Cisco Virtual Security Gateway High Availability

This chapter describes how to configure high availability (HA) for the Cisco Virtual Security Gateway (VSG).

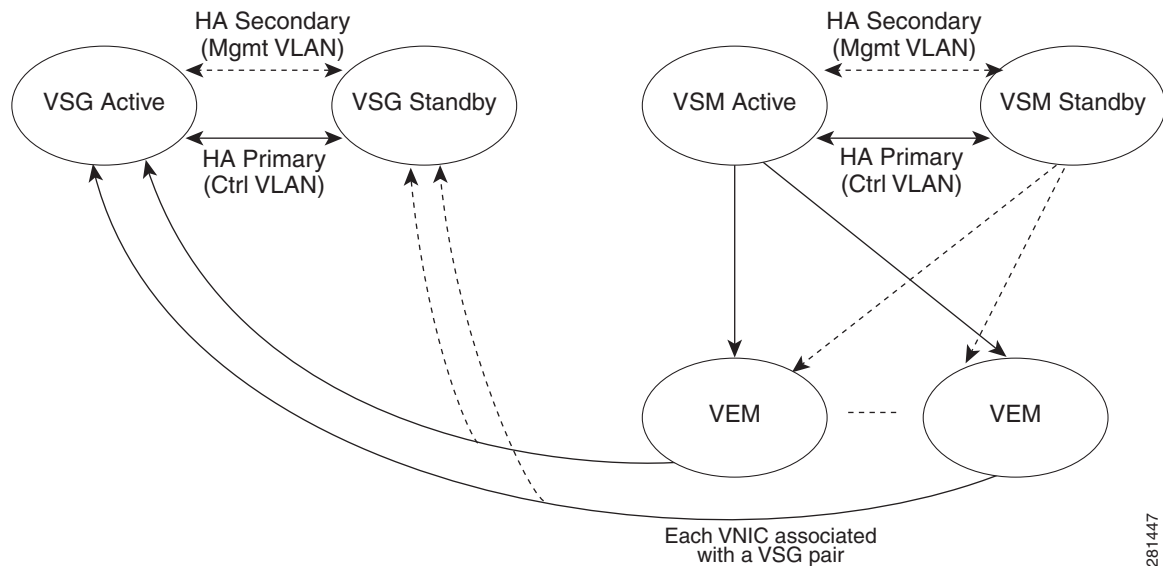This chapter includes the following sections:

Information About High Availability

Cisco VSG HA is a subset of the Cisco NX-OS HA. Redundancy or HA is provided by one active Cisco VSG and one standby Cisco VSG. The active Cisco VSG runs and controls all the system applications. Applications are started and initialized in standby mode on the standby Cisco VSG as they are synchronized and updated on the active Cisco VSG. When a failover occurs, the standby Cisco VSG takes over for the active Cisco VSG. The following HA features minimize or prevent traffic disruption in the event of a failure:

- Redundancy—HA pairing of devices
- Isolation of processes—Software component isolation
- Supervisor and Cisco VSG failover—HA pairing of the active/standby Cisco VSG

Figure 5-1 shows the Cisco VSG HA model.

Figure 5-1   ***Cisco VSG High Availability***

This section includes the following topics:

Redundancy

Cisco VSG redundancy is equivalent to HA pairing. The possible redundancy states are active and standby. An active Cisco VSG is paired with a standby Cisco VSG. HA pairing is based on the Cisco VSG ID. Two Cisco VSGs that are assigned the identical ID are automatically paired. All processes running in the Cisco VSG are critical on the data path. If one process fails in an active Cisco VSG, a failover to the standby Cisco VSG occurs instantly and automatically.

Isolation of Processes

The Cisco VSG software contains independent processes, known as services, that perform a function or set of functions for a subsystem or feature set. Each service and service instance runs as an independent, protected process. This way of operating provides a highly fault-tolerant software infrastructure and fault isolation between services. A failure in a service instance does not affect any other services that are running at that time. Additionally, each instance of a service can run as an independent process, which means that two instances of a routing protocol can run as separate processes.

Cisco VSG Failover

When a failover occurs, the Cisco VSG HA pair configuration allows uninterrupted traffic forwarding by using a stateful failover. For information about a Cisco VSG failover, see the "Cisco VSG HA Pair Failover" section on page 5-6.

System-Control Services

The Cisco VSG allows stateful restarts of most processes and services. Back-end management of processes, services, and applications is handled by the following high-level system-control services:

- System Manager
- Persistent Storage Service
- Message and Transaction Service
- HA Policies

Figure 5-2 shows the system-control services.

