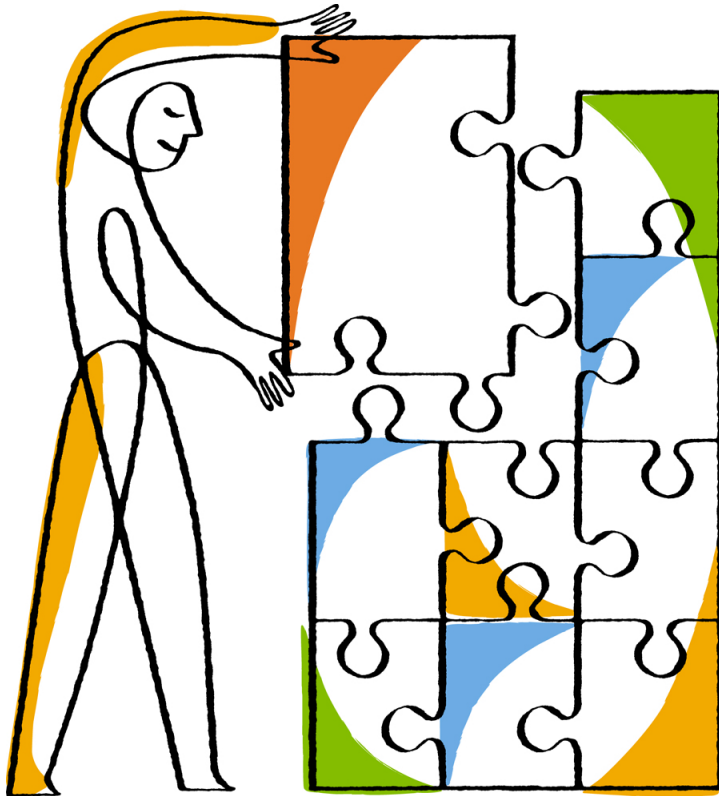




Config Advisor 3.5

Data Collector and Sanitizer Script Documentation



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089

Telephone: +1(408) 822-6000
Fax: +1(408) 822-4501
Support telephone: +1 (888) 463-8277

Part number: 215-08889
May 2014

Copyright Information

Copyright © 1994–2014 NetApp, Inc. All rights reserved. Printed in the U.S

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, FAServer, FastStak, FilerView, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft

Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

Table of Contents

1	USING CONFIG ADVISOR IN SECURE SITES.....	7
1.1	What Data Collector and Sanitizer script is	7
1.2	Prerequisites for using the Data Collector and Sanitizer script.....	8
1.2.1	Installing PowerShell 2.0	8
1.2.2	Installing Data ONTAP PowerShell toolkit 2.0	8
1.3	Running the script	9
1.4	Data collection methods for secure sites	11
1.4.1	Interactive data collection method	11
1.4.2	Batch-mode data collection method	12
1.4.3	Command-line argument method	13
1.4.4	Collecting data manually	16
1.5	Filtering and mapping.....	19
1.5.1	Collecting and filtering data.....	19
1.5.2	Filtering precollected data	20
1.6	Analyzing filtered data file.....	22
1.6.1	Importing filtered data file for analysis.....	22
1.7	Launching Help for the script	24

Preface

This document describes how to install, configure, and run Config Advisor to verify NetApp hardware installations in secure and non-secure sites.

AUDIENCE

The primary audience for this document is technical personnel such as systems administrators, engineers, professional services engineers, and professional services consultants at NetApp.

KEYBOARD AND FORMATTING CONVENTIONS

You can use your product more effectively when you understand how this document uses keyboard and formatting conventions to present information.

Keyboard conventions

Convention	What it means
Enter, enter	- Used to refer to the key that generates a carriage return; the key is named Return on some keyboards. - Used to mean pressing one or more keys on the keyboard and then pressing the Enter key, or clicking in a field in a graphical interface and then typing information into the field.

Formatting conventions

Convention	What it means
<i>Italic font</i>	- Words or characters that require special attention. - UI literals. - Placeholders for information that you must supply. For example, if the guide says to enter the arp -d host name command, you enter the characters "arp -d" followed by the actual name of the host.
Monospaced font	- Command names, option names, and daemon names. - Information displayed on the system console or other computer monitors. - Contents of files. - File, path, and directory names.
Bold monospaced font	Words or characters you type. What you type is always shown in lowercase letters; unless your program is case-sensitive and uppercase letters are necessary for it to work properly.

SPECIAL MESSAGES

This document might contain the following types of messages to alert you to conditions you must be aware of.

Note: A note contains important information that helps you install or operate the system efficiently.

HOW TO SEND YOUR COMMENTS

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us provide the most accurate and high-quality information.

If you have suggestions for improving this document, send us your comments by e-mail to doccomments@netapp.com. To help us direct your comments to the correct division, include the name of your product in the subject line.

TERMINOLOGY

To understand the concepts in this document, you might need to know the following terms defined here.

- *Controller or storage controller* - The component of a storage system that runs the Data ONTAP® operating system and controls its disk subsystem. Controllers or storage controllers are also sometimes called *storage appliances*, *appliances*, *storage engines*, *heads*, *CPU modules*, or *controller modules*.
- *Storage system* - The hardware device running Data ONTAP that receives data from and sends data to native disk shelves, third-party storage, or both. Storage systems that run Data ONTAP are sometimes referred to as *filers*, *appliances*, *storage appliances*, *V-Series systems*, or *systems*.

1 Using Config Advisor in secure sites

Config Advisor can be used to perform onsite and offsite data analysis. It can also be used to analyze data that is pre-collected by using the Data Collector and Sanitizer script.

Onsite data analysis: In this method, the user can use either the standard data collection methods built into the Config Advisor tool or the Data Collector and Sanitizer script. The collected data can then be used by Config Advisor to perform analysis and reporting.

