the root password, complete the following steps:

1. On the System Configuration Console menu, select Advanced, and then press Enter. The Advanced menu opens.
2. On the Advanced menu, select RootShell, and then press Enter.

A prompt for the root password appears.

3. Type the current root password, lan1cope, and then press Enter. The root shell prompt appears.

4. Type SystemConfig (case-sensitive), and then press Enter.

   This returns you to the System Configuration menu so that you can change the root password.

5. Select Password, and then press Enter. The password prompt appears.
6. Type the new root password, and then press **Enter**. A second prompt appears below the menu.

7. Retype the new root password, and then press **Enter**.

A message appears indicating that the password was updated successfully.

8. When your password change is successful, type **exit**, and then press **Enter**. You have now changed both of your default sysadmin and root passwords.

9. Press **Ctrl+Alt** to exit the console environment.

10. Have you completed all of the procedures in this chapter for all of the virtual appliances?
- If yes, continue with Configuring a Virtual Appliance System.
- If no, return to Configure the IP Addresses and repeat all of the procedures in this chapter for the next virtual appliance. Then, go to the Configuring a Virtual Appliance.
CONFIGURING A VIRTUAL APPLIANCE

Overview

This chapter provides the procedures for configuring the virtual appliance to begin processing traffic data. Once you have completed the steps in this chapter, the installation and configuration process is complete.

Note: Please refer to the checklist on “Before You Begin” on page 2 for the information you will need before proceeding.

Process Overview

Configuring a virtual Stealthwatch appliance involves completing the following procedures, which we discuss in this chapter:

1. Configuring the Individual Appliances
2. Configuring the UDP Director from the SMC
3. Configuration through the Appliance Admin Interface

Configuring the Individual Appliances

Initial configuration of every appliance is done with the Appliance Setup Tool. The first time you access the appliance, the Appliance Setup Tool is displayed.

It is important to install and configure your virtual appliances in the following order:

1. UDP Director VE
2. Flow Collector Database 5000 Console (if used)
3. All other Flow Collectors
4. All Flow Sensors
5. Cloud License Concentrator
6. Endpoint Concentrator
7. Secondary Stealthwatch Management Console
8. Primary Stealthwatch Management Console

Before you begin, gather the information detailed in the “Before You Begin” on page 2.

**Note:** Your screens may look slightly different from the ones presented here depending on your environment.

To configure an appliance, complete the following steps:

1. In the address field of your browser, type https:// followed by the IP address of the virtual appliance, and then press Enter.

2. The admin login page opens. Type **admin** and **lan411cope** (both are case sensitive), and then click **Login**. Go to step 5.

3. The Welcome page opens. Click **Continue**

![Welcome page](image)

The Management Network Interface page opens.
6. Review the settings you previously entered, and then click **Next**. The Password Management page opens.

7. In the appropriate fields, type your new admin password, and then click **Next**. The Host Name and Domain page opens.
8. In the appropriate fields, type the host name and the network domain name, and then click Next. The DNS Settings page opens.

9. Click the + button, and then type the IP address of the DNS server. Click Next. The NTP Settings page opens.
**Note:** Please set the first NTP server to be pool.ntp.org. This will allow the Stealthwatch appliance to access the random ntp.org pool of NTP servers to set the appliance’s time.

10. You can accept the default setting or enter another server by entering the IP address of your NTP server or selecting a name by clicking the list icon and selecting one from the drop-down list. See Configuration through the Appliance Admin Interface.

11. Click **Next**. The Review page opens.
12. Review your settings, and then click **Apply**. The confirmation dialogue opens.

![Confirmation Dialogue]

13. Allow a few minutes for your new system settings to take effect and then click **Next**. When finished, the login page for the appliance opens.

14. Enter the login credentials, and then click **Login**.

15. Are you managing the UDP Director from the SMC?
   - If yes, continue with the next section, **Configuring the UDP Director from the SMC**
   - If no, go to **Configuration through the Appliance Admin Interface**.

## Configuring the UDP Director from the SMC

If you have UDP Directors in your Stealthwatch System, you can configure them from the SMC Web Client so that the SMC manages the UDP Directors. In this configuration, the forwarding rules are configured on the SMC.
To manage the UDP Director individually (as a standalone appliance), see Configure the UDP Director VE Rules

Note: SSL is used to send messages from the UDP Director to the Stealthwatch Management Console (SMC).

Creating a Management Channel

Before the UDP Director can be added to the SMC, you must create a management channel between the two appliances.

1. Log in to the UDP Director Appliance Admin interface using your browser and the IP address of the appliance.
2. In the left navigation pane, click Configuration > Management Systems Configuration.
3. Click Add New Management System.
4. In the Management System IP Address field, type the SMC’s IP address.
5. Select the Is SMC check box.
6. Click Apply.

Adding a UDP Director

To add a UDP Director to the SMC, complete the following steps:

1. Log in to the SMC Web App.
2. From the navigation menu, click the user name at the top right of the page, and click UDP Director Configuration.

3. Click Add New Configuration.

4. Type in a name and the IP address of the UDP Director.
5. Click **Save**.
6. If you have additional UDP Directors, repeat steps 2-5 for each one.
7. Continue to the next section, **Configuring Forward Rules**

### Configuring Forward Rules

After adding a UDP Director to the SMC, you can configure forward rules for it.

To configure forwarding rules for a UDP Director, complete the following steps:

2. Click **Add New Rule**.

3. In the Description field, enter a brief description that identifies the rule.

4. In the Source IP Address:Port List field, type the IP address of the device that sends data to the UDP Director followed by the port number through which the data will be sent.

