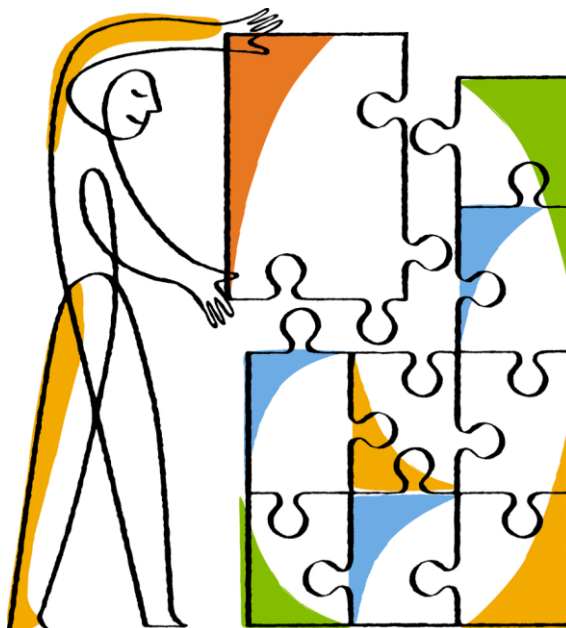




Config Advisor Plug-ins

Installation and Administration Guide



Contents

Overview of Config Advisor	5
Config Advisor plug-ins	6
Preparing for installation	7
Windows host requirements	7
Plug-in requirements	7
Installing Config Advisor plug-ins.....	8
Plug-in versions supported.....	8
Data collection using Config Advisor plug-in	10
Data collection using a profile	10
E-Series	11
NetApp SANtricity web services proxy 1.1.....	11
Network (SMcli)	12
E-Series Host-side collection.....	14
Managed ONTAP SAN	16
MetroCluster in clustered Data ONTAP	17
FlexPod	23
Data collection from FlexPod – clustered Data ONTAP	25
Data collection from FlexPod – 7-Mode.....	27
Viewing plug-in results in Config Advisor	30
Viewing FlexPod – clustered Data ONTAP results in Config Advisor	34
Viewing FlexPod 7-Mode results in Config Advisor.....	38
Generating reports from plug-in results	41
Saving plug-in credentials in Config Advisor	42
Loading saved plug-in credentials	43
Config Advisor AutoSupport for plug-in results.....	44
Upgrading Config Advisor plug-in	45
Uninstalling Config Advisor plug-in.....	46
Periodic data collection for issues diagnostic.....	47
Using Config Advisor through the command prompt.....	47
Scheduling periodic data collection	49
Email notification	49
Reporting plug-in issues in Config Advisor	51
Troubleshooting.....	52

Null script execution halted due to error – Smcli failed message displayed.	52
E-Series data collection fails when SANtricity storage manager client is not installed.....	53

Appendix 54

E-Series configuration validation and health checks	54
E-Series hosts configuration validation and health checks	55
Managed ONTAP SAN configuration validation and health checks	57
MetroCluster in clustered Data ONTAP configuration validation and health checks	59
FlexPod configuration validations & health checks	68

Copyright information 78

Trademark information..... 79

How to send your comments..... 80

Overview of Config Advisor

Config Advisor is a tool to validate configuration and health of NetApp Systems and it is used to check a NetApp system or solution for proper hardware, cabling, software configuration, and conformance of NetApp recommended best practice settings and standards.

Config Advisor 4.0 introduced a new plug-in architecture in which new profiles can be dynamically added, upgraded, or removed from existing list of static Config Advisor profiles.

Advantage of the new plug-in architecture is that the plug-in can be independently updated and released without the need for a Config Advisor tool release.

Config Advisor supports validation of FlexPod, MetroCluster in clustered Data ONTAP, E- Series storage arrays, and Mission Critical System Health Checks using the plug-in architecture.

Config Advisor 4.3 supports encryption of device credentials and saved queries and provides an option to require a password when launching Config Advisor.

Note: This guide includes installation and administration details for the Config Advisor plug-ins. For more information about Config Advisor, see the [Config Advisor Installation and Administration Guide](#).

Config Advisor plug-ins

Plug-ins may be added, upgraded or removed from the existing list of Config Advisor plug-ins that are installed. Profiles that come along with Config Advisor might also be overridden and extended using a plug-in.

Config Advisor supports the following plug-ins:

- **E-Series plug-in**

The E-Series plug-in has both a storage array configuration validation as well as a host-side validation option.

- **Managed ONTAP SAN plug-in**

The Managed ONTAP SAN plug-in enables data collection and validation of mission critical SAN deployments.

- **MetroCluster in clustered Data ONTAP plug-in**

The MetroCluster in clustered Data ONTAP plug-in enables data collection and validation of MetroCluster in clustered Data ONTAP.

- **FlexPod plug-in**

The FlexPod plug-in enables you to run a detailed health check for all of the components in the FlexPod stack.

The Config Advisor plug-ins are downloaded as separate installable packages. You must have Config Advisor 4.3 or later installed for any plug-in to work. Plug-ins are installed in the data directory of the Config Advisor tool. Plug-ins installed in the Config Advisor data directory may introduce new profiles accessible through the Config Advisor tool Profile drop-down box in the main window.

Using the Config Advisor profile, a user can collect data, view and analyze results, generate PDF reports, MS Word reports, and MS Excel reports, and post Config Advisor AutoSupport results to NetApp.

Preparing for installation

You must be aware of the prerequisites and requirements before installing the Config Advisor plug-ins.

Windows host requirements

Config Advisor plug-ins are supported with the following Windows operating systems:

- Windows 7 SP1 32-bit
- Windows 7 SP1 64-bit

Plug-in requirements

- You must have installed Config Advisor 4.3 or later. For more information about installing Config Advisor, see the [Config Advisor Installation and Administration Guide](#).
- You must have downloaded the plug-in installation package to the host machine, in which you have installed Config Advisor.

User type	Plug-in download location
External and internal users	http://mysupport.netapp.com/NOW/download/tools/config_advisor/

Installing Config Advisor plug-ins

You should install Config Advisor framework and then install the desired plug-in.

Plug-in versions supported

A list of compatible versions of Config Advisor and the plug-in available on the Support Site is provided in the following table.

Config Advisor Version	Plug-in Version
Config Advisor 4.1 or 4.2	E-Series plug-in 1.1 MetroCluster plug-in 1.1 in clustered Data ONTAP
Config Advisor 4.3	E-Series plug-in 1.2 MetroCluster plug-in 1.2 in clustered Data ONTAP
Config Advisor 4.4	E-Series plug-in 2.0 MetroCluster plug-in 1.3 in clustered Data ONTAP FlexPod plug-in 1.0 Managed ONTAP SAN plug-in 1.1
Config Advisor 4.5	FlexPod plug-in 1.1 MetroCluster plug-in 1.5 in clustered Data ONTAP Managed ONTAP SAN plug-in 2.0

You can install any of the following Config Advisor plug-ins:

- E-Series plug-in
- Managed ONTAP SAN plug-in
- MetroCluster in clustered Data ONTAP plug-in
- FlexPod plug-in

Steps

1. Unzip the plug-in installation package (*.zip file) to the host machine and place the contents of the package in the below mentioned folder location under ConfigAdvisorDataDirectory_Base\ConfigAdvisorData\plugin_eggs. Ensure that when entering the plug-in folder name under plugin_eggs you are able to see the plug-in files especially profileConfig.xml or profileExtensionConfig.xml.

Operating system	Directory path to place plug-in files
Windows 7 SP1 32-bit Windows 7 SP1 64-bit	C:\Users\<windows_login>\ConfigAdvisorData\plugin_eggs or {USERPROFILE}\ConfigAdvisorData\plugin_eggs

2. Relaunch **Config Advisor**.
3. In the Config Advisor user interface, the **Profiles** drop down list (top-left corner) displays the newly added plug-in along with other static profiles, such as **Clustered Data ONTAP, Data ONTAP 7 and 8 (7-Mode)**.
4. In the Config Advisor user interface, **Logs** window displays a message after the plug-in is installed successfully.

For example, if you have installed the E-Series plug-in, you should see the message, Plug-in ‘**E-Series**’ **Loaded.**’

Data collection using Config Advisor plug-in

After you have installed the required plug-in, you can select the profile (plug-in) using which Config Advisor performs the data collection.

In the Config Advisor user interface, under **Profile**, select the required profile for the option **Choose an Execution Profile**. You can select any of the following profiles:

- E-Series
- Managed ONTAP SAN
- MetroCluster in clustered Data ONTAP
- FlexPod

Data collection using a profile

Steps

1. In the Config Advisor user interface, under **Profile**, select the required profile for the option Choose an **Execution Profile**.
2. Enter the details in the profile tab and click **Collect Data**.
3. Enter the filename in which you want to save the collected data.

The commands and their outputs are stored in a file with *.xml.gz extension in the Config Advisor data directory. Config Advisor opens the file at the end of data collection and the computed results are displayed in the Config Advisor Result Viewer interface.

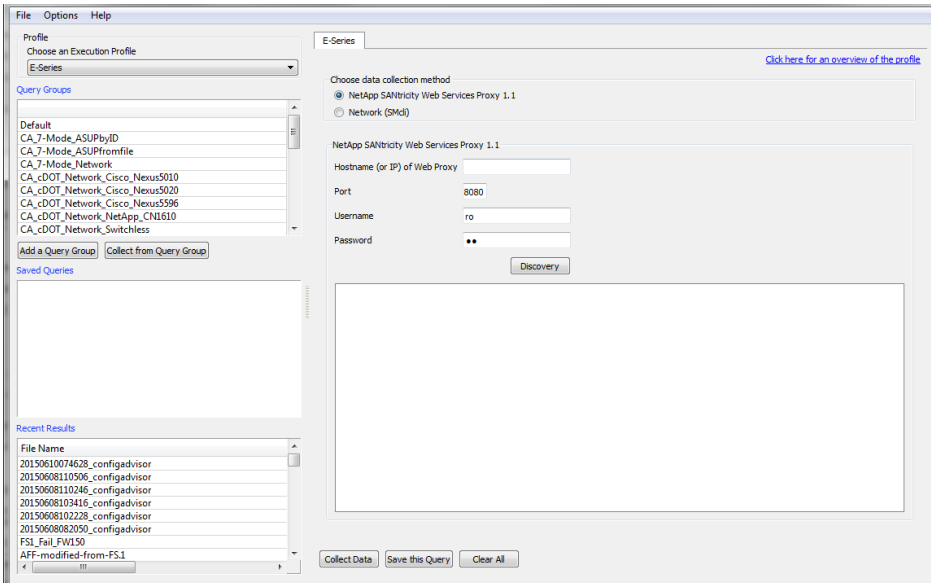
The previous data collection files are stored in the Config Advisor data directory and these results are displayed in the Config Advisor user interface, **Recent Results** pane.

For more information about using the **Recent Results** pane, see the [Config Advisor Installation and Administration Guide](#).

If you want to save the values entered in the sub profiles, you can use the **Save Query** option in the Config Advisor user interface.

E-Series

The E-Series profile page is shown below:



The E-Series Plug-in 2.0 is developed to work with Config Advisor tool, to enable data collection and validation of an E-Series Storage Array. The E-Series profile has two data collection methods that one can use:

- NetApp SANtricity Web Services Proxy 1.1
- Network (SMcli)

NetApp SANtricity web services proxy 1.1

The NetApp SANtricity Web Services Proxy provides Web APIs to configure, manage, and monitor E-Series and EF-Series arrays. The proxy provides access to a collection of REST (Representational State Transfer) style interfaces to access services defined for storage arrays. The proxy can be installed on a Windows or Linux system.

Config Advisor uses NetApp SANtricity Web Services Proxy to collect data from multiple E-Series Storage Arrays that is under the management of NetApp SANtricity Web Services Proxy. For more information, see

<http://community.netapp.com/t5/E-Series-SANtricity-and-Related-Plug-ins-Articles-and-Resources/NetApp-SANtricity-Web-Services/ta-p/86931>.

Information on how to install, configure, and uninstall NetApp SANtricity Web Services Proxy 1.2 can be found in the [NetApp SANtricity Web Services Proxy 1.2 Installation Guide](#). For more detailed information on configuring and using NetApp SANtricity Web Services Proxy 1.2 see the [NetApp SANtricity Web Services Proxy 1.2 User Guide](#). Please also refer to our [E-Series and EF-Series Systems Documentation Center](#) and look for SANtricity Web Services Proxy 1.2 that is found in the SANtricity Management Plug-ins link.

Credentials of the NetApp SANtricity Web Services Proxy is required to collect from E-Series Storage Systems that are under its management.

Field name	Description
Hostname (or IP) of Web Proxy	The full hostname or IPv4 address of the NetApp SANtricity Web Services Proxy.
Port	Port through which the REST service is available.
Username	Username is defaulted to 'ro'.
Password	Password is defaulted to 'ro'.

On clicking "Discovery" all the E-Series Storage Systems that are under the management of NetApp SANtricity Web Services Proxy is listed on a table below the "Discovery" button. Select the E-Series Storage Systems from which Config Advisor is to collect data and click on the **"Collect Data"** button.

Network (SMcli) (see [E-Series Plug-in 1.1 Installation and Administration Guide](#) for the following section).

Network (SMcli)

SANtricity Storage Manager Client is available as part of SANtricity Storage Manager Software for E-Series Storage Array. Config Advisor uses the SMcli.exe that gets installed with the SANtricity Storage Manager Client to collect data from the E-Series Storage Array. Currently Config Advisor is tested with SANtricity Storage Manager version 11.10.XX00.0020.

Steps

1. Download and install the E-Series/EF-Series SANtricity Storage Manager 11.10.XX00.0020 from
http://mysupport.netapp.com/NOW/download/software/eseries_santricity/11.10.XX00.0020/

Note: SANtricity Storage Manager installed in default location C:\Program Files (x86)\Storage Manager on Windows 7 Operating System does not have full administrative permissions to C:\ drive resulting in Config Advisor Error. See section [Troubleshooting](#) to resolve this error.

The E-Series Storage Array contains two controllers but only one controller is accessed for data collection. Credentials for either controller can be entered for data collection.

The credentials required for E-Series Storage Array are as follows: Credentials for E-Series Storage Array Description.

Field name	Description
Hostname (or IP)	The full hostname or IPv4 address of the E-Series Storage Array.
Username	Username is either 'admin' or 'monitor' only.
Password	Password if set on the Storage Array.