Figure 5-2   *System-Control Services*
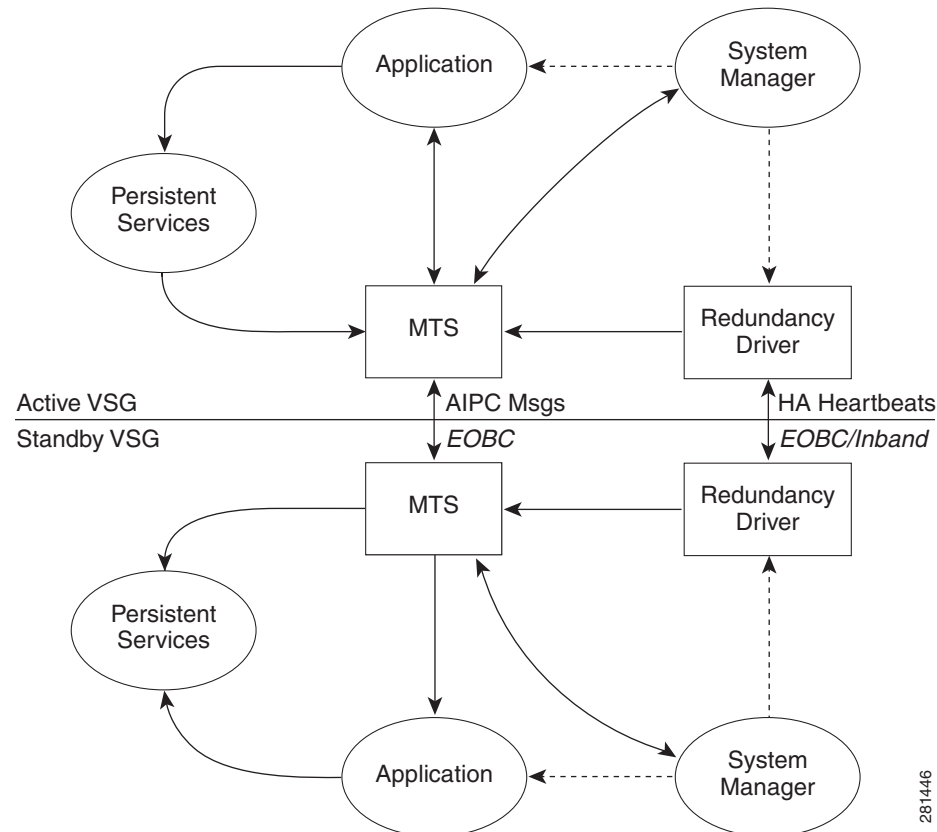
This section includes the following topics:

- System Manager, page 5-4
- Persistent Storage Service, page 5-4

System Manager

The System Manager (SM) directs overall system function, service management, and system health monitoring, and enforces high-availability policies. The SM is responsible for launching, stopping, monitoring, and restarting service, and for initiating and managing the synchronization of service states and supervisor states.

Persistent Storage Service

The Persistent Storage Service (PSS) stores and manages the operational run-time information and configuration of platform services. The PSS component works with system services to recover states if a service restart occurs. It functions as a database of state and run-time information, which allows services to make a checkpoint of their state information whenever needed. A restarting service can recover the last known operating state that preceded a failure.

Each service that uses PSS can define its stored information as private (it can be read only by that service) or shared (the information can be read by other services). If the information is shared, the service can specify that it is local (the information can be read only by services on the same supervisor) or global (it can be read by services on either supervisor or on modules).

Message and Transaction Service

The message and transaction service (MTS) is an interprocess communications (IPC) message broker that specializes in high-availability semantics. The MTS handles message routing and queuing between services on and across modules and between supervisors. The MTS facilitates the exchange of messages, such as event notification, synchronization, and message persistency, between system services and system components. The MTS can maintain persistent messages and logged messages in queues for access even after a service restart.

HA Policies

The Cisco NX-OS software usually allows each service to have an associated set of internal HA policies that define how a failed service is restarted. When a process fails on a device, System Manager either performs a stateful restart, a stateless restart, or a failover.

Note   Only processes that are borrowed by a Cisco VSG from a VSM restart. Processes that are native to a Cisco VSG, such as policy engine or inspect, do not restart. A failed native Cisco VSG process causes an automatic failover.

