



StealthWatch[®] System Disaster Recovery Guide Recommendations and Procedures

System version 6.7.x

Disaster Recovery Guide: StealthWatch System v6.5.x

© 2015 Lancope, Inc. All rights reserved.

Document Date: April 28, 2015

Trademarks

Lancope, StealthWatch, and other trademarks are registered or unregistered trademarks of Lancope, Inc. All other trademarks are properties of their respective owners.



CONTENTS

- 1 - INTRODUCTION 5**
 - Overview 5
 - Audience 5
 - How to Use This Guide 6
 - Documentation Notifications..... 6
 - Abbreviations 6
 - Other Resources 7

- 2 - SYSTEM CONFIGURATION FILES 8**
 - Overview 8
 - Configuration File 9
 - When Should You Back Up the Configuration File? 9
 - What is Backed Up?..... 9
 - What is Not Backed Up? 10
 - Backing Up the Configuration File 11

- 3 - STEALTHWATCH DATABASE..... 14**
 - Overview 14
 - Appliance Database 14
 - When Should You Back Up the Appliance Database? 15
 - What is Backed Up in the Database?..... 15
 - Backing Up the Database..... 16

- 4 - RESTORING THE STEALTHWATCH SYSTEM 20**
 - Overview 20
 - Restoring Your Appliance System Configuration 20
 - Restoring the StealthWatch Appliance Database 22



INTRODUCTION

OVERVIEW

With technology, disaster takes many shapes. At its mildest, a data file might become corrupt, or a piece of hardware might fail. At its worst, natural catastrophes can occur, such as hurricanes, completely destroying your physical infrastructure and wiping out all data critical to your business operations. Clearly, having a disaster recovery plan in place for all of your systems, including a remote storage site for backups, is imperative.

This document describes Lancope's best practice recommendations for performing regular backups of the StealthWatch system to:

- Help ensure continuous monitoring of your network
- Prevent data loss

In addition, this document provides procedures for performing backups as well as procedures for restoring information when necessary.

Warning: Consider geographic location when you choose your remote storage facility. If it is just down the road, a regional disaster could wipe out both sites.

Audience

This document is intended for system administrators and other personnel who are responsible for maintaining the StealthWatch system.



How to Use This Guide

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

Chapter	Description
2 - System Configuration Files	How to backup configuration files for all appliances
3 - StealthWatch	How to back up the database for all appliances
4 - Restoring the StealthWatch System	How to restore your system with your configuration files and the databases

Documentation Notifications

This document uses the following notifications to denote significant information.

Type	Description
Warning	Information you should consider to prevent physical injury, loss of data, or other similar problem
Important	Information to prevent significant consequences, such as the malfunction of software
Note	Additional information that you may find useful
Tip	Helpful information, such as shortcuts or easier ways of performing certain tasks

Abbreviations

This document uses the following terms and their abbreviations.

Acronym	Term
DNS	Domain Name System (Service or Server)
SMB	Server Message Block
SMC	StealthWatch Management Console
TGZ	Tape archive gzip file
VE	Virtual Edition



Other Resources

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

Related Documents

For additional information, customers can go to the Lancope Customer Community web site (community.lancope.com). If you do not have login access to the Customer Community, send an email requesting access to support@lancope.com.

NetFlow Ninjas Blog

Lancope's *NetFlow Ninjas* 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.

StealthWatch Video Library

The StealthWatch online video library (<http://www.lancope.com/resource-center/videos>) 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 support@lancope.com.
- Call +1 800-838-6574 (between 8:30 AM and 6:30 PM Eastern Standard Time).
- Submit a case using the Support form on the StealthWatch User 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 support@lancope.com. We appreciate your feedback.



