Config Advisor 3.2

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: **215-07531_A0**
February 2013

Copyright Information

Trademark Information

Table of Contents

Preface

This document describes how to install, configure, and run Config Advisor 3.2 to verify NetApp hardware installations in secure and non-secure sites.

AUDIENCE

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

KEYBOARD AND FORMATTING CONVENTIONS

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

Keyboard conventions

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

Formatting conventions

Convention	What it means
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.
`Monospaced` font	• Command names, option names, and daemon names. • Information displayed on the system console or other computer monitors. • Contents of files. • File, path, and directory names.
`Bold monospaced` font	Words or characters you type. What you type is always shown in lowercase letters; unless your program is case-sensitive and uppercase letters are necessary for it to work properly.

SPECIAL MESSAGES

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

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

HOW TO SEND YOUR COMMENTS

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

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

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

TERMINOLOGY

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

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

are sometimes referred to as *filers*, *appliances*, *storage appliances*, *V-Series systems*, or *systems*.

DEFINITIONS, ACRONYMS, AND ABBREVIATIONS

Abbreviation/Phrase	Explanation/ Definition
Clustered ONTAP configuration	The integration of Ethernet switch fabrics into NetApp's 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 Data 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
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's '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 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 etc. As such, these messages may contain data collected from multiple devices, both NetApp systems and non-NetApp systems.
UCS	Unified Computing System
FCP	Fiber Channel Protocol
FCoE	Fiber Channel over Ethernet
FQDN	Fully Qualified Domain Name

1 Introduction to Config Advisor

Config Advisor 3.2 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 NetApp-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 serial port, network, AutoSupport ID, and AutoSupport file. Config Advisor collects information from NetApp controllers, switches, and Cisco Unified Computing System (UCS) blades, which are compared with configuration best practices.

1.1 What Config Advisor is

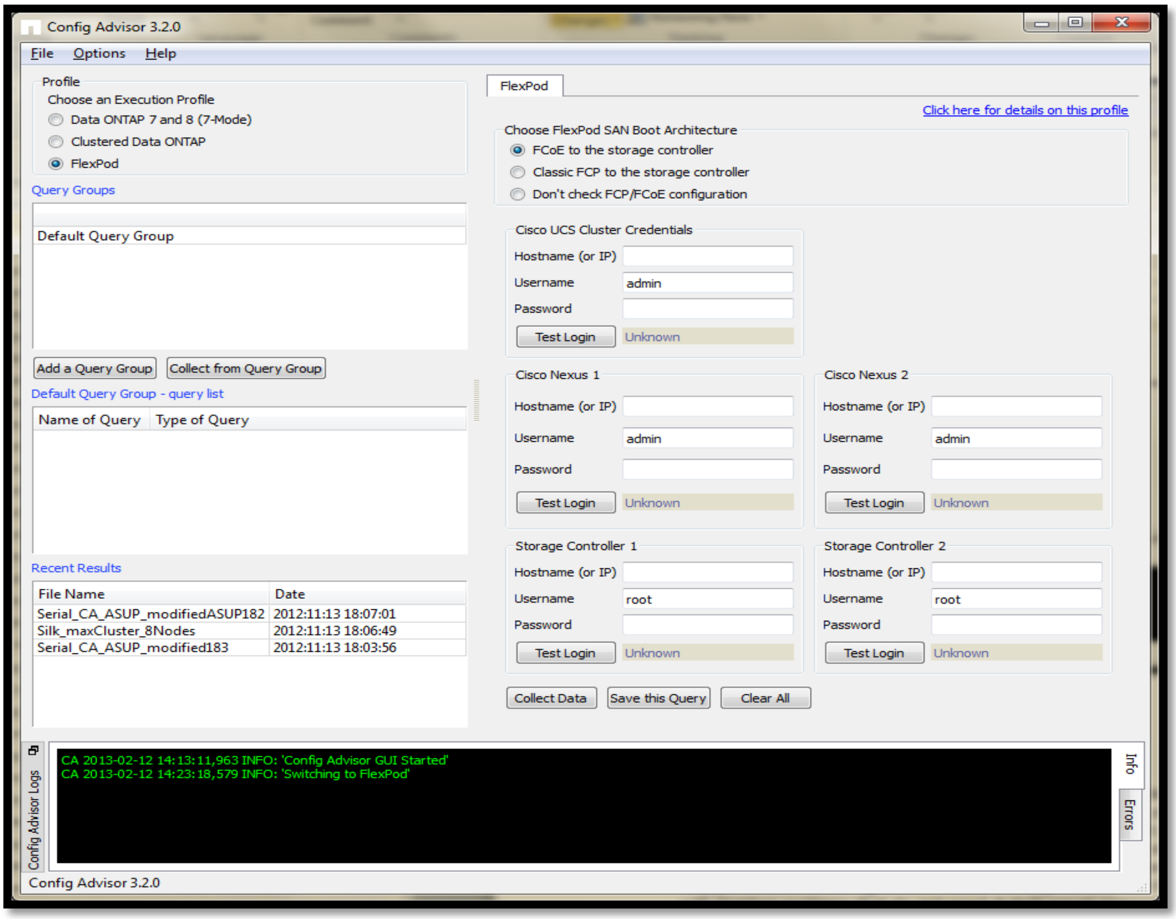
Config Advisor is the next generation WireGauge tool and is based on the WireGauge architecture. It has all the features of WireGauge along with some newly added features such as:

- Additional At-Risk-Systems (ARS) checks
- Clustered Data ONTAP checks
- FlexPod common configuration checks
- Ability to generate results in Microsoft Word or Excel to provide detailed configuration reports
- Collect, cleanse, and analyze secure site data

It 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:



Profile
Choose an Execution Profile
○ Data ONTAP 7 and 8 (7-Mode)
○ Clustered Data ONTAP
● FlexPod

Query Groups
Default Query Group

Default Query Group - query list

Name of Query	Type of Query

Recent Results

File Name	Date
Serial_CA_ASUP_modifiedASUP182	2012:11:13 18:07:01
Silk_maxCluster_8Nodes	2012:11:13 18:06:49
Serial_CA_ASUP_modified183	2012:11:13 18:03:56

Choose FlexPod SAN Boot Architecture
● FCoE to the storage controller
○ Classic FCP to the storage controller
○ Don't check FCP/FCoE configuration

Cisco UCS Cluster Credentials
Hostname (or IP):
Username: admin
Password:
Test Login: Unknown

Cisco Nexus 1
Hostname (or IP):
Username: admin
Password:
Test Login: Unknown

Cisco Nexus 2
Hostname (or IP):
Username: admin
Password:
Test Login: Unknown

Storage Controller 1
Hostname (or IP):
Username: root
Password:
Test Login: Unknown

Storage Controller 2
Hostname (or IP):
Username: root
Password:
Test Login: Unknown

```
CA 2013-02-12 14:13:11,963 INFO: 'Config Advisor GUI Started'
CA 2013-02-12 14:23:18,579 INFO: 'Switching to FlexPod'
```

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/secure sites**: Config Advisor can be used to triage and diagnose issues with NetApp systems that do not send AutoSupport messages.

1.2 Features in Config Advisor

The features available in Config Advisor 3.2 are as follows:

- Profile-based data collection and configuration checks
- Rich text upgrade message notification
- MPHA status checks
- Stack, shelf, and disk checks
- HA configuration checks
- AutoSupport enablement checks
- Configuration checks for switches and clustered Data ONTAP
- Configuration checks for FlexPod setup
- Secure site data collection and sanitization
- System configuration summary for 7-Mode controllers
- Firmware revision checks
- SAS cabling checks
- At-Risk-Systems checks
- Firmware revision checks
- Flexible reporting options: PDF, MS Word, MS Excel
- AutoSupport call home feature

1.3 Configurations supported by Config Advisor

Config Advisor is a lightweight Windows binary executable (less than 25 MB) that can run on Windows 7 (32-bit and 64-bit) and Windows XP SP3.

Config Advisor supports the FAS (2xxx, 3xxx, and 6xxx), N series, and V-Series storage controllers running Data ONTAP 7.3 and later, and clustered Data ONTAP 8.x and Data ONTAP 8.x operating in 7-Mode.

Note: MetroCluster systems are not supported.

Switch operating systems and configurations

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

Switch model	Switch firmware
Cisco Nexus 5010 and Cisco Nexus 5020	Cisco NX-OS release (Cluster switch) 5.0(2)N1(1)
Cisco Catalyst 2960	Cisco IOS release (Management switch) 12.2(55)SE
NetApp CN1610	Software version 1.0.0.4
NetApp CN1601	Software version 1.0.0.4
Cisco Nexus 5596	Cisco NX-OS release (Cluster switch) 5.2(1)N1(1)

The configurations supported are as follows:

Switch model	Configuration 1	Configuration 2	Configuration 3	Configuration 4	Configuration 5
Cluster switch	Cisco Nexus 5010	Cisco Nexus 5020	NetApp CN1610	NetApp CN1601	Cisco Nexus 5596
Management switch	Cisco Catalyst 2960	Cisco Catalyst 2960	NetApp CN1601	Not applicable	Cisco Catalyst 2960

The hardware configurations supported by Config Advisor for FlexPod setup (a platform jointly developed by Cisco and NetApp) are as follows:

Hardware/Software	Model/Version
NetApp Storage Controller	FAS 32xx
Cisco Switches	Nexus 5548
Cisco Fabric Interconnects	6248UP
Cisco UCS Manager	2.1(1a)

Note: Currently only a subset of the hardware is supported, however Config Advisor can be used with other FlexPod configurations also.

2 Installing, configuring, upgrading, and uninstalling Config Advisor

You can find information about how to download, install, perform initial configuration, uninstall, and upgrade the Config Advisor tool and its dependencies.

2.1 Installing Config Advisor

Steps

1. Download the Config Advisor binary file.
2. You can download the Config Advisor tool from the following links:
   - NetApp and its partners: tech.netapp.com/configadvisor
   - External customers: support.netapp.com/eservice/toolchest
3. Install the tool by completing the steps in the installation wizard.

Note: You should not change the default installation folder.

The default installation folders for Config Advisor 3.2 on different operating systems are as follows:

Default installation folder	Operating system
`C:\Program Files\ConfigAdvisor`	Windows XP SP3 32-bit and Windows 7 SP1 32-bit
`C:\Program Files (x86)\ConfigAdvisor`	Windows 7 SP1 64-bit

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

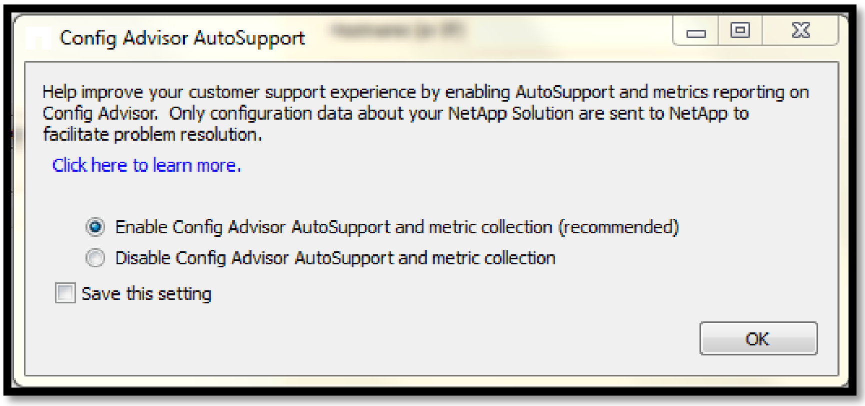
Note: The Data Collector and Sanitizer script is integrated in the tool and will be available in the installation folder as: `C:\Program Files\ConfigAdvisor\secure_datacollector.ps1`

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

2.2 Configuring Config Advisor

Similar to Data 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.

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



Config Advisor AutoSupport

Help improve your customer support experience by enabling AutoSupport and metrics reporting on Config Advisor. Only configuration data about your NetApp Solution are sent to NetApp to facilitate problem resolution.

Click here to learn more.

● Enable Config Advisor AutoSupport and metric collection (recommended)

○ Disable Config Advisor AutoSupport and metric collection

□ Save this setting

Note: Enabling or disabling of usage statistics affects both CA ASUP and the metric upload through FTP.

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

2.3 Upgrading Config Advisor

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 upgrade notification is temporarily unavailable` is displayed in the **Config Advisor Logs** pane.

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 renames the data folder as the latest folder and retains all the contents in the folder.

2.4 Uninstalling Config Advisor

Steps

1. Click **Start** > **Control Panel** > **Programs and Features**.
   On Windows XP, click **Start** > **Control Panel** > **Programs and Features** > **Add/Remove programs**.
2. Right-click **Config Advisor** and click **Uninstall/Change**.
   The confirmation dialog box is displayed.
3. Click **Yes**.
   The uninstallation process starts.

Note: To delete all the data files generated, navigate to the home directory, and delete the `ConfigAdvisorData` folder (applicable only for Windows 7). For example, `C:\Users\user name\ConfigAdvisorData`.

To delete the Data Collector and Sanitizer script, navigate to the folder you stored it in, and delete it.

Alternatively, you can also uninstall Config Advisor by re-running (double-click) the downloaded executable file (for example, `ConfigAdvisor-3.0.0-05042012.1541.exe`).

Note: In this case, the `uninstall.exe` file is not deleted automatically.

3 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 3.2 supports three data collection profiles:

- Data ONTAP 7 and 8 (7-Mode)
- Clustered Data ONTAP
- FlexPod

3.1 Collecting data from a Data ONTAP 7 and 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: AutoSupport (by ASUP Id) refers to AutoSupport IDs from NetApp's AutoSupport data warehouse.

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, Remote LAN Module (RLM), Baseboard Management Controller (BMC), or Alternate Control Path (ACP) are not supported in 7-Mode.

3.1.1 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 list** pane.

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

2. Select the checks to be included.

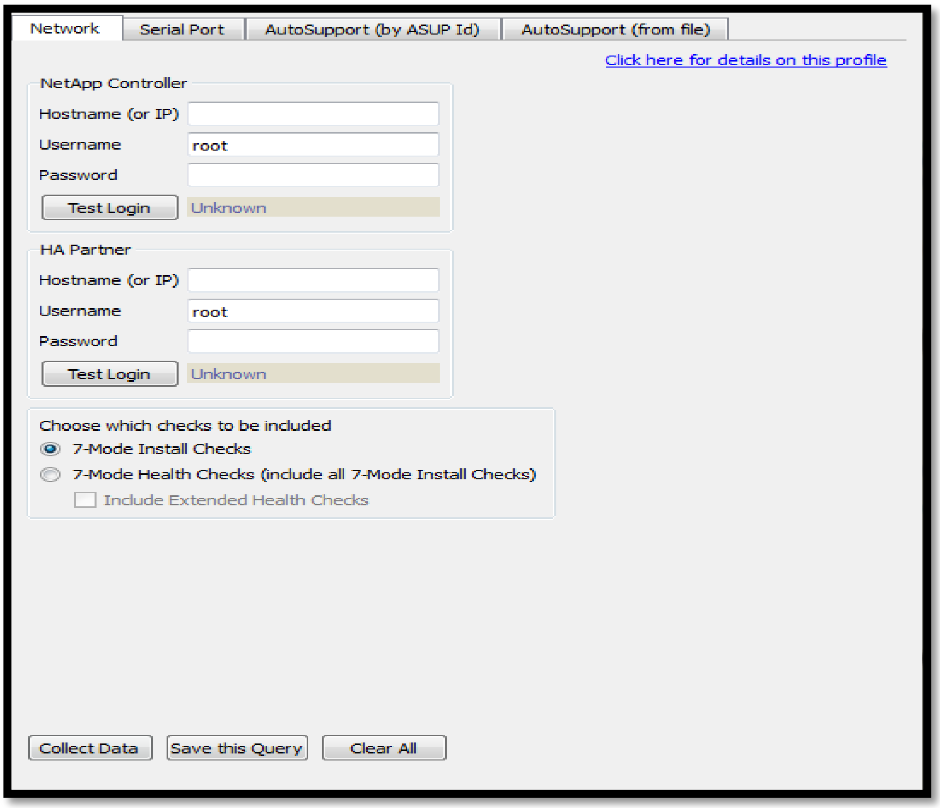
Note: If you select **7-Mode Health Checks (include all 7-Mode Install Checks)**, the **Include Extended Health Checks** check box is enabled. You can select this check box if you want to run additional checks on the system. The extended health checks involve parsing and analyzing `etc/messages`, which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

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



NetApp Controller

Hostname (or IP)

Username root

Password

Unknown

HA Partner

Hostname (or IP)

Username root

Password

Unknown

Choose which checks to be included

● 7-Mode Install Checks

○ 7-Mode Health Checks (include all 7-Mode Install Checks)

□ Include Extended Health Checks

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.