Cisco VSG HA Pairs

Cisco VSG HA pairs have the following characteristics:

- Redundancy is provided by one active Cisco VSG and one standby Cisco VSG.
- The active Cisco VSG runs and controls all the system applications.
- Applications are started and initialized in standby mode on the standby Cisco VSG.
- Applications are synchronized and updated on the standby Cisco VSG.
- When a failover occurs, the standby Cisco VSG takes over for the active Cisco VSG.

This section includes the following topics:

Cisco VSG Roles

The Cisco VSG roles are as follows:

- Standalone—This role does not interact with other Cisco VSGs. You assign this role when there is only one Cisco VSG in the system. This role is the default.
- Primary—This role coordinates the active/standby state with the secondary Cisco VSG. It takes precedence during bootup when negotiating the active/standby mode. That is, if the secondary Cisco VSG does not have the active role at bootup, the primary Cisco VSG takes the active role. You assign this role to the first Cisco VSG that you install in an HA Cisco VSG system.
- Secondary—This role coordinates the active/standby state with the primary Cisco VSG. You assign this role to the second Cisco VSG that you add to a Cisco VSG HA pair.

HA Pair States

The Cisco VSG HA pair states are as follows:

- Active—This state indicates the Cisco VSG is active and controls the system. It is visible to the user through the **show system redundancy status** command.
- Standby—This state indicates that the Cisco VSG has synchronized its configuration with the active Cisco VSG so that it is continuously ready to take over in case of a failure or manual switchover.

Cisco VSG HA Pair Synchronization

The active and standby Cisco VSGs automatically synchronize when the internal state of one is active and the internal state of the other is standby.

If the output of the **show system redundancy status** command indicates that the operational redundancy mode of the active Cisco VSG is none, the active and standby Cisco VSGs are not synchronized.

This example shows the internal state of Cisco VSG HA pair when they are synchronized:

```
vsg# show system redundancy status
Redundancy role
---------------
      administrative:   primary
         operational:   primary

Redundancy mode
---------------
      administrative:   HA
         operational:   HA

This supervisor (sup-1)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with HA standby

Other supervisor (sup-2)
-----------------------
    Redundancy state:   Standby
Supervisor state: HA standby
Internal state: HA standby
vsg#
```

Cisco VSG HA Pair Failover

The Cisco VSG HA pair configuration allows uninterrupted traffic forwarding using a stateful failover when a failure occurs. The pair operates in an active/standby capacity in which only one is active at any given time, while the other acts as a standby backup. The two Cisco VSGs constantly synchronize the state and configuration in order to provide a stateful failover of most services.

This section includes the following topics:

- Failover Characteristics, page 5-6
- Automatic Failovers, page 5-6
- Manual Failovers, page 5-7

Failover Characteristics

A failover occurs when the active Cisco VSG fails and it has the following characteristics:

- It is stateful, or nondisruptive, because control traffic is not affected.
- It does not disrupt data traffic because the Virtual Ethernet Modules (VEMs) are not affected.

Automatic Failovers

When a stable standby Cisco VSG detects that the active Cisco VSG has failed, it initiates a failover and transitions to active. When a failover begins, another failover cannot be started until a stable standby Cisco VSG is available. If a standby Cisco VSG that is not stable detects that an active Cisco VSG has failed, then instead of initiating a failover, it tries to restart the pair.

Manual Failovers

Before you can initiate a manual failover from the active to the standby Cisco VSG, the standby Cisco VSG must be stable. To find out if it is, see the "Verifying that a Cisco VSG Pair is Ready for a Failover" section on page 5-9. Once you have verified that the standby Cisco VSG is stable, you can manually initiate a failover. To find out if it is, see the "Manually Switching the Active Cisco VSG to Standby" section on page 5-10. Once a failover process begins, another failover process cannot be started until a stable standby Cisco VSG is available.

Cisco VSG HA Guidelines and Limitations

HA pairs have the following configuration guidelines and limitations:

*   Although primary and secondary Cisco VSGs can reside in the same host, to improve redundancy install them in separate hosts and, if possible, connect them to different upstream switches.

*   The console for the standby Cisco VSG is available through the vSphere client or by using the **attach module** [*1* | *2*] command depending on whether the primary is active or not, but configuration is not allowed and many commands are restricted. The **attach module** [*1* | *2*] command must be executed at the console of the active Cisco VSG.