Note: The credentials are not validated before data collection for E-Series.

2. Enter credentials and click Collect Data.
3. Enter the file name in which the collected data has to be saved.

Config Advisor uses SMCLI.exe from the SANtricity Storage to collect data from an E-Series Storage.

The commands and their outputs are stored in a file with .xml.gz extension in Config Advisor DATA directory. The tool opens this file at the end of data collection which shows computed results in Graphical User Interface which is the Config Advisor Result Viewer.

All the files of data collection stored in the in Config Advisor DATA directory are displayed on the tool on the main window > **Recent Results** at the bottom left pane.

For more information, see [Config Advisor Installation and Administration Guide](#).

E-Series Host-side collection

Collecting host-side information for analysis is currently limited to hosts running supported versions of the Linux operating system. This collection requires the use of a remote shell to execute commands and collect the results. Using 'telnet' to collect this information is considered insecure as the connection between Config Advisor and the host is not encrypted and can be "sniffed". The alternate to 'telnet' is to use Secure Shell, also known as "SSH". This option provides improved authentication facilities and the ability to encrypt the session between Config Advisor and the host.

SecureShell is a feature provided in standard Linux distributions and may already be enabled on the hosts you intend to collect information from. For details, consult Linux documentation.

Steps

1. Enter credentials and click **Collect Data**.
2. Enter the file name in which the collected data has to be saved.

Field name	Description
Hostname (or IP)	The full hostname or IPv4 address of the E-Series host system.
Username	By default, username is 'root'.
Password	Password of the E-Series host system.

You can run host side checks and run comparisons against IMT data for a Linux based E-Series host system. To run from a multiple host systems, you might use the **Collect from Query Group** feature. Save multiple E-Series host credentials into a single query group and click the **Collect from Query Group** button.

Rules analysis and reporting is grouped for multiple systems when using the **Collect from Query Group** feature.

The E-Series 2.0 plug-in for Config Advisor introduces support for collection of host-side information. Some of the known restrictions/limitations of host-side support are as follows:

The host-side collection is currently in Beta and known to work on the following Linux Operating Systems for Intel\AMD 64-bit systems (PowerPC architectures not tested). Additional support will be added in future releases:

- RHEL 6.6, 7.1, and 7.2

- SLES 11.3, 12.1
- OVM 6.2
- OEL 6.7
- CentOS 6.5
- IB-iSER configurations are reported as iSCSI protocol.
- Multipath validation is only performed for Device Mapper Multipath (DM-MP) configurations.

Managed ONTAP SAN

On the Config Advisor tool, in the main window, select > **Profile** > option > **Choose an Execution Profile** > **Managed ONTAP SAN** and the Managed ONTAP SAN page is loaded.

The Managed ONTAP SAN profile page is shown below:

The screenshot displays the 'Managed ONTAP SAN' configuration page. The 'Profile' dropdown is set to 'Managed ONTAP SAN'. The 'Cluster Node' section contains input fields for 'Hostname (or IP)', 'Username' (pre-filled with 'admin'), and 'Password'. The 'Query Groups' section lists various profiles such as 'Default', 'CA_7-Mode_ASUPbyID', and 'CA_cDOT_Network_Cisco_Nexus5010'. The 'Saved Queries' section is empty. The 'Recent Results' section shows a list of file names. At the bottom right, there are three buttons: 'Collect Data', 'Save this Query', and 'Clear All'.

The fields in Managed ONTAP SAN sub-profiles tab are as follows:

GUI field\GUI button	Description
Hostname (or IP)	Host name or IP address of the controller.
Username	User name to access the node.
Password	Password to access the controller.
Collect Data	Initiates the collect data request from Config Advisor.
Save this Query	Saves the profile details as a query for later use.
Clear All	Clears the details entered in the fields in the profile page.

MetroCluster in clustered Data ONTAP

The MetroCluster in clustered Data ONTAP profile page is shown below:

Details of common fields in the different profile pages are as follows:

Field name	Description
Hostname (or IP)	Hostname or IP address of the node, switch, or ATTO bridge.
Username	User name to access the node, switch, or ATTO bridge.
Password	Password to access the node, switch, or ATTO bridge.
Collect Data	Initiates the collect data request from Config Advisor.
Save this Query	Saves the profile details as a query for later use.
Clear All	Clears the details entered in the fields in the profile page.

Note: All switches mentioned here are the back-end Fibre Channel switches.

Note: The node that is entered in **Run Switchover Simulation on Cluster Node** must be one of the nodes that is configured in the 2Node or 4Node profile.

This profile collects data from MetroCluster in clustered Data ONTAP (MCC) setup.

There are three different profiles:

- **All MetroCluster configurations:** This is a new profile in the version 1.5 of the MetroCluster plugin and covers all MetroCluster configurations regardless of amount of nodes or topology. To use this profile only the existing components need to be entered. The only two mandatory fields are 2 storage controllers. All other components are optional. The plug-in will determine which checks to run for the specific configuration.
- **Two-node configuration:** This profile is used to configure the various two-node configurations. It is still present so that existing data can be analyzed and existing configurations do not need to be transferred to the “All MetroCluster configurations” profile. To configure new two-node configurations it is advisable to use the “All MetroCluster configurations”. In case the two-node configuration is expanded to a four-node configuration no new profile need to be configured but the existing configurations can be expanded by two nodes and switches as needed.
- **Four-node configuration:** This profile is used to configure the various four-node configurations. It is still present so that existing data can be analyzed and existing configurations do not need to be transferred to the “All MetroCluster configurations” profile. The same applies to the use of this profile.

It requires collecting data from nodes of the two clusters, backend Fibre Channel switches, and ATTO bridges. You can select a sub profile that best describes the MetroCluster in clustered Data ONTAP setup by clicking the appropriate tab and option buttons. If the number of ATTO bridges in MCC setup is fewer than available fields, extra fields can be left as-is. MCC plug-in 1.3 version supports NetApp ONTAP versions 8.3.0, 8.3.1, and 8.3.2. NetApp recommends performing data collection when all devices are up and running, make sure that the controllers are not in switch over or taken over state during data collection.

The following are two new features that have been implemented in the MetroCluster in clustered Data ONTAP:

- **Form Fill Assistance:** You can enter the credential once and have them copied for all of the similar components. IP addresses entered are incremented for each component.

- Data Collection Method Selection:** You can either select or clear the check boxes under the **Data Collection Method Selection** pane to control the data collection protocol fallback at the component level.

Note: If you are at a secure site, AutoSupport is switched off, user credentials are not collected, and Telnet is disabled. However, these settings may be revisited using **Options > Preferences** items.

All MetroCluster configuration:

The screenshot displays the 'All MetroCluster configurations' window, which is divided into several panes and sections:

- Profile:** A dropdown menu showing 'MetroCluster in clustered Data ONTAP'.
- Query Groups:** A list of query groups including 'CA_FlexPod_N7k_E2EFCoE', 'CFT', 'FlexPod', 'MCC', 'MCC_8_Pack', 'MCC_demo', 'NApp_CA_7-Mode_Network', 'NApp_CA_cDOT_Network_CN1610', and 'NApp_CA_MCC2Nodes_C9148'.
- Form Fill Assistance:** A link to 'Click here for an overview of the profile'.
- Choose your MetroCluster in clustered Data ONTAP configuration by Switch Model:** Radio buttons for 'Brocade 6505', 'Brocade 6510', 'Cisco 9148', 'Cisco 9148s', and 'Cisco 9250i'.
- Data collection method selection:** Checkboxes for 'SSH', 'Telnet', 'HTTP(s)', and 'Telnet' under 'Simulation Node', 'FibreBridge', 'Switch', and 'Storage Controller'.
- Run Switchover Simulation on Cluster Node:** Fields for 'Hostname (or IP)', 'Username', and 'Password'.
- Cluster A Node 1:** Fields for 'Hostname (or IP)', 'Username', and 'Password'.
- Cluster B Node 1:** Fields for 'Hostname (or IP)', 'Username', and 'Password'.
- Cluster A Node 2:** Fields for 'Hostname (or IP)', 'Username', and 'Password'.
- Cluster B Node 2:** Fields for 'Hostname (or IP)', 'Username', and 'Password'.
- Collect Data:** Buttons for 'Collect Data', 'Save this Query', and 'Clear All'.

Two-node with fabric configuration:

File Options Help

Profile
Choose an Execution Profile
MetroCluster in clustered Data ONTAP

Query Groups
CA_FlexPod_N7k_E2EFCoE
CFT
FlexPod
MCC
MCC_8_Pack
MCC_demo
NApp_CA_7-Mode_Network
NApp_CA_cDOT_Network_CN1610
NApp_CA_MCC2Nodes_C9148

Add a Query Group Collect from Query Group

Query Group Content for MCC_8_Pack

Saved Query Execution Profile
Vsim8pack MetroCluster in clustered Data ONTAP...
8NMCC - rha6-7-8pack MetroCluster in clustered Data ONTAP...

Recent Results

Name
Netapp-4-2016_configadvisor.xml.gz
Multi-VLANs_Duplicates_configadvisor.xml.gz
Multi-VLANs_Duplicate_configadvisor.xml.gz
Multi-VLANs_configadvisor.xml.gz
20160420092548_configadvisor.xml.gz
10.237.25.4610.237.25.4810.235.79.24010.235.79_201602
20160418093300_configadvisor.xml.gz
C-tempOWDCNAGPA_4_7_16-AFTER_configadvisor.xml

All MetroCluster configurations Two-node configuration Four-node configuration

Form Fill Assistance [Click here for an overview of the profile](#)

Choose your MetroCluster in clustered Data ONTAP configuration

☒ Two-node with FC storage fabrics
☐ Two-node with (optical) SAS cables
☐ Two-node with FC-to-SAS bridges

Choose your switch model

☒ Brocade 6505
☐ Brocade 6510
☐ Cisco 9148
☐ Cisco 9148s
☐ Cisco 9250i

Data collection method selection

	SSH	HTTP(s)	Telnet
Simulation Node	☒	☒	☒
FibreBridge	☒	☐	☒
Switch	☒	☐	☒
Storage Controller	☒	☒	☒

Run Switchover Simulation on Cluster Node

Cluster A Node 1

Hostname (or IP)
 Username
 Password

Cluster B Node 1

Hostname (or IP)
 Username
 Password

Fabric 1 Backend FC Switch 1 Fabric 1 Backend FC Switch 2

Collect Data Save this Query Clear All

- Two-node with FC Storage fabrics:** This requires collecting data from the devices [Controllers, switches, and Atto bridges] based on the type of FC Switch model that is being used in the configuration.
- Two-node with (optical) SAS cables:** This requires collecting data from both the nodes of the two clusters.
- Two-node with FC-to-SAS- bridges:** This requires collecting data from both the nodes of the two clusters and the Atto bridges.
- Four-node configurations:** This sub profile requires collecting data from the devices [Controllers, switches, and Atto bridges] based on the type of FC switch model that is being used in the configuration.

Four-node with fabric configuration:

The screenshot displays the Config Advisor web interface for a 'Four-node configuration'. The 'Profile' is set to 'MetroCluster in clustered Data ONTAP'. Under 'Query Groups', 'MCC_8_Pack' is selected. The 'Data collection method selection' table is as follows:

Component	SSH	Telnet	HTTP(s)
Simulation Node	☒	☒	☒
FibreBridge	☒	☒	☐
Switch	☒	☒	☐
Storage Controller	☒	☒	☒

Below the table, there are fields for 'Run Switchover Simulation on Cluster Node' (Hostname, Username, Password) and six clusters (A and B Node 1, 2, 3) with their respective Hostname, Username, and Password fields. At the bottom, there are buttons for 'Collect Data', 'Save this Query', and 'Clear All'.

Considerations for data collection

Based on the Profile selected, you can refer to the following sections. Data is collected for controllers using the SSH protocol. If connectivity fails, then the fall back mechanism selects HTTPS protocol as the alternative.

Data is collected for ATTO bridges using the Telnet protocol. If connectivity fails, then there is no fall back mechanism. The maximum number of ATTO bridges supported by Config Advisor is 40 in the two and four-node configuration profiles, 80 in the All MetroCluster configurations profile.

You can enter the data for the ATTO bridge as per the configuration. If the configuration contains less than 40 ATTO bridges, the remaining fields can be left blank.

Data collection on all sub profiles must be done in a state where all the nodes, switches, and bridges are running. If this requirement is not met, this results in some of the rules falling into the **Not Evaluated** state.

Additional data collection considerations that are dependent on the profile:

For MetroCluster in clustered Data ONTAP plug-in, the following sub profiles are supported:

- **Brocade 6510:** This profile is a four switch configuration with Brocade 6510 switches connecting all of the two or four nodes and ATTO bridges.
- **Brocade 6505:** This profile is a four switch configuration with Brocade 6505 switches connecting all of the two or four nodes and ATTO bridges.
- **Cisco 9148:** This profile is a four switch configuration with Cisco 9148 switches connecting all of the two or four nodes and ATTO bridges.
- **Cisco 9148S:** This profile is a four switch configuration with Cisco 9148S switches connecting all of the two or four nodes and ATTO bridges.
- **Cisco 9250i:** This profile is a four switch configuration with Cisco 9250i switches connecting all of the two or four nodes and ATTO bridges.

FlexPod

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 Cisco Nexus 5000\7000\9000 series switches, and NetApp storage controllers. Optionally, data may be collected from VMware vCenter Server to receive recommendations on the latest supported firmware from NetApp *Interoperability Matrix Tool*. As with all FlexPod setups, the recommendations are related only to the core infrastructure and SAN boot configuration-any application workloads running on the infrastructure are not checked.

Note: Config Advisor supports only NX-OS mode for Cisco Nexus 9000 series switches.

Note: All the FlexPod device (One Cisco UCS Cluster, two Cisco Nexus Switches, one Cluster Interconnect and NetApp 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.

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

Note: Config Advisor currently is tested against only a subset of the hardware. However, Config Advisor can also be used with other FlexPod configurations. Refer to NetApp Interoperability Matrix Tool and FlexPod Technical specification for FlexPod supported configurations. Config Advisor can be used only for FlexPod Datacenter and not for FlexPod Express or FlexPod Select.

You can use the Config Advisor FlexPod profile to run a detailed health check for all the components in the FlexPod stack. This profile can be used when commissioning a newly configured FlexPod system or when running the checks on the existing FlexPod stack. There are some checks that alert you about potential outage.

Note: Ensure that there are no pending configurations in FlexPod.

