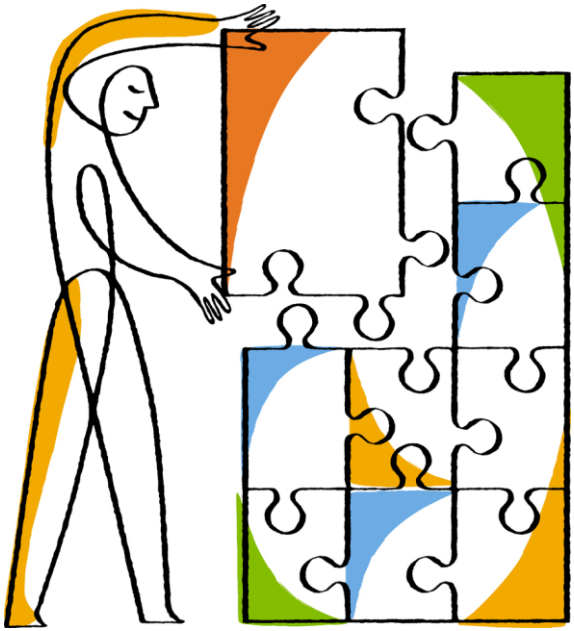
Config Advisor 4.6

Installation and Administration Guide



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

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-11674_A0
October 2016

Contents

Introduction to Config Advisor 10
What Config Advisor is..... 10
Features in Config Advisor 12
Configurations supported by Config Advisor 13
Installing, extending, configuring, upgrading, and uninstalling Config Advisor 17
Installing Config Advisor..... 17
Accessing Config Advisor..... 18
Configuring Config Advisor AutoSupport..... 19
Upgrading Config Advisor and firmware recommendations 20
Uninstalling plug-in..... 22
Collecting data..... 23
Collecting data from ONTAP..... 23
Collecting data by using the Network tab 24
Collecting data by using the Serial Port tab 27
Collecting data using AutoSupport (by ASUP Id) tab 29
Collecting data by using the AutoSupport (from File)..... 34
Collecting data from a Data ONTAP 7 and Data ONTAP 8 (7-Mode) installation .. 36
Collecting data by using the Network tab 37
Collecting data by using the Serial Port tab 40
Collecting data by using the AutoSupport (by ASUP Id) tab..... 43
Collecting data by using the AutoSupport (from file) tab 47
Collecting data to run Copy-Free Transition prechecks 49
Collecting data by using the Copy-Free Transition tab..... 50
Collecting data by using the batch data-collection mode 51
Collecting data from plug-ins..... 52
Collecting data from show tech-support..... 53
Working with results 54
Organization of Config Advisor Result file 54
Recent Results pane 54
Viewing results..... 55
What Config Advisor Viewer does 58
Viewing ONTAP results in Config Advisor..... 58
Nodes pane..... 59
Cluster Switches pane 60

Management Switches pane 61
Viewing 7-Mode results in Config Advisor 61
Controllers pane 63
Configuration validations and health checks pane 66
Generating a Cabling Diagram 68
Generating a PDF report 69
Generating an MS Excel report 70
Generating an MS Word report 70
Merging reports from multiple result files 70
Working with credentials 72
Password encryption 72
Updating query group password 73
Using forget password option 74
Saving credentials 75
Loading a query 76
Setting Preferences in Config Advisor 78
Disabling Telnet 78
Enabling Config Advisor AutoSupport 78
What Config Advisor AutoSupport is 79
Enabling or disabling Config Advisor logs pane 80
What Config Advisor logs pane is 80
Periodic data collection for issues diagnostic 81
Using Config Advisor through the command prompt 81
Scheduling periodic data collection 83
Email notification 84
Reporting issues in Config Advisor 85
Using Config Advisor in secure sites 86
Keeping the resource data updated 86
What data collector and sanitizer script is 86
Prerequisites for using the data collector and sanitizer script 87
Installing PowerShell 2.0 87
Installing Data ONTAP PowerShell toolkit 2.0 88
Running the script 89
Data collection methods for secure sites 91
Interactive data collection method 91
Batch-mode data collection method 93
Command-line argument method 94
Collecting data manually 98
Filtering and mapping 102

Collecting and filtering data 103
Filtering precollected data 103
Importing filtered data file for analysis 107
Launching Help for the script 109
Troubleshooting 110
Entering AutoSupport ID in the old format displays an error message 110
Cabling faults not identified for FC and SATA shelves 112
Format of the text file for the AutoSupport (from file) tab 113
Config Advisor logs pane displays data collection failure for certain ONTAP commands 113
Cabling faults not identified for optical SAS cables with non-integrated QSFP present in a stack 114
Sending email displays an error message 115
Appendix A: Configuration validations & health checks 116
Copyright information 127
Trademark information 128
How to send your comments 129

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. Partners and customers may use this document for 7-Mode to ONTAP transition use case.

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
Italic font	• 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.
`Consolas` 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 `consolas` 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.

Terminology

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

- *Controller, storage controller, or node*- The component of a storage system that runs the 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 ONTAP that receives data from and sends data to native disk shelves, third-party storage, or both. Storage systems that run ONTAP are sometimes referred to as *filers*, *appliances*, *storage appliances*, *V-Series systems*, or *systems*.

Definitions, acronyms, and abbreviations

Abbreviation/Phrase	Explanation/ Definition
ONTAP configuration	The integration of Ethernet switch fabrics into NetApp Scale Out Storage Cluster solution
LIF	Logical interface Formerly "VIF" in GX. A logical network port, representing a network access point to a node. LIFs currently correspond to IP addresses, but could be implemented by any interconnect
ISL	Inter-Switch Link
HA pair	High Availability pair The recovery capability provided by a pair of nodes (storage systems) called an HA pair that are configured to serve data for each other if one of the two nodes stops functioning. This functionality is referred to as an active/active configuration
LACP	Link Aggregation Control Protocol, part of IEEE 802.3ad, allows bundling of multiple physical network ports together to form a single logical channel (but need ONTAP 7.2.1 or later to use dynamic aggregation)
NIC	Network Interface Card Computer circuit board or card that is installed in a computer so that it can be connected to a network. Network interface cards provide a dedicated, full-time connection to a network
SFP	Small Form-factor Pluggable (a type of connector for fiber-optic cables)
CDP	Cisco Discovery Protocol

Abbreviation/Phrase	Explanation/ Definition
ARS	At Risk Systems
HA	High Availability (NetApp support for failover: one appliance assuming the duties of another that has failed)
ASUP	AutoSupport is NetApp 'phone home' mechanism that allows our products to do automated configuration, status and error reporting
FTP	File Transfer Protocol
MPHA	*Multipath High Availability* provides multiple and redundant connections from the controller to a storage
SP	Service Processor
RLM	Remote LAN Module
BMC	Baseboard Management Controller
ACP	Alternate Control Path
Config Advisor ASUP	AutoSupport feature that is used by Config Advisor to send Config Advisor ASUP (CA_ASUP) messages to NetApp. Config Advisor ASUP messages may contain information from multiple devices including controllers, switches and others. As such, these messages might contain data collected from multiple devices, both NetApp systems and non-NetApp systems
UCS	Unified Computing System
FCP	Fibre Channel Protocol
FCoE	Fibre Channel over Ethernet
FQDN	Fully Qualified Domain Name
QoS	Quality of Service
MTU	Maximum Transfer Unit
KVM	Keyboard Video Mouse
QSFP	Quad (4-channel) Small Form-factor Pluggable

Introduction to Config Advisor

Config Advisor is a configuration validation and health check tool for NetApp systems. It can be deployed at both secure sites and non-secure sites for data collection and analysis.

Config Advisor can be used to check a NetApp system for the correctness of hardware installations and conformance to the recommended settings. It runs a series of commands and checks for configurations with cabling, availability and resiliency issues. The flexible data collection architecture supports data collection from network, serial port, AutoSupport ID, and AutoSupport file. Config Advisor collects information from NetApp controllers, switches, and Cisco *Unified Computing System* (UCS*)*, which are compared with configuration best practices.

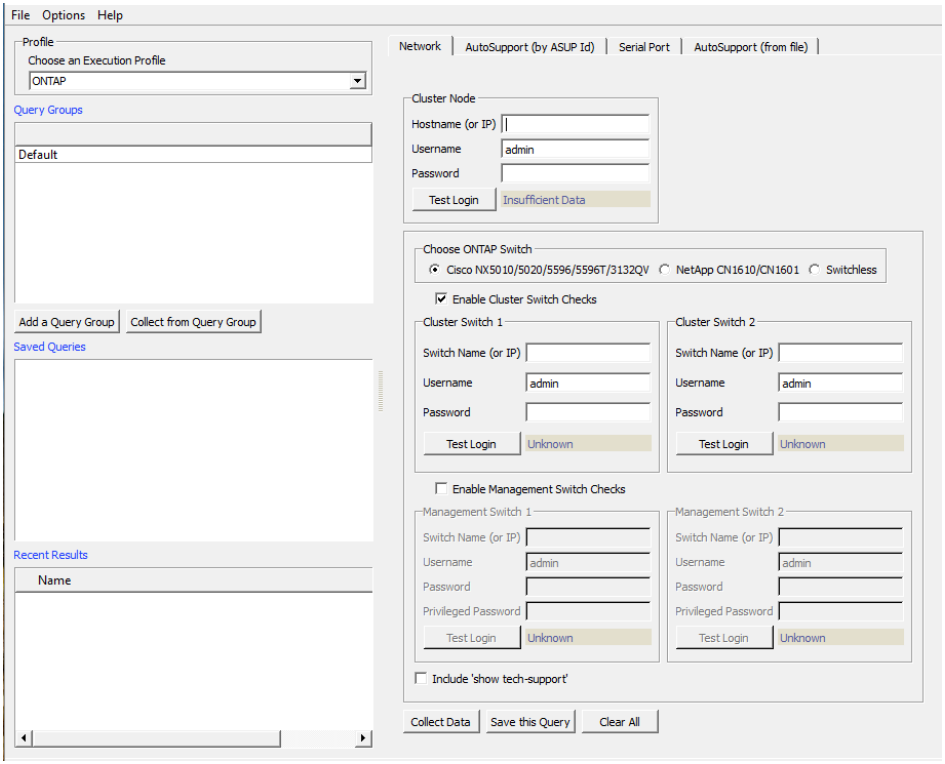
Starting from Config Advisor 4.0 you can extend the behavior of Config Advisor by installing third-party plug-ins. Plug-ins can introduce new profiles, such as MetroCluster in clustered Data ONTAP, E-Series, FlexArray, FlexPod, and Managed ONTAP SAN to the existing data collection profiles.

What Config Advisor is

Config Advisor is a light-weight tool that can be used to improve the quality of system setups, upgrades, and diagnostics.

Config Advisor has extended its support for secure sites that demand high levels of data security by adding capabilities for collecting and analyzing data in a secure manner. For more information, see *Using Config Advisor in secure sites*.

The **Config Advisor** tool is as shown:



Config Advisor can be used in the following scenarios:

- **System setup**: Config Advisor can be used during installation of new equipment, and adding of new disk shelves. It can also be used during moving, and changing of equipment as it requires close attention to cabling and conformance to NetApp best practices.
- **Operational health checks**: Config Advisor can be used on a monthly or quarterly basis to detect any new issues resulting from configuration changes or non-conformance to NetApp best practices.
- **Support case handling and secure sites**: Config Advisor can be used to triage and diagnose issues with NetApp systems that do not send AutoSupport messages.

- **Prechecks for Copy-Free Transition**: Copy-Free Transition enables you to disconnect all of the disk shelves from a 7-Mode HA pair and connect them to an HA pair in the target cluster. You can convert data in the disk shelves to ONTAP format and transition the 7-Mode configurations by using the 7-Mode Transition Tool.

  After connecting the disk shelves to ONTAP, you can use Config Advisor to run prechecks for Copy-Free Transition.

Features in Config Advisor

The features available in Config Advisor are as follows:

- Data collection from Data ONTAP 7 and Data ONTAP 8.x (7-Mode)
- Data collection from Clustered Data ONTAP 8.x and ONTAP 9.x (Cisco switches, NetApp switches, or switchless)
- Secure-site data collection and sanitization (systems running ONTAP operating in 7-Mode)
- Secure site install profile that disables AutoSupport posting, user registration, and restricts Telnet
- Native AutoSupport file maybe used as a data source
- Batch Mode Collection is available to all of the profiles
- Configuration checks for Data ONTAP 8.x and ONTAP 9.x
- SAS cabling checks for SAS-2 and SAS-3 shelves
- Prechecks for Copy-Free Transition
- Raw data viewer window
- System results view window (cabling, system configuration summary, evaluated rules, and so on)
- SAS cabling diagrams for SAS-2 shelves (Beta feature)
- Flexible reporting options: PDF, MS Word, and MS Excel
- Merge reports from multiple result files
- Config Advisor AutoSupport call home

- Encryption of device credentials saved in query groups
- Periodic configuration checks and email notification for plug-ins

  Config Advisor can be extended with additional features by installing plug-in. The plug-in available for download along with Config Advisor are as follows:

- Configuration checks for MetroCluster in clustered Data ONTAP
- Configuration checks for E-Series
- Mission critical system checks
- Configuration checks for FlexPod
- Configuration and topology checks for FlexArray

Configurations supported by Config Advisor

Config Advisor is a lightweight Windows binary executable (less than 60 MB) that can run on the following Windows versions.

- Windows 7 (64-bit and 32-bit)
- Windows 8 (64-bit and 32-bit)
- Windows 10 (64-bit and 32-bit)
- Windows 2008 R2 Server (64-bit and 32-bit)
- Windows 2012 R2 Server (64-bit)

Config Advisor supports the FAS (2xxx, 3xxx, 6xxx, 8xxx, and 9xxx) running Data ONTAP 8.x and ONTAP 9.x, Data ONTAP 7.x and 8.x operating in 7-Mode, and Copy-Free Transition prechecks on ONTAP, Config Advisor supports FlexPod Datacenter running Cisco Nexus 5000, 7000, and 9000 fabric switches, FlexArray, MetroCluster in clustered Data ONTAP, and E-Series as plug-ins.

Cisco Ethernet switch matrix

The Cisco Ethernet switches supported by Data ONTAP 8.x are as follows:

Cisco Switch Model	NX-OS Version	IOS Version	RCF Version	Data ONTAP Version	Notes
Cisco Nexus 3132Q-V	7.0(3)I4(1)		NX3132_RCF_v1.1_24p10g_26p40g.txt (default) NX3132_RCF_v1.1_72p10g_14p40g.txt	9.1.0	
NX5596T	7.1(1)N1(1)		1.3	8.3.1 or later	
	5.2(1)N1(8b)		1.3	8.2.3 and later	
NX5596UP	7.1(1)N1(1) 5.2(1)N1(8b) 5.2(1)N1(1)		1.3-64p	8.2.2 and later (8.3.1 or later for 7.1(1)N1(1))	Use RCF version 1.3-64p if you install a single 16-port unified expansion module; use version 1.3-80p if you install two expansion modules. This module is required if the cluster has more than 20 nodes, and all nodes require two cluster ports to be connected to each cluster switch.
			1.3-80p		

Cisco Switch Model	NX-OS Version	IOS Version	RCF Version	Data ONTAP Version	Notes
			1.3	8.1.2 and later	
NX5010/ NX5020 (cluster)	5.2(1)N1 (8b) 5.2(1)N1 (1)		1.3	8.2.2 and later	
	5.0(2)N1 (1)		1.2	8.0.2 to 8.1.x	If you are upgrading the cluster network switch to 5.0(2)N1(1) from 4.0(1a)N1(1a), you must download the cluster network switch RCF first for the purposes of a non-disruptive upgrade.
	4.0(1a)N 1(1a)		1.1	8.0 to 8.0.x	
Catalyst 2960 (Manage ment)		12.2.55. SE	1.3	8.1.2 and later	
			1.2	8.0.2 to 8.2.0	
Catalyst 2960 (Manage ment)		12.2.46. SE	1	8.0 to 8.0.1	

NetApp CN1601 and CN1610 switches

The switch operating systems supported by Data ONTAP 8.x and ONTAP 9.x are as follows:

Switch	Switch OS FASTPATH Version	RCF Version	Minimum Data ONTAP Versions	Notes
CN1610 Cluster Switch	1.2.0.7	1.2	8.2.4, 8.3.2RC1	
	1.1.0.8	1.1	8.2.3 and later, 8.3.1 and later	
	1.1.0.7	1.1	8.2.2 and later	
	1.1.0.5	1.1	8.2.2 and later	
	1.1.0.3	1.1	8.2 and later	
	1.1.0.1	1	8.1.x only	
CN1601 Management Switch	1.1.0.8	1.1	8.2.3and later, 8.3.1 and later	
	1.1.0.7	1.1	8.2.2 and later	
	1.1.0.5	1.1	8.2.2 and later	
	1.1.0.3	1.1	8.2 and later	
	1.1.0.1	1	8.1.x only	
CN1601 Cluster Switch	1.1.0.1	1	8.1.x only	The CN1601 used as a cluster switch is only compatible with NetApp FAS2220 platforms. This configuration is no

Switch	Switch OS FASTPATH Version	RCF Version	Minimum Data ONTAP Versions	Notes
				longer supported in 8.2 and later versions.

Installing, extending, configuring, upgrading, and uninstalling Config Advisor

You can download, install, extend, perform initial configuration, uninstall, and upgrade the Config Advisor tool and its dependencies.

Installing Config Advisor

Steps

1. Download the Config Advisor binary file.

   http://mysupport.netapp.com/tools/info/ECMS1357843I.html?productID=61923

2. Install the tool by completing the steps in the installation wizard.

   The default installation folders for Config Advisor on different operating systems are as follows:

Operating system	Default installation folder
Windows 32-bit	C:/Program Files/NetApp/ConfigAdvisor
Windows 64-bit	C:/Program Files (x86)/NetApp/ConfigAdvisor

3. You can edit the default installation folder and install Config Advisor in a shared folder or a pen drive.

4. You can select the Config Advisor data directory from the installation wizard which defaults to the user home directory. This configuration is available only at the time of

installation. With this, you can now install and launch Config Advisor from a shared folder or a pen drive.

Note: This document specifies the ConfigAdvisorData directory as ConfigAdvisorDataDirectory_Base.

5. You can install Config Advisor by selecting whether or not you are at a secure site. If you are at a secure site, AutoSupport is switched off, user credentials are not collected, and Telnet is disabled. However, these settings may be revisited using **Options** > **Preferences** items.

6. Select **Run Config Advisor** in the installer to automatically launch Config Advisor tool after the installation is complete.

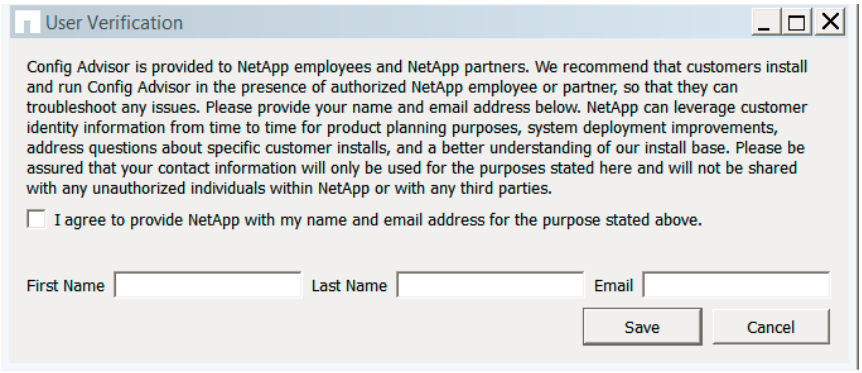
Note: The Data Collector and Sanitizer script is integrated in the tool and will be available in the installation folder as: C:/Program Files/NetApp/ConfigAdvisor or C:/Program Files (x86)/NetApp/ConfigAdvisor.

You can also start Config Advisor by using the Config Advisor icon on your desktop, or from the **Start** menu.

Accessing Config Advisor

On the first launch of Config Advisor, **User Verification** dialog box is displayed, which asks the user to enter the **First Name**, **Last Name**, and **Email** address.

You can use Config Advisor with or without providing the information in the **User Verification** window. If you enter the information, credentials included in the login screen are sent to NetApp in the Config Advisor AutoSupport messages.



In case, you decide not to enter the login details during the initial login, you can revisit the dialog box on later launches.

