SolidPractices:

Backup and Restore Procedures

SOLIDWORKS® PDM Professional

3DEXPERIENCE

DASSAULT SYSTEMES | **IF WE** ask the right questions we can change the world.

Table of Contents

Revision History

Rev #	Date	Description
1.0	*Apr 2020*	*Document and screenshot minor changes. Revised for use by customers and reset as document version 1.0*

Note

All SolidPractices are written as guidelines. It is a strong recommendation to use these documents only after properly evaluating your requirements. Distribution of this document is limited to Dassault Systèmes SolidWorks employees, VARs, and customers that are on active subscription. You may not post this document on blogs or any internal or external forums without prior written authorization from Dassault Systèmes SolidWorks Corporation.

This document was updated using version SOLIDWORKS 2020 SP2. If you have questions or need assistance in understanding the content, please get in touch with your designated reseller.

1) Preface

This SolidPractice document describes factors that influence the backup and restore processes for the SOLIDWORKS PDM Professional product set. The document discusses possible error scenarios that can occur when restoring not-synchronous server components, and how to fix a few of these errors. The document first describes details about the SOLIDWORKS PDM Professional architecture including:

- Backup strategies for the database, archives, and other parts of the system.
- How to set up a test environment for practicing restore scenarios.
- Information about how to address some inconsistencies that can arise while restoring not-synchronous server components.

There is no single strategy that applies in each setup. However, an understanding of all of the options available will help you to define the best strategy for your specific requirements.

The intention of this document is to expand and enhance this information over a period of years and versions to incorporate feedback from the field experience about the most useful areas.

Notes:

- This SolidPractice document provides guidelines. You should not use this document without proper alignment to specific requirements and situations. Not all of the alternative practices in this document are suitable for all customers.
- Information about specific commands or screen images refer to the Microsoft® SQL Server® 2014 database software unless noted otherwise. In most cases, the operations also apply to SQL Server 2008 R2, although some details may vary.

2) Understanding the SOLIDWORKS PDM Professional Architecture

Before defining a backup strategy, it is important to understand the SOLIDWORKS PDM Professional components. This gives you a good idea of the different components involved, and what data requires backup, and why.

For more information about how SOLIDWORKS PDM Professional handles files, see the article "*Understanding SOLIDWORKS PDM Professional Architecture*" in the **Support > SolidPractices** section of the VAR Resource Center (VRC).

The following image depicts a typical multisite SOLIDWORKS PDM Professional installation:
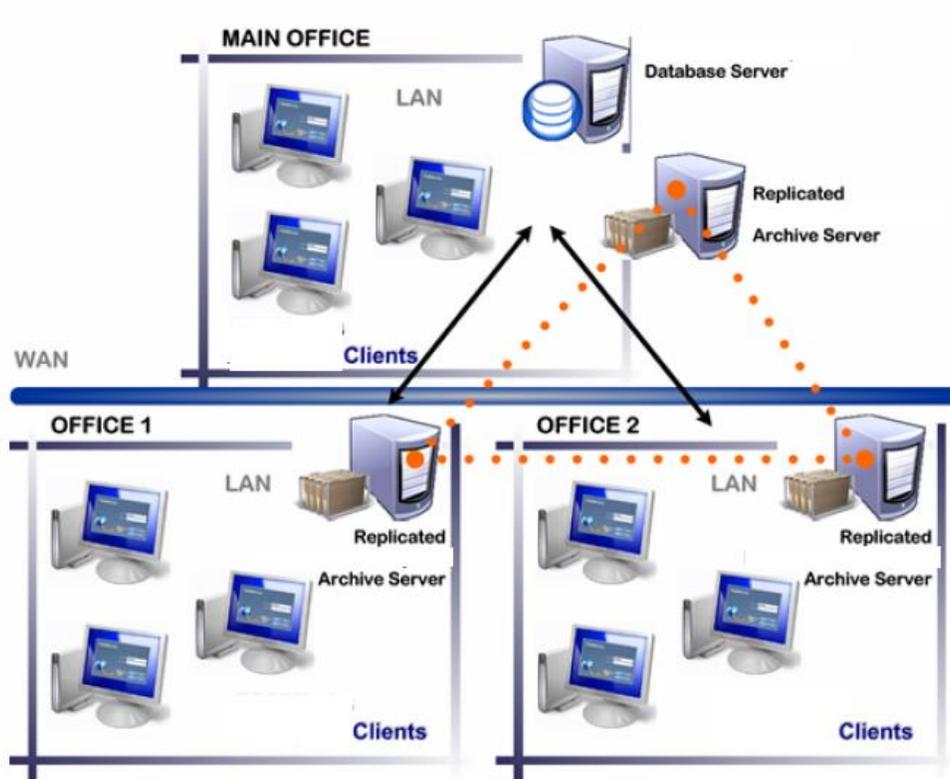