The FlexPod checks focus on the cabling between the FlexPod components and the configurations that run on them. The checks that focus on the cabling check for a minimum number of links that have to be present between the components as per the design. The checks that focus on the configuration collect the running configuration data of all the components and correlate them with

the validated design configuration. In addition, the checks indicate an appropriate severity level whenever there is a deviation in the cabling or configuration.

For configuration or cabling recommendations, see the Cisco Validated Design (CVD) guide available at cisco.netapp.com, www.cisco.com/go/flexpod, or contact technical support.

See [FlexPod configuration validations & health checks](#) for a detailed description of all the FlexPod checks that are run.

In the FlexPod profile, you can collect data by using one of the following tabs in Config Advisor:

- FlexPod – 7-Mode
- FlexPod – clustered Data ONTAP

Based on the Cisco Nexus switch model that you use, you can choose any one of the following options:

- Cisco Nexus 5000
- Cisco Nexus 7000
- Cisco Nexus 9000 (NX-OS mode only)

Select the Cisco UCS Model

- Cisco UCS
- Cisco UCS Mini

In the FlexPod clustered Data ONTAP profile, you can choose any one of the following cluster interconnects:

- Cisco NX5010\5020\5596\5596T
- NetApp CN1610
- Switchless

Note: When you choose Cisco Nexus 7000 series switch as your switch model, the FlexPod SAN Boot Architecture can only be End-to-End FCoE.

Note: When you choose Cisco Nexus 9000 series switch as your switch model, the FlexPod SAN Boot Architecture can only be iSCSI.

Based on the FlexPod SAN Boot architecture used, you can choose any one of the following options in the tab:

- FCoE to the storage controller
- Classic FCP to the storage controller
- Do not check FCP\FCoE configuration
- End-to-End FCoE
- iSCSI
- FC – Direct attach storage to UCS
- FCoE – Direct attach storage to UCS

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

Data collection from FlexPod – clustered Data ONTAP

The process of collecting data from any one of the FlexPod profiles is the same. For more information see, [Data collection from FlexPod – 7-Mode](#).

The **FlexPod– Clustered Data ONTAP** profile tab is as shown:

The screenshot displays the 'FlexPod - Clustered Data ONTAP' configuration window. The interface is organized into several sections:

- Profile:** A dropdown menu set to 'FlexPod'.
- Query Groups:** A list containing 'Default', 'Test 123', 'Test 456', and 'Test Sep'.
- Choose Nexus Switch Model:** Radio buttons for 'Cisco Nexus 5000' (selected), 'Cisco Nexus 7000', and 'Cisco Nexus 9000 (Cisco NX-OS mode)'.
- Choose Cisco UCS Model:** Radio buttons for 'Cisco UCS' (selected) and 'Cisco UCS Mini'.
- Choose Clustered Data ONTAP switch:** Radio buttons for 'Cisco NX5010/5020/5596/5596T' (selected), 'NetApp CN1610', and 'Switchless'.
- Choose FlexPod SAN Boot Architecture:** Radio buttons for 'FCoE to the storage controller', 'Classic FCP to the storage controller', 'Don't check FCP/FCoE configuration', 'End-to-End FCoE' (selected), 'FC - Direct attach storage to UCS', and 'FCoE - Direct attach storage to UCS'.
- Cisco UCS Cluster:** Fields for 'Hostname (or IP)', 'Username' (admin), 'Password', and a 'Test Login' button showing 'Unknown'.
- vCenter Server (optional):** Fields for 'Hostname (or IP)', 'Port' (443), 'Username' (root), 'Password', and a 'Test Login' button showing 'Unknown'.
- Cisco Nexus - Fabric A:** Fields for 'Switch Name (or IP)', 'Username' (admin), and a 'Test Login' button.
- Cisco Nexus - Fabric B:** Fields for 'Switch Name (or IP)', 'Username' (admin), and a 'Test Login' button.
- Include 'show tech-support':** A checkbox that is currently unchecked.
- Buttons:** 'Collect Data', 'Save this Query', and 'Clear All'.
- Recent Results:** A list showing a saved query named 'Default_20160217064900' with a file path '20160217064811_configadvisor.xml.gz'.

Fields in FlexPod – Clustered Data ONTAP profile tab

The fields in FlexPod setup profile tab are as follows:

GUI field\GUI button	Description
Admin VDC name (or IP)	Name of the Admin VDC or IP address (for a Cisco Nexus 7000 series switch)
Ethernet VDC name	Name of the Ethernet VDC (for a Cisco Nexus 7000 series switch)
Storage VDC name	Name of the Storage VDC (for a Cisco Nexus 7000 series switch)
Hostname (or IP)	Host name or IP address of the Cisco UCS Cluster, VMware vCenter Server, and NetApp Cluster
Switch Name (or IP)	Name or IP address of the Cisco Nexus Fabric A and B and Cisco Nexus Cluster Interconnect switches
Username	User name to access the Cisco UCS Cluster, VMware vCenter Server, Cisco Nexus Fabric A and B, NetApp Cluster, and Cisco Nexus Cluster Interconnect switches
Password	Password to access the Cisco UCS Cluster, VMware vCenter Server, Cisco Nexus Fabric A and B, NetApp Cluster, and Cisco Nexus Cluster Interconnect switches
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 using VMware vSphere SDK for VMware vCenter Server 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.

GUI field\GUI button	Description
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).

Data collection from FlexPod – 7-Mode

Steps

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

Note: For a Cisco Nexus 7000 series switch you have to enter the Admin VDC name (or IP); Ethernet VDC name and Storage VDC name to collect data.

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

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

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

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

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

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

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

The **FlexPod – 7-Mode** profile tab is as shown:

The screenshot displays the 'FlexPod - 7-Mode' profile configuration window. On the left, there's a sidebar with 'Profile' (FlexPod), 'Query Groups' (Default, Test 123, Test 456, Test Sep), 'Add a Query Group', 'Collect from Query Group', 'Saved Queries', and 'Recent Results'. The main area is divided into several sections: 'Choose Nexus Switch Model' (Cisco Nexus 5000, Cisco Nexus 7000), 'Choose FlexPod SAN Boot Architecture' (FCoE to the storage controller, Classic FCP to the storage controller, Don't check FCP/FCoE configuration, End-to-End FCoE), 'Cisco UCS Cluster' (Hostname, Username: admin, Password, Test Login, Unknown), 'Cisco Nexus - Fabric A' (Switch Name, Username: admin, Password, Test Login, Unknown), 'Cisco Nexus - Fabric B' (Switch Name, Username: admin, Password, Test Login, Unknown), 'Storage Controller 1' (Hostname), and 'Storage Controller 2' (Hostname). At the bottom, there are buttons for 'Collect Data', 'Save this Query', and 'Clear All'.

Fields in FlexPod – 7-Mode profile tab

The fields in FlexPod setup profile tab are as follows:

GUI field\GUI button	Description
Admin VDC name (or IP)	Name of the Admin VDC or IP address (for a Cisco Nexus 7000 series switch)
Ethernet VDC name	Name of the Ethernet VDC (for a Cisco Nexus 7000 series switch)
Storage VDC name	Name of the Storage VDC (for a Cisco Nexus 7000 series switch)
Hostname (or IP)	Host name or IP address of the Cisco UCS Cluster and NetApp storage HA pair
Switch Name (or IP)	Name or IP address of the Cisco Nexus Fabric A and B
Username	User name to access the Cisco UCS Cluster, Cisco Nexus Fabric A and B, and NetApp storage HA pair
Password	Password to access the Cisco UCS Cluster, Cisco Nexus Fabric A and B, and NetApp storage HA pair

GUI field\GUI button	Description
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).

Viewing plug-in results in Config Advisor

Using the selected Config Advisor plug-in (profile), the Config Advisor Result Viewer opens at the end of data collection displaying the computed results.

Example of data collection results from E-Series Storage Array

Impact Level	Category	Rule Target	Risk / Description	Details
High Impact	E-Series Volume Health Check	TME_ConfigAdvisor_Tst	Verifies if a storage array's volume health is optimal	No Tray loss protection for Volume VQ0_CA-TST. This can be corrected by reconfiguring the parent Volume Group or Disk Pool using SANtricity
Fail	E-Series Storage Array Auto Support Check	TME_ConfigAdvisor_Tst	Verifies if Auto Support is configured on the Storage Array	AutoSupport status missing
Pass	E-Series Drive Health Check	TME_ConfigAdvisor_Tst	Verifies if a storage array's drive health is optimal	All drives have optimal status
Pass	E-Series Hot Spare Coverage Check	TME_ConfigAdvisor_Tst	Verifies if there is adequate spare drive coverage in the case of fail over	Global spares configured for fail over protection (count = 1)
Pass	E-Series Storage Array Health Check	TME_ConfigAdvisor_Tst	Verifies the health of the Storage Array	Storage Array health status is optimal
Pass	E-Series Storage Array Battery Check	TME_ConfigAdvisor_Tst	Verifies the health of the cache battery	All batteries are healthy
Pass	E-Series Controller Firmware Check	TME_ConfigAdvisor_Tst	Checks to ensure Controller is at the most recent CFW level	Controller Firmware is at the latest level

Example of data collection results from E-Series Host (Result Viewer)

Impact Level	Category	Rule Target	Risk / Description	Details	More Information
High Impact	E-Series Host IMT check	rashidlinuxhel (Red Hat 6.5)	Verifies if a host configuration is supported as per IMT	Host not configured as per IMT. Following matrix is not supported OS: (Red Hat 6.5), Kernel: (2.6.32-431.el6.x86_64), Array Firmware: (unknown), Protocol: (unknown), Multipath: (Device-Mapper).	Please refer to NetApp Interoperability Matrix at support.netapp.com/matrix
High Impact	E-Series Host Multipath Syntax	rashidlinuxhel (Red Hat 6.5)	Verifies if any syntax errors in /etc/multipath.conf file.	Multipath is not installed	Device-Mapper Multipath must be installed for E-Series storage. The multipath rpm is not installed or this is an invalid Operating System
High Impact	E-Series Host Multipath Version	rashidlinuxhel (Red Hat 6.5)	Verifies if a host multipath version is recommended	Could not determine the multipath version.	If the service is not found, then Device-Mapper Multipath should be installed. Otherwise, the multipath service must be started!
High Impact	E-Series Host Multipath Service	rashidlinuxhel (Red Hat 6.5)	Verifies if a host multipath service is optimal	Multipathd service not running: not found	create an /etc/multipath.conf file and populate it if necessary
High Impact	E-Series Linux Host Multipath Configuration	rashidlinuxhel (Red Hat 6.5)	Verifies if a host multipath configuration is correct	/etc/multipath.conf does not exist. This is required to start the multipath service!	Device-Mapper Multipath must be installed for E-Series storage.
High Impact	E-Series Linux Host Type	rashidlinuxhel (Red Hat 6.5)	Verifies if correct host type selected in SANtricity Storage Manager	Multipath is not installed	

Example of data collection results from E-Series Host (Command Viewer)

Command	Output
a=\$(rpm -qa grep multipath); if [[\$a == ""]]; then echo notfound; else echo \$a; fi	a=\$(rpm -qa grep multipath); if [[\$a == ""]]; then echo notfound; else echo \$a; fi
cat /proc/mounts egrep -w ext4 xfs btrfs	notfound
cat /proc/scsi/scsi	notfound
command -v multipath > /dev/null 2>&1; if [\$? -eq 1]; then echo notfound; else multipath -ll fi	notfound
command -v multipath > /dev/null 2>&1; if [\$? -eq 1]; then echo notfound; else a=\$(readlink -f \$(lsblk grep multipath));	notfound
if [[-a /etc/os-release]]; then a=\$(cat /etc/os-release egrep '^NAME=' sed 's/\"/\"/g' tr -d '\n'); cat /etc/os-release e...	notfound
if [[-a /etc/multipath.conf]]; then cat /etc/multipath.conf; elif [[-a /etc/multipath.conf]]; then echo empty; else echo not...	notfound
uname -r	notfound

Example of data collection results from Managed ONTAP SAN

Clustered Data ONTAP		Configuration Check Profile : Managed ONTAP SAN :: dff_svc0_profile			
(f2240-197-119 (FAS2240-4)) (f2240-197-120 (FAS2240-4))		Filters: ☒ All Devices ☐ Only Selected Devices ☐ High Impact ☐ Medium Impact ☐ Low Impact ☒ Best Practice ☒ Pass ☐ Fail ☒ Not Evaluated			
Impact Level	Category	Rule Target	Risk / Description	Details	More Information
✓	Cluster Node Health Check	f2240-197-119	Verifies that nodes are up and communicating and can be queried for information	Node is healthy.	
✓	Cluster Node Health Check	f2240-197-120	Verifies that nodes are up and communicating and can be queried for information	Node is healthy.	
✓	SAN Data Network Interfaces Check	f2240-197-119	Verifying cluster only has SAN protocol lifs	only SAN lifs exist on the cluster.	
✓	SAN Data Network Interfaces Check	f2240-197-120	Verifying cluster only has SAN protocol lifs	only SAN lifs exist on the cluster.	
✓	Volumes per Node Check	f2240-197-119	Verifying the number of volumes per node	This node has an acceptable number of volumes	
✓	Snapshot per Volume Check	f2240-197-119	Verifying the number of snapshots per volume	All volumes have a number of snapshots within parameters	
✓	Dedupe Disabled Check	f2240-197-119	Verifying dedupe is disabled on all volumes	Volumes all have dedupe disabled	
✓	Compression Disabled Check	f2240-197-119	Verifying compression is disabled on all volumes	Compression is disabled on all volumes	
✓	Volumes per Node Check	f2240-197-120	Verifying the number of volumes per node	This node has an acceptable number of volumes	
✓	Snapshot per Volume Check	f2240-197-120	Verifying the number of snapshots per volume	All volumes have a number of snapshots within parameters	
✓	Dedupe Disabled Check	f2240-197-120	Verifying dedupe is disabled on all volumes	Volumes all have dedupe disabled	
✓	Compression Disabled Check	f2240-197-120	Verifying compression is disabled on all volumes	Compression is disabled on all volumes	