GUI field/ button	Description
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 criteria and not all NetApp best practices or At-Risk-Systems (ARS) criteria.
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.

3.1.2 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 cannot be 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 health 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.
   Alternatively, select the login credentials from the **Default Query Group – query list** pane. For more information, see Saving credentials.
3. Enter the login details.
4. Click **Collect Data** to start data collection.
   The **Results File** dialog box is displayed.
5. Enter a name for the result file or accept the default.
6. Select the **Include Extended Disk Shelf Checks** check box, if you want to run additional checks on the system.

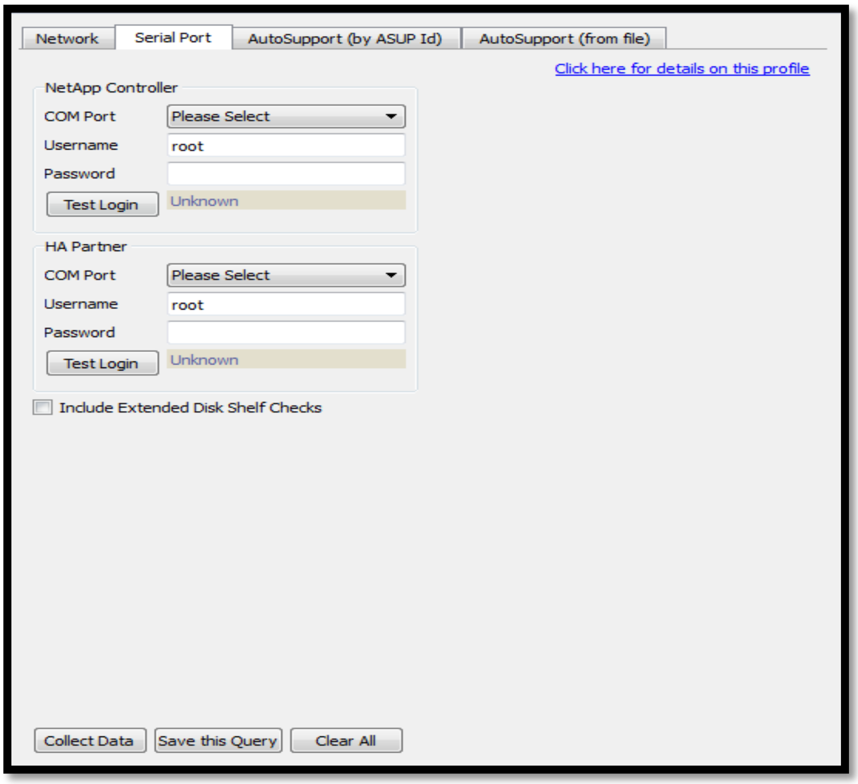
Note: If you select the **Include Extended Health Checks** check box, the `environment status` command is run. This allows Config Advisor to accurately validate the shelf-to-shelf cabling. However, this command might take a long time to run depending on the number of disks connected to the controller.

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

Note: In the **Serial Port** tab, a query can be saved only in **Default Query Group**.

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

The **Serial Port** tab is as shown:



NetApp Controller

COM Port: Please Select

Username: root

Password:

Test Login: Unknown

HA Partner

COM Port: Please Select

Username: root

Password:

Test Login: Unknown

□ Include Extended Disk Shelf Checks

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.

3.1.3 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.

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.

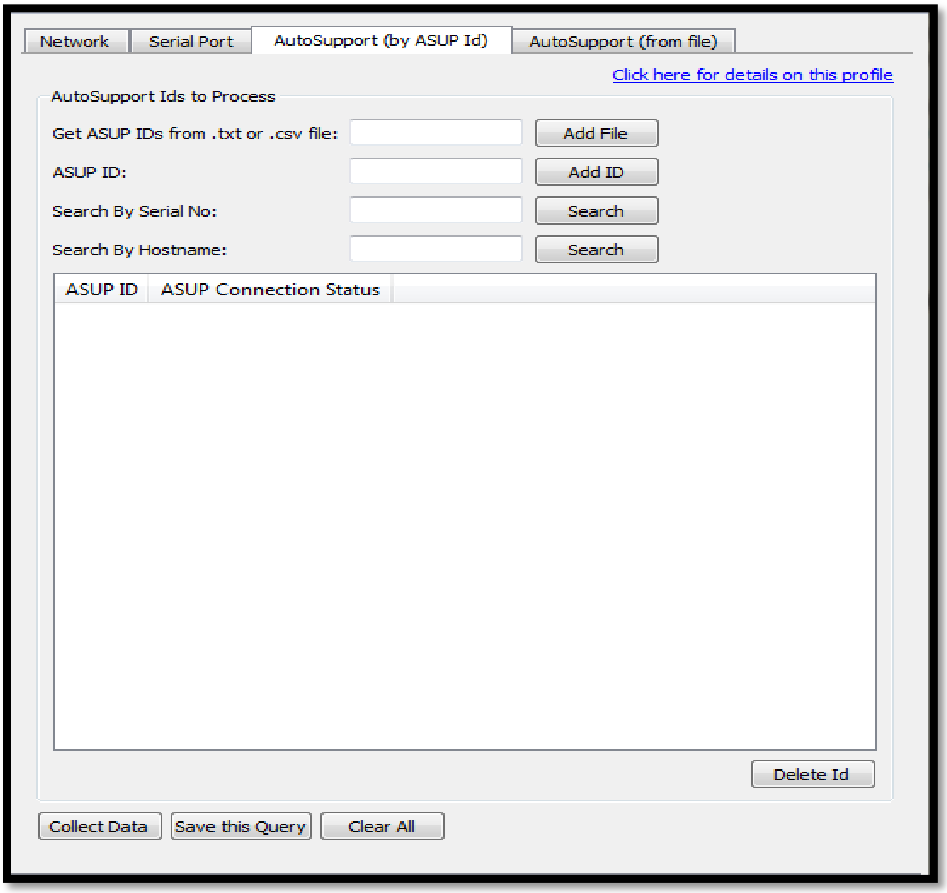
   b. Enter serial number of the controller in the **Search By Serial No** field, and click **Search**.
   c. The Config Advisor ASUP IDs from **Serial No Search** dialog box is displayed. Select the ASUP IDs, and click **Add Selected ASUPs**.

   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. Click **Collect Data** to start the data collection.
   The **Results File** dialog box is displayed.
7. 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.
8. 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's intranet and the AutoSupport data warehouse.

Fields in 7-Mode AutoSupport (by ASUP Id) tab

The fields in the 7-Mode **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.
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.

3.1.4 Collecting data by using the AutoSupport (from file) tab

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

Note: If you save an AutoSupport file from an email client such as Microsoft Outlook, the client might change the formatting of the information in the file. This might result in data collection failure when Config Advisor parses the file.

Steps

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

Note: The AutoSupport file should be a .txt file. AutoSupport files supported by Config Advisor are plain text files that are similar to files described in Collecting data manually. Data ONTAP 8.1 .x returns data without the headers. You have to add the headers manually in Config Advisor format for each command as described in Collecting data manually.

Alternatively, you can select a query from the **query list** 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, and click **Ok.**

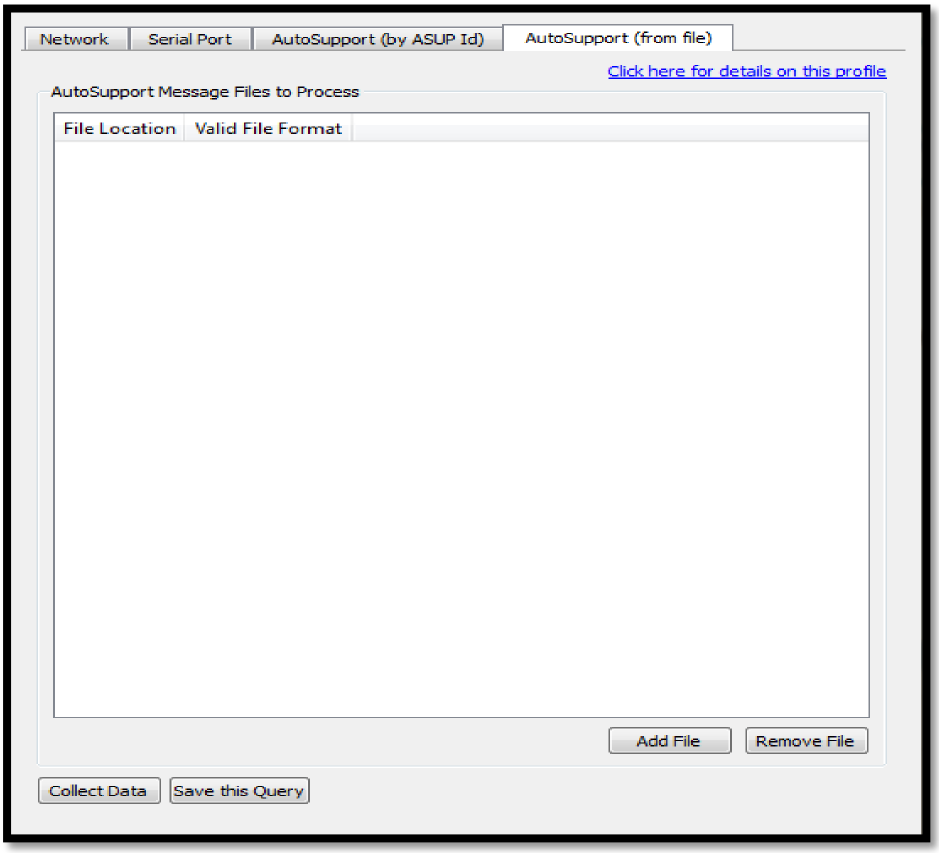
   When the data collection and analysis are complete, the result file is displayed in the **Recent Results** pane.

   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 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.
Save this Query	Saves the file path as a query for later use.

3.1.5 Collecting data by using the batch data collection mode

Data collection in batch mode is performed by grouping credentials in a query group. A query group has one or more query names, enabling you to construct a large batch mode query by using the existing saved credentials.

In batch collection mode, you can collect data from multiple systems by using the credentials that are saved as query groups.

Note: The recommended number of systems in a single batch mode operation is 50 or less to avoid errors caused when data collected exceeds the available physical memory.

The credentials can be saved as query groups from any or all of the following tabs:

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

Note: In batch data collection, credentials from clustered systems or serial port systems are not considered.

Steps

1. Click **Add a Query Group**.
2. Enter a query group name, and click **OK**.
   The name is added in the **query list** pane.
3. Enter the credentials in **Network**, **AutoSupport (by ASUP Id)**, and **AutoSupport (from file)**, 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 list** 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 credentials or queries saved within a query group, select the query group from the **Query Groups** pane and click **Collect from Query Group**.

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

   After the data collection is complete, the results for the queries are saved in a single Config Advisor file. The result file is displayed in the **Recent Results** pane, and the results window is displayed.

Note: The connections to a controller by using a Service Processor, Remote LAN Module (RLM),or Baseboard Management Controller (BMC) are not supported in Data ONTAP operating in 7-Mode.

3.2 Collecting data from clustered Data ONTAP

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

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

- Cisco NX5010/5020/5596
- NetApp CN1610/CN1601

To verify clustered 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.

Note: Config Advisor 3.2 supports data collection only from the Network tab for cluster switches.

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

If the credentials are not entered, the health checks for these switches are not executed. For more information about health checks, see Appendix: Configuration Validations and Health Checks.

3.2.1 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 at least one cluster switch and one cluster node.
   Alternatively, you can select the login credentials from the **Default Query Group – query list** pane.

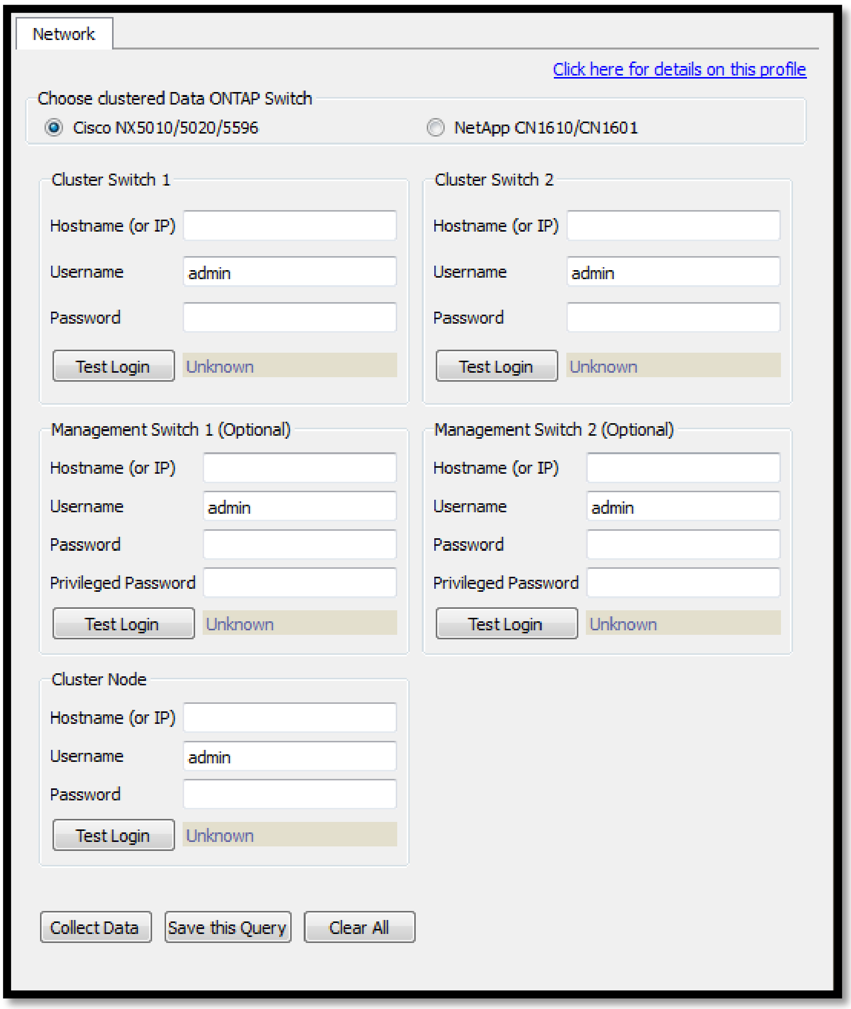
Note: In clustered Data ONTAP, a query can be saved only in **Default Query Group**.

   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 Cisco NX5010/5020/5596 and NetApp CN1610/CN1601 clustered Data ONTAP **Network** tab is as shown:



Network

Click here for details on this profile

Choose clustered Data ONTAP Switch

● Cisco NX5010/5020/5596 ○ NetApp CN1610/CN1601

Cluster Switch 1

Hostname (or IP):

Username: admin

Password:

Test Login: Unknown

Cluster Switch 2

Hostname (or IP):

Username: admin

Password:

Test Login: Unknown

Management Switch 1 (Optional)

Hostname (or IP):

Username: admin

Password:

Privileged Password:

Test Login: Unknown

Management Switch 2 (Optional)

Hostname (or IP):

Username: admin

Password:

Privileged Password:

Test Login: Unknown

Cluster Node

Hostname (or IP):

Username: admin

Password:

Test Login: Unknown

Fields in Cisco NX5010/5020/5596 and NetApp CN1610/CN1601 clustered Data ONTAP Network tab

The fields in Cisco NX5010/5020/5596 and NetApp CN1610/CN1601 clustered Data ONTAP **Network** tab are as follows:

GUI field/GUI button	Description
Hostname (or IP)	Host name or IP address of the controller or 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.

GUI field/GUI button	Description
Test Login	Displays the connection status. • Config Advisor attempts to connect to Cisco NX5010/5020/5596 in the following order: SSH > Telnet. • Config Advisor attempts to connect to NetApp CN1610/NetApp CN1601/Cisco Catalyst 2960 through Telnet. • Config Advisor attempts to connect to management switch through 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 clustered Data ONTAP.
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).

3.3 Collecting data from FlexPod setup

To verify some of the most common configuration errors in standard FlexPod setups, you must collect data from a single Cisco UCS Manager domain (two Cisco Fabric Interconnects), two storage controllers, and two Nexus 5000/5500-series switches. As with all FlexPod setups, the only recommendations are related to the core infrastructure and SAN boot configuration; the hypervisor or any application workloads running on the infrastructure are not checked.

Note: All the FlexPod device (One Cisco UCS, two Nexus Switches, and two Storage Controllers) credentials are mandatory.

These checks are not comprehensive, and absence of failures do not indicate proper configuration of the FlexPod setups.