The installation includes:

- A SOLIDWORKS PDM Professional vault database, which is a Microsoft SQL Server (MSSQL) database.

- One or more "archive" servers that store the file archives and archive server settings.

- One or more clients that connect to the central database and the archive server to exchange data.

The SOLIDWORKS PDM Professional data spreads across the archive server (which stores the actual document in a hexadecimal folder structure) and the metadata (data about data) information, which is stored in the central (common to all sites in case of replicated environment) MSSQL vault database.
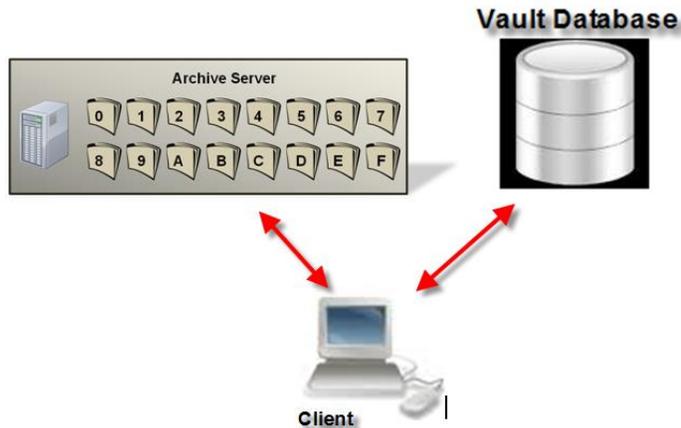
Each client works on data locally (where the data is cached to a user's local view) and saves changes to the server through the check in process.

Be aware that documents in the vault have matching ("in sync") information on the archive and database servers. Therefore, you should ideally back up these server components together for a perfect recovery.

Typical situations when restore of SOLIDWORKS PDM Professional components require more clean up and manual intervention (general recovery scenario) occur when the database and archive servers are not in sync.

For clients (local views), it is difficult to apply any backup policy. A good practice is to check in files after applying major changes. It is not necessary to check in the file each time you make a change. Doing so increases the size of the file archives on the archive server. In the event of a client computer crash, the data loss is minimal and restricted to any file changes that are not yet checked in through this local view. Information in a later section of this document discusses backup and recovery of server components.

3) Backup Strategies for the Vault Database

The following image depicts an MSSQL database that holds all metadata information for the entire vault. Any MSSQL database consists of two files. A master database file (MDF) and a transaction log file (LOG). The recovery model in use determines the backup strategy. There are three types of recovery models from which to choose; **Full**, **Simple**, and **Bulk logged**. You can change the recovery model in the database properties. By default, the **Full** recovery model creates new databases.
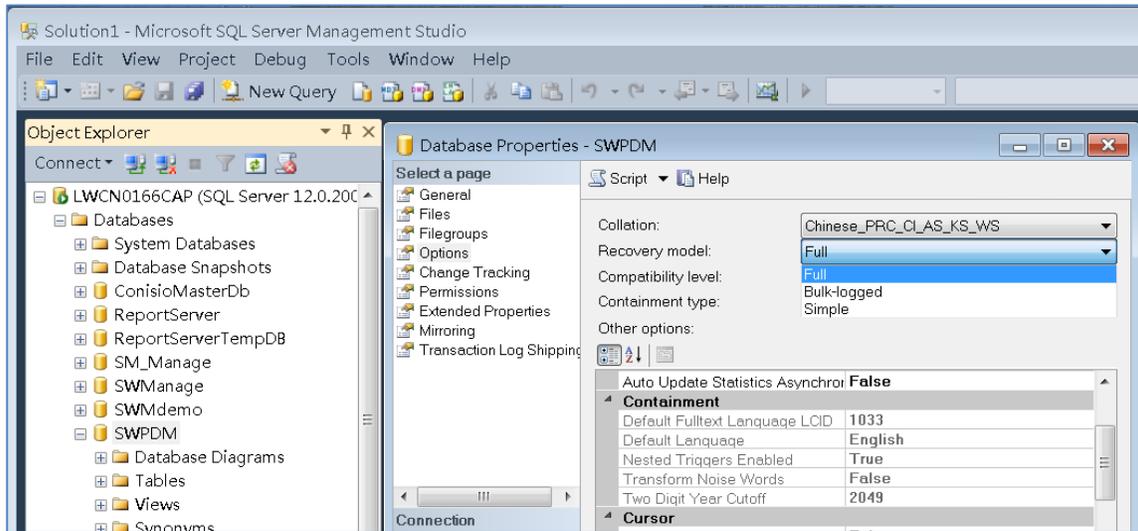
a) Simple Recovery Model