Note: In secure sites, you must disable usage metrics manually from **Preferences**. For more information, see [Setting Preferences in Config Advisor](#) in Config Advisor 3.5 Installation and Administration Guide.

Offsite data analysis: In this method, Config Advisor need not be installed on the secure site system. The Data Collector and Sanitizer script is used to collect data, and then filter, and parse the collected data. This sanitized data can then be sent to NetApp Technical Support or a partner for review. NetApp Technical Support enters this data into Config Advisor to perform configuration validations and health checks and provide a detailed report to the customer.

The Data Collector and Sanitizer script can be run on secure sites to collect controller-related information from NetApp storage controllers running Data ONTAP 7.x and Data ONTAP 8.x operating in 7-Mode. The script is written in Microsoft Windows PowerShell 2.0.

1.1 What Data Collector and Sanitizer script is

The Data Collector and Sanitizer script is a single, readable, digitally signed Microsoft PowerShell script. The script is used to collect controller-related information such as, volume names, volume types, storage information, and details about software licenses from NetApp storage controllers running Data ONTAP 7.x and Data ONTAP 8.x operating in 7-Mode. It also filters out uniquely identifiable data, such as IP addresses, aggregate names, volume names, and so on, or data that may be considered sensitive. The script can also be used to filter out sensitive data from the precollected data.

The script uses a fallback mechanism to connect to the controller. It attempts to connect through the HTTPS protocol first and then falls back to SSH, and finally to HTTP.

Note: If you want to connect through SSH instead of HTTPS or HTTP, then you should disable the HTTPS or HTTP service.

To disable the HTTPS or HTTP service on the controller, set the following to **Off**:

```
options httpd.admin.enable
options httpd.admin.ssl.enable
options httpd.enable
options ssl.enable
```

To enable SSH on the controller, set `options ssh.enable` to **On**.

1.2 Prerequisites for using the Data Collector and Sanitizer script

To use the Data Collector and Sanitizer script (written in Microsoft Windows PowerShell 2.0) that is a part of Config Advisor, you must install the following:

- PowerShell 2.0 or later
For information about installing PowerShell 2.0, see [Installing PowerShell 2.0](#).
- Data ONTAP PowerShell toolkit 1.5 or later
For more information, see [Installing Data ONTAP PowerShell toolkit 2.0](#).

1.2.1 Installing PowerShell 2.0

For information about downloading and installing PowerShell 2.0, see support.microsoft.com/kb/968929.

Note: Microsoft.NET Framework 2.0 is a prerequisite for PowerShell 2.0. Therefore, to install PowerShell 2.0 on an operating system such as Windows XP, you must install both PowerShell 2.0 and WinRM 2.0.

You can install Windows Management Framework from support.microsoft.com/kb/968929; it contains both PowerShell 2.0 and WinRM 2.0.

PowerShell 2.0 and WinRM 2.0 are preinstalled on Windows 7.

1.2.2 Installing Data ONTAP PowerShell toolkit 3.0

You can find information about the prerequisites for installing Data ONTAP PowerShell toolkit 1.5 and how to install Data ONTAP PowerShell toolkit 3.0.

Before you begin

- WinRM 2.0 must be installed.
- PowerShell 2.0 must be installed.

Note: You can install Windows Management Framework from support.microsoft.com/kb/968929; it includes PowerShell 2.0 and WinRM 2.0.

Steps

1. Log in to <https://communities.netapp.com> using Internet Explorer. You might face download issues if you use a different browser.
2. Download Data ONTAP PowerShell toolkit 3.0 from the Communities web site at <https://communities.netapp.com/servlet/JiveServlet/downloadBody/6138-102-8-25408/DataONTAP.zip>
3. Download the DataONTAP.ZIP file to a temporary directory on your machine. Unzip Data ONTAP PowerShell toolkit to get a folder called DataONTAP that contains the library files.
4. Copy the DataONTAP to the same folder as the PowerShell installation directory. This directory could be located at C:\Windows\System32\WindowsPowerShell\v1.0\Modules or C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules
5. Open a command prompt window (click **Start > Run**, type **cmd**, and then click **OK**) to verify that PowerShell exists by running the following command:
C:\>powershell

If the module exists, the following is displayed:

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
```

6. Open the **Windows PowerShell** command prompt window (click **Start > All Programs > Windows PowerShell**) and verify that the module exists by running the following command:
`PS C:\> Get-Module -listavailable`
7. Import the module by running the following command:
`PS C:\> Import-Module DataONTAP`

Note: All the extracted files must be in the same location. Files such as `ontapi.dll` must not be one level deeper in the directory tree structure.

If you prefer to add the module by unzipping the `DataONTAP.zip` file manually, you must first clear the security attribute in the file **Properties** window.

On some versions of Windows, you might need to add the “.NET Framework 3Help” feature.

1.3 Running the script

The Data Collector and Sanitizer script is included with the Config Advisor installation package and is available in the following installation folder: `C:\Program Files\ConfigAdvisor\secure_datacollector.ps1` and `C:\Program Files (x86)\ConfigAdvisor` for 64-bit OS.

The Data Collector and Sanitizer script can be used independent of Config Advisor for secure sites where deployment of Config Advisor binaries is not possible. You can copy the Data Collector and Sanitizer script from the folder and carry it to the secure site. At the secure site, copy the script onto the desktop or a writeable folder for execution.

Before you begin

1. You must have installed PowerShell 2.0 or later.
For more information, see [Installing PowerShell 2.0](#).
2. You must have installed Data ONTAP PowerShell toolkit 1.5 or later.
For more information, see [Installing Data ONTAP PowerShell toolkit 2.0](#).
3. You must have set the PowerShell Execution policy to Allsigned, RemoteSigned, or Unrestricted. It must not be set to Restricted.

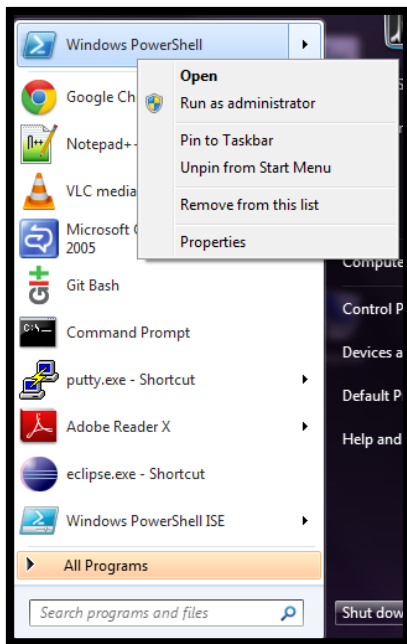
Additional information

The current PowerShell execution policy can be viewed by running the `Get-ExecutionPolicy` command.

The current PowerShell execution policy can be changed by running the `Set-ExecutionPolicy` command. You need to have administrator rights to run this command.

Steps

1. From the **Start** menu, right-click Windows PowerShell, and select **Run as administrator**, as shown:



The PowerShell command window is launched.

Alternatively, you can run the command in the Windows command prompt window.

2. Run the `Set-ExecutionPolicy` command.

For more information, see technet.microsoft.com/en-us/library/cc764242.aspx.

VeriSign's Code Signing Certificate

The Data Collector and Sanitizer script is digitally signed by NetApp by using VeriSign's Code Signing Certificate. VeriSign Code Signing Certificate adds a level of trust by providing third-party authentication of the code signer, which is recognized worldwide. The first time you run the script, you might be prompted to add NetApp Inc. to the list of trusted software publishers. If prompted, select **[A] Always run**.

The **VeriSign's Code Signing Certificate** is as shown:



1.4 Data collection methods for secure sites

For data collection in secure sites, you can use any one of the following methods:

1. Collecting data using the Data Collector and Sanitizer script
In this method, you can collect data from single or multiple controllers by using one of the following methods:
 - Interactive data collection
 - Batch-mode data collection
 - Command-line argument
2. Collecting data manually

1.4.1 Interactive data collection method

You can collect data by interactively providing the credentials of a single controller or multiple controllers.

Steps

1. Launch PowerShell.
2. Navigate to the directory where the script is located.
For example, if you have stored the script in the C drive, then enter `cd c:\.`
3. Invoke the Data Collector and Sanitizer script by entering `.\secure_datacollector.ps1`, and press **Enter**.
4. Based on your requirement, select either one of the options, and press **Enter**:

1. **Collect data unfiltered**

- If you enter **1**, the following message is displayed:

```
Default output folder will be: <homeDirectory>\ConfigAdvisorScriptData
Do you want to change the default output location? [Y/N].
```

Note: Home directory in this case refers to the PowerShell home directory (\$home). If the PowerShell home directory exists in any other drive then a ConfigAdvisorScriptData folder will be created under that drive or location.

- If you enter **Y**, the script requests for the name of the output folder where the result file will be stored. Provide a folder name, and press **Enter**.
 - If you choose **N**, then all the output files by default will be stored at `<homeDirectory>\ConfigAdvisorScriptData`.
2. **Collect data and filter sensitive data using mapped names and create a mapping file**
 - If you enter **2**, the script displays all the data items that can be filtered.
 - Enter the filtering level. The following message is displayed:

```
Default output folder will be: <homeDirectory>\ConfigAdvisorScriptData
Do you want to change the default output location? [Y/N].
```

- If you enter **Y**, the script requests for the name of the output folder where the result file will be stored. Provide a folder name, and press **Enter**.
- If you choose **N**, then all the output files by default will be stored at `<home Directory>\ConfigAdvisorScriptData`.

Note: You can enter the folder name to create a folder in the directory, where the script resides, if the folder specified does not exist.

You can enter a relative path such as `folder1/folder2`. In this case, the script will create `folder1` in the same directory where the script is located, and `folder2` will be sub-directory of `folder1`.

If the script resides in `C:\Program files\` or `C:\Program Files (x86)`, then you need administrator privileges to create the folder in `C:\Program files\` or `C:\Program Files (x86)`.

5. Enter **Y** for yes or **N** for no depending on whether you want to run extended checks on the controllers or not.

If you choose **Y**, then the `rdfile/etc/messages` command is run.

Note: Extended checks require historical log data from the controller. Collection and analysis of this data takes a long time.

The script displays the non-intrusive commands that will be run on the controllers.

6. Enter the host name or IP address of the controller, and press **Enter**.
7. Enter the user name, and press **Enter**.
8. Enter the password, and press **Enter**.

The script attempts to connect to the controller by using the fallback method.

The script allows you to enter the next controller details, if any.

9. Enter **Y** if you want to collect data for more controllers or **N** if you want to collect data from only one controller, and press **Enter**.

The script starts collecting data from the controller. After the data collection is complete the script displays the location of the output files.

Note: The naming convention of the generated output files is `Timestamp_hostname/FQDN/IPaddress of the controller.txt`. In case of multiple controllers, for each controller, a different `.txt` file is generated with the respective timestamp and the provided host name or IP address.

1.4.2 Batch-mode data collection method

You can collect data from multiple controllers by providing the credentials of multiple controllers in a single (Comma Separated Value) CSV file.

The CSV file should not contain any header. It must contain details, such as IP address or host name, user name, and password, of each controller on separate lines.

Example of a CSV file:

```
10.238.194.138, root, netapp123
```

```
fas-2040-32, root, netapp124
```

10.45.91.152, root, Admin123

Steps

1. Launch PowerShell.
2. Navigate to the directory where the script is located.
3. Invoke the Data Collector and Sanitizer script along with the credential file by entering the following command: `.\secure_datacollector.ps1 -credentials <filename.csv>`, and press Enter

Alternatively, you can invoke the Data Collector and Sanitizer script along with the credential file by entering the following command:

```
.\secure_datacollector.ps1 <filename.csv>
```

Note: The credentials file must be a CSV file without any header and with controller details, that is, IP address or host name, user name, and password on separate lines.

The user is prompted to select a data collection method, that is, type of filtering for the output data.

1. Select any one of the displayed options, and press **Enter**. The following message is displayed:

```
Default output folder will be: <homeDirectory>\ConfigAdvisorScriptData
Do you want to change the default output location? [Y/N].
```

- If you enter **Y**, the script requests for the name of the output folder where the result file will be stored. Provide a folder name, and press **Enter**.
- If you choose **N**, then all the output files by default will be stored at `<homeDirectory>\ConfigAdvisorScriptData`

The script requests for the name of the output folder where the result file will be stored.

2. Provide a folder name, and press **Enter**.

The script does not prompt for the controller details, but attempts to connect to the controller directly by using the fallback method, using HTTPS/SSH/HTTP.

1.4.3 Command-line argument method

You can provide all the script arguments in the command-line interface while invoking the script. You can also provide multiple filter levels as the argument.

Steps

1. Launch PowerShell.
2. Navigate to the directory where the script is located.
3. Invoke the Data Collector and Sanitizer script along with the command-line argument, and press **Enter**.

The script requests for more information or starts collecting data based on the command-line argument that you enter.

Note: If you provide multiple filter levels as the argument for the script, place the filter levels within double quotation marks. For example, `.\secure_datacollector.ps1 -l "a,b"`

If you provide multiple filtering items for filtering interactively, you need not use double quotation marks.

Examples of command-line arguments

Example 1

```
\secure_datacollector.ps1 -Output_folder C:\Data\output -n -m -l "a,d,e".
```

This command does not collect data from any controllers but only filters out all the sensitive data from all the existing text output files in C:\Data\output. The corresponding mapping file is generated in the same location.

Example 2