Steps

1. Navigate through the menu items **Options** > **User Verification Settings**.
2. Enter your name and email address.

Installing plug-in

Steps

1. Download the plug-in compressed file.

You can download the available plug-ins from the following link:

http://mysupport.netapp.com/NOW/download/tools/config_advisor/

Note: Do not install plug-in from any other sources as they could be malicious.

2. Unzip the plug-in and save the extracted folder into the ConfigAdvisorData/plugin_eggs directory. The ConfigAdvisorDataDirectory can be found in the user home directory or specified at the time of installation. This directory is created when the Config Advisor is launched. Make sure that when opening the plug-in folder under the plugin_eggs directory, you are able to see the plug-in files.
3. Re-launch Config Advisor. New plug-ins will be available in the profile drop-down box.

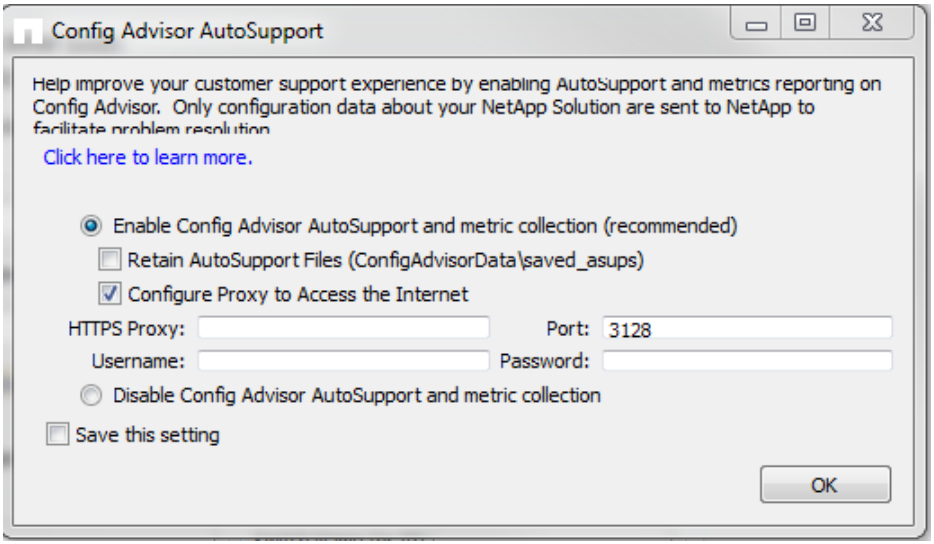
Note: Using the E-Series plug-in will require additional steps that are documented in the Plug-in Installation and Administration Guide.

Configuring Config Advisor AutoSupport

Similar to ONTAP, Config Advisor sends the collected configuration data back to NetApp through its own AutoSupport. This information is used by NetApp Support and partners to improve problem diagnostics. When you first launch Config Advisor, the **Config Advisor AutoSupport** dialog box is displayed. The dialog box provides you an option to enable or disable Config Advisor AutoSupport.

Note: If your internet connection is through a proxy, set the same proxy setting to enable Config Advisor AutoSupport. Basic authentication is supported for Proxy Servers.

The **Config Advisor AutoSupport** dialog box is as shown:



You can update your preference settings. For details, see Setting Preferences in Config Advisor.

You can select the Retain Config Advisor AutoSupports checkbox to save the Config Advisor AutoSupports in the ConfigAdvisorDataDirectory_Base/ConfigAdvisorData/saved_asups directory.

Note: If you enable Config Advisor AutoSupport, Config Advisor sends the First Name, Last Name, and Email ID along with the other configuration details to NetApp.

Upgrading Config Advisor and firmware recommendations

On startup, after the initial configuration, Config Advisor notifies you if a new version of the tool is available for upgrade. The **Config Advisor Notification** window is automatically displayed when an upgrade is available and the tool is connected to a network. If Config Advisor is not connected to the network, the log message "`Config Advisor update notification and resource file update failed. Reference "Using Config Advisor in secure sites" in the Installation and Administration Guide to update the file manually or relaunch with Network being available.`" is displayed in the **Config Advisor Logs** pane.

Config Advisor notification also updates Config Advisor to use the latest firmware recommendations. The latest recommendations are downloaded from the Internet and placed in the Config Advisor data folder.

Note: The notification window has a Remind me later check box. If checked and there is no new version from the notification, then the Config Advisor notification window is disabled for two weeks.

You can also manually check for new updates.

Steps

1. Open **Config Advisor** and click **Help** > **Check for Updates**.

   If a new version of the tool is available, the Config Advisor **Notification** dialog box is displayed.

2. Click the appropriate link in the dialog box to download the Config Advisor executable file and install the newer version.

Note: You should not uninstall the previous version of the tool or delete the data folder during the upgrade. The tool uninstalls the previous version and replaces it with the latest. It retains all the contents in the data folder.

If no network connection is available, the Config Advisor resource file should be manually kept updated. For more information, see *Keeping the resource data updated.*

Upgrading plug-in

On startup, after the initial configuration, Config Advisor notifies you if a new version of the plug-in extensions is available for upgrade. The **Config Advisor Notification** window is automatically displayed when an upgrade is available and the tool is connected to a network. If Config Advisor is not connected to the network the log message Config Advisor upgrade notification is temporarily unavailable is displayed in the **Config Advisor Logs** pane.

Note: The notification window has a Remind me later check box. If an upgrade is available, and the user selects the check box, then the Config Advisor notification window is disabled for two weeks or until the notification is updated with a newer release of Config Advisor plug-in.

The check box Remind me later is not displayed, if the notification window is accessed through Menu Bar.

You can also manually check for new updates.

Steps

1. Open Config Advisor and click **Help** > **Check for Updates**.

   If a new version of the plug-in is available, then the **Config Advisor Notification** dialog box is displayed.

2. Click the appropriate link in the dialog box to download the compressed plug-in file and install the newer version.

3. Extract and replace the plug-in folder in the ConfigAdvisorDataDirectory_Base/ConfigAdvisorData/plugin_eggs directory.

4. Relaunch Config Advisor. New version of the plug-ins will be available in the **Profile** drop-down box.

Uninstalling plug-in

Delete the plug-in from the ConfigAdvisorDataDirectory_Base /ConfigAdvisorData/plugin_eggs directory.

Collecting data

You can find information about the Config Advisor data collection, viewing the collection progress, collection profiles, data collection methods, fields in the tabs, saving your credentials, and viewing the collected results.

Note: If you are collecting data in a secure site, see *Using Config Advisor in secure sites*.

Data collection profiles

Config Advisor supports three data collection profiles:

- ONTAP
- Data ONTAP 7 and 8 (7-Mode)
- Transition

Collecting data from ONTAP

Config Advisor can be used to verify the ONTAP installation by analyzing data collected from a clustered controller, cluster switches, and management switches. To perform a minimal ONTAP data collection, you should enter the credentials for at least one cluster switch and a controller.

In the ONTAP profile, you can choose any one of the following (based on the network switch used):

- Cisco NX5010/5020/5596/5596T/3132QV
- NetApp CN1610/CN1601
- Switchless

To verify configurations, you should ensure the following:

- The data is collected from cluster switches, management switches, and a controller.
- The controller connection is made to either a cluster-management logical interface (LIF) or a node-management LIF (must be capable of responding to the data collection methods of Config Advisor).
- Based on the cluster switch used, the cluster type is chosen before the data collection.

The connections to a controller by using a Service Processor, RLM, BMC, or ACP are not supported.

If the credentials are not entered for the management switches, the health checks for these switches are not executed. For more information about health checks, see *Appendix A: Configuration validations & health checks*.

Collecting data by using the Network tab

Note: The process of collecting data from any one of the cluster profiles is the same.

Steps

1. Enter the login details for the controller, cluster switches, and management switches

   You must enter the credentials of a cluster switch and one cluster node. Alternatively, you can select the login credentials from the **Query Groups** pane. For more information, see *Saving credentials*.

2. Click **Test Login** to test the network connection for each system.

3. Click **Collect Data** to start the data collection.

   The **Results File** dialog box is displayed.

4. Enter a name for the result file or accept the default name, and click **OK.**

   The data collection starts and a progress bar is displayed. The command exceptions are displayed in the **Config Advisor Logs** pane.

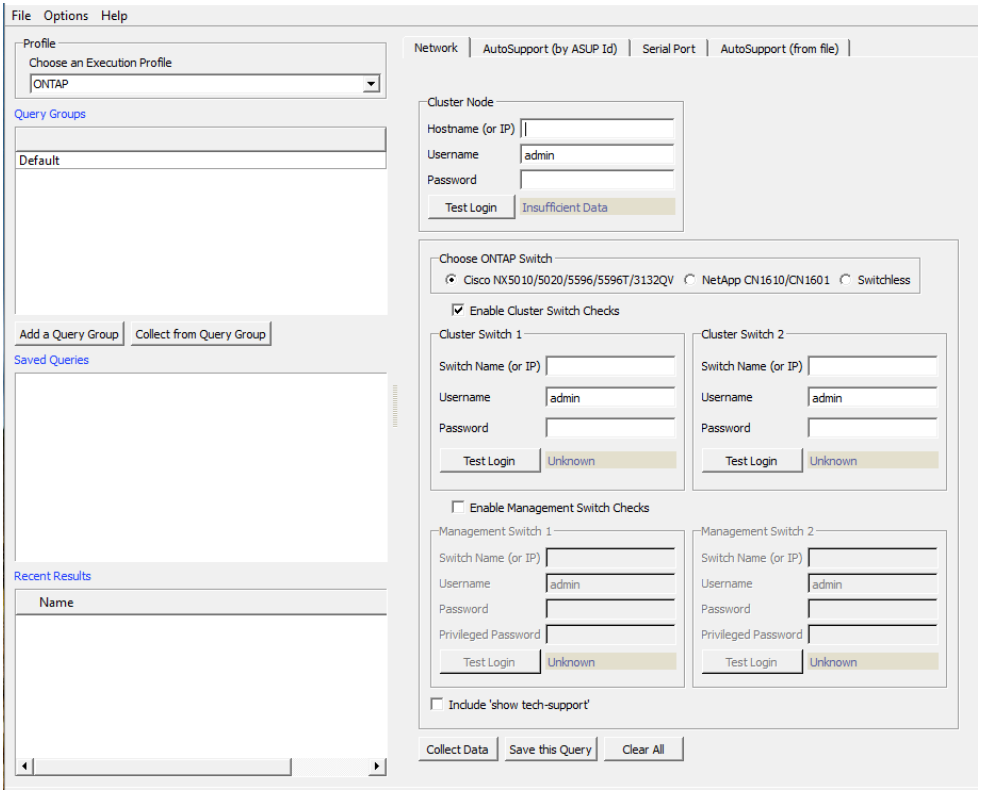
   After the data collection and analysis are complete, the result file is displayed in the **Recent Results** pane. For more information about this pane, see *Recent Results pane*.

Note: Data collection takes place and a Config Advisor result file is displayed even if the status check on a node fails.

5. Click **Save this Query** to save the credentials as a query.

For more information about saving credentials, see *Saving credentials*.

The ONTAP 8.x **Network** tab is as shown:



Fields in the ONTAP Network tab

The fields in the ONTAP 8.x Network tab are as follows:

GUI field/GUI button	Description
Hostname (or IP)	Host name or IP address of the controller or the switches
Switch Name (or IP)	Host name or IP address of the switches
Username	User name to access the controller or the switches
Password	Password to access the controller or the switches
Privileged Password	Password required to run certain special commands on the switches
Test Login	Displays the connection status • Config Advisor attempts to connect to Cisco NX5010/5020/5596/5596T/3132QV in the following order: SSH > Telnet • Config Advisor attempts to connect to NetApp CN1610/NetApp CN1601/Cisco Catalyst 2960 in the following order: SSH > Telnet • Config Advisor uses a protocol fallback mechanism to connect to the storage controller in the following order: HTTPS > HTTP > SSH > Telnet The statuses are as follows: • **Insufficient Data**: Displayed if the device name and credentials are not entered • **Click on 'Test Login' to verify**: Displayed if all the necessary details are entered • **Valid <login type> Login**: Displayed if the connection is valid, where the login type is HTTPS, HTTP, SSH, or Telnet • **Connection Failed**: Displayed if the connection to the device fails **Note**: The connection to a device fails if the host name or IP details are wrong, or if the device type is wrong, or if the device is powered off. Additional information about the failure is displayed in the **Config Advisor Logs** pane.
Collect Data	Collects data from Data ONTAP 8.x or ONTAP 9.x
Save this Query	Saves the login credentials as a query for later use
Clear All	Clears all the information entered in the fields

Note: The Config Advisor Log pane that is at the bottom of the main Config Advisor window has two tabs, Info and Errors. These tabs display details of data collection and connection

testing processes. The pane also shows log details for Status, Invalid Credentials, and Connection Failure (along with the reasons for failure).

Collecting data by using the Serial Port tab

You can use the **Serial Port** tab if you do not have access to the customer's network. Direct access to the controller firmware is gained through the serial port.

Note: The process of collecting data from any one of the cluster profiles is the same.

Steps

1. Choose a COM port from the drop-down list for the NetApp controller, cluster switches, and management switches.
2. Enter the login credentials.

   Alternatively, you can select the login credentials from the **Query Groups** pane. For more information, see *Saving credentials*.
3. Click **Test Login** to test the connection for each system.
4. Click **Collect Data** to start the data collection.

   The **Results File** dialog box is displayed.
5. Enter a name for the result file or accept the default name, and click **OK.**

   The data collection starts and a progress bar is displayed. The command exceptions are displayed in the **Config Advisor Logs** pane.

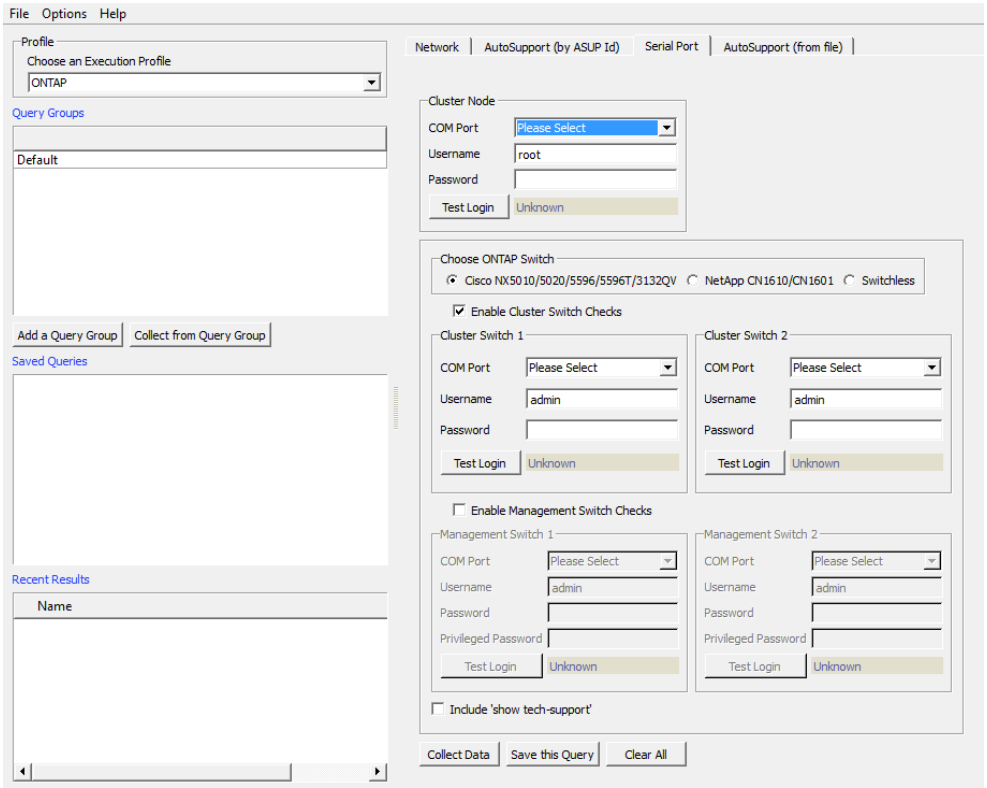
   After the data collection and analysis are complete, the result file is displayed in the **Recent Results** pane. For more information about this pane, see *Recent Results pane*.

Note: Data collection takes place and a Config Advisor result file is displayed even if the status check on a node fails.

6. Click **Save this Query** to save the credentials as a query.

For more information about saving credentials, see *Saving credentials*.

The ONTAP 8.x **Serial Port** tab is as shown:



Fields in the ONTAP Serial Port tab

The fields in the ONTAP 8.x **Serial Port** tab are as follows:

GUI field/GUI button	Description
COM Port	COM port to which you have connected the storage controller or switch
Username	User name to access the controller or the switches
Password	Password to access the controller or the switches
Privileged Password	Password required to run certain special commands on the switches
Test Login	The connection statuses are as follows: • **Insufficient Data**: Displayed if the device name and credentials are not entered • **Click on 'Test Login' to verify**: Displayed if all the necessary details are entered • **Valid <login type> Login**: Displayed if the connection is valid. • **Connection Failed**: Displayed if the connection to the device fails.
Collect Data	Collects data from ONTAP 8.x or ONTAP 9.x
Save this Query	Saves the login credentials as a query for later use
Clear All	Clears all the information entered in the fields

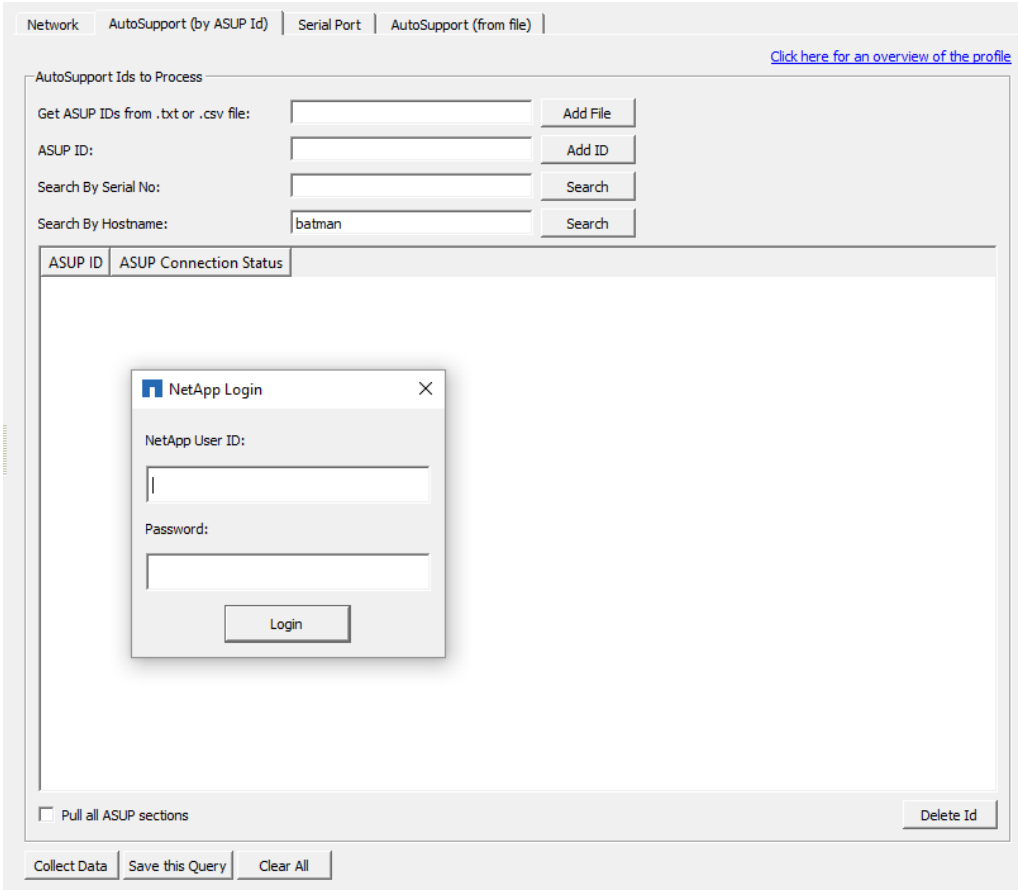
Collecting data using AutoSupport (by ASUP Id) tab

Config Advisor can perform analysis using the NetApp AutoSupport Datawarehouse as data input source. You can submit a list of AutoSupport Ids in a file or search for them interactively.

Note: This method is available only to NetApp personnel who have access to the intranet and the AutoSupport Data warehouse. It is not available to partners and NetApp customers.