As the name implies, this is the simplest of the recovery models. If you choose this model, you can restore only full or differential backups. You cannot restore backups to any specific point in time. SQL Server truncates the transaction logs when the database reaches a transaction checkpoint, and it leaves no log entries for disaster recovery. Therefore, you lose any changes to the data that occur between the last full or differential backup and the failure.

b) Bulk Logged Recovery Model

This recovery model is for use on databases that already use the **Full** recovery model and when performing bulk load operations (such as a data warehouse load).

If you choose the **Bulk logged** database recovery model, you have the ability to create transaction log backups. However, you are not able to restore to a specific point in time with these log backups. You must restore the entire transaction log backup. This is better than in the simple recovery model, because at least you do not lose any data. However, it is probably

not necessary to use the **Bulk logged** recovery model unless you continually perform data loads.

This method is not particularly applicable to SOLIDWORKS PDM Professional environments, so it is not discussed further in this document.

c) Full Recovery Model

The **Full** recovery model provides the most flexibility on the types of backups that you can create. You can use full database backups, file backups, differential backups, and transaction log backups. The choice of a backup strategy in this scenario varies greatly based on your database size, the backup medium, and the level of recoverability that you want to establish for the data.

d) Recommended Recovery Model

For ease of restoration, the recommendation is to use the **Simple** recovery model to control the transaction log file size, and to perform a **Full** backup rather than differential backups. If a dedicated database expert is available, then you can implement any convenient backup strategy as long as it restores the database correctly.

If you already have tools and processes in place for a different MSSQL database backup (which might be in use for a third-party system), you can use those for a SOLIDWORKS PDM Professional database also.

For more information about these recovery models, see the Microsoft topic "Recovery Models (SQL Server)."

SOLIDWORKS

DASSAULT SYSTEMES | **IF WE** ask the right questions we can change the world.