```
.\secure_datacollector.ps1 -Credentials nodes.csv -Output_folder C:\Data\output -m -l "e"
```

The node details are read from the CSV file. The output files are generated in C:\Data\output (even if this location is different from the script location). The output data is filtered and the sensitive data is replaced with generic names. Mapping files with original names mapped to new ones are generated in C:\Data\output. In this case, because the mapping level specified is e, aggregate names are filtered.

You can pass different combinations of command-line arguments. For more information about command-line arguments, see Parameters in Data Collector and Sanitizer script.

Parameters in the Data Collector and Sanitizer script

The command-line arguments that can be passed to the script while invoking it are as follows:

Parameter name	Alias	Description
Filename	-Credentials	This parameter specifies the name of credentials file containing the controller information of all the controllers for which data is to be collected. This can be the absolute path, relative path, or only the file name. In case only the file name is specified, the script attempts to search for the file in the folder where the script is located. If the file is not found, it looks in the current PowerShell directory. An exception occurs if the file is not found in any of the locations. The file must be a CSV file without any header and with the details of each controller, such as IP or host name, user name, and password, on separate lines.
Output_folder	-Out	This parameter specifies the name of the folder where the output files are generated. This can be the absolute path, relative path, or only the folder name. In case it is a folder name, it is expected to be in the same directory as the script. If the folder does not exist, it is created. If -n is chosen, no data collection is required. Only the files present in this folder are filtered.

Parameter name	Alias	Description																														
NoCollection	-n	This parameter indicates that data collection should be skipped and only data from the existing files (manually collected) should be filtered. In this case, only the existing files in the <code>Output_folder</code> location (provided through the input parameter) is filtered. Valid filtering options that can be used along with this parameter are <code>-m</code> , <code>-l</code> . Only .txt files are considered for filtering.																														
Unfiltered	-u	This parameter indicates that data from the controller should be collected without any filtering. Note: This parameter cannot be used in combination with the <code>Use_Mapping</code> option.																														
Use_Mapping	-m	This parameter indicates that sensitive data will be replaced with generic names such as <code>xx.xx.xx.01</code> (for replacing the IP address). A separate mapping file (CSV) is generated, which shows the replaced strings with the new strings. The format of the mapping file name is <code><timestamp>_MAPPING.csv</code>. If this option is selected, the output file name is changed to one of the mapped names as described in its corresponding mapping file. Note: This parameter cannot be used in combination with the <code>UnFiltered</code> option. Mapping information is not generated for license keys, MAC addresses, and HBA addresses.																														
FilterLevel	-l	This parameter specifies the level of filtering of output data. The following are the filter levels: Note: This parameter is valid only when used in combination with <code>- Use_Mapping</code>. <table><thead><tr><th>Level</th><th>Item</th></tr></thead><tbody><tr><td>a</td><td>IP Address</td></tr><tr><td>b</td><td>Host names</td></tr><tr><td>c</td><td>DNS Domain Name</td></tr><tr><td>d</td><td>License Codes</td></tr><tr><td>e</td><td>Aggregate Names</td></tr><tr><td>f</td><td>Volume Names</td></tr><tr><td>g</td><td>igroup Names</td></tr><tr><td>h</td><td>Email IDs</td></tr><tr><td>i</td><td>User names</td></tr><tr><td>j</td><td>Web server URLs</td></tr><tr><td>k</td><td>LUN Names</td></tr><tr><td>l</td><td>MAC Address</td></tr><tr><td>m</td><td>Host Bus Adapter Addresses (FC, SAS, IB, and so on)</td></tr><tr><td>n</td><td>All of the above</td></tr></tbody></table>	Level	Item	a	IP Address	b	Host names	c	DNS Domain Name	d	License Codes	e	Aggregate Names	f	Volume Names	g	igroup Names	h	Email IDs	i	User names	j	Web server URLs	k	LUN Names	l	MAC Address	m	Host Bus Adapter Addresses (FC, SAS, IB, and so on)	n	All of the above
Level	Item																															
a	IP Address																															
b	Host names																															
c	DNS Domain Name																															
d	License Codes																															
e	Aggregate Names																															
f	Volume Names																															
g	igroup Names																															
h	Email IDs																															
i	User names																															
j	Web server URLs																															
k	LUN Names																															
l	MAC Address																															
m	Host Bus Adapter Addresses (FC, SAS, IB, and so on)																															
n	All of the above																															

Note: You should not run the script when the system takeover or giveback is in progress.

If you are running the script from `C:\Program Files(x86)\ConfigAdvisor` or `C:\Program Files\ConfigAdvisor`, Windows might not allow the creation of the output

folder at the same location. In this case, either run the script as administrator or provide a location that has write-access for non-administrator user.

1.4.4 Collecting data manually

In certain secure sites, if it is not permitted to run the script on the system, you can manually run the Data ONTAP 7-Mode commands, provided in the following table, on the controller to collect data.

The output of these commands must be saved in AutoSupport format in a .txt file. Each command output must be placed under the respective AutoSupport section name.

AutoSupport section name mappings

The corresponding AutoSupport sections for ONTAP commands are:

Data ONTAP 7-Mode commands	AutoSupport names
Version	===== VERSION =====
sysconfig -a	===== SYSCONFIG-A =====
syconfig -r	===== SYSCONFIG-R =====
fcstat device_map	===== FC-DEVICE-MAP =====
storage show disk -a	===== STORAGE-DISK =====
storage show disk -p	===== STORAGE-DISK-P =====
rdfile /etc/rc	===== RC =====
rdfile /etc/hosts	===== HOSTS =====
rdfile /etc/exports	===== EXPORTS =====
exportfs	===== EXPORTFS =====
license	===== SOFTWARE-LICENSES =====
cf status	===== CSTATUS =====
cf partner	===== CPARTNER =====
hostname	===== HOSTNAME =====
fcv show cfmode	===== FCP-CFMODE =====
ifconfig -a	===== IFCONFIG-A =====
df	===== DF =====
df -A	===== DF-A =====
snap list -n	===== SNAP-LIST-N =====
options	===== OPTIONS =====
vol status -v	===== VOL-STATUS-V =====
lun show -v	===== LUN-CONFIGURATION =====
storage show acp -a	===== STORAGE-ACP =====
environment status	===== ENVIRONMENT =====
rlm status	===== RLM =====
sp status	===== SP =====
bmc status	===== BMC =====
cf monitor all	===== CF-MONITOR =====
igroup show	===== INITIATOR-GROUPS =====
lun show -m	===== LUN-SHOW-M =====
sis status	===== SIS-STATUS =====
date	===== DATE =====
snapmirror status	===== SNAPMIRROR-STATUS =====
snapvault status	===== SNAPVAULT-STATUS =====

Data ONTAP 7-Mode commands	AutoSupport names
aggr status -v	===== AGGR-STATUS-V =====

If you want to run extended checks on the collected data, run the `rdfile/etc/messages` command when collecting the data, and place the output under the `===== MESSAGES =====` AutoSupport section name.

Note: The section names should be exactly as shown in the table above, without any extra spaces.

Example of command output when placed under corresponding **AutoSupport** sections is as shown:

```
===== VERSION =====
NetApp Release 7.3.3: Thu Mar 11 22:29:52 PST 2010

===== SYSCONFIG-A =====
NetApp Release 7.3.3: Thu Mar 11 22:29:52 PST 2010
System ID: 0151695759 (fas3170-1); partner ID: <unknown> ()
System Serial Number: 80000741 (fas3170-1)
System Rev: a0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA

===== SYSCONFIG-R =====
Aggregate aggr0 (online, raid_dp) (block checksums)
Plex /aggr0/plex0 (online, normal, active)
RAID group /aggr0/plex0/rg0 (normal)

      RAID Disk      Device HA  SHELF BAY CHAN Pool Type  RPM  Used (MB/blks)  Phys
(MB/blks)
-----
---
dparity 2a.16 2a 1 0 FC:B - FCAL 15000 136000/278528000 137104/280790184
parity 2b.16 2b 1 0 FC:B - FCAL 15000 136000/278528000 137104/280790184
data 1c.16 1c 1 0 FC:A - FCAL 15000 136000/278528000 137104/280790184

Aggregate datagr (online, raid_dp, degraded) (block checksums)

===== FC-DEVICE-MAP =====
Loop Map for channel 1a:
Translated Map: Port Count 29
      7 29 28 27 25 26 23 22 21 20 16 19 18 17 24 45
      44 43 41 42 39 38 37 36 32 35 34 33 40

Shelf mapping:
      Shelf 1: 29 28 27 26 25 24 23 22 21 20 19 18 17 16
      Shelf 2: 45 44 43 42 41 40 39 38 37 36 35 34 33 32

===== STORAGE-DISK =====
Disk: 1c.16
Shelf: 1
Bay: 0
Serial: 3KN0QHYC00007617HUMG
Vendor: NETAPP
Model: X275_S15K4146F15