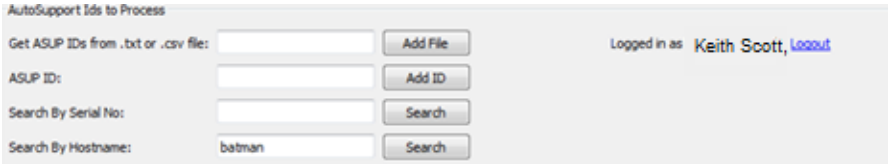
Config Advisor allows loading and collecting data from ASUPs only with NetApp SSO entitlements. Before Config Advisor allows for an ASUP query, SSO login dialog box is displayed.

SSO login dialog box is as shown:



On successful login, the ASUP query proceeds and the user name is presented in the UI with a **Logout** link.

The **Logout** link is as shown:



Note: When a query or data collection is initiated with entitlements it will proceed even when the Logout link is clicked. Subsequent queries or data collection will again request for entitlements.

Steps

1. Click **Add File** to select a file (.csv, .txt) containing multiple AutoSupport IDs.

Multiple AutoSupport IDs are displayed in the **ASUP ID** column along with their connection statuses.

2. Alternatively, you can add an AutoSupport ID using one of the following methods:

   a) Enter the ID in the **ASUP ID** field and click **Add ID**.

Note: The older ASUP ID format (for example, AE2010061286069) is not supported in Config Advisor 3.0 and later. You must enter the ASUP ID in the new format, for example, 2010061918120050.

   b) Enter serial number of the controller in the **Search By Serial No** field, and click **Search**.

   c) The Config Advisor ASUP IDs from **Serial No Search** dialog box is displayed. Select the ASUP IDs, and click **Add Selected ASUPs**.

The ASUP IDs are displayed in the **ASUP ID** column along with their connection statuses.

3. Enter host name of the controller in the **Search By Hostname** field, and click **Search**.

   The Config Advisor **ASUP IDs from Hostname Search** dialog box is displayed.

4. Select the appropriate ASUP IDs, and click **Add Selected ASUPs**.

The selected ASUP IDs are displayed in the **ASUP ID** column along with their connection statuses.

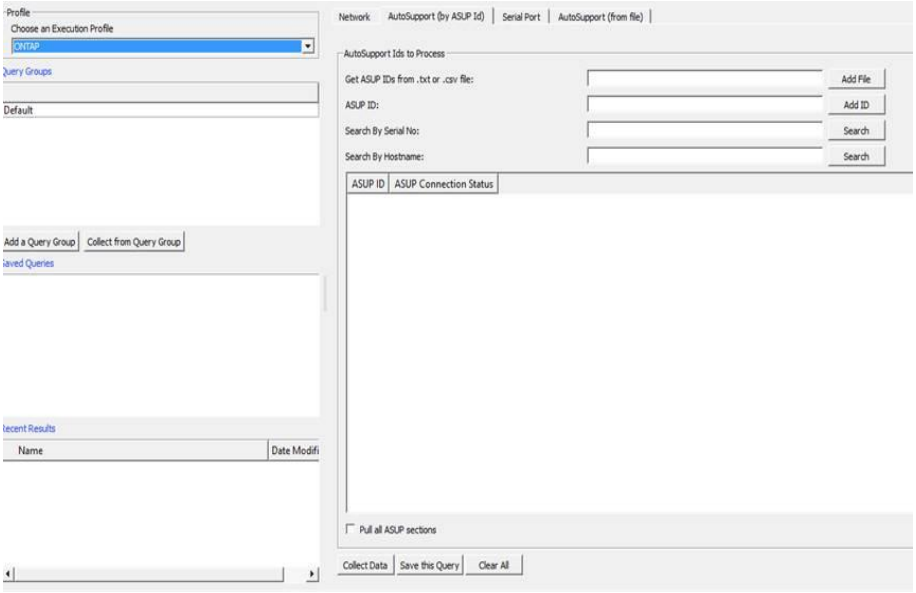
Note: You can enter multiple comma-separated host names or system serial numbers, with no space.

5. To delete an ASUP ID from the displayed list, select the ID and click **Delete ID**.
6. Select the **Pull all ASUP sections** check box to collect from all of the sections of the AutoSupport.
7. Click **Collect Data** to start the data collection.
8. The **Results File** dialog box is displayed.
9. Enter a name for the result file or accept the default, and click **Ok**. After the data collection and analysis are complete, the result file is displayed in the **Recent Results** pane.

For more information about the **Recent Results** pane, see *Recent Results pane.*

10. Click **Save this Query** to save the AutoSupport IDs as a query. For more information about saving credentials, see *Saving credentials*.

The **AutoSupport (by ASUP Id)** tab is as shown:



Note: This tab is visible only to users who have access to NetApp intranet and the AutoSupport Data warehouse.

Fields in AutoSupport (by ASUP Id) tab

The fields in the **AutoSupport (by ASUP Id)** tab are as follows:

GUI field/GUI button	Description
Get ASUP IDs from .txt or .csv file	.csv or .txt file containing multiple AutoSupport IDs
Add File	Adds the selected .csv or .txt file containing multiple AutoSupport IDs
ASUP ID	AutoSupport ID of a controller
Add ID	Adds the entered AutoSupport ID • The AutoSupport ID is verified and the status is displayed • You cannot make duplicate entries of the same AutoSupport ID
Search By Serial No.	Allows you to search for ASUP IDs by serial numbers of controllers
Search By Hostname	Allows you to search for ASUP IDs by host names of controllers

GUI field/GUI button	Description
ASUP Connection Status	Displays the status of the AutoSupport ID
Delete Id	Deletes the selected AutoSupport ID from the list
Collect Data	Collects data from a storage controller
Save this Query	Saves the AutoSupport IDs from the table as a query for later use
Clear All	Clears all the information entered in the fields

Collecting data by using the AutoSupport (from File)

Config Advisor can perform an analysis using the AutoSupport file from a NetApp storage system.

Steps

1. Click **Add File** and choose an AutoSupport file.

   AutoSupport files in the .tgz, .7z, and .txt formats are supported.

   a) Alternatively, you can select a query from the **Query Groups** pane. For more information, see *Saving credentials*.

   b) You can select the **Pull all ASUP sections** check box to collect from all of the sections of the AutoSupport.

2. Click **Collect Data** to start the data collection.

   The **Results File** dialog box is displayed.

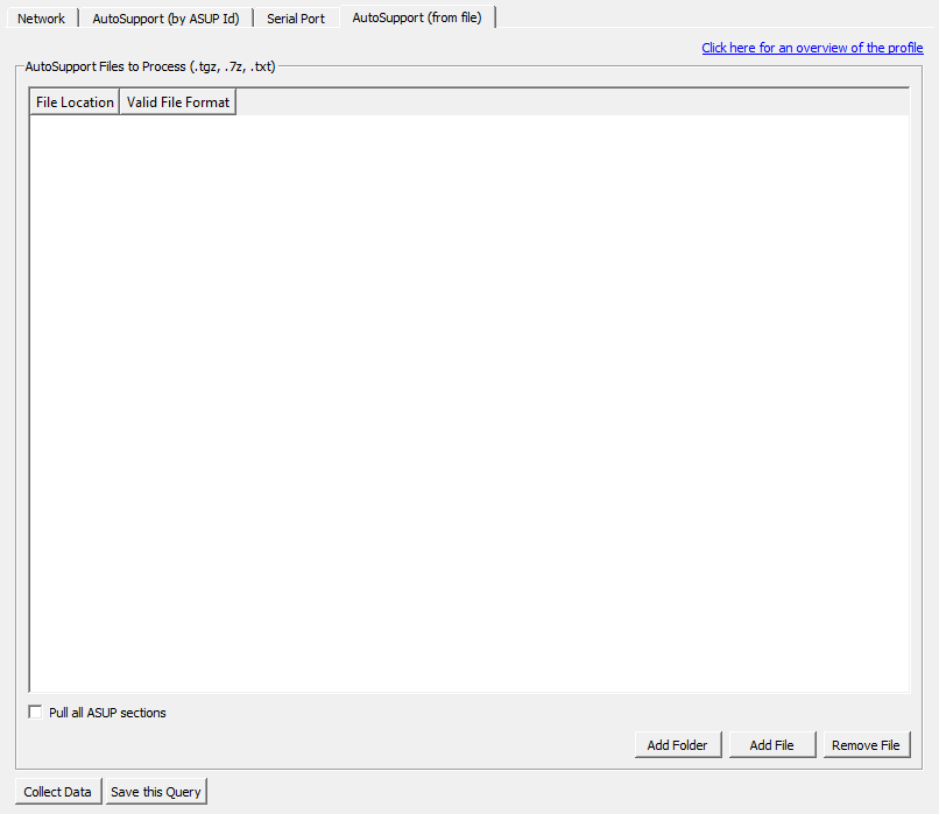
3. Enter a name for the result file or accept the default, and click **Ok**.

   When the data collection and analysis are complete, the result file is displayed in the **Recent Results** pane. For more information about this pane, see *Recent Results pane*.

4. Click **Save this Query** to save the file as a query.

   For more information about saving credentials, see *Saving credentials*.

The **AutoSupport (from file)** tab is as shown:



Fields in AutoSupport (from file) tab

The fields in the AutoSupport (from file) tab are as follows:

GUI field/GUI button	Description
File Location	Displays the path from where the file was loaded
Valid File Format	Displays Verified if Config Advisor is able to validate or read the file format
Add File	Adds a file from the selected location • When you add a file, it is verified before it is added to the list • If you add an invalid file, an error message is displayed and the file is not added to the list
Remove File	Removes the AutoSupport file from the list
Collect Data	Collects data from AutoSupport files
Save this Query	Saves the file path as a query for later use

Collecting data from a Data ONTAP 7 and Data ONTAP 8 (7-Mode) installation

In the Data ONTAP operating in 7-Mode profile, you can collect data by using one of the following tabs in Config Advisor:

- Network
- Serial Port
- AutoSupport (by ASUP Id)
- AutoSupport (from file)

Note: Config Advisor checks only the default vFiler context (pFiler).

Note: AutoSupport (by ASUP Id) refers to AutoSupport IDs from NetApp AutoSupport Datawarehouse.

AutoSupport (from file) refers to files from your local file system.

You can use the **Click here for details on this profile** link for each of the tabs to find out details about the current profile.

Note: The connections to a controller by using a Service Processor (SP), Remote LAN Module (RLM), Baseboard Management Controller (BMC), or Alternate Control Path (ACP) are not supported in 7-Mode.

Collecting data by using the Network tab

Using the **Network** tab, you can collect data from a single node or both nodes of a high-availability (HA) pair.

Note: You should not collect data from a single node of an HA pair, because it might result in HA-related health checks not being run.

Steps

1. Enter the login details for the two nodes in an HA pair

   Alternatively, select the login credentials from the **Query Groups** pane. For more information about saving the credentials, see *Saving credentials*.

2. Select the checks to be included.

   Note: If you select 7-Mode Health Checks (includes all 7-Mode Install Checks, best practice checks and At-Risk-System (ARS) checks), the Include Extended Health Checks check box is enabled. You can select this check box if you want to run additional checks on the system. The extended health checks involve parsing and analyzing etc/messages, which takes longer to process.

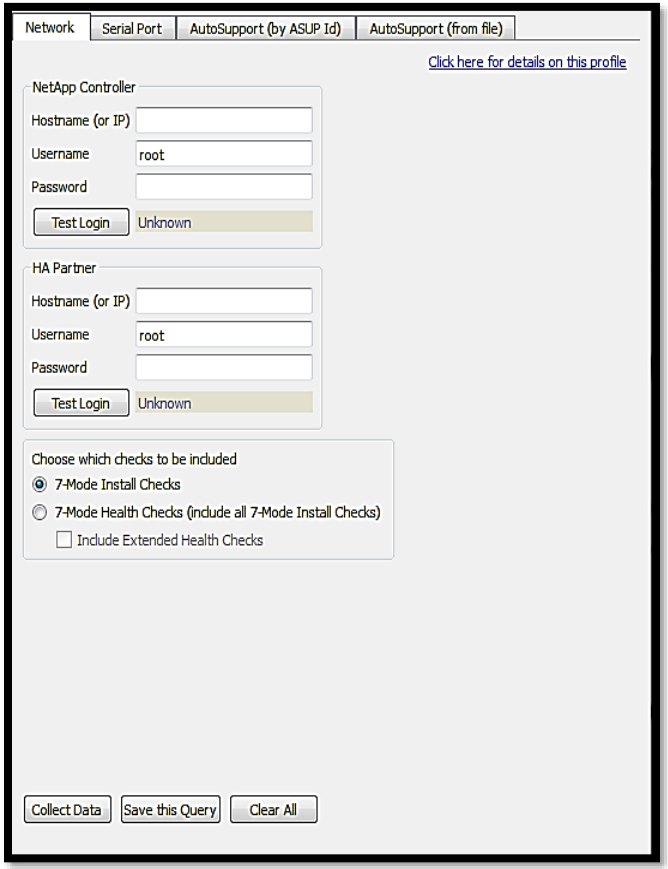
3. Click **Test Login** to test the connection.
4. Click **Collect Data** to start the data collection.
5. The **Results File** dialog box is displayed.
6. Enter a name for the result file or accept the default.
7. Click **Ok**.

   After the data collection and analysis are complete, the result file is displayed in the **Recent Results** pane.

   For more information about the **Recent Results** pane, see *Recent Results pane*.

The 7-Mode **Network** tab is as shown:

Fields in 7-Mode Network tab



The fields in the 7-Mode **Network** tab are described as follows:

GUI field/ button	Description
Hostname (or IP)	Host name or IP address of the controller
Username	User name to access the controller
Password	Password to access the controller
Test Login	Displays the connection status Config Advisor attempts to connect to the NetApp controller in the following order: • HTTPS • HTTP • SSH • Telnet The statuses are as follows: • **Insufficient Data**: Displayed if the device name and credentials are not entered • **Click on 'Test Login' to verify**: Displayed if all the necessary details are entered • **Valid <login type> Login**: Displayed if the connection is valid, where the login type is HTTPS, HTTP, SSH, or Telnet • **Connection Failed**: Displayed if the connection to the device fails • **Invalid Credentials**: Displayed if the invalid credentials for the device are entered **Note**: The connection to a device fails if the host name or IP details are wrong, or if the device type (the device type can only be 7-Mode storage controller) is wrong, or if the device is powered off. Additional information about the failure is displayed in the **Config Advisor Logs** pane.
7-Mode Install Checks	Collects data from a single NetApp storage system or both nodes of an HA pair running Data ONTAP 7.x or Data ONTAP 8.x operating in 7-Mode. It collects data through a network connection to each controller. The rules for this profile include only installation checks and not all NetApp best practices or At-Risk-Systems (ARS) checks.

GUI field/ button	Description
7-Mode Health Checks (include all 7-Mode Install Checks)	Collects data from a single NetApp storage system or both nodes of an HA pair running Data ONTAP 7.x or Data ONTAP 8.x operating in 7-Mode. It collects data through a network connection to each controller. The rules in this profile are a comprehensive set of installation checks, best practice checks, and At-Risk-Systems (ARS) checks.
Include Extended Health Checks	Runs additional checks on the system.
Collect Data	Collects data from a node or both nodes of an HA pair.
Save this Query	Saves the login credentials as a query for later use.
Clear All	Clears all the information entered in the fields.

Collecting data by using the Serial Port tab

You can use the **Serial Port** tab if you do not have access to the customer's network. Direct access to the controller firmware is gained through the serial port.

Limitations of using the Serial data collection method

The limitations of using the 7-Mode serial data collection method are as follows:

- It takes several minutes to run commands over a serial port at 9600 Bd (baud).
- Most of the checks are not run because of performance and throughput reasons over a slow serial link.

Config Advisor will run only the following commands:

- version
- sysconfig -a
- storage show disk -a
- storage show disk -p
- ifconfig -a
- rdfile /etc/rc
- rdfile /etc/hosts
- rdfile /etc/exports

- exportfs
- license
- options
- cf status
- cf partner
- hostname
- fcp show cfmode
- storage show acp -a
- environment status (extended health check command)

Note: If you want to run all the available disk shelf checks, you should use the Network or the AutoSupport tabs.

Steps

1. Choose a COM port from the drop-down list for NetApp controller.
2. Choose a COM port from the drop-down list for HA partner.
3. Alternatively, select the login credentials from the Query Groups pane. For more information, see *Saving credentials*.
4. Enter the login details – Username and Password.
5. Click **Test Login** to test the connection.
6. Click **Collect Data** to start data collection.

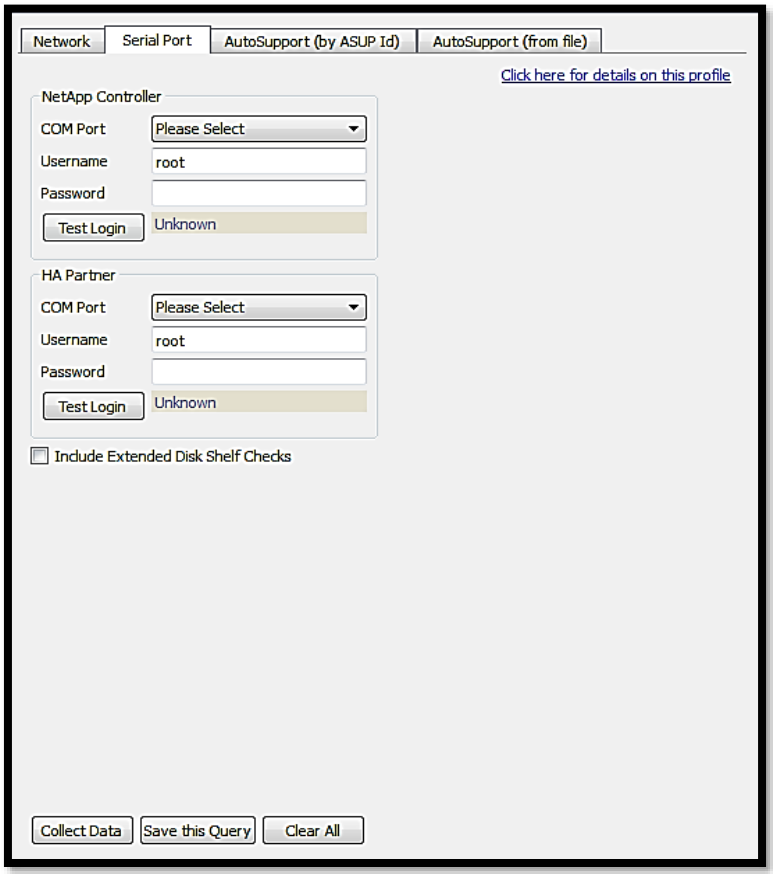
   The **Results File** dialog box is displayed.
7. Enter a name for the result file or accept the default.
8. Select the Include Extended Disk Shelf Checks check box, if you want to run additional checks on the system.

   Note: If you select the Include Extended Disk Shelf Checks check box, the environment status command is run. This allows Config Advisor to accurately validate the shelf-to-shelf cabling. However, this command might take a long time to run depending on the number of disks connected to the controller.
9. Click OK.

10. After the data collection and analysis are complete, the result file is displayed in the Recent Results pane. For more information about the Recent Results pane, see Recent Results pane.
11. Click Save this Query to save the login credentials as a query. For more information about saving credentials, see *Saving credentials*.

Note: Data collection takes place even if the status check on a node fails.

The 7-Mode Serial Port tab is as shown:



Fields in 7-Mode Serial Port tab

The fields in the 7-Mode **Serial Port** tab are described as follows:

GUI field/GUI button	Description
COM Port	COM port to which you have connected the storage controller
Username	User name to access the controller
Password	Password to access the controller
Test Login	Displays the serial port connection status The statuses are as follows: • **Insufficient Data**: Displayed if the device name and credentials are not entered. • **Click on 'Test Login' to verify**: Displayed if all the necessary details are entered. • **Valid <login type> Login**: Displayed if the connection is valid. • **Connection Failed**: Displayed if the connection to the device fails. • **Invalid Credentials**: Displayed if the invalid credentials for the device are entered. **Note**: The connection to a device fails if the host name or IP details entered are wrong, or if the device type (the device type can only be 7-Mode storage controller) is wrong, or if the device is powered off. Additional information is displayed in the **Config Advisor Logs** pane.
Include Extended Disk Shelf Checks	Runs the environment status command.
Collect Data	Collects data from the COM port.
Save this Query	Saves the login credentials as a query for later use.
Clear All	Clears all the information entered in the fields.