Config Advisor supports data collection from the controllers using Manage ONTAP Solution, SSH, or Telnet.

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

In the FlexPod profile, based on the FlexPod SAN Boot architecture used, you can choose any one of the following options as shown:

- FCoE to the storage controller
- Classic FCP to the storage controller
- Don't check FCP/FCoE configuration

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

Steps

1. Enter the login details for two NetApp storage system nodes, two Nexus switches, and one Cisco UCS cluster.

Alternatively, you can select the login credentials from the **Default Query Group – query list** pane.

Note: For FlexPod setup, a query can be saved only in **Default Query Group**.

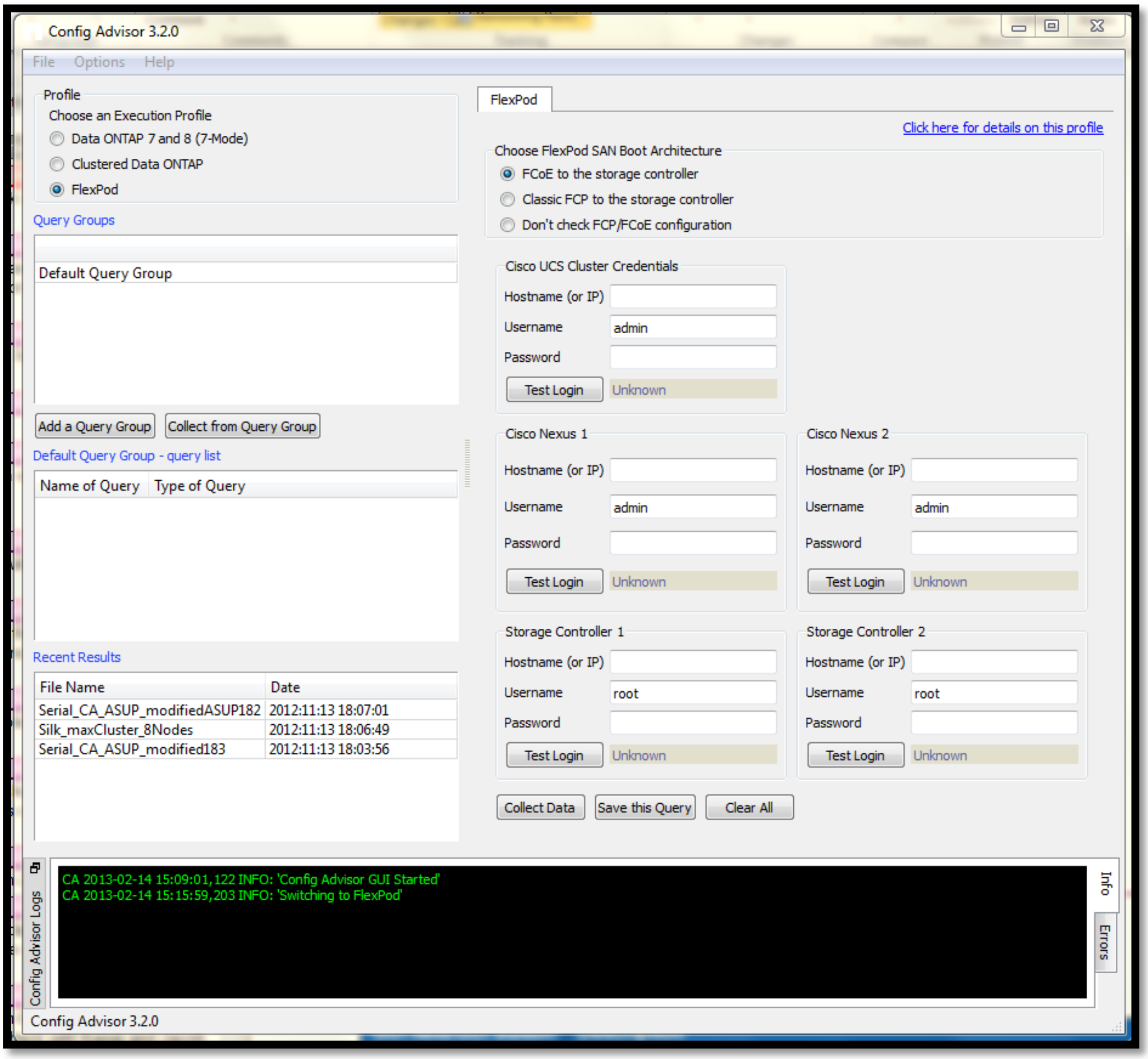
For more information, see Saving credentials.

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, see Recent Results pane.

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

5. Click **Save this Query** to save the credentials as a query.
   For more information, see Saving credentials.

The **FlexPod** profile tab is as shown:



Choose an Execution Profile
○ Data ONTAP 7 and 8 (7-Mode)
○ Clustered Data ONTAP
● FlexPod

Default Query Group

Name of Query	Type of Query

File Name	Date
Serial_CA_ASUP_modifiedASUP182	2012:11:13 18:07:01
Silk_maxCluster_8Nodes	2012:11:13 18:06:49
Serial_CA_ASUP_modified183	2012:11:13 18:03:56

Choose FlexPod SAN Boot Architecture
● FCoE to the storage controller
○ Classic FCP to the storage controller
○ Don't check FCP/FCoE configuration

Cisco UCS Cluster Credentials: Hostname (or IP) / Username admin / Password / Test Login Unknown

Cisco Nexus 1: Hostname (or IP) / Username admin / Password / Test Login Unknown

Cisco Nexus 2: Hostname (or IP) / Username admin / Password / Test Login Unknown

Storage Controller 1: Hostname (or IP) / Username root / Password / Test Login Unknown

Storage Controller 2: Hostname (or IP) / Username root / Password / Test Login Unknown

```
CA 2013-02-14 15:09:01,122 INFO: 'Config Advisor GUI Started'
CA 2013-02-14 15:15:59,203 INFO: 'Switching to FlexPod'
```

Fields in FlexPod profile tab

The fields in FlexPod setup profile tab are as follows:

GUI field/GUI button	Description
Hostname (or IP)	Host name or IP address of the controllers, switches, or UCS cluster.

GUI field/GUI button	Description
Username	User name to access the controllers, switches, or UCS cluster.
Password	Password to access the controller or the controllers, switches, or UCS cluster.
Test Login	Displays the connection status. - Config Advisor attempts to connect using Cisco UCS API for Cisco UCS Cluster in the following order: HTTPS > HTTP. - Config Advisor attempts to connect to Cisco Nexus in the following order: SSH >Telnet. - Config Advisor uses the network fallback mechanism to connect to the cluster node in the following order: Manage ONTAP Solution > 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 FlexPod setup.
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** 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 **Config Advisor Log** also shows log details for Status, Invalid Credentials, and Connection Failure (along with the reasons for failure).

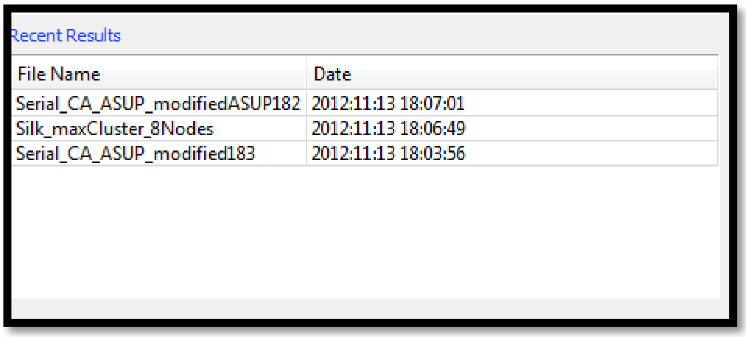
4 Working with results

You can find information about where to find the result files, how to view the 7-Mode, clustered Data ONTAP, and FlexPod 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.

4.1 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.

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



Recent Results

File Name	Date
Serial_CA_ASUP_modifiedASUP182	2012:11:13 18:07:01
Silk_maxCluster_8Nodes	2012:11:13 18:06:49
Serial_CA_ASUP_modified183	2012:11:13 18:03:56

The location of the result files is as follows:

Directory path	Operating system

`C:\Documents and Settings\<windows_login>`
`\ConfigAdvisorData\recent_results`
	Windows XP SP3 32- bit

`C:\Users\<windows_login>`
`\ConfigAdvisorData \recent_results`
	Windows 7 SP1 32-bit and 64-bit

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

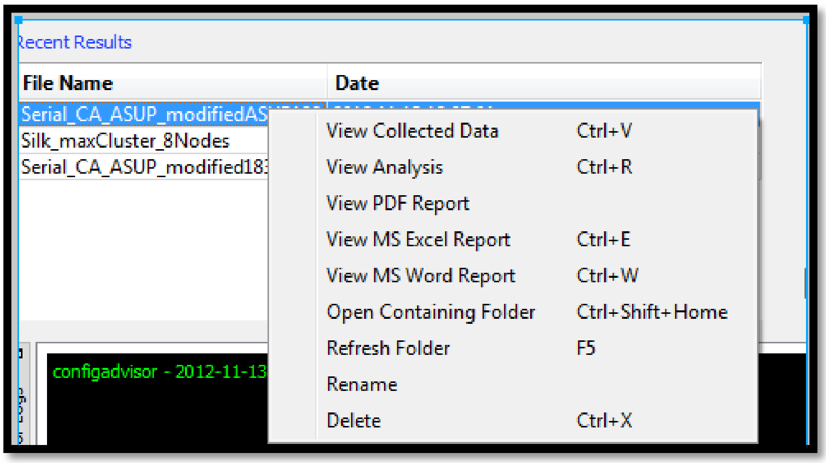
The files in the **Recent Results** pane are sorted in the descending order of their creation dates; starting from the latest file. You can right-click a file name for options. For more information, see Viewing results.

4.2 Viewing results

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

Note: The result files generated using Config Advisor 3.2 are not compatible with previous Config Advisor releases, the files are compatible only with Config Advisor 3.1 and later. However, the results files generated by using the earlier releases of Config Advisor are compatible with Config Advisor 3.2.

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


Recent Results
File Name
Date
Serial_CA_ASUP_modifiedAS
Silk_maxCluster_8Nodes
Serial_CA_ASUP_modified18
View Collected Data Ctrl+V
View Analysis Ctrl+R
View PDF Report
View MS Excel Report Ctrl+E
View MS Word Report Ctrl+W
Open Containing Folder Ctrl+Shift+Home
Refresh Folder F5
Rename
Delete Ctrl+X
configadvisor - 2012-11-13

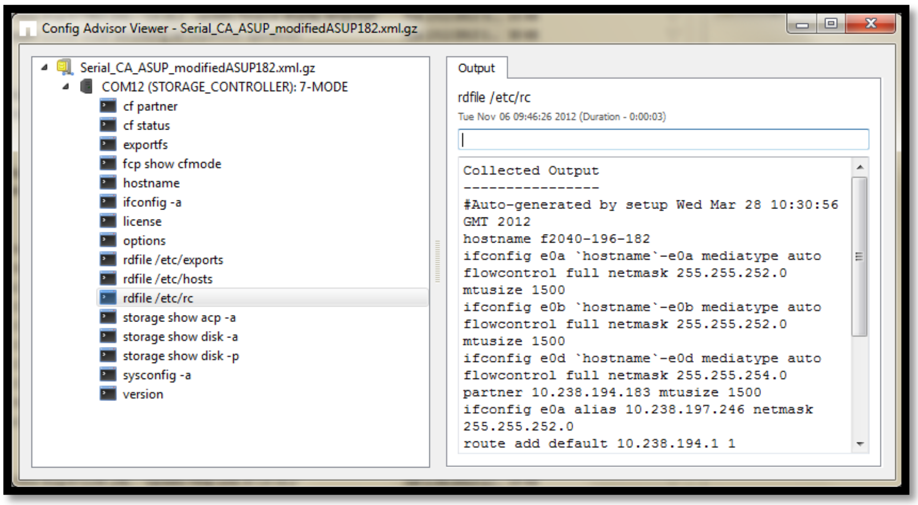
If you right-click a result file in the **Recent Results** pane, you see various options as follows:

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 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 a MS Word report.
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.

4.3 What Config Advisor Viewer does

The **Config Advisor Viewer** window displays the commands that were executed on the target(s) 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**.

The **Config Advisor Viewer** window is as shown:



rdfile /etc/rc

Tue Nov 06 09:46:26 2012 (Duration - 0:00:03)

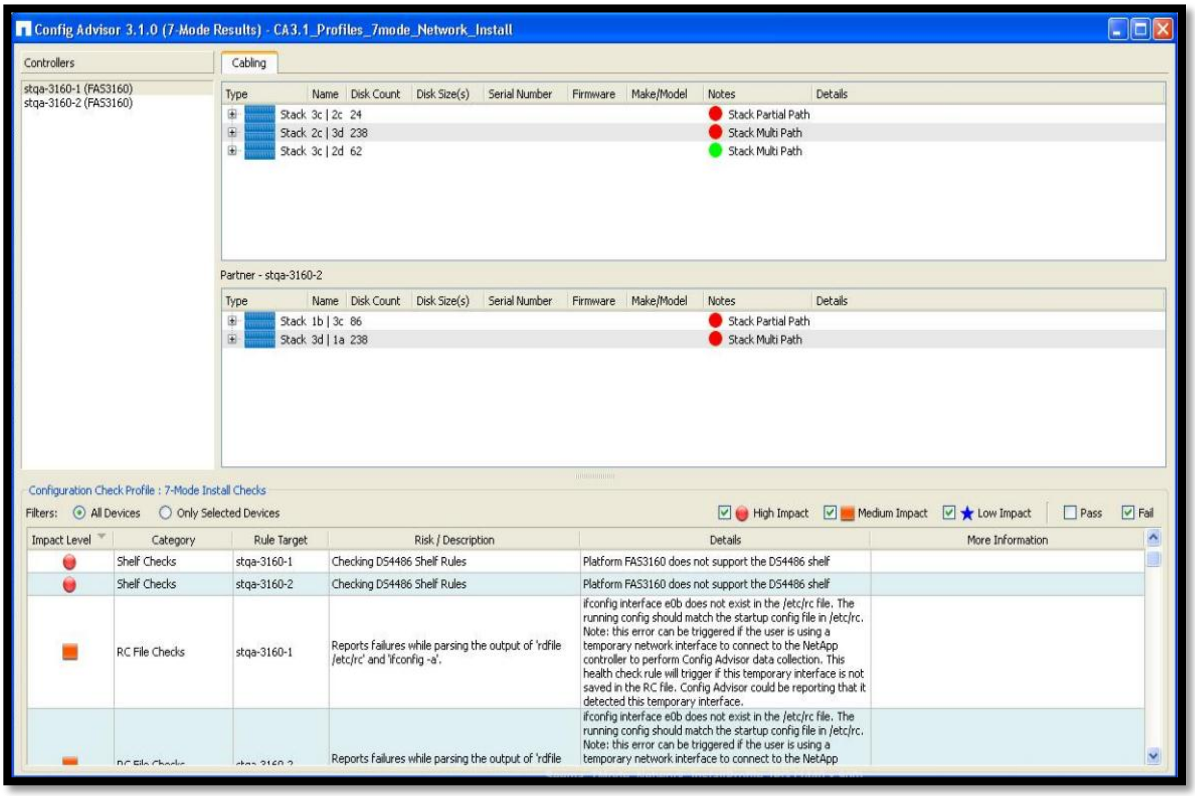
```
Collected Output
----------------
#Auto-generated by setup Wed Mar 28 10:30:56
GMT 2012
hostname f2040-196-182
ifconfig e0a `hostname`-e0a mediatype auto
flowcontrol full netmask 255.255.252.0
mtusize 1500
ifconfig e0b `hostname`-e0b mediatype auto
flowcontrol full netmask 255.255.252.0
mtusize 1500
ifconfig e0d `hostname`-e0d mediatype auto
flowcontrol full netmask 255.255.254.0
partner 10.238.194.183 mtusize 1500
ifconfig e0a alias 10.238.197.246 netmask
255.255.252.0
route add default 10.238.194.1 1
```

4.4 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:



Config Advisor 3.1.0 (7-Mode Results) - CA3.1_Profiles_7mode_Network_Install

Controllers

stqa-3160-1 (FAS3160)
stqa-3160-2 (FAS3160)

Type	Name	Disk Count	Disk Size(s)	Serial Number	Firmware	Make/Model	Notes	Details
Stack	3c | 2c	24					● Stack Partial Path	
Stack	2c | 3d	238					● Stack Multi Path	
Stack	3c | 2d	62					● Stack Multi Path	

