



Cisco StadiumVision Director Server Redundancy

First Published: November 4, 2011
Revised: July 19, 2012

Cisco StadiumVision Director supports an environment of two servers that run the Cisco StadiumVision Director software, where one of the servers operates as the primary active server, and the other server operates as a secondary backup server. If a failure occurs, you can configure the backup server to become the active server, but the failover process is not automatic.

Contents

- [Prerequisites for Cisco StadiumVision Director Server Redundancy, page 1](#)
- [Restrictions for Cisco StadiumVision Director Server Redundancy, page 2](#)
- [Information About Cisco StadiumVision Director Server Redundancy, page 2](#)
- [How to Configure Failover to the Secondary Server and Failback to the Primary Server, page 4](#)
- [Feature Information for Cisco StadiumVision Director Server Redundancy, page 12](#)

Prerequisites for Cisco StadiumVision Director Server Redundancy

Before you promote a secondary server to become the primary active server, be sure that the following requirements are met:

- Verify that you have a successful backup of the primary server on the secondary server. For more information, see the *Backing Up and Restoring Cisco StadiumVision Director* module.
- The Cisco StadiumVision Director backup server is on the same subnet as the primary server.
- The servers are using the Eth0 interface for connection to the network.

- Be sure that an SNE TAC account and login credential have been obtained for each server by your Cisco representative, or otherwise contact the Cisco Technical Assistance Center (TAC). This account will be needed to authenticate and obtain an access token for the Cisco StadiumVision server and to create a user with privileges to perform the system tasks.
- You have a user account with sudo root access on the Cisco StadiumVision Director servers, and you have a Cisco StadiumVision Director administrator account on both servers.

Restrictions for Cisco StadiumVision Director Server Redundancy

The Cisco StadiumVision Director server redundancy architecture has the following restrictions:

- The Cisco StadiumVision Director server architecture does not support automatic failover when a failure occurs on the active server.
- Depending on your environment, 30 minutes or more is needed to complete the manual failover process.
- In addition, after the manual failover process is completed, a script push will be required if you are in an active event, which depending on your deployment and content size, can take anywhere from minutes to an hour. When pushing the script again, there will be a service interruption.

Information About Cisco StadiumVision Director Server Redundancy

[Figure 1](#) shows the architecture of Cisco StadiumVision Director server redundancy under normal network conditions and operation. The primary and secondary servers are addressed as independent hosts with two different IP addresses on the same subnet in the Cisco Connected Stadium network.

While the secondary server is still connected to the network, notice that communication and control only occurs between the primary Cisco StadiumVision Director server and the rest of the network, including the Digital Media Players (DMPs).

The secondary server is only connected to the network to be made available as a backup to the primary should a failure occur. In addition, the secondary server can (and should) be configured to be backed up with data from the primary server on a scheduled basis.

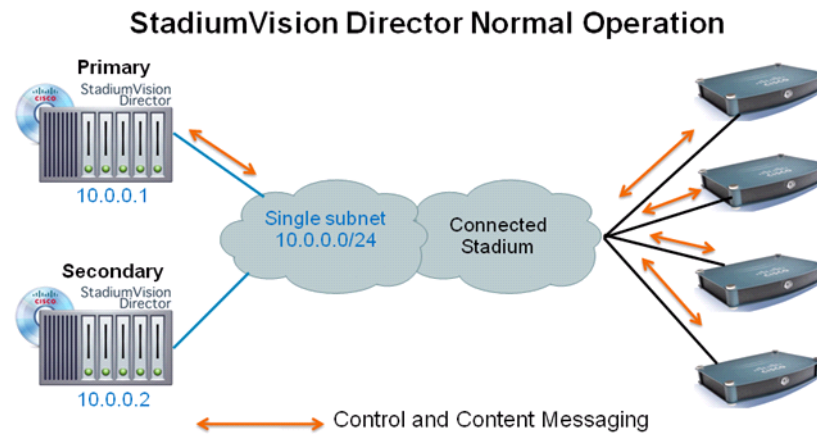
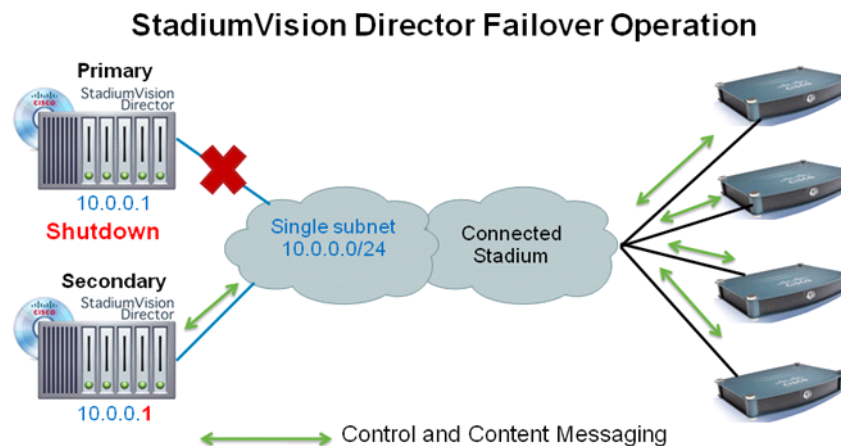
Figure 1 Cisco StadiumVision Director Server Redundancy Under Normal Operation

