cisco



Backing Up and Restoring Cisco StadiumVision Director Servers

Release 2.3

April 2011

Corporate Headquarters Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 526-4100 THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at

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. (1005R)

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.

Cisco StadiumVision Backing and Up and Restoring SV Director

Copyright © 2011 Cisco Systems, Inc. All rights reserved.

Table of Contents

Table of Contents	3
Document History	4
Backing Up the Primary Server	5
Performing an Immediate Backup	6
Scheduling a Backup	8
Managing the Backup Directory	8
Manually Copying Backup Files from the Primary to the Secondary	9
Configuring Automatic Copying of Backup Files to the Secondary Server	10
Creating a Backup User	10
Defining 'backup.username' and 'backup.secondarylp'	10
Setting Up Public and Private Keys for the Backup and Restore Task	12
Setting Up the Restore Directory	13
Verifying Automatic Copying of Backup Files	13
Restoring the Primary Server	15
Running a 'Restore system data from backup'	15
Managing the Restore Directory	16
Renaming Backup and Restore Files	17
Scheduling a RestoreTask to Run Ad-Hoc	17
Running an Immediate "RestoreTask"	18
Running a Scheduled Restore	19
Restoring System Data from a Scheduled Backup File	20

Document History

Table 1. Revision History

Date	Comments
May 2, 2011	First release for Cisco StadiumVision Director Release 2.3

There are several components to SV Director that need to be backed up. The backup process backs up the:

- SV Director database
- System configuration files
- Content repository
- Ad Insertion Manager database

Each backup operation results in a tar file that contains separate compressed files for each of the above. When complete, the backup file will be located in /var/sv/BACKUP on the primary and /var/sv/RESTORE on the secondary server if there is a secondary server and the steps for <u>Configuring Automatic Copying of</u> <u>Backup Files to the Secondary Server</u> were completed. The name will be in the following format:

sv-VER-YYYYMMDDHHMMSSTZOFFSET.tar

where:

- Ver is the StadiumVision version the backup was created from.
- YYYYMMDDHHMISS is the time of the backup in year, month, day, hour, minute, second, of backup.
- TZOFFSET is the time zone offset of the server in relation to GMT. An example would be a file called "sv-2.2.55-20110202121212-0800.tar".

To list the contents of a backup file, replace the "sv-2.2.55-20110202121212-0800.tar" with the backup file you would like to list and run the following:

tar tvf sv-2.2.55-20110202121212-0800.tar

StadiumVision Director does not automatically delete backups from the /var/sv/BACKUP or /var/sv/RESTORE directory. Disk space should be monitored accordingly and un-needed backup files should be erased accordingly. As an option, you can add a daily cron job to remove old files from the /var/sv/BACKUP or /var/sv/RESTORE directories. For example, to remove all files from the backup directory that are more than 30 days old run a command like:

/usr/bin/find /var/sv/BACKUP -mtime +30 -exec rm {} \;

Be sure to note that when running or scheduling a backup, it cannot be run while an event script is running. When the backup starts, it first checks to see if an event script is running. If a running script is detected it aborts the backup. This situation can be identified by looking for the following message in the "sv_dev_debug.log":

"Backup is aborting, as a script is currently running"

Performing an Immediate Backup

To initiate an immediate backup of the system:

1. Open SV Director by entering the following at your browser

http://SV_Director_IP_addr:8080/

where SV Director IP addr is the IP address of the SV Director server.

The StadiumVision Director login page displays.

cisco	StadiumVision Version: 2.3	Usemame:
		Password:
		Log In Reset

2. Login with administrator privileges. The StadiumVision Director Main page displays:

cisco	Cisco StadiumVision Director						
	Control Panel						
	Management Dashboard						
	Ad Insertion Manager						
	🗹 Video Distribution Manager						
	System State Reports						
	Custom Applications						
	😅 Dynamic Menu Boards						
	Im TVs Off						
	Logout						

- 3. Click Management Dashboard.
- 4. Select **Tools > Advanced**.
- 5. Select **Run a Task > BackupTask**. Refer to Figure 1.
- 6. Click Apply.

