Endpoint License
Virtual Edition
Installation and Configuration Guide
(for Stealthwatch System v6.9.0)
Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>iii</td>
</tr>
<tr>
<td>Introduction</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>4</td>
</tr>
<tr>
<td>How to Use This Guide</td>
<td>11</td>
</tr>
<tr>
<td>Other Resources</td>
<td>12</td>
</tr>
<tr>
<td>Installing the Endpoint Concentrator VE</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>Logging in to the VMware vSphere Client</td>
<td>16</td>
</tr>
<tr>
<td>Adding a Resource Pool</td>
<td>17</td>
</tr>
<tr>
<td>Installing the Endpoint Concentrator VE</td>
<td>19</td>
</tr>
<tr>
<td>Configuring the Virtual Environment</td>
<td>29</td>
</tr>
<tr>
<td>Overview</td>
<td>29</td>
</tr>
<tr>
<td>Configure the IP Addresses</td>
<td>29</td>
</tr>
<tr>
<td>Change the Default User Passwords</td>
<td>33</td>
</tr>
<tr>
<td>Changing the sysadmin Password</td>
<td>33</td>
</tr>
<tr>
<td>Changing the root Password</td>
<td>35</td>
</tr>
<tr>
<td>Configuring the Endpoint Concentrator VE</td>
<td>39</td>
</tr>
<tr>
<td>Overview</td>
<td>39</td>
</tr>
</tbody>
</table>
INTRODUCTION

Overview

This is an installation and configuration guide for the Endpoint Concentrator VE in a network using vSphere Client v4.x or later.

**Note:** Stealthwatch VE appliances that are running under VMware ESX v3.x are not compatible with ESX v4.x. If you upgrade VMware to ESX v4.x, you must delete your existing Stealthwatch VE appliances and reinstall them.

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 software.

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 vSphere client interface, and then the Appliance Administration (Admin) interface. You can use the tables provided in this section to record settings you will need to install and configure the Stealthwatch VE appliances.

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.

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 Stealthwatch 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 ESX server where you will be installing the virtual appliances reflect 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 OVF (Open Virtualization Format) file from the Download and Licensing Center. For instructions on downloading the file for each appliance, see the Downloading and Licensing Stealthwatch Products document in the Download and Licensing Center or in the Documentation Library found in Help of the Stealthwatch appliances. Cisco AnyConnect configuration guides are at the Cisco web site.

Resource Requirements

This section provides the resource requirements for the Endpoint Concentrator.
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 the vSphere Client Interface

<table>
<thead>
<tr>
<th>Setting</th>
<th>ESX/vSphere 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>(Default = 192.168.1.x)</td>
<td></td>
</tr>
<tr>
<td>Netmask IP Address</td>
<td>(Default = 255.255.255.0)</td>
<td></td>
</tr>
<tr>
<td>Gateway IP Address</td>
<td>(Default = 192.168.1.1)</td>
<td></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.
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 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 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:

<table>
<thead>
<tr>
<th>NetFlow Parser</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Running</td>
<td>An icon that indicates if the service is running: green check-mark if running, red dash if not.</td>
</tr>
<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>

<table>
<thead>
<tr>
<th>NetFlow Generator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Running</td>
<td>An icon that indicates if the service is running: green check-mark if running, red dash if not.</td>
</tr>
<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.

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

© 2017 Cisco Systems, Inc. All Rights Reserved.
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>
</tbody>
</table>
| Up        | The state of the interface, as follows:
- True - Enabled
- False - Disabled |
| IP Address| The IP address associated with the interface. Only the management |
Field | Description
--- | ---
port (eth0) will show an IP address. | 
MAC Address | The MAC address associated with the interface.
Auto Neg | The state of the auto-negotiation setting, either:
  - True - The setting is On.
  - False - The setting is Off.
Link Speed (bps) | The speed at which the interface is sending and receiving data.
Duplex | The duplex setting for the interface, either:
  - Full - for Full Duplex
  - Half - for Half Duplex
MTU | The maximum packet size the interface is allowed to transmit per transaction.
RX | Statistics for the received data according to the following characteristics:
  - Bytes - The amount of undamaged data received, in bytes.
  - Packets - The amount of undamaged data received, in packets.
  - Errors - The number of damaged packets in the received data.
  - Dropped - The number of dropped packets in the received data.
TX | Statistics for the transmitted data according to the following characteristics:
  - Bytes - The amount of undamaged data transmitted, in bytes.
  - Packets - The amount of undamaged data transmitted, in packets.
  - Errors - The number of damaged packets in the transmitted data.
  - Dropped - The number of dropped packets in the transmitted data.
Action | Includes an Edit link to the Network Interface Configuration page that allows you to manually configure the interface.

