Configuring CFS

This chapter describes how to use Cisco Fabric Services (CFS), a Cisco proprietary feature that distributes data, including configuration changes, to all Cisco NX-OS devices in a network.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

About CFS

You can use Cisco Fabric Services (CFS) to distribute and synchronize a configuration on one Cisco device with all other Cisco devices in your network. CFS provides you with consistent and, in most cases, identical configurations and behavior in your network.

Applications that Use CFS to Distribute Configuration Changes

CFS distributes configuration changes for the applications listed in the following table.

Table 1: CFS-Supported Applications

Application	Default State
Device alias	Enabled
DPVM	Enabled
FC domain	Disabled
FC port security	Disabled
FC timer	Disabled
IVR	Disabled
NTP	Disabled
RADIUS	Disabled
RSCN	Disabled
Smart Call Home	Disabled
TACACS+	Disabled
User roles	Disabled

CFS Distribution

CFS distributes configuration changes to multiple devices across a complete network. CFS supports the following types of distribution:

- CFS over Ethernet (CFSoE)—Distributes application data over an Ethernet network.

- CFS over IP (CFSoIP)—Distributes application data over an IPv4 network.

- CFS over Fibre Channel (CFSoFC)—Distributes application data over a Fibre Channel, such as a virtual storage area network (VSAN). If the device is provisioned with Fibre Channel ports, CFSoFC is enabled by default.

  Beginning with Cisco NX-OS Release 5.2, you can configure Fibre Channel over Ethernet (FCoE), which allows Fibre Channel traffic to be encapsulated over a physical Ethernet link. To run FCoE on a Cisco Nexus 7000 Series switch, you must configure a dedicated storage virtual device context (VDC). If FCoE is enabled on the device, CFSoFC services can be used. The applications that require CFS distribution to be enabled in the storage VDC are noted in the configuration instructions throughout this chapter. For more information on FCoE and storage VDCs, see the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500* and the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide.

Note All of the information in this chapter applies to both CFSoIP and CFSoFC, unless otherwise noted.

CFS Distribution Modes

CFS supports three distribution modes to accommodate different feature requirements. Only one mode is allowed at a given time.

- Uncoordinated distributions—Distribute information that is not expected to conflict with that from a peer. Parallel uncoordinated distributions are allowed for an application.

- Coordinated distributions—Distribute information that can be manipulated and distributed from multiple devices (for example, the port security configuration). Coordinated distributions allow only one application distribution at a given time. CFS uses locks to enforce this. A coordinated distribution is not allowed to start if locks are acquired for the application anywhere in the network. A coordinated distribution consists of three stages:

    - A network lock is acquired.

    - The configuration is distributed and committed.

    - The network lock is released.

  CFS can execute these stages in response to an application request without intervention from the application or under complete control of the application.

- Unrestricted uncoordinated distributions—Allow multiple parallel distributions in the network in the presence of an existing coordinated distribution. Unrestricted uncoordinated distributions are allowed to run in parallel with all other types of distributions.

CFS Connectivity in a Mixed Fabric

CFS is an infrastructure component that also runs on the Cisco Nexus 7000 Series switches, Cisco Nexus 5000 Series switches, and Cisco MDS 9000 switches. A mixed fabric of different platforms (such as the Cisco Nexus 9000 Series, Cisco Nexus 7000 Series, Cisco Nexus 5000 Series, and Cisco MDS 9000 switches) can interact with each other.

Using CFSoIP, the respective CFS clients can also talk to their instances running on the other platforms. Within a defined domain and distribution scope, CFS can distribute the client's data and configuration to its peers running on other platforms.

All three platforms support both CFSoIP and CFSoFC. However, the Cisco Nexus 7000 Series and Cisco Nexus 5000 Series switches require an FC or FCoE plugin and corresponding configuration in order for CFSoFC to operate. Both options are available by default on the Cisco MDS 9000 switches.