Changing the Cisco VSG Role

You can change the role of a Cisco VSG to one of the following after it is already in service:

*   Standalone

*   Primary

*   Secondary

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

⚠

Caution Changing the role of a Cisco VSG can result in a conflict between the pair. If a primary and secondary see each other as active at the same time, the system resolves this problem by resetting the primary Cisco VSG. If you are changing a standalone Cisco VSG to a secondary Cisco VSG, be sure to first isolate it from the other Cisco VSG in the pair to prevent any interaction with the primary Cisco VSG during the change. Power the Cisco VSG off before reconnecting it as standby.

*   You are logged into the CLI in EXEC mode.

*   To activate a change from a primary to a secondary Cisco VSG, you must reload the primary Cisco VSG by doing one of the following:

    –   Enter the **reload** command.

    –   Power the Cisco VSG off and then on from the vSphere Client.

*   A change from a standalone to a primary Cisco VSG takes effect immediately.

To change a standalone Cisco VSG to a secondary Cisco VSG, see the "Pairing a Second Cisco VSG with an Active Cisco VSG" section on page 5-13.

SUMMARY STEPS

1. (Optional) **system redundancy role** {**standalone** | **primary** | **secondary**}
2. (Optional) **show system redundancy status**
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	`system redundancy role {standalone | primary | secondary}`
	
	Example:
	`vsg# system redundancy role primary`
		Specifies the HA role of a Cisco VSG.

Step 2	`show system redundancy status`
	
	Example:
	`vsg# show system redundancy status`
		(Optional) Displays the current redundancy status for the Cisco VSG.

Step 3	`copy running-config startup-config`
	
	Example:
	`vsg# copy running-config startup-configure`
		(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows how to specify the HA role of a Cisco VSG:

```
vsg# system redundancy role standalone
vsg#
```

This example shows how to display the system redundancy status of a standalone Cisco VSG:

```
vsg# show system redundancy status
Redundancy role
---------------
      administrative:   standalone
         operational:   standalone

Redundancy mode
---------------
      administrative:   HA
         operational:   None

This supervisor (sup-1)
-----------------------
   Redundancy state: Active
   Supervisor state: Active
   Internal state: Active with no standby

Other supervisor (sup-2)
-----------------------
   Redundancy state:   Not present
vsg#
```

This example shows how to copy the running configuration to the startup configuration:

```
vsg# copy running-config startup-config
[#######################################] 100%
vsg#
```

Configuring a Failover

This section includes the following topics:

Guidelines and Limitations

Failovers have the following configuration guidelines:

- When you manually initiate a failover, system messages are generated that indicate the presence of two Cisco VSGs and identify which one is becoming active.
- A failover can only be done when both Cisco VSGs are functioning.

Verifying that a Cisco VSG Pair is Ready for a Failover

You can verify that both an active and standby Cisco VSG are in place and operational before proceeding with a failover.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged into the CLI in EXEC mode.
- If the standby Cisco VSG is not in a stable state (the state must be **ha-standby**), a manually initiated failover cannot be done.

SUMMARY STEPS

1. **show system redundancy status**

DETAILED STEPS

	Command	Purpose

Step 1	`show system redundancy status`
	
	Example:
	`vsg# show system redundancy status`
		Displays the current redundancy status for the Cisco VSG(s).
		
		If the output indicates the following, you can proceed with a system failover, if needed:
		
		• The presence of an active Cisco VSG
		
		• The presence of a standby Cisco VSG in the HA standby redundancy state

EXAMPLES

This example shows how to verify that a Cisco VSG pair is ready for a failover:

```
vsg# show system redundancy status
Redundancy role
---------------
    administrative:   primary
        operational:   primary

Redundancy mode
---------------
    administrative:   HA
        operational:   None

This supervisor (sup-1)
----------------------
   Redundancy state:   Active
   Supervisor state:   Active
     Internal state:   Active with no standby

Other supervisor (sup-2)
----------------------
   Redundancy state:   Active
   Supervisor state:   Active
     Internal state:   Active with no standby
```

Manually Switching the Active Cisco VSG to Standby

You can manually switch an active Cisco VSG to standby in an HA pair.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

• You are logged in to the active Cisco VSG CLI in EXEC mode.

• You have completed the steps in the "Verifying that a Cisco VSG Pair is Ready for a Failover" section on page 5-9 and have found the system to be ready for a failover.

• A failover can be performed only when two Cisco VSGs are functioning.

• If the standby Cisco VSG is not in a stable state, you cannot initiate a manual failover and you see the following error message:

```
Failed to switchover (standby not ready to takeover in vdc 1)
```

- Once you enter the **system switchover** command, you cannot start another failover process on the same system until a stable standby Cisco VSG is available.