===== STORAGE-DISK-P =====
PRIMARY PORT SECONDARY PORT SHELF BAY
-----
1c.16 A 2c.16 B 1 0
1c.17 A 2c.17 B 1 1
1c.18 A 2c.18 B 1 2
2c.19 B 1c.19 A 1 3
2c.20 B 1c.20 A 1 4
2c.21 B 1c.21 A 1 5

===== RC =====
#Regenerated by registry Tue Mar 16 13:21:36 GMT 2010
```

```

#Auto-generated by setup Fri Mar 12 17:25:32 GMT 2010
hostname fas3170-1

===== HOSTS =====
#Generated by setup Tue Mar 16 13:21:36 GMT 2010
#Auto-generated by setup Fri Mar 12 17:25:32 GMT 2010
127.0.0.1 localhost

===== EXPORTS =====
#Auto-generated by setup Fri Mar 12 17:25:32 GMT 2010
/vol/vol0 -sec=sys,rw,anon=0,nosuid
/vol/vol0/home -sec=sys,rw,nosuid
/vol/spadminlog_fv -sec=sys,rw,nosuid
/vol/spadmindb_fv -sec=sys,rw,nosuid
/vol/testlog_fv -sec=sys,rw,nosuid

===== EXPORTFS =====
/vol/sqlebsdb4_fv -sec=sys,rw,nosuid
/vol/sqllog4_fv -sec=sys,rw,nosuid
/vol/sqlsyslog_fv -sec=sys,rw,nosuid
/vol/sspsearchlog_fv -sec=sys,rw,nosuid
/vol/sqlebsdb3_fv -sec=sys,rw,nosuid
/vol/sqlebslog5_fv -sec=sys,rw,nosuid

===== SOFTWARE-LICENSES =====
a_sis not licensed
cifs IWNGUPC
cluster not licensed
cluster_remote not licensed
compression not licensed
disk_sanitization not licensed
fcp site ICRNCZG

===== HOSTNAME =====
fas3170-1

===== FCP-CFMODE =====
fcp show cfmode: standby

===== IFCONFIG-A =====
e0M: flags=0x200c866<BROADCAST,RUNNING,MULTICAST> mtu 1500
ether 00:a0:98:0a:21:72 (auto-unknown-cfg_down) flowcontrol full
e0a: flags=0x2c4c867<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

===== DF =====
Filesystem            kbytes      used      avail capacity  Mounted on
/vol/vol0/            115343360  110615160  4728200      96%  /vol/vol0/
/vol/vol0/.snapshot          0    419468        0    ---%  /vol/vol0/.snapshot
/vol/spadmindb_fv/    104857600  84062176  20795424      80%  /vol/spadmindb_fv/

===== DF-A =====
Aggregate            kbytes      used      avail capacity
dataggr              5614278088  4721985892  892292196      84%

===== SNAP-LIST-N =====
Volume vol0
working...

