Backups

Regular backups are required in order to keep your system up and running. That sounds obvious and even if using RAID 1 disk redundancy and a solid machine, things can go wrong. The last thing you want to do in an emergency is re-enter all the configuration information. sipXecs facilitates the automation of backups so that adminstration of the system is streamlined. Backup can be automated by copying files to the local drive, FTP to another server, or copied via convenient links that are provided when the backup is completed.

The sipXecs system provides automated backup using the sipXecs Configuration Server. Backup is found by going to System/Backup.

- Manual Backup
- Scheduled Automatic Backups
- Backup for High Availability (HA) systems
    - Restoring a Distributed System

Manual Backup

Clicking on *Backup Now* creates two different backup archives. A configuration Tar file, and a Voicemail Tar file. You can select how many backup files to store on the local server with a dropdown box. After successful completion of the backup process links to the two files are presented. By clicking on these links the backup files can be downloaded to your PC.

WinSCP is an example of one tool that can be used to copy files manually to another machine.

Scheduled Automatic Backups

Scheduled backups creates backup files on the sipXecs server itself. In most cases this is not very practical and therefore you should use a Linux console or some other tool to get the files copied to another system.

Backup files are created in `/var/sipxdata/backup` in a subdirectory whose name corresponds to the date and time the backup was made. To get the backup files onto another system, you can

- Use NFS or a similar mechanism to mount this directory to a different machine
  or
- Automatically FTP the files to a remote server
    - To backup to an FTP server, pasv_enable must be set to YES.

Backup for High Availability (HA) systems

In an HA cluster, the server with the Management role has all the configuration data needed to recreate a complete configuration for any of the other servers. This makes it especially important that the Management server be backed up regularly, and simplifies restoring the configuration of any other server.

Restoring a Distributed System

To restore configuration data to a distributed system, select the system on the System>Servers page, and execute the "Send Profiles" command.

If the above fails, check to see if there is network connectivity to the distributed system. If not, correct the network problem. If there is network connectivity, then the problem may be that the TLS/SSL certificate for the distributed system has been lost. To restore it, go to the Server page for that server and find the system setup password for it, then log in as root on the distributed system and execute `sipxecs-setup`: it will prompt you for the full name of your Management host and the setup password and use that information to reload the certificate and other initial setup data from the Management system.