PATHOGEN ASSET CONTROL SYSTEM

PACS BACKUP GUIDE

SI-P-5-8-001-01

Revision 3

Contents

REVISION HISTORY

Revision	Issue Date	Comments
1	October 11, 2021	Initial version
2	October 19, 2021	Formatting and style changes
3	November 1, 2021	Correction made to text in Section 6.3; Formatting and style changes

1. INTRODUCTION

This document describes the backup process of the Pathogen Asset Control System (PACS).

2. CLASSIFICATION

2.1 AREA

- Hardware
  - o Off-site Backup
  - o RDX Cartridges Replacement
- Software
  - o PACS Backup Strategy
  - o Backup Jobs
  - o PACS Database Backup/Restore Procedure

2.2 INSTRUCTION TYPE

- Maintenance and Support

2.3 APPLICABLE PRODUCT VERSION(S)

- Windows Server 2019/2016/2012/2012 R2 Standard Edition
- Microsoft SQL Server 2019/2017/2016/2014/2012 Standard Edition, 2019 Express Edition
- Pathogen Asset Control System (PACS) 5.8.834

3. REFERENCE DOCUMENTS

This document has the following reference documents:

Document Abbreviation	Document Official Name	Link (if applicable)
M&S Plan	SI-P-5-8-001-00 PACS Maintenance and Support Plan	https://pacs.btrp.net/wp-content/uploads/2021/08/SI-P-5-8-001-00-PACS-Maintenance-and-Support-Plan.pdf
PACS Setup Guide	SI-P-5-8-000-01 PACS SETUP GUIDE	https://pacs.btrp.net/wp-content/uploads/2021/05/SI-P-5-8-000-01-PACS-Server-Workstation-Brief-Configuration_052721.pdf

4. PREREQUISITES

This instruction has the following prerequisites:
1) The PACS Setup Guide instruction shall precede the current instruction.
2) The M&S Plan instruction shall precede the current instruction.

5. PACS Backup for PACS Database on a server

If your center / facility stores PACS database on a server, then it means that the PACS is being automatically backed up daily at the pre-configured time, and the backup stack depth stored on the server are:

- Daily backups going back 7 days.
- Weekly backups going back 4 weeks per Server Configuration.
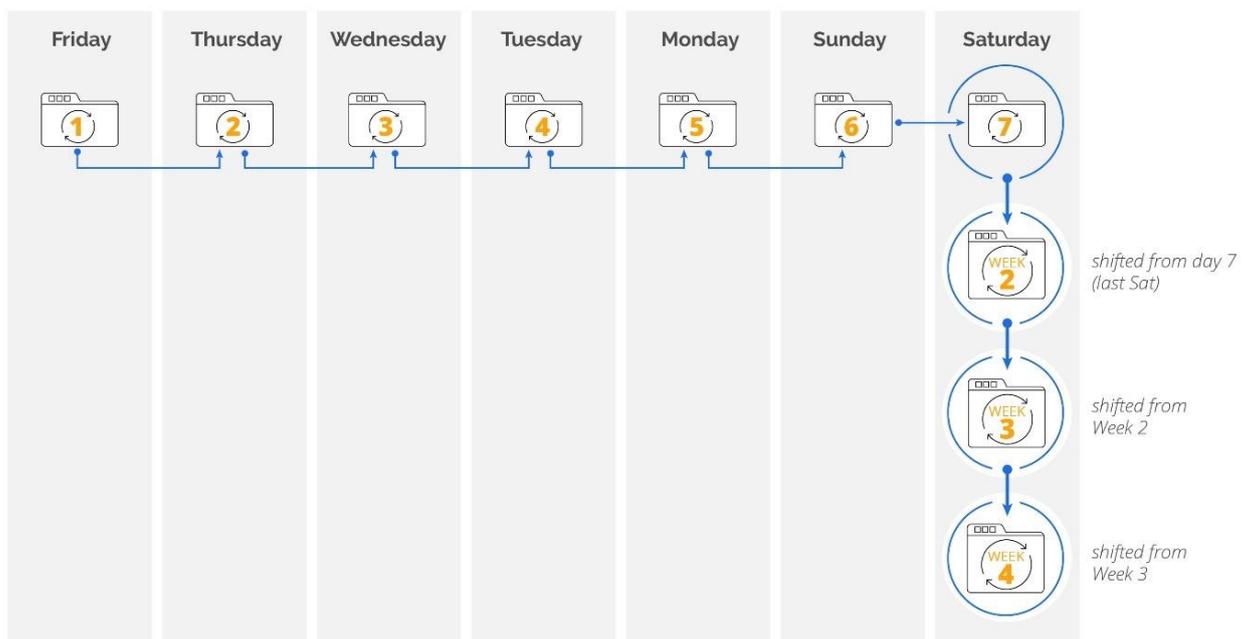
Figure 1. PACS Backup Stack Depth Illustration

Each time the PACS application is updated, an SQL database backup is also taken during the process.