date          name
-----
Mar 02 00:00  nightly.0

===== OPTIONS =====
auditlog.enable          on
auditlog.max_file_size   10000000
auditlog.readonly_api.enable off
autologout.console.enable on
autologout.console.timeout 60

```

You must save the collected data as a .txt file. If you want to filter multiple controller data, save the data of each controller in a separate .txt file, and save the files in a single folder and provide this folder name for filtering.

1.5 Filtering and mapping

For secure sites that do not want to disclose the system data is considered to be sensitive or uniquely identifiable, the Data Collector and Sanitizer script can be used to filter the data. After the filtering is complete, a mapping file is generated along with the results file.

You can filter uniquely identifiable data, such as IP addresses, aggregate names, volume names, and so on, or any data that may be considered sensitive. The script can also be used to filter sensitive data from the collected data.

Data filtering Items

The data items that can be filtered and their levels are as follows:

Filtering level	Filter item
a	IP Address
b	Host names
c	DNS Domain Name
d	License Codes
e	Aggregate Names
f	Volume Names
g	Igroup Names
h	Email IDs
i	User names
j	Web server URLs
k	LUN Names
l	MAC Address
m	Host Bus Adapter Addresses (FC, SAS, IB, and so on.)
n	All of the above

Note: In HBA filtering, 'Logical identifier' is filtered along with the following data:

For SAS HBA and FCVI HBA: FC Node names, FC port names, Base WWN, Host Port WWN, Host Loop ID, Host Port ID

For InfiniBand: LID, Remote LID and GUID

For iSCSI HBA: HBA, IQN, EUI and NAA name formats

1.5.1 Collecting and filtering data

You can both collect and filter data using one of the mentioned methods (Interactive, Batch-mode, or Command-line argument method).

In case of IP address filtering, host name filtering, and filtering of all available filtering items (filter level n), depending on what the user has provided (either the host name or IP address) the result file name will be named.

Result file name for IP address filtering

Input credential	Output file format
IP Address	<time_stamp>_Mapped-IPAddress.txt
Hostname	<time_stamp>_Mapped-Hostname.txt
FQDN	<time_stamp>_Mapped_FQDN.txt

Result file name for host name filtering

Input credential	Output file format
IP Address	<time_stamp>_Mapped-Hostname.txt
Hostname	<time_stamp>_Mapped-Hostname.txt
FQDN	<time_stamp>_Mapped_FQDN.txt

1.5.2 Filtering precollected data

The Data Collector and Sanitizer script can be used to filter manually collected data. For more information about manual data collection, see [Collecting data manually](#).

After manually collecting data and saving the collected data as a .txt file, you can use the script to filter a combination of data items by providing comma-separated values (for example, "c, e").

Steps

1. Launch PowerShell.
2. Navigate to the directory where the script is located.
For example, if you have stored the script in the C drive, then enter `cd c:\`
3. Invoke the Data Collector and Sanitizer script by entering `.\secure_datacollector.ps1 -n`, and press **Enter**.
 - a. The script displays all the data items that can be filtered.
 - b. Enter the filtering level.

The `Please enter the output folder location:` message is displayed.

4. Enter the output folder path where the precollected data file exists.

Files in the folder will be filtered and mapping file will get generated in the same folder.

Additional information

When you filter the precollected data, the original results file is overwritten with the filtered and mapped data.

In case of IP address filtering, host name filtering, and filtering of all available filtering items (filter level n) is selected for filtering of precollected data, the original result file name is replaced with `TimeStamp_MaskedHostname.txt`.

In the mapping files, during aggregate and volume name filtering, the controller mapping information will contain an extra column in the file specifying the type of volume (FlexVol or traditional volume), as shown:

	Original name	Mapped name	Volume type
--	---------------	-------------	-------------

	Original name	Mapped name	Volume type
Volume	vol0	Vol44565	Traditional
Aggregate	vol0	Vol44565	Traditional
	Lng	aggr42216	
	Data	aggr42215	

The sensitive data is filtered and mapped as follows:

- Aggregate names are replaced with `aggr3425` (any random number).
- Volume names are replaced with `vol34235` (any random number).
- Email ID is replaced with `xxxx2523524@xxx.com` (any random number).
- User name is replaced with `user342532` (any random number).
- Domain name is replaced with `xxxx.234234.com` (any random number).
- Host name is replaced with `Host_234234` (any random number).
- Webserver URL is replaced with `Server28374/xxxx` (any random number).
- IPv4 or IPv6 address is replaced with sequential generic names:
`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:1... n`. (The mapped addresses increase linearly, that is, `...xx.xx.xx.255`, `xx.xx.1.0`, `xx.xx.1.1`, and so on.).
- Igroup names are replaced with `lgrp4234` (any random number).