Note Some applications are not compatible with their instances running on different platforms. Therefore, Cisco recommends that you carefully read the client guidelines for CFS distribution before committing the configuration.

For more information on CFS for the Cisco Nexus 7000 Series, Cisco Nexus 5000 Series, and Cisco MDS 9000 switches, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*, *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide*, and *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*, respectively.

CFS Merge Support

An application keeps the configuration synchronized in the fabric through CFS. When two such fabrics become reachable to one another, CFS triggers a merge. These two fabrics could have two different sets of configuration information that need to be reconciled in the event of a merge. CFS provides notification each time an application peer comes online. If a fabric with M application peers merges with another fabric with N application peers and if an application triggers a merge action on every notification, a link-up event results in MxN merges in the fabric.

CFS supports a protocol that reduces the number of merges required to one by handling the complexity of the merge at the CFS layer. This protocol runs per application per scope. The protocol involves selecting one device in a fabric as the merge manager for that fabric. The other devices do not have a role in the merge process.

During a merger of two networks, their designated managers exchange configuration databases. The application on one of them merges the databases, decides if the merge is successful, and notifies all other devices.

In the merge is successful, the merged database is distributed to all devices in the combined fabric, and the entire new fabric remains in a consistent state.

Locking the Network

When you configure an application that uses the CFS infrastructure, that application starts a CFS session and locks the network. When a network is locked, the device software allows configuration changes to this application only from the device holding the lock. If you make configuration changes to the application from another device, the device issues a message to inform the user about the locked status. The configuration changes are held in a pending database by that application.

If you start a CFS session that requires a network lock but forget to end the session, an administrator can clear the session. If you lock a network at any time, your username is remembered across restarts and switchovers. If another user (on the same machine) tries to perform configuration tasks, that user's attempts are rejected.

CFS Regions

A CFS region is a user-defined subset of devices for a given feature or application. You usually define regions to localize or restrict distribution based on devices that are close to one another. When a network covers many geographies with many different administrators who are responsible for subsets of devices, you can manage the scope of an application by setting up a CFS region.

CFS regions are identified by numbers ranging from 0 through 200. Region 0 is reserved as the default region and contains every device in the network. You can configure regions from 1 through 200.

Note   If an application is moved (that is, assigned to a new region), its scope is restricted to that region, and it ignores all other regions for distribution or merging purposes. The assignment of the region to an application has precedence in distribution over its initial scope.

You can configure a CFS region to distribute configurations for multiple applications. However, on a given device, you can configure only one CFS region at a time to distribute the configuration for a given application. Once you assign an application to a CFS region, its configuration cannot be distributed within another CFS region.

High Availability

Stateless restarts are supported for CFS. After a reboot or a supervisor switchover, the running configuration is applied. For more information on high availability, see the *Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*.

Prerequisites for CFS

CFS has the following prerequisites:

- CFS is enabled by default. All devices in the fabric must have CFS enabled, or they do not receive distributions.

- If CFS is disabled for an application, that application does not distribute any configuration, and it does not accept a distribution from other devices in the fabric.

Guidelines and Limitations for CFS

CFS has the following configuration guidelines and limitations:

- If the virtual port channel (vPC) feature is enabled for your device, do not disable CFSoE.

Note CFSoE must be enabled for the vPC feature to work.

- All CFSoIP-enabled devices with similar multicast addresses form one CFSoIP fabric.

- Make sure that CFS is enabled for the applications that you want to configure.

- Anytime you lock a fabric, your username is remembered across restarts and switchovers.

- Anytime you lock a fabric, configuration changes attempted by anyone else are rejected.

- While a fabric is locked, the application holds a working copy of configuration changes in a pending database or temporary storage area, not in the running configuration.

- Configuration changes that have not been committed yet (still saved as a working copy) are not in the running configuration and do not display in the output of **show** commands.

- If you start a CFS session that requires a fabric lock but forget to end the session, an administrator can clear the session.