5.1 How to verify the integrity of the backups

According to the best practices and information security standards, including ISO27001, it is highly recommended to periodically check stored archive data for its timely creation, relevance, confidentiality, integrity, and availability. The backup storage device and the data stored on it should be checked every two weeks, and any loss or missing data should immediately be reported to the organization's relevant leadership for further investigation.

The integrity of the stored archive data can be verified by checking the location where the backups are stored – the "_rotate" folder on the server (**E:\BACKUP_rotate** folder). There should be folders 1-7 (for daily stack), and 3 other folders: Week 2, Week 3, and Week 4. Go to folder "1" – this will contain the latest backup. If the file was modified yesterday or today, this means that the backup is working correctly. Please feel free to contact BV support personnel if you have any questions.
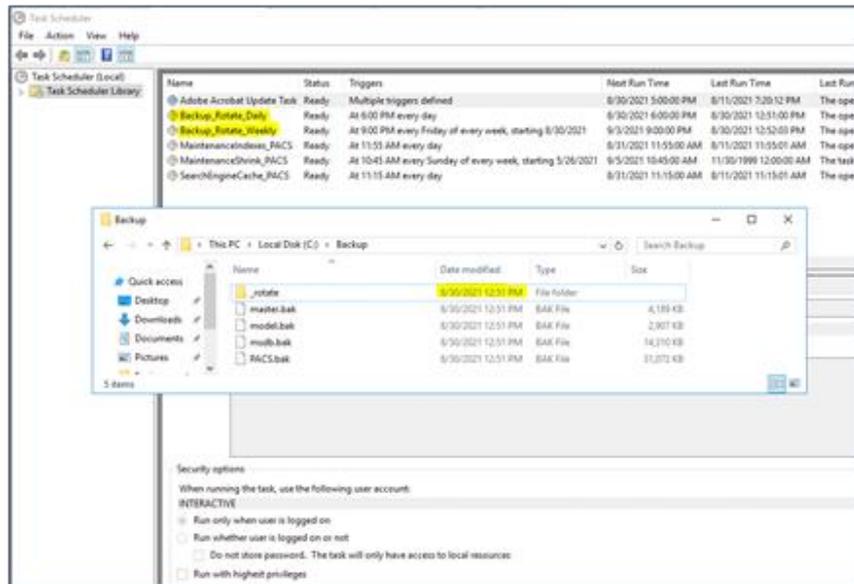
Figure 2. Task Scheduler

In Windows Task Scheduler, *Backup_Rotate_Daily* and *Backup_Rotate_Weekly* tasks (in yellow highlight) provides information on what time the backups are scheduled to occur; Date modified column in *Backup* folder or the "*_rotate*" folder details the date and time last modified (in yellow highlight). This should be checked every 2 weeks to ensure backup is working correctly.

Additionally, the whole PACS Virtual Machine (VM) is usually backed up to an external tape (RDX cartridge) or LTO (LTO6/7/8) weekly. These tapes/LTO should ideally be changed each week, and stored off-site, in case there is any force majeure event, then at least all information up until that week will still be recoverable.

5.2 RDX Cartridges replacement procedure

Ejecting Cartridge

1. Press the **Eject** button on the front panel.
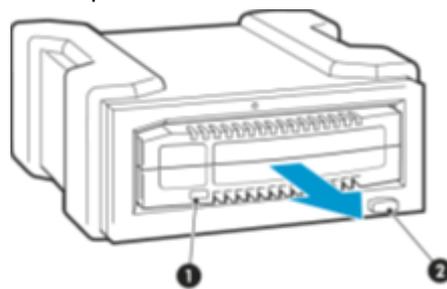
Figure 3. ❶ – Cartridge activity LED; ❷ – Eject button

*Note: On the internal model, the **Eject** button is to the right of the cartridge slot.*
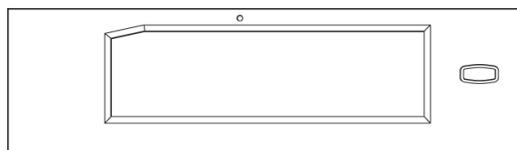
Figure 4. Front panel of an internal drive

2. The drive completes any task it is currently performing and ejects the cartridge. When the cartridge has been ejected by the unit, grasp the exposed sides of the cartridge, and pull it straight out.