Partner - stqa-3160-2

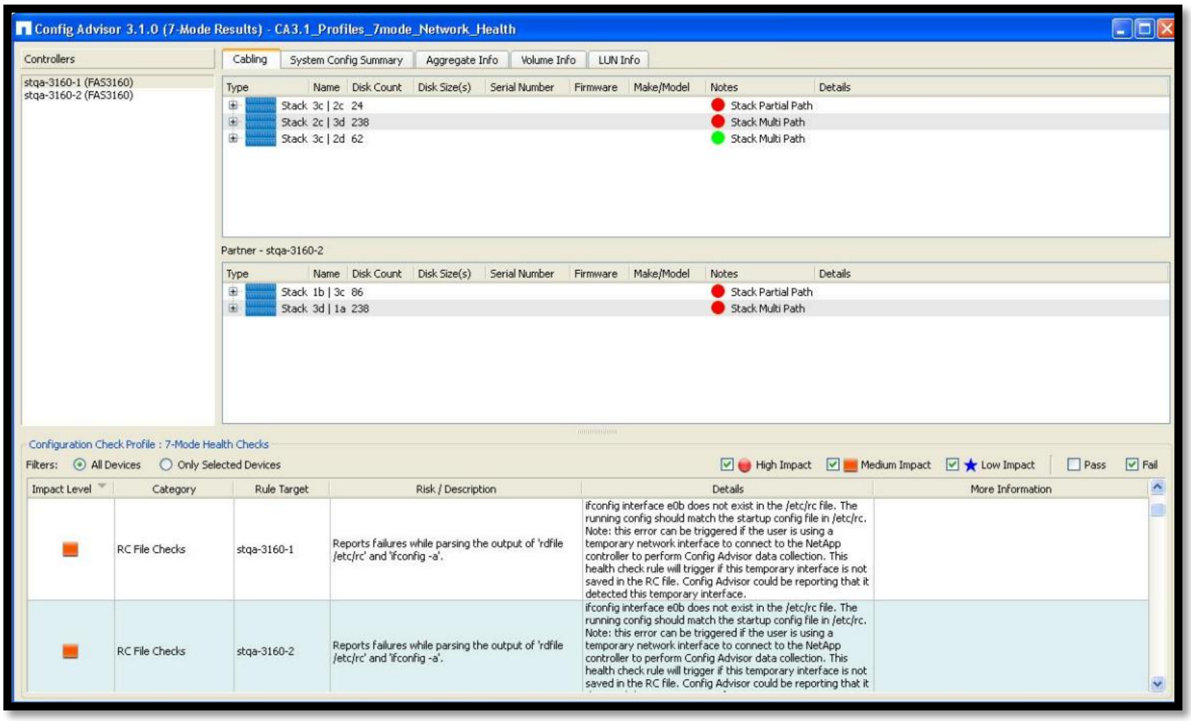
Type	Name	Disk Count	Disk Size(s)	Serial Number	Firmware	Make/Model	Notes	Details
Stack	1b | 3c	86					● Stack Partial Path	
Stack	3d | 1a	238					● Stack Multi Path	

Configuration Check Profile : 7-Mode Install Checks

Filters: ● All Devices ○ Only Selected Devices ☑ ● High Impact ☑ ■ Medium Impact ☑ ★ Low Impact □ Pass ☑ Fail

Impact Level	Category	Rule Target	Risk / Description	Details	More Information
●	Shelf Checks	stqa-3160-1	Checking DS4486 Shelf Rules	Platform FAS3160 does not support the DS4486 shelf	
●	Shelf Checks	stqa-3160-2	Checking DS4486 Shelf Rules	Platform FAS3160 does not support the DS4486 shelf	
■	RC File Checks	stqa-3160-1	Reports failures while parsing the output of 'rdfile /etc/rc' and 'ifconfig -a'.	ifconfig interface e0b does not exist in the /etc/rc file. The running config should match the startup config file in /etc/rc. Note: this error can be triggered if the user is using a temporary network interface to connect to the NetApp controller to perform Config Advisor data collection. This health check rule will trigger if this temporary interface is not saved in the RC file. Config Advisor could be reporting that it detected this temporary interface.	
■	RC File Checks	stqa-3160-2	Reports failures while parsing the output of 'rdfile	ifconfig interface e0b does not exist in the /etc/rc file. The running config should match the startup config file in /etc/rc. Note: this error can be triggered if the user is using a temporary network interface to connect to the NetApp	

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



Config Advisor 3.1.0 (7-Mode Results) - CA3.1_Profiles_7mode_Network_Health

Controllers

stqa-3160-1 (FAS3160)
stqa-3160-2 (FAS3160)

Type	Name	Disk Count	Disk Size(s)	Serial Number	Firmware	Make/Model	Notes	Details
Stack	3c | 2c	24					● Stack Partial Path	
Stack	2c | 3d	238					● Stack Multi Path	
Stack	3c | 2d	62					● Stack Multi Path	

Partner - stqa-3160-2

Type	Name	Disk Count	Disk Size(s)	Serial Number	Firmware	Make/Model	Notes	Details
Stack	1b | 3c	86					● Stack Partial Path	
Stack	3d | 1a	238					● Stack Multi Path	

Configuration Check Profile : 7-Mode Health Checks

Filters: ● All Devices ○ Only Selected Devices ☑ ● High Impact ☑ ■ Medium Impact ☑ ★ Low Impact □ Pass ☑ Fail

Impact Level	Category	Rule Target	Risk / Description	Details	More Information
■	RC File Checks	stqa-3160-1	Reports failures while parsing the output of 'rdfile /etc/rc' and 'ifconfig -a'.	ifconfig interface e0b does not exist in the /etc/rc file. The running config should match the startup config file in /etc/rc. Note: this error can be triggered if the user is using a temporary network interface to connect to the NetApp controller to perform Config Advisor data collection. This health check rule will trigger if this temporary interface is not saved in the RC file. Config Advisor could be reporting that it detected this temporary interface.	
■	RC File Checks	stqa-3160-2	Reports failures while parsing the output of 'rdfile /etc/rc' and 'ifconfig -a'.	ifconfig interface e0b does not exist in the /etc/rc file. The running config should match the startup config file in /etc/rc. Note: this error can be triggered if the user is using a temporary network interface to connect to the NetApp controller to perform Config Advisor data collection. This health check rule will trigger if this temporary interface is not saved in the RC file. Config Advisor could be reporting that it	

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.

4.4.1 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 controller details are displayed in a separate tab.

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.
Firmware	Displays the firmware on the disk.
Make/Model	Displays the model information for the shelf and disk.
Notes	Displays the pathing 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 Name**: Displays the serial number of the controller. **Model**: Displays the controller model (FAS, V-Series, or N-series). **ONTAP version**: Displays the current version of Data ONTAP that is installed on the controller. **Total Raw Capacity (GB)**: Displays the total disk space. **Total Usable Capacity (GB)**: Displays the available disk space. **Total Used Capacity (GB)**: Displays the used disk space. **Installed Software**: Displays all the licensed software on the controller.
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.
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 Disk Drives**: Displays the count of the data disk drives. **# of Parity Drives**: Displays the count of the parity disk drives. **# of Spare Disks**: Displays the count of the spare disk drives.

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.

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.

Field	Description
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.

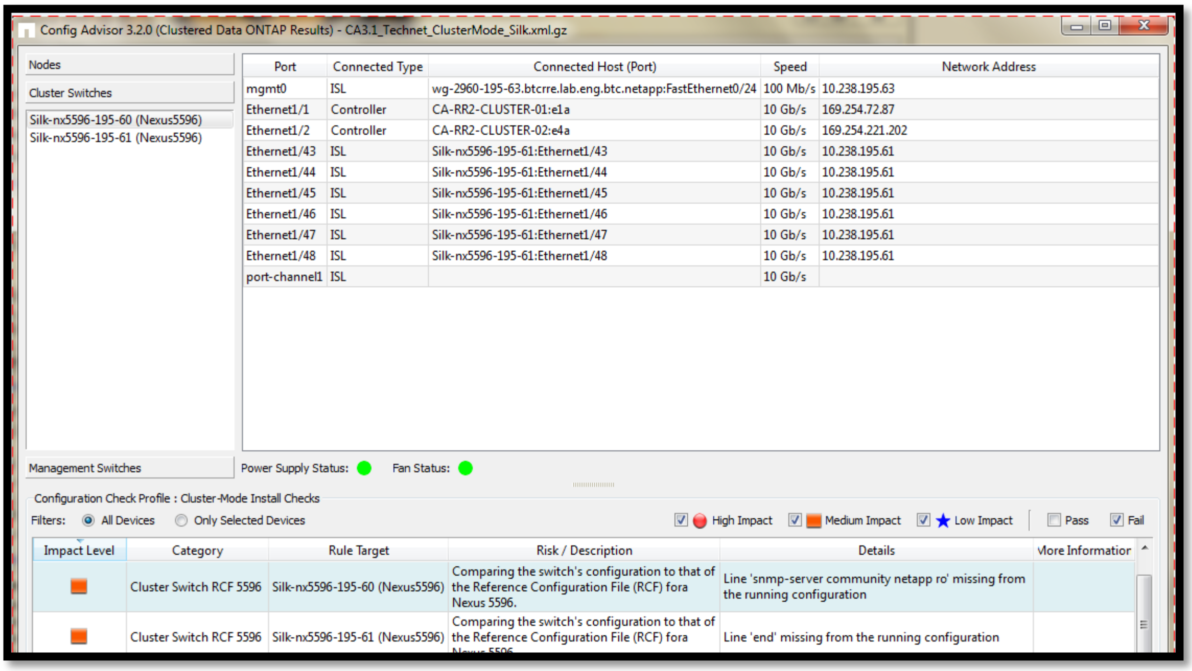
4.5 Viewing clustered Data ONTAP results in Config Advisor

Steps

1. In the **Recent Results** pane, right-click a clustered Data ONTAP results file.
2. Select **View Analysis**.

   The **Config Advisor (Clustered Data ONTAP Results)** window is displayed.

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



Config Advisor 3.2.0 (Clustered Data ONTAP Results) - CA3.1_Technet_ClusterMode_Silk.xml.gz

Silk-nx5596-195-60 (Nexus5596)
Silk-nx5596-195-61 (Nexus5596)

Port	Connected Type	Connected Host (Port)	Speed	Network Address
mgmt0	ISL	wg-2960-195-63.btcrre.lab.eng.btc.netapp:FastEthernet0/24	100 Mb/s	10.238.195.63
Ethernet1/1	Controller	CA-RR2-CLUSTER-01:e1a	10 Gb/s	169.254.72.87
Ethernet1/2	Controller	CA-RR2-CLUSTER-02:e4a	10 Gb/s	169.254.221.202
Ethernet1/43	ISL	Silk-nx5596-195-61:Ethernet1/43	10 Gb/s	10.238.195.61
Ethernet1/44	ISL	Silk-nx5596-195-61:Ethernet1/44	10 Gb/s	10.238.195.61
Ethernet1/45	ISL	Silk-nx5596-195-61:Ethernet1/45	10 Gb/s	10.238.195.61
Ethernet1/46	ISL	Silk-nx5596-195-61:Ethernet1/46	10 Gb/s	10.238.195.61
Ethernet1/47	ISL	Silk-nx5596-195-61:Ethernet1/47	10 Gb/s	10.238.195.61
Ethernet1/48	ISL	Silk-nx5596-195-61:Ethernet1/48	10 Gb/s	10.238.195.61
port-channel1	ISL		10 Gb/s	

Power Supply Status: ● Fan Status: ●

Configuration Check Profile : Cluster-Mode Install Checks

Filters: ● All Devices ○ Only Selected Devices ☑ ● High Impact ☑ 🟧 Medium Impact ☑ ★ Low Impact □ Pass ☑ Fail

Impact Level	Category	Rule Target	Risk / Description	Details	More Information
🟧	Cluster Switch RCF 5596	Silk-nx5596-195-60 (Nexus5596)	Comparing the switch's configuration to that of the Reference Configuration File (RCF) fora Nexus 5596.	Line 'snmp-server community netapp ro' missing from the running configuration	
🟧	Cluster Switch RCF 5596	Silk-nx5596-195-61 (Nexus5596)	Comparing the switch's configuration to that of the Reference Configuration File (RCF) fora Nexus 5596	Line 'end' missing from the running configuration	

The **Config Advisor (Clustered Data 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 Configuration Validations and Health Checks pane.

4.5.1 Nodes pane

The **Nodes** pane displays details of the nodes within a cluster. The details are displayed in the **Network Interfaces** and **Cabling** 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
Logical Interface	Displays the name of the logical interface created on the cluster.
Role	Displays the role of the logical interface (node-management, cluster, or data) created on the cluster.
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).

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.
Firmware	Displays the firmware on the disk.
Make/Model	Display the model information of a shelf and disk.
Notes	Displays the pathing system in a stack, shelf, and disk, in green, orange, or red flags.
Details	Displays information about the shelf or disk that has a red indicator in the **Notes** column.

4.5.2 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.
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.

4.5.3 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.

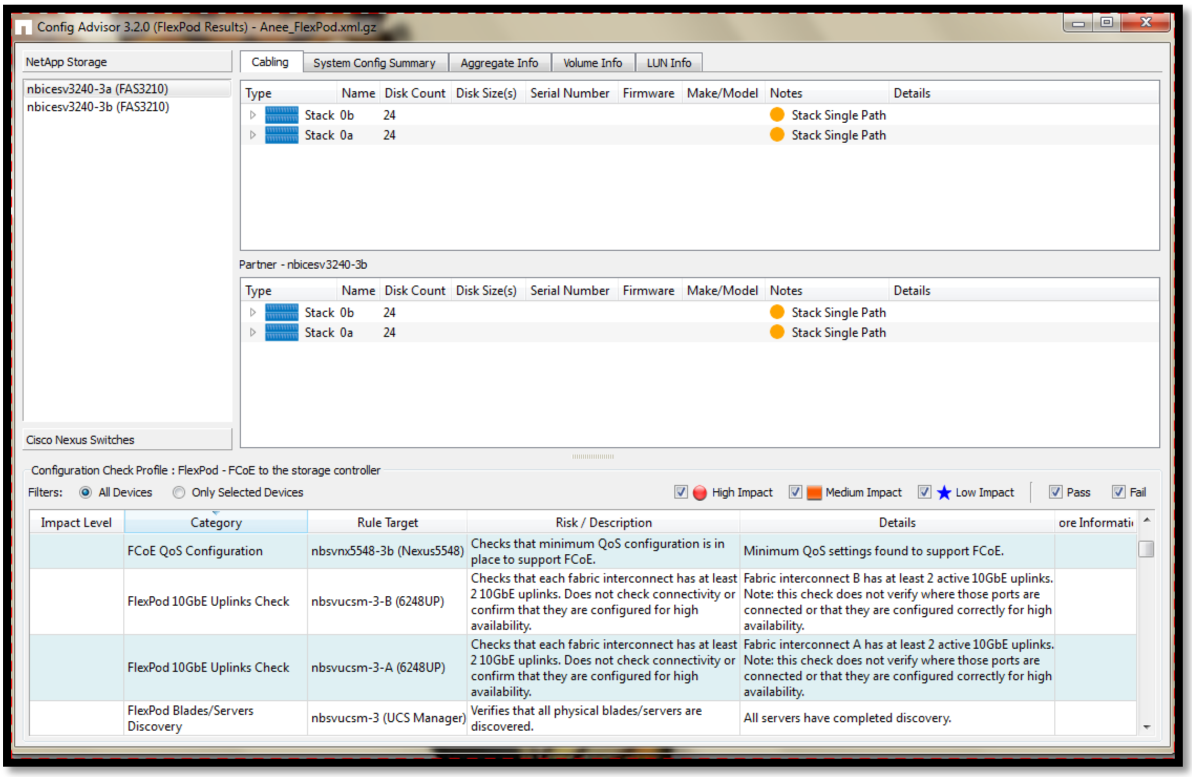
4.6 Viewing FlexPod results in Config Advisor

Steps

1. In the **Recent Results** pane, right-click the required file.
2. Select **View Analysis**.

   The **Config Advisor (FlexPod Results)** window is displayed.