Figure 1. Running the Backup Task

😰 Dashboard	Advanced		
Device Configuration		Command	
Z Event Viewer	Name:	Run a Task	
Director Configuration	Description:	Choose a task to run immediate	ely.
Tools		Parameters	
Settings Advanced	Tasks to Run	ArchivePofPDataTask	•
Generate Proof of Play CSV		BackupTask	=
Manage In Memory Log		CleanupScriptInstancesTask	
Menu Load for Point Of Sale		GeneratePofPCSVTask	
Registry		HPMDMPCommandTask	
Reload log4j properties		HPMPingTask	
Reset Active Script		HPMReportTask	•
Restore system data from backup.			
Run a Task	Apply		
Scheduled Tasks			
Set Active Script			
Switch Phone Desktop Graphic			

The backup will begin immediately. When complete, the backup tar file will be created in /var/sv/BACKUP on the primary server or /var/sv/RESTORE on the secondary server if there is a secondary server and the steps for <u>Configuring</u> <u>Automatic Copying of Backup Files to the Secondary Server</u>.



The reply "success" means the backup task has started. It does not mean the backup process is completed.

- 7. Verify the backup process is complete before moving to the next step:
 - a. Check the output messages from the backup:

/opt/sv/servers/control/logs/sv_dev_debug.log

b. Check the /var/sv/BACKUP directory for two recent files, one of which ends in .chksum, the other in .tar. The .chksum file contains an md5 checksum for the .tar file.

Scheduling a Backup

To schedule a backup to run at regular intervals:

- 1. Open the Management Dashboard.
- 2. Select **Tools > Advanced**.
- 3. Select Scheduled Tasks.
- 4. Click Add Row and scroll to the new blank line. Refer to Figure 2.
- 5. Click in the Task Type column and type **BackUpTask**.
- 6. Click in the Task Time column and specify the time at which you would like the backup to run.
- 7. Click Apply.

Figure 2. Adding the BackUpTask

Cubberd .		Alument						
Di Berne Las Aprellas		1993	243					
2 Event Frener		Cem	PLOPE					
The second looks when		Parrie offe	aver tang					
			and a second second					
Tasla		Peranters						
tellings Advanced		Scheduced Task Date	•					
Revenue Print of Day 250			Tank ID	Task Fape	Facts Three	hereon.		
Tanage in Mémory Log	- 281		1	If age Art of Corps	04/45	invite		
Nerta Load for Point Of Italia			4	PerforMenaTeri	60.00	100Kg		
f e godina			2	And every POPCatal and	04(20	integ		
Releast legity properties				HOWINGTAIN	00-00	10.074		
Faret Autor Dorgit				Hittittana Tark	(96.730)	aredy		
Festive costany data from Section				BARCETAR	85:30	ninte		
fun a Tarix			Add Rent Dulete R					
Charulad Yorks			Sectores Sectores					

Managing the Backup Directory

StadiumVision Director does not currently attempt to manage disk space on the backup directory. You should ensure that the disk does not fill up. All files output from the backup on the primary server are placed into /var/sv/BACKUP.

To manage disk space in the backup directory, add a daily cron job in the Unix cron scheduler to remove old files from that directory. For example to remove all files from the backup directory more than 30 days old run the following command:

/usr/bin/find /var/sv/BACKUP -mtime +30 -exec rm {} \;

Manually Copying Backup Files from the Primary to the Secondary

1. On the primary server cd to the backup directory using "cd /var/sv/BACKUP" and perform a "ls -lt" to locate the backup file you want to copy