Example of data collection results from MetroCluster in clustered Data ONTAP

Backend Fibre Channel Switches		Configuration Check Profile : MetroCluster in clustered Data ONTAP :: Cisco 9148			
dpg-mcc-cisco9148-02-A-fabX (Mds 9148 fc) dpg-mcc-cisco9148-02-B-fabX (Mds 9148 fc) dpg-mcc-cisco9148-02-A-fabY (Mds 9148 fc) dpg-mcc-cisco9148-02-B-fabY (Mds 9148 fc)		Filters: ☒ All Devices ☐ Only Selected Devices ☒ High Impact ☒ Medium Impact ☐ Low Impact ☒ Best Practice ☒ Pass ☐ Fail ☒ Not Evaluated			
Impact Level	Category	Rule Target	Risk / Description	Details	
✓	CorrectCombinationStorage	dpg-mcc-8020-02-a1	Verify that each adapters connecting storage are of the correct combination	All Storage adapters are connecting vali of storage devices	
✓	CorrectCombinationStorage	dpg-mcc-8020-02-b1	Verify that each adapters connecting storage are of the correct combination	All Storage adapters are connecting vali of storage devices	
✓	CorrectCombinationStorage	dpg-mcc-8020-02-a2	Verify that each adapters connecting storage are of the correct combination	All Storage adapters are connecting vali of storage devices	
✓	CorrectCombinationStorage	dpg-mcc-8020-02-b2	Verify that each adapters connecting storage are of the correct combination	All Storage adapters are connecting vali of storage devices	
✓	SwitchGeneric_SwUniqueName	dpg-mcc-cisco9148-02-A-fabX	Verify that all switches have a unique name.	Switch names are unique within this DR	
✓	SwitchGeneric_SwUniqueName	dpg-mcc-cisco9148-02-A-fabY	Verify that all switches have a unique name.	Switch names are unique within this DR	
✓	SwitchGeneric_SwUniqueName	dpg-mcc-cisco9148-02-B-fabY	Verify that all switches have a unique name.	Switch names are unique within this DR	
✓	SwitchGeneric_SwUniqueName	dpg-mcc-cisco9148-02-B-fabX	Verify that all switches have a unique name.	Switch names are unique within this DR	
✓	SwitchGeneric_DrGroupCorrectNumSwitches	dpg-mcc-8020-02-a1	Verify that all controllers within the DrGroup connect to the correct number of switches.	Controller dpg-mcc-8020-02-a1 is conn correct number of switches	
✓	SwitchGeneric_DrGroupCorrectNumSwitches	dpg-mcc-8020-02-a2	Verify that all controllers within the DrGroup connect to the correct number of switches.	Controller dpg-mcc-8020-02-a2 is conn correct number of switches	
✓	SwitchGeneric_DrGroupCorrectNumSwitches	dpg-mcc-8020-02-b2	Verify that all controllers within the DrGroup connect to the correct number of switches.	Controller dpg-mcc-8020-02-b2 is conn correct number of switches	
✓	SwitchGeneric_DrGroupCorrectNumSwitches	dpg-mcc-8020-02-b1	Verify that all controllers within the DrGroup connect to the correct number of switches.	Controller dpg-mcc-8020-02-b1 is conn correct number of switches	
✗	SwitchGeneric_SwitchFwSupported	Switch	Verify that the switch and switch module firmware is supported for this version of ONTAP for this DrGroup.	Rule cannot be evaluated with this versi	
✗	SwitchGeneric_SwitchBladeSupported	Switch	Verify that the switch and blade connecting the DR-Group(s) is supported for this version of ONTAP	Rule cannot be evaluated with this versi	
✓	StorageHba_RelatedAdapterSameSpeed	dpg-mcc-8020-02-a1	Verify that all related adapters operate at the same speed.	Storage adapters operate at same speed	
✓	StorageHba_RelatedAdapterSameSpeed	dpg-mcc-8020-02-b1	Verify that all related adapters operate at the same speed.	Storage adapters operate at same speed	
✓	StorageHba_RelatedAdapterSameSpeed	dpg-mcc-8020-02-a2	Verify that all related adapters operate at the same speed.	Storage adapters operate at same speed	
✓	StorageHba_RelatedAdapterSameSpeed	dpg-mcc-8020-02-b2	Verify that all related adapters operate at the same speed.	Storage adapters operate at same speed	
✓	StorageHba_ConnectEvenlyToFabrics	dpg-mcc-8020-02-a1	Verifies that the related storage adapters evenly connect into the fabrics of blades	Storage adapters connect evenly to the Configuration	
✓	StorageHba_ConnectEvenlyToFabrics	dpg-mcc-8020-02-b1	Verifies that the related storage adapters evenly connect into the fabrics of blades	Storage adapters connect evenly to the Configuration	
✓	StorageHba_ConnectEvenlyToFabrics	dpg-mcc-8020-02-a2	Verifies that the related storage adapters evenly connect into the fabrics of blades	Storage adapters connect evenly to the Configuration	
✓	StorageHba_ConnectEvenlyToFabrics	dpg-mcc-8020-02-b2	Verifies that the related storage adapters evenly connect into the fabrics of blades	Storage adapters connect evenly to the Configuration	
✓	StorageHba_MinMaxPath	dpg-mcc-8020-02-a1	Verify that no less than min-Path and not more than max-path HBA initiator ports are used to connect storage devices.	Storage adapters have optimum path tc and FibreBridge's	
✓	StorageHba_MinMaxPath	dpg-mcc-8020-02-b1	Verify that no less than min-Path and not more than max-path HBA initiator ports are used to connect storage devices.	Storage adapters have optimum path tc and FibreBridge's	
✓	StorageHba_MinMaxPath	dpg-mcc-8020-02-a2	Verify that no less than min-Path and not more than max-path HBA initiator ports are used to connect storage devices.	Storage adapters have optimum path tc and FibreBridge's	
✓	StorageHba_MinMaxPath	dpg-mcc-8020-02-b2	Verify that no less than min-Path and not more than max-path HBA initiator ports are used to connect storage devices.	Storage adapters have optimum path tc and FibreBridge's	

The results window is divided into the following panes:

- **Device Listing:** You can view the details of the devices from the results pane.
- **Configuration Validations and Health Checks:** You can use filters to view the rules that were run on the collected data and the results. For more information about the results, see the [Config Advisor Installation and Administration Guide](#).

Details of fields in the Config Advisor **Result Viewer** pane are as follows:

Field name	Description
Configuration Check Profile	Displays the profile on which the configuration check was done. For example, if Managed ONTAP SAN is selected as the execution profile, then the value is Managed ONTAP SAN: diff_svcs_profile.
Filters	Provides an option to filter the results in the configuration check pane. You can use the following options to filter the results: • All Devices: Displays the configuration checks for all the controllers and switches • Only Selected Devices: Displays the configuration checks for only the selected controllers or switches •  High Impact: Critical impact potential, and should be addressed immediately •  Medium Impact: Disruptive impact potential, and should be addressed as soon as possible •  Low Impact: Low impact potential, and should be addressed in the next maintenance window •  Best Practice: Best practice recommendations •  Pass: Displays the rules that have passed the configuration checks • Fail: Displays the rules that have failed •  Not evaluated: Displays the rules that have not been evaluated

Field name	Description
Dashboard failures	Can be activated by clicking ‘View Details’ link on a FlexPod Dashboard. Displays configuration checks related to that link. To revert to normal view select ‘All Devices’.
Impact Level	Displays the impact level of the configuration checks and can be set to any one of the following values: •  High Impact •  Medium Impact •  Low Impact •  Best Practice •  Pass • Fail: •  Not evaluated
Category	Displays the name of the configuration check.
Rule Target	Displays the name of the E-Series storage array, or Managed ONTAP SAN node of interest, or MetroCluster in clustered Data ONTAP.
Risk\Description	Displays the short description of the configuration check.
Details	Displays the details of the configuration check describing the outcome of the rule check.
More Information	Displays additional information or links, if any.

The Config Advisor result details from previous data collections are displayed in the Config Advisor main window, **Recent Results** pane. You can right-click any one of the results to view the available options.

For more information on Saving and Loading credentials, see [Config Advisor Installation and Administration Guide](#).

Viewing FlexPod – clustered Data ONTAP results in Config Advisor

Steps

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

Following is the Config Advisor (FlexPod Results) window is displayed:

Dashboard	Port	Connected Type	Connected Device (Port)	Speed	Network Address
Firmware Recommendation	mgm0	Switch	NBI-AS01-14H12:GigabitEthernet1/36	1000 Mb/s	10.72.242.4
Nodes	Ethernet1/1	Controller	nbice-fp3-stcl-01-e2a	10 Gb/s	192.168.72.241
	Ethernet1/2	Controller	nbice-fp3-stcl-02-e2a	10 Gb/s	10.72.242.239
Cluster Interconnect Switches	Ethernet1/4	Controller	nbice-fp3-stcl-04-e2b	10 Gb/s	
Cisco Nexus Switches	Ethernet1/8	Switch	NBI-AS01-14H12:GigabitEthernet1/20	1000 Mb/s	10.72.242.4
nbice-fp3-sw1 (Nexus5548)	Ethernet1/13	Switch	nbice-fp3-sw2:Ethernet1/13	10 Gb/s	10.72.242.249
nbice-fp3-sw2 (Nexus5548)	Ethernet1/14	Switch	nbice-fp3-sw2:Ethernet1/14	10 Gb/s	10.72.242.249
	Ethernet1/19	Switch	nbice-fp3-uc1-A:Ethernet1/19	10 Gb/s	10.72.242.246
	Ethernet1/20	Switch	nbice-fp3-uc1-B:Ethernet1/19	10 Gb/s	10.72.242.247
	fcl/31	FC		8 Gb/s	
	port-channel1	Controller	nbice-fp3-stcl-01	10 Gb/s	
	Ethernet1/3	Switch		10 Gb/s	
	port-channel16	Switch	nbice-fp3-uc1-B:port-channel16	10 Gb/s	
	fcl/32	FC		8 Gb/s	
	port-channel12	Controller	nbice-fp3-stcl-02	10 Gb/s	
	port-channel1	Switch	NBI-AS01-14H12	1000 Mb/s	
Power Supply Status: ● Fan Status: ●					

Configuration Check Profile : FlexPod - End-to-End FCoE					
Filters:	☒ All Devices	☐ Only Selected Devices	☐ Dashboard Failures	☒ High Impact ☒ Medium Impact ☒ Low Impact ☒ Best Practice ☐ Pass ☒ Fail ☐ Not Evaluated	
Impact Level	Category	Rule Target	Risk / Description	Details	More Information
●	FlexPod Secure Management Check	clus_12240-197-119-120 (Cluster)	Check that HTTPS administration is on and HTTP administration is off on the firewall policy.	HTTP is enabled. You are strongly encouraged to use HTTPS instead.	
●	FlexPod Nexus License Feature Check	nbice-fp3-sw1 (Nexus5548)	Check if the features - fcoe and npiv are enabled to use FC switching features (required for FC & FCoE).	The switch must have the FC_FEATURES_PKG installed to use FC switching features (required for FC & FCoE). Feature is in Grace Period: expired.	
●	FlexPod Nexus License Feature Check	nbice-fp3-sw2 (Nexus5548)	Check if the features - fcoe and npiv are enabled to use FC switching features (required for FC & FCoE).	The switch must have the FC_FEATURES_PKG installed to use FC switching features (required for FC & FCoE). Feature is in Grace Period: expired.	
●	FlexPod VFC-FCoE UCS-FI Port Channel Binding Check	nbice-fp3-sw1 (Nexus5548)	A VFC interface must be bound to the fcoe port-channel between the Nexus and the FI and the VFC interface should be assigned to the Fabric in	A VFC interface must be bound to the fcoe port-channel between the Nexus and the FI	

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

- **Dashboard, Firmware Recommendation, Nodes, Cluster Interconnect Switches, and Cisco Nexus Switches:**
- **Nodes** - Network Interfaces, Cabling, System Config Summary, Aggregate Info tabs
- **Cluster Interconnect Switches** – (port, Connected Type, Connected Host, Speed, Network Interface) tab
- **Cisco Nexus Switches** – (port, Connected Type, Connected Host, Speed, Network Interface) tab
- **Configuration Validations & Health Checks:** You can use filters to see the rules that were run on the collected data and the results.
- **Navigation pane**

The navigation pane allows the user to navigate between Dashboard, Firmware Recommendation, Nodes, Cluster Interconnect Switches, and Cisco Nexus Switches of the FlexPod setup. By default, Dashboard is selected.

- **Dashboard tab**

The **Dashboard** tab lists the inventory of FlexPod categorized by Compute, Network and Storage. Each category has the following sections:

- **Hardware Validated**

This section checks for minimum hardware requirement as per FlexPod technical specifications ([TR-4036](#)).

- **Cabling Validated**

This section checks for minimum cabling requirement as per FlexPod technical specifications ([TR-4036](#)).

The possible values in this section are highlighted in green check mark (✓) and a red cross mark (x). In case of any failure, the cross mark is displayed and upon clicking **View Details** it shows the corresponding errors.

The filter **Dashboard failures** is selected by default when you click the **View Details** link. This filter cannot be selected otherwise. To revert, select the **All Devices** filter.

- **Firmware Recommendation tab**

On the left pane, a list of Cisco UCS blade servers running VMware is displayed. You can select any one of the blade servers to receive the latest recommended firmware versions for the entire FlexPod stack. The first blade server is selected by default.

Firmware Recommendation tab lists the current running and latest recommended firmware version for Hypervisor (VMware), Compute, Network, and Storage. The latest recommended firmware revision is received from IMT at the time of Config Advisor launch if the network access is available.

Dashboard

Firmware Recommendation

VM-Host-Infra-01

Nodes

Cluster Interconnect Switches

Cisco Nexus Switches

Infrastructure	Components	Running Firmware	Recommended Firmware
Hypervisor	Host OS	✓ VMware ESXi 5.5 (Update 2)	VMware ESXi 5.5 (Update 2)
	Cisco UCS HBA enic Firmware	✓ 2.1.2.62	2.1.2.62
	Cisco UCS HBA fmc Firmware	✓ 1.6.0.12b	1.6.0.12b
Compute	Cisco UCS Manager	✓ 2.2(3)	2.2(3)
	Cisco Ix-OS	✓ 7.1(0)H1(1a)	7.1(0)H1(1a)
Network	NetApp Clustered Data ONTAP	✓ 8.3	8.3
Storage			

As per NetApp Interoperability Matrix Tool, running configuration is in 'known good state'.