- Any unsaved running configuration that was available in the active Cisco VSG is still unsaved in the new active Cisco VSG. You can verify this unsaved running configuration by using the **show running-config diff** command. Save that configuration, if needed, as you would do in the other Cisco VSG by entering the **copy running-config startup-config** command.

SUMMARY STEPS

1. **system switchover**

2. (Optional) **show running-config diff**

3. **configure**

4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**system switchover** Example: vsg# system switchover	Initiates a manual failover from the active Cisco VSG to the standby Cisco VSG. Note Once you enter this command, you cannot start another failover process on the same system until a stable standby Cisco VSG is available. Note Before proceeding, wait until the switchover completes and the standby supervisor becomes active.
Step 2	**show running-config diff** Example: vsg# show running-config diff	(Optional) Verifies the difference between the running and startup configurations. Any unsaved running configuration in an active Cisco VSG is also unsaved in the Cisco VSG that becomes active after a failover. Save that configuration in the startup if needed.
Step 3	**configure** Example: vsg# configure	Places you in global configuration mode.
Step 4	**copy running-config startup-config** Example: vsg# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows how to switch an active Cisco VSG to the standby Cisco VSG and displays the output that appears on the standby Cisco VSG as it becomes the active Cisco VSG:

```
vsg# system switchover
--------------------------
```

```
2011 Jan 18 04:21:56 n1000v %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_PRE_START:
This supervisor is becoming active (pre-start phase).
2011 Jan 18 04:21:56 n1000v %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_START:
This supervisor is becoming active.
2011 Jan 18 04:21:57 n1000v %$ VDC-1 %$ %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2011 Jan 18 04:22:03 n1000v %$ VDC-1 %$ %PLATFORM-2-MOD_REMOVE: Module 1 removed (Serial
number )
```

This example shows how to display the difference between the running and startup configurations:

```
vsg# show running-config diff
*** Startup-config
--- Running-config
***************
*** 1,38 ****
  version 4.0(4)SV1(1)
  role feature-group name new
  role name testrole
  username admin password 5 $1$S7HvKc5G$aguYqHl0dPttBJAhEPwsy1  role network-admin
  telnet server enable
  ip domain-lookup
```

This example shows how to copy the running configuration to the startup configuration:

```
vsg# configure
vsg(config)# copy running-config startup-config
[#####################################] 100%
vsg(config)#
```

Assigning IDs to HA Pairs

You can create Cisco VSG HA pairs. Each HA pair is uniquely identified by an identification (ID) called an HA pair ID. The configuration state synchronization between the active and standby Cisco VSGs occurs between those Cisco VSG pairs that share the same HA pair ID.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in configuration mode.

SUMMARY STEPS

1. **configure**
2. **ha-pair id** {*number*}

DETAILED STEPS

	Command	Purpose

Step 1	`configure`
	
	Example:
	`vsg# configure`
		Places you in global configuration mode.

	Command	Purpose

Step 2	`ha-pair id {number}`
	
	Example:
	`vsg(config-svs-domain)# ha-pair id 10`
		Assigns an ID to an HA pair.

EXAMPLES

This example shows how to assign an ID to an HA pair:

```
vsg# configure
vsg(config)# ha-pair id 10
vsg(config)#
```

Pairing a Second Cisco VSG with an Active Cisco VSG

You can change a standalone Cisco VSG into an HA pair by adding a second Cisco VSG.

This section includes the following topics:

- Changing the Standalone Cisco VSG to a Primary Cisco VSG, page 5-13
- Verifying the Change to a Cisco VSG HA Pair, page 5-15

BEFORE YOU BEGIN

Before adding a second Cisco VSG to a standalone system, you must know or do the following:

- You are logged into the CLI in EXEC mode.
- Although primary and secondary Cisco VSGs can reside in the same host, you can improve redundancy by installing them in separate hosts and, if possible, connecting them to different upstream switches.
- When installing the second Cisco VSG, assign it with the secondary role.
- Set up the port groups for the dual Cisco VSG VMs with the same parameters in both hosts.
- After the secondary Cisco VSG is paired, the following occurs automatically:
  - The secondary Cisco VSG is reloaded and added to the system.
  - The secondary Cisco VSG negotiates with the primary Cisco VSG and becomes the standby Cisco VSG.
  - The standby Cisco VSG synchronizes its configuration and state with the primary Cisco VSG.