The **Config Advisor 3.2 (FlexPod Results)** window is as shown:



Config Advisor 3.2.0 (FlexPod Results) - Anee_FlexPod.xml.gz

nbicesv3240-3a (FAS3210)
nbicesv3240-3b (FAS3210)

Type	Name	Disk Count	Disk Size(s)	Serial Number	Firmware	Make/Model	Notes	Details
▷	Stack 0b	24					● Stack Single Path	
▷	Stack 0a	24					● Stack Single Path	

Partner - nbicesv3240-3b

Type	Name	Disk Count	Disk Size(s)	Serial Number	Firmware	Make/Model	Notes	Details
▷	Stack 0b	24					● Stack Single Path	
▷	Stack 0a	24					● Stack Single Path	

Configuration Check Profile : FlexPod - FCoE to the storage controller

Filters: ● All Devices ○ Only Selected Devices ☑ ● High Impact ☑ ■ Medium Impact ☑ ★ Low Impact ☑ Pass ☑ Fail

Impact Level	Category	Rule Target	Risk / Description	Details	ore Informati
	FCoE QoS Configuration	nbsvnx5548-3b (Nexus5548)	Checks that minimum QoS configuration is in place to support FCoE.	Minimum QoS settings found to support FCoE.	
	FlexPod 10GbE Uplinks Check	nbsvucsm-3-B (6248UP)	Checks that each fabric interconnect has at least 2 10GbE uplinks. Does not check connectivity or confirm that they are configured for high availability.	Fabric interconnect B has at least 2 active 10GbE uplinks. Note: this check does not verify where those ports are connected or that they are configured correctly for high availability.	
	FlexPod 10GbE Uplinks Check	nbsvucsm-3-A (6248UP)	Checks that each fabric interconnect has at least 2 10GbE uplinks. Does not check connectivity or confirm that they are configured for high availability.	Fabric interconnect A has at least 2 active 10GbE uplinks. Note: this check does not verify where those ports are connected or that they are configured correctly for high availability.	
	FlexPod Blades/Servers Discovery	nbsvucsm-3 (UCS Manager)	Verifies that all physical blades/servers are discovered.	All servers have completed discovery.	

The **Config Advisor 3.2 (FlexPod Results)** window is divided into the following panes:

- **NetApp Storage**, and **Cisco Nexus Switches**: **NetApp Storage** (**Cabling**, **System Config Summary**, **Aggregate Info**, **Volume Info**, **LUN Info** tabs), **Cisco Nexus Switches** (**Network Interfaces** tab).
- **Configuration Validations & Health Checks:** You can use filters to see the rules that were run on the collected data and the results. For more information, see Configuration Validations and Health Checks pane.

4.6.1 Navigation pane

The navigation pane allows the user to navigate between **NetApp Storage** and **Cisco Nexus Switches** of the FlexPod setup. By default, **NetApp Storage** is selected.

NetApp Storage tab

You can view the details of the nodes of the 7-Mode HA pair with the host name (model) of each controller.

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 controller details are displayed in a separate tab.

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.
Firmware	Displays the firmware on the disk.
Make/Model	Displays the model information for the shelf and disk.
Notes	Displays the pathing 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 in 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 Name**: Displays the serial number of the controller. **Model**: Displays the controller model (FAS, V-Series, or N-series). **ONTAP version**: Displays the current version of Data ONTAP that is installed on the controller. **Total Raw Capacity (GB)**: Displays the total disk space. **Total Usable Capacity (GB)**: Displays the available disk space. **Total Used Capacity (GB)**: Displays the used disk space. **Installed Software**: Displays all the licensed software on the controller.
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.
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 Disk Drives**: Displays the count of the data disk drives. **# of Parity Drives**: Displays the count of the parity disk drives. **# of Spare Disks**: Displays the count of the spare disk drives.

Aggregate Info tab

You can view the aggregate information in 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.

Field	Description
Used (GB)	Displays the used space of the aggregate.
Available (GB)	Displays the available 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 both FlexVol and traditional volumes.
Containing Aggregate	Displays the containing aggregate for the volume (if it is a FlexVol volume).
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.

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).

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

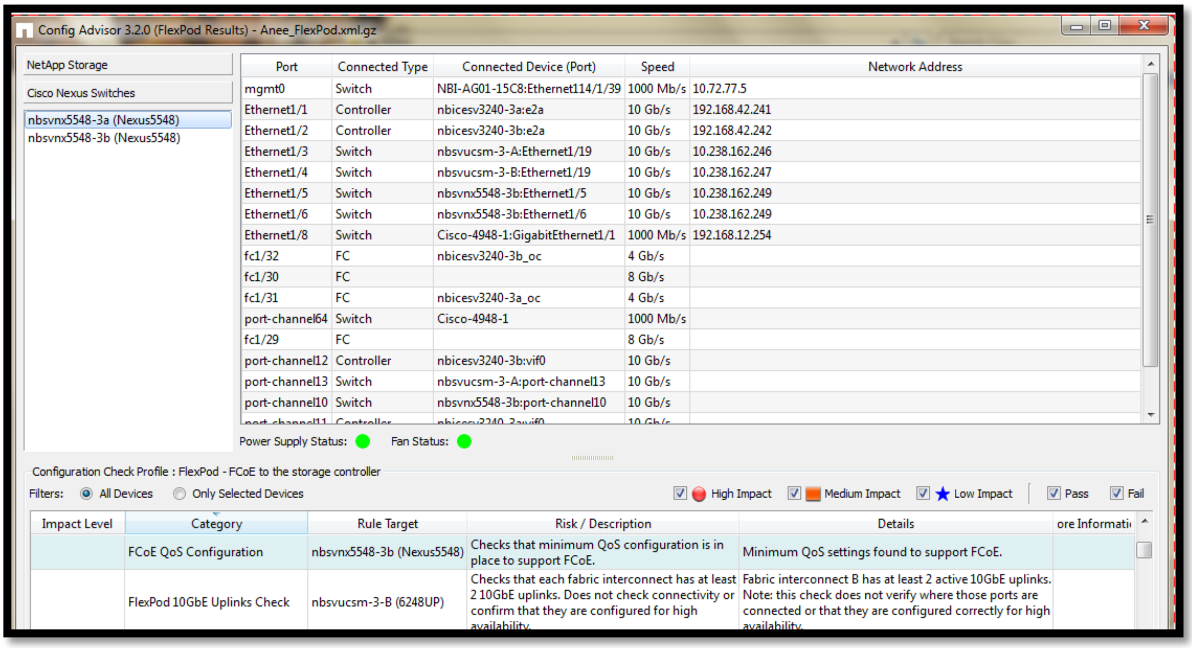
Field	Description
Type	Displays the hierarchy (stack, shelf, or disk).
Name	Displays the name of the stack, shelf, and disk.
Disk Count	Displays the count for a stack and shelf.
Disk Size(s)	Displays the size of the disk.
Serial Number	Displays the serial number of the disk.
Firmware	Displays the firmware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

Field	Description
Make/Model	Display the model information of a shelf and disk.
Notes	Displays the pathing system in a stack, shelf, and disk, in green, orange, or red flags.
Details	Displays information about the shelf or disk that has a red indicator in the **Notes** column.

Cisco Nexus Switches tab

You can view the details of a switch by selecting a switch from the **Cisco Nexus Switches** tab.

The **Config Advisor 3.2 (FlexPod Results)** window for Cisco Nexus Switches is as shown:



Config Advisor 3.2.0 (FlexPod Results) - Anee_FlexPod.xml.gz

NetApp Storage

Cisco Nexus Switches

nbsvnx5548-3a (Nexus5548)
nbsvnx5548-3b (Nexus5548)

Port	Connected Type	Connected Device (Port)	Speed	Network Address
mgmt0	Switch	NBI-AG01-15C8:Ethernet114/1/39	1000 Mb/s	10.72.77.5
Ethernet1/1	Controller	nbicesv3240-3a:e2a	10 Gb/s	192.168.42.241
Ethernet1/2	Controller	nbicesv3240-3b:e2a	10 Gb/s	192.168.42.242
Ethernet1/3	Switch	nbsvucsm-3-A:Ethernet1/19	10 Gb/s	10.238.162.246
Ethernet1/4	Switch	nbsvucsm-3-B:Ethernet1/19	10 Gb/s	10.238.162.247
Ethernet1/5	Switch	nbsvnx5548-3b:Ethernet1/5	10 Gb/s	10.238.162.249
Ethernet1/6	Switch	nbsvnx5548-3b:Ethernet1/6	10 Gb/s	10.238.162.249
Ethernet1/8	Switch	Cisco-4948-1:GigabitEthernet1/1	1000 Mb/s	192.168.12.254
fc1/32	FC	nbicesv3240-3b_oc	4 Gb/s	
fc1/30	FC		8 Gb/s	
fc1/31	FC	nbicesv3240-3a_oc	4 Gb/s	
port-channel64	Switch	Cisco-4948-1	1000 Mb/s	
fc1/29	FC		8 Gb/s	
port-channel12	Controller	nbicesv3240-3b:vif0	10 Gb/s	
port-channel13	Switch	nbsvucsm-3-A:port-channel13	10 Gb/s	
port-channel10	Switch	nbsvnx5548-3b:port-channel10	10 Gb/s	
port-channel11	Controller	nbicesv3240-3a:vif0	10 Gb/s	

Power Supply Status: ● Fan Status: ●

Configuration Check Profile : FlexPod - FCoE to the storage controller

Filters: ● All Devices ○ Only Selected Devices ☑ ● High Impact ☑ ■ Medium Impact ☑ ★ Low Impact ☑ Pass ☑ Fail

Impact Level	Category	Rule Target	Risk / Description	Details	ore Informati
	FCoE QoS Configuration	nbsvnx5548-3b (Nexus5548)	Checks that minimum QoS configuration is in place to support FCoE.	Minimum QoS settings found to support FCoE.	
	FlexPod 10GbE Uplinks Check	nbsvucsm-3-B (6248UP)	Checks that each fabric interconnect has at least 2 10GbE uplinks. Does not check connectivity or confirm that they are configured for high availability.	Fabric interconnect B has at least 2 active 10GbE uplinks. Note: this check does not verify where those ports are connected or that they are configured correctly for high availability.	

The fields in the **Cisco Nexus Switches** 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.
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.

4.7 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, Clustered Data ONTAP Results, FlexPod 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.
Status	Displays the status of the risk.
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.
🔴	Indicates a high level of risk that might lead to a service outage. Corrective action should be taken immediately.
🟧	Indicates a medium level of risk that might affect normal operations of the system or place the system in a degraded state. Corrective action should be taken.
★	Displays a low level of risk. Corrective action must be taken to comply with NetApp's recommended best practices.
Pass	Displays the rules that passed the configuration checks.
Fail	Displays the rules that failed the configuration checks.

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

4.8 Generating a PDF report

You can generate a PDF report containing the 7-Mode results, clustered Data ONTAP results, or FlexPod results. 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.

Steps

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

   A PDF file is displayed with the 7-Mode results, clustered Data ONTAP results, or FlexPod results with the selected profile.

Note: The reports are saved in the following location: `~\ConfigAdvisorData\pdf_files`

4.9 Generating an MS Excel report

You can generate an MS Excel report containing the 7-Mode results.

Steps

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 7-Mode results with the selected profile.

Note: The reports are saved in the following location: `~\ConfigAdvisorData\excel_files`

Excel reports are not supported in clustered Data ONTAP.

4.10 Generating a MS Word report

You can generate a MS Word report containing the 7-Mode results.

Steps

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 7-Mode results with the selected profile.

Note: The reports are saved in the following location: `~\ConfigAdvisorData\doc_files`

Word reports are not supported in clustered Data ONTAP.

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.

5 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 `.json` extension.

The location of the files is as follows:

Directory path	Operating system
`C:\Documents and Settings\<windows_login>\ConfigAdvisorData`	Windows XP SP3 32-bit
`C:\Users\<windows_login>\ConfigAdvisorData`	Windows 7 SP1 32-bit and 64-bit

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

5.1 Saving credentials

Steps

1. Enter the credentials in the tabs (Network, AutoSupport (by ASUP Id), and AutoSupport (from file)).
2. You can save the credentials that you enter in the Hostname or IP Address, Username, and Password fields.

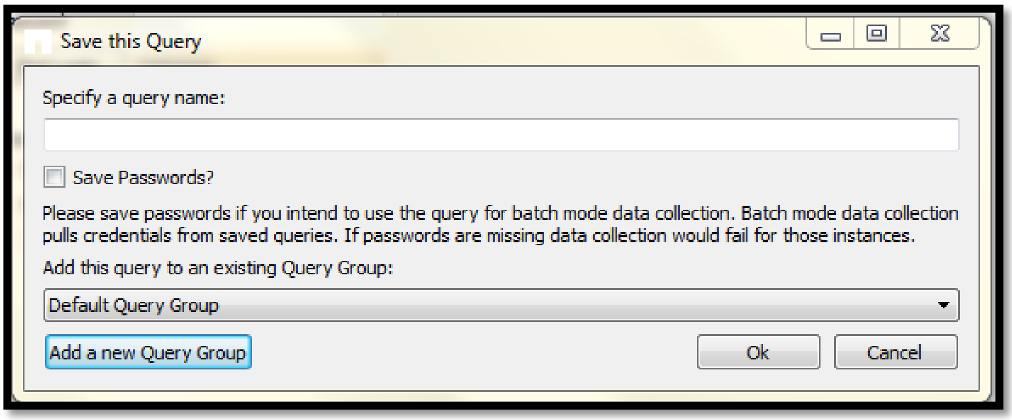
Note: A JavaScript Object Notation (JSON) file is created to save the credentials, and the file is located in `$HOME\ ConfigAdvisorData\ Default Query Group.json`.

3. Click **Save this Query** in each tab.

Note: For data collection in clustered Data ONTAP and by using the **Serial Port** tab in 7-Mode, and FlexPod setup, the query is saved only into the default query group.

4. Enter a name for the query in the **Specify a query name** field.
5. Select the **Save Passwords?** check box displayed in **Network** tab, if you want to save passwords, and click **Ok**.
   The password field has a simple encryption to prevent a casual observer from reading the password.
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:



Save this Query

Specify a query name:

□ Save Passwords?

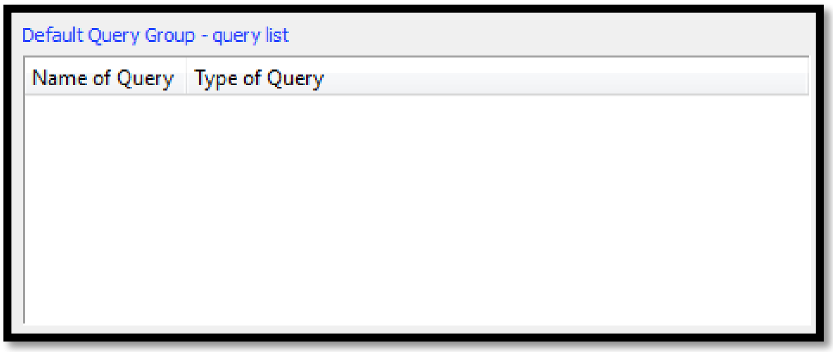
Please save passwords if you intend to use the query for batch mode data collection. Batch mode data collection pulls credentials from saved queries. If passwords are missing data collection would fail for those instances.

Add this query to an existing Query Group:

Default Query Group

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 list** pane.

The **query list** pane is as shown:



The fields in the **query list** pane are as follows:

Field	Description
Name of Query	Displays the name of the saved query.
Type of Query	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.

5.2 Saving a query

Steps

1. Click **Save this Query** to save the login credentials as a query.
2. Enter a query name and click **Ok**.

   For more information, see Saving credentials.
3. Select **Save Passwords?**, if you want to save passwords, and click **Ok**.

   The password field has a simple encryption to prevent a casual observer from reading the password.

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

The tasks that you can perform on a saved query are as follows:

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 renamed.
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.

6 Setting Preferences in Config Advisor

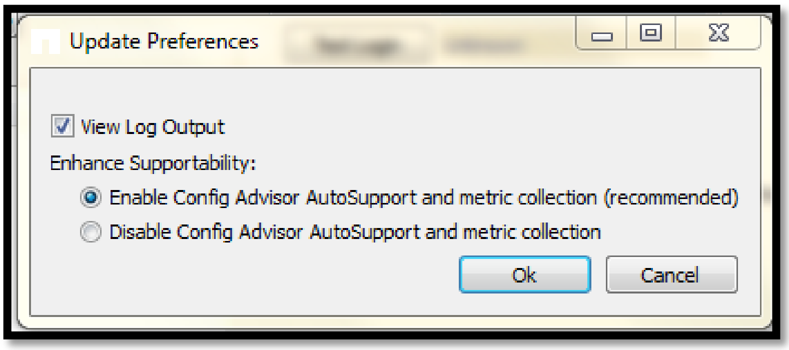
You can find information about FTP metrics, and Config Advisor ASUP, and how to change the initial settings to enable or disable these.

6.1 Enabling Config Advisor AutoSupport

You can enable a Config Advisor AutoSupport message from the host running Config Advisor by clicking **Options > Preferences > Enable Config Advisor AutoSupport and metric collection (recommended)**. If you select this option in the **Update Preferences** dialog box, Config Advisor will send a Config Advisor AutoSupport message after every data collection.