Inserting cartridge

1. Insert a cartridge into the unit with the keyed corner facing the upper left corner of the RDX Removable Disk Backup System. The cartridge fits in only one orientation. (The write-protect tab is on the back right of the cartridge.)

2. Push the cartridge gently into the unit until it locks into place with a clicking sound.
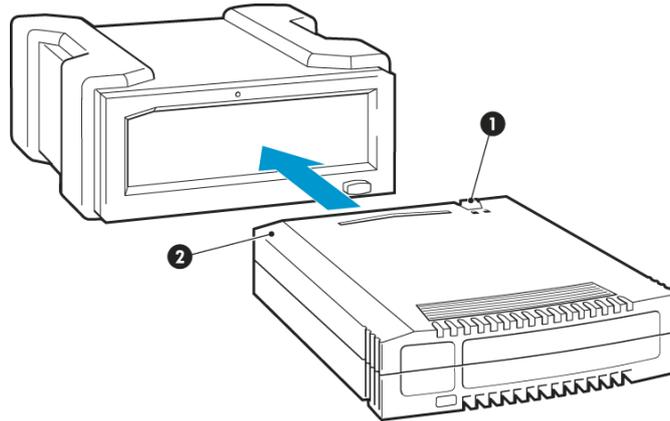
Figure 5. ❶ – Write protect tab; ❷ – Keyed corner

5.3 Performing Manual Backup

Additionally, IT and ICT professionals who are responsible for the update and maintenance procedures can manually perform a backup in SQL Management Studio by the following steps:

1. Expand "Databases" item on the left in Object Explorer.

2. Right click on PACS and from the *context menu* navigate to **Tasks → Back Up** as per Figure 6.
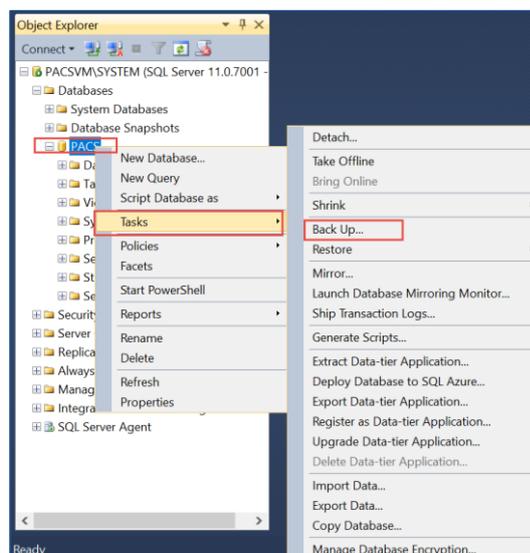
Figure 6. PACS Back Up from context menu in SQL Management Studio
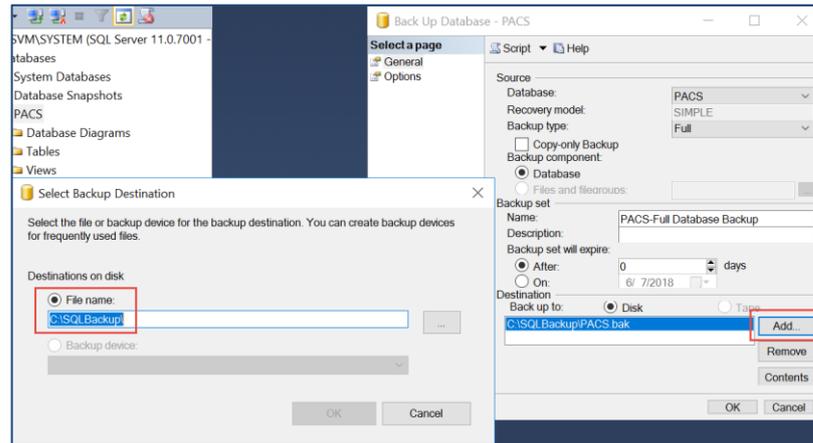
Figure 7. Back Up Database – PACS window

3. The **Back Up Database – PACS** window opens as per Figure 7.

4. In the General window click **Add**.

5. The **Select Back Up Destination** window opens. Type a unique name for the backup, e.g., *PACS_5.8.852_07OCT2021.bak*. Click **OK** to confirm the process.