4) Backing Up the File Vault Database - Manual Method

1. In Microsoft SQL Server Management Studio **Object Explorer**, expand the node for the SQL Server instance.

2. Right-click the database that you want to back up > select **Tasks >** and then click **Back Up**. The **Backup Database** dialog box appears.
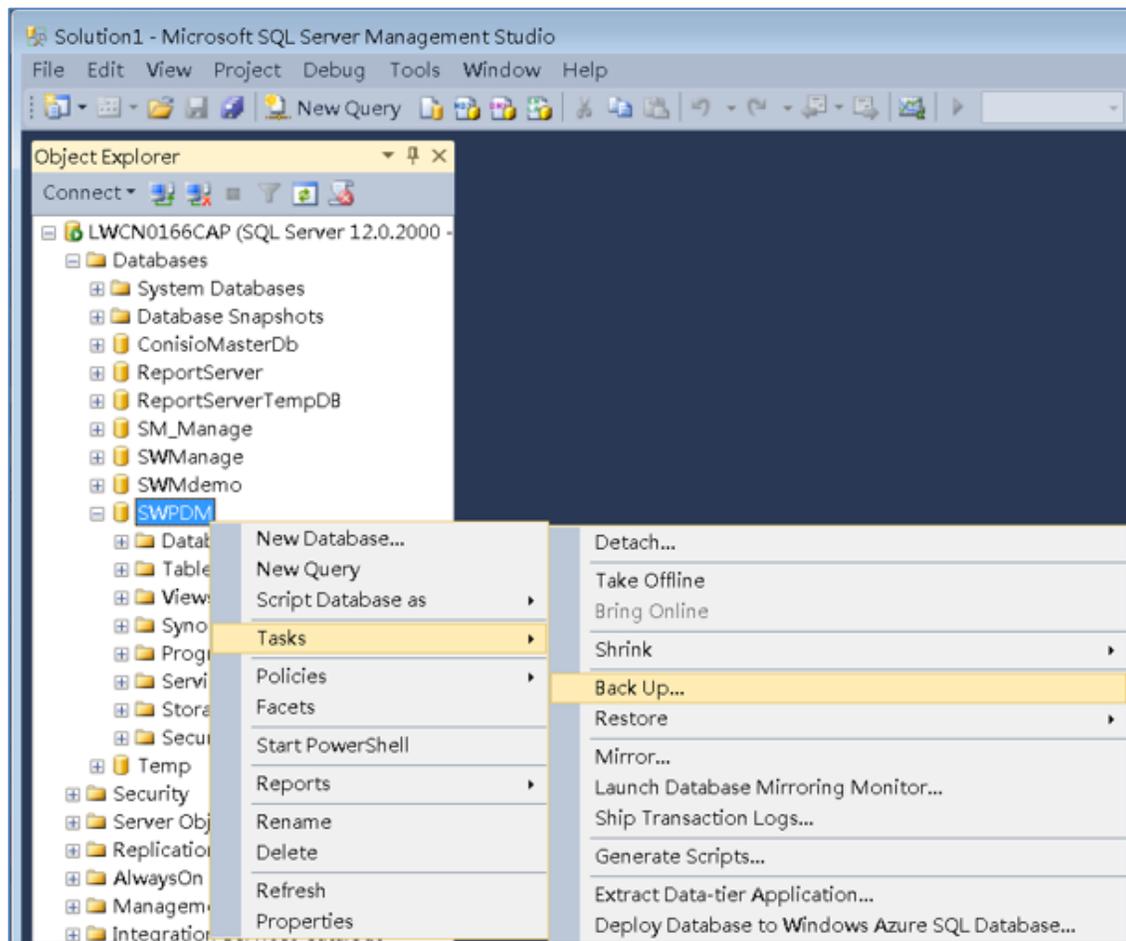
3. For **Backup type**, select the **Full** option. Note that this is different from the "**Full** recovery model" discussed earlier in this document.

ƆS SOLIDWORKS   **ƆS DASSAULT SYSTEMES** | IF WE ask the right questions we can change the world.
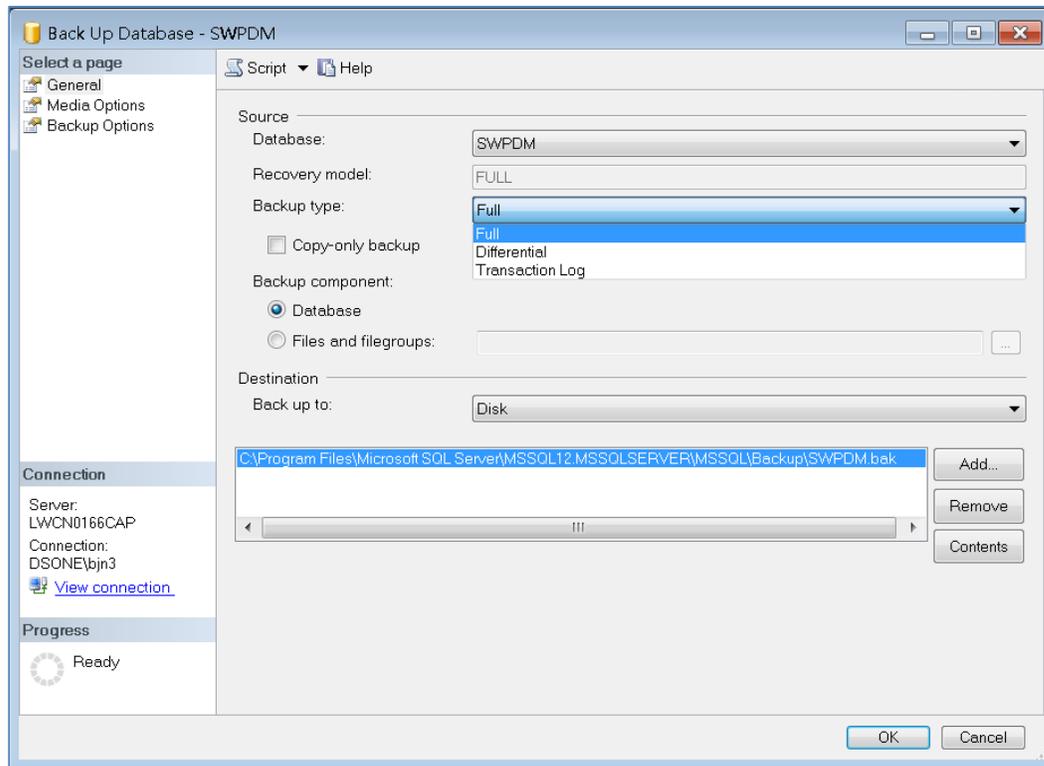
4. In the **Destination** group, specify the location in which you want to store the backup. By default, the tool specifies the location as: `%SQL Server Installation Path%\Backup\[database name].bak`. However, this is not ideal. It is better to define a location specifically suited for the purpose - preferably on another disk drive.

