

# UDP Director Virtual Edition (also known as FlowReplicator VE) Installation and Configuration Guide (for StealthWatch System v6.7.0)



## Installation and Configuration Guide: UDP Director VE v6.7.0

© 2015 Lancope, Inc. All rights reserved.

Document Date: March 23, 2015

### **Trademarks**

Lancope, StealthWatch, and other trademarks are registered or unregistered trademarks of Lancope, Inc. Cisco, Cisco Identity Services Engine, and Cisco TrustSec are trademarks or registered trademarks of Cisco Systems, Inc., and/or affiliates in the U.S. and other countries. All other trademarks are properties of their respective owners.

# CONTENTS

<b>1-INTRODUCTION.</b> Overview         Audience         Before You Begin         Downloading the VE Software         Resource Requirements.         UDP Director VE (also known as FlowReplicator VE)         Information Needed for the vSphere Client Interface         Information Needed for the Appliance Admin Interface         About the UDP Director VE         How to Use This Guide         Documentation Icons         Abbreviations         Other Resources.	5 5 6 6 6 6 7 7 8 9 9
2-INSTALLING A VIRTUAL APPLIANCE.	13 14 15 15 19
Configure the IP Addresses	31 32 37 37
Overview	44 50

Configure the System Time	51
Change the Admin Password	53
Configure UDP Director VE Rules	55
Restart the Virtual Appliance	58

# INTRODUCTION

## OVERVIEW

This is an installation and configuration guide for the UDP Director VE (also known as FlowReplicator VE) in a network using vSphere Client v4.x or v5.x. Beginning with v6.6.0, the FlowReplicator VE is called the UDP Director VE.



### 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.

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

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

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

## Audience

The primary audience for this guide is administrators who need to install and configure StealthWatch UDP Director VE (also known as FlowReplicator VE) appliances. This guide assumes the audience has a basic familiarity with VMware software.

## Lancope

## 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.

You need to install and configure your virtual appliances in the following order:

- 1. UDP Director VE (also known as FlowReplicator VE)
- 2. FlowSensor VE
- 3. FlowCollector VE
- 4. SMC VE

If you do not follow this recommended order, when you set up the StealthWatch system, the SMC VE 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.

## **Resource Requirements**

This section provides the resource requirements for the virtual appliances.

## UDP Director VE (also known as FlowReplicator VE)

The UDP Director VE requires that the VMware server meets the following specifications:

- 4 GB RAM
- 50 GB disk space



Lancope recommends thick provisioning although thin provisioning can be used if disk space is limited.



Information	Needed	for the	vSphere	Client	Interface
-------------	--------	---------	---------	--------	-----------

Setting	ESX/vSphere Server	UDP Director VE
Login User Name		
Login Password		
IP Address		(Default = 192.168.1.2)
Netmask IP Address		(Default = 255.255.255.0)
Gateway IP Address		(Default = 192.168.1.1)

## Information Needed for the Appliance Admin Interface

Setting	UDP Replicator VE
IP Address	(Default = 192.168.1.2)
Host Name	
Network Domain Name	
NTP Server IP Address(es)	
DNS Server IP Address(es)	



### Note:

The password must be between 5 and 30 alphanumeric characters in length with no spaces. You also may use the following special characters: ...

## About the UDP Director VE

Using the same technology as the FlowReplicator appliance, the UDP Director VE (also known as FlowReplicator VE) is a virtual appliance that serves as a central collector for flow data generated by flow-enabled devices.

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

As it receives UDP packets from multiple sources, the FlowReplicator aggregates the information into a single data stream. It then modifies the packets to appear as though



they came from the original source, and sends the data to multiple destinations. Network and security administrators define the rules by which aggregated information is collected and distributed, based on source IP, destination IP and destination port.

## How to Use This Guide

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

Chapter	Description	
Chapter 2, "Installing a Virtual Appliance."	How to install VE appliances on an ESX server using vSphere Client v4.x or v5.x	
Chapter 3, "Configuring the Virtual Environment."	How to set up the virtual environment for the appliances	
Chapter 4, "Configuring a Virtual Appliance."	How to configure appliances to begin processing traffic data	

## **Documentation Icons**

This guide uses the following documentation icons.

lcon	Meaning	Includes Information
	Тір	Such as a shortcut or an easier way of performing a certain task.
	Note	You may find useful as you use this document or the StealthWatch System.
	Important	You must observe to prevent significant consequences, such as the malfunction of software.
	Caution	You must observe to prevent loss of data or damage to hardware.
	Warning	You must observe to prevent risk of personal injury.

## Abbreviations

The following abbreviations appear in this guide:

Abbreviations	Definition
DNS	Domain Name System (Service or Server)
dvPort	Distributed Virtual Port
ESX	Enterprise Server X
GB	Gigabyte
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
OVF	Open Virtualization Format
SMC	StealthWatch Management Console

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

## **Other Resources**

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

## **Related Documents**

Please refer to your StealthWatch Documentation CD for information about StealthWatch appliances and their installation and configuration.