Note: If Config Advisor AutoSupport is enabled immediately after data collection from the Network or Serial tab (7-Mode or clustered Data ONTAP), a Config Advisor ASUP file for the collected results is created in the `$HOME\ConfigAdvisorData\asup_files` folder. This file is posted to NetApp ASUP infrastructure. If the post is successful, then the file is deleted. If not, then on consecutive Config Advisor launches, the tool attempts to post the file.
If Config Advisor ASUP is disabled, then none of the collected data will be uploaded to NetApp.

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



Update Preferences

☑ View Log Output

Enhance Supportability:

● Enable Config Advisor AutoSupport and metric collection (recommended)

○ Disable Config Advisor AutoSupport and metric collection

6.1.1 What Config Advisor AutoSupport is

Config Advisor AutoSupport (ASUP) is similar to Data ONTAP ASUP. Config Advisor sends its collected data back to NetApp over HTTPS, where the content is stored in NetApp's 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, NetApp switches, and FlexPod setups.

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 clustered Data ONTAP also.

6.2 What FTP Metrics are

FTP metrics contain usage and rules execution results information. FTP metrics are sent back to NetApp Technical Support periodically. FTP metrics are used for product improvement and return on investment (ROI) analysis.

The FTP metrics sent to NetApp Technical Support are as follows:

- Number of disks
- Pathing issues found
- Number of shelves
- Disk, shelf, and stack count
- Storage system configuration type, model, and serial number
- Data ONTAP version and model
- Time taken for data collection, date, and session ID
- Profile of the health checks executed on the system

Note: Login name, company name, email address, and user type are not sent as part of FTP metrics.

FTP Metrics for 7-Mode

For a 7-Mode results file, all the controllers within the file share a session ID. Each controller has a separate FTP file.

FTP Metrics for clustered Data ONTAP

For a clustered Data ONTAP results file, separate files are sent for individual nodes within the cluster. All the files within the cluster share a session ID. One node within the cluster sends metrics related to the switches in addition to its own metrics.

FTP Metrics for FlexPod setup

For FlexPod results file, separate files are sent for each controller. One of the controllers sends metrics related to Nexus switches, Cisco Fabric Interconnects, and Cisco UCS Manager.

Note: FlexPod UCS, Cisco Fabric Interconnects, and Nexus Switch details are not sent through a FTP message. Only the trigger codes of the FlexPod setup are sent along with one of the nodes in the HA pair.

Note: If the FTP file is not sent, it is saved in the `ConfigAdvisorData\ftp_files` folder. When Config Advisor is restarted, it attempts to send the FTP files. The files are deleted after they are sent.

6.2.1 Sample of an FTP Metrics file

```
<?xml version="1.0" ?>
<configadvisor>
    <reference>
        <captureInformation captureTimer="114" capturedate="20120315102843"
sessionId="2012031915461790797" capturemethod="" salesorder=""/>
        <userInfo Company="" Email="" Name="Anonymous" UserType=""/>
        <creator name="Config Advisor" platform="Windows" version="3.0.0"/>
    </reference>
    <summary diskCount="430" resultsCode="101000" shelfCount="12" stackCount="8"
sysconfigMP="Multi-Path HA"/>
    <controller model="V6280" serialnumber="8000022761"
ontapversion="RrollingrockN_120307_2045" ontapmode="7-mode">
      <metrics>
           <code metric="720" subcode="3021"></code>
           <code metric="720" subcode="3022"></code>
           <code metric="720" subcode="3025"></code>
           <code metric="750" subcode="384218"></code>
           <code metric="750" subcode="384218"></code>
           <code metric="750" subcode="384218"></code>
           <code metric="750" subcode="384218"></code>
           <code metric="750" subcode="460445"></code>
           <code metric="750" subcode="460445"></code>
           <code metric="750" subcode="460445"></code>
           <code metric="730" subcode="4001"></code>
           <code metric="730" subcode="4002"></code>
      </metrics>
    </controller>
</configadvisor>
```

6.3 Enabling or disabling Config Advisor Logs pane

Steps

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

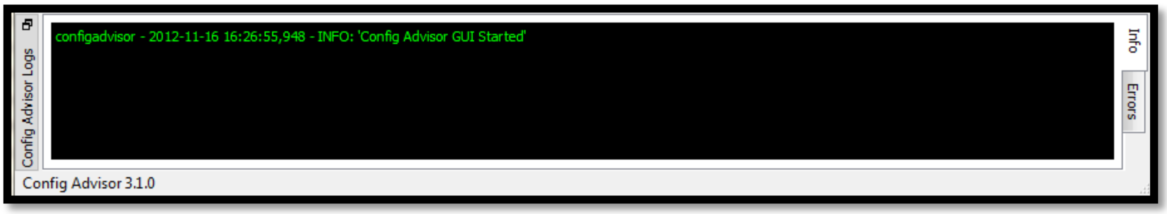
6.3.1 What Config Advisor Logs pane is

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:



```
configadvisor - 2012-11-16 16:26:55,948 - INFO: 'Config Advisor GUI Started'
```

7 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.

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.

8 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 precollected by using the Data Collector and Sanitizer script.

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

Note: In secure sites, you must disable usage metrics manually from **Preferences.** For more information, see Setting Preferences in Config Advisor .

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.

8.1 What Data Collector and Sanitizer script is

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

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

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

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

```
options httpd.admin.enable

options httpd.admin.ssl.enable

options httpd.enable

options ssl.enable
```

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

8.2 Prerequisites for using the Data Collector and Sanitizer script

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

- PowerShell 2.0 or later
  For information about installing PowerShell 2.0, see Installing PowerShell 2.0.
- Data ONTAP PowerShell toolkit 1.5 or later
  For more information, see Installing Data ONTAP PowerShell toolkit 2.0.

8.2.1 Installing PowerShell 2.0

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

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

You can install Windows Management Framework from http://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.

8.2.2 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 http://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 https://communities.netapp.com/community/products_and_solutions/microsoft/powershell.

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

To download samples of PowerShell code, you must log in to the NetApp Support Site.

To only view the code samples, you can access the **Communities** (https://communities.netapp.com) and **Forums** (http://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.

8.3 Running the script

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

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

Before you begin

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

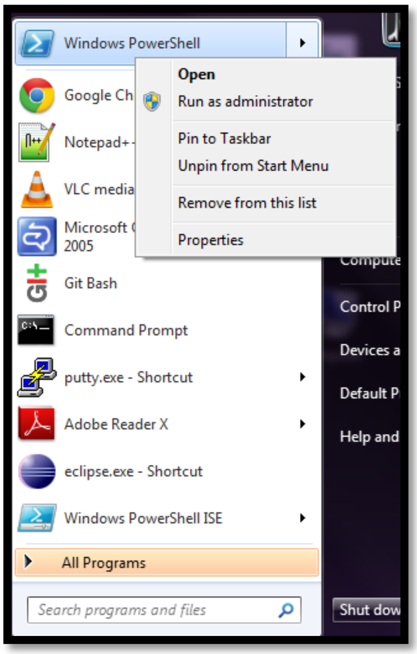
Additional information

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

The current PowerShell execution policy can be changed by running the `Set-ExcecutionPolicy` 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.

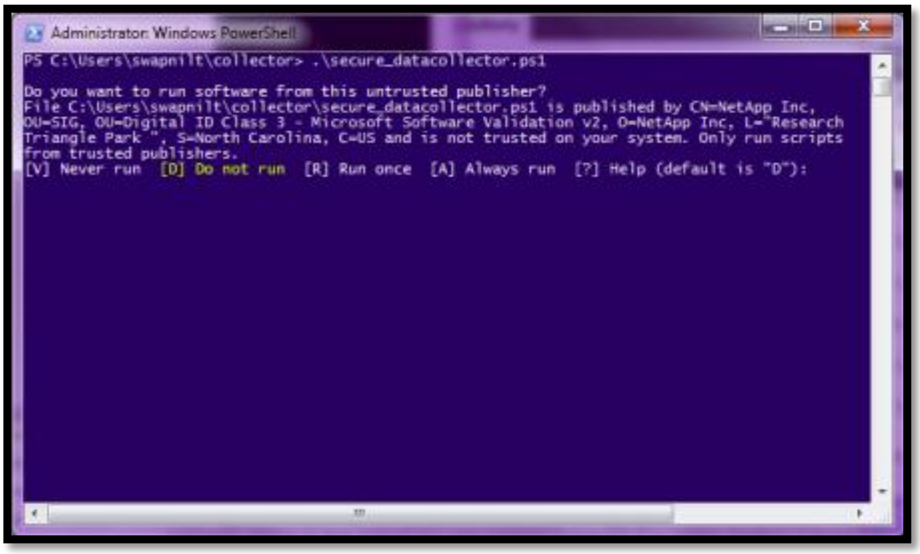
   Alternatively, you can run the command in the Windows command prompt window.

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:



```
PS C:\Users\swapnilt\collector> .\secure_datacollector.ps1

Do you want to run software from this untrusted publisher?
File C:\Users\swapnilt\collector\secure_datacollector.ps1 is published by CN=NetApp Inc,
OU=SIG, OU=Digital ID Class 3 - Microsoft Software Validation v2, O=NetApp Inc, L="Research
Triangle Park ", S=North Carolina, C=US and is not trusted on your system. Only run scripts
from trusted publishers.
[V] Never run  [D] Do not run  [R] Run once  [A] Always run  [?] Help (default is "D"):
```

8.4 Data collection methods for secure sites

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

1. Collecting data using the Data Collector and Sanitizer script

   In this method, you can collect data from single or multiple controllers by using one of the following methods:

   - Interactive data collection
   - Batch-mode data collection
   - Command-line argument
2. Collecting data manually

8.4.1 Interactive data collection method

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

Steps

1. Launch PowerShell.
2. Navigate to the directory where the script is located.

   For example, if you have stored the script in the C drive, then enter `cd c:\`.
3. Invoke the Data Collector and Sanitizer script by entering `.\secure_datacollector.ps1`, and press **Enter**.
4. Based on your requirement, select either one of the options, and press **Enter**:
   1. **Collect data unfiltered**
      - If you enter **1**, the following message is displayed:

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

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

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

2. **Collect data and filter sensitive data using mapped names and create a mapping file**

- If you enter **2**, the script displays all the data items that can be filtered.
- Enter the filtering level. The following message is displayed:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.4.2 Batch-mode data collection method

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

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

Example of a CSV file:

```
10.238.194.138, root, netapp123

fas-2040-32, root,netapp124

10.45.91.152, root, Admin123
```