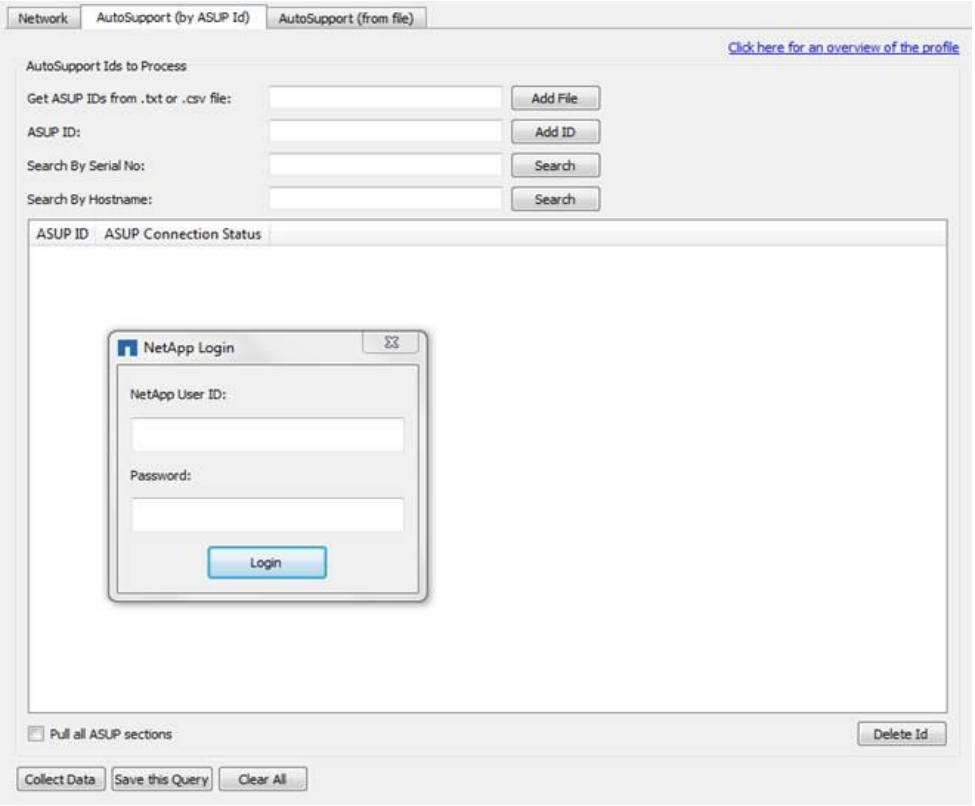
Collecting data by using the AutoSupport (by ASUP Id) tab

Config Advisor can perform analysis using the NetApp AutoSupport Data warehouse as data input source. You can submit a list of AutoSupport Ids in a file or search for them interactively.

Note: This method is available only to NetApp personnel who have access to the intranet and the AutoSupport Data warehouse. It is not available to partners and NetApp customers.

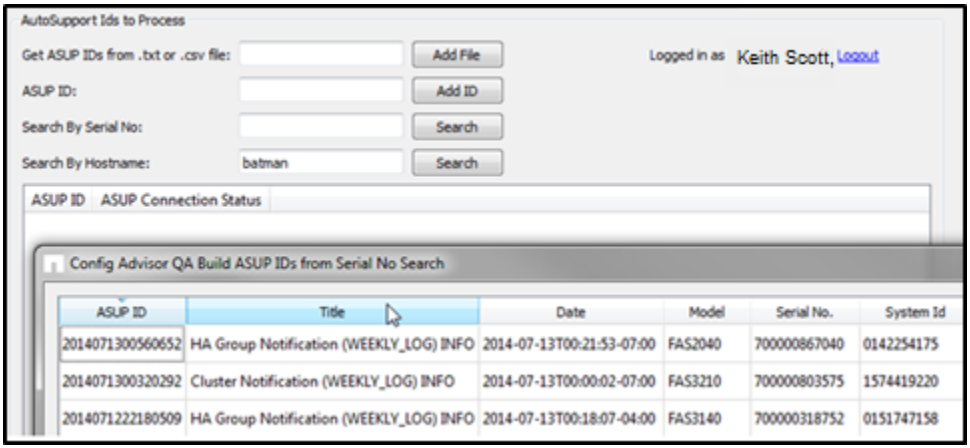
Config Advisor allows loading and collecting data from ASUPs only with NetApp SSO entitlements. Before Config Advisor allows for an ASUP query, SSO login dialog box is displayed.

SSO login dialog box is as shown:



On successful login, the ASUP query proceeds and the user name is presented in the interface with a **Logout** link.

The **Logout** link is as shown:



Note: Once a query or data collection is initiated with entitlements it will proceed even when the Logout link is clicked. Subsequent queries or data collection will again request for entitlements.

Steps

1. Click **Add File** to select a file (.csv, .txt) containing multiple AutoSupport IDs.

   Multiple AutoSupport IDs are displayed in the **ASUP ID** column along with their connection statuses.

2. Alternatively, you can add an AutoSupport ID using one of the following methods:

   a) Enter the ID in the **ASUP ID** field and click **Add ID**.

   Note: The older ASUP ID format (for example, AE2010061286069) is not supported in Config Advisor 3.0 and later. You must enter the ASUP ID in the new format, for example, 2010061918120050.

   b) Enter serial number of the controller in the **Search By Serial No** field, and click **Search**.

   c) The Config Advisor ASUP IDs from **Serial No Search** dialog box is displayed. Select the ASUP IDs, and click **Add Selected ASUPs**.

The ASUP IDs are displayed in the **ASUP ID** column along with their connection statuses.

3. Enter host name of the controller in the **Search By Hostname** field, and click **Search**.

   The Config Advisor ASUP IDs from Hostname Search dialog box is displayed.

4. Select the appropriate ASUP IDs, and click **Add Selected ASUPs**.

   The selected ASUP IDs are displayed in the **ASUP ID** column along with their connection statuses.

   Note: You can enter multiple comma-separated host names or system serial numbers, with no space.

5. To delete an ASUP ID from the displayed list, select the ID and click **Delete ID**.
6. You can select the **Pull all ASUP sections** check box to collect from all of the sections of the AutoSupport.
7. Click **Collect Data** to start the data collection.
8. The **Results File** dialog box is displayed.
9. Enter a name for the result file or accept the default, and click **Ok**. After the data collection and analysis are complete, the result file is displayed in the **Recent Results** pane.
10. For more information about the **Recent Results** pane, see *Recent Results pane*.
11. Click **Save this Query** to save the AutoSupport IDs as a query. For more information about saving credentials, see *Saving credentials*.

    Note: This tab is visible only to users who have access to NetApp intranet and the AutoSupport Data warehouse.

Fields in AutoSupport (by ASUP Id) tab

The fields in the **Fields in AutoSupport (by ASUP Id)** tab are as follows:

GUI field/GUI button	Description
Get ASUP IDs from .txt or .csv file	.csv or .txt file containing multiple AutoSupport IDs
Add File	Adds the selected .csv or .txt file containing multiple AutoSupport IDs
ASUP ID	AutoSupport ID of a controller

GUI field/GUI button	Description
Add ID	Adds the entered AutoSupport ID • The AutoSupport ID is verified and the status is displayed • You cannot make duplicate entries of the same AutoSupport ID
Search By Serial No.	Allows you to search for ASUP IDs by serial numbers of controllers
Search By Hostname	Allows you to search for ASUP IDs by host names of controllers
ASUP Connection Status	Displays the status of the AutoSupport ID
Delete Id	Deletes the selected AutoSupport ID from the list
Collect Data	Collects data from a storage controller
Save this Query	Saves the AutoSupport IDs from the table as a query for later use
Clear All	Clears all the information entered in the fields

Collecting data by using the AutoSupport (from file) tab

Config Advisor can perform an analysis using the AutoSupport file from a NetApp storage system.

Steps

1. Click **Add File** and choose an AutoSupport file.

   AutoSupport files in the .tgz, .7z, and .txt formats are supported.

   Alternatively, you can select a query from the **Query Groups** pane. For more information, see *Saving credentials*.

2. You can select the **Pull all ASUP sections** check box to collect from all of the sections of the AutoSupport.

3. Click **Collect Data** to start the data collection.

   The **Results File** dialog box is displayed.

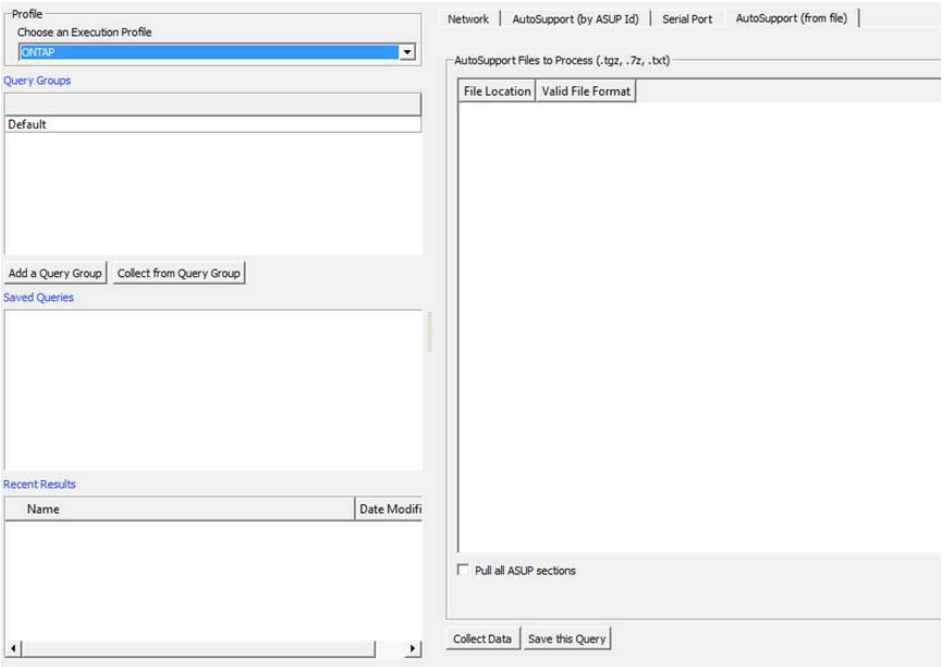
4. Enter a name for the result file or accept the default, and click **Ok**.

   When the data collection and analysis are complete, the result file is displayed in the **Recent Results** pane. For more information about this pane, see *Recent Results pane*.

5. Click **Save this Query** to save the file as a query.

   For more information about saving credentials, see *Saving credentials*.

The **AutoSupport (from file)** tab is as shown:



Fields in 7-Mode AutoSupport (from file) tab

The fields in the 7-Mode AutoSupport (from file) tab are as follows:

GUI field/GUI button	Description
File Location	Displays the path from where the file was loaded
Valid File Format	Displays Verified if Config Advisor is able to validate or read the file format
Add File	Adds a file from the selected location • When you add a file, it is verified before it is added to the list • If you add an invalid file, an error message is displayed and the file is not added to the list
Remove File	Removes the AutoSupport file from the list
Collect Data	Collects data from AutoSupport files

GUI field/GUI button	Description
Save this Query	Saves the file path as a query for later use

Collecting data to run Copy-Free Transition prechecks

Copy-Free Transition enables you to disconnect all disk shelves from a 7-Mode HA pair and connect them to an HA pair in the target cluster. You can convert data in the disk shelves to ONTAP format and transition the 7-Mode configurations by using the 7-Mode Transition Tool.

The unit of a Copy-Free Transition is an HA pair. You must move all the disk shelves from the 7-Mode HA pair to the target cluster nodes.

Before starting transition, you can validate the cabling of the source controllers (7-Mode HA pair) using Config Advisor. To do this, use the "**7-Mode Install Check**s" option from the "*Data ONTAP 7 and 8 (7-Mode)*" execution profile.

After connecting the disk shelves to ONTAP, you can use Config Advisor to run prechecks for Copy-Free Transition. To run the prechecks, you must provide the IP address of the cluster-management LIF.

Note: For more information about transition checks, see *Appendix A: Configuration validations & health checks*.

Collecting data by using the Copy-Free Transition tab

Steps

1. Select **Transition** from the execution profile drop-down menu under the **Profile** section.

   Enter the IP address or host name of the cluster-management LIF and the login credentials of the cluster.

   Alternatively, you can select the login credentials from the **Query Groups** pane. For more information, see *Saving credentials*.

2. Click **Collect Data** to start the data collection.

   The **Results File** dialog box is displayed.

3. Enter a name for the result file or accept the default name, and click **OK**.

   The data collection starts and a progress bar is displayed. The command exceptions are displayed in the **Config Advisor Logs** pane.

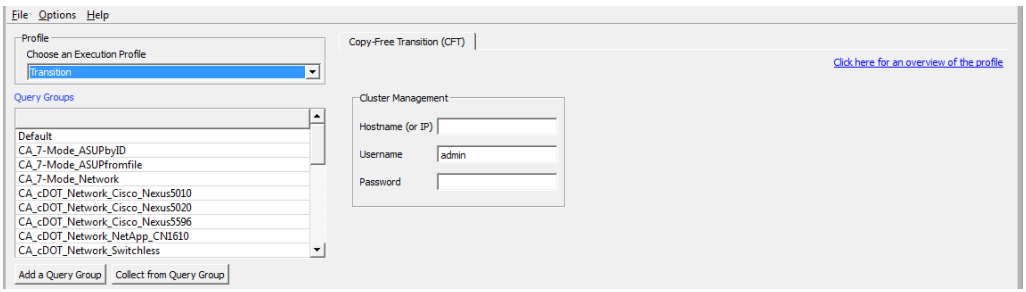
   After the data collection and analysis is complete, the result file is displayed in the **Recent Results** pane. For more information about this pane, see *Recent Results pane*.

   Note: Data collection takes place and a Config Advisor result file is displayed even if the status check on a node fails.

4. Click **Save this Query** to save the credentials as a query.

   For more information about saving credentials, see *Saving credentials*.

   The **Transition** tab is as shown:



Fields in the Transition tab

The fields in the tab are as follows:

GUI field/GUI button	Description
Hostname (or IP)	Host name or IP address of the cluster-management LIF
Username	User name to access the cluster
Password	Password to access the cluster
Collect Data	Collects data from systems running Data ONTAP 8.x
Save this Query	Saves the login credentials as a query for later use
Clear All	Clears all the information entered in the fields

Note: The Config Advisor Log pane that is at the bottom of the main Config Advisor window has two tabs, Info and Errors. These tabs display details of data collection and connection testing processes. The pane also shows log details for Status, Invalid Credentials, and Connection Failure (along with the reasons for failure).

Collecting data by using the batch data-collection mode

In the batch data-collection mode, you can collect data from multiple queries saved from different profiles.

On clicking the **Collect from Query Group** button, a folder is created in the **Recent Result** tab with the same name as that of the query group. Data collection proceeds from each query within the query group as though it was loaded into the UI and the **Collect Data** button is clicked. Individual result files are named after the query name with date stamp and placed in that particular folder.

Note: The Results Viewer window does not automatically open when the data collection completes for the individual queries when Config Advisor ASUP is disabled.

Note: Queries from 7-Mode network and E-Series host are grouped into a single result file. PDF, MS Word, and MS Excel reports are also grouped for these profiles when using **Collect from Query Group**.

Steps

1. Click **Add a Query Group**.

   The **New Query Group** dialog box is displayed.

2. Enter a query group name, and click **OK**.

   The name is added in the **Query Groups** pane.

3. Enter the credentials in **Network** tab and click **Save this Query** in each tab.

   The **Save this Query** dialog box is displayed.

4. Enter a query name or accept the default name, and select the query group from the drop-down list.

   For more information about saving credentials, see *Saving credentials*.

5. Click **Ok**.

6. Double-click the required query group displayed in the **Name of Query Group** pane to list the credentials within that query group.

   The credentials saved in that query group are listed in the **Query Groups** pane.

   Note: You can double-click individual credentials files to load the credentials in to the tabs they were saved from.

7. To collect data from all the queries saved within the query group, click the **Collect from Query Group** button.

   The data collection for a query group starts and a progress bar is displayed.

Collecting data from plug-ins

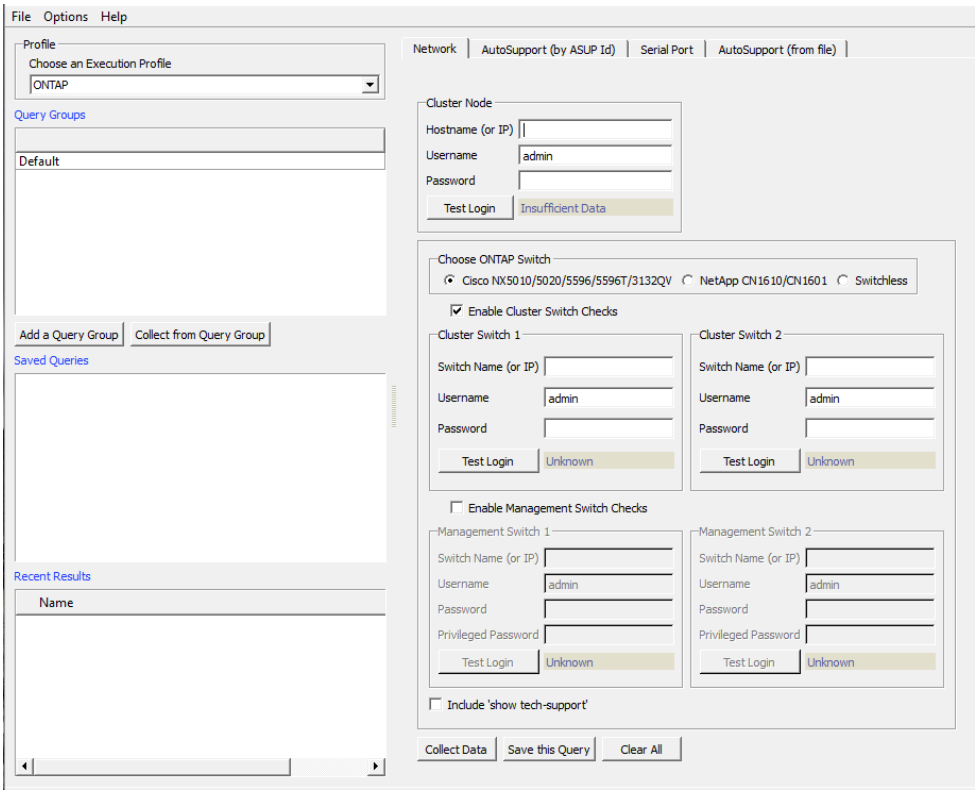
Plug-in create profiles just like the existing profiles within Config Advisor. You can also save and load credentials for plug-ins same as the existing profiles within Config Advisor. For details of individual plug-ins refer to the documentation that comes included with the plug-in.

Collecting data from show tech-support

When you select the **Include 'show tech-support'** check box from a ONTAP profile, the command 'show tech-support' is included for the cluster interconnect and management switches.

Because this command output is large, it is collected separately and stored in the ~ ConfigAdvisorDataDirectory_Base/ConfigAdvisorData/show_techsupport_outputs folder. A folder is created with the same name as the results file. For each switch, a separate text file is created with the show tech-support command output. Using the Command Viewer, you can see the command output; however, if you modify or change the file or folder name, you will lose the mapping for the Command Viewer to work.

This feature is also available in FlexPod profiles where the data is collected only from Cluster Interconnects and not from Fabric Switches.



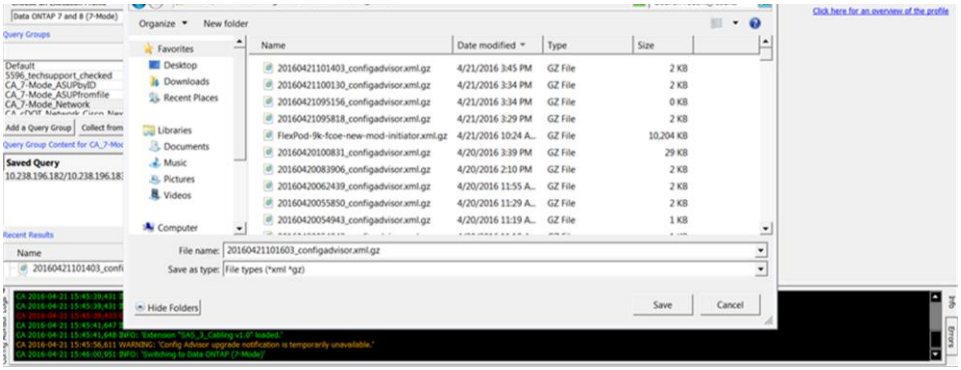
Working with results

You can find information about where to find the result files, how to view the 7-Mode, ONTAP, and Copy-Free Transition results, and the analysis of the results. You can also find the description of the fields in the Config Advisor results window, and information about how to download the results in PDF, Microsoft Word, and Microsoft Excel formats.