Additional information is available in the Lancope Community Web site (<u>community.lancope.com/</u>). If you do not have login access to the web site, send an email requesting access to <u>support@lancope.com</u>.

### **NetFlow Ninjas Blog**

Lancope's *NetFlow Ninjas* blog at <u>http://www.lancope.com/blog/</u> provides a wealth of information about NetFlow, the NetFlow industry, and new StealthWatch features, as well as tips and tricks on using StealthWatch.

## StealthWatch Video Library

The StealthWatch online video library at <u>http://www.lancope.com/resource-center/videos/</u> showcases the benefits of StealthWatch for network performance and security management.

### **Contacting Support**

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

- Contact your local Lancope partner.
- Send an email requesting assistance to <a href="mailto:support@lancope.com">support@lancope.com</a>.
- Call +1 800-838-6574.
- Submit a case using the Support form on the Lancope Customer Community web site (https://community.lancope.com)

You will need to provide the following information:

- Your name
- Your company name
- Location





## **Document Feedback**

If you have comments about this document, please contact Lancope at <a href="mailto:support@lancope.com">support@lancope.com</a>. We appreciate your feedback.





# INSTALLING A VIRTUAL APPLIANCE

# OVERVIEW



#### Note:

For instructions on how to install a StealthWatch physical appliance, see the *StealthWatch System v6.5x Hardware Installation Guide*.

This chapter describes how to install the virtual appliances using VMware vSphere Client v4.x or v5.x.



#### 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.** Adding a Resource Pool
- **3.** Installing the Virtual Appliance

# 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 diagram and tables shown in this section to configure your network so that the appliances can communicate through the network.

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

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP389
- UDP 514
- UDP 2055
- UDP 3514
- UDP 6343

## **Communication Ports**

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

From (Client)	To (Server)	Port	Protocol
Admin User PC	All appliances	TCP/443	HTTPS
All appliances	Network time source	UDP/123	NTP
Active Directory	SMC	TCP/389, UDP/389	LDAP
Cisco ISE	SMC	TCP/443	HTTPS
- continued -			

From (Client)	To (Server)	Port	Protocol	
Cisco ISE	SMC	UDP/3514	SYSLOG	
External log sources	SMC	UDP/514	SYSLOG	
FlowCollector	SMC	TCP/443	HTTPS	
SLIC	SMC	TCP/443 or proxied connection	HTTPS	
UDP Director (also known as FlowReplicator)	FlowCollector - sFlow	UDP/6343	sFlow	
UDP Director (also known as FlowReplicator)	FlowCollector - NetFlow	UDP/2055*	NetFlow	
UDP Director (also known as FlowReplicator)	3 <sup>rd</sup> Party event management systems	UDP/514	SYSLOG	
FlowSensor	SMC	TCP/443	HTTPS	
FlowSensor	FlowCollector - NetFlow	UDP/2055	NetFlow	
IDentity	SMC	TCP/2393	SSL	
NetFlow Exporters	FlowCollector - NetFlow	UDP/2055*	NetFlow	
sFlow Exporters	FlowCollector - sFlow	UDP/6343*	sFlow	
SMC	Cisco ISE	TCP/443	HTTPS	
SMC	DNS	UDP/53	DNS	
SMC	FlowCollector	TCP/443	HTTPS	
SMC	FlowSensor	TCP/443	HTTPS	
SMC	IDentity	TCP/2393	SSL	
SMC	Flow Exporters	UDP/161	SNMP	
User PC	SMC	TCP/443	HTTPS	

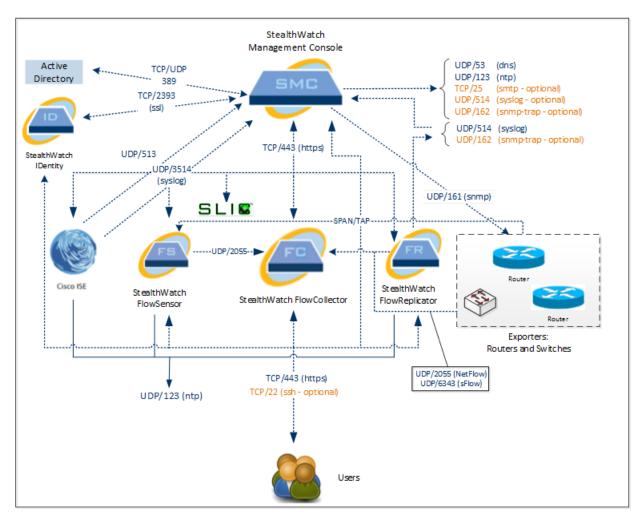
\*This is the default NetFlow port, but any UDP port could be configured on the exporter.

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

From (Client)	To (Server)	Port	Protocol
All appliances	User PC	TCP/22	SSH

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

The following diagram shows the various connections used by the StealthWatch System. The ports marked as *optional* may be used according to your own network needs.



## Lancope



### Note:

The screen images are for VMWare v5.0 and may appear slightly different from your screens, but the commands are the same.