Configuration Check Profile : FlexPod - End-to-End FCoE

Filters:

All Devices

Only Selected Devices

Dashboard Failures

High Impact

Medium Impact

Low Impact

Best Practice

Pass

Fail

Not Evaluated

Impact Level	Category	Rule Target	Risk / Description	Details	More Information
High	FlexPod Secure Management Check	clus-f2240-197-119-120 (Cluster)	Check that HTTPS administration is on and HTTP administration is off on the firewall policy.	HTTTP is enabled. You are strongly encouraged to use HTTPS instead.	
High	FlexPod Nexus License Feature Check	nbice-fp3-sw1 (Nexus5548)	Check if the features - fcoe and nviv are enabled	The switch must have the FC_FEATURES_PKG installed to use FC switching features (required for FC & FCoE). Feature is in Grace Period: signed.	
High	FlexPod Nexus License Feature Check	nbice-fp3-sw2 (Nexus5548)	Check if the features - fcoe and nviv are enabled	The switch must have the FC_FEATURES_PKG installed to use FC switching features (required for FC & FCoE). Feature is in Grace Period: signed.	
High	FlexPod VFC-FCoE UCS-FI Port Channel Binding Check	nbice-fp3-sw1 (Nexus5548)	A VFC interface must be bound to the fcoe port-channel between the Nexus and the FI and the VFC interface should be assigned to the Fabric in	A VFC interface must be bound to the fcoe port-channel between the Nexus and the FI	

In the case of secure sites, no network access is available. You are required to manually download *resource_binary.zip* from

http://mysupport.netapp.com/public/config_advisor/bin/resources_binary.zip and place it in the C:\Users\<windows_login> \ConfigAdvisorData folder and replace any existing file with the same name. Restart Config Advisor for the new file to take effect.

If the current running Firmware version is unsupported, a red (x) is displayed next to the Firmware version. If the current running Firmware version is supported, a green check mark (✓) is displayed.

Dashboard

Firmware Recommendation

VM-Host-Infra-01

VM-Host-Infra-02

Nodes

Cluster Interconnect Switches

Cisco Nexus Switches

Infrastructure	Components	Running Firmware	Recommended Firmware
Hypervisor	Host OS	✔ VMware ESXi 5.5.0	VMware ESXi 5.5 (Update 2)
	Cisco UCS HBA enic Firmware	✖ 1.4.2.15c	2.1.2.62
	Cisco UCS HBA fnic Firmware	✖ 1.5.0.4-1vmw	1.6.0.12b
Compute	Cisco UCS Manager	✖ 2.2(3c)B	2.2(3)
	Cisco NX-OS	✔ 5.2(1)N1(1b)	7.1(0)N1(1a)
Network	NetApp Clustered Data ONTAP	✔ 8.2.2	8.3

As per NetApp Interoperability Matrix Tool, running configuration is not supported. Refer 'Recommended Firmware' column for the supported firmware matrix.

Configuration Check Profile : FlexPod - End-to-End FCoE

Filters:

All Devices

Only Selected Devices

Dashboard Failures

✔

High Impact

✔

Medium Impact

✔

Low Impact

✔

Best Practice

✔

Pass

✔

Fail

✖

Not Evaluated

Impact Level	Category	Rule Target	Risk / Description	Details	More Information
High	Cluster Node Port Roles	nbice-fp3-stcl-01	Verifying that the cluster ports and the management ports are on valid slots for the cluster network.	clus2 cluster port set to e1b is wrong. Expecting e1a, e2a configured for Platform FAS3270.	
High	Cluster Node Port Roles	nbice-fp3-stcl-02	Verifying that the cluster ports and the management ports are on valid slots for the cluster network.	clus2 cluster port set to e1b is wrong. Expecting e1a, e2a configured for Platform FAS3270.	
High	Cluster Node Port Roles	nbice-fp3-stcl-04	Verifying that the cluster ports and the management ports are on valid slots for the cluster network.	clus2 cluster port set to e1b is wrong. Expecting e1a, e2a configured for Platform FAS3250.	
High	FlexPod Secure Management Check	nbice-fp3-stcl (Cluster)	Check that HTTPS administration is on and HTTP administration is off on the firewall policy.	HTTPS is enabled. You are strongly encouraged to use HTTPS instead.	

- **Nodes tab**

You can view the details such as Network Interfaces, Cabling, System Config Summary, and Aggregate Info of the nodes of the clustered Data ONTAP system.

- **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 (FlexPod Results)** window for Cisco Nexus Switches is as shown:

Dashboard	Port	Connected Type	Connected Device (Port)	Speed	Network Address
NetApp Storage	Admin VDC: mgmt0	Switch	icem-1.rtp.netapp.com:GigabitEthernet1/27	1000 Mb/s	172.20.100.4
Cisco Nexus Switches	Storage VDC: Ethernet4/31	Switch	icef3-uc1-A:Ethernet1/31	10 Gb/s	172.20.100.45
	Storage VDC: Ethernet4/32	Switch	icef3-uc1-A:Ethernet1/32	10 Gb/s	172.20.100.45
icef3-sw1 (Nexus7000 C7004)	Storage VDC: Ethernet4/37	Controller	icef3-stc1-01:e3a	10 Gb/s	
icef3-sw2 (Nexus7000 C7004)	Storage VDC: Ethernet4/38	Controller	icef3-stc1-02:e3a	10 Gb/s	
	Storage VDC: Ethernet4/39	Controller	icef3-st1a:e3a	10 Gb/s	
	Storage VDC: Ethernet4/40	Controller	icef3-st1b:e3a	10 Gb/s	
	Ethernet VDC: Ethernet4/1	Controller	icef3-stc1-01:e1b	10 Gb/s	172.20.102.151
	Ethernet VDC: Ethernet4/2	Controller	icef3-stc1-02:e1b	10 Gb/s	172.20.102.164
	Ethernet VDC: Ethernet4/3	Controller	icef3-st1a:e1b	10 Gb/s	172.20.102.153
	Ethernet VDC: Ethernet4/4	Controller	icef3-st1b:e1b	10 Gb/s	172.20.102.154
	Ethernet VDC: Ethernet4/17	Switch	icef3-vsm:control0	1000 Mb/s	172.20.101.193
	Ethernet VDC: Ethernet4/19	Switch	icef3-vsa:mgmt0	1000 Mb/s	172.20.101.192
	Ethernet VDC: Ethernet4/27	Switch	icef3-uc1-A:Ethernet1/19	10 Gb/s	172.20.100.45
	Ethernet VDC: Ethernet4/28	Switch	icef3-uc1-B:Ethernet1/19	10 Gb/s	172.20.100.46
	Ethernet VDC: Ethernet4/41	Switch	icef3-sw2-data:Ethernet4/41	10 Gb/s	172.20.100.72
	Ethernet VDC: Ethernet4/42	Switch	icecore:Ethernet1/17	10 Gb/s	10.61.185.3

Impact Level	Category	Rule Target	Risk / Description	Details	More Information
	FlexPod SSH and Telnet Check (Admin VDC)	icef3-sw1 (Nexus7000 C7004)	Check that only secure management methods are being used for switch administration.	Telnet is enabled on icef3-sw1 (Nexus7000 C7004). Use of non-encrypted management methods is strongly discouraged.	
	FlexPod Running Config Checks (Admin VDC)	icef3-sw1 (Nexus7000 C7004)	Checks that the Cisco Nexus Switch running-config matches its startup-config.	Command output 'show running diff' is not empty. There are unsaved changes to the switch configuration. If the switch is rebooted, the startup configuration will be loaded and these changes will be lost.	
	FlexPod Running Config Checks (Ethernet VDC)	icef3-sw1 (Nexus7000 C7004)	Checks that the Cisco Nexus Switch running-config matches its startup-config.	Command output 'show running diff' is not empty. There are unsaved changes to the switch configuration. If the switch is rebooted, the startup configuration will be loaded and these changes will be lost.	

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

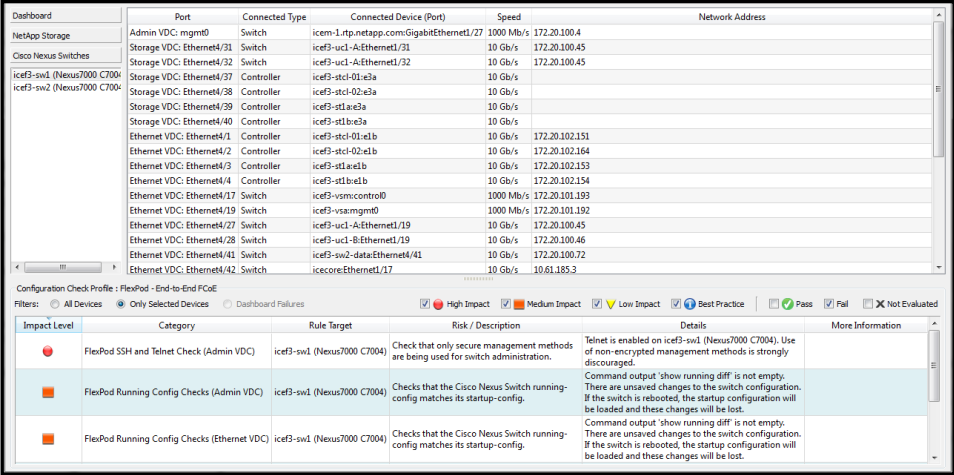
Fields	Description
	Displays that the power supply or fan works without errors

Viewing FlexPod 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 (FlexPod Results) window is displayed.

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



Dashboard	Port	Connected Type	Connected Device (Port)	Speed	Network Address
NetApp Storage	Admin VDC: mgmt0	Switch	icem-1.rtp.netapp.com:GigabitEthernet1/27	1000 Mb/s	172.20.100.4
Cisco Nexus Switches	Storage VDC: Ethernet4/31	Switch	iccf3-uc1-A:Ethernet1/31	10 Gb/s	172.20.100.45
	Storage VDC: Ethernet4/32	Switch	iccf3-uc1-A:Ethernet1/32	10 Gb/s	172.20.100.45
	Storage VDC: Ethernet4/37	Controller	iccf3-stcl-01:e3a	10 Gb/s	
	Storage VDC: Ethernet4/38	Controller	iccf3-stcl-02:e3a	10 Gb/s	
	Storage VDC: Ethernet4/39	Controller	iccf3-st1a:e3a	10 Gb/s	
	Storage VDC: Ethernet4/40	Controller	iccf3-st1b:e3a	10 Gb/s	
	Ethernet VDC: Ethernet4/1	Controller	iccf3-stcl-01:e1b	10 Gb/s	172.20.102.151
	Ethernet VDC: Ethernet4/2	Controller	iccf3-stcl-02:e1b	10 Gb/s	172.20.102.164
	Ethernet VDC: Ethernet4/3	Controller	iccf3-st1a:e1b	10 Gb/s	172.20.102.153
	Ethernet VDC: Ethernet4/4	Controller	iccf3-st1b:e1b	10 Gb/s	172.20.102.154
	Ethernet VDC: Ethernet4/17	Switch	iccf3-vsm:control0	1000 Mb/s	172.20.101.193
	Ethernet VDC: Ethernet4/19	Switch	iccf3-vsa:mgmt0	1000 Mb/s	172.20.101.192
	Ethernet VDC: Ethernet4/27	Switch	iccf3-uc1-A:Ethernet1/19	10 Gb/s	172.20.100.45
	Ethernet VDC: Ethernet4/28	Switch	iccf3-uc1-B:Ethernet1/19	10 Gb/s	172.20.100.46
	Ethernet VDC: Ethernet4/41	Switch	iccf3-sw2-data:Ethernet4/41	10 Gb/s	172.20.100.72
	Ethernet VDC: Ethernet4/42	Switch	iccf3-sw2-data:Ethernet4/41	10 Gb/s	10.61.185.3

Impact Level	Category	Rule Target	Risk / Description	Details	More Information
High	FlexPod SSH and Telnet Check (Admin VDC)	iccf3-sw1 (Nexus7000 C7004)	Check that only secure management methods are being used for switch administration.	Telnet is enabled on iccf3-sw1 (Nexus7000 C7004). Use of non-encrypted management methods is strongly discouraged.	
Medium	FlexPod Running Config Checks (Admin VDC)	iccf3-sw1 (Nexus7000 C7004)	Checks that the Cisco Nexus Switch running-config matches its startup-config.	Command output 'show running diff' is not empty. There are unsaved changes to the switch configuration. If the switch is rebooted, the startup configuration will be loaded and these changes will be lost.	
Medium	FlexPod Running Config Checks (Ethernet VDC)	iccf3-sw1 (Nexus7000 C7004)	Checks that the Cisco Nexus Switch running-config matches its startup-config.	Command output 'show running diff' is not empty. There are unsaved changes to the switch configuration. If the switch is rebooted, the startup configuration will be loaded and these changes will be lost.	

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

- Dashboard, 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.
- Navigation pane

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

- **Dashboard tab**

The Dashboard tab lists the inventory of FlexPod categorized by **Compute**, **Network**, and **Storage**. Each category has the following sections:

- **Hardware Validated**

This section checks for minimum hardware requirement as per FlexPod technical specifications ([TR-4036](#)).

- **Cabling Validated**

This section checks for minimum cabling requirement as per FlexPod technical specifications ([TR-4036](#)).

The possible values in this section are highlighted in green check mark (√) and a red cross mark (x). In case of any failure, the cross mark is displayed and upon clicking **View Details** it shows the corresponding errors.

The filter **Dashboard failures** is selected by default when you click the **View Details** link. This filter cannot be selected otherwise. To revert, select the **All Devices** filter.

- **NetApp Storage tab**

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

- **Cabling tab**

You can view the details of a controller from the nodes 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  in the **Cabling** tab and expanding the stack tree. For more information on the fields in this tab, see [Cabling tab](#).

- **System Config Summary tab**

You can view the hardware overview, module details, shelf details, and disk overview in the **System Config Summary** tab. For more information on the fields in this tab, see [System Config Summary tab](#).

- **Aggregate Info tab**

You can view the aggregate information in the **Aggregate Info** tab. For more information on the fields in this tab, see [Aggregate Info tab](#).

- **Volume Info tab**

You can view the volume information by clicking the **Volume Info** tab. For more information on the fields in this tab, see [Volume Info tab](#).

- **LUN Info tab**

You can view the LUN information by clicking the **LUN Info** tab. For more information on the fields in this tab, see [LUN Info tab](#).