**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 install the Endpoint Concentrator on an ESX server using vSphere Client v4.x or later</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 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>Abbreviations</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------</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>IT</td>
<td>Information Technology</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>

**Other Resources**

In addition to this guide, you may find these documents and online resources useful.

**Related Documents**


Additional information is available in the Lancope Community web site ([https://lancope.force.com/Customer/CustomerCommLogin](https://lancope.force.com/Customer/CustomerCommLogin)). If you do not have login access to the web site, send an email requesting access to Support.

**Lancope Blog**

Lancope’s *Inside the Threat* blog at [http://www.lancope.com/blog/](http://www.lancope.com/blog/) provides a wealth of information about NetFlow, the NetFlow industry, and new Stealthwatch features, as well as tips and tricks on using Stealthwatch.
Lancope Resources & Tools for Advanced Cybersecurity

For further information about Stealthwatch, go to the Lancope Resources & Tools for Advanced Cybersecurity site [https://www.lancope.com/resources](https://www.lancope.com/resources). It includes resources such as an online video library, white papers, and Webinars.

Contacting Support

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

- Contact your local Cisco partner.
- Call +1 800-838-6574.

Document Feedback

If you have comments about this document, please contact us at support@lancope.com. We appreciate your feedback.
INSTALLING THE ENDPOINT CONCENTRATOR VE

Overview

This chapter describes how to install the Endpoint Concentrator VE using VMware vSphere Client v4.x or later.

Note: Make sure 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.

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. Logging in to the VMware vSphere Client
3. Adding a Resource Pool
4. Installing the Endpoint Concentrator VE

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 shown 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</td>
<td>UDP/2055*</td>
<td>NetFlow</td>
</tr>
<tr>
<td></td>
<td>UDP Director</td>
<td>UDP/2055*</td>
<td>NetFlow</td>
</tr>
</tbody>
</table>

* These ports are configurable.

**Logging in to the VMware vSphere Client**

To install the virtual appliance, you must first log in to the VMware vSphere Client, by completing the following steps:

**Note:** The screen images are for VMware v5.0 and may appear slightly different from your screens, but the commands are the same. If you use the VMware Web Client interface,
1. Launch the VMware vSphere Client software. The Login dialog opens.

2. Type the IP address of the ESX server and your login credentials, and then click Login. The Home page opens.

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

Adding a Resource Pool

A virtual appliance needs a resource pool with specific CPU and memory resources allocated to it so that it can operate without affecting other virtual machines. This procedure describes how to add a new resource pool with the proper allocations for the Endpoint Concentrator VE.

Note: If desired, you can use an existing resource pool for a virtual appliance. However, you should examine this procedure to make sure the existing resource pool has enough resources allocated to it for a virtual appliance to operate properly. If you use the VMware Web Client v5.5 interface, some of the screens shown here will differ. Therefore, the differences in the options will be pointed out where necessary.

To add a resource pool for a virtual appliance on the ESX server where it will reside, complete the following steps:

1. In the Inventory tree on the left, right-click the ESX server IP address, and then select New Resource Pool from the popup menu or on the Web client select All vCenter Actions > New Resources Pool.
2. In the **Name** field, type the name you want to use to identify this resource group.
3. Do not change any of the settings in the CPU Resources section.
4. In the Memory Resources section, do the following:
   - Change the Reservation field as recommended in the chart for the appliance in "Resource Requirements" on page 3.
   - Click the **Unlimited** checkbox to clear it.
5. Click **OK**. The resource pool appears beneath the ESX server on the Inventory tree.
8. Select the resource pool, and then click the **Resource Allocation** tab to review the CPU and memory resource allocations. On the Web Client, click the Manage tab and then click **CPU Resources & Memory Resource**.