Figure 2 shows the redundancy environment when connectivity from the primary Cisco StadiumVision Director server fails. When the primary server fails, a manual process must take place to restore the secondary server from a backup, shut down the primary server, and activate the secondary server as the primary.

Notice that the secondary server must be reconfigured to use the same IP address the original primary server. In this example, the secondary server IP address is changed to 10.0.0.1 (from 10.0.0.2) to match the primary server address. When the process is complete, communication and control only occurs between the newly activated secondary server and the rest of the network.

**Note**

The word “failover” does not mean automatic activation of a secondary server. The failover process is manual.

Figure 2 Cisco StadiumVision Director Server Redundancy Under Failover Operation

How to Configure Failover to the Secondary Server and Failback to the Primary Server

This section describes the related tasks to perform when a primary Cisco StadiumVision Director server fails in a redundant server environment. It includes tasks to activate the secondary server to replace the functionality of the primary server for Cisco StadiumVision operation, followed by the tasks to fail back to the original primary server.

This section includes the following tasks:

- [Promoting a Standby Secondary Server to the Active Server, page 4](#) (required)
- [Failing Back to the Primary Server, page 8](#) (optional)

**Note**

Failing back to the primary server requires a service interruption and should only be conducted during scheduled downtime. Be aware that until you change the IP address of the primary server to remove the addressing conflict with the newly active secondary server, you will be unable to schedule backups between the two servers. You will also need to reconfigure the backup/restore environment using the Text Utility Interface (TUI) after failback. For more information, see the *Backing Up and Restoring Cisco StadiumVision Director* module.

Promoting a Standby Secondary Server to the Active Server

This section includes the following tasks:

- [Prerequisites, page 4](#)
- [Starting and Configuring the Services on the Secondary Server, page 5](#) (required)
- [Restoring the Secondary Server with System Data From a Backup File, page 5](#) (required)
- [Stopping Services on and Shutting Down the Primary Server, page 5](#) (required)
- [Shutting Down Services on the Secondary Server and Changing the IP Address, page 6](#) (required)
- [Clearing the ARP Cache on the Switch, page 7](#) (optional)
- [Restarting Services on the Secondary Server, page 8](#) (required)
- [Verifying the Cisco StadiumVision Director Configuration on the Secondary Server, page 8](#) (required)

Prerequisites

Before you promote the standby secondary server to become the new active server, be sure that there is a successful backup on the secondary server. For more information, see the *Backing Up and Restoring Cisco StadiumVision Director* module.

Starting and Configuring the Services on the Secondary Server

To start and configure the services on the secondary server, complete the following steps:

-
- Step 1** Log in to the *secondary* server as a root user using an SSH client.
- Step 2** Start the Cisco StadiumVision Director services on the secondary server using the following commands:
- ```
sudo service mysql start
sudo service liferay start
sudo service svd start
sudo service httpd start
```
- Step 3** After these services start, configure the following services to start automatically when a reboot occurs by entering the following commands:
- ```
sudo /sbin/chkconfig httpd on
sudo /sbin/chkconfig liferay on
sudo /sbin/chkconfig mysql on
sudo /sbin/chkconfig svd-aim on
sudo /sbin/chkconfig svd-config on
sudo /sbin/chkconfig svd-control on
sudo /sbin/chkconfig svd-hornetq on
sudo /sbin/chkconfig svd-monitor on
```
-

