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

© 2018 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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>iii</td>
</tr>
<tr>
<td><strong>Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td>Overview</td>
<td>1</td>
</tr>
<tr>
<td>Audience</td>
<td>1</td>
</tr>
<tr>
<td>About Endpoint License</td>
<td>1</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>3</td>
</tr>
<tr>
<td>Admin Home Page Usage</td>
<td>5</td>
</tr>
<tr>
<td>How to Use This Guide</td>
<td>12</td>
</tr>
<tr>
<td>Contacting Support</td>
<td>13</td>
</tr>
<tr>
<td><strong>Installing the Endpoint Concentrator VE</strong></td>
<td>15</td>
</tr>
<tr>
<td>Overview</td>
<td>15</td>
</tr>
<tr>
<td>Process Overview</td>
<td>15</td>
</tr>
<tr>
<td>Configuring Your Firewall for Communications</td>
<td>15</td>
</tr>
<tr>
<td>Communication Ports</td>
<td>16</td>
</tr>
<tr>
<td><strong>Installing the Endpoint Concentrator VE using VMware vSphere Client</strong></td>
<td>17</td>
</tr>
<tr>
<td>Overview</td>
<td>17</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>17</td>
</tr>
<tr>
<td>Process Overview</td>
<td>17</td>
</tr>
<tr>
<td>Logging in to the VMware vSphere Client</td>
<td>18</td>
</tr>
<tr>
<td>Installing the Endpoint Concentrator VE</td>
<td>18</td>
</tr>
<tr>
<td><strong>Installing a Virtual Appliance on a KVM Host</strong></td>
<td>27</td>
</tr>
<tr>
<td>Overview</td>
<td>27</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>28</td>
</tr>
<tr>
<td>Process Overview</td>
<td>28</td>
</tr>
<tr>
<td>Installing a Virtual Appliance on a KVM Host</td>
<td>28</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configuring the Virtual Environment</td>
<td>35</td>
</tr>
<tr>
<td>Overview</td>
<td>35</td>
</tr>
<tr>
<td>Configure the IP Addresses</td>
<td>35</td>
</tr>
<tr>
<td>Change the Default User Password</td>
<td>39</td>
</tr>
<tr>
<td>Changing the sysadmin Password</td>
<td>39</td>
</tr>
<tr>
<td>Changing the root Password</td>
<td>41</td>
</tr>
<tr>
<td><strong>Configure the Endpoint Concentrator VE</strong></td>
<td>45</td>
</tr>
<tr>
<td>Overview</td>
<td>45</td>
</tr>
<tr>
<td>Process Overview</td>
<td>45</td>
</tr>
<tr>
<td>Configuring the Individual Appliances</td>
<td>45</td>
</tr>
<tr>
<td>Configuration through the Appliance Admin Interface</td>
<td>50</td>
</tr>
<tr>
<td>Log in to the Appliance Administration Interface</td>
<td>50</td>
</tr>
<tr>
<td>Configure the System Time</td>
<td>52</td>
</tr>
<tr>
<td>Configure the Endpoint Concentrator VE</td>
<td>54</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>56</td>
</tr>
<tr>
<td>Restart the Endpoint Concentrator VE</td>
<td>57</td>
</tr>
</tbody>
</table>
INTRODUCTION

Overview

This is an installation and configuration guide for the Endpoint Concentrator VE in a network. Read this chapter to learn more about this guide and how to contact Support, if needed. This chapter includes the following sections:

- Audience
- About Endpoint License
- Before You Begin
- Admin Home Page Usage
- How to Use This Guide
- Resource Requirements

Audience

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

About Endpoint License

The Cisco Stealthwatch Endpoint License solution enhances the network visibility provided by the Cisco Stealthwatch System with endpoint data provided by the Cisco AnyConnect Network Visibility Module. The figure below provides a high level overview of the Stealthwatch Endpoint License solution and its components.
AnyConnect with NVM: The Cisco AnyConnect NVM installed on network attached endpoints sending vzFlow records to the Stealthwatch Endpoint Concentrator.