---

**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. Unzip the virtual appliance software (OVF) file that you downloaded earlier.
2. On the vSphere client menu, click **File > Deploy OVF Template**. On the Web client, right-click the host, and then select **Deploy OVF Template**.
**Note:** The Web client OVF template wizard has slightly different wording and numbering for the steps of the procedure, but the steps are the same. 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.
3. Click **Browse**, and then navigate to select the virtual appliance OVF file.
4. Click **Next** to display the OVF Template Details page (Web Client: 1.b. Review details).

![Display OVF Template](image)

5. Click **Next**. The End User License Agreement opens (1c. Accept EULAs).
6. After reviewing the information, click **Accept**, and then click **Next**. The Name and Location page opens (2a. Select name and folder).
7. If desired, change the name for the virtual appliance as it will appear in the Inventory tree, and then click **Next**.

   - If the Specify a Specific Host page opens, select the host or cluster where the virtual appliance will reside.
• If the Host/Cluster page opens, select the host or cluster where the appliance will reside.

8. Click **Next**. The Resource Pool page opens.
9. Select the resource pool that you defined earlier, and then click **Next**.
   a. If the Datastore page opens, go to step 10.
   b. If the Disk Format page opens, go to step 11.

   **Note:** On the Web Client the Select storage page opens and includes both the datastore and the disk format.

10. On the Datastore page, select where you want to store the virtual appliance, and then click **Next**.
The Disk Format page opens.

12. From the Destination Networks drop-down list, select a virtual appliance management port.

13. Click **Next**. The Ready to Complete page opens with a summary of the settings.

15. When the deployment is completed, click Close to close the progress dialog. The virtual appliance appears in the Inventory tree.

16. Continue with the next chapter, 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. If necessary, launch the vSphere Client software and log in. The Getting Started page opens.

2. In the Inventory tree, select the Endpoint Concentrator.

3. On the Getting Started page, click the “Power on the virtual machine” link. You may need to scroll down to see the link.

   **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 memory reservation limit for the appliance and its resource pool.
   - Increase the available resources on the system where the appliance is installed.

4. Click the **Console** tab. (On the Web client, click the Summary tab and then click the Launch Console link.) Allow the virtual appliance to finish booting up. The Administrative IP Address page opens.
5. Click on the page, and then enter the IP address for the Endpoint Concentrator.
6. Select OK, and then press Enter. The IP Netmask page opens with the default network mask IP address.

7. 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.
8. Do the following:

- Accept the default value or enter a new one based on your environment.
- Select OK and press \texttt{Enter} to continue.

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

9. Do the following:

- Accept the default value or enter a new one based on your environment.
- Select OK and press \texttt{Enter} to continue.

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

11. Press **Enter**. The system restart page opens.

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

13. 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.

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

Change the Default User Passwords

To ensure that your network is secure, you must change both the default passwords of the sysadmin and root passwords on the virtual appliance.

Changing the sysadmin Password

To change the sysadmin password, complete the following steps:

1. At the login page, do the following:
   a. When the password prompt appears, type lan1cope, and then press Enter.
   b. Type sysadmin (case-sensitive), 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 5 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 with RootShell highlighted](image)

A prompt for the root password appears.

![Root password prompt](image)

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

![Root shell prompt](image)

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 a Virtual Appliance System.”
- If yes, continue with “Configuring a Virtual Appliance System.”
- If no, return to “Configure the IP Addresses” on page 29 and repeat all of the procedures in this chapter for the next virtual appliance. Then, go to the “Configuring a Virtual Appliance System.”
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.

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. Depending on your system, you should configure the Flow Sensors and Flow Collectors before the UDP Directors, and then, lastly, configure the SMC. When you complete the initial setup for the SMC, the system setup tool opens and you can configure your Stealthwatch System.

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

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

7. 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.
8. 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"

10. Review your settings, and then click **Apply**. The confirmation dialogue opens.

11. Click **OK**. The Complete page opens.

12. 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.

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

14. 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 9 and later and Firefox version 3 and later.
- If you have trouble loading any of the pages, 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://](https://) followed by the IP address of the virtual appliance, and then press Enter.
2. Are you opening the SMC VE Appliance Admin interface?
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**.

**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**.

![Image of navigation page with Configuration and Collection options highlighted]

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 50.

**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.

© 2017 Cisco Systems, Inc. All Rights Reserved.
- Enable SSH access to the Endpoint Concentrator via the web admin page.
- Configuration -> 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 “/lancupe/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**.

   ![Restart Appliance Menu](image)

   The confirmation dialog opens.
2. Click **Yes**.