SYSTEM CONFIGURATION FILES

OVERVIEW

This section discusses the options available for backing up StealthWatch system configuration files for the following appliances:

- SMC and SMC VE
- FlowCollector (NetFlow, sFlow) & FlowCollector VE
- FlowSensor and FlowSensor VE
- FlowReplicator and FlowReplicator VE

Notes:

- The appliance continues to monitor your system during the backup processes.
- Images for the Appliance Administrative interface are from v6.5.3.

Important: You must back up each appliance's configuration file. Simply backing up the SMC configuration file does not fully restore the configuration of the appliances connected to it.



CONFIGURATION BACKUP

The configuration of an appliance includes all of the settings for your appliance. It does not include any of the data that the system collects such as flows or alarms. The appliance automatically backs up its configuration and stores it locally every day. You can also back up the configuration file manually. In either case, the same information is saved.

Note: A full backup of a FlowCollector or SMC involves backing up the appliance configuration and the appliance database. (See page 14.) You will need both backups to restore these appliances fully.

When Should You Back Up the Appliance Configuration?

We recommend that you save the StealthWatch appliance configuration file (TGZ) to a remote location as follows:

- After you initially install the appliance
- Before and after any upgrades
- Whenever you make major changes to the appliance

The file is not large and takes only a few minutes to save.

What is Backed Up?

The content of the configuration file can vary depending on the type of appliance. For example the SMC configuration file includes information about the FlowCollectors sending data to it. Other appliances would not have this information. Another example is the FlowReplicator, which includes the settings for its rules. These rules are not part of other appliance configuration files. In other words, the configuration file includes all the files needed to restore an appliance's unique settings.

In general, though, the TGZ file includes the following:

- Trusted Hosts
- Appliance Users
- Host Policies
- Alarm configuration (not data)
- Security Events (including mitigation configurations)
- Scheduled Report configurations (not the reports themselves)
- Static Routes
- ARP Caches



Lancope

- StealthWatch Appliances:
 - Subnet Mask
 - Gateway Address
 - Host Name
 - Domain Name
 - DNS Server(s)
 - Device Type
 - IP Address

What is Not Backed Up?

The TGZ file does *not* include the following information such as:

- Individual host policies
- Traffic data
- Flow data
- Alarm data
- Mitigation data