Stealthwatch Endpoint Concentrator: A purpose built appliance that will receive vzFlow records from multiple endpoints and forward endpoint flow records to the Stealthwatch Flow Collector. The Stealthwatch Endpoint Concentrator will appear as a single exporter to the Stealthwatch System and is a required component of the Endpoint License.

Stealthwatch Flow Collector: Serves as a central collector for flow data generated by NetFlow-enabled devices. The Stealthwatch Flow Collector monitors, categorizes, and analyzes network traffic to create comprehensive security intelligence at both the network and host level.

Stealthwatch Management Console: Manages, coordinates, and configures all Stealthwatch appliances to correlate security and network intelligence across the enterprise.

The Stealthwatch Endpoint License solution enables the Flow Collector to extract endpoint specific fields from the flow records forwarded to it by the Endpoint Concentrator and through its process of stitching and de-duplication insert the endpoint fields into the conversational flow record maintained in the Flow Collector database. In the initial release the following fields will be attributed to flows where the host with the AnyConnect NVM is the initiator of the flow:

- Process name
- Process hash
- Process account
- Parent process name
- Parent process hash

**Note:** It is important to note that in the initial release of the Stealthwatch Endpoint License it is necessary that the Stealthwatch Flow Collector receive corresponding flow records from a network device.
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 vSphere Client v6.x or KVM (Kernel-based Virtual Machine) for the virtual appliance installation. It is important to review the following compatibility information:

**VMware vSphere Client v6.x or Later**

- **VMware ESX Version**: Stealthwatch VE appliances that are running on older versions of VMware ESX are not compatible with ESX v6.x. If you upgrade VMware to ESX v6.x, you must 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

You need to install and configure these Endpoint components in the following order:

1. Flow Collector
2. Endpoint Concentrator
3. Agent

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.

As an add-on licensed feature to the Stealthwatch System, before beginning the setup of the Stealthwatch Endpoint License you will first need to install and configure the Stealthwatch System. Once this is complete you may proceed with the installation and configuration of the Endpoint License Concentrator. If you do not have a fully operational Stealthwatch deployment before the deployment of the Endpoint Concentrator your Stealthwatch deployment may not be able to effectively collect endpoint data.

**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. Cisco AnyConnect configuration guides are on the Cisco website.

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.
Endpoint Concentrator

These are the requirements for the Endpoint Concentrator VE 1000:

<table>
<thead>
<tr>
<th>Reserved CPU</th>
<th>Reserved Memory</th>
<th>Maximum FPS Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>8 GB</td>
<td>20,000</td>
</tr>
</tbody>
</table>

**Note:** The capacity of your Flow Collector should be taken into consideration in determining the number of endpoint concentrators needed for your deployment.

Information Needed for Console Access

<table>
<thead>
<tr>
<th>Setting</th>
<th>Hypervisor Server</th>
<th>Endpoint Concentrator 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.x)</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>Endpoint Concentrator VE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>(Default = 192.168.1.x)</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>

Admin Home Page Usage

For this release you need to understand the Home page of the Endpoint Concentrator VE Admin interface. The current Help pages do not reflect the correction information needed. Use this section to understand how the Home page, which is refreshed every minute, displays statistics about the
appliances in the following sections. You can also use this page to perform certain administrative tasks, such as restarting or stopping processes that are running on the appliance. It includes several sections, which are described below.

**System**

Use this section to find information about the appliance, such as the IP address, host name, version, or serial number.