- **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 (FlexPod Results)** window for Cisco Nexus Switches is as shown:

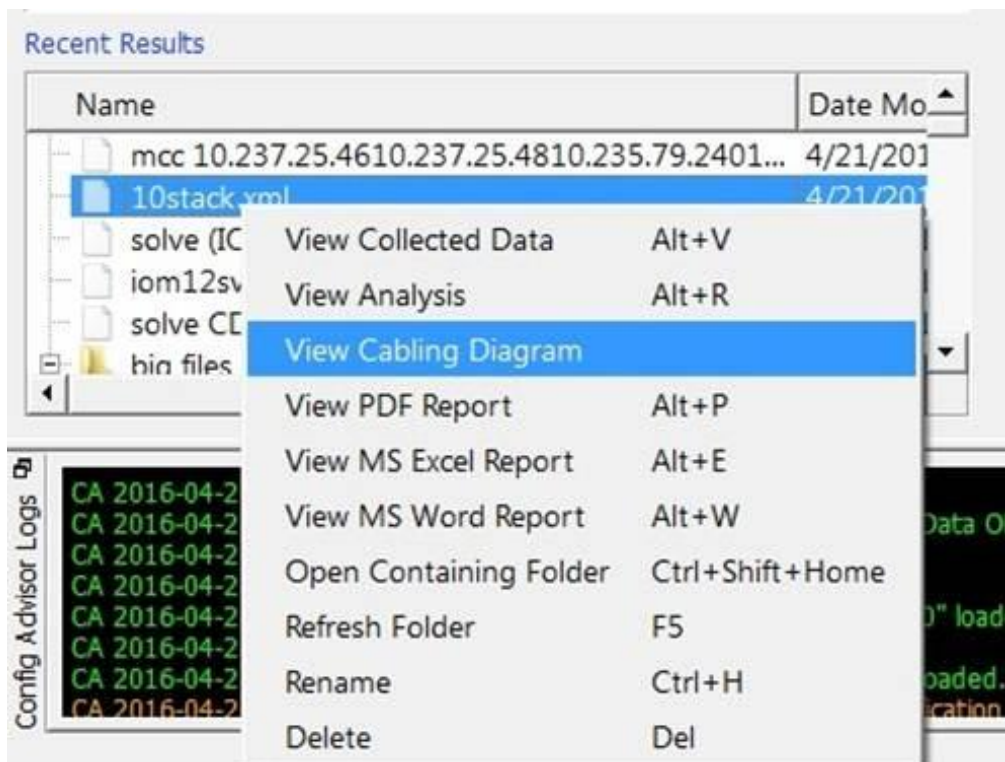
The fields in the **Cisco Nexus Switches** are as follows:

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.

Generating reports from plug-in results

You can generate PDF, MS, Word, or MS Excel reports from the Config Advisor plug-in results file, which contains the summary of the configuration and the failed checks.

In the Config Advisor main window, **Recent Results** pane, on any of the results file, right-click and select either **View PDF Report**, **View MS Excel Report**, or **View MS Word Report** to generate report of the results.



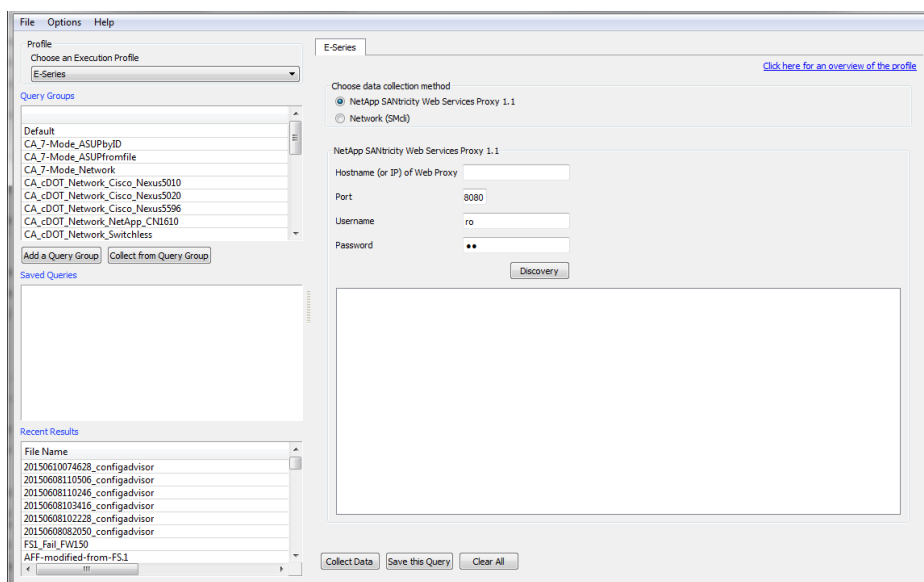
The generated reports are stored in the Config Advisor data directory under the folders pdf_files, doc_files, or excel_files.

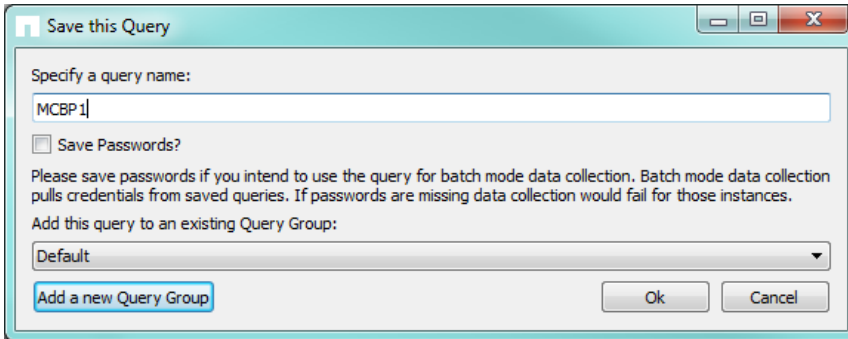
Saving plug-in credentials in Config Advisor

You can save the plug-in credentials entered for data collection for later use.

Steps

1. Enter the credentials in the plug-in page for which you want save the details, and click **Save this Query**.
2. A dialog box appears, enter the name with which the plug-in credentials have to be saved. You can specify a query name or use the default name.
3. Click **Ok**.
4. You can select the option **Save Passwords** to save the plug-in credentials with a password. The passwords are encrypted when saved.





Loading saved plug-in credentials

You can view the saved credentials query name and the associated profiles from the Config Advisor main window.

Steps

1. Navigate to the Config Advisor main window.
2. Double-click a name from the list to load the saved credentials to the specific plug-in page.
3. The **Saved Query** with the **Execution Profile** is displayed.

Query Group Content for Default Query Group

Saved Query	Execution Profile
10.96.176.135	E-Series - Network (SMcli)
Eric_24nodeCluster1	Clustered Data ONTAP
SecureASUPid	7-Mode AutoSupport Id
Rayon_Mindtech	Clustered Data ONTAP
vgv8020f129a.gdl.engla...	MCC - Cisco 9148
10.96.176.135_nopassword	E-Series - E-Series Subprofile
10.96.176.135	E-Series - E-Series Subprofile
10.96.176.136	E-Series - E-Series Subprofile
Augusta_Karnendu	Clustered Data ONTAP

4.

Note: You can right-click the query name and choose to modify or delete a saved plug-in query.

Config Advisor AutoSupport for plug-in results

If the Config Advisor AutoSupport option is enabled, then at the end of each plug-in data collection, Config Advisor sends an AutoSupport message to the NetApp AutoSupport WareHouse.

The Config Advisor AutoSupport message generated contains details of data collected by the plug-in and the computed results. The log window provides details of when the Config Advisor AutoSupport is generated and posted.

For more information on Config Advisor AutoSupport configuration, see the [Config advisor Installation and Administration Guide](#).

Upgrading Config Advisor plug-in

If a new version of Config Advisor plug-in for E-Series or Managed ONTAP SAN or MetroCluster for clustered Data ONTAP is available, when you launch Config Advisor, a notification is displayed in the tool.

You can download the new plug-in version and follow the installation steps mentioned in the [Installing Config Advisor plug-in](#) section.

The upgrade notification can be hidden for two weeks using the Remind Me Later option.

Optionally, you can check for updates from the Config Advisor **Main Menu > Help > Check for Updates**.

Uninstalling Config Advisor plug-in

You must delete the plug-in specific folder from the Config Advisor DATA directory to uninstall a Config Advisor plug-in from the host machine.

- For E-Series, plug-in folder is eseries
- For Managed ONTAP SAN, plug-in folder is ONTAP_SAN
- For MetroCluster for clustered Data ONTAP, plug-in folder is MCC_plugin

You can access the plug-in folders from the following locations:

Operating system	Config Advisor DATA directory location
Windows 7 SP1 32-bit and 64-bit	ConfigAdvisorDataDirectory_Base\ConfigAdvisorData\plugin_eggs

Periodic data collection for issues diagnostic

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

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

Note: For getting help on creating scheduled tasks, refer to MSDN articles.

Using Config Advisor through the command prompt

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

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

```
configadvisor.exe -query <absolute_path_to_the_crypt_file> [--password
<USER_DEFINED_PASSWORD> --destination <absolute_path_to_save_files_generated]
```

- -q or -query is a mandatory argument for the CLI. Here you must specify the location of the .crypt file containing the credentials saved from the plug-in profile. For details on the .crypt file, see Working with credentials in the [Config advisor Installation and Administration Guide](#).
- The query saved in the .crypt file knows which plug-in was used to create the query. The same plug-in profile is then used to determine the data collection commands and rules that require execution.
If there are more than one query within the .crypt file, data collection will not proceed and an error is displayed in the log file.
- -p or -password is a mandatory argument if the .crypt file specified as a value for -query is encrypted with a user defined password. If you do not provide the password, then it is presumed that the .crypt file was encrypted using the default password.

- `-d` or `--destination` is an optional argument. It specifies the directory location to save the collected data, PDF report, log information and AutoSupport file. AutoSupport file also contains the rule results in XML.

If the argument is not specified, `ConfigAdvisorDataDirectory_Base` is set as the destination folder.

You must ensure that the destination folder specified has sufficient space and is writable. For every instance of data collection, sub folders are created inside the destination folder before placing the result files. The sub folders are created automatically using the following format: `<ProfileName>\Year\Month\Day\Time`. For example `<destination>\MetroCluster in clustered Data ONTAP \2014\08\10\21_30\`.

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

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

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

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

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

- `ConfigAdvisorDataDirectory_Base\logs`
- `<DESTINATION_FOLDER_SPECIFIED>\<ProfileName>\Year\Month\Day\Time`

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

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

Scheduling periodic data collection

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

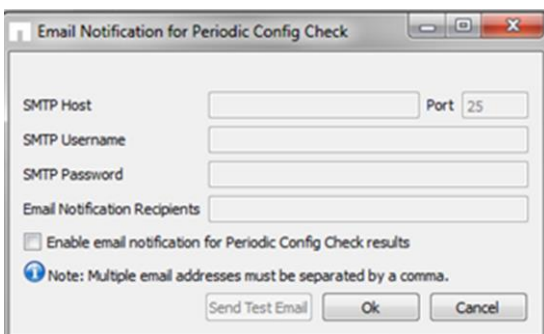
For creating a basic task or an advanced task, see Windows Task Scheduler documentation that can help you invoke the Config Advisor Command Line interface based on a predetermined schedule (for example, hourly or daily).

Email notification

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

Steps

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



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

SwitchOver Simulation

MetroCluster 1.2 supports performing switchover simulation in all of the sub profiles of MCC setup as a use case, this check can be run on any node in a cluster.

This feature ensures that all of the 10 essential checks are performed and MetroCluster setup is in a good state if disaster strikes. However, you must not run this rule with periodic data collection and also very frequently. Running this check can tentatively impair switchover capabilities (by a few minutes).

Note: Discretion is advised in using this feature.

Reporting plug-in issues in Config Advisor

You can report any issues with the Config Advisor plug-ins, from the Config Advisor **Main Menu** > **Help** > **Open Support Ticket**.

For more information on reporting in Config Advisor, see the [Config advisor Installation and Administration Guide](#).

Troubleshooting

You can find information about how to troubleshoot some of the issues that you might come across when you use the Config Advisor plug-ins. You can find details of the issue, possible cause and workaround for the issue.

Null script execution halted due to error – Smcli failed message displayed

Issue

E-Series data collection fails for the show storageArraySummary command, the Config Advisor result file does not open the ConfigAdvisor AutoSupport generation fails.

Config Advisor error for E-Series plug-in:



Possible cause

SANtricity Storage Manager is installed in the default location C:\Program Files (x86)\StorageManager on Windows 7 operating system and you do not have full administrative permissions to the C:\ drive resulting in the error.

Workaround

Option 1: Install SANtricity in a non-default location on the Windows 7 operating system.

Steps

1. Install the E-Series/EF-Series SANtricity Storage Manager 11.10.XX00.0020 on the host machine desktop or any other folder for which you have complete permissions.

Example:

2. You can install SANtricity Storage Manager in a specific folder created on the host machine.

C:\Users\<windows_login>\Desktop\SANtricity

Option 2: Modify the permissions of the default installation folder where SANtricity is installed.

Steps

1. Navigate to C:\Program Files (x86)\StorageManager, and select the folder client.
2. **Right-click** the client folder and select **Properties**.
3. In the **Properties** window, click the **Security** tab, and check if **Full control** is enabled for the specific user.
4. If the user does not have **Full control** enabled, click **Advanced**, and in the **Permissions** tab check the permissions allowed for the specific user.
5. Click **Change Permissions**, select the specific user in the **Permission** entries list, and click **Edit**.
6. In the **Permission Entry** window, select the Full control check box in the **Allow** column.
7. Click **Ok**.

E-Series data collection fails when SANtricity storage manager client is not installed

E-Series data collection failure when SANtricity Storage Manager Client is not installed is as shown:

Issue

E-Series data collection fails when SANtricity Storage Manager Client is not installed.

Possible Cause

SANtricity Storage Manager Client is not installed on the same system as Config Advisor.

Work Around

Install SANtricity Storage Manager Client by following [NetApp SANtricity web services proxy 1.1](#) section.