5.4 What you need to do

*   **Cold Backup:** On a weekly basis replace RDX cartridge and store the cartridge offsite (outside of the server room, ideally in a separate building from the server room).

*   **Regular Monitoring:** Twice a month check the **DATE** and **TIME** modified on the PACS _*rotate* folder to ensure that the backup is performing correctly. During this, ensure that the **ACTUAL SIZE** of backup folder and *.bak files located inside it, is more than 0 Kb. Alternatively, you can check in **Windows Task Scheduler** as per Figure 8, *Backup_Rotate_Daily* and *Backup_Rotate_Weekly* tasks (in yellow highlight) – *Last Run Result* column, which should indicate that the operation completed successfully.

Figure 8. Windows Task Scheduler – PACS daily/weekly backup tasks (Last Run Result) window

6. PACS Backup for PACS Database on a workstation/standalone installation

If your PACS database is installed in a standalone mode, i.e., on one machine, then it is even more important for you to ensure that you have a good and properly configured backup schedule. PACS is being automatically backed up daily at the pre-configured time, and the backup stack depth stored on the workstation itself are:

- Daily backups going back 7 days.
- Weekly backups going back 4 weeks per Server Configuration.
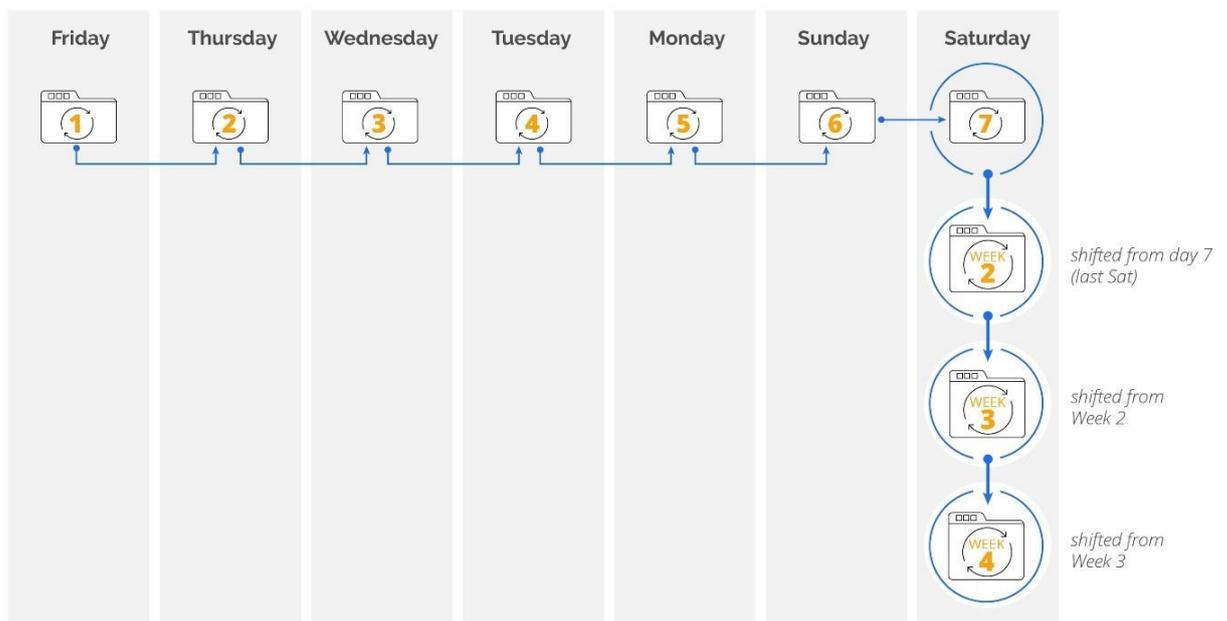
Figure 9. PACS Backup Stack Depth Illustration

Each time the PACS application is updated, an SQL database backup is also taken during the process.

