zCustom.OnlineBackupSimple

Version History

* 20131121 – work in progress….initial version, Glen Pitt-Pladdy (InterSystems)

# Important

These tools are developed for the needs of the TrakCare UK Infrastructure team and reflect conventions and approaches used to meet the needs of deployments in the UK. They are released on the basis that they may be useful to others within InterSystems.

The development process is on an ad-hoc basis, generally based on adding or updating tools as needed for deployments. There is negligible testing and no QD process nor any sort of managed release process. These are simply rolling snapshots of work in progress and may be in a severely broken state.

Use at your own risk.

# Purpose

Backups are a critical part of any robust business continuity plan, yet widely neglected. When all else fails, backups are the final mechanism for recovery so it is imperative that they can be used to restore systems to fully operational.

For main TrakCare environments the comprehensive zCustom.SnapBackup toolset would normally be used in the UK, however some peripheral systems with minimal data and configuration (eg. Simplecode Audit Database) may benefit from a simple Online Backup and that is what this tool provides: A basic schedule item that can be customized to do backups of databases and Security Export on a regular basis, purging older backups as needed.

# Usage

## Installation

The .xml is simply imported into the appropriate namespace, typically %SYS and compiled. This may be done via Studio, Caché Terminal or the SMP.

At that point the Scheduled Task should be available in the appropriate namespace.

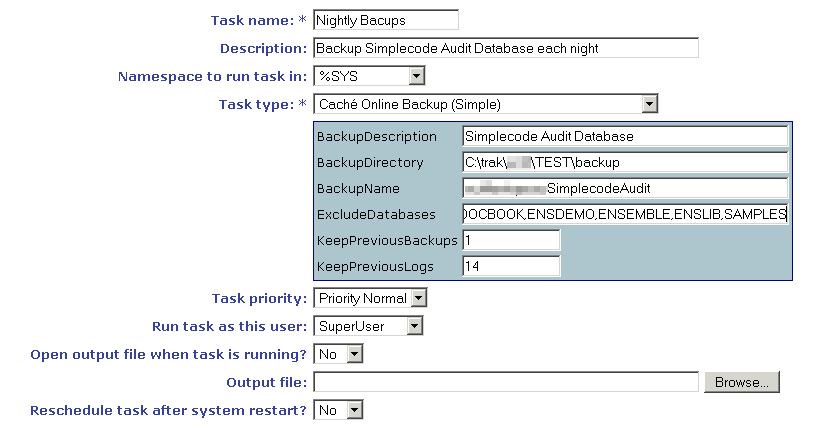
## Configuration

Simply create a new Task and select "Caché Online Backup (Simple)" as the Task type.

Fields are:

* BackupDescription – this is used in the .cbk file for the backup description so useful to have a description that will be meaningful at a later date should recovery be needed
* BackupDirectory – this is the directory on the system where backups should be kept. This directory must be writable by Caché and should not be used for other purposes as conflicts could occur
* BackupName – this is the filename to use for backups and it will be prefixed with a timestamp and suffixed with the type and an appropriate extension
* ExcludeDatabases – this is the set of databases to exclude from backups. It's important to exclude rather than add databases since any new databases will be automatically included which reduces the risk of human error resulting in critical data loss. This is a comma separated list and will normally be low-value and system database such as: CACHELIB,CACHETEMP,DOCBOOK,ENSDEMO,ENSEMBLE,ENSLIB,SAMPLES
* KeepPreviousBackups – this is the number of generations of backups to keep. The purge is done after backup so space needs to be available to store at least two generations. This ensures that there is always one complete backup.
* KeepPreviousLogs – this is the number of generations of log files to keep. The same applies as with backups, however it may be useful to keep more log files for reference.

Example Scheduled Task:



## Testing

Once configured its worth running a test and verifying a few iterations of backups, and periodically testing that the system is still working.

When a backup is performed it should create 3 files for each backup:

### YYYYMMDD-hhmmss-ConfiguredBackupName-Backup.cbk

This is the main Caché online backup file and is likely to be the largest file. It should contain backups of all the databases not excluded.

### YYYYMMDD-hhmmss-ConfiguredBackupName-Backup.log

This is the log file for the corresponding Caché online backup.

### YYYYMMDD-hhmmss-ConfiguredBackupName-SecurityExport.xml

This is a Security Export which gives configuration data relating to security which may be needed to restore the system without reconfiguring dependent systems.

## Monitoring

Backups are critical and thus important to monitor. While regular manual checks and tests of backups are important, it's also recommended that Caché is configured to email any failure reports so that problems can be immediately addresses and backups kept fully functioning.

Additional monitoring may be configured with external systems (eg. Nagios) which checks the size is sane and freshness (recent) of backup files as well as parses the .log file to ensure successful backups.