**Notes:**
- Use the syntax [IP address]:[Port Number], as shown in the examples below.
You can use Classless Inter-Domain Routing (CIDR) notation to enter a range of IP addresses.
You can type "All" to accept data from any source IP address on this port.
You can add Source IP Address:Port combinations within a rule by adding them to a new line.

Examples:
- 10.11.16.38:5322
- 192.168.0.0/16:9000
- All:2055

5. In the Destination IP Address field, enter the IP address of the device receiving data from the UDP Director.
6. In the Destination Port Number field, enter the port number for the receiving device.
7. Click Save. The new rule is added to the table on Forwarding Rules page.
8. Do you want to sync the changes?
   a. If yes, click the Sync button at the top of the page. The new rule is saved.
   b. If no, click the Discard Edits button at the top of the page. When the Configuration dialogue appears, click Yes.
9. Repeat the procedure to add forwarding rules as needed.
10. Continue with the next section, Configuration through the Appliance Admin Interface.

Note: If you want to have a secondary UDP Director, you must have added it with at least one forwarding rule. You first need to configure the Primary UDP Director and then repeat the configuration on the Secondary one.

Note: High Availability is only available on UDP Director hardware appliances. High Availability is not available on virtual appliances.

Configuration through the Appliance Admin Interface

This section provides the following procedures to complete the configuration of a virtual appliance using its Appliance Admin interface:

1. Log in to the Appliance Administration Interface
2. Configure the System Time
3. Configure the UDP Director VE Rules
4. Restart the Virtual Appliance

Log in to the Appliance Administration Interface

To log in to the Appliance Administration (Admin) interface, complete the following steps:

Notes:
- The supported browsers for Stealthwatch are Internet Explorer version 11 and later, and the latest versions of Firefox, Google Chrome, and Safari.
- If you have trouble loading any of the pages, try a different browser, or clear your browser cache, close and re-open your browser, and then log in again.

1. In the address field of your browser, type https:// followed by the IP address of the virtual appliance, and then press Enter.

   Note: Depending on the speed of your VM host, it may take approximately 30 minutes for all services to boot up.

2. Are you opening the SMC VE Appliance Admin interface?
   - If yes, the Landing page opens. In the upper right corner, click the Settings icon, and then click Administer Appliance.

- If no, the virtual appliance Login page opens.
3. In the **User Name** field, type **admin**.
4. In the **Password** field, type the admin password you created in the appliance setup.
5. Click **Login**. The Appliance Admin interface Home page opens.
6. Continue with the next section, “Configure the System Time.”

Configure the System Time

To configure the Network Time Protocol (NTP) and system time (time zone) settings on the virtual appliance, complete the following steps:

**CAUTION!** Use the same NTP server used for the Flow Collectors and other devices that feed information to the SMC.

1. On the Appliance Admin interface navigation pane, click the plus sign (+) beside **Configuration** and then click **System Time and NTP**.

The NTP Server page opens showing the NTP server that you set in the initial configuration using the Appliance Setup Tool.
2. Scroll down to the Time Zone section of the page to configure the virtual appliance system time.

3. Do the following:
   - Select the Continent from the drop-down list.
   - Select the Country from the drop-down list.
   - Select the Timezone from the drop-down list.

   The Apply notice appears.

4. Click **Apply** to make the changes permanent. The confirmation window opens.

5. Click **OK**.

6. Continue with the next section, **Configure the UDP Director VE Rules**.
Configure the UDP Director VE Rules

If you are not managing the UDP Director from the SMC, you can configure the forwarding rules on the appliance Admin Forwarding Rules page. For the UDP Director VE, you need to configure the exporter to send flows to be forwarded to the IP address of eth0. The UDP Director will then forward these from eth0 while preserving the original IP and MAC address of each exporter for forwarded packets.

Note: For promiscuous reception, you should use a span filter for all traffic of interest. The network must allow traffic on the ports being used from the exporters to the UDP Director and then to the receivers (ACLs).

Note: If you prefer to configure the SMC to manage the UDP Director, go to Configuring the UDP Director from the SMC.

To configure the rules for the UDP Director, complete the following steps:

1. On the Admin Web interface menu, click Configuration > Forwarding Rules.

The Forwarding Rules page opens.
2. In the Description field, type a description of the rule.
3. In the Source IP Address:Port List field, type the IP address of the device that sends data to the UDP Director followed by the port number through which the data will be sent. Use the following syntax:

[IP address]:[Port Number] as in 10.201.1.41:2057

**Note:** To receive all traffic from any device from a specific port, type All:[port number]. For example, type All:3123 to receive all data from port 3123. You can also use CIDR (Classless Inter-Domain Routing) notation to enter a range of IP addresses. For example, type 172.200.1.0/16:9000

4. To add another entry, press Enter and type the next IP address and port number.
5. In the Destination IP Address field, type the IP address of the device that receives data from the UDP Director.
6. In the Destination Port Number field, type the port number for the receiving device.
7. If you have more than one device sending data to the UDP Director to be forwarded to another receiving device, click Add.

A new line appears where you can enter the settings. Repeat this step until you have entered all devices for this UDP Director.

8. When finished, click Apply. The UDP Director Configuration screen refreshes and the system updates the configuration file. Any errors appear at the top of the screen.
9. Continue with the next section, Restart the Virtual Appliance

### Restart the Virtual Appliance

To restart the virtual appliance, complete the following steps:

1. On the Appliance Admin interface menu, select **Operations > Restart Appliance**.
The confirmation dialog opens.

2. Click Yes.
3. After you restart the appliance, continue installing and configuring your appliances in the order shown in Configuring the Individual Appliances. After you activate the product licenses on the appliance, the UDP Director VE will begin collecting data and sending it to the configured destinations. See the Downloading and Licensing Guide for details.