Restoring the Secondary Server with System Data From a Backup File

To restore the secondary server with system data from a backup file, complete the following steps:

-
- Step 1** Log in to Cisco StadiumVision Director on the *secondary* server using an administrator account.
- Step 2** From the Cisco StadiumVision Director main menu, click **Management Dashboard**.
- Step 3** From the Dashboard Drawers, select **Tools > Advanced > Restore system data from backup**.
- Step 4** Select the components that you want to restore, and select the date of the backup file to use for the restore.
- Step 5** Click **Apply**.
- The restore begins. A dialog box appears notifying you when the restore process has successfully completed.
-

Stopping Services on and Shutting Down the Primary Server

**Note**

If the primary server has become unavailable for this task, be sure that you power down the server so that it will not conflict with the newly active secondary server.

To stop services on and shut down the primary server, complete the following steps:

- Step 1** Log in to the *primary* server as a root user using an SSH client.
- Step 2** To prevent services from starting again if the primary server is rebooted, enter the following commands on the primary server:
- ```
sudo /sbin/chkconfig httpd off
sudo /sbin/chkconfig liferay off
sudo /sbin/chkconfig mysql off
sudo /sbin/chkconfig svd-aim off
sudo /sbin/chkconfig svd-config off
sudo /sbin/chkconfig svd-control off
sudo /sbin/chkconfig svd-hornetq off
sudo /sbin/chkconfig svd-monitor off
```
- Step 3** When the services are stopped, shut down the primary server using the following command:
- ```
sudo shutdown -h now
```

Shutting Down Services on the Secondary Server and Changing the IP Address



Note

This task uses sample IP addresses shown in [Figure 1](#) and [Figure 2](#). Be sure to use the appropriate corresponding IP addresses for your network environment.

To shut down services on the secondary server and change the IP address, complete the following steps:

- Step 1** Log in to the *secondary* server with root access using an SSH client.
- Step 2** Shut down the Cisco StadiumVision Director services using the following commands:
- ```
sudo service httpd stop
sudo service svd stop
sudo service liferay stop
sudo service mysql stop
```
- Step 3** Display the contents of the `/etc/hosts` file using the following command:
- ```
cat /etc/hosts
```

Look for the localhost and secondary server hostname entries in the display from the `/etc/hosts` file, and confirm the IP address of the secondary server.

In the following sample entries, notice that the IP address of the secondary server hostname reflects the address as shown in our example in [Figure 1](#):

```
127.0.0.1 localhost
10.0.0.2 secondary-hostname
```



Note

The system will run if only the localhost entry exists and the hostname entry is missing. However, when the secondary hostname exists, the IP address of the secondary server must be changed to match the IP address of the primary server.

- Step 4** Enter the following command to open a text editor for the `/etc/hosts` file:
- ```
sudo vi /etc/hosts
```

- Step 5** Change the IP address of the secondary server to match the address of the primary server as shown in the sample entry below for our example in [Figure 2](#):
- ```
10.0.0.1 secondary-hostname
```
- Step 6** Change the IP address of the actual interface using the following command:
- ```
sudo system-config-network
```
- Step 7** Restart the network daemon to put the IP address change into effect on the secondary server using the following command:
- ```
sudo service network restart
```
- Step 8** Verify connectivity to the secondary server using the ping command, as shown in the following example:
- ```
ping 10.0.0.1
```
- If you cannot reach the secondary server, go to the [“Clearing the ARP Cache on the Switch”](#) section on [page 7](#).
- 

## Clearing the ARP Cache on the Switch

This task is optional, as the ARP cache on the switch will refresh in 5-10 minutes. However, if you cannot access the secondary server after changing its IP address, you can clear the ARP cache for that IP address on the switch using the **clear ip arp** privileged EXEC command.