[username@svd1 ~]\$ cd /var/sv/BACKUP

[username@svd1 BACKUP]\$ ls -lt total 9395340 -rw-r--r-- 1 root root 85 Nov 11 05:36 sv-2.2.0.55-20101111053000+0000.chksum -rw-r--r-- 1 root root 508692480 Nov 11 05:36 sv-2.2.0.55-20101111053000+0000.tar

2. Use "scp" to copy the ".tar" and ".chksum" file of the backup you want to copy from the primary server to the secondary server:

[username@svd1 BACKUP]\$ scp sv-2.2.0.55-20101030053134+0100.tar username@172.16.52.10:/var/sv/RESTORE sv-2.2.0.55-20101030053134+0100.tar 100% 452MB 11.3MB/s 00:40

[username@svd1 BACKUP]\$ scp sv-2.2.0.55-20101030053134+0100.chksum username@172.16.52.10:/var/sv/RESTORE sv-2.2.0.55-20101030053134+0100.chksum 100% 85 0.1KB/s 00:00



In the above example replace 'username' with the username you will use for the copy, sv-2.2.0.55-20101030053134+0100.tar and sv-2.2.0.55-20101030053134+0100.chksum with the values pulled from step 1 and 172.16.52.10 with the IP address of the secondary server.

3. SSH into the secondary server and verify if the data is correctly copied with the md5sum command on the .tar file copied and compare the results with the .chksum file copied over:

[username@svd2 ~]\$ cat /var/sv/RESTORE/sv-2.2.0.55-20101030053134+0100.chksum

77eab49b132ffd2a08644df3125768af /var/sv/BACKUP/sv-2.2.0.55-20101030053134+0100.tar

[username@svd2 ~]\$md5sum /var/sv/RESTORE/sv-2.2.0.55-20101030053134+0100.tar

77eab49b132ffd2a08644df3125768af /var/sv/RESTORE/sv-2.2.0.55-20101030053134+0100.tar

Configuring Automatic Copying of Backup Files to the Secondary Server

The SV Director backup program has the ability to copy the backup to a secondary server at the completion of the backup process.



The automatic backup copy process to the secondary server is not supported in release 2.3 and therefore needs to be done manually as described here.

Creating a Backup User

In this step we're assuming the username that will be created is 'backUpUser'; however any non-existing username will work. Be sure to a unique username and not an existing account or anyone's username for the backup user. To configure the backup user do the following:

- 1. Log into the Secondary server via SSH.
- 2. Run the command 'sudo adduser backupUser'.
- 3. Select a **secure password** (12 characters with at least 1 of special character, upper-case, lower-case and number).
- 4. Run the command 'sudo passwd backupUser' and specify the **secure password** from step 3.

Defining 'backup.username' and 'backup.secondarylp'

- 1. Open the Management Dashboard on the primary server
- 2. Select Tools > Advanced > Registry.
- 3. In the Registry Data window, select backup.username



If 'backup.username' does not exist click **Add Row** and specify 'backup.username' as the registry key.

- 4. Click in the Value field and type the backup user created on the Secondary server (See section <u>Creating Backup User</u> if this user has not been created).
- 5. Click **Apply**.

Figure 3. Creating a Backup Username

🔯 Dashboard		Advanced						
🛞 Device Configuration	-							
📝 Event Viewer	-	Nama R	emite					
Director Configuration	1	Description	Mame) Registry					
Tools		p	arameters					
Settings Advanced		Registry Date						
Generate Proof of Play CSV	1		Key	Value	11			
Managa In Memory Log			activeOverlayCount	1	÷.			
Menu Load for Point Of Sale			activeOverlaying	0	10			
Registry			allowUniformBlockingOftPPhone	Ū.				
Reload log-ly properties	-		allowUniformBlockingOfThirdParts	0				
Reset Active Script			beskoplurememe	backupUser				
Restore system data from backup.			channel@uideToDisplay	a				
Run a Task			Add Row Delete Row					
Scheduled Tarks	1.1							
Set Active Script								
Svitch Phone Desktop Graphic		Annh						

- 6. Click Add Row
- 7. Specify **backup.secondarylp** for the Key
- 8. In the Registry Data window, select backup.secondarylp.
- 9. Click in the Value field and type the IP address of the Secondary server.
- 10. Click Apply.