Appendix

E-Series configuration validation and health checks

Check name	Description
E-Series Volume Health Check	Verifies if a storage array's volume health is optimal.
E-Series Drive Health Check	Verifies if a storage array's drive health is optimal.
E-Series Hot Spare Coverage Check	Verifies if there is adequate spare drive coverage in case of fail over.
E-Series Storage Array Auto Support Check	Verifies if Auto Support is configured on the storage array.
E-Series Storage Array Health Check	Verifies the health of the storage array.
E-Series Storage Array Battery Check	Verifies the health of the cache battery.
E-Series Controller Firmware Check	Checks to ensure the Controller is at its most recent CFW level.
E-Series Thin Provisioning with SSD	Checks to ensure that E-Series Thin Provisioned Volumes are not created when SSDs are configured as a DDP.
E-Series Drive Location in DE6600	Verifies if drives are properly located by slot position within a DE6600 Enclosure.
E-Series SSD Wear Leveling	Checks SSD's lifecycle. Warns when >80% wear, recommending replacement.
FDE and Non FDE Drives co-	Verifies if FDE and Non FDE Drives are

existing in same RAID Group	configured in the same RAID Group or DDP.
E-Series Tray Loss Check	Checks for Tray Loss when using DE6600 Shelves.
E-Series Thin Provisioned Volume Check	Checks to ensure that E-Series Thin Provisioned Volumes are not created when SSDs are configured as a DDP.
E-Series Drive/Slot Location	Checks to make sure Drives are populated in the front 20 slots on DE6600.
E-Series FDE/NON-FDE Check	Verifies if FDE and Non FDE Drives are configured in the same RAID Group or DDP.

Note: The preceding section provides high-level rules and each rule has one or more triggers. For more details on the E-Series checks\triggers, visit <https://fieldportal.netapp.com/configadvisor.aspx#139861>.

E-Series hosts configuration validation and health checks

Check name	Description
E-Series Host Multipath Service	Verifies if a host multipathed service is optimal
E-Series Host Multipath Version	Verifies if a recommended host multipath service is installed
E-Series Host Multipath Configuration	Verifies if a host multipath configuration is correct
E-Series Host Multipath Configuration File	Verifies if any syntax errors in the multipath configuration file
E-Series Host Type Check	Verifies if the correct host type is selected in SANtricity Storage Manager

E-Series Host IMT Check ¹	Verifies if a host configuration is supported as per IMT
E-Series Host File System Checks	Verifies if host file systems are configured properly

¹ Because this is the first beta release of the host IMT check for E-Series, there are limited fields in IMT being checked at this point. A successful pass on this rule does NOT mean that the configuration is in total compliance with IMT. That functionality will be built out in future versions of the E-Series plug-in.

Managed ONTAP SAN configuration validation and health checks

Check name	Description
Node Health Check	Verifies the nodes are healthy and can be queried for information.
Differentiated Services and All Flash Optimized Bit Check	Verifies that all nodes have been marked for differentiated services and are Optimized for All Flash
Model Check	Verifies that all nodes are of supported models for the manage ONTAP SAN program.
Network Interfaces Check	Ensures that only SAN LIFs exist on the cluster.
Aggregates per Node Check	Verifies there are between 1 and 10 data aggregates on each node.
Aggregates at Home Check	Verifies all Aggregates are currently being serviced by their owning node.
Aggregates Utilization Check	Verifies that no aggregates exceed 75% utilization.
Aggregate Raid Group Size Check	Verifies that raid groups do not exceed 16 disks.
SSDs per Aggregate Check	Verifies that data aggregates have at least 4 SSDs.
Volumes per Node Check	Verifies no nodes owning more than 200 volumes.
Snapshots per Volume Check	Verifies no volumes have more than 40 snapshots.
Offline Dedupe with one stream maximum (runs only on 8.3.1 or later versions and earlier than 9.x versions)	Verifies Offline Dedupe is restricted to one stream.
Inline Compression is Enabled	Verifies Inline compression is enabled.
Disk Type check	Verifies all disks are of type SSD
SFO check	Verifies that all nodes have SFO enabled
SAN SVM (formerly Vserver) QOS check	Verifies QOS is enabled on all SVMs
LUNs per Node Check	Earlier than ONTAP 9.x versions: Verifies nodes

Check name	Description
	owning less than 4096 LUNs. Later than ONTAP 9.x versions: Verifies nodes owning less than 8192 LUNs.
LUN Space Allocation Check	Verifies that space-allocation is disabled for all LUNs.

Note: The preceding section provides high level rules and each rule has one or more triggers. For more details on the Managed ONTAP SAN checks\triggers, visit <https://fieldportal.netapp.com/configadvisor.aspx#139861>.

MetroCluster in clustered Data ONTAP configuration validation and health checks

Rule Name	Rule Description	2Node Direct Connect		2Node, 4Node and 8Node Fabric Configurations			
		Direct SAS	ATTO FibreBridge	Brocade		Cisco	
				NetApp Disk	Storage Array	NetApp Disk	Storage Array
Rules that run for every configuration							
PreCheck	Prepare the environment and determine checks to run.	✓	✓	✓	✓	✓	✓
Switchover_Simulate	Verifies if switchover simulation succeeds.	✓	✓	✓	✓	✓	✓
ControllerPlatformSupported	Verifies that the hardware platform is supported.	✓	✓	✓	✓	✓	✓
DrGroupSameControllerType	Verifies that all nodes in the DrGroup are of the same platform type.	✓	✓	✓	✓	✓	✓
NodeInDrGroupSameOntap	Verifies that all nodes in the DrGroup are running the same version of ONTAP.	✓	✓	✓	✓	✓	✓
DrGroupSysIdMatch	Verifies that the hardware SysID and HaSysID match, and that the node SysIds match the table SysIds.	✓	✓	✓	✓	✓	✓
DrGroupNameMatch	Verifies that the names in the tables	✓	✓	✓	✓	✓	✓

	match on all nodes.						
DrGroupBIOSFwMatch	Verifies that all nodes in the DrGroup run the same BIOS firmware.	✓	✓	✓	✓	✓	✓
DrGroupSPFwMatch	Verifies that all nodes in the DrGroup run the same Service Processor firmware.	✓	✓	✓	✓	✓	✓
HaConfigChassisControllerSetting	Verifies that the correct HAOSC setting is configured for chassis on controller	✓	✓	✓	✓	✓	✓
AdapterWithMixedHbaAndFcvipersonality	Verifies that the Quad port HBA using 2 ports in FCVI mode is only supported on the FAS8020 platform	✓	✓	✓	✓	✓	✓
StorageHba_RelatedAdapterSameSpeed	Verifies that all related adapters operate at the same speed.	✓	✓	✓	✓	✓	✓
CorrectCombinationStorage	Verifies that each adapters connecting storage are of the correct combination.	✓	✓	✓	✓	✓	✓
StorageHba_MinMaxPath	Verifies that no less than min-Path and not more than max-path HBA initiator ports are used to connect storage devices.	✓	✓	✓	✓	✓	✓

FcViAdapterSameSpeed	Verifies that all FcVI adapters operate at the same speed.	✓	✓	✓	✓	✓	✓
StackShelfCombinationSupported	Verifies that the combination of shelves in each stack is supported.	✓	✓	✓	✓	✓	✓
ShelfUniqueID	Verifies that all shelves in the DrGroup have a unique shelf ID.	✓	✓	✓	✓	✓	✓
DiskVisibleOnAllRelAdapters	Verifies that all storage devices (NetApp disk or Array LUN) are visible on all related adapters, that no failed disks, no disks with invalid serial number and no disk 'found in scan' are present.	✓	✓	✓	✓	✓	✓
AllPlexMirrored	Verifies that all plexes are mirrored.	✓	✓	✓	✓	✓	✓
AllPlexOnePoolOnly	Verifies that all plexes consist of disks from one pool only.	✓	✓	✓	✓	✓	✓
Rules that run if a fabric switch is present to connect storage							
MccConsistentOODSetting	Verifies that the OOD setting on the controllers are matching for all controllers.			X	X	X	X
SwitchGeneric_SwitchBladeSupported	Verifies that the switch and blade connecting the DR-Group(s) is supported for this			✓	✓	✓	✓

	version of ONTAP.						
SwitchGeneric_SwitchFirmwareSupported	Verifies that the switch and switch module firmware is supported for this version of ONTAP for this DrGroup.			✓	✓	✓	✓
SwitchGeneric_SwitchUniqueName	Verifies that all switches have a unique name.			✓	✓	✓	✓
SwitchGeneric_DrGroupCorrectNumberSwitches	Verifies that all controllers within the DrGroup connect to the correct number of switches.			✓	✓	✓	✓
SwitchGeneric_Topology	Verifies that all controllers within the DrGroup have a consistent view of the fabric topology.			✓	✓	✓	✓
StorageHba_ConnectedEvenlyToFabrics	Verifies that the related storage adapters evenly connect into the fabrics of blades.			✓	✓	✓	✓
FcViSamePortBothSwitches	Verifies that a FCVI Adapter in one node connects to the same ports on both switches/blades.			✓	✓	✓	✓
FCVIMaxCommonSpeed	Verifies that the FCVI adapter and switch port it is connected to is operating at the max common speed.			✓	✓	✓	✓
DiskAssignedPoolsCorrectSite	Verifies that all disks are assigned at the correct site. All disk assigned to Pool0 must be assigned to switches local the controller, all disks assigned to Pool1 must be assigned to switches at the remote site.			✓	✓	✓	✓

Rules that run if Brocade switches are found to connect storage							
SwBrocade_VfDisabled	Verify that the virtual fabric (VF) feature is disabled.			✓	✓		
SwBrocade_RoutingPolicies	Verifies that the routing in the fabric and on the controllers in the DrGroup are consistent and matching the OOD settings on the controllers.			✓	✓		
HBAEncryptionCompression	Verifies that a switch port connecting a storage initiator (HBA) port has valid Encryption and Compression settings.			✓	✓		
SwitchportToHBAFixedSpeedCheck	Verifies that a switchport connecting storage initiator (HBA) is set to fixed speed.			✓	✓		
HBADistanceSettingCheck	Verifies that a switchport connecting a storage initiator HBA has a distance setting of L0.			✓	✓		
FCVIEncryptionCompression	Verifies that a switch port connecting an FCVI interconnect port has valid Encryption and Compression settings.			✓	✓		
FCVIFixedSpeed	Verifies that a switchport connecting FCVI interconnect is set to fixed speed.			✓	✓		
FCVIDistanceOfL0	Verifies that a switchport FCVI interconnect is connected to is set			✓	✓		

	to L0 distance.						
Brocade FCSwitchISLSameDistanceModeCheck	Verifies that the ISL ports operate at the same distance mode.			✓	✓		
Brocade FCSwitchISLSameDistanceCheck	Verifies that the ISL ports operate at the same distance.			✓	✓		
Brocade FCSwitchISLPortSameSpeedCheck	Verifies that the ISL ports in one fabric operate at the same speed.			✓	✓		
Brocade FCSwitchISLPortSpeedCheck	Verifies that the ISL ports have their speed set to a fixed speed and not auto-negotiate.			✓	✓		
Brocade FCSwitchISLPortTrunkingCheck	Verifies that the ISLs are trunked.			✓	✓		
SwBrocadeISLEncryptionCompression	Verifies that the ISL ports have a valid setting for Encryption and compression.			✓	✓		
BrocadeISLQoSEnabledCheck	Verifies that all ISLs have QoS enabled and active.			✓	✓		
BrocadeISLMinSpeedCheck	Verifies that the ISL ports are operating at the minimal supported speed.			✓	✓		
NoTrafficIsolationZone	Verifies that no TrafficIsolation (TI) zone exist on any of the back-end switches.			✓	✓		
FCVIZoneCheck	Verifies that a zone exists in the effective			✓	✓		

	configuration containing all FCVI ports from one DrGroup in one fabric that this zone is a QoS zone with high priority and all zone members are represented by domain\port and not by WWN.						
Rules that run if Atto FibreBridges are found that are connected to a Brocade fabric							
AttoEncryptionCompression	Verifies that a switchport connecting ATTO FibreBridge has valid settings for Encryption and Compression.			✓			
ATTOMaxComm onSpeed	Verifies that a switchport connecting ATTO FibreBridge is set to fixed speed of 8G\16G based on the ATTO bridge type (6500N\7500N) used.			✓			
ATTODistanceof L0	Verifies that a switchport connecting ATTO FibreBridge has a distance setting of L0.			✓			
FASStorageZoningCheck	Verifies that zones exist in the effective configuration where each zone contains the correct number of storage initiator ports (this number may vary for ATO 7500N configurations and depends on the number of FC ports			✓			

	used on the FibreBridge) and one single target port connecting ATTO FibreBridge. All zone members must be represented by domain\port and not by WWN.						
Rules that run if storage arrays are found that are connected to a Brocade fabric							
VStorage ZoningCheck	Verifies that the zoning is correct to connect storage arrays.				✓		
Rules that run if ATTO FibreBridges are found							
ListOrphanedBridges	List FibreBridges that are configured in ConfigAdvisor and not seen by any node, or FibreBridges that are seen by at least one node and are not configured in ConfigAdvisor.		✓	✓		✓	
AttoFW	Verify that the ATTO bridges running the minimum required firmware.		✓	✓		✓	
AttoSpeedSetting	Verifies that the speed of the connected FC port on the Atto FibreBridge is set to fixed speed.		✓	✓			
AttoTopology	Verifies that the topology of the connected FC port on the Atto FibreBridge is set to the correct topology.		✓	✓		✓	
AttoCorrectFcPort	Verifies that the Atto FibreBridge is		✓	✓		✓	

	connected via the correct FC ports.						
AttoSNMP	Verifies SNMP feature is disabled if Atto FibreBridge is running firmware version is 1.60\1.61.		✓	✓		✓	
Rules that run if storage arrays are found							
VSeriesLicense	Verifies that if Array LUNs are connected to the controller a V_StorageAttach license is present and if one controller in the DrGroup has Array LUNS connected, then all controllers in this DrGroup require a V_StorageAttach license.				✓		✓
V_SharedInitiatorsTargets	Verifies that there are no shared HBA Initiator and target array ports or that the shared HBA and target ports is according to the guidelines for the version of ONTAP.				✓		✓

FlexPod configuration validations & health checks

Check Name	Description	Supports Cluster Mode	Supports 7-Mode
FlexPod Running Config Check	Checks that the Cisco Nexus Switch running-config matches its startup-config.	✓	✓
FlexPod SSH and Telnet Check (Cisco Nexus)	Checks that only secure management methods are being used for switch administration.	✓	✓
FlexPod SSH and Telnet Check (Storage)	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	Checks if LACP is enabled on the switches. LACP and Virtual Port Channels are used on the Cisco Nexus switches to provide redundant connectivity within the FlexPod.	✓	✓
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 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 or storage virtual machine). Checks that only secure management methods are being used for storage controller administration.	✓	✓