Organization of Config Advisor Result file

On clicking **Collect Data** from any profile, you will be presented with a **File Browser** dialog box, which allows multiple folders to be created to organize the results file after data collection. You will also have the ability to create folders and save result files outside of the default data directory: ~ConfigAdvisorDataDirectory_Base /ConfigAdvisorData/recent_results.

However, the result files created outside of the default directory will not be listed under **Recent Results** pane on the interface.

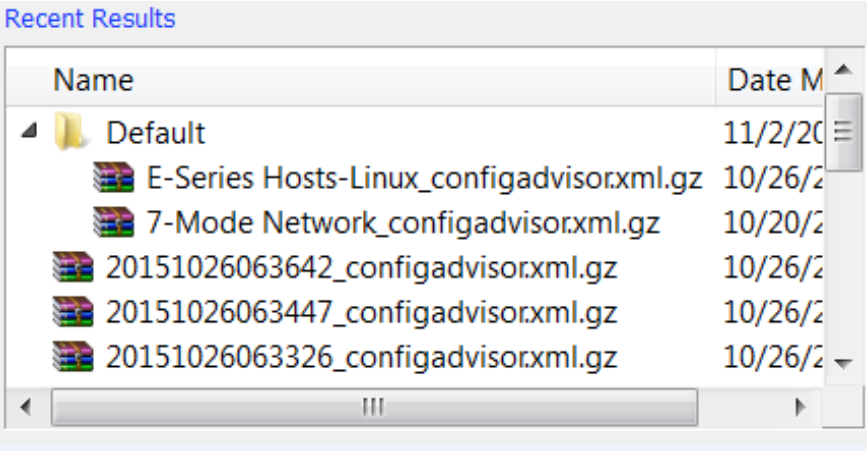


Recent Results pane

The collected and analyzed data is saved as a Config Advisor file in the xml.gz format. You can access these files from the **Recent Results** pane in Config Advisor.

You can organize your result files inside folders manually.

The **Recent Results** pane is as shown:



The location of the result files is as follows:

Directory path
ConfigAdvisorDataDirectory_Base/ConfigAdvisorData/recent_results

The fields in the **Recent Results** pane are as follows:

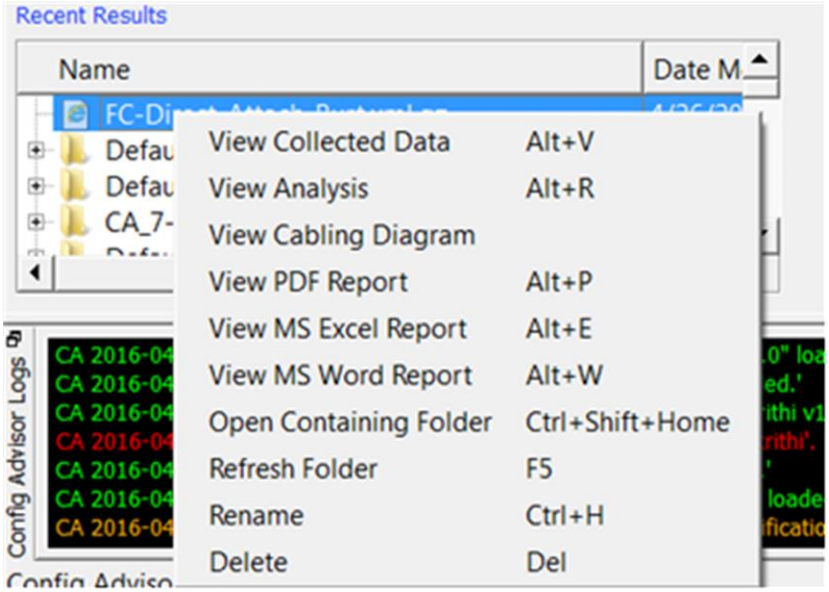
Field	Description
File Name	Displays the name of the Config Advisor file.
Date	Displays the date on which the file was created.

The files in the **Recent Results** pane are sorted in the descending order of their creation dates; starting from the latest file. You can right-click a file name for options. For more information, see Viewing results.

Viewing results

You can view the results by right-clicking a result file name displayed in the **Recent Results** pane.

The right-click options of a result file in the **Recent Results** pane is as shown:



If you right-click a result file in the **Recent Results** pane, you see multiple options as follows:

Input field	Description
View Collected Data	Displays the **Config Advisor Viewer** window with the output of the commands that were executed on the storage controllers and switches. For more information, see *What Config Advisor Viewer does*.
View Analysis	Displays the **Results** window with the details of the results.
View Cabling Diagram	Displays the SAS cabling diagram for SAS-2 shelves. For more information, see *Generating a Cabling Diagram*.
View PDF Report	Generates a PDF report for the results. For more information, see *Generating a PDF report*.
View MS Excel Report	Generates a Microsoft Excel report for the results. For more information, see *Generating an MS Excel report*.
View MS Word Report	Generates a Microsoft Word report for the results. For more information, see *Generating an MS Word report*.
Open Containing Folder	Opens the folder that stores the Config Advisor data files.

Input field	Description
Refresh Folder	Refreshes the folder for new or modified Config Advisor files.
Rename	Renames the Config Advisor file.
Delete	Deletes the Config Advisor file.

What Config Advisor Viewer does

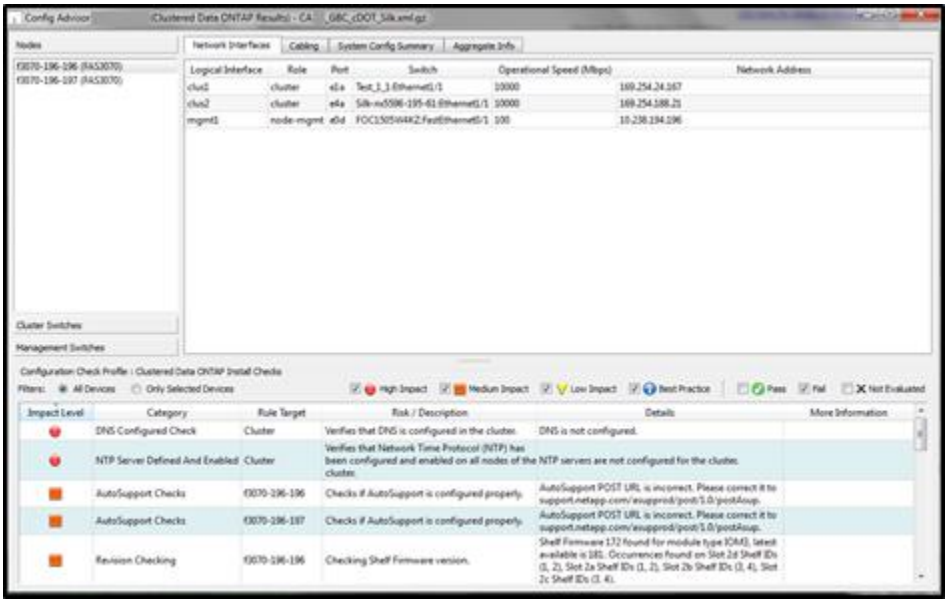
The **Config Advisor Viewer** window displays the commands that were executed on the target(s) and displays the command and the collected data. The **Config Advisor Viewer** window is displayed when you right-click a file in **Recent Results** and select **View Collected Data**.

Viewing ONTAP results in Config Advisor

Steps

1. In the **Recent Results** pane, right-click an ONTAP results file.
2. Select **View Analysis**. The **Config Advisor (ONTAP Results)** window is displayed.

   The **Config Advisor (ONTAP Results)** window is as shown:



The **Results View - Network Interface** table is as shown:

Network Interfaces | Cabling | System Config Summary | Aggregate Info

Storage Virtual Machine	Logical Interface	IPspace	Port	Switch	Operational Speed (Mbps)	Network Address
Cluster	f2240-197-119_clus1	Cluster	e1b	Silk-nx5596-195-61:Ethernet1/3	10000	169.254.91.221
Cluster	f2240-197-119_clus2	Cluster	e1b	Silk-nx5596-195-61:Ethernet1/3	10000	169.254.118.225
Cluster	f2240-197-120_clus1	Cluster	e1a	Test_1_1:Ethernet1/4	10000	169.254.168.88
Cluster	f2240-197-120_clus2	Cluster	e1b	Silk-nx5596-195-61:Ethernet1/4	10000	169.254.122.64
clus_f2240-197-119-120	cluster_mgmt	Default	e0a		1000	10.238.197.119
clus_f2240-197-119-120	f2240-197-119_mgmt1	Default	e0M	FOC1505W4KZ:FastEthernet0/3	100	10.238.195.68
clus_f2240-197-119-120	f2240-197-120_mgmt1	Default	e0M	FOC1505V2D3:FastEthernet0/3	100	10.238.195.69

The **Config Advisor (ONTAP Results)** window is divided into the following panes:

- **Nodes, Cluster Switches, and Management Switches**: You can see the node, cluster switch, and management switch details.
- **Configuration Validations & Health Checks:** You can use filters to see the rules that were run on the collected data and results. For more information, see Appendix A: Configuration validations & health checks.

Nodes pane

The **Nodes** pane displays details of the nodes within a cluster. The details of the nodes are displayed in the **Network Interfaces**, **Cabling**, **System Config Summary**, and **Aggregate Info** tabs.

Network Interfaces tab

You can view the details of a node by selecting a controller from the **Nodes** pane. The **Network Interfaces** tab displays information about all the network interfaces of the cluster.

The fields in the **Network Interfaces** tab are as follows:

Fields	Description
Storage Virtual Machine	Displays the name of the Storage Virtual Machine.
Logical Interface	Displays the name of the logical interface created on the cluster.
IP Space	Displays the IP space.
Role	Displays the role of the logical interface (node-management, cluster, or data) created on the cluster.

Fields	Description
Port	Displays the physical interface of the node on which the logical interface is configured.
Switch	Displays the host name and interface name of the switch (cluster switch or management switch) to which the logical interface of the cluster is connected.
Operational Speed (Mbps)	Displays the operational speed of the logical interfaces of the cluster.
Network Address	Displays the network IP address configured on the logical interfaces of the cluster.

Note: On NetApp CN1601, port 13 is listed only when it is active. The details of the port are not displayed because it is connected to a service port of the cluster switch for 10G connections.

Cabling tab

The **Cabling** tab displays the shelf and disk information of the controllers. You can also view the cabling diagram of the node and partner node (if HA is enabled and configured within the cluster nodes). For more information on the fields in the **Cabling** tab, see *Cabling tab.*

System Config Summary tab

You can view the hardware overview, module details, shelf details, and disk overview by clicking the **System Config Summary** tab. For more information on the fields in this tab, see *System Config Summary tab*.

Aggregate Info tab

You can view the aggregate information by clicking the **Aggregate Info** tab. For more information on the fields in this tab, see *Aggregate Info tab*.

Cluster Switches pane

You can view the details of a switch by selecting a switch from the **Cluster Switches** pane.

The fields in the **Cluster Switches** pane are as follows:

Fields	Description
Port	Displays the interfaces on the cluster switches that are physically connected to the cluster nodes or the management switches, or an Inter-Switch Link (ISL) to the other cluster switch.

Fields	Description
Connected Type	Displays the type of the device to which the cluster switch interface is connected (Controller or ISL).
Connected Host (Port)	Displays the host name and interface name of the cluster node or switch (cluster switch or management switch) to which the interface of the cluster switch is connected.
Speed	Displays the speed of the interfaces of the cluster switch.
Network Address	Displays the network IP address configured on the interfaces of the cluster switch.
	Displays that the power supply or fan has errors.
	Displays that the power supply or fan works without errors.

Management Switches pane

You can to view the details of a selected switch from the **Management Switches** pane.

The fields in the **Management Switches** pane are as follows:

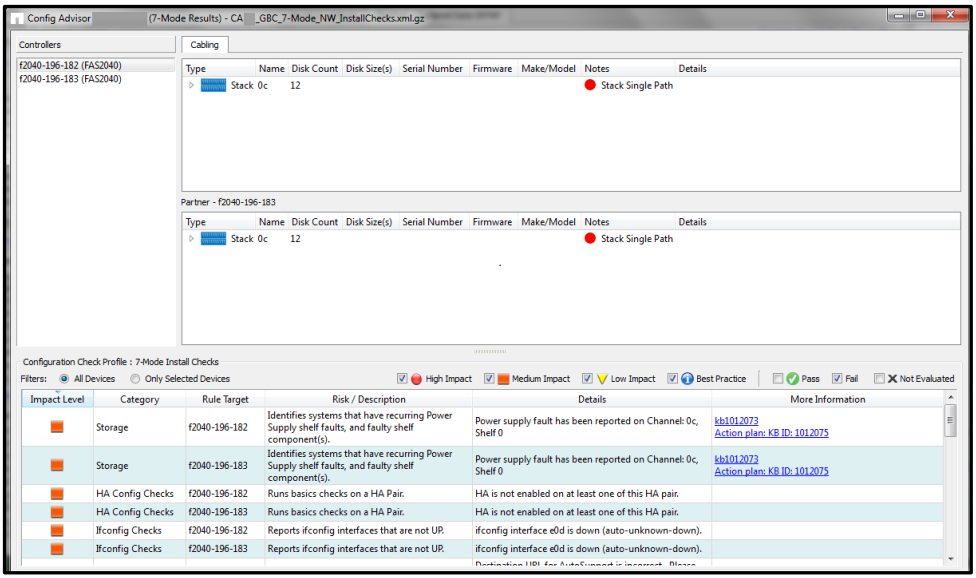
Fields	Description
Port	Displays the interfaces on the management switches that are physically connected to the cluster nodes or the cluster switches, or an Inter-switch Link (ISL) of another management switch.
Connected Type	Displays the type of the device to which the management switch interface is connected (Controller or ISL).
Connected Host (Port)	Displays the host name and interface name of the cluster node or switch (management switch or cluster switch) to which the interface of the management switch is connected.
Speed	Displays the speed of the interfaces of the management switch.
Network Address	Displays the network IP address configured on the interfaces of the management switch.
	Displays that the power supply or fan has errors.
	Displays that the power supply or fan works without errors.

Viewing 7-Mode results in Config Advisor

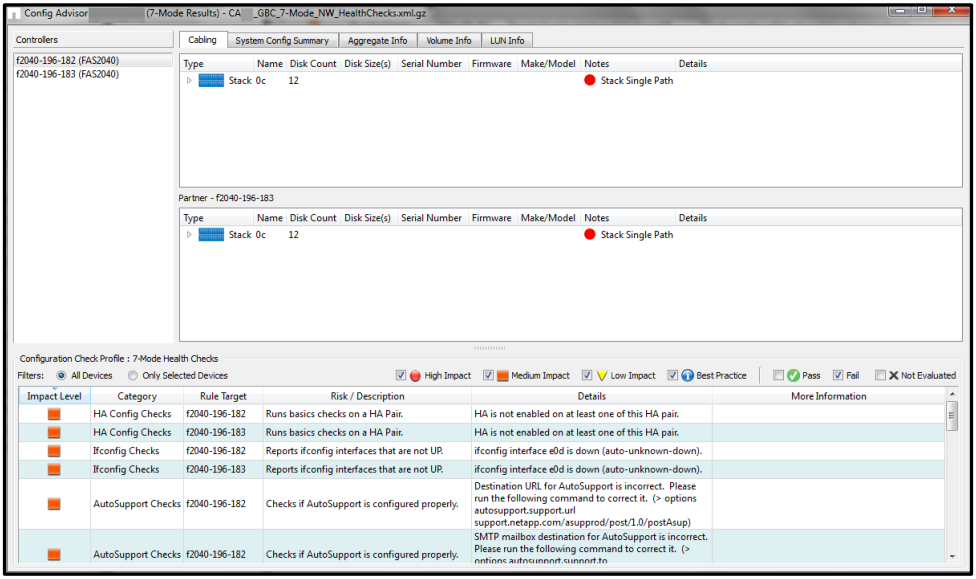
Steps

1. In the **Recent Results** pane, right-click the required file.
2. Select View Analysis. The Config Advisor (7-Mode Results) window is displayed.

The **Config Advisor (7-Mode Results)** window is as shown:



The **Config Advisor (7-Mode Results)** window (when the **Include Extended Health check** box is selected) is as shown:



The **Config Advisor (7-Mode Results)** window is divided into the following parts:

- The **Controllers** pane lists all the nodes in the Config Advisor file.
- The **Cabling** tab displays the details for the selected node. (The **System Config Summary**, **Aggregate Info**, **Volume Info**, and **LUN Info** tabs are displayed based on the profile selected).
- The result analysis pane that has filters that display the rules that were run on the collected data and the results.

Controllers pane

The **Controllers** pane displays the controllers from which the data is collected. The details about the controllers or the HA pair are displayed in the **Cabling**, **System Config Summary**, **Aggregate Info**, **Volume Info**, and **LUN Info** tabs based on the profiles selected.

Cabling tab

You can view the details of a controller from the **Controllers** pane.

- The controller stack diagram is displayed in the **Cabling** tab.
- If you are viewing the details of an HA pair, the partner stack is displayed below the controller stack diagram.

Note: If the partner controller details of an HA pair are not available in the Config Advisor file, they are not displayed.

You can view shelf and disk information by clicking the ▷ icon in the **Cabling** tab and expanding the stack tree.

The fields in the **Cabling** tab are as follows:

Field	Description
Type	Displays the hierarchy (stack, shelf, or disk).
Name	Displays the name of the stack, shelf, and disk.
Disk Count	Displays the count for a stack and shelf.
Disk Size(s)	Displays the size of the disk.
Serial Number	Displays the serial number of the disk.

Field	Description
Firmware	Displays the firmware on the disk.
Make/Model	Displays the model information for the shelf and disk.
Notes	Displays the path system used in a stack, shelf, and disk, with a green, orange, or red flag.
Details	Displays information about the shelf or disk that has a red or orange indicator in **Notes**.

System Config Summary tab

You can view the hardware overview, module details, shelf details, and disk overview by clicking the **System Config Summary** tab.

The fields in the **System Config Summary** tab are as follows:

Field	Description
Hardware Overview	**Host name**: Displays the host name of the controller. **Serial Number:** Displays the serial number of the controller. **Model**: Displays the controller model. **ONTAP version**: Displays the current version of ONTAP that is installed on the controller. **Total Raw Capacity (GB)**: Displays the total raw capacity of all the disks owned by the node. **Total Usable Capacity (GB)**: Displays the total usable capacity for aggregates on the node. **Total Used Capacity (GB)**: Displays the total used capacity for aggregates on the node. **Installed Software**: Displays all the licensed features on the node.
Module Details	**Module Type**: Displays the shelf input/output module. **# of Shelf Modules**: Displays the count of each shelf input/output module.
Shelf Details	**Shelf Type**: Displays the shelf model attached to the controller. **# of Shelves**: Displays the count of each shelf model attached to the controller.

Field	Description
Disk Overview	**Disk Model**: Displays the disk model. **Disk Type**: Displays the type of disk (FC, SATA, SAS, and so on). **Disk Mktg Size (GB)**: Displays the Disk Marketing size. **# of Owned Disk:** Displays the number of owned disks. **# of Data Drives**: Displays the total number of data drives forming the aggregates on the node. **# of Parity Drives**: Displays total number of parity drives forming the aggregates on the node. **# of Spare Disks**: Displays total number of spare drives owned by the node. # **of ADP Disks**: Displays the total number of drives that have advanced disk partitioning enabled. **# of Unowned Disks**: Displays the unowned disks for the HA pair.

Aggregate Info tab

You can view the aggregate information by clicking the **Aggregate Info** tab.

The fields in the **Aggregate Info** tab are as follows:

Field	Description
Aggregate Name	Displays the name of the aggregate.
RAID type	Displays the RAID type of the aggregate (RAID 4, RAID DP, and so on).
Disk Count	Displays the count of the disks that form the aggregate.
Total (GB)	Displays the total space of the aggregate.
Used (GB)	Displays the used space of the aggregate.
Available (GB)	Displays the available space of the aggregate.
% Used	Displays the percentage of used space of the aggregate.