Refer to Figure 4.

Dashboard	Advanced					
🚰 Device Configuration 🍠 Evont Viewer	(Namai R	ommand agistry				
Director Configuration		Description: 4				
Tools		F	arameters			
Settings Advanced		Registry Data				
Generate Proof of Play COV	A		Key		Value	
fanage In Memory Log			volume5		50	
Nenu Load for Point Of Sale			volume6		60	
teautry			volume7		70	
Reload log4j properties			Volume8		80	
Reset Active Script			volume9		90	
Restore system data from backup.			backup.reco	ndarvip	type IP address here	
Run a Task			Add Row	Delete Row		
Scheduled Tasks	1.0			Landson and the second		
Set Active Script	111					

Setting Up Public and Private Keys for the Backup and Restore Task

Follow these steps to set up the ssh keys to allow the primary server to copy files into the secondary server.

1. On the primary server, run **sudo ssh-keygen** and when prompted to 'Enter passphrase' and 'Enter same passphrase again' press Enter.



If prompted for a password with the prompt 'Password:', it is relational to the sudo action so specify your user's password

[jdoe@ primary-sv ~] \$ sudo ssh-keygen Password: Generating public/private rsa1 key pair. Enter file in which to save the key (/root/.ssh/identity): /root/.ssh/id_rsa): Enter passphrase (empty for no passphrase): Enter same passphrase again: Your identification has been saved in /root/.ssh/id_rsa. Your public key has been saved in /root/.ssh/id_rsa.pub. The key fingerprint is: 22:bc:0b:fe:f5:06:1d:c0:05:ea:59:09:e3:07:8a:8c

2. Enter the following commands, replacing 10.10.10.10 with the IP address of the secondary SV server, and replacing 'backupUser' with the backup user created in the <u>Creating Backup User</u> step.



The password prompt in this section is relational to what was set for the user in the <u>Creating Backup User</u> section. Also, you may be prompted to save the RSA key fingerprint of the server. It is safe to say yes if this occurs.

[jdoe@ primary-sv ~] \$ sudo ssh-copy-id -i /root/.ssh/id_rsa backupUser@10.10.10.10 0 manufac@10.10.10.10's password:

3. Now try logging into the machine, with "ssh ' backupUser@10.10.10.10', and check in:

.ssh/authorized_keys

to make sure you haven't added extra keys that you weren't expecting.

4. To verify that this is now working correctly, try to have root log in to the secondary server by entering the following commands:

[jdoe@ primary-sv ~] $\$ sudo scp /etc/hosts backupUser@10.10.10.21:/tmp hosts 100% 43 0.0KB/s 00:00

If the transfer completes with no errors, the setup successfully completed.

Setting Up the Restore Directory

- 1. SSH into the secondary server
- 2. If the directory '/var/sv/RESTORE' doesn't exist create it with the following command:

[jdoe@ primary-sv ~] \$ sudo mkdir /var/sv/RESTORE



 Issue the following command to adjust the owner of the directory /var/sv/RESTORE to the username created in the <u>Creating Backup User</u> step. In the following example, 'backupUser' is used as the user name.

[jdoe@ primary-sv ~] \$ sudo chown backupUser /var/sv/RESTORE



If prompted for a password use your users password

Verifying Automatic Copying of Backup Files

After completing all steps in the <u>Configuring Automatic Copying of Backup Files to</u> <u>the Secondary Server</u> section, verify that it is functioning correctly with the following steps.