Changing the Standalone Cisco VSG to a Primary Cisco VSG

You can change the role of a Cisco VSG from standalone to primary in a Cisco VSG HA pair.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged into the CLI in EXEC mode.
- A change from a standalone to a primary takes effect immediately.

SUMMARY STEPS

1. **system redundancy role primary**

2. **show system redundancy status**

3. **configure**

4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**system redundancy role primary** **Example:** vsg# system redundancy role primary	Changes the standalone Cisco VSG to a primary Cisco VSG. The role change occurs immediately.
Step 2	**show system redundancy status** **Example:** vsg# show system redundancy status	Displays the current redundancy state for the Cisco VSG.
Step 3	**configure** **Example:** vsg# configure	Places you in global configuration mode.
Step 4	**copy running-config startup-config** **Example:** vsg(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows how to change the standalone Cisco VSG to a primary Cisco VSG:

```
vsg# system redundancy role primary
vsg#
```

This example shows how to display the current system redundancy status for a Cisco VSG:

```
vsg# show system redundancy status
Redundancy role
---------------
      administrative:   primary
         operational:   primary


Redundancy mode
--------------
      administrative:   HA
         operational:   None


This supervisor (sup-1)
----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with no standby


Other supervisor (sup-2)
-----------------------
    Redundancy state:   Not present
```

This example shows how to copy the running configuration to the startup configuration:

```
vsg# configure
vsg(config)# copy running-config startup-config
[#######################################] 100%
vsg(config)#
```

Verifying the Change to a Cisco VSG HA Pair

You can verify a change from a single Cisco VSG to a Cisco VSG HA pair.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged into the CLI in EXEC mode.
- You have already changed the single Cisco VSG role from standalone to primary. See the

SUMMARY STEPS

1. **show system redundancy status**

DETAILED STEPS

	Command	Purpose
Step 1	**show system redundancy status** **Example:** vsg# show system redundancy status	Displays the current redundancy status for Cisco VSGs in the system.

EXAMPLES

This example shows how to display the current redundancy status for Cisco VSGs in the system. In this example, the primary and secondary Cisco VSGs are shown following a change from a single Cisco VSG system to a dual Cisco VSG system.

```
vsg# show system redundancy status
   Redundancy role
   ---------------
   administrative: primary
   operational: primary
   Redundancy mode
   ---------------
   administrative: HA
   operational: HA
```

```
        This supervisor (sup-1)
        -----------------------
        Redundancy state: Active
        Supervisor state: Active
        Internal state: Active with HA standby
Other supervisor (sup-2)
-----------------------
Redundancy state: Standby
Supervisor state: HA standby
Internal state: HA standby
```

Replacing the Standby Cisco VSG in an HA Pair

You can replace a standby/secondary Cisco VSG in an HA pair.

Note   Equipment Outage—This procedure requires that you power down and reinstall a Cisco VSG. During this time, your system will be operating with a single Cisco VSG.

PROCEDURE

Step 1   Power off the standby Cisco VSG.

Step 2   Install the new Cisco VSG as a standby, with the same domain ID as the existing Cisco VSG.

After the new Cisco VSG is added to the system, it synchronizes with the existing Cisco VSG.

Replacing the Active Cisco VSG in an HA Pair

You can replace an active/primary Cisco VSG in an HA pair.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged into the CLI in EXEC mode.

- You must configure the port groups so that the new primary Cisco VSG cannot communicate with the secondary Cisco VSG or any of the VEMs during the setup. Cisco VSGs with a primary or secondary redundancy role have built-in mechanisms for detecting and resolving the conflict between two Cisco VSGs in the active state. In order to avoid these mechanisms during the configuration of the new primary Cisco VSG, you must isolate the new primary Cisco VSG from the secondary Cisco VSG.

Note   Equipment Outage—This procedure requires powering down and reinstalling a Cisco VSG. During this time, your system will be operating with a single Cisco VSG.

PROCEDURE

Step 1   Power off the active Cisco VSG.

The secondary Cisco VSG becomes active.

Step 2   On a vSphere Client, change the port group configuration for the new primary Cisco VSG to prevent communication with the secondary Cisco VSG and the VEMs during setup.

Step 3   Install the new Cisco VSG as the primary, with the same domain ID as the existing Cisco VSG.

Step 4   On the vSphere Client, change the port group configuration for the new primary Cisco VSG to permit communication with the secondary Cisco VSG and the VEMs.