Volume Info tab

You can view the volume information by clicking the **Volume Info** tab.

The fields in the **Volume Info** tab are as follows:

Field	Description
Volume Name	Displays the volume name of either FlexVol or traditional volumes.
Containing Aggregate	Displays the containing aggregate for the volume (if it is a FlexVol).
Vol type	Displays the type of the volume.
Vol State	Displays the state of the volume (online and so on).
Total (GB)	Displays the total space of the volume.
Used (GB)	Displays the used space of the volume.
Free (GB)	Displays the available space of the volume.
Used %	Displays the percentage of used space of the volume.

LUN Info tab

You can view the LUN information by clicking the **LUN Info** tab.

The fields in the **LUN Info** tab are as follows:

Field	Description
LUN Path	Displays the LUN name along with the full path.
LUN Type	Displays the LUN multiprotocol type.
LUN Size	Displays the size of the LUN.
Mapped igroup Name	Displays the initiator group to which the LUN is mapped.
igroup Type	Displays the type of the initiator group mapped to the LUN.
Space Reservation	Displays whether space reservation is enabled or disabled on the LUN.

Configuration validations and health checks pane

Configuration validations and health checks are the checks that are run on the collected data when you open the **7-Mode Results, ONTAP Results, plug-in Results** window in Config Advisor.

In the Results view, the profile used for data collection is displayed above the rules table.

The fields in the **Configuration Validations & Health Checks** pane are as follows:

Field	Description
Configuration Check Profile	Displays the profile selected
Impact Level	Displays the level of risk
Category	Displays the category of the rule
Rule Target	Displays the controller or switch on which the rule is run
Risk / Description	Displays the description of the check that is run
Details	Displays the details of the risk
More Information	Displays additional information about the status of the risk

The **Configuration Validations & Health Checks** pane contains filters, which can be used to customize the display of rules. The filters are as follows:

Filters	Description
All Devices	Displays the configuration checks for all the controllers and switches
Only Selected Devices	Displays the configuration checks for only the selected controllers or switches
High Impact	Critical impact potential, and should be addressed immediately
Medium Impact	Disruptive impact potential, and should be addressed as soon as possible
Low Impact	Low impact potential, and should be addressed during the next maintenance window
Best Practice	Best practice recommendations
Pass	Displays the rules that passed the configuration checks
Not evaluated	Displays rules that could not be evaluated

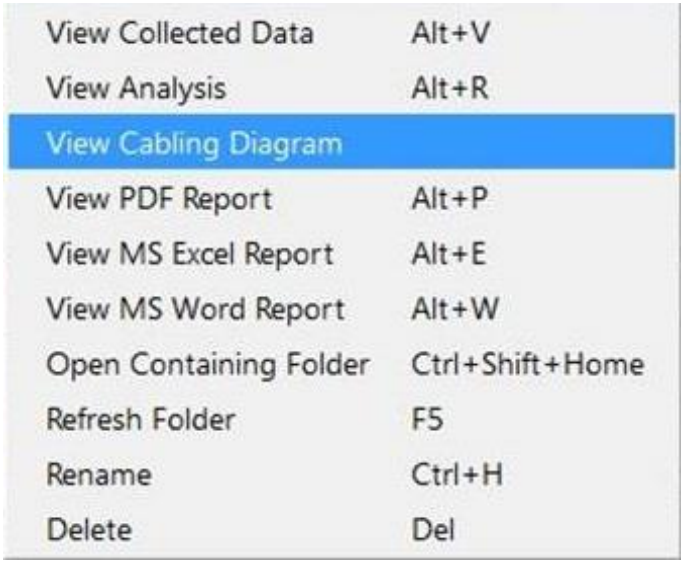
See *Appendix A: Configuration validations & health checks* for a detailed description of all the configuration validations and health checks that are run.

Generating a Cabling Diagram

This is a feature to visualize the SAS cabling. Currently, Config Advisor supports 7-Mode, ONTAP, and FlexPod profiles. Only SAS-2 shelves are supported.

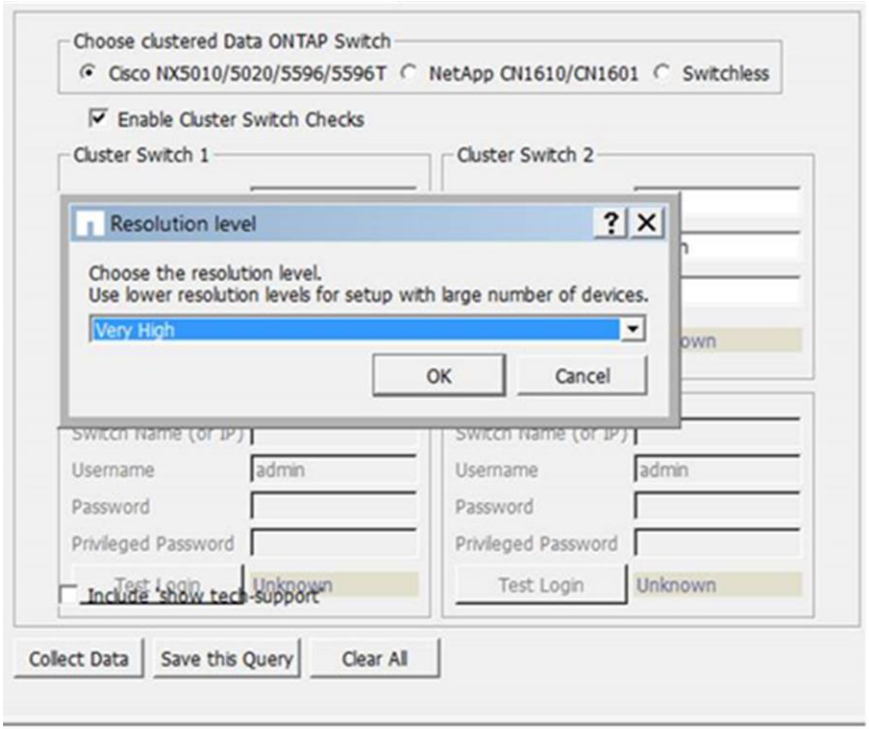
Steps

1. To view the cabling diagram, right-click the **Results file**, select **View Cabling Diagram**.



Note: You can specify the image resolution which should be reduced when memory error is displayed.

The resolution level of the output image can be set by selecting one of the options from the drop-down list.



The cabling diagrams are created and saved under ConfigAdvisorData/cabling_images.

Generating a PDF report

You can generate a PDF report from any of the Config Advisor collected result files. The PDF report is designed to provide a quick summary of the system storage configuration and validation check results. It contains fewer details than the MS Excel and MS Word reports.

A single consolidated PDF report is generated that lists storage configuration and rule results for a diverse set of collected files in a folder.

Step

1. Right-click the directory under the **Recent Results** pane, and select **View PDF Report**.

   A PDF file is displayed with the results of the selected file.

Note: The reports are saved in the following location: ~ ConfigAdvisorDataDirectory_Base/ConfigAdvisorData/pdf_files.

Generating an MS Excel report

You can generate an MS Excel report containing the results of the selected file.

Step

1. In the **Recent Results** pane, right-click a Config Advisor file, and select **View MS Excel Report**.

   An Excel file is displayed with the results of the selected profile.

Generating an MS Word report

You can generate an MS Word report containing the results of the selected file.

Step

1. In the **Recent Results** pane, right-click a Config Advisor file, and select **View MS Word Report**.

   A Word file is displayed with the results with the selected profile.

   Note: The reports are saved in the following location: ~/ ConfigAdvisorDataDirectory_Base/ConfigAdvisorData/doc_files.

   The report is saved automatically with the same name as the result file. However, when you open the document, you are asked to save the document again. You can click **NO** to ignore this.

Merging reports from multiple result files

The **Recent Results** pane supports the display of all the result files within the ConfigAdvisorDataDirectory_Base/ConfigAdvisorData/recent_results folder. This includes navigation of sub directories within that folder. These sub directories are created either from

Collect from Query Group or when collecting data from any one profile. You can use Windows Explorer to also create folders and organize your result files. You can navigate those files and folders from the **Results** pane.

The folders listed in the **Recent Results** pane have the following menu items when you right-click.

Input field	Description
Open Containing Folder	Opens the folder that stores the Config Advisor data files.
Refresh Folder	Refreshes the folder for new or modified Config Advisor files.
Rename	Renames the Config Advisor file.
Delete	Deletes the Config Advisor file.
View Merged PDF Report	Generates a merged PDF report for all the result files within the folder.
View Merged Excel Report	Generates a merged Excel report for all the result files within the folder.
View Merged Word Report	Generates a merged Word report for all the result files within the folder.

By placing the result files of different profiles or multiple clusters into a folder, you can use the folder options to generate a consolidated report.

Working with credentials

You can save credentials such as, device host name or IP address, login credentials, serial port information, AutoSupport ID details, and AutoSupport file details used for data collection. The credentials can be saved as a query. One or more queries can be grouped as a query group. Query groups are saved as files with a .crypt extension.

The location of the files is as follows:

Directory path
C:/Users/<windows_login>/ConfigAdvisorData

Note: To save a query, the credentials need not be validated or complete.

Password encryption

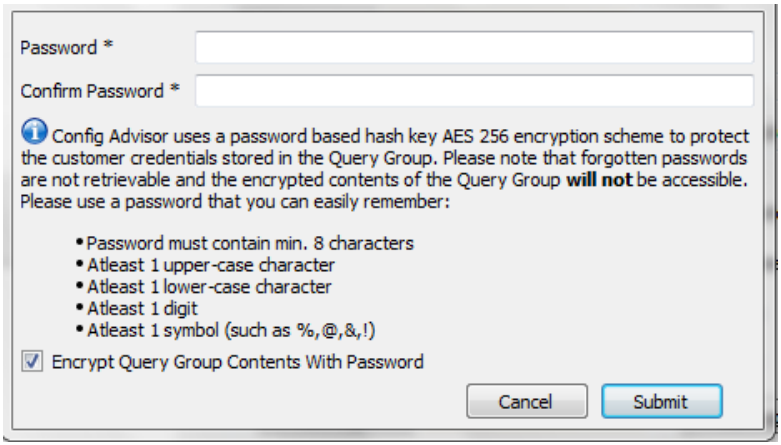
To prevent unauthorized access to device credentials, Config Advisor has introduced password based cryptography.

Starting with Config Advisor, all previously created query groups are encrypted with a new password based key and AES 256 encryption scheme.

On the first attempt to creating a query, loading a query, or saving credentials the user is prompted with the following dialog box to set a password or use the default password.

You must consider the following when setting a password:

- Password cannot be retrieved if you forget the password. Config Advisor will not be able to load the queries because the encrypted files cannot be decrypted without the password used for encryption.
- Password retry attempts can be used for a prolonged time to try multiple combinations to crack the password.



You have to use the following minimum criteria for creating a password:

- Password must contain a minimum of 8 characters
- At least 1 uppercase character
- At least 1 lowercase character
- At least 1 digit
- At least 1 special character

There is no restriction on maximum password length. NetApp recommends using a password containing a maximum of 12 or 14 characters, which ensures secure encryption.

If password validation fails, then an error is displayed

You have an option to use a system default password by clearing the **Encrypt Query Group Contents With Password** check box. This is however not advisable as using the default password encryption can potentially compromise the passwords in the Query Group.

Updating query group password

You can update the password setting for adding a query or saving a query.

Steps

1. Navigate to **Menu** > **Option**.
2. Click **Update Query Group Password**.

3. Enter the new password in the **Password** and **Confirm Password** fields.

   If you want to continue using the system default password, clear the **Encrypt Query Group Contents With Password** check box.

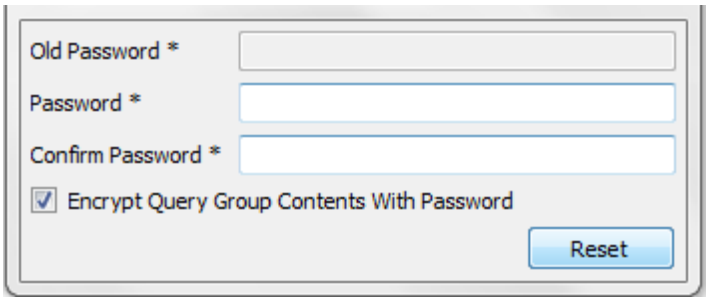
Using forget password option

If you forget the previously created password, create a new password.

Steps

1. Navigate to **Menu** > **Option**.
2. Click **Update Query Group Password**.
3. Click **Forgot Password**.

   A warning dialog box is displayed notifying you that '**Previously encrypted files cannot be decrypted and credentials cannot be loaded.**' After you confirm, you can create a new password.



After using the **Forgot Password** option, you will lose all the previously created query groups data.

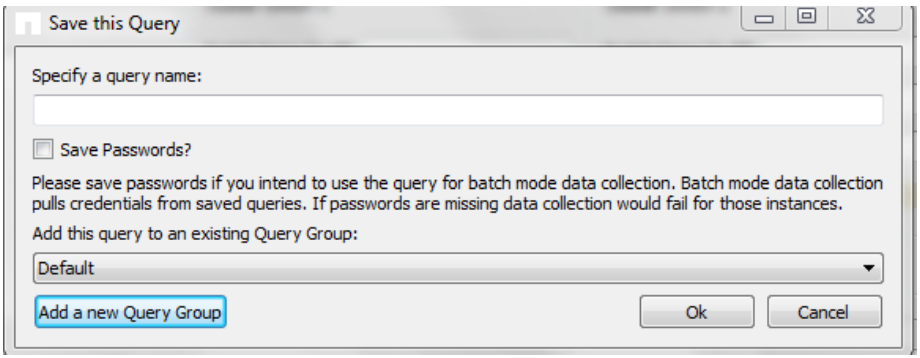
Saving credentials

Steps

1. Enter the credentials in the tabs.
2. You can save the credentials that you enter in the Hostname or IP Address, Username, and Password fields.
3. Click **Save this Query** button provided in each tab.
4. Enter the previously set password or create a new password. If you have chosen to use the default system password, then the password is not required. Enter a name for the query in the **Specify a query name** field.
5. Select the **Save Passwords?** check box, if you want to save passwords, and click **Ok**.
6. Add the query to an already existing query group by selecting a query group from the drop-down list.

   Alternatively, you can click **Add a new Query Group** to create a new query group. The **New Query Group** dialog box is displayed.

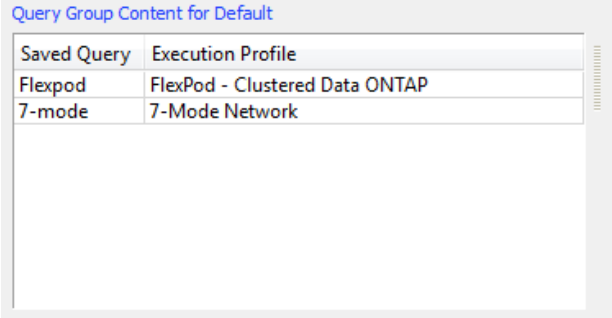
   The **New Query Group** dialog box is as shown:



7. Enter a query group name, and click **OK**. The name is added in the **Query Groups** pane.

   You can double-click a group to list all the queries in the **Query Groups** pane.

   The **Query Groups** pane is as shown:



The fields in the **Query Groups** pane are as follows:

Field	Description
Saved Query	Displays the name of the saved query
Execution Profile	Displays the collection method used Example: If the data is collected in the 7-Mode profile and the **Network** tab is used, 7-Mode Network is displayed

Note: In the Serial Port tab, the COM port details might not be saved correctly.

Loading a query

Following are the tasks that you can perform on a saved query:

If you want to…	Then…
Open a saved query	Double-click the query that you want to open. The relevant credentials are populated in the tab and the status check is performed automatically.
Rename a query	1. Select the query that you want to rename and right - click it. Alternatively, you can select the query that you want to rename and use the Ctrl-H shortcut. 2. Select **Rename Query**. 3. Enter a new query name in the **Rename Query** dialog box. **Note**: "**Default**" query group cannot be deleted.

If you want to…	Then…
Delete a query	1. Select the query that you want to delete and right-click it. Alternatively, you can select the query that you want to delete and use the Ctrl-Z shortcut. 2. Select **Delete**. The query is deleted from the list. **Note**: "**Default**" query group cannot be deleted.

Note: Data collection takes place even if the earlier status checks on a node failed.

Setting Preferences in Config Advisor

You can find information about Config Advisor ASUP, and how to change the initial settings to enable or disable them.

Disabling Telnet

You can disable Telnet as it is an insecure data collection protocol across all of the profiles in Config Advisor by clicking **Options > Preferences > Disable Telnet**.

Enabling Config Advisor AutoSupport

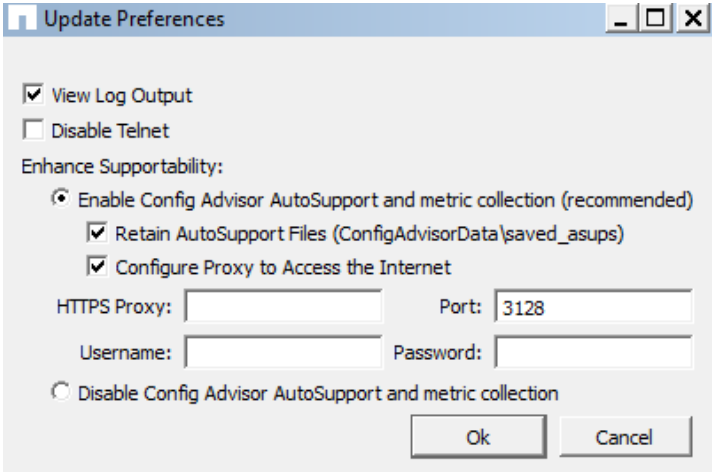
You can enable Config Advisor AutoSupport during the initial launch or by clicking **Options > Preferences > Enable Config Advisor AutoSupport and metric collection (recommended)**. When you enable Config Advisor AutoSupport, Config Advisor sends a Config Advisor AutoSupport message to NetApp after every data collection.

A HTTPS proxy can be configured if proxy setting is required to access the internet. Currently HTTPS proxy will only be enabled while posting Config Advisor ASUPs. Config Advisor also supports additional Basic HTTP Authentication for proxy setting if Username and Password Fields are entered. A default port value of 3128 is set initially.

Note: A Config Advisor AutoSupport file containing the collected data, equipment details, and evaluated rules is created in the ConfigAdvisorDataDirectory_Base/ConfigAdvisorData/asup_files folder. This file is posted to the NetApp ASUP infrastructure. If an Internet connection is available and the post is successful, then the file is deleted. If not, then Config Advisor attempts to post the file during the consecutive tool launch. If Config Advisor ASUP is disabled, then none of the collected data is uploaded to NetApp.

Note: You can retain AutoSupport files in the ConfigAdvisorDataDirectory_Base/ConfigAdvisorData/saved_asups by selecting Preferences > Retain AutoSupport Files check box.

The **Update Preferences** dialog box is as shown:



What Config Advisor AutoSupport is

Config Advisor AutoSupport (ASUP) is similar to Data ONTAP ASUP. Config Advisor sends its collected data, equipment details, and evaluated rules back to NetApp over HTTPS, where the content is stored in NetApp AutoSupport data warehouse. This content provides NetApp Support and partners with configuration details that are useful during case triage or service engagements. Config Advisor ASUP is enabled by default during installation. Config Advisor ASUP is encapsulated in the .xml.gz file format and can contain configuration information about the NetApp systems.

Note: If CA ASUP is enabled, the following information from the collected data will be filtered out to protect customer privacy:

======OPTIONS=====

autosupport.to

autosupport.from

autosupport.support.to

=======SYSCONFIG –A or BMC STATUS======

ASUP from:

ASUP recipients:

These items are filtered unless they contain the following values:

support.netapp.com/asupprod/post/1.0/postAsup

autosupport@netapp.com

eccgw01.boulder.ibm.com/support/electronic/nas

callhome@de.ibm.com

Similar sanitization is done for Data ONTAP 8.x also.

Enabling or disabling Config Advisor logs pane

Steps

1. Click **Options** > **Preferences**.
2. The **Update Preferences** dialog box is displayed.
3. Select the **View Log Output** check box to display the **Config Advisor Logs** pane.
4. Clear the **View Log Output** check box to hide the **Config Advisor Logs** pane.
5. Click **Ok** to update.