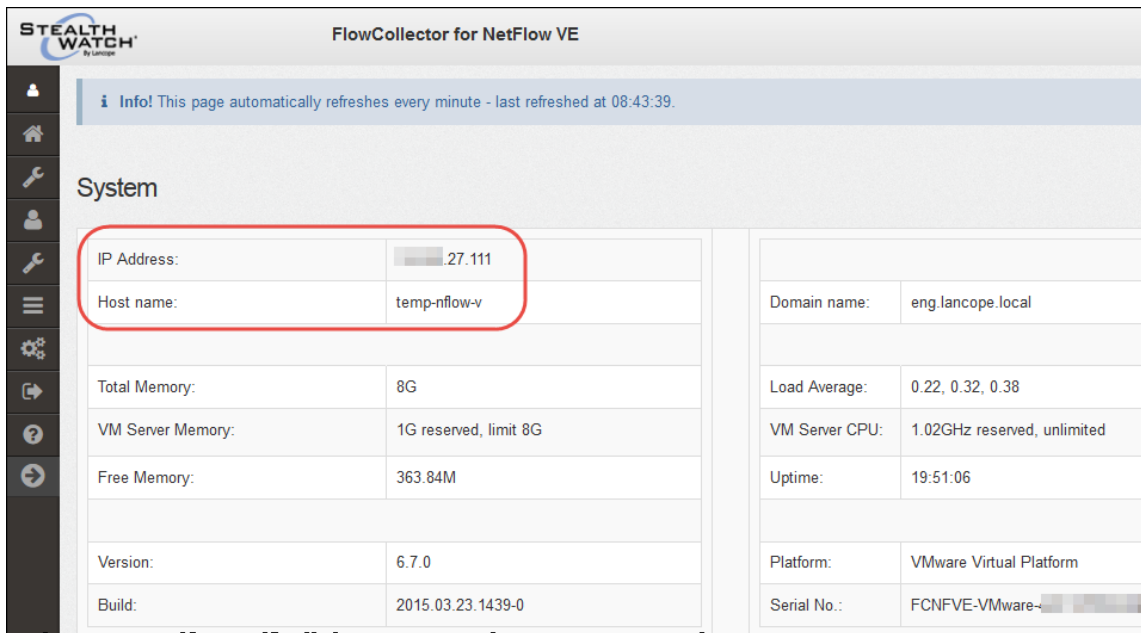


BACKING UP THE CONFIGURATION

In order to restore your system after a disaster, you need to have a backup of the appliance configuration.

To back up an appliance configuration, complete these steps:

1. Log in as the admin user to the Appliance Administration Interface. The Home page appears.

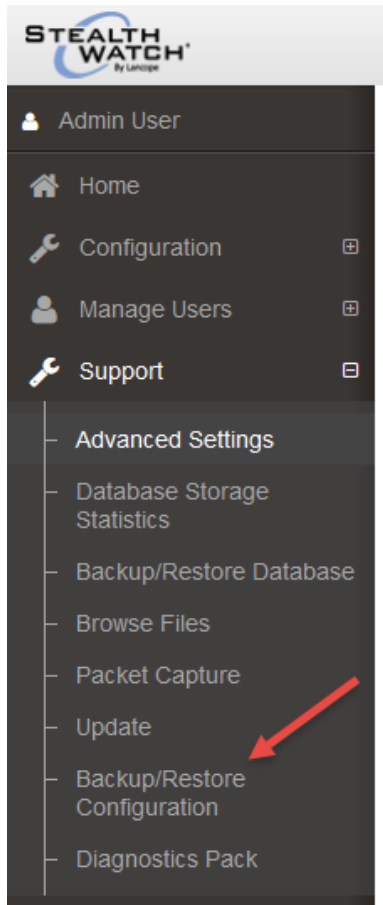


The screenshot displays the 'FlowCollector for NetFlow VE' administration interface. The page title is 'FlowCollector for NetFlow VE' and the logo 'STEALTH WATCH By Lancope' is visible in the top left. A navigation pane on the left contains icons for Home, Tools, Users, Settings, and Refresh. The main content area shows system information under the heading 'System'. A red box highlights the 'IP Address' and 'Host name' fields. The IP Address is partially obscured by a grey box, showing only '.27.111'. The Host name is 'temp-nflow-v'. Other system information includes Domain name: eng.lancope.local, Total Memory: 8G, VM Server Memory: 1G reserved, limit 8G, Free Memory: 363.84M, Version: 6.7.0, Build: 2015.03.23.1439-0, Load Average: 0.22, 0.32, 0.38, VM Server CPU: 1.02GHz reserved, unlimited, Uptime: 19:51:06, Platform: VMware Virtual Platform, and Serial No.: FCNFVE-VMware-.

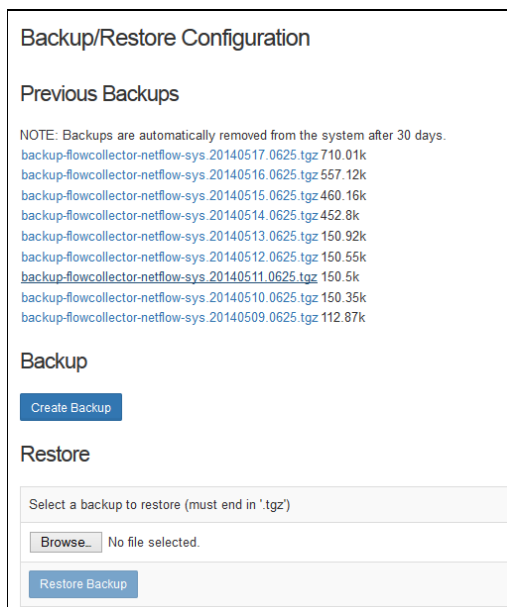
System	
IP Address:	.27.111
Host name:	temp-nflow-v
Domain name:	eng.lancope.local
Total Memory:	8G
VM Server Memory:	1G reserved, limit 8G
Free Memory:	363.84M
Load Average:	0.22, 0.32, 0.38
VM Server CPU:	1.02GHz reserved, unlimited
Uptime:	19:51:06
Version:	6.7.0
Platform:	VMware Virtual Platform
Build:	2015.03.23.1439-0
Serial No.:	FCNFVE-VMware-