Step 5   Power up the new primary Cisco VSG.

The new primary Cisco VSG starts and automatically synchronizes all configuration data with the secondary, which is currently the active Cisco VSG. Because the existing Cisco VSG is active, the new primary Cisco VSG becomes the standby Cisco VSG and receives all configuration data from the existing active Cisco VSG.

Verifying the HA Status

You can display and verify the HA status.

SUMMARY STEPS

1. **show system redundancy status**

DETAILED STEPS

	Command	Purpose
Step 1	**show system redundancy status** **Example:** vsg# show system redundancy status	Displays the HA status of the system.

EXAMPLES

This example shows how to display the system redundancy status:

```
vsg# show system redundancy status
Redundancy role
---------------
administrative: primary
operational: primary
Redundancy mode
---------------
administrative: HA
operational: HA
```

```
This supervisor (sup-1)
-----------------------
Redundancy state: Active
Supervisor state: Active
Internal state: Active with HA standby
Other supervisor (sup-2)
-----------------------
Redundancy state: Standby
Supervisor state: HA standby
Internal state: HA standby
```

This example shows how to display the state and start count of all processes:

```
vsg# show processes
PID    State  PC        Start_cnt   TTY   Process
-----  -----  --------  ----------  ----  ------------
    1    S    b7f8a468           1    -   init
    2    S           0           1    -   ksoftirqd/0
    3    S           0           1    -   desched/0
    4    S           0           1    -   events/0
    5    S           0           1    -   khelper
   10    S           0           1    -   kthread
   18    S           0           1    -   kblockd/0
   35    S           0           1    -   khubd
  188    S           0           1    -   pdflush
  189    S           0           1    -   pdflush
  190    S           0           1    -   kswapd0
  191    S           0           1    -   aio/0
  776    S           0           1    -   kseriod
  823    S           0           1    -   kide/0
  833    S           0           1    -   ata/0
  837    S           0           1    -   scsi_eh_0
 1175    S           0           1    -   kjournald
 1180    S           0           1    -   kjournald
 1740    S           0           1    -   kjournald
 1747    S           0           1    -   kjournald
 1979    S    b7f6c18e           1    -   portmap
 1992    S           0           1    -   nfsd
 1993    S           0           1    -   nfsd
 1994    S           0           1    -   nfsd
 1995    S           0           1    -   nfsd
 1996    S           0           1    -   nfsd
 1997    S           0           1    -   nfsd
 1998    S           0           1    -   nfsd
 1999    S           0           1    -   nfsd
 2000    S           0           1    -   lockd
 2001    S           0           1    -   rpciod
 2006    S    b7f6e468           1    -   rpc.mountd
 2012    S    b7f6e468           1    -   rpc.statd
 2039    S    b7dd2468           1    -   sysmgr
 2322    S           0           1    -   mping-thread
 2323    S           0           1    -   mping-thread
 2339    S           0           1    -   stun_kthread
 2340    S           0           1    -   stun_arp_mts_kt
 2341    S           0           1    -   stun_packets_re
 2376    S           0           1    -   redun_kthread
 2377    S           0           1    -   redun_timer_kth
 2516    S           0           1    -   sf_rdn_kthread
 2517    S    b7f37468           1    -   xinetd
 2518    S    b7f6e468           1    -   tftpd
 2519    S    b79561b6           1    -   syslogd
 2520    S    b7ecc468           1    -   sdwrapd
 2522    S    b7da3468           1    -   platform
 2527    S           0           1    -   ls-notify-mts-t
```

```
2541     S   b7eabbe4            1   -   pfm_dummy
2549     S   b7f836be            1   -   klogd
2557     S   b7c09be4            1   -   vshd
2558     S   b7e4f468            1   -   stun
2559     S   b7b11f43            1   -   smm
2560     S   b7ea1468            1   -   session-mgr
2561     S   b7cd1468            1   -   psshelper
2562     S   b7f75468            1   -   lmgrd
2563     S   b7e6abe4            1   -   licmgr
2564     S   b7eb5468            1   -   fs-daemon
2565     S   b7e97468            1   -   feature-mgr
2566     S   b7e45468            1   -   confcheck