What Config Advisor logs pane is

Progress and error details during data collection are displayed in **Config Advisor Logs** located at the bottom of the tool. You can enable or disable the **Config Advisor Logs** pane.

- The **Info** tab displays the connection and command progress.
- The **Errors** tab displays the details of the errors in case of connection failure.

You can choose to hide or display the Config Advisor Logs pane, by using the Alt-V shortcut.

The **Config Advisor Logs** pane is as shown:

Periodic data collection for issues diagnostic

Support staff requires periodic data collection for troubleshooting complex customer issues. There are certain CAP/Escalation cases and other potential support engagements in which periodic data collection is required to debug the root cause.

To support periodic data collection, a Command Line Interface (CLI) is provided to launch and execute Config Advisor. This along with Microsoft Task Scheduler allows you to periodically collect, execute rules, and store results in a chronological folder structure.

Using Config Advisor through the command prompt

For a typical installation, Config Advisor is installed in C:/Program Files (x86) /NetApp/ConfigAdvisor/ or C:/Program Files/NetApp/ConfigAdvisor/. This folder contains the configadvisor.exe executable file. If no command line arguments are specified in the executable file, Graphical User Interface is launched.

The CLI for Config Advisor requires the following three command line arguments.

configadvisor.exe –query <absolute_path_to_the_crypt_file> [--password <USER_DEFINED_PASSWORD> --destination <absolute_path_to save_files_generated]

- -q or –query is a mandatory argument for the CLI. Here you must specify the location of the .crypt file containing the credentials saved from the plug-in profile. For details on the .crypt file, see *Working with credentials*.
  The query saved in the .crypt file knows which plug-in was used to create the query. The same plug-in profile is then used to determine the data collection commands and rules that require execution.
  If there are more than one query within the .crypt file, data collection will not proceed and an error is displayed in the log file.
- -p or –password is a mandatory argument if the .crypt file specified as a value for –query is encrypted with a user defined password. If you do not provide the password, then it is presumed that the .crypt file was encrypted using the default password.
- -d or –destination is an optional argument. It specifies the directory location to save the collected data, PDF report, log information and AutoSupport file. AutoSupport file also

contains the rule results in XML.
If the argument is not specified, ~ ConfigAdvisorDataDirectory_Base/ConfigAdvisorData is set as the destination folder. You must ensure that the destination folder specified has sufficient space and is writable. For every instance of data collection, sub folders are created inside the destination folder before placing the result files. The sub folders are created automatically using the following format: <ProfileName>/Year/Month/Day/Time. For example: <destination>/ MetroCluster in clustered Data ONTAP /2014/08/10/21_30/.

If you specify a valid query, data collection will proceed and the following files will be created in the destination folder.

- **Collected data file** – This is a .gzip file that contains the collected raw data in XML. This same file can be reopened using the Config Advisor GUI. Navigate through the GUI menu, click **File** > **Open Config Advisor File**.
- **AutoSupport file** – The AutoSupport file is not posted, but pasted into the same directory location. This file is a tgz (tar.gz) file containing the Collected Data, Rules Results in XML, Equipment Details, Manifest File, and a header. You should send this file back to NetApp for support.
- **PDF report** – A PDF report is generated by evaluating and presenting the Rule Results in a PDF format.

Note: The PDF file is not automatically opened. You must locate the file inside the destination folder to view the contents.

- Log data – A plain text log is also provided that specifies the command line execution status. Here, the exceptions are also recorded.

If data collection fails and equipment is not correctly identified, then the AutoSupport File and PDF report is not generated. The Collected Data File and Log Data will be available. If the plug-in is not identified and Data Collection is not even initiated, only the Log Data will be present. The Log Data file will be available in either of the following locations depending on the execution progress:

- ConfigAdvisorDataDirectory_Base/ConfigAdvisorData/logs
- <DESTINATION_FOLDER_SPECIFIED>/<ProfileName>/Year/Month/Day/Time

If you execute Config Advisor on the CLI, you will be redirected to the command prompt. Standard output and errors are not captured on the console. When using the CLI, you can rely only on the log data file created in the destination folder, or ConfigAdvisorDataDirectory_Base/ConfigAdvisorData/logs as specified in the preceding section. The log file is named as <timestamp>_log.txt where timestamp is the Greenwich Mean Time of the system.

With CLI, you can execute the Config Advisor through the command prompt and generate the preceding four files into the destination folder location. You can execute multiple instances of Config Advisor using CLI and they do not conflict with each other.

Scheduling periodic data collection

For scheduling periodic data collection, you need to use the Windows Task Scheduler. Task Scheduler is a Microsoft Windows component. You can use Task Scheduler to run programs or scripts at a time that is most convenient for you. The Windows Event Log service must run before the Task Scheduler starts up.

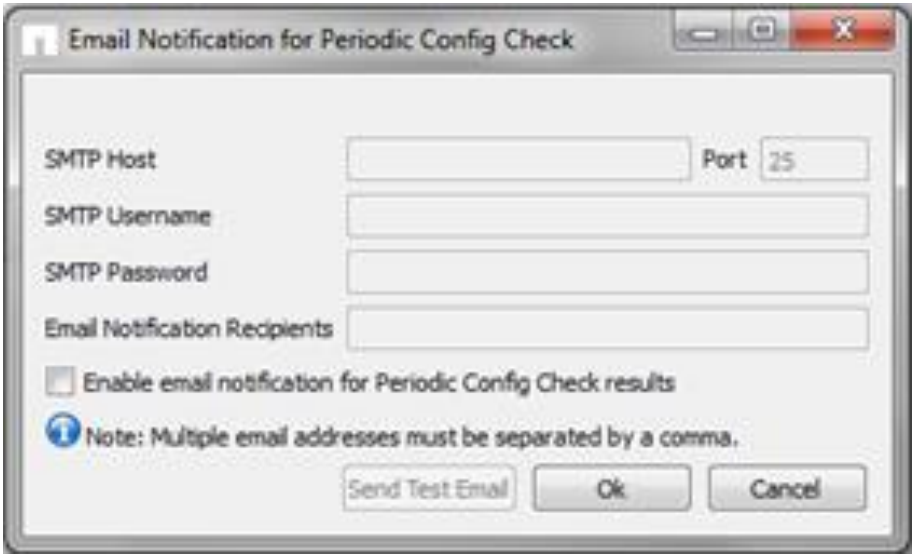
For creating a basic task or an advanced task, see Windows Task Scheduler documentation that can help you invoke the Config Advisor Command Line interface based on a predetermined schedule (for example, hourly or daily).

Email notification

You can enable an Email Notification feature if you encounter high impact issues during Periodic Data Collection. This feature is enabled through the Graphical User Interface.

Steps

1. Navigate to GUI **Menu** > **Options** > **Email Notification for Periodic Config Check**.



2. Enter the SMTP server host, port, username, password, and email addresses. Select the check box if you want to receive email notification periodically.
3. Use the **Send Test Email** button to test the SMTP server. A test email will be send to the email notification recipients.

Reporting issues in Config Advisor

Support for Config Advisor is provided only online. You can report issues in Config Advisor by opening a support ticket within Config Advisor.

Steps

1. In the Config Advisor tool, click **Help** > **Open Support Ticket**.

   The *track.netapp.com* web page is displayed.

2. Enter your user name and password, and click **Login**.

   Note: If you do not have an account, you can create a new account by clicking **Sign up Now!**.

3. Enter the required support details in the form.

   Note: The fields marked with an asterisk are mandatory.

4. Attach the Config Advisor result file in the xml.gz format. For more information, see *Recent Results pane*.

5. Click **Save**.

   A reference number for your issue is displayed. You must save this reference number for future use.

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.
- **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.

Keeping the resource data updated

Config Advisor uses a resources file that contains latest firmware recommendations and compatibility matrixes. This file is automatically updated if the Internet network is available.

In the case of secure sites, no network access is available. You are required to manually download resource_binary.zip from *http://mysupport.netapp.com/public/config_advisor/bin/resources_binary.zip* and place it in the ConfigAdvisorDataDirectory_Base/ folder replacing the “resources_binary” file. Do not extract the zip file. Rename the file to remove .zip extension.

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 ONTAP 7.x and 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**.

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*.

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. 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.

Installing Data ONTAP PowerShell toolkit 2.0

You can find information about the prerequisites for installing Data ONTAP PowerShell toolkit 1.5 and how to install Data ONTAP PowerShell toolkit 2.0.

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. Download the Data ONTAP PowerShell toolkit 2.0 or later from the Communities web site at *communities.netapp.com/community/products_and_solutions/microsoft/powershell*.

Note: To download the NetApp Data ONTAP PowerShell Library, you must log in to communities.netapp.com.

To download samples of PowerShell code, you must log in to the http://mysupport.netapp.com/

To only view the code samples, you can access the **Communities** (communities.netapp.com) and **Forums** (www.netapp.com/us/communities/community-forums.html) web pages.

2. Download the DataONTAP.ZIP file to a temporary directory on your machine.
3. Unzip the Data ONTAP PowerShell toolkit to the same folder as the PowerShell installation directory: C:/Windows/System32/WindowsPowerShell/v1.0/Modules.

   Alternatively, you can use the Install.ps1 script, which unzips and copies the files. The script checks whether to copy the files to each location in the PSModulePath environment variable, one at a time.
4. 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.
```

5. 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

6. 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.

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:

Data collection methods for secure sites

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

Steps

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.

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.
3. For example, if you have stored the script in the C drive, then enter cd c:/.
4. Invoke the Data Collector and Sanitizer script by entering ./secure_datacollector.ps1, and press Enter.
5. Based on your requirement, select either one of the options, and press Enter:

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 <home Directory>/ConfigAdvisorScriptData.

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).

Steps

1. Enter Y for yes or N for no depending on whether you want to run extended checks on the controllers or not.
2. 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.

3. Enter the host name or IP address of the controller, and press **Enter**.

4. Enter the user name, and press **Enter**.
5. 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.
6. 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.

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.

4. 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].
```

   a) 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.

   b) If you choose N, then all the output files by default will be stored at <home Directory>/ConfigAdvisorScriptData.

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

5. 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.

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.

Parameter name	Alias	Description
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.
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 Output_folder location (provided through the input parameter) is filtered. Valid filtering options that can be used along with this parameter are -m, -l. 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 **Use_Mapping** option.
Use_Mapping	-m	This parameter indicates that sensitive data will be replaced with generic names such as xx.xx.xx.01 (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 <timestamp>_MAPPING.csv. 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 **UnFiltered** option. Mapping information is not generated for license keys, MAC addresses, and HBA addresses.

<table>
<tr><th>Parameter name</th><th>Alias</th><th>Description</th></tr>
<tr><td>FilterLevel</td><td>-l</td><td>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 **-Use_Mapping**.

Note:
<table>
<tr><th>Level</th><th>Item</th></tr>
<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>
</table></td></tr>
</table>

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.

Collecting data manually

In certain secure sites, if it is not permitted to run the script on the system, you can manually run the 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:

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 =====
fcp 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 =====

ONTAP 7-Mode commands	AutoSupport names
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 =====
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 preceding table, without any extra spaces.

An 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 dataggr (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.

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

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

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
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 Igrp4234 (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

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.

Importing filtered data file for analysis

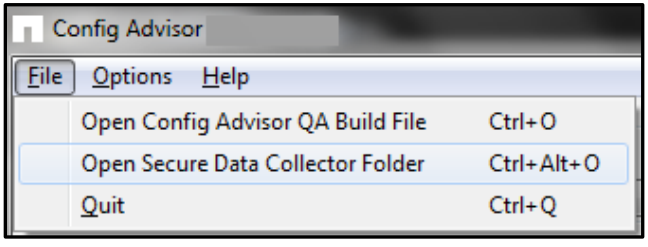
Config Advisor uses a resources file that contains latest firmware recommendations and compatibility matrixes. This file is automatically updated if the Internet network is available.

In the case of secure sites, no network access is available. You are required to manually download resource_binary.zip from *http://mysupport.netapp.com/public/config_advisor/bin/resources_binary.zip* and place it in the ConfigAdvisorDataDirectory_Base/ folder and replace the “resource_binary” file. Note that the replaced file does not have the .zip extension. Restart Config Advisor for the new file to take effect.

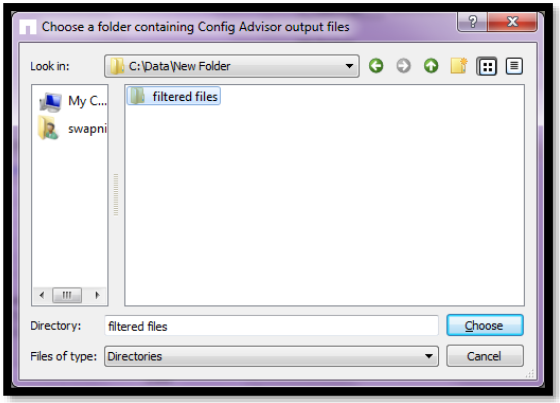
Steps

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**.

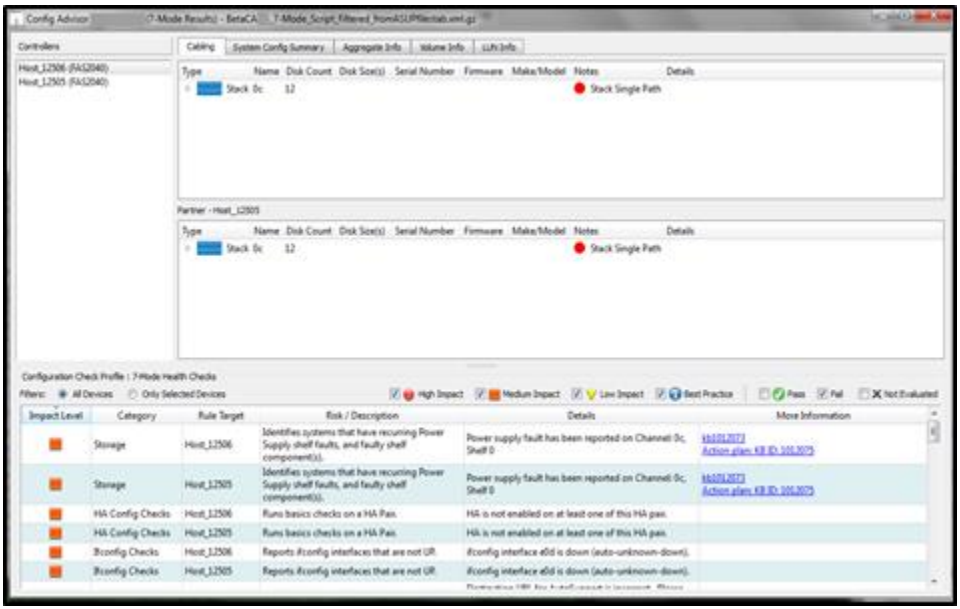


3. Provide the name of the Config Advisor result file.

   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.