2. Look at the IP address and host name shown on the Home page. Verify that this is the appliance you want to backup.
3. In the navigation pane, click **Support** and then **Backup/Restore Configuration**.

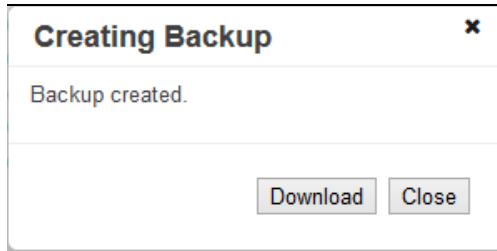




4. The Backup/Restore page opens.



5. Under the Backup section of the page, click **Create Backup**. A progress window appears and indicates when the process is finished.



6. Click **Download** and save the backup (TGZ) file to your preferred location.
7. Click **Close** to close the progress window.



STEALTHWATCH DATABASE

OVERVIEW

This section discusses the options available for backing up StealthWatch data for the SMC, the FlowCollector for NetFlow, and FlowCollector for sFlow appliances.

Note: The SMC continues to monitor your system during the backup process.

APPLIANCE DATABASE

StealthWatch uses rsync (a software utility) over a SMB (Server Message Block) file share to store the database in a remote location. You should back up the databases for the SMC and FlowCollectors in your network.

The appliance database contains all data observed on your network, such as traffic data, alarm data, and host data. Because this data changes continuously, the database can be quite large and can take hours, or even days, to back up.

The amount of time a backup takes depends on a number of factors including how heavily loaded the StealthWatch system is, how fast and stable the network connection to the SMB server is, and the stability and load on the SMB server itself.

The time required to perform a database backup is approximately between 0.5 GB and 2 GB per minute. For example, an initial backup for a 2 TB system would take approximately 3 days. Consequently, if you ever need to restore the database, the restoration process can take just as long.

Subsequent backups will be much shorter. For example, on a significantly busy system storing 60 GB per day a backup would take approximately two hours.

Important: Subsequent backups must be on the same share in order to back up only what has been changed from the initial backup. If the backup is made in another share, then the backup will start from scratch and take as long as an original backup.

Tip: The best backup solution for the SMC database is a redundant SMC, which will always have a mirror copy of the data files. Having a redundant SMC would also allow for quicker restorations, if needed. However, if a redundant SMC is not an option for you, the SMC allows you to back up the database manually.

When Should You Back Up the Appliance Database?

Because the data on your network is constantly changing, we recommend that you back up the appliance database as often as possible (per your company's policy) to avoid losing data. At a minimum, you should probably back up the appliance database before any upgrades and before any major changes to your system.

What is Backed Up in the Database?

The database includes the following information:

- Traffic data gathered from the monitored StealthWatch appliances
- Alarm and probe suppression settings for host policies
- Most of the data collected for display in standard appliance documents

Note: The database does not include scheduled reports.