## 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 a StealthWatch virtual appliance.



#### 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.

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

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



2. Enter the IP address of the ESX server and your login credentials, and then click Login. The Getting Started page opens.



**3.** In the Inventory tree on the left, right-click the ESX server IP address, and then select **New Resource Pool** from the popup menu.

File	Edit	View	Inventory Administration	Plug-ins Help
4			Home 🕨 🚮 Inventory	Inventory
6	6			
		12.0.00		
Ŧ	1	- 61	New Virtual Machine	Ctrl+N <sup>n</sup> VN
		6	New Resource Pool	Ctrl+0
		2	Enter Maintenance Mode	
			Rescan for Datastores	
			Add Permission	Ctrl+P run
		6	Shut Down	eso
		D.	Reboot	es a
			Report Summary	al
			Report Performance	a
		_	Open in New Window	Ctrl+Alt+N

The Create Resource Pool dialog opens.

🕢 Edit Settings	×
Name: la	ncope2
CPU Resources	
Shares:	Normal • 4000 -
Reservation:	0 🕂 MHz
	Expandable Reservation
Limit:	∫ 56636 <u>→</u> MHz
	✓ Unlimited
Memory Resource	ies
Shares:	Normal
Reservation:	~ 8192 + MB
	Expandable Reservation
Limit:	↓ 177617 ÷ MB
	Unlimited
A Remaining res	ources available
Help	OK Cancel

- 4. In the **Name** field, type the name you want to use to identify this resource group.
- 5. Do not change any of the settings in the CPU Resources section.
- 6. 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 6.
  - Change the Limit field to at least **4 GB** (**8 GB** recommended).

• Click the **Unlimited** checkbox to clear it.

### CAUTION:

Less than 4 GB of memory is not supported. If less than 4 GB is allocated, a Low Memory alarm will be triggered, and no flows will be stored in the database.

7. 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.

CPU		Memory		
Configured Reservation:	0 MHz	Configured Reservation:	8292 MB	
Reservation Type:	Expandable	Reservation Type:	Expandable	
Used Reservation:	0 MHz	Used Reservation:	0 MB	
AvailableReservation:	31960 MHz	AvailableReservation:	39357 MB	

9. Continue with the next section, "Installing the Virtual Appliance."

# INSTALLING THE VIRTUAL APPLIANCE

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

- 1. Unzip the virtual appliance software (OVF) file that you downloaded earlier.
- 2. On the vSphere client menu, click File > Deploy OVF Template.

File	Edit	View	Inventory	Adminis
	New			•
	Dep	oy OVI	F Template.	
	Expo	ort		F
	Repo	ort		+
	Brov	vse VA	Marketplac	e
	Print	t Maps		Þ
	Fxit			

The Deploy OVF Template wizard opens.

💋 Deploy OVF Template	
Source Select the source location.	
Source OVF Template Details Name and Location Host / Cluster Resource Pool Disk Format Ready to Complete	Deploy from a file or URL C:Users'bfield'Documents'OVF files'SMC-VE-6.2.0-2012.02 Browse Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
Help	<back next=""> Cancel</back>

3. Click **Browse**, and then navigate to select the virtual appliance OVF file.

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

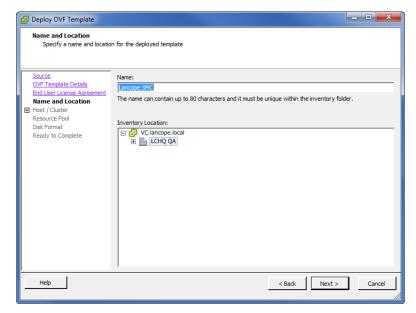
Deploy OVF Template				- • ×
OVF Template Details Verify OVF template details.				
Source OVF Template Details End User License Agreement Name and Location El Host / Cluster Resource Pool Disk Format Ready to Complete	Product: Version: Vendor: Publisher:	Lancope SMC		
	Download size: Size on disk:	1.8 GB		
	Description:	3.1 GB (thin provisioned) 50.0 GB (thick provisioned)		
Help			< Back Next >	Cancel