The following table provides the field descriptions for the System:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build</td>
<td>An alphanumeric code that identifies the build version of the appliance.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The domain name that is assigned to the appliance.</td>
</tr>
<tr>
<td>Free Memory</td>
<td>The amount of memory that is currently available for use.</td>
</tr>
<tr>
<td>Load Average</td>
<td>A measure of the average system load over the past one-, five-, and</td>
</tr>
<tr>
<td></td>
<td>fifteen-minute periods, respectively.</td>
</tr>
<tr>
<td>Platform</td>
<td>The virtual platform on which the appliance software is installed.</td>
</tr>
<tr>
<td>Serial No.</td>
<td>The serial number or ID of the appliance. You need the serial number to</td>
</tr>
<tr>
<td></td>
<td>activate the license for the appliance.</td>
</tr>
<tr>
<td>Total Memory</td>
<td>The total amount of memory installed on the appliance.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The amount of time since the appliance was last rebooted.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the software that is installed on the appliance.</td>
</tr>
</tbody>
</table>
Endpoint Status

The Endpoint Status section indicates the amount of flow data of the NetFlow Parser and the NetFlow Generator that this appliance has collected or dropped every minute and over the course of the day and the number of UDP packets received.

The following tables provide the field descriptions for Endpoint Status:

### NetFlow Parser

<table>
<thead>
<tr>
<th>Service Running</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Received</td>
<td>UDP Packets the service has received from exporters.</td>
</tr>
<tr>
<td>FPS (Flow Rate)</td>
<td>The average rate at which flows have been processed by the appliance in the corresponding time period.</td>
</tr>
<tr>
<td>Data Sets Dropped</td>
<td>The total number of flows that were lost, usually due to network congestion, in the corresponding time period.</td>
</tr>
<tr>
<td>Placed in Queue</td>
<td>Records placed on a queue for the next service (Netflow-Generator) to receive.</td>
</tr>
</tbody>
</table>

### NetFlow Generator

<table>
<thead>
<tr>
<th>Service Running</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received from Queue</td>
<td>Number of messages received from exporters for each period.</td>
</tr>
<tr>
<td>Dropped Data</td>
<td>The total number of flows that were dropped, usually due to network congestion, for each period.</td>
</tr>
<tr>
<td>Parsed Data</td>
<td>Number of flows processed from received messages for each period</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Number of UDP packets forwarded to the Flow Collector for each period.</td>
</tr>
</tbody>
</table>
Services

The Services section displays the status of the processes that are running on this appliance and how much memory they are using.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of each service</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the corresponding service</td>
</tr>
<tr>
<td>PID</td>
<td>The process identifier of the corresponding service</td>
</tr>
<tr>
<td>Started</td>
<td>The amount of time that the corresponding service has been running. If it has been less than 24 hours, the amount of time is shown. If it has been more than 24 hours, the date that the service started is shown.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>The percentage of the CPU’s (central processing unit) total capacity that is being used by the corresponding service.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>The percentage of the appliance’s total memory that is being used by the corresponding service.</td>
</tr>
<tr>
<td>Action</td>
<td>You should only stop or restart a service at the direction of Customer Support. If you restart a service that is running, there may be a short period in which data is not captured. This column contains buttons that allow you to manually execute actions for the corresponding service. The following actions may be available: Stop, Start, Restart</td>
</tr>
</tbody>
</table>

Docker Services

The Docker Services section displays the status of the Docker processes that are running on this appliance.
The following table provides the field descriptions for Docker Services:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of each service:</td>
</tr>
<tr>
<td>Zookeeper</td>
<td>The ISE-Client is a service that receives user session information and sends mitigation actions to Cisco's Identity Services Engine (ISE) through the Cisco Platform Exchange Grid (PxGrid).</td>
</tr>
<tr>
<td>Kafka</td>
<td>Cognitive Threat Analytics Data Uploader forwards netflow to the CTA cloud for analysis by their supervised machine-learning algorithms to detect malware.</td>
</tr>
<tr>
<td>Netflow-Parser</td>
<td>Data Exporter exports a restricted set of netflow for use by third-party applications that are written by professional services or customers.</td>
</tr>
<tr>
<td>Netflow-Generator</td>
<td>Kafka is a distributed, partitioned, replicated commit log service that provides the functionality of a messaging system.</td>
</tr>
<tr>
<td>Legacy-Auth</td>
<td>Legacy-Auth is an authentication service that validates user credentials.</td>
</tr>
<tr>
<td>Token-Authority</td>
<td>Flow-Aggregation-Receiver is a service that populates the First Seen and Last Seen fields on the Host List page.</td>
</tr>
<tr>
<td></td>
<td>Flow-aggregation-stream aggregates the information for the First Seen and Last Seen fields and sends it to the flow aggregation receiver.</td>
</tr>
<tr>
<td></td>
<td>NetFlow Parser is a service that receives and forwards endpoint messages to the NetFlow Generator.</td>
</tr>
<tr>
<td></td>
<td>NetFlow Generator is a service that forwards endpoint flows to the Flow Collector or the UDP Director.</td>
</tr>
<tr>
<td></td>
<td>Stealthwatch Policy allows you to configure policies for various types of hosts that interact with your Stealthwatch System to enable you to monitor different areas of your network.</td>
</tr>
<tr>
<td></td>
<td>Stealthwatch Reporting is a function that offers consolidated</td>
</tr>
</tbody>
</table>
and customizable reports.