5. Click **OK**. This initiates a full backup of the database. When the backup is complete, the following confirmation message appears.
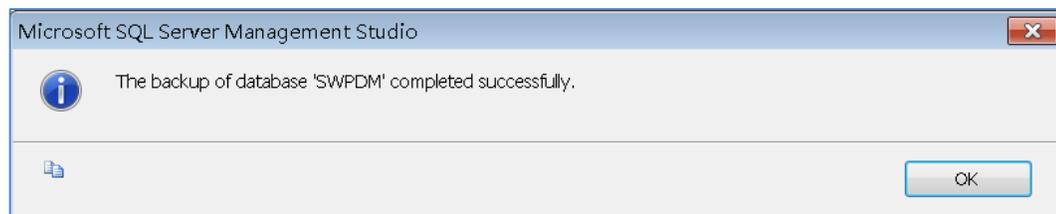
6. Click **OK** to dismiss the message.

You can schedule a periodic backup by accessing the **Maintenance Plan Wizard** from the context menu for the **Maintenance Plans** folder of the SQL Server instance. Before running the backup, it is a good idea to check the database integrity. Make sure that you store backup files generated by the maintenance plan in isolation from working MDF and LDF files.
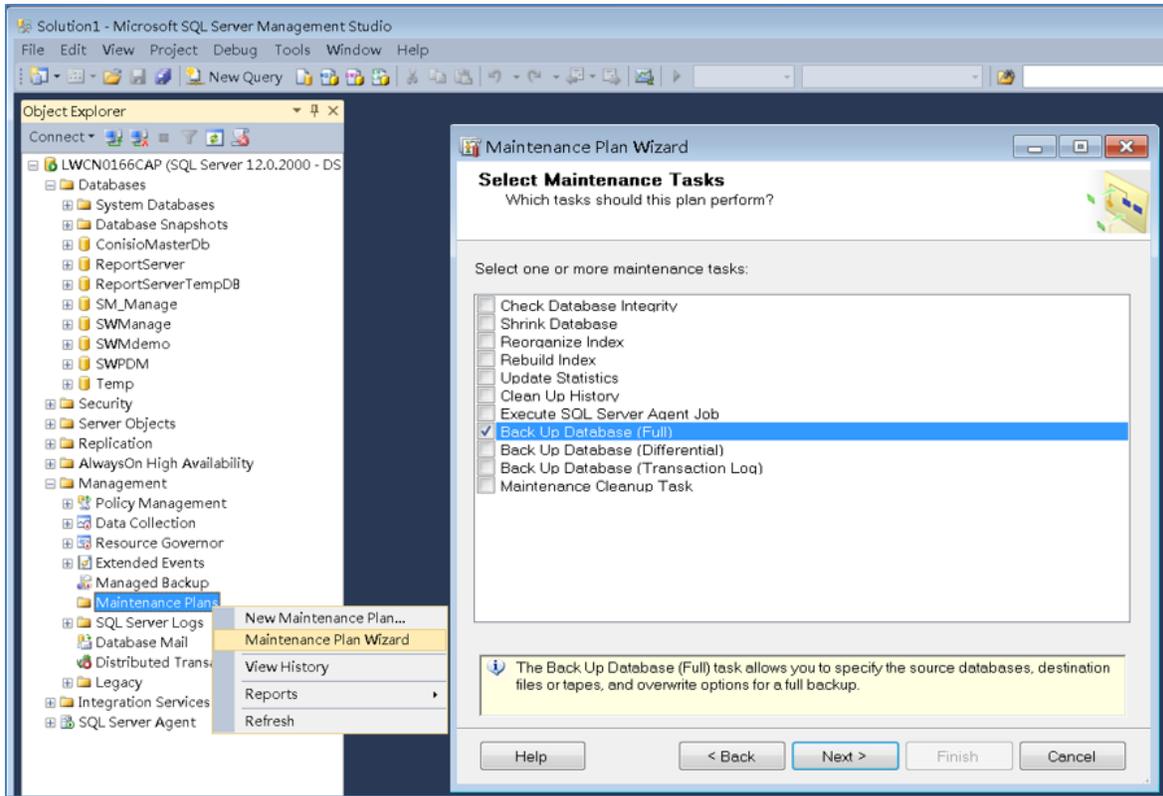
Users can configure the database to send email alerts with regard to a scheduled backup task, a consistency check failure, and others conditions. For instructions about how to configure database email messages, see the SOLIDWORKS Knowledge Base solution S-027967 and the Microsoft SQL Server documentation. This feature makes it possible for the database administrator to receive notifications about successful and failed backups. The administrator can then initiate corrective actions as necessary to minimize subsequent problems.