5. Click Next. The End User License Agreement opens.

Deploy OVF Template	
End User License Agreemen Accept the end user license	
Source OVF Template Details End User License Agreemu Name and Location II Host / Cluster Resource Pool Disk Format Ready to Complete	YOU MUST CAREFULLY READ THE TERMS AND CONDITIONS OF THIS CLICK WRAP SOFTWARE LICENSE AGREEMENT ('AGREEMENT') BEFORE INSTALLING OR USING THE SOFTWARE OR DOCUMENTATION (THE 'SOFTWARE'). BY CLICKING 'ACCEPT ALL LICENSE AGREEMENTS' BELOW AND/OR OTHERWISE PROCEEDING WITH INSTALLITON OR USE OF THE SOFTWARE, YOU ACRONOWLEDGE YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. THEN DO NOT LICK 'ACCEPT ALL LICENSE AGREEWENTS' BELOW AND DO NOT INSTALL OR USE THE SOFTWARE, YOU O'CUSTOMER, 'YOU' OR YOUR' IN THIS AGREEMENT ON BEHALF OF AN OGRANIZATION, ALL REFERENCES TO 'CUSTOMER, 'YOU' OR YOUR' IN THIS AGREEMENT WILL MEAN COLLECTIVELY THE ORGANIZATION AND THE INDIVIDUAL END USER OF THE SOFTWARE. IN CORGANIZATION AND THE INDIVIDUAL END USER OF THE SOFTWARE. ALL REFERENCES TO 'LANCOPE' OR 'WE' WILL MEAN LANCOPE, INC., A DELAWARE CORPORATION. FOR GOOD AND VALUABLE CONSIDERATION, THE RECEIPT AND SUFFICIENCY OF WHICH ARE ACKNOWLEDGED, LANCOPE AND CUSTOMER AGREE AS FOLLOWS: 1. LICENSE OF SOftware. This is a license to the Software. The Software is provided to you subject to the following terms and conditions which define what you can and cannot do with the Software, as well as limitations on waranties and remedies. 2. Grant of License; Inteleval Property Rights. 2.1. LICENSE to Software. Lancope hereby grants to Customer a personal, non-transferable, non-exclusive, world-wide, perpeting updates, upgrades, changes or enhancements that
۰ III ا	Accept
Help	< Back Next > Cancel



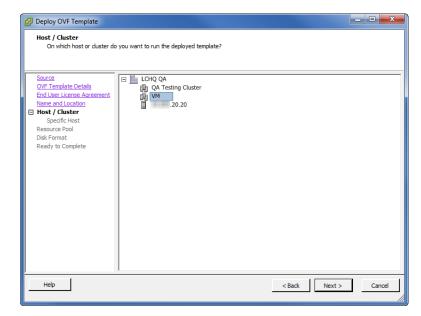
6. After reviewing the information, click **Accept**, and then click **Next**. The Name and Location page opens.



- 7. If desired, change the name for the virtual appliance as it will appear in the Inventory tree, and then click **Next**.
  - a. If the Specify a Specific Host page opens, select the host or cluster where the virtual appliance will reside.

Deploy OVF Template	
Specify a Specific Host On which host within the d	uster should the deployed template run?
Source OVF Template Details End User License Agreement Name and Location Host / Cluster Specific Host Resource Pool Disk Format Ready to Complete	Choose a specific host within the duster. On dusters that are configured with Whare HA or Manual mode VMware DRS, each virtual machine must be assigned to a specific host, even when powered off. Select a host from the list below: Host Name 0.18 0.19
Help	< Back Next > Cancel

b. If the Host/Cluster page opens, select the host or cluster where the appliance will reside.



8. Click Next. The Resource Pool page opens.

Deploy OVF Template	<b>-</b> - <b>-</b>
Resource Pool Select a resource pool.	
Source QVF Template Details End User License Agreement Name and Location ☐ Host / Cluster Resource Pool Datastore Disk Format Network Mapping Ready to Complete	Select the resource pool within which you wish to deploy this template. Resource pools allow hierarchical management of computing resources within a host or duster. Virtual machines and child pools share the resources of their parent pool. WM Appliances S. J.OGroup S. Vic.ZGroup S. Vic.ZGroup Desktops Servers S. vMotionEven S. vMotionOdd
Help	< Back Next > Cancel

## Lancope

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

Where do you want to stor	e the virtual machine fi	les?					
Source	Select a datastore in v	which to store th	e VM files:				
OVF Template Details End User License Agreement	Name	Capacity	Provisioned	Free	Туре	Thin Provisioning	Acces
Name and Location	[qa-storage-isc	557.75 GB	331.01 GB	288.48 GB	VMFS	Supported	Multip
Host / Cluster	[qa-storage-02]	299.75 GB	122.45 GB	177.30 GB	VMFS	Supported	Multip
Resource Pool	[qa-storage03]	1.64 TB	957.15 GB	781.57 GB	VMFS	Supported	Multip
Datastore	[qa01]	949.75 GB	957.27 GB	190.03 GB	VMFS	Supported	Multip
Disk Format	[qa02]	949.75 GB	979.85 GB	171.64 GB	VMFS	Supported	Multip
Network Mapping Ready to Complete	[datastore1(2)]	460.25 GB	421.55 GB	141.60 GB	VMFS	Supported	Single
							•



Lancope

The Disk Format page opens.

Deploy OVF Template Disk Format In which format do you we	nt to store the virtual diaks?
Source OVF Template Details End User License Agreement Name and Location Host / Cluster Resource Pool Datastore <b>Disk Format</b> Network Mapping Ready to Complete	Information about the selected datastore: Name: datastore 1 (2) Capacity: 460.3 GB Free space: 11.6 GB Select a format in which to store the virtual machines virtual disks: (° Thin provisioned format The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disk. Estimated disk usage: 3.1 GB (° Thick provisioned format All storage is allocated immediately. Estimated disk usage: 50.0 GB
Help	< Back Next > Cancel



Note:

The vSphere Client v5 has two thick-provisioned formats: Lazy Zeroed and Eager Zeroed. Choose the one that best suits your disk storage needs. Use the Thin Provision format only if your disk space is limited. For further information, refer to your VMware documentation.

