Thinware vBackup version 5.0 has many new features. This document will simply cover the high-points on what's new—mostly for the purpose of helping you understand how to get the most out of version 5.0 and its support for VMware vSphere 6.5 and 6.7.

Settings:

Integration Utilities:

- Removed support for VMware Consolidated Backup and VMware vCenter Converter Server (for physical machine replication).

Logging (new tab):

- Added ability to enable/disable Windows Event logging.
- Added ability to enable/disable task logging. Task logging replaces the text file based logging in prior versions. The new task logging feature comes with the ability to set how many tasks are maintained in history as well as the ability to enable/disable logging of support data. Support data can be used by Thinware support staff to aid in troubleshooting. All support data is encrypted when you export it to send to Thinware Support. This ensures the security of your data should the communication be intercepted by a malicious third-party.

Email Notification:

- Added ability to enable/disable e-mail notification.
- Added UI place holders for future "notification level" feature. In a future release you will be able to control when e-mail notifications are sent (e.g. always, when a job fails or completes with errors or only when a job fails).
- Moved SMTP server settings to separate tab.

SMTP Server (new tab):

- Added support for enabling Explicit SSL.

Client Preferences:

- Changed "Expand all servers at startup" default value to True. Note: setting is now called "Expand all datacenters and servers at startup". The ability to add Datacenters and organize management servers and host servers (and their virtual machines) is planned for a future release. Optionally, in version 5.0, if you want to get a head start on this, you can set/change the Datacenter setting for management servers and host servers directly in the database. To do this; simply edit the vBackup.xml file in the vBackup application directory and set/change the Datacenter setting value. This value will be recorded in all task entries created so that the task history can be filtered by datacenter (in future releases).
- Added new setting: Tasks to Display in History. This setting controls how many task entries are loaded in the Task History tab for datacenters, for management servers, host servers and virtual machines (note: version 5.0 will only include the ability to see task history for virtual machines).
- Added UI place holder for timeout of future "recent tasks" feature.

Scheduled Tasks:

Version 5.0 now includes the ability to view, execute, enable and disable vBackup related scheduled tasks from within vBackup Client. This is accomplished by means of a new Task Scheduler Intermediary service. This service sits between vBackup and Windows Task Scheduler. Our hope here is to add tighter integration with Windows Task Scheduler and avoid creating another scheduling service that runs on the backup server. We are still open to the idea of adding a separate, vBackup dedicated, scheduler, but we would like to see how this configuration is received by our users first.

To enable the Task Scheduler Intermediary service you need to do complete the following steps:

1. In Windows Task Scheduler, create a folder called “Thinware” under “Task Scheduler Library”. Create a second folder called “vBackup” under the Thinware folder.
2. Move your vBackup related scheduled tasks to the new “Task Scheduler Library\Thinware\vBackup” folder. You can do this by simply exporting your current scheduled tasks and then importing them into the new folder. IMPORTANT: Be sure to delete or disable the original scheduled tasks so that you do not have two duplicate scheduled tasks trying to run at the same time. You might consider disabling the original scheduled tasks before you export them and then use vBackup Client to enable the scheduled tasks once they are imported into the new folder (and once the intermediary service is started, see step 3 below).
3. Create a new scheduled task to start the Task Scheduler Intermediary service at system startup. This scheduled task should be stored in the “Task Scheduler Library” folder. Add a trigger to begin the scheduled task “At startup” and add an action to “Start a program” and set the “Program/script” to “%VBACKUP_APP_DIR%\vBackup_TaskSchedulerIntermediary.exe”. Replace “%VBACKUP_APP_DIR%” with the path to the vBackup application directory as configured on your system. Name the scheduled task “vBackup_TaskSchedulerIntermediary” and set it to run using an account with admin rights on the backup server, whether the user is logged in or not, and with highest privileges.
4. The vBackup_TaskSchedulerIntermediary scheduled task will need to be running in order to keep vBackup and Windows Task Scheduler synchronized. Right-click the scheduled task and click Run.