However, this means that if something goes wrong with this machine, this can pose a threat to the stored backups as well. **Thus, it is extremely important that someone on-site is designated to perform weekly export of stored backup to an external hard drive.**

6.1 How to verify integrity of backup

According to the best practices and information security standards, including ISO27001, it is highly recommended to periodically check stored archive data for its timely creation, relevance, confidentiality, integrity, and availability. The backup data should be checked every two weeks, and any loss or missing data should immediately be reported to the organization's relevant leadership for further investigation.

The integrity of the stored archive data can be verified by checking the location where the backups are stored – the "_rotate" folder on the server (**D:\BACKUP_rotate** folder). There should be folders 1-7 (for daily stack), and 3 other folders: Week 2, Week 3, and Week 4. Go to folder "1" – this will contain the latest backup. If the file was modified yesterday or today, this means that the backup is working correctly. Please feel free to contact BV support personnel if you have any questions.
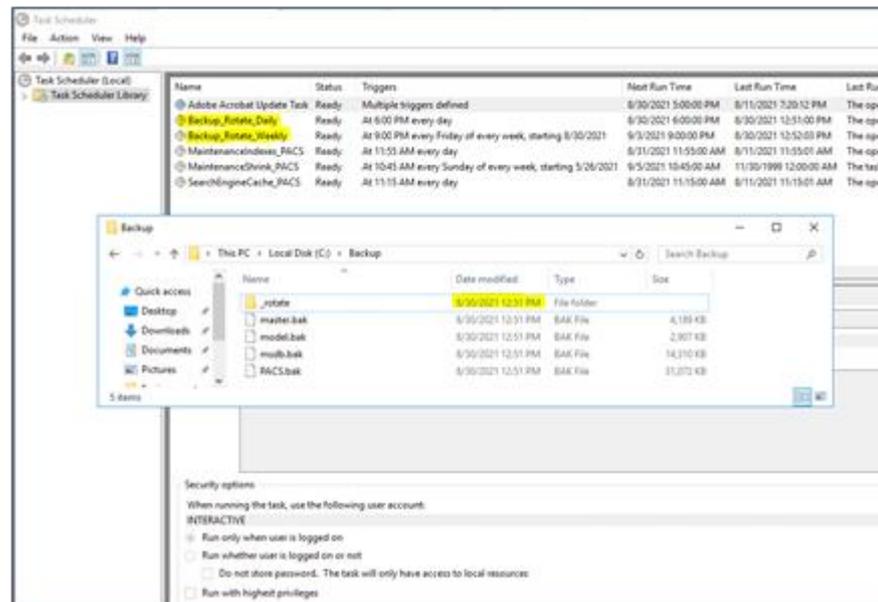
Figure 10. Task Scheduler

In Windows Task Scheduler, *Backup_Rotate_Daily* and *Backup_Rotate_Weekly* tasks (in yellow highlight) provides information on what time the backups are scheduled to occur; Date modified column in *Backup* folder or the "_rotate" folder details the date and time last modified (in yellow highlight). This should be checked every 2 weeks to ensure backup is working correctly.

It is recommended that the IT/ICT professional or PACS Admin responsible for PACS maintenance and support exports all PACS backup files and transfers them to an external hard drive on a weekly basis. It is very important that the external hard drive is stored off-site, in case there is any force majeure event, then at least all information since the last backup will still be recoverable.

6.2 Configuring start time of Daily and Weekly Backups

It is very important to properly configure the start time of Backup_Rotate_Daily and Backup_Rotate_Weekly tasks on a Standalone workstation, since by script's default, the start time is configured to 6PM (the time when most facilities have already switched off the workstations, thus the backup will not run), unlike a server which is usually operational 24/7. This can be manually done from Windows Task Scheduler by the following steps:

1. Right click on the task name and from the *context menu* navigate to **Properties** as per Figure 11.
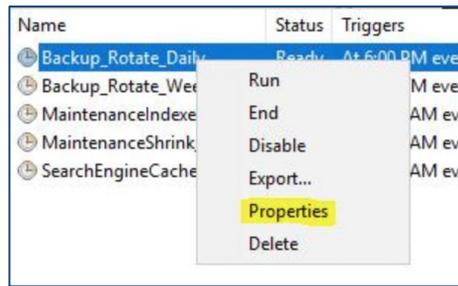
Figure 11. Windows Task Scheduler – PACS daily/weekly backup tasks (context menu) window