**11.** On the Disk Format page, select **Thick provisioned format**, and then click **Next**. The Network Mapping page opens.

💋 Deploy	OVF Template			
	rk Mapping lat networks should the de	eployed template use?		
	mplate Details er License Agreement	Map the networks used in this OVF t	emplate to networks in your inventory	
	and Location	Source Networks	DestinationNetworks	
Host /		VM Network	.0.0/19	
	ore	Description:		
		The VM Network network		*
Help			< Back Next	> Cancel

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

Network Mapping What networks should the deployed template use?			
Source OVF Template Details End User License Agreement		template to networks in your inventory	
Name and Location	Source Networks	DestinationNetworks	
Host / Cluster     Resource Pool	VM Network	.0.0/19	
Datastore			
Disk Format			
Network Mapping			
Ready to Complete			
		and an a second s	

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

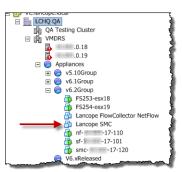
Deploy OVF Template Ready to Complete Are these the options you	want to use?
Source OVF Template Details End User License Acreement Name and Location III Host / Cluster Resource Pool Datastore Disk Format Network Mapping Ready to Complete	When you click Finish, the deployment task will be started.         Deployment settings:         OVF file:       C:\Users\bfeld\Documents\OVF files\SMC-VE-6.2.0-2012.02.06.2131-1-OVF\Lancope         Download size:       1.8 GB         Size on disk:       3.1 GB         Name:       Lancope SMC         Folder:       LOPQ QA         Host/Cluster:       VM         Specific Host:       0.19         Resource Pool:       v6.2Group         Datastore:       Thick.Provisioning         Network Mapping:       "VM Network" to "
Help	< m + Cancel

14. After reviewing the settings, click Finish. A progress dialog opens.

🕜 12% Deploying Lancope SMC
Deploying Lancope SMC
Deploying disk 1 of 1 from C:\Users\bfield\Documents\OVF files\SMC-VE-6.2.0-2012.02.06.2131-1-0VF\Lancope_SMC-disk1.vmdk
Cancel
2 minutes and 31 seconds remaining



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



- **16.** Have you completed all of the procedures in this chapter for all of the FlowReplicators?
  - ▶ If yes, continue with Chapter 3, "Configuring the Virtual Environment."
  - If no, return to "Adding a Resource Pool" on page 19 and repeat all of the procedures in this chapter for the next virtual appliance. Then go to "Configuring the Virtual Environment" on page 31.

## Lancope°

# CONFIGURING THE VIRTUAL ENVIRONMENT

# OVERVIEW

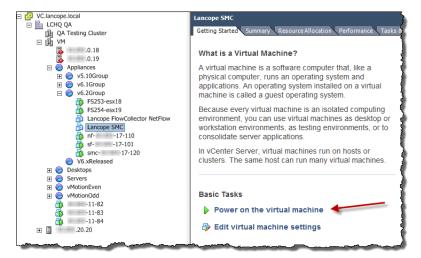
After you install the StealthWatch VE appliances, you are ready to configure the virtual environment for them. This process involves completing the following procedures as detailed in this chapter:

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

# CONFIGURE THE IP ADDRESSES

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

1. If necessary, launch the vSphere Client software and log in. The Getting Started page opens.



- **2.** In the Inventory tree, select the StealthWatch virtual appliance you want to configure.
- **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.
- Decrease the memory allocation and reservation to 4 GB.

### CAUTION:



Do not reduce the memory reservation so that it is lower than the allocation, and never reduce the setting to less than 4 GB. For guidance, see the chart for the applicable appliance in "Resource Requirements" on page 6.

**4.** Click the **Console** tab. Allow the virtual appliance to finish booting up. The virtual appliance Administrative IP Address page opens.

Enter the SMC Admin	System Config histrative IP Addre		
.1.11_			
	< 0X >	<cancel></cancel>	



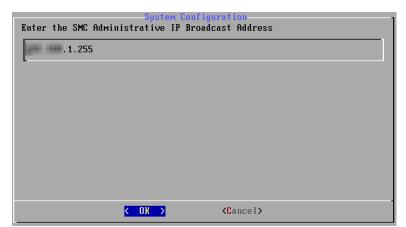
### Note:

You may need to enable the Full Screen Mode (Ctrl+Alt+Enter) to view the entire screen.

- 5. Click on the page, and then enter the IP address for the virtual appliance.
- 6. Select **OK**, and then press **Enter**. The IP Netmask page opens with the default network mask IP address.

System Config Enter the SMC Administrative IP Netma	urationsk
. 255.0	
<mark>&lt; 0X &gt;</mark>	<cancel></cancel>

- 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 **Enter** to continue.