- **Token-Authority** is a service that manages tokens (JWT) securely.
- **Zookeeper** is a centralized service for maintaining configuration information, naming, providing distributed synchronization, and providing group services.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The current status of the corresponding service.</td>
</tr>
<tr>
<td>Started</td>
<td>The amount of time that the corresponding service has been running. If it has been less than 24 hours, the amount of time is shown. If it has been more than 24 hours, the date that the service started is shown.</td>
</tr>
</tbody>
</table>
| Action  | You should only stop or restart a service at the direction of Customer Support. If you restart a service that is running, there may be a short period in which data is not captured and all logged in users will need to re-authenticate. This column contains buttons that allow you to manually execute actions for the corresponding service. The following actions may be available: 
  - Restart
  - Stop |

## Network Interfaces

The Network Interfaces section displays the data for the hardware interfaces on the appliance.

The following table provides the field descriptions for Network Interfaces:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The text identifier for the interface.</td>
</tr>
<tr>
<td>Up</td>
<td>The state of the interface, as follows:</td>
</tr>
<tr>
<td></td>
<td>- True - Enabled</td>
</tr>
<tr>
<td></td>
<td>- False - Disabled</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address associated with the interface. Only the management</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>port (eth0)</td>
<td>will show an IP address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address associated with the interface.</td>
</tr>
<tr>
<td>Auto Neg</td>
<td>The state of the auto-negotiation setting, either:</td>
</tr>
<tr>
<td></td>
<td>- True - The setting is On.</td>
</tr>
<tr>
<td></td>
<td>- False - The setting is Off.</td>
</tr>
<tr>
<td>Link Speed (bps)</td>
<td>The speed at which the interface is sending and receiving data.</td>
</tr>
<tr>
<td>Duplex</td>
<td>The duplex setting for the interface, either:</td>
</tr>
<tr>
<td></td>
<td>- Full - for Full Duplex</td>
</tr>
<tr>
<td></td>
<td>- Half - for Half Duplex</td>
</tr>
<tr>
<td>MTU</td>
<td>The maximum packet size the interface is allowed to transmit per transaction.</td>
</tr>
<tr>
<td>RX</td>
<td>Statistics for the received data according to the following characteristics:</td>
</tr>
<tr>
<td></td>
<td>- Bytes - The amount of undamaged data received, in bytes.</td>
</tr>
<tr>
<td></td>
<td>- Packets - The amount of undamaged data received, in packets.</td>
</tr>
<tr>
<td></td>
<td>- Errors - The number of damaged packets in the received data.</td>
</tr>
<tr>
<td></td>
<td>- Dropped - The number of dropped packets in the received data.</td>
</tr>
<tr>
<td>TX</td>
<td>Statistics for the transmitted data according to the following characteristics:</td>
</tr>
<tr>
<td></td>
<td>- Bytes - The amount of undamaged data transmitted, in bytes.</td>
</tr>
<tr>
<td></td>
<td>- Packets - The amount of undamaged data transmitted, in packets.</td>
</tr>
<tr>
<td></td>
<td>- Errors - The number of damaged packets in the transmitted data.</td>
</tr>
<tr>
<td></td>
<td>- Dropped - The number of dropped packets in the transmitted data.</td>
</tr>
<tr>
<td>Action</td>
<td>Includes an Edit link to the Network Interface Configuration page that allows you to manually configure the interface.</td>
</tr>
</tbody>
</table>