2567     S   b7ea9468            1   -   capability
2568     S   b7cd1468            1   -   psshelper_gsvc
2576     S   b7f75468            1   -   cisco
2583     S   b779f40d            1   -   clis
2586     S   b76e140d            1   -   port-profile
2588     S   b7d07468            1   -   xmlma
2589     S   b7e69497            1   -   vnm_pa_intf
2590     S   b7e6e468            1   -   vmm
2591     S   b7b9c468            1   -   vdc_mgr
2592     S   b7e73468            1   -   ttyd
2593     R   b7edb5f5            1   -   sysinfo
2594     S   b7d07468            1   -   sksd
2596     S   b7e82468            1   -   res_mgr
2597     S   b7e49468            1   -   plugin
2598     S   b7bb9f43            1   -   npacl
2599     S   b7e93468            1   -   mvsh
2600     S   b7e02468            1   -   module
2601     S   b792c40d            1   -   fwm
2602     S   b7e93468            1   -   evms
2603     S   b7e8d468            1   -   evmc
2604     S   b7ec4468            1   -   core-dmon
2605     S   b7e11468            1   -   bootvar
2606     S   b769140d            1   -   ascii-cfg
2607     S   b7ce5be4            1   -   securityd
2608     S   b77de40d            1   -   cert_enroll
2609     S   b7ce2468            1   -   aaa
2611     S   b7b0bf43            1   -   l3vm
2612     S   b7afef43            1   -   u6rib
2613     S   b7afcf43            1   -   urib
2615     S   b7e05468            1   -   ExceptionLog
2616     S   b7daa468            1   -   ifmgr
2617     S   b7ea5468            1   -   tcap
2621     S   b763340d            1   -   snmpd
2628     S   b7f02d39            1   -   PMon
2629     S   b7c00468            1   -   aclmgr
2646     S   b7b0ff43            1   -   adjmgr
2675     S   b7b0bf43            1   -   arp
2676     S   b793b896            1   -   icmpv6
2677     S   b79b2f43            1   -   netstack
2755     S   b77ac40d            1   -   radius
2756     S   b7f3ebe4            1   -   ip_dummy
2757     S   b7f3ebe4            1   -   ipv6_dummy
2758     S   b78e540d            1   -   ntp
2759     S   b7f3ebe4            1   -   pktmgr_dummy
2760     S   b7f3ebe4            1   -   tcpudp_dummy
2761     S   b784640d            1   -   cdp
2762     S   b7b6440d            1   -   dcos-xinetd
2765     S   b7b8f40d            1   -   ntpd
2882     S   b7dde468            1   -   vsim
2883     S   b799340d            1   -   ufdm
2884     S   b798640d            1   -   sal
2885     S   b795940d            1   -   pltfm_config
```

```
2886     S  b787640d             1    -  monitor
2887     S  b7d71468             1    -  ipqosmgr
2888     S  b7a4827b             1    -  igmp
2889     S  b7a6640d             1    -  eth-port-sec
2890     S  b7b7e468             1    -  copp
2891     S  b7ae940d             1    -  eth_port_channel
2892     S  b7b0a468             1    -  vlan_mgr
2895     S  b769540d             1    -  ethpm
2935     S  b7d3a468             1    -  msp
2938     S  b590240d             1    -  vms
2940     S  b7e8d468             1    -  vsn_service_mgr
2941     S  b7cc0468             1    -  vim
2942     S  b7d57468             1    -  vem_mgr
2943     S  b7d25497             1    -  policy_engine
2944     S  b7e6a497             1    -  inspect
2945     S  b7d33468             1    -  aclcomp
2946     S  b7d1c468             1    -  sf_nf_srv
2952     S  b7f1deee             1    -  thttpd.sh
2955     S  b787040d             1    -  dcos-thttpd
3001     S  b7f836be             1    1  getty
3003     S  b7f806be             1   S0  getty
3004     S  b7f1deee             1    -  gettylogin1
3024     S  b7f836be             1   S1  getty
15497    S  b7a3840d             1    -  in.dcos-telnetd
15498    S  b793a468             1   20  vsh
19217    S  b7a3840d             1    -  in.dcos-telnetd
19218    S  b7912eee             1   21  vsh
19559    S  b7f5d468             1    -  sleep
19560    R  b7f426be             1   21  more
19561    R  b7939be4             1   21  vsh
19562    R  b7f716be             1    -  ps
    -   NR       -               0    -  tacacs
    -   NR       -               0    -  dhcp_snoop
    -   NR       -               0    -  installer
    -   NR       -               0    -  ippool
    -   NR       -               0    -  nfm
    -   NR       -               0    -  private-vlan
    -   NR       -               0    -  scheduler
    -   NR       -               0    -  vbuilder
vsg#
```