Configuration File Backup and Restore

To help with recovery in the event of a hardware failure, the CSN includes a backup mechanism that backs up its configuration files to Netmail Store and then allows restore of those backups at a later date. The backup list and functions can be accessed from the **Backup and Restore** tab.

Backup Manifest

A manifest anchor stream is created in the storage cluster with the first backup set and updated with every subsequent backup. The UUID for the manifest is displayed at the top of the backup interface. It will not display until after the 2nd backup has been created.

> *Note: Administrators should copy this UUID into a safe location so that in the event of a complete system failure the list of backup sets can be retrieved from the storage cluster.*

The backup manifest is written with metadata that allows retrieval from the cluster with Content Router if the UUID is ever lost. Specifically the two following headers will be present on the manifest anchor stream:

```
CAStor-Application: backup_csn

CAStor-Application-Component: manifest
```

Automatic Backups

The backup utility watches a pre-determined list of CSN configuration files for file metadata changes. When a change is detected, the utility waits until the changes stabilize to prevent multiple incremental backups in a short time period and then creates a gzipped tar file with a complete set of all designated configuration files. This tar file is staged locally and then written to the storage cluster for protection. If for any reason, a backup

fails to write to Netmail Store, an error will be logged and the backup will be retried periodically. The UUID of the backup set is also written into the Backup Manifest but is not displayed in the user interface. If the Backup Manifest is not retrievable for any reason, the backup set is written with metadata that allows retrieval from the Netmail Store cluster using Content Router. Specifically, the following two headers will be present:

```
CAStor-Application-Automatic-Backup: yes
```

```
CAStor-Application-Component: saveset
```

The backup utility will periodically purge backups based on both age and backup count. The utility will keep at least 20 backups and, if there are more than 20 backups, it will purge any that are more than 30 days old.

> **Note:** All backup times are displayed in Universal Time (UTC) and may not, therefore, correspond with the local system clock.

Manual Backups

Administrators may wish to occasionally create a backup manually in conjunction with CSN maintenance activities (system updates, server downtime, etc). To create a manual backup set at anytime, click the **Create Backup** button. You will be prompted to enter a description for the backup to allow you to easily identify it in the backup list at a later date. The user interface will confirm that the backup request has been successfully received but cannot display errors if the backup fails several minutes later. Administrators may wish to monitor system logs for Error messages as a result. Aside from the manual initiation and description, manual backups are identical to automatic backups. Manual backups are supported once every 30 seconds.

Restoring a Backup

To restore the service configuration files and enabled/disabled status as they existed as part of a specific backup set, select the radio button next to the desired backup set and click the **Restore Backup** button. This will restore all configuration files and each service's status (enabled or disabled) to their saved state at the time of the selected backup and reboot the server to reinitialize the network with the previous configuration. Following a successful reboot, administrators should immediately restart their Netmail Store cluster to ensure the internal networks are aligned and the node IP addresses are maintained.

After upgrade, previous backup sets may be marked as being compatible with a previous software version if the backup format or system layout has been changed. These backups cannot be restored with the current version but will remain available if the software is reverted to a previous version using the csn-reset functionality.

Failover

If a primary CSN fails, an administrator can choose to promote a secondary CSN to the primary CSN role by restoring the primary's backup manifest UUID onto the secondary and then restoring a backup set from the restored manifest list. The primary's backup manifest must have at least 2 backups in it prior to being used for failover. To assist with this transition, the secondary CSN periodically pulls the primary's Backup Manifest UUID via the privileged SSH channel and stores it in the following location on the secondary: */etc/caringo/csn/primary-manifest.txt*. A timestamp on this file will notate the last time it was updated.

To restore a manifest, click the **Change Manifest** button at the top of the backup interface. This will bring up a entry box where the UUID you would like to restore can be entered. The entered UUID must be for a valid backup manifest created by the backup utility. If restoring a manifest on a machine that has an existing manifest and associated backups, admins must be aware that the backup list will be completely overwritten when the entered manifest is restored.

Administrators should be aware that the secondary will effectively take on the identify of the primary when the manifest and a selected backup within it are restored.

> **Note:** Demotion of a Secondary CSN's backup set onto a Primary CSN is not supported. Failover should only be done when the Primary is not expected to return to service soon enough for the environment's needs. A complete software rebuild of the original Primary to reconfigure it as a Secondary will be necessary before returning it to service after a Secondary has taken over its role.

Failover Without Netmail Store

If the failure or demotion of the Primary CSN coincides with an outage of the Netmail Store cluster, you will be unable to pull the Primary's Backup Manifest UUID from the cluster to restore it onto the Secondary. In this scenario, an administrator can manually restore the Primary CSN's last recorded backup set, which is updated hourly on the Secondary CSN if it has changed. The following command will restore the Primary's backup set onto the Secondary, effectively making the Secondary assume the role of the Primary CSN. The script should only be performed from the Secondary CSN with both the Primary CSN and the CAStor cluster offline:

```
/opt/caringo/csn/bin/failover_without_castor
```

The script will restart the Secondary CSN after the Primary's configuration has been restored.