5) Backing Up the Remainder of the Enterprise System

a) Synchronization of the Database and Archive File Backups

A critical point to consider when managing the overall backup of the SOLIDWORKS PDM Professional environment is the interaction between the SQL Server database and the archive file storage.

As shown in the architecture diagram, the archive server stores vault files in a vault archive folder. The vault archive folder stores individual file archives within 16 subfolders.

The vault initialization creates a single folder with the vault name in the "root folder". This folder represents the "top" of the vault. The initialization then creates 16 subfolders. The subfolders have names that are numbered 0-9 and A-F in hexadecimal notation.
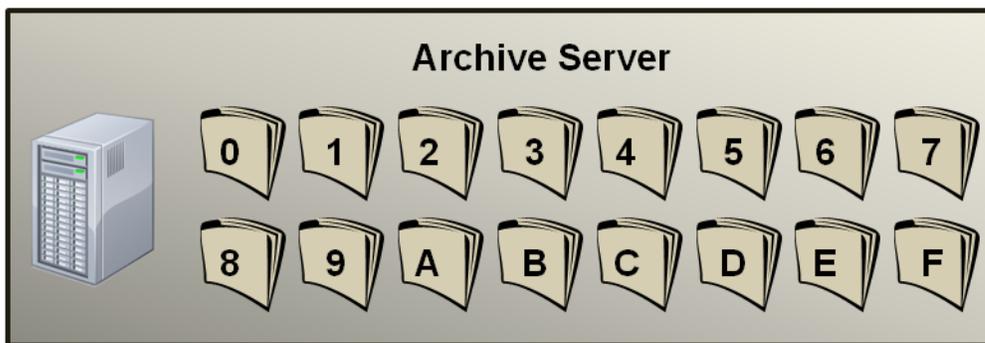
The enterprise database contains references (file pointers) to the content in this file repository. To ensure maximum consistency between the database file references and the actual content of the file repository, you must pay close attention to backing up both the database and the file repository simultaneously.

In a replicated environment, it is mandatory to back up the file archives on each archive server for a file vault. Although there is no such concept as "master" and "slave" archive servers in a replicated environment, it is still a good practice to designate one archive server as the "master" for back up purposes. You can define frequent replication schedules to ensure that the maximum number of files replicate to this server before backing up the archives.

Using Redundant Array of Independent Disks (RAID) architecture to apply redundancy for archive folders greatly reduces the risk of disaster.

b) Backing up the Archive Files

It is a recommendation that there be no active users during the period of backup. This helps to avoid any concurrent activity in the vault. However, this may not be practical in 24x5 client environments that support users from offices in different geographies and time zones.