Steps

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

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

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

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].
```

- 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`

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.

8.4.3 Command-line argument method

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

Steps

1. Launch PowerShell.
2. Navigate to the directory where the script is located.
3. Invoke the Data Collector and Sanitizer script along with the command-line argument, and press **Enter**.
   The script requests for more information or starts collecting data based on the command-line argument that you enter.

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

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

Examples of command-line arguments

Example 1

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

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

Example 2

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

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

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

Parameters in the Data Collector and Sanitizer script

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

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

8.4.4 Collecting data manually

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

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

AutoSupport section name mappings

The corresponding AutoSupport sections for ONTAP commands are:

Data ONTAP 7-Mode commands	AutoSupport names
Version	===== VERSION =====
sysconfig -a	===== SYSCONFIG-A =====
syconfig -r	===== SYSCONFIG-R =====
fcstat device_map	===== FC-DEVICE-MAP =====
storage show disk -a	===== STORAGE-DISK =====
storage show disk -p	===== STORAGE-DISK-P =====
rdfile /etc/rc	===== RC =====
rdfile /etc/hosts	===== HOSTS =====
rdfile /etc/exports	===== EXPORTS =====
Exportfs	===== EXPORTFS =====
License	===== SOFTWARE-LICENSES =====
cf status	===== CSTATUS =====

Data ONTAP 7-Mode commands	AutoSupport names
`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 =====`
`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 table above, without any extra spaces.

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

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

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

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

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

Aggregate 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.

8.5 Filtering and mapping

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

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

Data filtering Items

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

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

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

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

For InfiniBand: LID, Remote LID and GUID

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

8.5.1 Collecting and filtering data

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

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

Result file name for IP address filtering

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

Input credential	Output file format
Hostname	<time_stamp>_Mapped-Hostname.txt
FQDN	<time_stamp>_ Mapped_FQDN.txt

Result file name for hostname 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

8.5.2 Filtering precollected data

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

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

Steps

1. Launch PowerShell.
2. Navigate to the directory where the script is located.

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

   The `Please enter the output folder location:` message is displayed.
4. Enter the output folder path where the precollected data file exists.

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

Additional information

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

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

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

	Original name	Mapped name	Volume type
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).

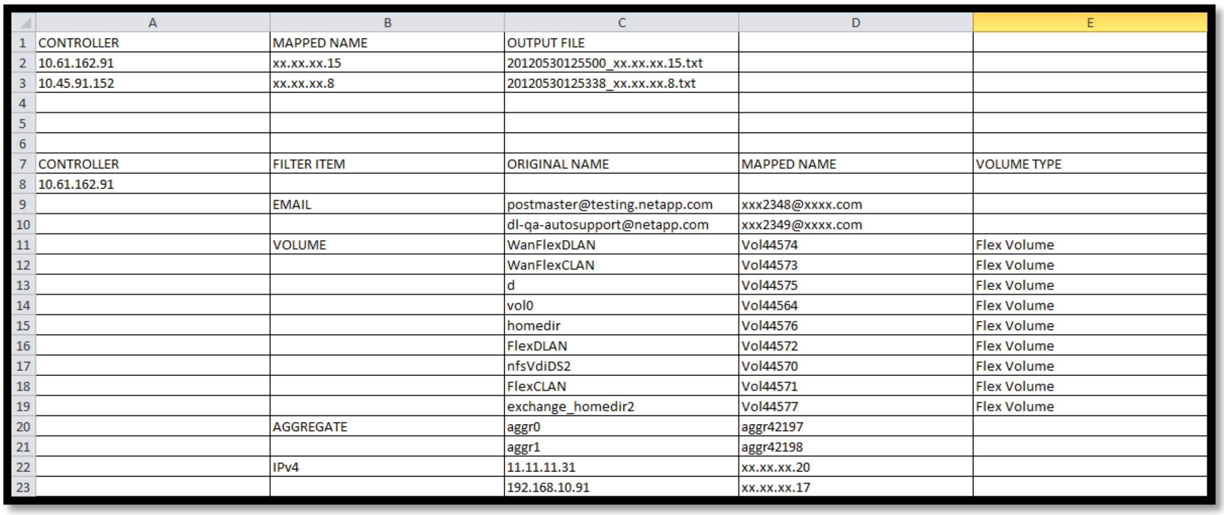
If the Domain Naming Service (DNS) entered is an IP address, then as a part of IP address filtering, this IP address also gets filtered.

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	

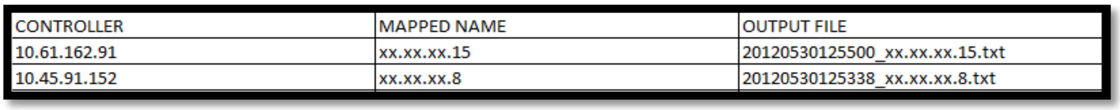
The filtering of volume names, aggregate names, and all items (filter level n) is aborted if the command output of `vol status -v` is absent in the result file. In case of incomplete command output, the filtered data will be incorrect.

(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 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

8.6 Analyzing filtered data file

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

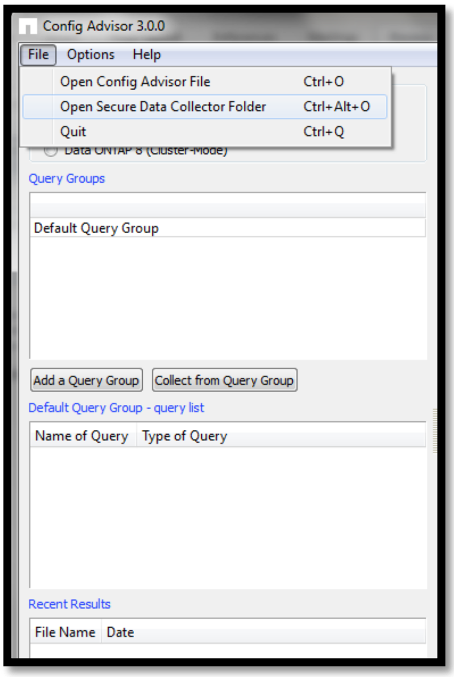
Multiple files can be imported into the tool at once. For this, all the files should be placed in a single directory. Import the file or directory by using the **File** menu option. After the import is completed, a single Config Advisor result file is created.

8.6.1 Importing filtered data file for analysis

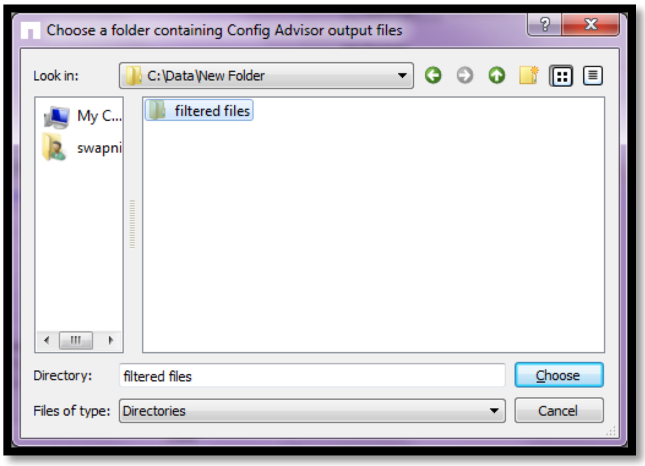
Steps

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

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

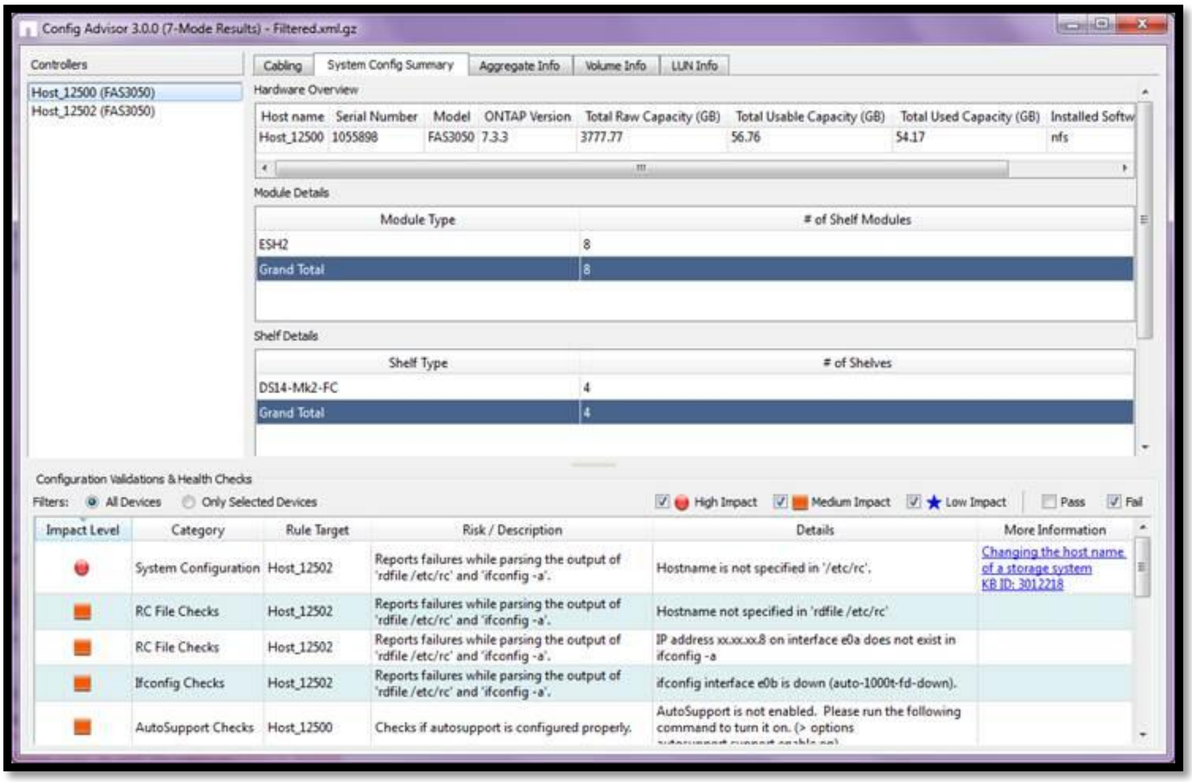


2. Select the folder where the data files are located, and click **Choose**.



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

The results window is as shown:


Config Advisor 3.0.0 (7-Mode Results) - Filtered.xml.gz
Controllers
Host_12500 (FAS3050)
Host_12502 (FAS3050)
Cabling
System Config Summary
Aggregate Info
Volume Info
LUN Info
Hardware Overview
Module Details
Shelf Details
Configuration Validations & Health Checks
Filters: ● All Devices ○ Only Selected Devices
☑ ● High Impact ☑ 🟧 Medium Impact ☑ ★ Low Impact □ Pass ☑ Fail

Host name	Serial Number	Model	ONTAP Version	Total Raw Capacity (GB)	Total Usable Capacity (GB)	Total Used Capacity (GB)	Installed Softw
Host_12500	1055898	FAS3050	7.3.3	3777.77	56.76	54.17	nfs

Module Type	# of Shelf Modules
ESH2	8
Grand Total	8

Shelf Type	# of Shelves
DS14-Mk2-FC	4
Grand Total	4

Impact Level	Category	Rule Target	Risk / Description	Details	More Information
●	System Configuration	Host_12502	Reports failures while parsing the output of 'rdfile /etc/rc' and 'ifconfig -a'.	Hostname is not specified in '/etc/rc'.	Changing the host name of a storage system KB ID: 3012218
🟧	RC File Checks	Host_12502	Reports failures while parsing the output of 'rdfile /etc/rc' and 'ifconfig -a'.	Hostname not specified in 'rdfile /etc/rc'	
🟧	RC File Checks	Host_12502	Reports failures while parsing the output of 'rdfile /etc/rc' and 'ifconfig -a'.	IP address xx.xx.xx.8 on interface e0a does not exist in ifconfig -a	
🟧	Ifconfig Checks	Host_12502	Reports failures while parsing the output of 'rdfile /etc/rc' and 'ifconfig -a'.	ifconfig interface e0b is down (auto-1000t-fd-down).	
🟧	AutoSupport Checks	Host_12500	Checks if autosupport is configured properly.	AutoSupport is not enabled. Please run the following command to turn it on. (> options	

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

8.7 Launching Help for the script

You can find usage and help information for the script.

Steps

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

9 Troubleshooting

You can find information about how to troubleshoot some of the issues that you might come across when you use Config Advisor 3.2. You can also find explanations for the issues, possible causes, and solutions.

9.1 Nx50xx with 5.2.x displays multiple firmware related error messages

Issue

Config Advisor 3.2 does not validate clustered ONTAPs Nexus 5010 and Nexus 5020 switches running firmware 5.2(1)N1(1), therefore warning messages are..

Possible cause

Config Advisor currently does not validate clustered ONTAPs Nexus 5010 and Nexus 5020 switches running firmware 5.2(1)N1(1).

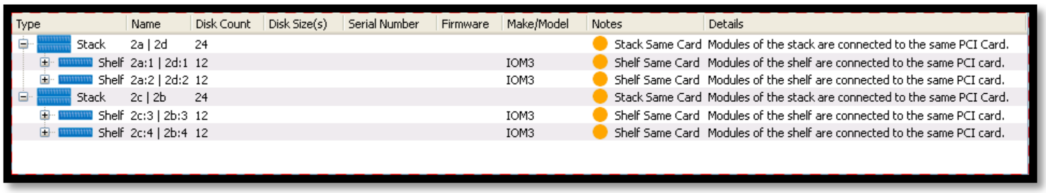
Workaround

Ignore such warning messages.

9.2 Stack Same Card and Stack Same Bridge messages displayed

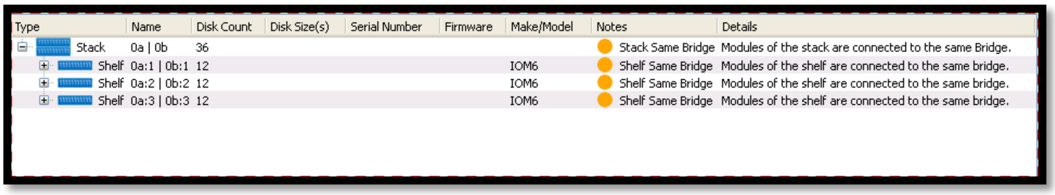
Issue

Config Advisor displays a Stack Same Card or Shelf Same Card warning as follows:



Type	Name	Disk Count	Disk Size(s)	Serial Number	Firmware	Make/Model	Notes	Details
⊟ Stack	2a | 2d	24					● Stack Same Card	Modules of the stack are connected to the same PCI Card.
⊞ Shelf	2a:1 | 2d:1	12				IOM3	● Shelf Same Card	Modules of the shelf are connected to the same PCI card.
⊞ Shelf	2a:2 | 2d:2	12				IOM3	● Shelf Same Card	Modules of the shelf are connected to the same PCI card.
⊟ Stack	2c | 2b	24					● Stack Same Card	Modules of the stack are connected to the same PCI Card.
⊞ Shelf	2c:3 | 2b:3	12				IOM3	● Shelf Same Card	Modules of the shelf are connected to the same PCI card.
⊞ Shelf	2c:4 | 2b:4	12				IOM3	● Shelf Same Card	Modules of the shelf are connected to the same PCI card.

Config Advisor displays a Stack Same Bridge or Shelf Same Bridge warning as follows:



Type	Name	Disk Count	Disk Size(s)	Serial Number	Firmware	Make/Model	Notes	Details
⊟ Stack	0a | 0b	36					● Stack Same Bridge	Modules of the stack are connected to the same Bridge.
⊞ Shelf	0a:1 | 0b:1	12				IOM6	● Shelf Same Bridge	Modules of the shelf are connected to the same bridge.
⊞ Shelf	0a:2 | 0b:2	12				IOM6	● Shelf Same Bridge	Modules of the shelf are connected to the same bridge.
⊞ Shelf	0a:3 | 0b:3	12				IOM6	● Shelf Same Bridge	Modules of the shelf are connected to the same bridge.

Possible cause

This might be because of the usage of only a single host bus adapter (HBA) card or onboard ports. Usage of only onboard ports or a single HBA results in a single point of failure in the storage configuration.

MPHA is supported for configurations that use only a single HBA. You should split connections between the ASICs of the HBAs. On a quad-port HBA, this means that ports A and B use one ASIC, and ports C and D use the other.

Workaround

The ports should be paired across the ASICs on the HBA (for example, A and C ports, and B and D ports). For SAN attached storage (SAS) connections, see the Universal SAS Cabling Guide, available on the NetApp Support Site.

Using only onboard ports is also supported. For example, the FAS3200 series includes two onboard SAS ports for storage connectivity. For systems that use only a single stack of storage, NetApp supports using only the two onboard ports for MPHA connectivity. You should use an HBA in addition to the onboard ports for additional hardware resiliency.

9.3 Entering AutoSupport ID in the old format displays an error message

Issue

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

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

Possible cause

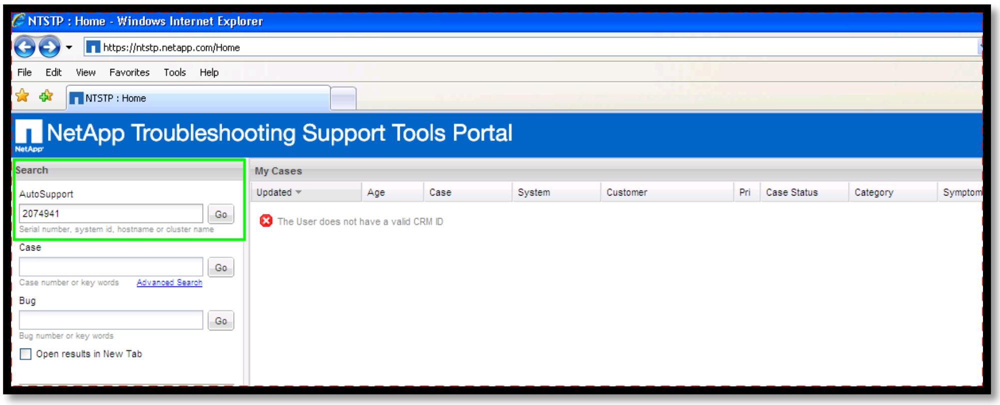
Config Advisor 3.0 and WireGauge 2.1.x do not support the earlier AutoSupport ID format, which begins with AE, followed by 15 digits.

Workaround

Steps

1. Log in to the NetApp Support Site 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:

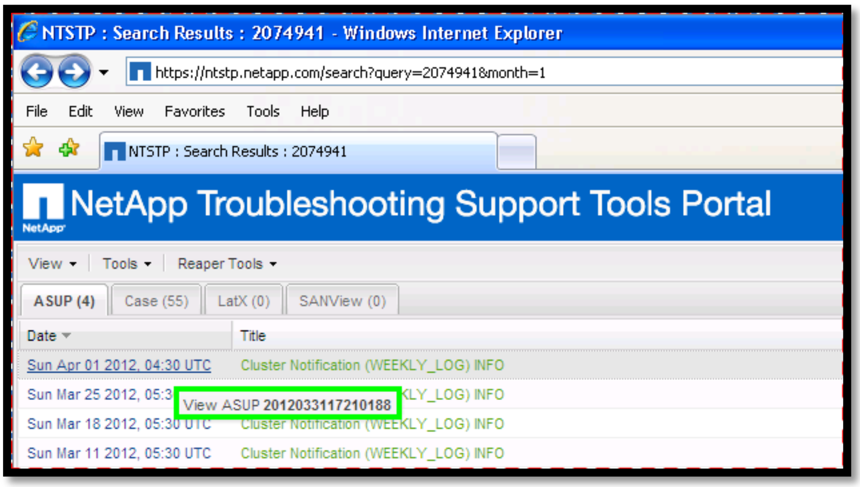

NTSTP : Home - Windows Internet Explorer
https://ntstp.netapp.com/Home
File Edit View Favorites Tools Help
NTSTP : Home
NetApp Troubleshooting Support Tools Portal
Search
My Cases
Updated
Age
Case
System
Customer
Pri
Case Status
Category
Symptom
Case
Go
Case number or key words
Advanced Search
Bug
Go
Bug number or key words
□ Open results in New Tab

AutoSupport: 2074941 Go

Serial number, system id, hostname or cluster name

The User does not have a valid CRM ID

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:

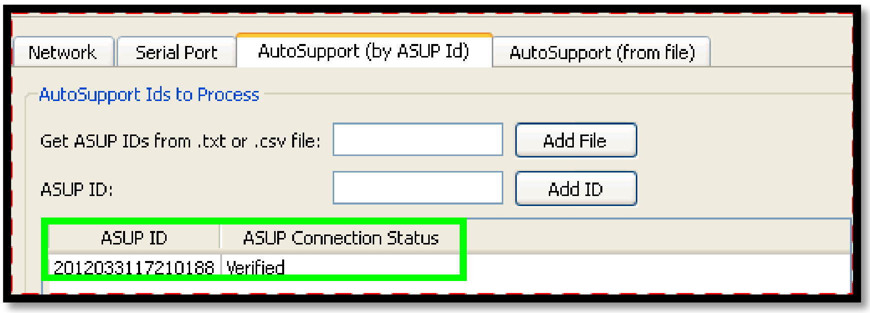

NTSTP : Search Results : 2074941 - Windows Internet Explorer
https://ntstp.netapp.com/search?query=2074941&month=1
File Edit View Favorites Tools Help
NTSTP : Search Results : 2074941
NetApp Troubleshooting Support Tools Portal
View Tools Reaper Tools
ASUP (4)
Case (55)
LatX (0)
SANView (0)

Date	Title
Sun Apr 01 2012, 04:30 UTC	Cluster Notification (WEEKLY_LOG) INFO
Sun Mar 25 2012, 05:3	KLY_LOG) INFO
Sun Mar 18 2012, 05:30 UTC	Cluster Notification (WEEKLY_LOG) INFO
Sun Mar 11 2012, 05:30 UTC	Cluster Notification (WEEKLY_LOG) INFO

View ASUP 2012033117210188

4. Enter the new format of the AutoSupport ID.

The ID is verified as shown:



Get ASUP IDs from .txt or .csv file:

ASUP ID:

ASUP ID	ASUP Connection Status
2012033117210188	Verified

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

9.4 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 Data ONTAP, and also reports only for SAS shelves.

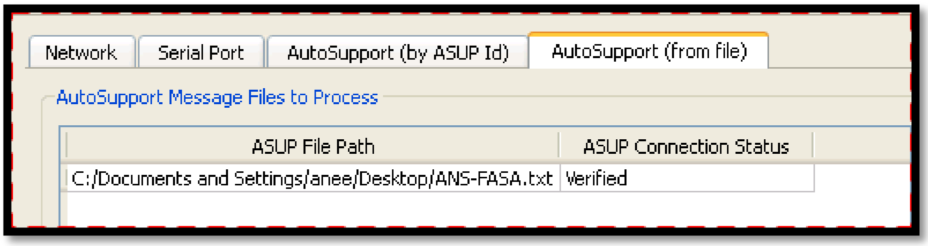
Workaround

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 NetApp Support Site. The same approach can also be used for FC cabling.

For FC and SATA shelves, the physical cabling can be verified only manually.

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

The AutoSupport (from file) tab is as shown:



ASUP File Path	ASUP Connection Status
C:/Documents and Settings/anee/Desktop/ANS-FASA.txt	Verified

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:
   - The `rdfile /etc/rc` command output under the header `===== RC =====`
   - The `rdfile /etc/hosts` command output under the header `===== HOSTS =====`
   - 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).

A. Appendix: Configuration Validations & Health Checks

Check name	Description	Supports 7- Mode	Supports clustered Data ONTAP	Supports FlexPod setup
Shelf Path Checks	Catches issues where both the modules of the stack are connected to the same bridge	√	√	√
Shelf Checks	Checks for shelf compatibility for individual slots	√	√	√
Shelf Checks	Checks FAS2220 Shelf Rules	√	√	√
Shelf Checks	Checks for DS4486 Shelf Rules	√	√	√
Shelf Checks	Checking DS4246 shelf configuration and best practices.	√	√	√
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 Disk Shelves cabling against the Universal SAS and ACP Guide	√	√	√
HA Configuration	Checks if required options are set the same in an HA pair	√	-	√
HA Configuration	Identifies systems where the HA functionality has been manually disabled	√	-	√
HA Configuration	Checks if software license(s) match on both the nodes of the HA pair	√	√	√
HA Configuration	Checks if signature applies to 7-Mode HA configurations that have been operating in a takeover state for at least seven days	√	-	√
HA Configuration	Checks if there is shelf count mismatch between the members of a cluster pair	√	-	√
HA Configuration	Identifies systems where the interconnect links are down	√	-	√