Check Name	Description	Supports Cluster Mode	Supports 7-Mode
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 that 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 Cisco Nexus 5k switches (using CDP).	✓	✓
FlexPod Storage Protocols Check	Checks that storage protocols features are enabled: fcoe, npiv, fport-channel-trunk.	✓	✓
FlexPod FCP Check (Storage)	Checks 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 Cisco Nexus 5k switches (using CDP)	✓	✓
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: 1. Check for missing CoS value 2. Check for missing class-fcoe in network-qos, Queuing policy 3. Check for 'mtu 2158' for FCoE	✓	✓

Check Name	Description	Supports Cluster Mode	Supports 7-Mode
FlexPod Chassis Discovery Policy	Checks the chassis discovery policy. 1. Checks for aggregate links 2. Checks for at least 2-link	✓	✓
FlexPod FEX Uplink Check	Checks that each FEX has at least 2 10GbE uplinks to the fabric interconnect	✓	✓
FlexPod Device Online	Checks that the FlexPod devices were online and data collection successful.	✓	✓
FlexPod Redundant Cisco Nexus Switch	Exactly 2 Cisco Nexus 5000 or 7000 series switches (must be same model)	✓	✓
FlexPod Redundant FAS	Checks for FAS controllers in HA pair	✓	✓
FlexPod UCS Server Config	Checks for at least 1 blade chassis with at least 2 blades or at least 2 Fabric Extenders with at least 2 servers	✓	✓
FlexPod UCS IO Module Check	Blade Chassis requires exactly 2 IO modules.	✓	✓
FlexPod Storage FC Uplinks	FAS must be directly connected to Cisco Nexus using Fibre Channel links	✓	✓
FlexPod Jumbo Frames	Ensures jumbo frames are enabled on the Cisco Nexus switches	✓	✓
FlexPod Redundant UCS-FI Check	Exactly 2 UCS fabric interconnects in cluster (HA) relationship.	✓	✓
FlexPod Cisco Nexus vPC Peer Link	Checks that Cisco Nexus switches has a working peer-link for vPC failover traffic. At least 2 10GbE links must be connected between the two Cisco Nexus switches in a port channel for use as a vPC peer-link.	✓	✓
FlexPod SAN Boot Features	Ensures features necessary for SAN boot are licensed and enabled on the Cisco Nexus switches.	✓	✓
FlexPod UCS Server KVM Addresses	Check that there is a KVM IP address pool with at least as many addresses as KVM-IP-less blades in the environment	✓	✓

Check Name	Description	Supports Cluster Mode	Supports 7-Mode
FlexPod FC Zoning Check	Ensures that FC zones are configured correctly. 1. Check the initiator WWPN is zoned in Cisco Nexus 2. Check for the initiator WWPN is part of the igroup 3. Check for active zonesets 4. Check for 1 initiator WWPN present in a zone 5. Check for LUN is mapped and online 6. Check for 2 initiators are present in igroup	✓	✓
FlexPod Firmware recommendations (All components)	All components must be running at least the minimum validated software versions.	✓	✓
FlexPod UCS Ethernet End-Host Mode	UCS must be configured in End-Host mode for Ethernet	✓	✓
FlexPod VLAN Correlation Check	Checks that allowed VLAN lists are consistent across the infrastructure.	✓	✓
FlexPod Cisco Nexus VSAN-FCoE VLAN Mapping Check	Each Cisco Nexus switch must have a VSAN configured for the respective Fabric and FCoE vlan mapped to it	✓	✓
FlexPod VFC-FCoE UCS-FI Port Channel Binding Check	A vfc interface must be binded to the fcoe port-channel between the Cisco Nexus and the FI and the VFC interface should be assigned to the Fabric in the vsan database	✓	✓
FlexPod VFC-Storage Interface Binding Check	A vfc interface must be bound to all the Ethernet interfaces that are connected to the Storage, the VFC interfaces should have the Fabric vsan as the allowed VSAN and the VFC interface should be assigned to Fabric in vsan database	✓	✓
FlexPod VFC-Storage Interface Binding Check	A vfc interface must be bound to all the Ethernet interfaces that are connected to the Storage, the VFC interfaces should have the Fabric vsan as the allowed VSAN and the VFC interface should be assigned to Fabric in vsan database	✓	✓

Check Name	Description	Supports Cluster Mode	Supports 7-Mode
FlexPod vPC Peer-Link no FCoE VLAN Check	The FCoE VLAN in each Cisco Nexus should not be in the allowed VLANs list in the vPC peer-link port-channel	✓	✓
FlexPod Cisco Nexus-FI FCoE Port Channel-no vPC Check	The fcoe port-channel between the Cisco Nexus and the FI should not be configured as a vpc	✓	✓
FlexPod UCS FCoE Uplink Ports Check	For FCoE traffic, a minimum of 2 interfaces must be configured as FCoE Uplink Ports in each FI and Admin State of the interfaces must be Enabled	✓	✓
FlexPod UCS VSAN-FCoE VLAN Mapping Check	Each FI must have a VSAN configured for the respective Fabric and FCoE vlan should be mapped to it	✓	✓
FlexPod UCS VSAN-FCoE VLAN Mapping Check	Each FI must have a VSAN configured for the respective Fabric and FCoE vlan should be mapped to it	✓	✓
FlexPod UCS-FI FCoE Port-Channel Check	Each FI must have a FCoE Port-channel configured	✓	✓
FlexPod UCS FCoE Uplink Check	Each FI must uplink into the northbound Cisco Nexus in the same FCoE Fabric	✓	✓
FlexPod Cisco Nexus Spanning Tree Portfast Check	The end-host ports should have the spanning tree portfast feature to enable Bridge assurance	✓	✓
FlexPod Running Config Check (Admin VDC)	Checks that the running-config matches its startup-config.	✓	✓
FlexPod Running Config Check (Ethernet VDC)	Checks that the running-config matches its startup-config.	✓	✓
FlexPod Running Config Check (Storage VDC)	Checks that the running-config matches its startup-config.	✓	✓
FlexPod SSH and Telnet Check (Admin VDC)	Check that only secure management methods are being used for switch administration.	✓	✓
FlexPod SSH and Telnet Check (Ethernet VDC)	Check that only secure management methods are being used for switch administration.	✓	✓

Check Name	Description	Supports Cluster Mode	Supports 7-Mode
FlexPod SSH and Telnet Check (Storage VDC)	Check that only secure management methods are being used for switch administration.	✓	✓
FlexPod LACP Check (Ethernet VDC)	Checks if LACP is enabled on Ethernet VDC of the switches.	✓	✓
FlexPod LACP Check (Storage VDC)	Checks if LACP is enabled on Ethernet VDC of the switches.	✓	✓
FlexPod VPC Check (Ethernet VDC)	Checks if VPC is enabled on the Ethernet VDC of switches. Virtual Port Channels are used on the Nexus switches to provide redundant connectivity within the FlexPod.	✓	✓
FlexPod UDLD Check	Checks if UDLD is enabled on Ethernet VDC of the switches.	✓	✓
FlexPod Nexus 7K 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 Nexus 7K Storage Protocols Check	Checks that storage protocols features are enabled: fcoe, npiv, lldp.	✓	✓
FlexPod Jumbo Frames Check	Ensures jumbo frames are enabled on the Nexus switches.	✓	✓
FlexPod Nexus 7K vPC Peer Link Check	The Nexus switches must have a working peer-link for vPC failover traffic. At least 2 10GbE links must be connected between the two Nexus switches in a port channel for use as a vPC	✓	✓
FlexPod Nexus 7000 - FCoE VLAN allowed on the vFC port-channel between Nexus and UCS FI check	The FCoE vlan should be allowed in vFC port channel between Nexus and UCS FI	✓	✓
FlexPod Nexus 7000 - UCS FI FCoE port channel bound to vFC port channel check	The FCoE port-channel should be bound to a vFC port channel between Nexus and UCS FI	✓	✓

Check Name	Description	Supports Cluster Mode	Supports 7-Mode
FlexPod Nexus 7000 - vFC port-channel between Nexus and UCS FI added to vsan database check	The vFC port-channel between Nexus and UCS FI should be added to VSAN database	✓	✓
FlexPod Nexus 7000 Ethernet VDC Check	The Nexus Switch must have an Ethernet VDC	✓	✓
FlexPod Nexus 7000 Ethernet VDC Interfaces Check	A minimum of eight Ethernet interfaces have to be allocated to the Ethernet VDC to facilitate all the configurations	✓	✓
FlexPod Nexus 7000 F2-series module license check	F2-series module should be licensed to use FCoE	✓	✓
FlexPod Nexus 7000 FCoE QoS check	Check for system wide FCoE QoS and define the QoS policy to be used	✓	✓
FlexPod Nexus 7000 F-series module Compliance Check	The Ethernet VDC should be compliant for F-series module(s) being used	✓	✓
FlexPod Nexus 7000 global FCoE feature-set check	Check for FCoE feature-set installed globally	✓	✓
FlexPod Nexus 7000 Global MTU Check	The Ethernet VDC in the Nexus Switch must be enabled for jumbo frame support	✓	✓
FlexPod Nexus 7000 spanning tree defaults check	The spanning tree defaults should be enabled on Ethernet VDC to enable Bridge assurance	✓	✓
FlexPod Nexus 7000 spanning tree portfast enabled on ports connected to FAS storage check	The end-host ports should have the spanning tree portfast feature to enable Bridge assurance	✓	✓
FlexPod Nexus 7000 Storage Switch Network Correlation Check	Check each storage controller is directly connected to each Nexus switch	✓	✓
FlexPod Nexus 7000 Storage VDC Check	The Nexus Switch must have a Storage VDC	✓	✓

Check Name	Description	Supports Cluster Mode	Supports 7-Mode
FlexPod Nexus 7000 Storage VDC fcoe feature-set Check	Checks if the FCoE feature-set is enabled in the Storage VDC	✓	✓
FlexPod Nexus 7000 Storage VDC FCoE VLAN Check	There must be a FCoE VLAN configured in the Storage VDC of the Nexus Switch	✓	✓
FlexPod Nexus 7000 Storage VDC FCoE VLAN range Check	A FCoE VLAN has to be allocated to the Storage VDC	✓	✓
FlexPod Nexus 7000 Storage VDC FCoE VSAN Check	The Storage VDC VSAN must be set as the FCoE VSAN in the Nexus Switch	✓	✓
FlexPod Nexus 7000 Storage VDC Interfaces Check	A minimum of four Ethernet interfaces have to be allocated to the Storage VDC to facilitate all the configurations.	✓	✓
FlexPod Nexus 7000 Storage VDC VLAN FCoE VSAN Mapping Check	The IDs of the FCoE VLAN and VSAN must be the same in the Storage VDC of the Nexus Switch	✓	✓
FlexPod Nexus 7000 Storage VDC VSAN Check	The Storage VDC in the Nexus Switch must have a VSAN configured	✓	✓
FlexPod Nexus 7000 Switch Storage Portchannel MTU Check	The Ethernet Portchannels between the Ethernet VDC of the Nexus Switch and NetApp Storage must have an MTU value of 9216	✓	✓
FlexPod Nexus 7000 Switch UCS FCoE Uplink Check	Each FI must uplink into Storage VDC of the northbound Nexus7000 switch in the same FCoE Fabric	✓	✓
FlexPod Nexus 7000 Switch UCS Portchannel MTU Check	The Ethernet Portchannels between the Ethernet VDC of the Nexus Switch and Cisco UCS Fabric Interconnects must have a MTU value of 9216	✓	✓
FlexPod UCS Nexus 7000 Switch Network Correlation Check	Checks that fabric interconnect has an uplink port channel connected to a Virtual Port Channel (vPC) on the Nexus 7K switches (using CDP)	✓	✓

Check Name	Description	Supports Cluster Mode	Supports 7-Mode
FlexPod Cisco UCS C-Series Server Connectivity Check	C-Series servers can be connected to the Fabric Interconnects either directly or via a pair of Fabric Extenders. While running UCS Manager version lower than 2.2 the servers can only be connected via the Fabric Extenders."	✓	✓
FlexPod FAS8000-UTA2 Port Mode Check	The UTA2 ports type must be in 'fc' mode and in 'target' type to support the 'Classic FCP to the storage controller' SAN boot architecture.	✓	✓
FlexPod UCS iSCSI Initiators in Storage igroup Check	Check if the UCS initiators are present in storage igroup	✓	
FlexPod Storage iSCSI Feature Check	Check if iSCSI is licensed and enabled on the controller.	✓	
FlexPod Storage iSCSI LUN Map Check	Check if LUN is provisioned and mapped to igroup.	✓	
FlexPod Lifecycle Management	Check if running configuration is supported as per NetApp Interoperability Matrix Tool .	✓	
FlexPod FCoE Storage Port check – Direct attach UCS	Check if Cisco UCS Fabric Interconnect should have a minimum of 2 ports configured as FCoE storage ports.		✓
FlexPod FCoE Uplinks – Direct attach UCS	Minimum of 2 FCoE links from each NetApp FAS storage node should be directly connected to Cisco UCS Fabric Interconnect.		✓
FlexPod UCS FC switching Mode – Direct attach UCS	Ensure the Cisco UCS Fabric Interconnect is in FC switching mode.		✓
FlexPod FC Storage Port check – Direct attach UCS	Cisco UCS Fabric Interconnect should have a minimum of 2 ports configured as FC storage ports.		✓
FlexPod FC Uplinks – Direct attach UCS	Minimum of 2 FC links from each NetApp FAS storage node should be directly connected to Cisco UCS Fabric Interconnect.		✓
FlexPod UCS FC switching Mode – Direct attach UCS	Ensure the Cisco UCS Fabric Interconnect is in FC switching mode.		✓

Check Name	Description	Supports Cluster Mode	Supports 7-Mode
FlexPod – UCS Service profile iSCSI vNIC(s) presence Check	Checks the UCS service profile for HA configuration on the iSCSI vNICs. (Either failover or multipath).	✓	
FlexPod Nexus no fabricpath feature check	Checks the UCS service profile boot policy is configured with type “iSCSI.”	✓	
Cisco Nexus VPC Domain Feature check	Each Cisco Nexus switch must have the VPC Domain features enabled.	✓	
FlexPod UCS - iSCSI vNIC target check	Checks the UCS iSCSI vNIC A and B has same target name.	✓	
FlexPod UCS iSCSI boot policy check	Checks the UCS service profile boot policy is configured with type “iSCSI.”	✓	

Copyright information

Copyright © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S

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

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

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

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

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

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

Trademark information

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

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

How to send your comments

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

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

You can also contact us in the following ways:

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