**Disk Usage**

The Disk Usage section displays information about the hard drive space on this appliance.
The following table provides the field descriptions for Disk Usage:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The location in the appliance’s directory structure where the corresponding data exists.</td>
</tr>
<tr>
<td>Used</td>
<td>The amount of available space (in percentage) occupied by the corresponding data. When the percentage reaches 75%, the row turns red. If this occurs the data is dropped. You can prevent this from happening by expanding the virtual disk space.</td>
</tr>
<tr>
<td>Size (byte)</td>
<td>The amount of space (in bytes) allocated for the corresponding data.</td>
</tr>
<tr>
<td>Used (byte)</td>
<td>The amount of space (in bytes) occupied by the corresponding data.</td>
</tr>
<tr>
<td>Available (byte)</td>
<td>The amount of unused space (in bytes) for the corresponding data.</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 Endpoint Concentrator</td>
</tr>
<tr>
<td>Configuring a Virtual Appliance System</td>
<td>How to configure the Endpoint Concentrator 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>
</tbody>
</table>
Abbreviations | Definition
---|---
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
OVF | Open Virtualization Format
SMC | Stealthwatch Management Console
TB | Terabyte
UUID | Universally Unique Identifier
VDS | vNetwork Distributed Switch
VE | Virtual Edition
VLAN | Virtual Local Area Network
VM | Virtual Machine

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 THE ENDPOINT CONCENTRATOR VE

Overview

This chapter describes how to install the Endpoint Concentrator VE.

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 v6.x or later
- 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.

Use the port information in this section to configure your network so the appliances can communicate on through the network:

- TCP 22
- TCP 443
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 514
- UDP 2055
- UDP 3514

### Communication Ports

The following table shows the ports needed for Endpoint Concentrator communications:

<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>AnyConnect</td>
<td>Endpoint Concentrator</td>
<td>UDP/2055*</td>
<td>NetFlow</td>
</tr>
<tr>
<td>Endpoint Concentrator</td>
<td>Flow Collector NetFlow</td>
<td>UDP/2055*</td>
<td>NetFlow</td>
</tr>
<tr>
<td>Endpoint Concentrator</td>
<td>UDP Director</td>
<td>UDP/2055*</td>
<td>NetFlow</td>
</tr>
</tbody>
</table>

* These ports are configurable.

**Note:** Go to the section that is applicable to your virtual appliance installation: [VMware vSphere Client](https://www.vmware.com/) or [KVM](https://www.kernel.org/).
Installing the Endpoint Concentrator VE using VMware vSphere Client

Overview

This chapter describes how to install the Endpoint Concentrator VE using VMware vSphere Client v6.

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 Endpoint Concentrator VE
Logging in to the VMware vSphere Client

To install the virtual appliance, you must first log in to the VMware vSphere Client v6.x, 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 Endpoint Concentrator VE

To install the Endpoint Concentrator VE 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**.
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.
The Disk Format page opens.
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. Go to **Configuring the Virtual Environment**

# INSTALLING A VIRTUAL APPLIANCE ON A KVM HOST

## Overview

This chapter describes how to install the Endpoint Concentrator VE 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 Endpoint Concentrator VE, 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 Endpoint Concentrator VE, 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 Administrative IP Address page opens.
6. Click on the page. Enter the IP address for the Endpoint Concentrator.

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.

![Advanced menu screenshot]

A prompt for the root password appears.