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

Enter the SMO	C Administrative II	Configuration P Gateway Address	
.1.1			
-			
	< 0K >	<cancel></cancel>	

- 9. 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.



- **10.** Review the information. Are the settings are correct?
  - If yes, go to step 11.
  - If no, go to step 13.
- **11.** Press **Enter**. The system restart page opens.

System Configuration
Primary network parameters have been modified. Please note that modifying the settings for the primary network interface may disable network access to this system which will require console access to repair. This system will now be restarted to implement these changes.
<mark>⊂ x</mark> o

- **12.** Press **Enter**. The system restarts and implements the changes. On completion, a login prompt appears. Go to "Change the Default User Passwords," next in this chapter.
- **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.

Lancope.

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 should 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. 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.

Management <mark>Password</mark> TrustedHosts	Change the Management Port Networking Change the password for the current user Change the Trusted Hosts
Advanced	Advanced Operations

#### 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.

<pre></pre>	Managemen Password TrustedHo. Advanced	Change the password for the current user
		<pre>&lt; OK &gt; <cancel></cancel></pre>
next two prompts.	At the prompt, type : next two prompts.	in your current password. Then type your new password at t

**3.** Type the current password, and then press **Enter**.

The prompt for a new password appears.

Management Password Trustedfosts Advanced	
	OK > <cancel></cancel>
<u> </u>	

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

#### Note:



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.

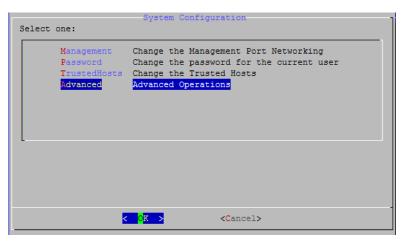
< OK >	<cancel></cancel>
L	
At the prompt, type in your current passwo next two prompts.	ord. Then type your new password at the
Changing password for sysadmin.	
(current) UNIX password:	
Password:	
Retype new password:	
passwd: password updated successfully	
Password was successfully changed.	
Press return to continue.	

- 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. .

FactoryDefaults RefreshImage	Restore System to its Factory Defaults Refresh the System Image
InterfaceSettings	
	Expand Platform Data Storage
RootShell	Open a Root Shell
< <b>0</b> 7	<cancel></cancel>

A prompt for the root password appears.

1	ſype	the	root	password	at	the	prompt	open	root	shell.
Passv	word:									

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



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

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

5. Select **Password**, and then press **Enter**. The password prompt appears.

Select on	e:	
м	anagement	Change the Management Port Networking
P	assword	Change the password for the current user
	rustedHosts	Change the Trusted Hosts
A	dvanced	Advanced Operations
L		
		OK > <cancel></cancel>
	<u> </u>	Cancers
the next	two prompts.	type in the new password.
sword:	,	at the second

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

	< ok >	<cancel></cancel>	
L			
At the next two prom	ots, type in the n	ew password.	
Password:		tew password.	
BAD PASSWORD: is too Retype new password:	simple		
passwd: password upd	ated successfully		
Password was success	fully changed.		
Press return to cont	inue.		

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

At the next two prompts, Password: Retype new password: password updated	type in the new password.
Password was successfully Press return to continue exit	- 7 changed.

A message appears indicating that the password was updated successfully.

- 8. When your password change is successful, type exit, and then press Enter. You have now changed both of your default sysadmin and root passwords.
- 9. Press Ctrl+Alt to exit the console environment.
- **10.** Have you completed all of the procedures in this chapter for all of the virtual appliances?
  - If yes, continue with "Configuring a Virtual Appliance."
  - If no, return to "Configure the IP Addresses" on page 32 and repeat all of the procedures in this chapter for the next virtual appliance. Then, go to the "Configuring a Virtual Appliance" on page 43.



# CONFIGURING A VIRTUAL APPLIANCE

# OVERVIEW

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

Please refer to the checklist on page 6 for the information you will need before proceeding.

### **Process Overview**

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

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

# CONFIGURING THE INDIVIDUAL APPLIANCES

Initial configuration of every appliance is done with the Appliance Setup Tool. The first time you access the appliance the Appliance Setup Tool is displayed. Depending on your system, you should configure the FlowSensors and FlowCollectors before the UDP Directors (also known as FlowReplicators), 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 "Before You Begin" on page 6.



#### Note:

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

To configure an appliance, complete the following steps:

- 1. In the address field of your browser, type **https:**// followed by the IP address of the virtual appliance, and then press **Enter**.
- 2. The admin login page opens. Type **admin** and **lan411cope** (both case sensitive), and then click **Login**. Go to step 4.



**3.** For the SMC VE, the landing page opens.



#### To log in, do the following:

User Name	
User Name	4
Password	
Password	_ ₽
	Sign in

- a. In the User Name field, type **admin**.
- b. In the Password field, type **lan411cope**.
- c. Click Sign In.
- 4. The Welcome page opens. Click **Continue**.