- 1. SSH into the secondary server and list all current restore items available using the Is -It /var/sv/RESTORE command.
- 2. Perform the steps in the section Performing an Immediate Backup.
- SSH into the primary server and "tail" the file /opt/sv/servers/config/logs/sv_dev_debug.log until you see 'completed backup task'.

```
[jkobinsk@sande-iapps-b29-5 ~]$ tail /opt/sv/servers/config/logs/sv_dev_debug.log
2011-04-28 15:41:12,332 [DefaultQuartzScheduler_Worker-7] DEBUG com.cisco.sv.backup.BackupManager -
BackupManager Completed md5sum process.
2011-04-28 15:41:12,336 [DefaultQuartzScheduler_Worker-7] DEBUG com.cisco.sv.backup.BackupManager -
BackupManager getMd5Sum computed checksum of 19718340e1b630544f64def42e58311c /var/sv/BACKUP/sv-
2.3.0.70-20110428154000-0700.tar
```

2011-04-28 15:41:12,336 [DefaultQuartzScheduler_Worker-7] DEBUG com.cisco.sv.backup.BackupManager - BackupManager writeChksumFile: writing to file /var/sv/BACKUP/sv-2.3.0.70-20110428154000-0700.chksum message 19718340e1b630544f64def42e5 8311c /var/sv/BACKUP/sv-2.3.0.70-20110428154000-0700.tar

2011-04-28 15:41:12,338 [DefaultQuartzScheduler_Worker-7] INFO com.cisco.sv.backup.BackupManager -BackupManager backup not copying to secondary server, as none is configured in registry backup.secondarylp 2011-04-28 15:41:12,338 [DefaultQuartzScheduler_Worker-7] INFO com.cisco.sv.backup.BackupManager -BackupManager Backup completed.

2011-04-28 15:41:12,338 [DefaultQuartzScheduler_Worker-7] INFO com.cisco.sv.schedule.BackupTask - completed backup task.

4. SSH back into the secondary server and perform another Is -It /var/sv/RESTORE.

[jkobinsk@sande-iapps-b29-5 ~]\$ Is -It /var/sv/RESTORE total 11009588 -rw-r--r-- 1 root root 85 Apr 28 15:41 sv-2.3.0.70-20110428154000-0700.chksum -rw-r--r-- 1 root root 1159065600 Apr 28 15:41 sv-2.3.0.70-20110428154000-0700.tar -rw-r--r-- 1 root root 85 Apr 27 15:41 sv-2.3.0.70-20110427154000-0700.chksum -rw-r--r-- 1 root root 1158625280 Apr 27 15:41 sv-2.3.0.70-20110427154000-0700.tar -rw-r--r-- 1 root root 85 Apr 26 15:41 sv-2.3.0.67-20110426154000-0700.chksum -rw-r--r-- 1 root root 1158625280 Apr 26 15:41 sv-2.3.0.67-20110426154000-0700.tar 85 Apr 25 15:41 sv-2.3.0.67-20110425154000-0700.chksum -rw-r--r-- 1 root root -rw-r--r-- 1 root root 1157355520 Apr 25 15:41 sv-2.3.0.67-20110425154000-0700.tar -rw-r--r-- 1 root root 85 Apr 24 15:41 sv-2.3.0.67-20110424154000-0700.chksum -rw-r--r-- 1 root root 1107640320 Apr 24 15:41 sv-2.3.0.67-20110424154000-0700.tar -rw-r--r-- 1 root root 85 Apr 23 15:41 sv-2.3.0.67-20110423154000-0700.chksum -rw-r--r-- 1 root root 1107650560 Apr 23 15:41 sv-2.3.0.67-20110423154000-0700.tar -rw-r--r-- 1 root root 85 Apr 22 15:41 sv-2.3.0.67-20110422154000-0700.chksum -rw-r--r-- 1 root root 1107650560 Apr 22 15:41 sv-2.3.0.67-20110422154000-0700.tar 85 Apr 21 15:41 sv-2.3.0.67-20110421154001-0700.chksum -rw-r--r-- 1 root root -rw-r--r-- 1 root root 1107650560 Apr 21 15:41 sv-2.3.0.67-20110421154001-0700.tar -rw-r--r-- 1 root root 85 Apr 19 15:41 sv-2.3.0.65-20110419154002-0700.chksum -rw-r--r-- 1 root root 1099212800 Apr 19 15:41 sv-2.3.0.65-20110419154002-0700.tar -rw-r--r-- 1 root root 85 Apr 18 15:41 sv-2.3.0.65-20110418154000-0700.chksum -rw-r--r-- 1 root root 1099212800 Apr 18 15:41 sv-2.3.0.65-20110418154000-0700.tar