**To clear the ARP cache on the switch, complete the following steps:**

- 
- Step 1** Use a directly-connected console, or if you know the IP address of the switch, use Telnet to access the switch as shown in the following example, where *ip-address* is the address of your switch:
- ```
telnet ip-address
```
- Step 2** At the corresponding prompts, enter your login information as shown in the following example, where *yourname* and *yourpass* are your username and password:
- ```
Username: yourname
Password: yourpass
switch>
```
- Step 3** Enter privileged EXEC mode using the **enable** command and corresponding password:
- ```
switch> enable
Password: enablepassword
switch#
```
- Step 4** To clear the ARP cache of the newly-assigned IP address now used by the secondary server, use the **clear ip arp** command as shown in the following example:
- ```
clear ip arp 10.0.0.1
```
-

## Restarting Services on the Secondary Server

To restart services on the secondary server, complete the following steps:

**Step 1** Using the changed IP address, log in to the *secondary* server as a root user using an SSH client.

**Step 2** Restart Cisco StadiumVision Director services using the following commands:

```
sudo service mysql start
sudo service liferay start
sudo service svd start
sudo service httpd start
```

## Verifying the Cisco StadiumVision Director Configuration on the Secondary Server

To verify the Cisco StadiumVision Director configuration on the secondary server, complete the following steps:

**Step 1** Log in to Cisco StadiumVision Director on the *secondary* server using an administrator account.

**Step 2** From the Cisco StadiumVision Director main menu, click **Management Dashboard**.

**Step 3** From the Dashboard Drawers, select **DMP and TV Controls > Monitoring > Get Status**.

Confirm that you have successful communication between the DMPs and Cisco StadiumVision Director.

**Step 4** Verify that all of the content is on this server.

**Step 5** To establish control of the DMPs, start a script without any content and with the No Staging radio button selected. This should only require less than 10 minutes.



**Note** You can push a script with content, but this will result in a longer period of downtime.

## Failing Back to the Primary Server



**Note** This task requires a service interruption.

At a scheduled downtime, you should fail back to the primary server to re-establish your normal operating environment and clean up the original primary server from the failure, make IP addressing changes, and have regularly scheduled backups again between the two servers.

This section includes the following tasks:

- [Prerequisites, page 9](#)
- [Shutting Down Services on the Secondary Server and Changing the IP Address, page 9](#) (required)
- [Starting Services on the Original Primary Server, page 10](#) (required)



- [Restoring the Original Primary Server with System Data From a Backup File, page 11](#) (as required)
- [Restarting the Local Control Service, page 11](#) (required after restore run)
- [Verifying the Cisco StadiumVision Director Configuration on the Original Primary Server, page 12](#) (required)

## Prerequisites

If you have made any administrative changes on the active secondary server, be sure that a successful backup has been run.

## Shutting Down Services on the Secondary Server and Changing the IP Address

To shut down services on the secondary server and change the IP address, complete the following steps:

- Step 1** Log in to the *secondary* server as a root user using an SSH client.
- Step 2** Stop the Cisco StadiumVision Director services on the secondary server using the following commands:
- ```
sudo service mysql stop
sudo service liferay stop
sudo service svd stop
sudo service httpd stop
```

- Step 3** To prevent services from starting again if the primary server is rebooted, enter the following commands on the secondary server:

```
sudo /sbin/chkconfig httpd off
sudo /sbin/chkconfig liferay off
sudo /sbin/chkconfig mysql off
sudo /sbin/chkconfig svd-aim off
sudo /sbin/chkconfig svd-config off
sudo /sbin/chkconfig svd-control off
sudo /sbin/chkconfig svd-hornetq off
sudo /sbin/chkconfig svd-monitor off
```

- Step 4** Display the contents of the `/etc/hosts` file using the following command:

```
cat /etc/hosts
```

Look for the `localhost` and `secondary server` hostname entries in the display from the `/etc/hosts` file, and confirm the IP address of the secondary server.

In the following sample entries, notice that the IP address of the secondary server hostname reflects the address as shown in the example in [Figure 2](#):

```
127.0.0.1 localhost
10.0.0.1 secondary-hostname
```



Note The system will run if only the `localhost` entry exists and the hostname entry is missing. The IP address of the secondary server must be changed back to its original IP address.

- Step 5** Enter the following command to open a text editor for the `/etc/hosts` file:

```
sudo vi /etc/hosts
```

- Step 6** Change the IP address of the secondary server to reflect its original address as a standby server, as shown in the sample entry below for the example in [Figure 1](#):

```
10.0.0.2 secondary-hostname
```

- Step 7** Change the IP address of the actual interface using the following command:

```
sudo system-config-network
```

- Step 8** Restart the network daemon to put the IP address change into effect on the secondary server using the following command:

```
sudo service network restart
```

- Step 9** Verify connectivity to the secondary server using the ping command, as shown in the following example:

```
ping 10.0.0.2
```

If you cannot reach the secondary server, go to the [“Clearing the ARP Cache on the Switch”](#) section on [page 7](#) and clear the ARP cache entry for IP address 10.0.0.2.