BACKING UP THE DATABASE

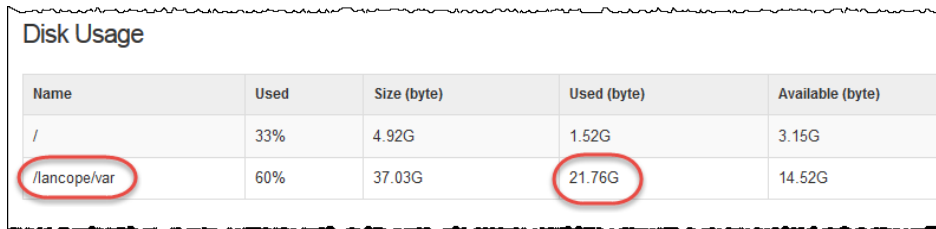
This section describes how to back up a FlowCollector or SMC database.

Once the operation has started, you can leave the page (i.e., "mouse away") and the process will continue without interruption. When you return, the status will be updated.

Note: If you click **Cancel** (or if the process cannot continue for some reason), the backup process stops. If the process is stopped, the process begins where it left off the next time you click the **Create Backup** button. (In this case, be sure that the previously stopped backup file is not locked.)

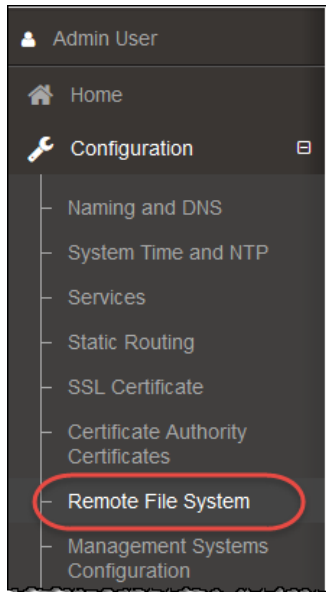
To back up the database to a remote file system, complete these steps:

1. Log in as the admin user to the Appliance Administration Interface.
2. To determine how much space you will need on the remote file system to store the database backup, do the following:
 - a. On the Home page, scroll down to the Disk Usage section.



Name	Used	Size (byte)	Used (byte)	Available (byte)
/	33%	4.92G	1.52G	3.15G
/lancope/var	60%	37.03G	21.76G	14.52G

- b. Look at the Used (byte) column for the /lancope/var file system as shown in the example. You will need this much space plus 15% on the remote file system to store the data
3. In the navigation pane, click **Configuration**, and then click Remote File System.



The Remote File System page opens:

A screenshot of the 'Remote File System' configuration page. The page has a white background and a title 'Remote File System'. Below the title is a form with five input fields: 'IP Address' (containing '15.32'), 'Port Number' (containing '445'), 'Share Name' (containing 'Backup'), 'Username' (empty), and 'Password' (masked with dots). At the bottom of the form are four buttons: 'Test', 'Clear Configuration', 'Reset', and 'Apply'.

4. Complete the fields using the settings for the remote file system where you want to store the backup files.

Note: The StealthWatch file share uses the CIFS (Common Internet File System) protocol, also known as SMB (Server Message Block).

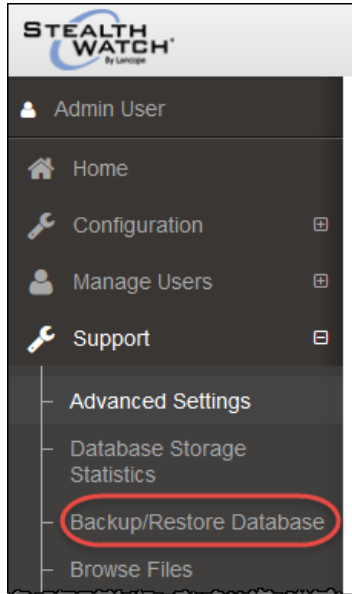
5. When finished, click Apply to place the settings in the configuration file.
6. Click Test to verify that the StealthWatch appliance and the remote file system can communicate with each other. You should see the following message at the bottom of the Remote File System page when the test is complete:



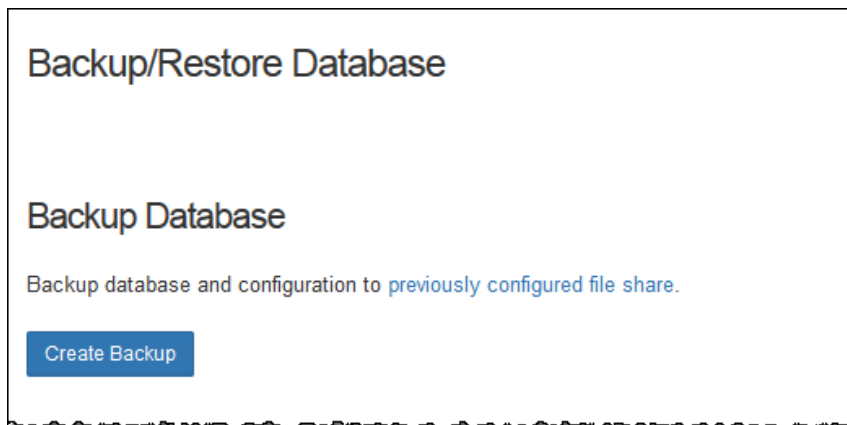
Lancope

File sharing appears to be properly configured.

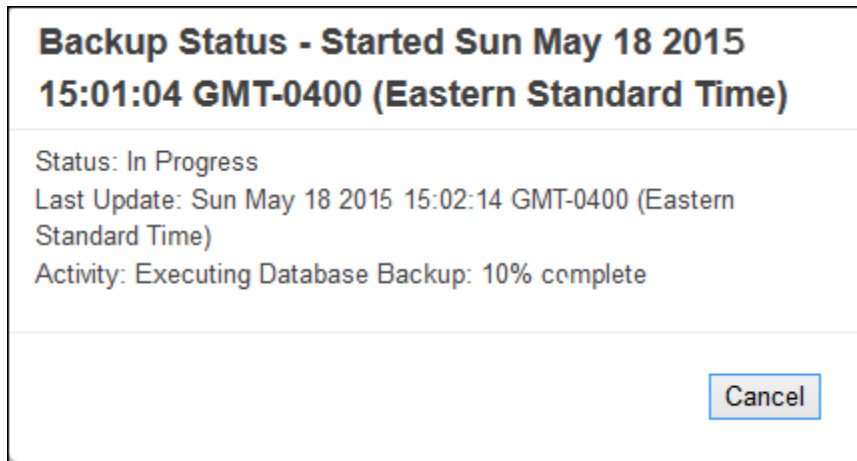
7. In the navigation pane, click Support, and then Backup/Restore Database.



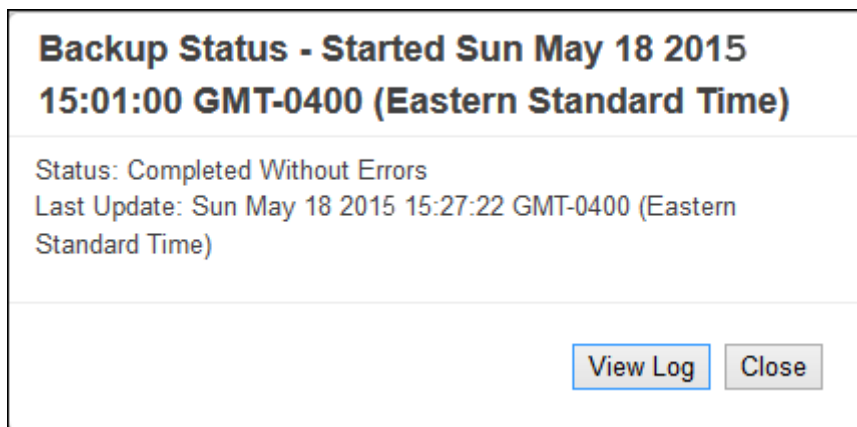
8. The Backup/Restore Database page appears.