Management Servers:

Properties:

- Added new setting: “Web Services Port”. This setting is used to change the port used to communicate with the management server via VMware vSphere Web Services API. Typically you will leave this setting blank (defaulting to 443); however, if you have another service using port 443 on your network and you need to change the listening port on your management server vBackup will now support this configuration.
- Removed “VADP Port” and “VCB Port” settings.

Host Servers:

Properties:

- Added new setting: “Web Services Port”. This setting is used to change the port used to communicate with the host server via VMware vSphere Web Services API. Typically you will leave this setting blank (defaulting to 443); however, if you have another service using port 443 on your network and you need to change the listening port on your host server vBackup will now support this configuration.
- Added new setting: “Command Protocol”. This setting replaces the “SSH” and “VADP” in the “Type” setting for jobs in version 4.x, making the command protocol setting now stored at the host server level.
- Added new setting: “Data Transfer Protocol”. This is a new feature which allows for using SCP (or SCP with compression) for moving files to/from local (backup server) accessible storage and host server accessible storage. If you want to store backup data on local accessible storage and you will be backing up virtual machines on a host server running VMware ESXi 6.5 or newer you will need to use SCP or SCP+C as NFC is not supported beginning with VMware ESXi 6.5.
- Added new setting: “NFC Port”. This setting is used to change the port used by VMware Virtual Disk Manager to backup virtual machine virtual disk files to local accessible storage. Typically you will leave this setting blank (defaulting to 902).
- Removed “VADP Port” and “VCB Port” settings.

Virtual Machines:

Properties:

- Added UI place holders for future “virtual machine specific e-mail notification settings” feature.

Virtual Machines – Jobs:

Properties:

- Added new setting: “Backup Repository Type”. This setting allows for backup to host server accessible storage targets. Host server accessible storage is any storage accessible to the VMware ESXi host server. This can be a datastore on local storage or on a SAN, NFS or iSCSI storage device. Our users often call this new feature a “game changer” as, when implemented, it is possible to get 2-4x backup speeds over prior versions, restores which only take seconds and the new ability to centralize backup management and control backup and restore operations over a WAN connection.
- Added new setting: “Expire (and delete) old backups before new backup is created”. Enabling this setting is useful when you have a shortage of backup storage and need to make room for new backups before they are created. All prior versions required you to maintain enough free space on your backup storage target to create and store one additional backup.

Virtual Machines – Jobs (continued):

Properties (continued):

- Added new setting: “Save backup disks in hosted disk format”. In all prior versions backup virtual machine virtual disks were always created in hosted disk format. Because of this, the backup restore process in all prior versions had to convert virtual machine virtual disks back to “managed” format when copying them back to the host server. Disabling this option removes the requirement to convert the disk format during restore operations and, when backups are stored on host server accessible storage, allows for *instant* recovery of the virtual machine to a VMware ESXi host server. Disabling this option also removes compatibly of backups with VMware Workstation or VMware Player, so please consider this when setting this option. One way to look at this is; if your backups will be stored on local (backup server) accessible storage, you might want them to be compatible with VMware’s hosted virtualization products (i.e. VMware Workstation or VMware Player). If your backups will be stored on host server accessible storage you will probably want them to be readily available to run on the host server; so, leaving them in managed format might make more sense.
- Added new setting: “Split backup disks into 2GB extents”. This setting allows you to disable splitting backup virtual machine virtual disk files into multiple files. In all prior versions backup virtual machine virtual disks were always split into multiple files.
- Added UI place holders for future “incremental backup” feature.
- Added UI place holders for future “multi-threaded disk backup” feature.
- Added UI place holders for future “backup process priority override” feature.
- Added UI place holders for future “virtual machine state control” feature.
- Added new setting: “If temporary snapshot abandoned by previous job run…”. The options in this setting allow you to control what happens when a job encounters a temporary snapshot abandoned by a previous job run. In all prior versions the job would simply fail and report that a temporary snapshot exists. This required manual intervention to remove the abandoned temporary snapshot before the job could be ran again. In version 5.0 you can now set a job to automatically remove the abandoned temporary snapshot and proceed without failing automatically.
- Added UI place holders for future “job specific e-mail notification settings” feature.