Starting Services on the Original Primary Server

To start services on the original primary server, complete the following steps:

- Step 1** Power on the original primary server.

- Step 2** Log in to the *original primary* server as a root user using an SSH client.



Note It might take a few minutes for SSH to be available as the server boots.

- Step 3** Configure the following services to start automatically when a reboot occurs by entering the following commands:

```
sudo /sbin/chkconfig httpd on
sudo /sbin/chkconfig liferay on
sudo /sbin/chkconfig mysql on
sudo /sbin/chkconfig svd-aim on
sudo /sbin/chkconfig svd-config on
sudo /sbin/chkconfig svd-control on
sudo /sbin/chkconfig svd-hornetq on
sudo /sbin/chkconfig svd-monitor on
```

- Step 4** Restart Cisco StadiumVision Director services using the following commands:

```
sudo service httpd start
sudo service svd start
sudo service liferay start
sudo service mysql start
```

- Step 5** Depending on the state of the server when it went down and what was done while the server was down, a script might be running on the original primary StadiumVision Director server. If a script is running, end the script.

Restoring the Original Primary Server with System Data From a Backup File

If any administrative changes were made to the system while in failover to the other server, you should restore the backup from the secondary.

Prerequisites

Before you restore the backup from the secondary server, you will need to manually copy the backup file from the secondary server. For more information, see the *Backing Up and Restoring Cisco StadiumVision Director* module.

To restore the original primary server with system data from a backup file, complete the following steps:

-
- Step 1** Log in to Cisco StadiumVision Director on the *original primary* server using an administrator account.
 - Step 2** From the Cisco StadiumVision Director main menu, click **Management Dashboard**.
 - Step 3** From the Dashboard Drawers, select **Tools > Advanced > Restore system data from backup**.
 - Step 4** Select the components that you want to restore, and select the date of the backup file to use for the restore.
 - Step 5** Click **Apply**.
The restore begins.
-

Restarting the Local Control Service

After you perform a restore, you must stop and start the local control service (svd-localctl) to resume normal operation of the local control application programming interface (API).

To restart the local control service, complete the following steps:

-
- Step 1** Use a directly connected console, or use an SSH client from a laptop computer that is connected to the Cisco StadiumVision Server network to run a secure login to the primary Cisco StadiumVision Director server using the IP address for your server.
 - Step 2** When the login prompt appears, enter the installer userid followed by the installer password at the password prompt.
 - Step 3** When the StadiumVision Director Configuration menu appears, type the letter beside the option to Start / Stop Services (**f**) and press **Enter**.
 - Step 4** Type the number beside the option to stop the SVD-LOCALCTL service (**14**) and press **Enter**.
 - Step 5** Type the number beside the option to start the SVD-LOCALCTL service (**13**) and press **Enter**.
 - Step 6** Log out.
-

Verifying the Cisco StadiumVision Director Configuration on the Original Primary Server

To verify the Cisco StadiumVision Director configuration on the original primary server, complete the following steps:

-
- Step 1** Log in to Cisco StadiumVision Director on the *original primary* server using an administrator account.
 - Step 2** From the Cisco StadiumVision Director main menu, click **Management Dashboard**.
 - Step 3** From the Dashboard Drawers, select **DMP and TV Controls > Monitoring > Get Status**.
Confirm that you have successful communication between the DMPs and Cisco StadiumVision Director.
 - Step 4** Verify that all of the content is on this server.
 - Step 5** Test the system by looking at the status in the Management Dashboard and by running test scripts to verify operation of the system.
-

Feature Information for Cisco StadiumVision Director Server Redundancy

Table 1 lists the release history for this feature.

Table 1 Feature Information for Cisco StadiumVision Director Server Redundancy

Date	Releases	Feature Information
November 4, 2011	Release 2.4.0-147	Initial release for Cisco StadiumVision Director Release 2.4.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011–2012 Cisco Systems, Inc. All rights reserved.