9. Click **Create Backup**. A progress window appears and indicates the status. When finished, you can choose to view the backup log file or close the dialog as shown in the following example:



10. When finished, another progress window opens indicating that the backup process has completed.



Important: After the backup process has started, you can mouse away from the page without interrupting the process. However, if you click **Cancel** while the backup is in progress, you may not be able to resume the backup without restarting the appliance.

11. If desired, click **View Log** to view details of the backup process.
12. Click **Close** to close the progress window.



RESTORING THE STEALTHWATCH SYSTEM

OVERVIEW

This chapter describes the restoration processes after a disaster. You should back up both the configuration file and the database.

Restoring Your Appliance System Configuration

Warning: Do not interrupt the restoration process once it has begun.

Notes:

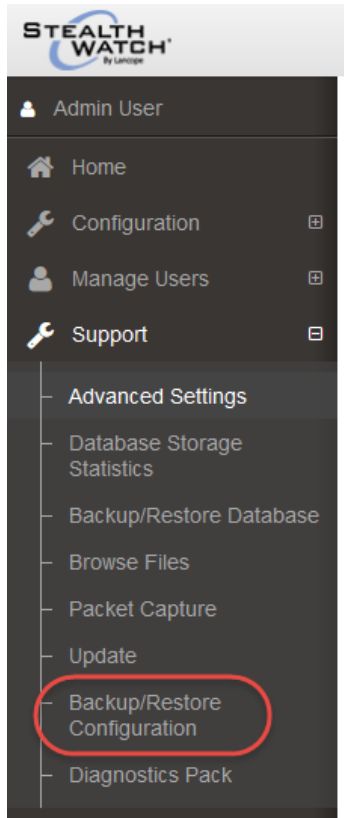
The SMC will not process requests during the restoration process.

If you restore an SMC that is part of a failover pair, you must also restore the configuration on the other SMC in the pair. You must restore each of the SMCs.

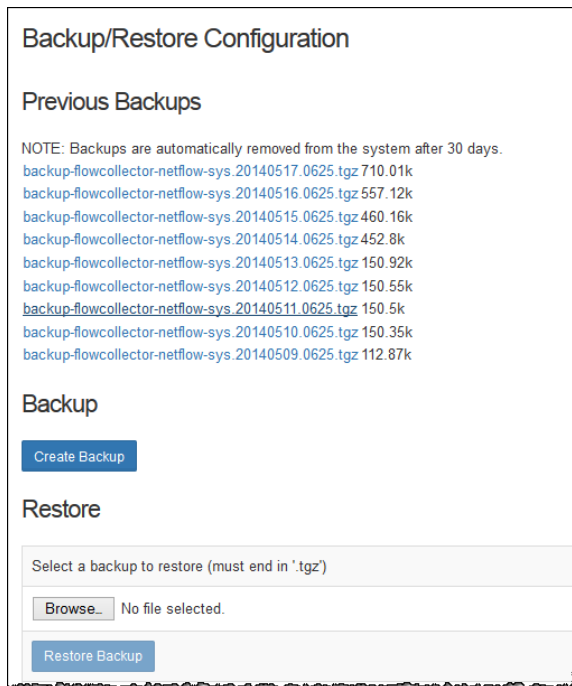
Complete these steps to restore your appliance configuration:

1. Log in as the admin user to the Appliance Administration Interface.
2. In the navigation pane, click **Support** and then **Backup/Restore Configuration**.





3. The Backup/Restore page opens.



4. Click **Browse**.

5. The File Upload dialog appears.



Lancope

6. Navigate to where the backup TGZ file is located, and click **Open**.
7. The **File Name** field populates with the selected path and file name.
8. Click **Backup**.
9. The system begins restoring the selected configuration file. During this process, the Restore appliance Configuration screen displays the restoration progress. Since the configuration files are generally small, the upload should take only a few minutes.
10. The upload and restoration of the configuration file are complete when the progress information shows **Restoration Complete** or **Restoration Failure**. If the restoration progress information reports a failure, go back to step 3 and retry the restore.
11. If you continue to have problems, look at the following log files for additional information:
 - `/lancope/var/logs`
 - [https://IP_address/\[product\]*](https://IP_address/[product]*)