5. If there are new files, perform a md5sum on the new .tar file and compare it to the .chksum file. If the values match, everything is working as intended.

[jkobinsk@sande-iapps-b29-5 ~]\$ cat /var/sv/RESTORE/sv-2.3.0.70-20110428154000-0700.chksum **19718340e1b630544f64def42e58311c** /var/sv/BACKUP/sv-2.3.0.70-20110428154000-0700.tar

[jkobinsk@sande-iapps-b29-5 ~]\$ md5sum /var/sv/RESTORE/sv-2.3.0.70-20110428154000-0700.tar **19718340e1b630544f64def42e58311c** /var/sv/RESTORE/sv-2.3.0.70-20110428154000-0700.tar

After a backup is done on the primary server, you can do a restore on the primary system right away. Assuming the secondary server is configured, you can do an automated or manual restore on the secondary server as well. This restore will be able to use the files that the backup task will place on the secondary server at completion of the backup step. The backup files will be on both systems.

In the event a disaster occurs, you can manually copy a backup. For example if the primary server loses a backup set that exists on the secondary server, you can copy the backup from the secondary to the primary, and then do a restore. One item to note is that the backup is really comprised of two files with the same name but different suffices. The file sv-2.2*.tar is a tar file with all the data of the backup. The file sv-2.2*.chksum is a checksum file containing the md5 signature of the tar file. You must copy both files. The restore script will verify the md5 signature.

The backups on the primary server are stored in a directory /var/sv/BACKUP. On the secondary server, the backups are copied to /var/sv/RESTORE. When the manual restore screen is displayed, it lists backups in either directory, concatenated together. This allows you to run manual restore on either the primary or the secondary. An automated restore only looks for files in the RESTORE directory.

Two components warrant special explanation. The backup system assumes that StadiumVision will run with an automated High Available configuration. In this configuration, some of the Unix level files are different between the primary and secondary servers. Therefore, the Unix files are not automatically restored in the RestoreTask on the Dashboard.

Likewise, the schedule of tasks to run in the primary database and the secondary database will be different, due to the existence of the backup and restore tasks. Therefore, the schedule itself is not automatically restored. To restore the schedule from a backup file, specify that component as described in the <u>Running a Manual</u> <u>Restore</u> procedure.

Running a 'Restore system data from backup'

The automatic restore process is appropriate when setting up a High Availability backup server to automatically get the state from the primary server. However, there may be cases when you need to restore a backup on demand as described here:

- 1. Open SV Director and click Management Dashboard.
- 2. Select Tools > Advanced > Restore system data from backup.
- 3. Select the desired components to restore and select the date of the backup file to use for the restore.
- 4. Click **Apply**. The restore will run.

5. Examine the logs in the primary server /opt/sv/servers/control/catalina.out to see if there were any errors during backup.



If you run a manual restore right after a backup, the Dashboard does not properly refresh its list of available backups when you navigate from the backup to the restore section of the Advanced >Tools sections. To refresh the backups listed in the restore screen, exit the Dashboard (e.g. close your browser) and then log back in.