- An empty commit is allowed if configuration changes are not previously made. In this case, the **commit** command results in a session that acquires locks and distributes the current database.

- You can use the **commit** command only on the specific device where the fabric lock was acquired.

- CFSoIP and CFSoE are not supported for use together.

- CFS regions can be applied only to CFSoIP applications.

- You cannot distribute the user role configuration between a Cisco MDS 9500 Series switch and the storage VDC configured for a Cisco Nexus 7000 Series switch. To prevent this distribution, make sure to assign the user role configuration in Cisco MDS and the Cisco Nexus 7000 storage VDC to different CFS regions.

- CFS uses the same MAC address 01:80:c2:00:00:0e as the standard IEEE protocol Link Layer Discovery Protocol (LLDP), and sniffer software such as Ethanalyzer or Wireshark decodes CFS traffic as LLDP traffic.

Default Settings for CFS

Table 2: Default CFS Parameters

Parameters	Default
CFS distribution on the device	Enabled
CFSoIP	Disabled
IPv4 multicast address	239.255.70.83
CFSoFC	Enabled, if FCoE is present
CFSoE	Disabled

Configuring CFS Distribution

Enabling CFS Distribution for Applications

Enabling CFS to Distribute Smart Call Home Configurations

You can enable CFS to distribute Call Home configurations to all Cisco NX-OS devices in the network. The entire Call Home configuration is distributed except the device priority and the sysContact names.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **callhome**	Enters Call Home configuration mode.
Step 3	switch(config-callhome)# **distribute**	Enables CFS to distribute Smart Call Home configuration updates.

	Command or Action	**Purpose**
Step 4	(Optional) switch(config-callhome)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 5	(Optional) switch(config-callhome)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# distribute
switch(config-callhome)# show callhome status
Distribution : Enabled
switch(config-callhome)# copy running-config startup-config
```

Enabling CFS to Distribute Device Alias Configurations

You can enable CFS to distribute device alias configurations in order to consistently administer and maintain the device alias database across all Cisco NX-OS devices in the fabric.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **device-alias distribute**	Enables CFS to distribute device alias configuration updates.
Step 3	(Optional) switch(config)# **show cfs application**	Displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute device alias configurations:

```
switch(config)# device-alias distribute
switch(config)# show cfs application
----------------------------------------------
Application Enabled Scope
----------------------------------------------
```

```
device-alias Yes Physical-fc
switch(config)# copy running-config startup-config
[#######################################] 100%
```

Enabling CFS to Distribute DPVM Configurations

You can enable CFS to distribute dynamic port VSAN membership (DPVM) configurations in order to consistently administer and maintain the DPVM database across all Cisco NX-OS devices in the fabric.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Make sure that you enable the DPVM feature. To do so, use the **feature dpvm** command.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **dpvm distribute**	Enables CFS to distribute DPVM configuration updates.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute DPVM configurations:

```
switch(config)# dpvm distribute
switch(config)# show dpvm status
Distribution is enabled.
switch(config)# copy running-config startup-config
[#######################################] 100%
```

Enabling CFS to Distribute FC Domain Configurations

You can enable CFS to distribute Fibre Channel (FC) domain configurations in order to synchronize the configuration across the fabric from the console of a single Cisco NX-OS device and to ensure consistency in the allowed domain ID lists on all devices in the VSAN.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **fcdomain distribute**	Enables CFS to distribute FC domain configuration updates.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute FC domain configurations:

```
switch(config)# fcdomain distribute
switch(config)# show fcdomain status
fcdomain distribution is enabled
switch(config)# copy running-config startup-config
[#######################################] 100%
```

Enabling CFS to Distribute FC Port Security Configurations

You can enable CFS to distribute Fibre Channel (FC) port security configurations in order to provide a single point of configuration for the entire fabric in the VSAN and to enforce the port security policies throughout the fabric.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Make sure that you enable the FC port security feature. To do so, use the **feature fc-port-security** command.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **fc-port-security distribute**	Enables CFS to distribute FC port security configuration updates.
Step 3	(Optional) switch(config)# **show cfs application**	Displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute FC port security configurations:

```
switch(config)# fc-port-security distribute
switch(config)# show cfs application
----------------------------------------
Application Enabled Scope
----------------------------------------
fc-port-securi Yes Logical
switch(config)# copy running-config startup-config
[#####################################] 100%
```

Enabling CFS to Distribute FC Timer Configurations

You can enable CFS to distribute Fibre Channel (FC) timer configurations for all Cisco NX-OS devices in the fabric.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **fctimer distribute**	Enables CFS to distribute FC timer configuration updates.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute FC timer configurations:

```
switch(config)# fctimer distribute
switch(config)# show fctimer status
Distribution : Enabled
switch(config)# copy running-config startup-config
[#####################################] 100%
```

Enabling CFS to Distribute IVR Configurations

You can enable CFS to distribute inter-VSAN routing (IVR) configurations in order to enable efficient IVR configuration management and to provide a single point of configuration for the entire fabric in the VSAN.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Make sure that you enable the IVR feature. To do so, use the **feature ivr** command.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **ivr distribute**	Enables CFS to distribute IVR configuration updates.
		Note You must enable IVR distribution on all IVR-enabled switches in the fabric.
Step 3	(Optional) switch(config)# **show cfs application**	Displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute IVR configurations:

```
switch(config)# ivr distribute
switch(config)# show cfs application
----------------------------------------------
Application Enabled Scope
----------------------------------------------
ivr Yes Physical-fc
switch(config)# copy running-config startup-config
[#######################################] 100%
```

Enabling CFS to Distribute NTP Configurations

You can enable CFS to distribute NTP configurations to all Cisco NX-OS devices in the network.

Before you begin

Make sure that you enable the NTP feature (using the **feature ntp** command).

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **ntp distribute**	Enables CFS to distribute NTP configuration updates.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# ntp distribute
switch(config)# show ntp status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

Enabling CFS to Distribute RADIUS Configurations

You can enable CFS to distribute RADIUS configurations to all Cisco NX-OS devices in the network.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **radius distribute**	Enables CFS to distribute RADIUS configuration updates.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# radius distribute
switch(config)# show radius status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

Enabling CFS to Distribute RSCN Configurations

You can enable CFS to distribute registered state change notification (RSCN) configurations to all Cisco NX-OS devices in the fabric.

Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **rscn distribute**	Enables CFS to distribute RSCN configuration updates.
Step 3	(Optional) switch(config)# **show cfs application**	Displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable CFS to distribute RSCN configurations:

```
switch(config)# rscn distribute
switch(config)# show cfs application
----------------------------------------------
Application Enabled Scope
----------------------------------------------
rscn Yes Logical
switch(config)# copy running-config startup-config
[########################################] 100%
```

Enabling CFS to Distribute TACACS+ Configurations

You can enable CFS to distribute TACACS+ configurations to all Cisco NX-OS devices in the network.

Before you begin

Make sure that you enable the TACACS+ feature (using the **feature tacacs+** command).

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **tacacs+ distribute**	Enables CFS to distribute TACACS+ configuration updates.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.

	Command or Action	**Purpose**
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# tacacs+ distribute
switch(config)# show tacacs+ status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

Enabling CFS to Distribute User Role Configurations

You can enable CFS to distribute user role configurations to all Cisco NX-OS devices in the network.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **role distribute**	Enables CFS to distribute user role configurations.
Step 3	(Optional) switch(config)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# role distribute
switch(config)# show role status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

Specifying a CFS Distribution Mode

You can specify and enable an Ethernet or IPv4 CFS distribution mode.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **cfs {eth	ipv4} distribute**	Globally enables CFS distribution over Ethernet or IPv4 for all applications on the device.
Step 3	(Optional) switch(config)# **show cfs status**	Shows the current state of CFS, including the distribution mode.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# cfs ipv4 distribute
switch(config)# show cfs status
Distribution : Enabled
Distribution over IP : Disabled
Distribution over Ethernet : Enabled
switch(config)# copy running-config startup-config
```

