Best Practices: Client

This document contains the best practices for a local client machine running Steelgate Cloud Backup

Introduction

Steelgate Technologies recommends the following best practices in setting up and running Steelgate Cloud Backup.

Offsite

- Use offsite backup with critical data to help avoid a single point of failure.
- Select only critical information to back up offline to minimize the amount of data being transferred, and increase overall performance.
- (xSP) To enable FastBIT transfers for a file, that file must have at least 2 copies previously backed up on the server.
- (xSP) To enhance FastBIT, make sure the Work directory has free disk space totaling at least 3x the total amount of data you want to transfer.
- Make sure ports 308 and 4502 are open in both directions.

Local

- Create a rotation schedule as opposed to running each backup manually to increase the stability and performance of your backups.
- Schedule weekly Full Backups and daily Incremental Backups to maximize your rotation's efficiency.
- Use more than one device for your backups, ideally alternating between devices regularly to avoid a single point of failure.
- Schedule jobs to run after office hours to ensure that all information is current and that the software will not interfere with normal procedures while it runs.

Disaster Recovery

- Update Disaster Recovery (DR) images monthly. More frequent images are generally inefficient and less frequent images can be outdated.
- DR Images can be scheduled to run monthly by scheduling it to run on a single day (for example, Saturday) and setting it to run only every 4th day. This tells the software to run a DR Image every 4th Saturday.
- Ideally, keep 2-3 DR images stored separately to avoid a single point of failure.
- Create a new DR image any time new hardware or software is installed to minimize compatibility issues.
- If your machine requires a hardware replacement, make sure any new hardware is as similar as possible (preferably identical) to minimize compatibility issues.

- Store at least one recent DR image at an offsite location to protect your data in the event of a serious disaster, such as a flood or fire at your business.

- If backing up to a removable device, keep one device onsite and one device offsite, and swap these weekly. You will always have the previous week's data offsite in case of a major disaster.

- Create DR boot disks for each device – one boot disk will not work across all devices.

Plugins

- If using Exchange 2007, place the Steelgate Could Backup Exchange 2007 plugin into the BIN folder of the Exchange directory. Set the Steelgate Cloud Backup service to run as a Domain Administrator with credentials that can be recognized by Exchange/SQL.

- Our SQL plugin supports MSSQL only, will not work with MySQL or Pervasive.

- Only one instance of SQL can be installed and running, other instances will cause a conflict.

Restores

- Stop any non-essential services when running a restore to increases overall stability during the restore.

- Ensure that the hardware configuration has not changed, or is as similar as possible to the configuration when the data was backed up.

- The "Restore File to Alternate Location" setting allows you to restore files without overwriting existing information.

Logging

- Logging Options can be found under Settings > Notification.

- Set logging to Summary (default) unless you are troubleshooting an issue with backing up/restoring.

- Email logs to monitor your backup jobs remotely.