Figure 5. Running a Manual Restore

cisco StadiumVision Management D)a	asl	nboard	
🔯 Dashboard			Advanced	
Device Configuration				Command
Event Viewer			Name:	Restore system data from backup.
Director Configuration			Description:	Restore system data from backup
Tools				Parameters
Settings Advanced			Components	 All Components except Unix, Scheduled tasks
Generate Proof of Play CSV	•			Content Management System
Manage In Memory Log				🔵 Database - Ad Mgr (AIM)
Menu Load for Point Of Sale				🔵 Database - Director (iApps)
Registry				💭 Database - Liferay (menu)
Reload log4j properties				
Reset Active Script				U Database - Proof of Play (PofP)
Restore system data from backup.				Proof of Play Processed Data
Run a Task				Scheduled Tasks
Scheduled Tasks				Unix files
Set Active Script				
Switch Phone Desktop Graphic			System backu	p time
			Apply	

Managing the Restore Directory

As with the backup directory, SV Director does not automatically manage space in the restore directory. To manage disk space in the restore directory, add a daily cron job in Unix cron scheduler to remove old files from that directory. For example to remove all files from the restore directory more than 30 days old run the following command:

/usr/bin/find /var/sv/RESTORE -mtime +30 -exec rm {} \;

Renaming Backup and Restore Files

By default, the files in the backup and restore directories use the following naming convention:

sv-<software version>-<date time>-<time zone>.chksum

where:

software version = current software version (with a dash) and build number. For example: 2-2.0.30

date time = YYYY/MMDDHHMMSS. For example: the entry 20100731152417 is July 31 2010 at 15:24:17

Time zone = the assigned value for the time zone.

For example:

If <version> = "2.2.0.25"

If <date time > = "20100721105831

If <time zone> = "0700"

then the format would be:

sv-2.2.0.25-20100721105831-0700.chksum sv-2.2.0.25-20100721105831-0700.tar

You can change the directory name to add a meaningful description, and change the date, time, and time zone. However, this needs to be done in a very specific location in order for restore to work.

Below is an example of how to add the description 'AfterGiantsGame' to the default restore file name:

mv sv-2.2.0.30-20100721152417-0400.chksum sv-2.2.0.30AfterGiantsGame-20100721152417-004.chksum mv sv-2.2.0.30-20100721152417-0400.tar sv-2.2.0.30AfterGiantsGame-20100721152417-004.tar

You must reload the Dashboard to make the rename take effect.

Important! If you add a description after the version, you must remove the dash.

Scheduling a RestoreTask to Run Ad-Hoc

You can configure the secondary server to periodically restore the backup copied into its /var/sv/RESTORE directory as follows:

- 1. On the secondary server, open the Dashboard and select **Tools > Advanced > Scheduled Tasks**.
- 2. Select Add Row and enter **RestoreTask** for the Task Type.
- 3. Click **Apply**.

4. To run the restore task on demand, select **Tools > Advanced > Scheduled Tasks**.



failboard	Advarced	Advanced								
🛞 Lawra for Agentian	10000									
y frank Tauras	turn the	and Tasks								
Diractor Loofiguration	Carry phines and the	inter for their single Sec.								
a taala	Para	Paramotors.								
Inthings Advanced	toodated Task Sala									
lamanuta Proof of Play CPV		Task 10	Tanin Type	Fash Torse	Dervern					
Nanage In Memory Log		¥.	Hatterigtank	1251.004	10170					
Nets Land for Park Of Lan			INFRIDE ALL PARK	1964 (100	retta	10				
Tegistry			BankgTash	5% 66	10.08 g					
teload look properties			RestoreTail							
Land Article Scool						1				
Carbon operant data films ballup.										
fun a Tash		Add Poor	12							
Information Tanks	1	Constructional Association	1			_				
tet Adaya Bolat										

Running an Immediate "RestoreTask"

To initiate an immediate restore of the system:

- 1. Open SV Director and click Management Dashboard.
- 2. Select Tools > Advanced > Run a Task.
- 3. Select RestoreTask. Refer to Figure 9.
- 4. Click **Apply**.