DS SOLIDWORKS

DS DASSAULT SYSTEMES | IF WE ask the right questions we can change the world.

There are two approaches that you can use depending on what is most suitable for the environment.

- **Option 1**: The SOLIDWORKS PDM Administration tool provides a vault-specific **Block Log-ins** option shown in the following image. To access this option, right-click the file vault > **Vault** > **Properties**.
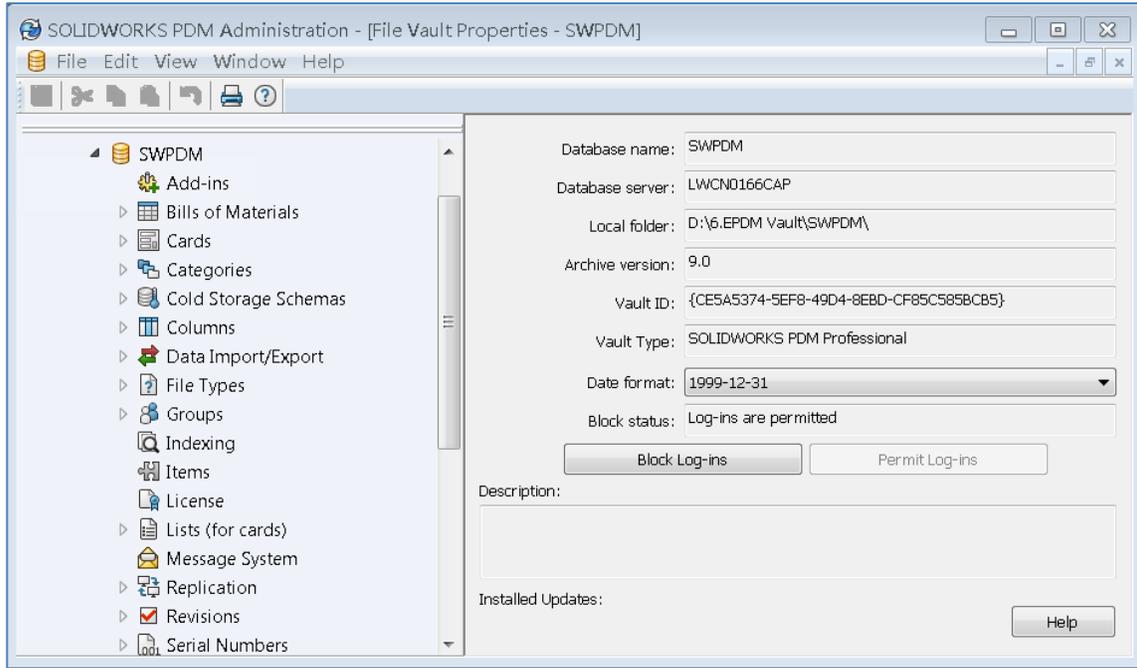
After selecting this option, new users cannot log in to the vault. You can use the SQL queries from Knowledge Base solution S-08712 to identify users with active sessions, and then ask those users to log off. You can then proceed to back up the database and archives.

- **Option 2**: Create online backups and accept some small potential inconsistencies. You can minimize the risks of using this approach by running the backups during periods of low activity.

You can create a backup of the archive file set by using whichever tools are available at the server site. To make a full copy of the entire folder structure, you might use something as simple as a shell script that uses the `XCOPY /S` command. There are also third-party tools available that are capable of performing full or incremental backups. Such tools are a recommendation where the number of files, the file size, and the available downtime for backup is a factor of concern.

The time necessary to back up the database is significantly smaller when comparing to archives for a relatively larger vaults.

c) Backing up the Archive Server Settings

The archive server contains file vault settings such as passwords and defined login types. It also contains the paths to the physical location of the PDM vault archive files. Remember that backing up the archive server settings does not back up the archive files.

To back up the archive server settings:

1. On the archive server, from the Windows® **Start** menu, go to **All Programs** > **SOLIDWORKS PDM Professional** > **Archive Server Configuration**.