2. Navigate to **Triggers** tab, select the **Details** of the Trigger, and click **Edit** as per Figure 12.
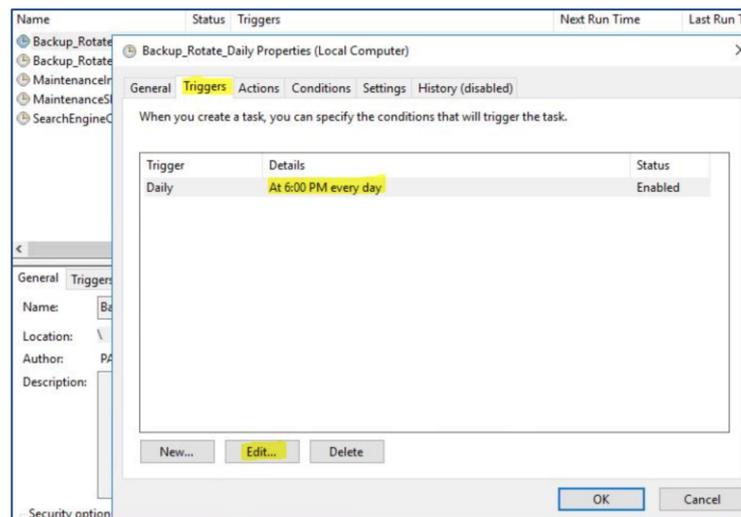
Figure 12. Windows Task Scheduler – **Backup_Rotate_Daily Properties** – Triggers window

3. **Edit** the Start time of selected task according to facility's standard working hours and click **OK** to save the configuration as per Figure 13.
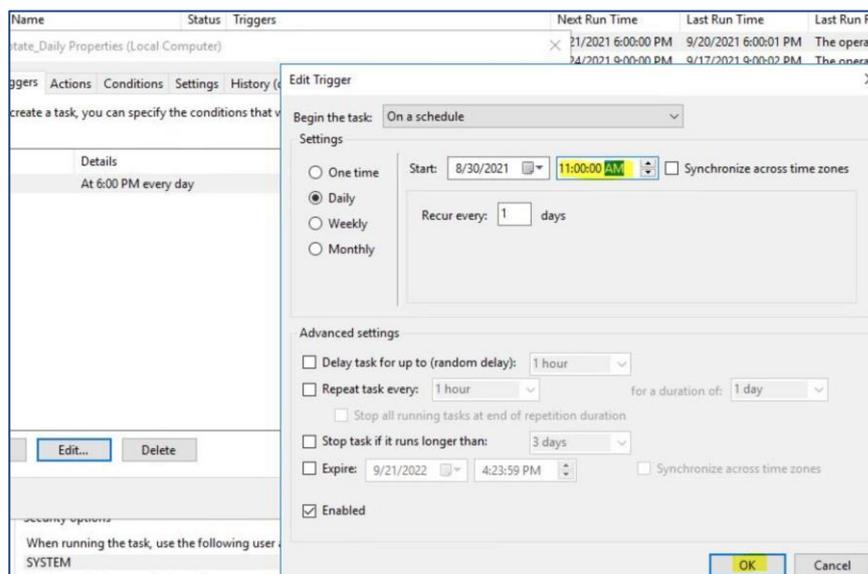
Figure 13. Windows Task Scheduler – **Edit Trigger** window

6.3 What you need to do

- **Cold Backup:** On a weekly basis copy the PACS backup file from Folder "1" to an external hard drive and store the external hard drive off-site (ideally in a separate building from the workstation).

- **Regular Monitoring:** Twice a month check the **DATE** and **TIME** modified on the PACS _rotate folder to ensure that the backup is performing correctly. During this, ensure that the **ACTUAL SIZE** of backup folder and *.bak files located inside it is more than 0 Kb. Alternatively, you can check in **Windows Task Scheduler** as per Figure 14, *Backup_Rotate_Daily* and *Backup_Rotate_Weekly* tasks (in yellow highlight) – **Last Run Result** column, which should indicate that the operation completed successfully.

Figure 14. Windows Task Scheduler – PACS daily/weekly backup tasks (Last Run Result) window