Welcome to the StealthWatch Appliance Setup Tool! This lool will help you configure your StealthWatch appliance step by step.
<ul> <li>Before you begin:</li> <li>Ensure your firewalls and ACLs will allow access.</li> <li>Gather the host name for the appliance and IP addresses for the following: <ul> <li>Appliance</li> <li>Subnet mask</li> <li>Default and broadcast gateways</li> <li>NTP and DNS servers</li> </ul> </li> </ul>
For more information, refer to your StealthWatch System documentation.

The Management Network Interface page opens.

StealthWatch Management C Appliance Setup Serial Number: SMCVE-VM ware- Version: 6.5.0 Build: 2014 02:25.0336-1	eonsole VE			STEALTH WATCH'
Step 1: — Management Network Interface	Management	Network Inte	erface	
Step 2: Host Name and Domain			and the network. Default network s onfer with your network administrat	
Step 3: DNS Settings	Interface Name:	eth0	Interface MAC Address:	64:d5
Step 4: NTP Settings				
Review: Review Your Settings				
				Next →

5. Review the settings you previously entered, and then click **Next**. The Host Name and Domain page opens:

StealthWatch Management Co Appliance Setup Serial Number: SMCVE-VMware- Version 8:53 Bulik: 2014.02.25 0338-1	onsole VE		STEALTH WATCH'
Step 1: Management Network Interface	Host Name a	nd Domain	
Step 2: Host Name and Domain	Enter identifying inform		
Step 3: DNS Settings		smc-01	
• Step 4: NTP Settings			
Review: Review Your Settings			
	🗲 Back		Next →



6. In the appropriate fields, type the host name and the network domain name, and then click Next. The DNS Settings page opens.



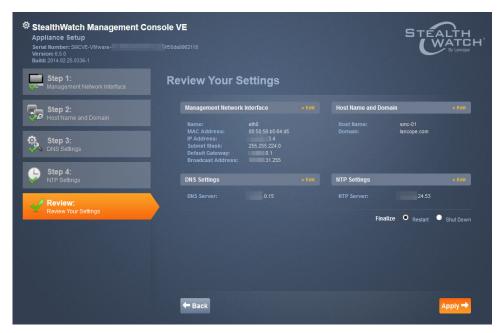
7. Click the + button, and then type the IP address of the DNS server. Click Next. The NTP Settings page opens.

StealthWatch Management Co Appliance Setup Serial Number: SUCVE-VII/ware- Version: 65.0 Build: 2014.02.25.0336-1	bnsole VE dx9962118	STEALTH WATCH
Step 1: Management Network Interface	NTP Settings	
Step 2: Host Name and Domain	Select or enter the IP address(es) or name(s) of your network time protocol server(s) server(s) used for other devices that (eed information to the StealthWatch FlowCollecto server, click the + button. To delete a server, select the corresponding checkbox, and th	r for NetFlow. To add a
Step 3: DNS Settings	Delete NTP Server	
Step 4: NTP Settings	4.53	
Review: Review Your Settings		
	+ Back	Next 🔿

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.



9. Click Next. The Review page opens.



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



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

StealthWatch Management Co Appliance Setup Serial Number: SMCVE-VMware- Werston: 6:5 0 Build: 2014 0:225 0:338-1	rsodas9662118	STEALTH
Step 1: Management Network Interface	Complete	
Step 2: Host Name and Domain	The system has been restarted. Click Next to continue. Please allow a few minutes for your new system settings to take effect.	
Step 3: DNS Settings		
Step 4: NTP Settings		
Review: Review Your Settings		
		Next 🔿

- **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 or the SMC landing page opens.
- **13.** Enter the login credentials if needed, and then click **Login**.
- 14. Do you have any other appliances to configure?
  - If yes, return to Step 1 and repeat this procedure for the next appliance. Remember to configure the primary SMC last.
  - If no, go to the next step.
- **15.** 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. Change the Admin Password
- 4. Configure UDP Director VE Rules
- 5. Restart the Virtual Appliance

### Log in to the Appliance Administration Interface

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



#### Note:

The supported browsers for StealthWatch are Internet Explorer version 9 and later and Firefox version 3 and later.

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

	ATCH <sup>®</sup> By Lancope
lowCollector for	
	Login >:

**2.** In the **Username** field, type **admin**.

3. In the **Password** field, type the default password **lan411cope**.



#### Important:

To help ensure security, change the admin password after you finish configuring the virtual appliance (**Configuration > Change Password**).

4. Click Login. The Appliance Admin interface Home page opens.

StealthWatch Management Console VE				• ≡
i Info! This page automa	atically refreshes every minute - last refres	hed at 13:35:22.		
System				
IP Address:	.26.141			
Host name:	r6-6-smc-v	Domain name:	eng.lancope.local	
Total Memory:	8G			
VM Server Memory:	1G reserved, unlimited	Load Average: VM Server	0.00, 0.03, 0.05	
Free Memory:	3.43G	CPU:	1.02GHz reserved, unlimited	
		Uptime:	2 days, 21:36:04	
Version:	6.6.0			
Build:	2014.09.09.1223-1	Platform:	VMware Virtual Platform	
		Serial No.:	SMCVE-VMware-4	

5. Continue with the next section, "Configure the System Time."

## Configure the System Time

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



#### CAUTION:

Use the same NTP server used for the FlowCollectors 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.