HDD Firmware Bug	Seagate drives running out-of-date firmware can cause loop instability. Upgrade to NA07/NA08 or a newer firmware version	√	√	√
HDD Firmware Bug	Seagate "Moose" HDDs drives found that can potentially become unresponsive after power-cycle. Upgrade to a current version of firmware	√	√	√
HDD Firmware Bug	Catches issues where a Seagate disk drive has NA00 firmware that can cause Parity Inconsistency errors	√	√	√
I/O Module Firmware Bug	I/O Module firmware checks	√	-	√
Platform	Multiple 'EMERGENCY' messages are present. There is some environmental instability that needs to be addressed	√	-	√

Check name	Description	Supports 7- Mode	Supports clustered Data ONTAP	Supports FlexPod setup
Platform	Identifies all filers/platforms that have power supplies that have compromised the power redundancy	√	-	√
Software Bug	ONTAP version '7.3.1', '7.3.1.1', '7.3.1.1L1' found and SMB 2.0 is on. This system is at risk of data corruption of files equal to or greater than 4 GB.	√	-	√
Software Bug	Data ONTAP version 7.2.6.1 or 7.2.6.1P1 and "R" variants found running the CIFS protocol with quotas enabled is exposed to a potential panic	√	-	√
Software Bug	Clustered systems with Data ONTAP version 7.3.5 is actively running FCP or has the ability of running FCP, the Data ONTAP version is listed in a bug report and is susceptible to a panic	√	-	√
Storage	Identifies systems that have recurring Power Supply shelf faults, and faulty shelf component(s)	√	-	√
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	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	Checks for shelf compatibility for individual slots.	√	√	√
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	Data ONTAP 7.3 and later releases do not support the DS14mk1 disk shelf, LRC or ESH	√	-	√
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	This signature identifies single path standalone FAS3XXX and FAS6XXX systems.	√	-	√
Storage	Identifies systems exposed to TSB-1007-04 where systems running Data ONTAP less than 7.3.4 (and 7.3.3P*) with DS4243 disk shelves are potentially vulnerable to data loss.	√	-	√

Check name	Description	Supports 7- Mode	Supports clustered Data ONTAP	Supports FlexPod setup
Storage	Checks for failed disks and disks that are not reporting properly to ONTAP.	√	-	√
Storage	Checks for Systems with DS14-type IO module missing.	√	-	√
System Configuration	The option raid.min_spare_count is set to 0. No "out of spares" warning messages will be displayed.	√	-	√
System Configuration	FAS3140/3160/3170 with PAM1 and PCI-e adapter cards report Resource Conflict error at boot	√	-	√
System Configuration	Compares the host name from outputs of /etc/rc and ‘hostname’	√	-	√
System Firmware Bug	FAS3000 systems running BIOS versions less than 2.2 may experience a CPU panic as described in the bug report.	√	-	√
System Firmware Bug	FAS2020/FAS2050 system with BMC firmware version 1.1 is susceptible to a spurious shutdown reported as 'BMC lost heartbeat' or 'BATTERY LOW' condition.	√	-	√
System Firmware Bug	FAS6000 systems running system BIOS versions less than 1.5.0 may experience a CPU panic as described in bug report.	√	-	√
RC File Checks	Checks if the host name is specified in /etc/rc	√	-	√
RC File Checks	Checks for a duplicate VLAN for a given interface	√	-	√
RC File Checks	Checks if the VLAN add command was would execute before the VLAN create command.	√	-	√
RC File Checks	Checks if the default route is set in /etc/rc	√	-	√
RC File Checks	Checks if the ifconfig setting in /etc/rc for an interface refers to a non-existent interface hostname	√	-	√
RC File Checks	Checks if an interface was configured without a VLAN being created	-	-	-
RC File Checks	Warns if an interface explicitly states a broadcast address	√	-	√
RC File Checks	Checks if an interface is missing a Netmask	√	-	√
RC File Checks	Checks if an IP address setting for an interface is missing from the output of ‘ifconfig –a’	√	-	√
Ifconfig Checks	Ifconfig interface is down	√	-	√
Ifconfig Checks	Ifconfig interface flowcontrol is not full	√	-	√

Check name	Description	Supports 7- Mode	Supports clustered Data ONTAP	Supports FlexPod setup
Ifconfig Checks	ifconfig interface has IP addresses but is not UP	√	-	√
RC File Checks	Checks if a ‘ifconfig –a’ interface does not exist in the /etc/rc file	√	-	√
RC File Checks	Checks if an IP address setting for an interface in ‘ficonfig –a’ is missing from the /etc/rc file	√	-	√
RC File Checks	Ifconfig netmask setting in /etc/rc and ‘ifconfig –a’ output differ	√	-	√
RC File Checks	Ifconfig broadcast setting in /etc/rc amd ‘ifconfig –a’ output differ	√	-	√
Exports File Check	Output of exportfs differs from /etc/exports. /etc/exports contains '%s'	√	-	√
Exports File Check	Output of exportfs differs from /etc/exports. exportfs contains '%s'	√	-	√
Host File Checks	Failed to lookup in-line host reference for an interface in '/etc/hosts'	√	-	√
Host File Checks	Checks if the host name appears in /etc/hosts	√	-	√
MTU Checks	Checks if ifconfig MTU is different to /etc/rc setting for a given interface	√	-	√
MTU Checks	Checks if ifconfig MTU is not set in /etc/rc for an interface	√	-	√
AutoSupport Checks	Checks if the destination URL for AutoSupport is set correctly	√	√	√
AutoSupport Checks	Checks if the SMTP mailbox destination for AutoSupport is set correctly	√	√	√
AutoSupport Checks	Checks if AutoSupport enabled	√	√	√
Max Snapshot Checks	Snapshots are within 90% of recommended setting for NDU upgrade	√	√	√
Max Flex Volumn Checks	FlexVol are within 90% of recommended setting for NDU upgrade	√	√	√
HA Option Checks	Checks if RC options are the same in for an HA pair	√	-	√
HA Config Checks	Checks if controller model number is the same in the HA pair	√	-	√
HA Config Checks	Verifies if failover mode (cfmode) is the same in the HA pair	√	-	√

Check name	Description	Supports 7- Mode	Supports clustered Data ONTAP	Supports FlexPod setup
HA Config Checks	Verifies if host name and partner name are different in SYSCONFIG-A	√	-	√
HA Config Checks	Checks if Partner Name and Partner's Host name are different in SYSCONFIG-A	√	-	√
HA Config Checks	Checks if Data ONTAP versions are different in HA pair	√	-	√
HA Config Checks	Checks if clustering is not enabled	√	-	√
Revision Checking	System Firmware against the latest available version.	√	-	√
Revision Checking	Shelf Firmware found for module type against the latest available.	√	-	√
Revision Checking	Disk Firmware against the latest available version.	√	-	√
Revision Checking	RLM Firmware against the latest available version.	√	-	√
Revision Checking	SP Firmware against the latest available version.	√	-	√
Revision Checking	BMC Firmware against the latest available version.	√	-	√
Cluster Switch RFC 5010	Compares the switch's configuration to the "Reference Configuration File (RCF) for a Nexus 5010."	-	√	-
Cluster Switch RFC 5020	Compares the switch's configuration to that of the "Reference Configuration File (RCF) for a Nexus 5020."	-	√	-
Cluster Switch RCF CN1610/1601	Compares the Cluster Switch's configuration to the Reference Configuration File (RCF)	-	√	-
Cluster Switch RCF 5596	Compares the switch's configuration to that of the Reference Configuration File (RCF) for a Nexus 5596.	-	√	-
Cluster Switch Software Version	Compares the Cluster switch IOS version to the expected version, which is matched to the Reference Configuration File. This rule will be run against each cluster switch.	-	√	-
Cluster Switch ISL Count	Checks if each cluster switch has the appropriate number of ISL connections between the two cluster switches. This rule only needs to be run against one cluster switch, since the result will be the same for the other switch.	-	√	-

Check name	Description	Supports 7- Mode	Supports clustered Data ONTAP	Supports FlexPod setup
Cluster Switch ISL Ports	The ISL links between each cluster switch should be on specified ports (which will vary based on the switch model). This rule will be applied to both cluster switches. For each ISL port, compare the ports where ISL links exist to appropriate row for that port in the compatibility matrix (for the given switch model, switch firmware, and ONTAP revision).	-	√	-
Cluster Switch Fan	Verifies that the fans in the cluster network switches are running ok.	-	√	-
Cluster Switch PS	Verifies that the power supplies in the cluster network switch are running ok.	-	√	-
Cluster Switch CDP	Verifies that Cisco Discovery Protocol is running and can see all other devices in the cluster network.	-	√	-
Cluster Switch SFP By Port	Determine that each port has an SFP that complies with the correct speed expected for that port.	-	√	-
	Confirms that the SFP associated with each interface is correct for its interface type.	-	√	-
Cluster Switch Exp Module Model	Determines if the expansion module is of the correct module	-	√	-
Mgmt Switch Reference Configuration File 2960	Compares the switch's configuration to that of the "Reference Configuration File" for a Catalyst 2960.	-	√	-
Mgmt Switch Reference Configuration File 1601	Compares the switch's configuration to that of the "Reference Configuration File" for a Nexus CN 1601	-	√	-
Mgmt Switch Software Version	Compares the management switch IOS version, which is matched to the Reference Configuration File. This rule will be run against each management switch.	-	√	-
Mgmt Switch ISL Count	Each management switch should have the appropriate number of ISL connections between the two switches.	-	√	-
Mgmt Switch ISL Ports	The ISL links between each management switch should be on the specified port. This rule should be applied to both management switches. Interface GigabitEthernet0/1 on ‘switch1’ should be connected to Interface GigabitEthernet0/2 on ‘switch2’	-	√	-
Mgmt Switch Fan	Verifies that the fans in the management network switch are running ok.	-	√	-
Mgmt Switch PS	Verifies that the power supply in the management network switches is running ok.	-	√	-
Mgmt Switch CDP	Verifies that Cisco Discovery Protocol is running and can see all other devices in the management network.	-	√	-

Check name	Description	Supports 7- Mode	Supports clustered Data ONTAP	Supports FlexPod setup
Cluster Node Connect To Cluster Switch	Each cluster node should have one connection to each cluster switch. The connections should be to the same port on each cluster switch	-	√	-
Cluster Node Connect To Mgmt Switch	Each cluster node should have at least one connection to a management switch.	-	√	-
Node Cluster NIC Model	Only certain model Network Interface Cards (NICs) are allowed to be used as for a cluster network interface. Verifies that the NICs being used for the cluster network are correct.	-	√	-
Node Cluster NIC Slot	The NICs used for the cluster network are only allowed to be in certain PCI slots. Verifies the cluster network ports are in valid slots for the cluster network. The ports will vary based on the controller model.	-	√	-
All Nodes Same ONTAP	Verifies that all nodes in the cluster are running the same version of Data ONTAP	-	√	-
Cluster Node Port Roles	Verifies that the cluster ports and the management ports are on valid slots for the cluster network	-	√	-
Cluster Node CDP	Verifies that Cisco Discovery Protocol is running on the cluster nodes	-	√	-
NTP Server Defined And Enabled	Verifies that Network Time Protocol (NTP) has been configured and enabled on all nodes of the cluster.	-	√	-
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.	-	√	-
FlexPod Running Config Check	Checks that the Cisco Nexus Switch running-config matches its startup-config.	-	-	√
FlexPod SSH and Telnet Check	Checks that telnet is off and ssh is on, on the Cisco Nexus Switches.	-	-	√
FlexPod SSH and Telnet Check	Checks that telnet is off and ssh is on, on the storage controllers.	-	-	√
FlexPod CDP Check	Checks if Cisco Discovery Protocol is enabled on FAS controller for use in connectivity checks.	-	-	√
FlexPod LACP and VPC Check	LACP and Virtual Port Channels are used on the Nexus switches to provide redundant connectivity within the FlexPod.	-	-	√

Check name	Description	Supports 7- Mode	Supports clustered Data ONTAP	Supports FlexPod setup
FlexPod UCSM HA Check	Ensures high availability for the UCS Manager by checking that both fabric interconnects are operable and in a cluster relationship.	-	-	√
FlexPod Service Profile vNICs Check	Checks the service profile for HA configuration on the vNICs. (Either failover or multipath)	-	-	√
FlexPod VPC Health Check	Checks that the Virtual Port Channel domain is healthy: peer is alive, peer-link is up, and all vPCs are consistent and online.	-	-	√
FlexPod Secure Management Check	Checks that https administration is on and http administration is off on the physical controller (vfiler0). Checks that only secure management methods are being used for storage controller administration.	-	-	√
FlexPod 10GbE Uplinks Check	Checks that each fabric interconnect has at least 2 10GbE uplinks. Does not check connectivity or confirm that they are configured for high availability.	-	-	√
FlexPod Service Profile HA	Checks the service profile level if HA is configured on the HBAs. Assigned service profiles should have at least one vHBA on each SAN fabric.	-	-	√
FlexPod Maintenance Policy	Checks that the default maintenance policy is set to something other than 'immediate'.	-	-	√
FlexPod Storage Switch Network Correlation Check	Checks that storage controller has an ifgroup connected to a Virtual Port Channel (vPC) on the Nexus 5k switches (using CDP).	-	-	√
FlexPod Storage Protocols Check	Checks that storage protocols features are enabled.	-	-	√
FlexPod FCP Check	Check that FCP is licensed and enabled on the controller.	-	-	√
FlexPod UCS Switch Network Correlation Check	Checks that fabric interconnect has an uplink port channel connected to a Virtual Port Channel (vPC) on the Nexus 5k switches (using CDP)	-	-	√
FlexPod VLAN Correlation Check	Checks that allowed VLAN lists are consistent across the infrastructure.	-	-	√
FlexPod SAN port channel Check	Checks that each Fabric Interconnect has an uplink SAN port channel with at least 2 links.	-	-	√
FlexPod Service Profile State Check	Reports service profiles in the 'config-failure' state.	-	-	√
FlexPod Blades/Servers Discovery	Verifies that all physical blades/servers are discovered.	-	-	√
FCoE QoS Configuration	Checks that minimum QoS configuration is in place to support FCoE	-	-	√

Check name	Description	Supports 7- Mode	Supports clustered Data ONTAP	Supports FlexPod setup
FlexPod Chassis Discovery Policy	Checks the chassis discovery policy.	-	-	√
FlexPod FEX Uplink Check	Checks that each FEX has at least 2 10GbE uplinks to the fabric interconnect	-	-	√
FlexPod RC and Exports File Check	Checks that storage controller has all necessary running config written to /etc/rc and /etc/exports.	-	-	√
FlexPod Device Online	Checks that the FlexPod devices were online and data collection successful.	-	-	√

Index