Actions:

- Added new context (right-click) menu item: “Execute Now (test mode)”. Running this command allows for testing all job settings, connectivity and configuration of virtual infrastructure and availability of backup storage without actually moving any data. This replaces the “debug breakpoint” terminology and functions in prior versions.
- Added new context (right-click) menu item: “View Task History”. Running this command allows for automatic filtering of virtual machine task history based on the job selected (see below). This replaces the “view log” function in prior versions.

Virtual Machines – Restoring Backups Located on Host Server Accessible Storage:

With version 5.0's new ability to store backups on host server accessible storage, restoring a backup has never been easier *and* production recovery has never been faster.

The following is a simplified recovery process that can be used to recover backups created with version 5.0 (when backups are stored on host server accessible storage). For more complex scenarios (such as when you would like to rename a restored VM or change the provisioning type of a restored VM's disk files, etc.) see the vBackup Administrator's Guide.

Note: For a single-part recovery process, simply skip steps 3-4 in part 1 and steps 1-4 in part 2 (only complete steps 1-2 in part 1 and steps 5-7 in part 2).

Part 1 – Instant Recovery:

1. Open VMware vSphere Client (web or desktop) and login to the host server.
2. Use the datastore browser to locate the backup you wish to restore.
3. Right-click the VMX file in the backup directory and click "Register VM" (note: in the desktop version of vSphere Client this menu item reads "Add to Inventory").
4. Locate the VM in inventory and power-on. The VM will now be running from backup storage.

Part 2 – Permanent Recovery:

Once a tech window can be scheduled you can easily move the recovered VM back to production storage using the following steps.

Note: The following steps assume Part 1 – Instant Recovery steps were completed previously.

1. Open VMware vSphere Client (web or desktop) and login to the host server.
2. Locate the VM in inventory and power-off.
3. Right-click VM and click "Remove from Inventory".
4. Use the datastore browser to locate the backup you wish to restore.
5. Right-click the backup directory and click Move. Select new location for VM data folder on production storage.
6. Once backup directory is moved to production storage, right-click the VMX file (located in the new data folder location) and click "Register VM".
7. Locate the VM in inventory and power-on. The VM will now be running from production storage.

Virtual Machines – Task History:

- Added new tab: "Task History". This tab allows for viewing the backup job history per virtual machine. The task list can easily be filtered based on task description, job name, backup name, which user executed the job, or the date/time the job was started or completed.

Physical Machines:

- Removed support for creating replicas of physical machines. This feature was never really adopted by our users and therefore was never moved out of "experimental" status. Removing this feature allowed us to clean up the code base a little and allows us to move forward and zero in on what we are really good at anyway—virtualization.

Miscellaneous/Performance Enhancements:

- Added support for TLS v1.1 and v1.2. In version 5.0, connections to management servers and host servers are established using the highest server supported security protocol.
- Ping no longer used as a part of connectivity validation. In support of newer security standards, version 5.0 no longer requires a ping response in connectivity validation processes. Connectivity validation processes in version 5.0 now use TCP port and service connection tests.
- Federal Information Processing Standard (FIPS) compliancy. All security and encryption algorithms in version 5.0 have been redesigned, tested and validated against current U.S. government computer security standards. Enabling FIPS-compliant algorithms in Windows Group Policy was not supported with prior versions. Version 5.0 resolves the incompatibility issues and supports FIPS-compliant algorithms being enabled.
- Completely redesigned and redeveloped the backup engine. When we say that the backup engine in version 5.0 is brand new this is not an over statement. With this version, when it comes to the backup engine, we started with a clean slate—an empty code project—and completely redesigned and rewrote every line of code. We know that vBackup version 5.0 has been a long time coming. This was a huge investment for us and we believe it was worth it because our users will definitely benefit from the several years worth of man hours we spent in recreating vBackup.
- Added new database write locking feature. When running multiple backup jobs concurrently, previous versions of vBackup would sometimes encounter write collisions. The new database write locking feature in version 5.0 should alleviate this issue and allow for more aggressive backup configurations.

Thinware vBackup – What's New (v4.0 to v5.0)
Revision: 5.0.0-1

The latest product updates and most up-to-date documentation can be found on the Thinware website at: http://www.vbackup.com/

Thinware, Inc.
http://www.thinware.net/