Figure 7. Running an Immediate Restore



Running a Scheduled Restore

The secondary server can be configured to mirror the primary server by periodically restoring to the secondary server, the backup of the primary server that is periodically automatically copied to the secondary server's /var/sv/RESTORE directory. To schedule an automatic restore of the primary server's data on the secondary server, to run at regular intervals, do the following on the secondary server:

- 1. Log in to the Management Dashboard.
- 2. Select Tools> Advanced > Scheduled Tasks.
- 3. Click Add Row and scroll to the new blank line. Refer to Figure 11.
- 4. Type an ID.
- 5. Click in the Task Type column and type RestoreTask.
- 6. Click in the Task Time column and type the time at which you would like the backup to run.
- 7. Click **Apply**.

Fiaure 8.	Running a Scheduled	(Automated)	Restore
i igai o oi	rtanning a Contoaaloa	(, iaioinaioa)	,

Bashlourd .	Means	Advanced										
😸 Device Costiguration			2224									
🖋 Everet Warner		Name Enabled Tonic										
21 Director Configuration	Deep	Description and Amme in the register.										
a bask		Persenters										
Settings Advanced	504											
enerate Proof of Blas CEV			Back 100	Taul: Type	Task Term	turners						
arage In Memory Log	101		2	StageArtive 2mps	04.45	central						
envised for Point Of Sale			1	ParticultureTask.	38.46	and g						
un and a second s			1.	PerformenterDataTask.	04:20	0.07.0						
ties and kinging properties				HPMP-regEarts	05.00	and g						
and Addies Strept				H#MERatusTarik	06:10	cantig	_					
estore system data from backup.				RephreTail.	01.00	and a						
un e Teak			Add Nor	Bare								
Nexded 7844			had not been and the state of the	HINN'S.								
at Autina Barlat												

Restoring System Data from a Scheduled Backup File

The automated restore assumes that SV Director is running in an automated, highly-available configuration. In this configuration, some of the Unix files differ between the primary and secondary servers. Therefore, the Unix files are not automatically restored through the RestoreTask.

Also, the schedule of tasks to run in the primary database and the secondary database will be different, due to the existence of the backup and restore tasks. Therefore, the schedule itself is not automatically restored.

To restore the schedule from a backup file:

- 1. Open SV Director and click Management Dashboard.
- 2. Select Tools> Advanced > Restore system data from backup.
- 3. Enable the **Scheduled Tasks** radio button. Refer to <u>Restoring System Data from</u> <u>a Scheduled Backup File.</u>
- 4. Click Apply.

🗑 Dashboard			Advanced				
🙀 Configuration							
音 Tools				Comm	and		
Settings Advanced			Name:	Restore	system data from backup.		
Generate Proof of Play CSV			Description:	Restore	system data from backup		
Manage In Memory Log			Parameters				
Manage Global DMP Settings			Components	All Components except Unix, Scheduled tasks			
Menu Load for Point Of Sale							
Registry				Content Management System			
Reload log4j properties				🔵 Database - Ad Mgr (AIM)			
Reset Active Script			 Database - Director (iApps) Database - Proof of Play (PofP) 				
Restore system data from backup.							
Run a Task Scheduled Tasks Set Active Script				eduled Tasks			
				Unix files			
Switch Phone Desktop Graphic			System backu	p time	Mon May 17 10:36:27 PDT 201		
					Fri May 14 08:35:34 PDT 2010 🗏		
					Tue May 11 13:59:17 PDT 2010		
	≣				Tue Mar 02 14:51:28 PST 2010		
					Tue Mar 02 14:13:42 PST 2010		
					Tue Mar 02 01:28:43 PST 2010		
					Mon Mar 01 17:37:33 PST 2010 👻		
			Analy				

Figure 9. Restoring System Data from a Scheduled Backup File