Configuring an IP Multicast Address for CFSoIP

For CFS protocol-specific distributions, such as the keepalive mechanism for detecting network topology changes, use the IP multicast address to send and receive information. You can configure the IP multicast address used to distribute CFSoIPv4.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no cfs ipv4 distribute**	Globally disables CFSoIP distribution for all applications on the device.
		Note You must disable CFSoIP before you can change the multicast address.
Step 3	switch(config)# **cfs ipv4 mcast-address** *ip-address*	Configures the multicast address for CFS distribution over IPv4. The ranges of valid IPv4 addresses are 239.255.0.0 through 239.255.255.255 and 239.192/16 through 239.251/16.
Step 4	switch(config)# **cfs ipv4 distribute**	Globally enables CFSoIP distribution for all applications on the device.
Step 5	(Optional) switch(config)# **show cfs status**	Shows the current state of CFS, including whether it is enabled, its IP mode, and its multicast addresses.

	Command or Action	Purpose
Step 6	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# no cfs ipv4 distribute
This will prevent CFS from distributing over IPv4 network.
Are you sure? (y/n) [n] y
switch(config)# cfs ipv4 mcast-address 239.255.1.1
Distribution over this IP type will be affected
Change multicast address for CFS-IP?
Are you sure? (y/n) [n] y
switch(config)# cfs ipv4 distribute
switch(config)# show cfs status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.1.1
switch(config)# copy running-config startup-config
```

Configuring CFS Regions

Creating a CFS Region

You can create a CFS region and add an application, such as Smart Call Home, to it.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)#**cfs region** *region-number*	Creates the region and enters the configuration mode for the specified region.
Step 3	switch(config-cfs-region)#*application-name*	For the specified region, adds the named application.
Step 4	(Optional) switch(config-cfs-region)#**show cfs regions brief**	Shows all configured regions and applications but does not show peers.
Step 5	(Optional) switch(config-cfs-region)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# cfs region 4
```

```
switch(config-cfs-region)# callhome
switch(config-cfs-region)# show cfs regions brief
-------------------------------------
Region Application Enabled
-------------------------------------
4      callhome    yes
switch(config-cfs-region)# copy running-config startup-config
```

Moving an Application to a Different CFS Region

You can move an application to a different region. For example, you can move NTP from region 1 to region 2.

Note   When you move an application, its scope is restricted to the new region. It ignores all other regions for distribution or merging purposes.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **cfs region** *region-number*	Enters the configuration mode for the specified region.
Step 3	Required: switch(config-cfs-region)# *application-name*	Specifies the applications to be moved.
Step 4	(Optional) switch(config-cfs-region)# **show cfs regions name** *application-name*	Displays peers and region information for a given application.
Step 5	(Optional) switch(config-cfs-region)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# cfs region 2
switch(config-cfs-region)# callhome
switch(config-cfs-region)# show cfs regions name callhome
Region-ID : 2
Application: callhome
Scope : Physical-fc-ip
-------------------------------------------------------------------------
Switch WWN IP Address
-------------------------------------------------------------------------
20:00:00:22:55:79:a4:c1 172.28.230.85 [Local]
switch
Total number of entries = 1
switch(config-cfs-region)# copy running-config startup-config
```

Removing an Application from a CFS Region

You can remove an application from a region. Removing an application from a region is the same as moving the application back to the default region. The default region is usually region 0. This action brings the entire fabric into the scope of distribution for the application.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **cfs region** *region-number*	Enters the configuration mode for the specified region.
Step 3	Required: switch(config-cfs-region)# **no** *application-name*	Removes the specified application from the region.
Step 4	(Optional) Repeat Step 3 for each application that you want to remove from this region.	
Step 5	(Optional) switch(config-cfs-region)# **show cfs regions brief**	Shows all configured regions and applications but does not show peers.
Step 6	(Optional) switch(config-cfs-region)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# cfs region 2
switch(config-cfs-region)# no ntp
switch(config-cfs-region)# show cfs regions brief
-------------------------------------
Region Application Enabled
-------------------------------------
4      tacacs+     yes
6      radius      yes
switch(config-cfs-region)# copy running-config startup-config
```