If the Domain Naming Service (DNS) entered is an IP address, then as a part of IP address filtering, this IP address also gets filtered.

During filtering (applicable to both, collect and filter, and for filtering on precollected data), the traditional volume names, if any, are also filtered along with aggregate names or volume names.

The traditional volume name is entered twice in the mapping file because the traditional volume names are filtered as part of Aggregate name and part of Volume name.

The traditional volume name is entered twice in the mapping file in case of filtering of all items also.

The **mapping information for each controller (in case of collect and filter)** is placed one below the other in the same file as shown:

	A	B	C	D	E
1	CONTROLLER	MAPPED NAME	OUTPUT FILE		
2	10.61.162.91	xx.xx.xx.15	20120530125500_xx.xx.xx.15.txt		
3	10.45.91.152	xx.xx.xx.8	20120530125338_xx.xx.xx.8.txt		
4					
5					
6					
7	CONTROLLER	FILTER ITEM	ORIGINAL NAME	MAPPED NAME	VOLUME TYPE
8	10.61.162.91				
9		EMAIL	postmaster@testing.netapp.com	xxx2348@xxxx.com	
10			dl-qa-autosupport@netapp.com	xxx2349@xxxx.com	
11		VOLUME	WanFlexDLAN	Vol44574	Flex Volume
12			WanFlexCLAN	Vol44573	Flex Volume
13			d	Vol44575	Flex Volume
14			vol0	Vol44564	Flex Volume
15			homedir	Vol44576	Flex Volume
16			FlexDLAN	Vol44572	Flex Volume
17			nfsVdiDS2	Vol44570	Flex Volume
18			FlexCLAN	Vol44571	Flex Volume
19			exchange_homedir2	Vol44577	Flex Volume
20		AGGREGATE	aggr0	aggr42197	
21			aggr1	aggr42198	
22		IPv4	11.11.11.31	xx.xx.xx.20	
23			192.168.10.91	xx.xx.xx.17	

The filtering of volume names, aggregate names, and all items (filter level n) is aborted if the command output of `vol status -v` is absent in the result file. In case of incomplete command output, the filtered data will be incorrect.

(Applicable to both collected and filtered data and for precollected data) If the result files in the data folders contain any comment lines (any command output preceded by #), during filtering, the script deletes all the comment lines.

Note: After running the Data Collector and Sanitizer script on the data (collected manually or otherwise), certain unfiltered sensitive data might still be present in the controller log messages section of the output. Therefore, before processing the output, you must manually verify the log messages section to check whether any unfiltered sensitive data is present. This is applicable only when message logs are included in the data collection process.

An index section is placed at the top of the mapping file describing the host name, mapped host name and its corresponding output file name.

An example of the index section containing controller names mapping is as shown:

CONTROLLER	MAPPED NAME	OUTPUT FILE
10.61.162.91	xx.xx.xx.15	20120530125500_xx.xx.xx.15.txt
10.45.91.152	xx.xx.xx.8	20120530125338_xx.xx.xx.8.txt

1.6 Analyzing filtered data file

You can find information about how to import the filtered data file to Config Advisor for analysis.

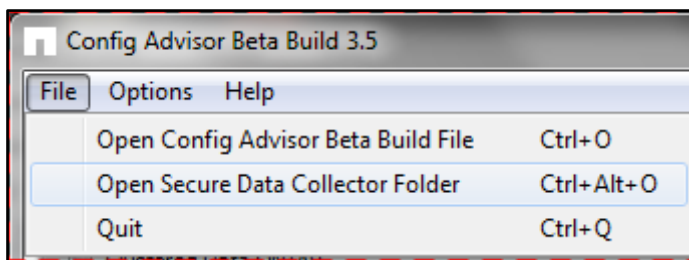
Multiple files can be imported into the tool at once. For this, all the files should be placed in a single directory. Import the file or directory by using the **File** menu option. After the import is completed, a single Config Advisor result file is created.

1.6.1 Importing filtered data file for analysis

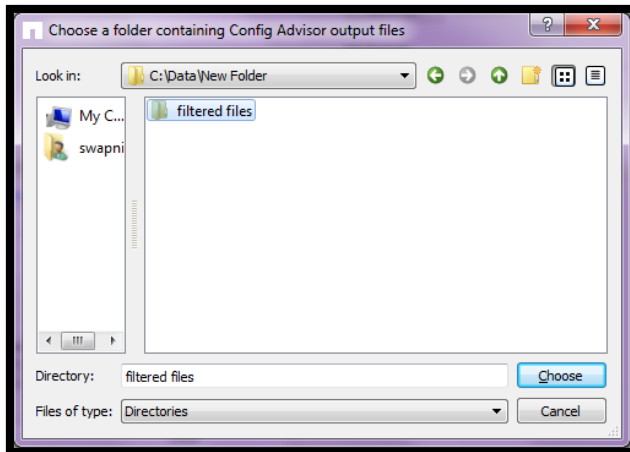
Steps

1. In the Config Advisor tool, click **File > Open Config Advisor Folder**.

The **Open Secure Data Collector Folder** is as shown:

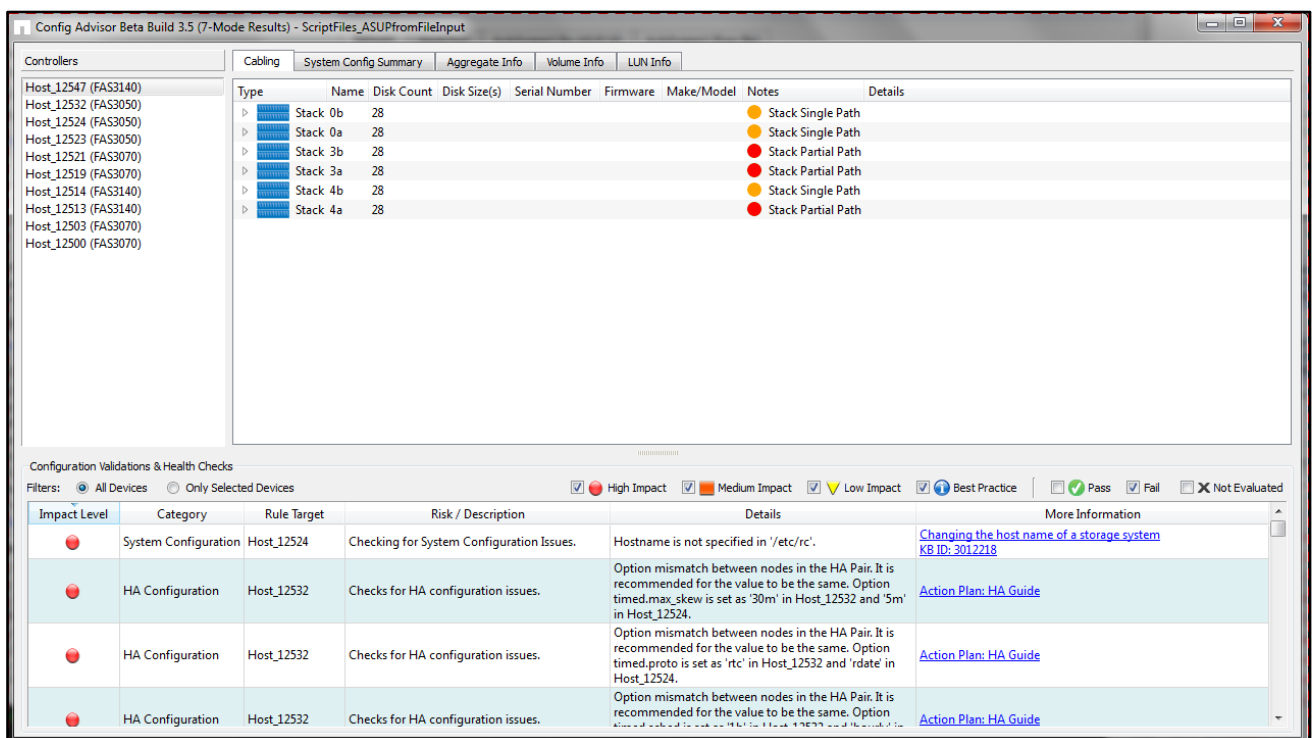


2. Select the folder where the data files are located, and click **Choose**.



3. Provide the name of the Config Advisor result file.
The import process starts and the progress is displayed in the log window.
4. The rules check results window is displayed after the import process is completed.

The results window is as shown:



The corresponding file name is populated in the **Recent Results** window.

1.7 Launching Help for the script

You can find usage and help information for the script.

Steps

1. From the **Start** menu, click **Start > All programs > Accessories > Windows PowerShell**.
2. Open a Windows PowerShell terminal and navigate to the folder containing the Data Collector and Sanitizer script.
3. For usage and help content for the script, run one of the following commands:
 - `Get-Help .\secure_datacollector.ps1` or
 - `help .\secure_datacollector.ps1`
4. For detailed help information, run the following command:
`Help .\secure_datacollector.ps1 -detailed`
5. For examples of script usage, run the following command:
`Help .\secure_datacollector.ps1 -examples`
6. For additional help and other notes, run the following command:
`Help .\ secure_datacollector.ps1 -full`

Index

C

Config Advisor..... 1, 5, 7, 8

controllers.....6, 7, 11, 12, 13, 14, 15

D

Data Collector and Sanitizer script....7, 8, 9, 10, 11, 13, 14, 15, 21, 22, 24

Data ONTAP PowerShell toolkit 1.5 8, 9

F

FlexPod 2

P

PowerShell 2.0 7, 8, 9

S

secure sites 5, 7, 11, 16, 19

V

validations and health checks 7