*where the product is "smc" for SMC, "swa" for FlowCollector, "fs" for FlowSensor, and "fr" for FlowReplicator.
12. If you are unable to resolve the problem yourself, provide these log files to Lancope Customer Care.
13. If you have restored an SMC that is part of a failover pair, you must also restore the configuration on the other SMC in the pair.
14. If you have restored an SMC that is part of a failover pair, then both SMCs in the pair become secondary SMCs. You must access the SMC client interface to configure one of the SMCs to be the primary. See the *SMC Client Online Help* for more information.

Restoring the StealthWatch Appliance Database

This section describes how to restore the database for a StealthWatch SMC or FlowCollector. Restore the database only after you have restored the configuration for the appliance. (See page 11.)

WARNING: Do not interrupt the restoration process after it has begun.

Note: You cannot use a backup file from a previous version of the StealthWatch appliance to restore an appliance database. The backup version must match the version of the appliance.

A command line interface is available for you to restore a previous backup of the database. The database that is restored is the database that exists in the previously configured [remote file system](#) (i.e., file share).

Important: We recommend that you contact Customer Support before restoring a database.

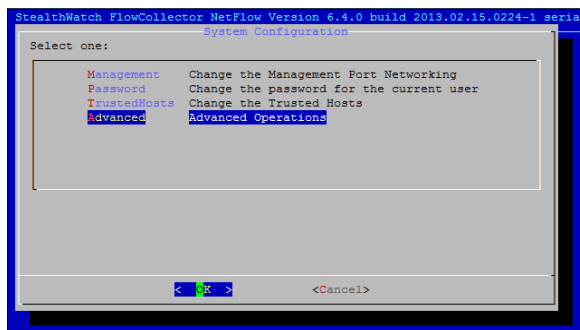
Procedure

To restore a database, log into the appliance as sysadmin to access the root shell:

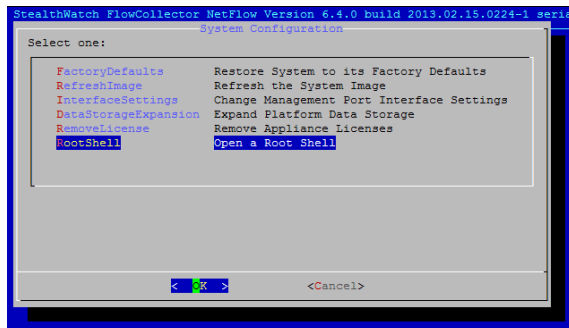
1. Type **sysadmin**, and then press **Enter**.
2. When the password prompt appears, type **lan1cope**, and then press **Enter**.

```
login as: sysadmin
sysadmin@10.202.27.137's password: █
```

3. At the next prompt, type **SystemConfig**, and then press **Enter**.



4. On the System Configuration menu, select **Advanced**, and then press **Enter**. The Advanced menu appears.



5. Select **Root Shell**, and then press **Enter**.

```
Type the root password at the prompt to open a root shell.
Password: █
```

6. Type the root shell password, and then press **Enter**.
7. Issue the following command

```
cd /var/tmp
nohup doDbRestore -c -q &
```



Tip: If you want to see the switches that are available with this tool, enter this command:

```
doDbRestore -h
```

Note: If you do not specify the name of the database to be restored, the default name (your system's serial number) will be used.

To check the status of a restore operation that is in progress, you can display two files:

```
/lancope/var/logs/VerticaRestore.log  
/lancope/var/logs/DatabaseRestore.log
```

Once the system completes the restore it will reboot itself and then begin collecting data.

Just as the backup took several hours (or days), the restore will take a long time as well—the time should be shorter, but depends greatly on the network speed and the speed of the SMB server.