Deleting a CFS Region

You can delete a region and move all included applications back to the default region.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no cfs region** *region-number*	Deletes the specified region after warning that this action causes all applications in the region to move to the default region.

	Command or Action	Purpose
		Note After you delete the region, you are returned to the global configuration mode.
Step 3	(Optional) switch(config)# **show cfs regions brief**	Shows all configured regions and applications but does not show peers.
Step 4	(Optional) switch(config)# **show cfs application name** *application-name*	Shows local application information by name.
Step 5	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# no cfs region 4
WARNING: All applications in the region will be moved to default region.
Are you sure? (y/n) [n] y
switch(config)# show cfs regions brief
-------------------------------------
Region Application Enabled
-------------------------------------
6      callhome      no
switch(config)# show cfs application name callhome
Enabled : Yes
Timeout : 20s
Merge Capable : Yes
Scope : Physical-fc-ip
Region : Default
switch(config)# copy running-config startup-config
```

Creating and Distributing a CFS Configuration

You can create a configuration change for an application and then distribute it to its application peers.

⚠

Caution   If you do not commit the changes, they are not distributed and saved in the running configuration of application peer devices.

⚠

Caution   If you do not save the changes to the startup configuration in every application peer device where distributed, changes are retained only in their running configurations.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	Required: switch(config)# *application-name*	Specifies that CFS starts a session for the specified application name and locks the fabric.
Step 3	Required: switch(config-callhome)# *application-command*	Specifies that configuration changes are saved as a working copy and are not saved in the running configuration until you enter the **commit** command.
Step 4	(Optional) Repeat Step 3 for each configuration command that you want to add.	
Step 5	(Optional) switch(config-callhome)# **show** *application-name* **status**	For the specified application, displays the CFS distribution status.
Step 6	Required: switch(config-callhome)# **commit**	CFS distributes the configuration changes to the running configuration of every application peer device. If one or more external devices report a successful status, the software overwrites the running configuration with the changes from the CFS working copy and releases the fabric lock. If none of the external devices report a successful status, no changes are made, and the fabric lock remains in place.
Step 7	(Optional) switch(config-callhome)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# snmp-server contact personname@companyname.com
switch(config)# callhome
switch(config-callhome)# email-contact admin@Mycompany.com
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)# street-address 123 Anystreet st. Anytown,AnyWhere
switch(config-callhome)# show callhome status
Distribution : Enabled
switch(config-callhome)# commit
switch(config-callhome)# copy running-config startup-config
```

Clearing a Locked Session

You can clear a lock held by an application from any device in the fabric.

<table>
<tr><td rowspan="2"></td></tr>
</table>

⚠

Caution When you clear a lock in the fabric, any pending configurations in any device in the fabric are discarded.

Before you begin

You must have administrator permissions to release a lock.

Procedure

	Command or Action	**Purpose**
Step 1	(Optional) switch# **show** *application-name* **status**	Shows the current application state.
Step 2	Required: switch# **clear** *application-name* **session**	Clears the application configuration session and releases the lock on the fabric. All pending changes are discarded.
Step 3	(Optional) switch# **show** *application-name* **status**	Shows the current application state.