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:
   a) Get-Help ./secure_datacollector.ps1 or
   b) 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
   ```

Troubleshooting

You can find information about how to troubleshoot some of the issues that you might come across when you use Config Advisor. You can also find explanations for the issues, possible causes, and solutions.

Entering AutoSupport ID in the old format displays an error message

Issue

Config Advisor 3.1 or later displays an error message when you enter an AutoSupport ID in the AE123456789867654 format.

Note: This issue is relevant only for users with access to NetApp intranet.

Possible cause

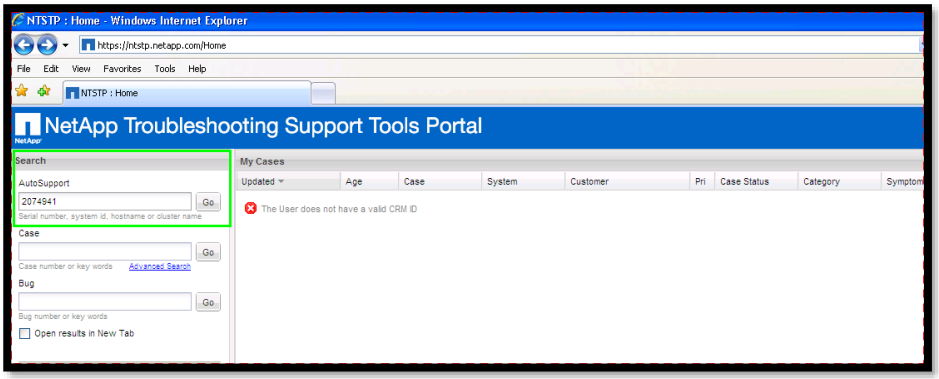
Config Advisor does not support the earlier AutoSupport ID format, which begins with AE, followed by 15 digits.

Workaround

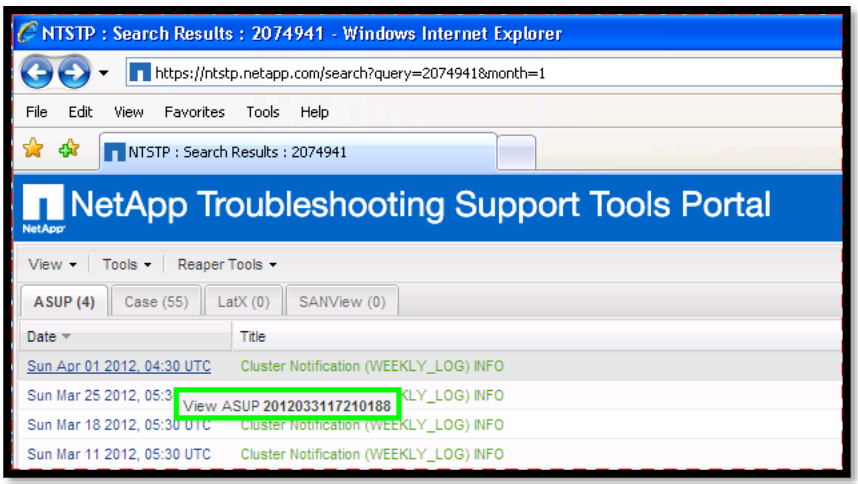
Steps

1. Log in to the *http://mysupport.netapp.com/* using your Single Sign-On credentials.
2. Enter the serial number, system ID, and host name or cluster name of the controller for which the new format of the AutoSupport ID is to be found in the AutoSupport field.

A list of AutoSupport IDs is displayed as shown:

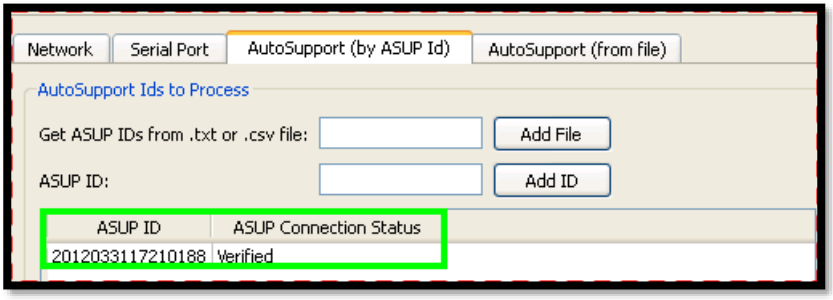


3. Select a date for the AutoSupport ID and point the cursor on the ID to get the new format of that AutoSupport ID as shown:



4. Enter the new format of the AutoSupport ID.

The ID is verified as shown:



Note: If you only delete AE from the earlier AutoSupport ID format, the new format is not generated automatically.

Cabling faults not identified for FC and SATA shelves

Issue

Config Advisor does not show physical cabling faults for FC and serial advanced technology attachment (SATA) shelves.

Possible cause

Config Advisor recognizes cabling faults only with serial-attached SCSI (SAS) shelves and ONTAP, and also reports only for SAS shelves.

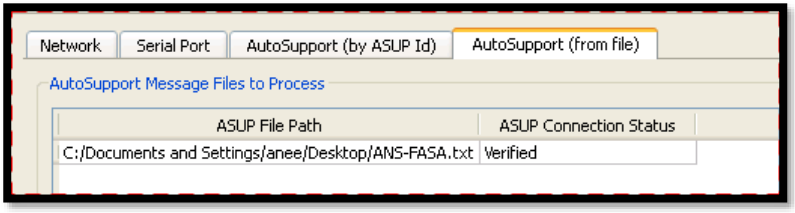
Workaround

A Best practice cabling method has been developed that enables ASIC, HBA, and port isolation for all configurations. This method also enables correct top or bottom cabling for the stacks. You should use this cabling method for all NetApp storage configurations. The **Universal SAS Cabling Guide** is the official source for all SAS MPHA cabling; it is available on the *http://mysupport.netapp.com/* .

The same approach can also be used for FC cabling. For FC and SATA shelves, the physical cabling can be verified only manually.

Format of the text file for the AutoSupport (from file) tab

The AutoSupport (from file) tab is as shown:



Explanation

Config Advisor supports only text files as input for AutoSupport (from file) tab.

There are two sources of input:

1. The AutoSupport sections taken directly from the controller (from /etc/log/autosupport). The RC file contents, HOSTS file contents, and OPTIONS contents, are not present in the file. Therefore, you have to copy the following:
   a. The rdfile /etc/rc command output under the header ===== RC =====
   b. The rdfile /etc/hosts command output under the header ===== HOSTS =====
   c. The Options command output under the header ===== OPTIONS =====
2. The AutoSupport sections taken only from the AutoSupport IDs on the web (only NetApp partners) or email (configured in the AutoSupport options).

Config Advisor logs pane displays data collection failure for certain ONTAP commands

Issue

Config Advisor logs pane displays data collection failure for some commands on certain versions of ONTAP, for example:

- 7-Mode command: `license show`
- ONTAP commands: `storage failure show -fields mode, system license status show, vServer services dns show`

Description

These commands are not found or deprecated in certain versions of ONTAP, and ONTAP version is not determined by Config Advisor during data collection. Hence these commands are displayed as failed in **Config Advisor logs** pane. After the data is collected by Config Advisor, the **Config Advisor Viewer** window, which displays the raw data at the time of data collection, does not display these commands.

Workaround

After the data is collected by Config Advisor, the "viewer window" which displays the raw data at the time of data collection does not display these commands.

Cabling faults not identified for optical SAS cables with non-integrated QSFP present in a stack

Issue

For ONTAP versions older than 9.x, Config Advisor does not identify physical cabling faults for Optical SAS cables with non-integrated QSFP in a stack. Config Advisor does support All-in-One (AOC) Optical SAS cable.

Possible cause

Config Advisor traces the physical cabling through the same serial number on both ends of the twinax SAS cables. For optical SAS cables with non-integrated QSFP, the serial numbers are different at both the ends.

Workaround

A best practice cabling method has been developed that enables ASIC, HBA, and port isolation for all configurations. This method also enables correct top or bottom cabling for the stacks. You should use this cabling method for all NetApp storage configurations. The Universal SAS Cabling Guide is the official source for all SAS MPHA cabling; it is available on *http://mysupport.netapp.com/*.

The same approach can also be used for optical SAS cabling.

When optical SAS cables with non-integrated QSFP are used, the physical cabling can be verified only manually.

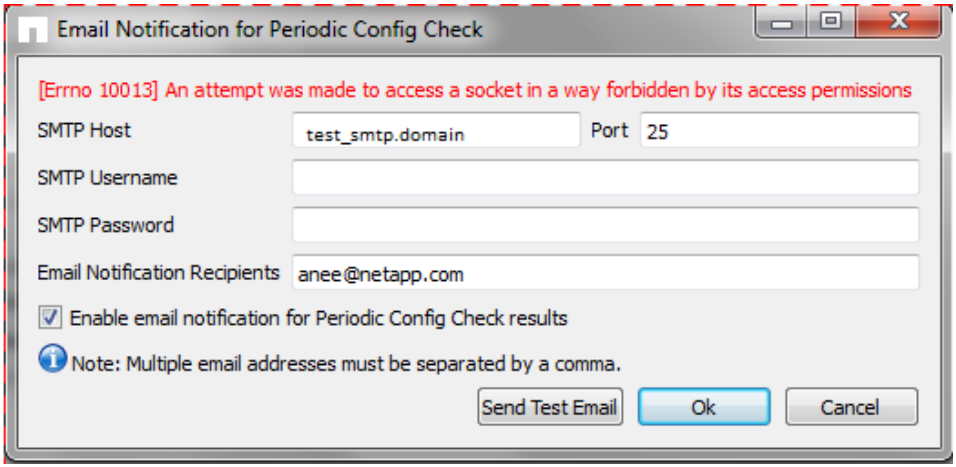
Sending email displays an error message

Issue

Email that is sent fails with an error “An attempt was made to access a socket in a way forbidden by its access permissions.”

Description

Email feature available for Config Advisor plug-ins from command line [menu “Options” > “Email notification for Periodic Config Check”] shows the following error when “Send Test Email” or “**Ok**” button clicked.



Probable cause

“configadvisor.exe” is blocked by access protection policy of the antivirus or blocked by the firewall.

Proposed solution

Check the antivirus logs or firewall logs. Contact your IT team for support stating the issue.

Appendix A: Configuration validations & health checks

Check Name	Description	Supports Cluster Mode	Supports 7-Mode	Supports Transition
Shelf Path Checks	Checks the path configuration of the shelves.	✓	✓	✓
Shelf Checks	Checks the shelf compatibility within a stack.	✓	✓	✓
Shelf Compatibility Checks	Checks FAS2220/N3150 Shelf Rules.	✓	✓	✓
Shelf Compatibility Checks	Checks for DS4486 Shelf Rules.	✓	✓	✓
Shelf Compatibility Checks	Checks DS4246 shelf configuration and best practices.	✓	✓	✓
Shelf Compatibility Checks	Runs various shelf compatibility checks.	✓	✓	✓
ACP Cabled and Configured	Checks to see if ACP cables are installed correctly and ACP is enabled on the storage controller.	✓	✓	✓
SAS Cabling Checks	Checks SAS Cabling. **Note**: It is not executed when ATTO bridges are used.	✓	✓	✓
HA Auto-giveback Enabled	Ensures HA systems are configured for auto-giveback.	✓		
Storage Failover State	Validates Storage Failover State to ensure Non-Disruptive Operations.	✓		
Service Processor Status	Improves 10GBE performance. Set flow control to none/none on all 10GBE cluster/data ports.	✓		
Flow Control Set to None	Ensures Service Processor is available and operational.	✓		

Check Name	Description	Supports Cluster Mode	Supports 7-Mode	Supports Transition
NTP Server Defined and Enabled	Verifies that Network Time Protocol (NTP) has been configured and enabled on all nodes of the cluster.	✓		
Timezone Set	Verifies that the time zone is consistent across all nodes in the cluster.	✓		
DNS Configured Check	Verifies that DNS is configured in the cluster.	✓		
Cluster HA	Checks to see if Cluster High Availability is configured correctly.	✓		
One Node Cluster Check	Checks if the node is a single node cluster and has the appropriate settings.	✓		
Uniform and Single License Checks	Checks for a valid cluster license, or if all nodes have uniform node locked licenses. Raise an alert if there is only a single node locked license in a cluster.	✓		
V-Series License Checks	Checks to ensure that at least one V_STORAGEATTACH license is installed in the cluster when a v-series is in use.	✓		
All Nodes Same ONTAP	Verifies that all nodes of the cluster are running the same version of ONTAP.	✓		
All Nodes Same ONTAP	Verifies that all nodes of the cluster have the same default ONTAP image version.	✓		
All Nodes Same ONTAP	Verifies that the current and default ONTAP image versions for the cluster nodes are the same.	✓		
Cluster Node CDP	Verifies that Cisco Discovery Protocol is running on the Cluster.	✓		
Switchless Cluster Port Check	Checks the ports in a switchless cluster.	✓		
HA Configuration	Checks for HA configuration issues.		✓	
HDD Firmware Bug	Checks for failed disks and disks that are not reporting properly to ONTAP.	✓	✓	✓
HDD Firmware Bug	Checks for HDD firmware issues.	✓	✓	
I/O Module Firmware Bug	I/O Module firmware checks.		✓	

Check Name	Description	Supports Cluster Mode	Supports 7-Mode	Supports Transition
Platform	Checks for multiple EMERGENCY messages that report some environmental instability.		✓	
Platform	Identifies all storage controllers that have power supplies that have compromised the power redundancy.		✓	
Platform	Checks for platform related at Risk System issues.		✓	
Software Bug	Checks the ONTAP version for related software bugs.		✓	
Storage	Checks for failed disks and disks that are not reporting properly to ONTAP.	✓	✓	✓
Storage	This signature identifies single path standalone FAS3XXX and FAS6XXX systems.		✓	
Storage	Identifies 7G Multipath HA configurations that are miswired. Both the primary and redundant path to one (or more) disk shelves is connected to the same shelf IO module.		✓	
Storage	Identifies systems that have recurring Power Supply shelf faults, and faulty shelf component(s).		✓	
Storage	Checks filers that have bypassed drives.		✓	
Storage	Identifies systems that have Temperature Sensor faults, and faulty shelf component(s).		✓	
Storage	Identifies a v-series system that does not have enough paths to the backend storage.		✓	
Storage	Identifies systems that have Module (I/O) Faults, and the faulty shelf component(s).		✓	
Storage	Greater than 6 DS14-type shelves on a loop is unsupported		✓	
Storage	ONTAP 7.3 and later releases do not support LRC, ESH and ESH2 modules in the DS14mk1 disk shelf, and the LRC and ESH modules in the DS14mk2 disk shelf.		✓	

Check Name	Description	Supports Cluster Mode	Supports 7-Mode	Supports Transition
Storage	Identifies Shelf Cooling Unit (FAN) faults.		✓	
Storage	The LSI Logic 949E HBA cards with a board version rev. A1 and A.2 may experience PCI Express error panic caused by MfTLB (Malformed TLP).		✓	
Storage	Identifies systems exposed to TSB-1007-04 where systems running ONTAP less than 7.3.5 (and 7.3.3P*) with DS4243 disk shelves are potentially vulnerable to data loss. Relevant Burts are 381855 and 392452.		✓	
Storage	Checks for Systems with DS14-type IO module missing.		✓	
Storage	Checks for storage related at Risk System checks.	✓	✓	✓
System Firmware Bug	Checks for system firmware bugs.		✓	
System Configuration	Checks for System Configuration Issues.		✓	
RC File Checks	Reports failures while parsing the output of 'rdfile /etc/rc' and 'ifconfig -a'.		✓	
If config Checks	Reports ifconfig interfaces that are not UP.		✓	
Exports File Check	Compares the exports from /etc/exports and exportsfs.		✓	
Host File Checks	Checks if the hostname appears as in /etc/hosts.		✓	
MTU Checks	Reports MTU inconsistencies while parsing the output of 'rdfile /etc/rc' and 'ifconfig -a'.		✓	
Autosupport Checks	Checks if AutoSupport is configured properly.	✓	✓	
Max Snapshot Checks	Checks the Snapshot limits for the given ONTAP release are within 90% of recommended setting for NDU upgrade.	✓	✓	
Max Flex Volume Checks	Checks the FlexVol limits for the given ONTAP release are within 90% of recommended setting for NDU upgrade.	✓	✓	

Check Name	Description	Supports Cluster Mode	Supports 7-Mode	Supports Transition
V-Series License Checks	Checks to ensure that a V_STORAGEATTACH license is installed when a v-series is in use.		✓	
HA Config Checks	Runs basics checks on an HA Pair.	✓	✓	
HA Option Checks	Checks if the /etc/rc options are symmetrical on the HA pair.	✓	✓	
HA License Checks	Checks if software license(s) match on both nodes of HA pair	✓	✓	
Revision Checking	Checks System Firmware revision.	✓	✓	✓
Revision Checking	Checks Shelf Firmware version.	✓	✓	✓
Revision Checking	Checks Disk Firmware revision.	✓	✓	✓
Revision Checking	Checks RLM Firmware version.	✓	✓	✓
Revision Checking	Checks Service Processor(SP) Firmware version.	✓	✓	✓
Revision Checking	Checks BMC Firmware version.	✓	✓	✓
Cluster Switch RFC 5010	Compares the switch's configuration to that of the Reference Configuration File (RCF) for a Cisco Nexus 5010.	✓		
Cluster Switch RCF 5020	Compares the switch's configuration to that of the Reference Configuration File (RCF) for a Cisco Nexus 5020.	✓		
Cluster Switch RCF 5596/5596T	Compares the switch's configuration to that of the Reference Configuration File (RCF) for a Cisco Nexus 5596/5596T.	✓		
Cluster Switch RCF 3132QV	Compares the switch's configuration to that of the Reference Configuration File (RCF) for a Cisco Nexus RCF 3132QV	✓		
Cluster Switch Software Version	Compares the Cluster switch IOS version to the expected version, which is matched to the Golden Config. This rule will be run against each cluster switch.	✓		

Check Name	Description	Supports Cluster Mode	Supports 7-Mode	Supports Transition
Cluster Switch ISL Count	Verifies the ISL count between the cluster switches.	✓		
Cluster Switch ISL Ports	Verifies that the ISL links between each cluster switch is on the specified ports which will vary based on the switch model.	✓		
Cluster Switch Ports	Verifies that the links between each cluster switch is on the specified ports which will vary based on the switch model.	✓		
Cluster Switch Fan	Verifies that the fans in the cluster switch are running.	✓		
Cluster Switch Power Supply	Verifies that there is power supply in the cluster switch.	✓		
Cluster Switch CDP	Verifies that Cisco Discovery Protocol is running on the switch.	✓		
Cluster Switch SFP	Verifies that the SFP associated with each interface is correct.	✓		
Cluster Switch Exp Module Model	Verifies that the expansion module is of the correct model.	✓		
Mgmt Switch RCF 2960	Compares the switch's configuration to that of the Reference Configuration File (RCF) for a Catalyst 2960.	✓		
Mgmt Switch Software Version	Compares the management switch IOS version, which is matched to the Golden Config. This rule will be run against each management switch.	✓		
Mgmt Switch ISL Count	Verifies the management switch ISL count.	✓		
Mgmt Switch ISL Ports	Verifies that the ISL links between each management switch are on specified ports.	✓		
Mgmt Switch Fan	Verifies that the fans in the management switch are running.	✓		
Mgmt Switch PS	Verifies that there is power supply in the management switch.	✓		
Mgmt Switch CDP	Verifies that Cisco Discovery Protocol is enabled on the switch.	✓		

Check Name	Description	Supports Cluster Mode	Supports 7-Mode	Supports Transition
Cluster Node Connect to Cluster Switch	Verifies that all cluster nodes have a connection to each cluster switch.	✓		
Cluster Node Connect to Mgmt Switch	Verifies that all cluster nodes have a connection to a management switch.	✓		
Node Cluster NIC Model	Verifies that the NIC models are compatible in the cluster network.	✓		
Cluster Node Port Roles	Verifies that the cluster ports and the management ports are on valid slots for the cluster network	✓		
Cluster Switch RCF CN1610	Compares the switch's configuration to that of a Reference Configuration File (RCF) for a CN1610.	✓		
Cluster Switch RCF CN1601	Compares the switch's configuration to that of a Reference Configuration File (RCF) for a CN1610.	✓		
Cluster Switch Software Version	Checks the switch OS FASTPATH version.	✓		
Cluster Switch ISL Count	Verifies Cluster Switch ISL count.	✓		
Cluster Switch ISL Ports	Verifies that the ISL links between each cluster switch is on the specified ports which will vary based on the switch model.	✓		
Cluster Switch Ports	Checks cluster switch port speed.	✓		
Cluster Switch Fan	Verifies that the fans in the cluster switch are running.	✓		
Cluster Switch PS	Verifies that there is power supply in the cluster switch.	✓		
Cluster Switch ISDP	Verifies that ISDP is running and can see all other devices in the cluster network.	✓		
Mgmt Switch Golden Config 1601	Compares the switch's configuration to that of the Reference Configuration File (RCF) for a CN1601 Management Switch.	✓		
Mgmt Switch Software Version	Checks the switch OS FASTPATH version.	✓		

Check Name	Description	Supports Cluster Mode	Supports 7-Mode	Supports Transition
Mgmt Switch ISL Count	Verifies Management Switch ISL count.	✓		
Mgmt Switch ISL Ports	Verifies that the ISL links between each management switch are on specified ports.	✓		
Mgmt Switch Fan	Verifies that the fans in the management switch are running.	✓		
Mgmt Switch PS	Verifies that there is power supply in the management switch.	✓		
Cluster Switch ISDP	Verifies that ISDP is running and can see all other devices in the management network.	✓		
Cluster Node Connect to Cluster Switch	Verifies that all cluster nodes have a connection to each cluster switch.	✓		
Cluster Node Connect to Mgmt Switch	Verifies that all cluster nodes have a connection to a management switch.	✓		
Cluster Node Port Roles	Verifies that the cluster ports and the management ports are on valid slots for the cluster network.	✓		
Node Cluster NIC Model	Verifies that the NIC models are compatible in the cluster network.	✓		
AFF SSD Ownership	Verifies that SSDs have been properly assigned to each node on AFF systems.	✓		
ARS Sig_Burt: 866045	Unsupported SAS card in FAS80x0 controller.	✓	✓	
ARS Sig_Burt: 905019	Checks for Single-Mode ifgroups in an ONTAP system.	✓		
ARS Sig_Burt: 885134	Checks for Foreign Aggregates in an ONTAP system.	✓	✓	
ARS Sig_Burt: 770979	Takeover is not possible	✓		
ARS Sig_Burt: 847975	Checks for an ineligible node in a cluster.	✓	✓	
ARS Sig_Burt: 771008	In a two-node cluster, cluster HA ensures that the failure of one node does not disable the cluster.	✓		

Check Name	Description	Supports Cluster Mode	Supports 7-Mode	Supports Transition
ARS Sig_Burt: 817749	Checks for SAS shelves with the same disk shelf ID.	✓	✓	
ARS Sig_Burt: 823216	Checks if all the nodes in the cluster are running the same ONTAP version.	✓		
Controller Hostname Check	Verifies that controller hostname contains only valid characters.	✓		
ARS Sig_Burt: 717777	If a LIF's failover-group is not configured properly, it is possible that the LIF will migrate to a port that is unable to reach and will be unable to serve data until migrated to the home port.	✓ (ASUP only)		
ARS Sig_Burt: 2121	ASUP delivery may fail when choosing an unexpected network route or LIF.	✓ (ASUP only)		
ARS Sig_Burt: 2085	Checks if the digital certificate for an SVM has expired. Clients may not be able to connect to the cluster over secure (SSL based) protocols.	✓ (ASUP only)		
ARS Sig_Burt: 2122	ASUP delivery may fail when the intercluster LIF resides on the same subnet as the node-mgmt LIF.	✓ (ASUP only)		
ARS Sig_Burt: 2184	Checks if Cluster HA is not configured properly.	✓ (ASUP only)		
ARS Sig_Burt: 2186	System shuts down due to the battery in NO_CHARGE state.	✓ (ASUP only)		
ARS Sig_Burt: 2191	An issue in the NVRAM9 configuration RAM (CRAM) might cause panic.	✓ (ASUP only)		
ARS Sig_Burt: 2197	Checks if Data ONTAP version has reached end of support.	✓ (ASUP only)		

Check Name	Description	Supports Cluster Mode	Supports 7-Mode	Supports Transition
ARS Sig_Burt: 910684	Either SMB 2.x needs to be disabled (SMB 2.x connected clients, reboot required) or upgrade to a fixed-in version of Data ONTAP.	✓ (ASUP only)		
ARS Sig_Burt: 886225	A system disruption might occur. This issue can be the result of a race condition or of an on-disk corruption in the aggregate.	✓ (ASUP only)		
ARS Sig_Burt: 885132	SVM(s) has/have Telnet and/or RSH enabled.	✓ (ASUP only)		
SVM Management LIF Check	Verifies the management LIF configured for Storage Virtual Machine.	✓		
Node Management LIF Check	Verifies if all the node management interfaces are configured correctly.	✓		
Cluster Management LIF Check	Verifies if all the cluster management interfaces are configured correctly.	✓		
IFGRP Configuration Check	Verifies configuration mode and health of the ifgroup.	✓		
Device Online Check	Checks that the devices were online and data collection was successful.	✓		
Broadcast Domain Configuration Check	Checks if Broadcast Domain is correctly configured.	✓		
IPspace Configuration Check	Checks if IPspace is correctly configured.	✓		

Check Name	Description	Supports Cluster Mode	Supports 7-Mode	Supports Transition
HA Interconnect Links Check	Checks if all of the interconnect links are up for each node.	✓		

Copyright information

Copyright © 1994–2016 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, Go Further, Faster, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. A current list of NetApp trademarks is available on the web at *http://www.netapp.com/us/legal/netapptmlist.aspx*.

Cisco and the Cisco logo are trademarks of Cisco in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

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 to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277