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

![Root shell prompt]

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. Continue with Configuring the Endpoint Concentrator VE.
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 the Endpoint Concentrator VE**.
CONFIGURING THE ENDPOINT CONCENTRATOR VE

Overview

This chapter provides the procedures for configuring the Endpoint Concentrator 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 3 for the information you will need before proceeding.

Process Overview

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

1. Configuring the Individual Appliances
2. Configuration through the Appliance Admin Interface

Configuring the Individual Appliances

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

Before you begin, gather the information detailed in the “Before You Begin” on page 3.

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

To configure the Endpoint Concentrator VE, complete the following steps:

1. In the address field of your browser, type https:// followed by the IP address of the virtual the Endpoint Concentrator VE, 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**

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

![Password Management Page](image)

7. In the appropriate fields, type your new admin password, and then click **Next**. The Host Name and Domain page opens.

![Host Name and Domain Page](image)

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.

13. Click **OK**. The Complete page opens.
14. 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.

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

16. Continue with the next section, **Configuration through the Appliance Admin Interface**.

### 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 Endpoint Concentrator VE
4. Restart the Endpoint Concentrator VE

### 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.
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, Configuring the Endpoint Concentrator VE.

Configure the Endpoint Concentrator VE

For the Endpoint Concentrator VE you need to configure the connection to a NetFlow Flow Collector from the Endpoint appliance. You can set only one Flow Collector.

To configure the connection to the NetFlow Collector, complete the following steps:

1. In the navigation page, click the plus sign (+) beside Configuration, and then click Collection.
The NetFlow Collector page opens.

2. In the Assign NetFlow Collector fields, type the IP Address and the port number of the Flow Collector or UDP Director that you want the Endpoint Concentrator to send the data to. The default port is 2055.
3. Click Add. This will validate the IP address and port and move the entry to the table.
4. If the information is correct, click Apply. This will restart the services with the new information.

**Note:** This field will only accept one value. If you need to add recipients, consider using a Cisco UDP Director.
The NetFlow Collector settings appear in the table at the top of the page.

**Note:** If you need to change the setting for the Collector, first delete the current Collector by clicking the Delete check box, and then clicking **Apply**. Then you can configure a new Collector.

5. In the main menu, click **Home** and check the Docker Services table:

6. Do all of the docker services have a status of “Running”?
   a. If not, continue to the next section, **Troubleshooting**.
   b. If yes, continue with the section, “**Restart the Endpoint Concentrator VE**” on page 57.

**Troubleshooting**

After the AnyConnect Agents and the Endpoint Concentrator have been configured, there are a few items that can be checked to determine if the system is operational. These steps may be used if it is determined that the system is not processing data as expected.

1. Validate that the Endpoint Concentrator is receiving flows from the AnyConnect Agents to the Collector.
Enable SSH access to the Endpoint Concentrator via the web admin page.

Configuration -&gt; Services - Check **Enable SSH**

2. SSH into the Endpoint Concentrator, run “docker ps”:
   - Validate that there are four entries that contain kafka, netflow-parser, zookeeper, and netflow-generator. Note that the Container IDs and Image versions will differ.
   - If not they are not running, restart the Services from the appliance.

3. Change Directories to “/lancop/var/logs/containers” and run “tail -f netflow-parser.log”. Verify in the Stats print out that the counts are not zero.

4. Now, run “tail -f netflow-generator.log”. Verify in the Stats print out that the counts are not zero. If the stats read as below, the Endpoint Concentrator is not producing Netflow.

5. Validate AnyConnect Agents can send data to the Endpoint Concentrator.
   - On one of the machines running the AnyConnect Agent, open a terminal or command prompt and run “ping <IPofEndpointConcentrator>”.
   - If there are response bytes, the Agent most likely can export to the Endpoint Concentrator.

**Restart the Endpoint Concentrator VE**

To restart the virtual appliance, complete the following steps:

1. On the Appliance Admin interface menu, select **Operations > Restart Appliance**.

The confirmation dialog opens.

© 2018 Cisco Systems, Inc. All Rights Reserved.
2. Click **Yes**.