Example

```
switch# show ntp status
Distribution : Enabled
Last operational state: Fabric Locked
switch# clear ntp session
switch# show ntp status
Distribution : Enabled
Last operational state: No session
```

Discarding a CFS Configuration

You can discard configuration changes and release the lock.

⚠

Caution If you discard configuration changes, the application flushes the pending database and releases locks in the fabric.

Procedure

	Command or Action	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	Required: switch(config)# *application-name* **abort**	Aborts the application configuration, discards the configuration changes, closes the CFS session, and releases the fabric lock.

	Command or Action	Purpose
		Note The **abort** command is supported only on the device where the fabric lock is acquired.
Step 3	(Optional) switch(config)# **show** *application-name* **session status**	For the specified application, displays the CFS session status.

Example

```
switch# configure terminal
switch(config)# ntp abort
This will prevent CFS from distributing the configuration to other switches.
Are you sure? (y/n) [n] y
switch(config)# show ntp session status
Last Action Time Stamp : Wed Aug 14 16:07:25 2013
Last Action : Abort
Last Action Result : Success
Last Action Failure Reason : none
```

Disabling CFS Distribution Globally

You can disable CFS distribution for a device, isolating the applications using CFS from fabric-wide distributions while maintaining physical connectivity. When CFS is globally disabled on a device, CFS operations are restricted to the device, and all CFS commands continue to function as if the device was physically isolated.

Before you begin

If the virtual port channel (vPC) feature is enabled, only IP distribution is disabled. You must first disable vPC before you can disable CFS distribution.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no cfs distribute**	Globally disables CFS distribution for all applications on the device.
Step 3	(Optional) switch(config)# **show cfs status**	Displays the global CFS distribution status for the device.
Step 4	(Optional) switch(config)# **copy running-config startup config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# no cfs distribute
This will prevent CFS from distributing the configuration to other switches.
Are you sure? (y/n) [n] y
switch(config)# show cfs status
Distribution : Disabled
Distribution over IP : Disabled
IPv4 multicast address : 239.255.70.83
Distribution over Ethernet : Disabled
switch(config)# copy running-config startup-config
```

Verifying the CFS Configuration

Command	Purpose
show *application-name* **session status**	Displays the configuration session status, including the last action, the result, and the reason if there was a failure.
show *application-name* **status**	For the specified application, displays the CFS distribution status.
show cfs application	Displays the applications that are currently CFS enabled.
show cfs application name *application-name*	Displays the details for a particular application, including the enabled or disabled state, timeout as registered with CFS, merge capability if registered with CFS for merge support, distribution scope, and distribution region.
show cfs internal	Displays information internal to CFS including memory statistics, event history, and so on.
show cfs lock	Displays all active locks.
show cfs merge status name *name* [**detail**]	Displays the merge status for a given application.
show cfs peers	Displays all the peers in the physical fabric.
show cfs regions	Displays all the applications with peers and region information.
show cfs status	Displays the status of CFS distribution on the device as well as IP distribution information.
show logging level cfs	Displays the CFS logging configuration.
show tech-support cfs	Displays information about the CFS configuration required by technical support when resolving a CFS issue.

Additional References for CFS

Related Documents

Related Topic	Document Title
CFS CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference* *Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference*
CFS configuration for device alias CFS configuration for DPVM CFS configuration for FC domain CFS configuration for FC port security CFS configuration for FC timer CFS configuration for IVR CFS configuration for RSCN	*Cisco Nexus 7000 Series NX-OS SAN Switching Configuration Guide*
FCoE	*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*
RADIUS	*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*
TACACS+	*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*
User roles	*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*

MIBs

MIBs	MIBs Link
CISCO-CFS-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for CFS

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 3: Feature History for CFS

Feature Name	Release	Feature Information
CFS protocol	5.2(1)	Added CFS over Fibre Channel (CFSoFC) distribution support for device alias, DPVM, FC domain, FC port security, FC timer, IVR, and RSCN.
CFS protocol	4.1(2)	This feature was introduced.