System Time and N	TP			
<b>A</b> Warning: You should restart the system after applying changes to system time settings.				
NTP Server	I			
NTP Server		Delete		
.3.35				
Select a NTP server to add:		¥		
Enter a server name to add:			Add	
Reset Apply				
Time Zone				

**2.** Scroll down to the Time Zone section of the page to configure the virtual appliance system time.

Time Zone	
Current Server Time Zone:	Etc/UTC
Select Continent:	· ·
Select Country:	•
Select Timezone:	
Reset Apply	1

- **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.

Current Server Time Zone:	Etc/UTC	
Select Continent:	North America	~
Select Country:	United States	~
Select Timezone:	America/New_York Eastern Standard Time [GMT-5]	۷

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

Are You Sure?	×
You should restart the s after making changes to you sure you wish to ap	these settings. Are
	OK Cancel

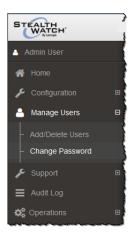
- 5. Click OK.
- 6. Continue to the next section, "Change the Admin Password."

### Change the Admin Password

To help ensure the security of your network, change the default admin user password. You will restart the system after this procedure.

To change your password, complete the following steps:

1. In the Appliance Admin interface navigation pane, click the plus sign (+) beside Manage Users and then click Change Password.





The Change Password page opens.

	is password by at least 4 characters.
Enter current password:	•••••
Enter new password:	
Confirm new password:	

- 2. Do the following in the applicable fields:
  - Type the current password, lan411cope.



#### Note:

- Type the new password.
- Type the new password again to confirm it.
- To activate click the **Apply** button.

Change Password				
<ul> <li>i Password Format (Case-Sensitive)</li> <li>Must be between 8 and 30 characters.</li> <li>Must be different from the previous password by at least 4 characters.</li> </ul>				
Enter current password:	•••••			
Enter new password:				
Confirm new password:	•••••			
Apply				

**3.** Click **Apply** to change the password. The password change confirmation appears.

Password successfully changed.

4. Continue with the next section, "Configure UDP Director VE Rules."

# Configure UDP Director VE Rules

For the UDP Director VE (also known as FlowReplicator VE), you need to configure the exporter to send flows to be forwarded to the IP address of eth0. The FlowReplicator will then forward these from eth0 while preserving the original IP and MAC address of each exporter for forwarded packets.



#### Note:

For promiscuous reception, Lancope recommends that you use a span filter for all traffic of interest.

The network must allow traffic on the ports being used from the exporters to the FlowReplicator and then to the receivers (ACLs).



To configure the rules for the FlowReplicator, complete the following steps:

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



The Forwarding Rules page opens.

Forv	varding Rules				
Rule #	Description	Source IP Address:Port List	Destination IP Address	Destination Port Number	Delete
1.	NFLOW .::	All:2055 .::	26.103	2055	
2.	SFLOW	All:6343 .::	.26.105	6343	
Add	Арріу				

- 2. In the Description field, type a description of the rule.
- **3.** In the Source IP Address:Port List field, type the IP address of the device that sends data to the FlowReplicator followed by the port number through which the data will be sent. Use the following syntax:

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

2	-

Note:

To receive all traffic from any device from a specific port, type **All:[port number]**. For example, type **All:3123** to receive all data from port 3123.

You can also use CIDR (Classless Inter-Domain Routing) notation to enter a range of IP addresses. For example, type **172.200.1.0**/ **16:9000** 

4. To add another entry, press **Enter** and type the next IP address and port number.



- 5. In the Destination IP Address field, type the IP address of the device that receives data from the FlowReplicator.
- **6.** In the Destination Port Number field, type the port number for the receiving device.
- 7. If you have more than one device sending data to the FlowReplicator to be forwarded to another receiving device, click **Add**.

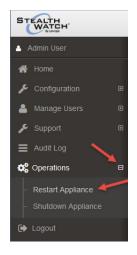
A new line appears where you can enter the settings. Repeat this step until you have entered all devices for this FlowReplicator.

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

### **Restart the Virtual Appliance**

To restart the virtual appliance, complete the following steps:

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



#### The confirmation dialog opens.

Please Confirm	×
Are you sure you want to restart the appliance?	
It may take a while.	
No	es

- 2. Click Yes.
- **3.** After restarting, the UDP Director VE will begin collecting data and sending it to the configured destinations.



# Lancope

# Lancope°

©2015 Lancope, Inc. All rights reserved. Lancope, StealthWatch, and other trademarks are registered or unregistered trademarks of Lancope, Inc. All other trademarks are properties of their respective owners. SW-Install-Config-UDVE-v0670-03232015

www.lancope.com