2. Select **Tools** > **Backup settings**.

3. In the **Backup Settings** dialog box, select the **Include all vaults** option. This is the default option.
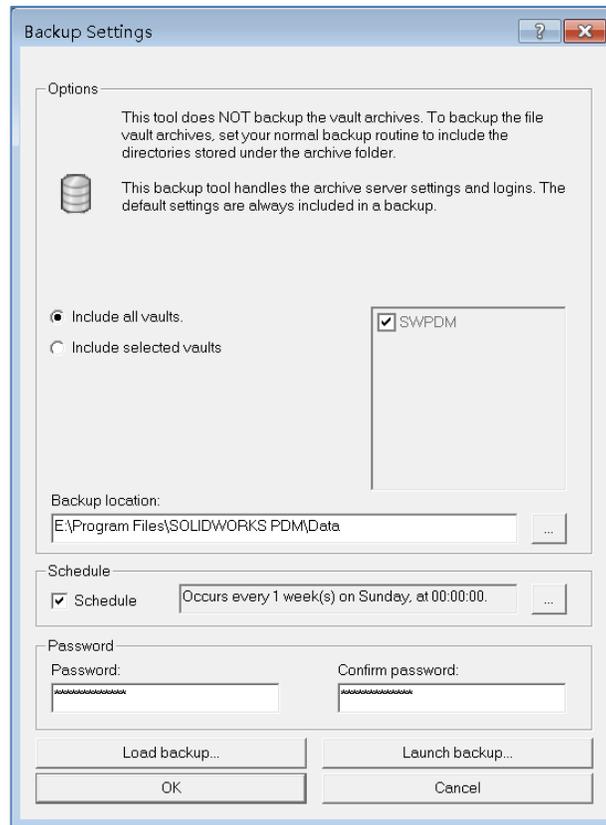
Alternatively, you can select the **Include selected vaults** option and then specify the file vaults for which the settings will be backed up.

4. Specify or select the **Backup location**. The default location is the archive root folder.

5. To schedule an automatic backup, activate the **Schedule** option and specify the schedule.

6. Type and confirm a password for the backup file. This password is required while restoring these settings.

7. To perform a backup, do either of the following:

   a. To perform the backup at the scheduled time, click **OK**.

   b. To perform the backup immediately, select **Launch backup** and then click **OK** in the confirmation message.

The backup file saves in the specified location with name "*Backup.dat*". The archive server settings backup should typically occur at either the same time as the file archive back up, or after. This information changes only when the archive server settings change. In a replicated setup, it is a best practice to back up the file archives and archive server settings on each archive server.

6) Restore Strategies

In the case of a disaster recovery, you can choose one of the following recovery options:

- **Restore to last synchronous back up**. This requires the least user intervention. However, changes that occur after the last known good state are lost. This approach may be useful if there are minimal changes. In addition, the chances are good that a user's local views might have recently modified files that can be recovered and added again following recovery.

- **Recover only the failed component**. This approach covers only archives in case of archive server failure, or the vault database in case of SQL server failure. You might expect some inconsistencies that require repair if possible. Upcoming sections of this document focus on a few of the possible errors in a nonsynchronous environment.

a) Practicing Restore

Practicing a restore operation is a key to successful restore. To avoid any disruptions to production servers, you must practice on isolated (sandbox) servers. Each vault database has a unique ID. The recovery of a test database side-by-side on the same SQL Server instance can create problems because the restored database will have same unique ID as the active production database.

b) Additional Steps to Perform Prior to Restoring

- When configuring Microsoft SQL Server in the sandbox environment, make sure to document the "*sa*" password.

- Create a full back up of the **ConisioMasterDB** database along with the vault database.

7) How to Perform a Basic Restore Operation in a Standalone or Sandbox Environment

A basic restore operation in a standalone or sandbox environment involves the following steps:

1. Install Microsoft SQL Server and the SOLIDWORKS PDM server and client components in the environment.

2. Restore the archive folders.

3. Restore the full vault database and the **ConisioMasterDB** database from a backup. If using differential backups, then restore the full back up and the additional incremental backups.

4. Clean up replication information. When using replication, perform a database cleanup. When practicing the restore process in a sandbox, you typically simulate a non-replicated environment. This exercise is intended to practice the restore process and check the consistency of the backup data.

5. Import the archive server settings and restore the archive backups.

6. Recreate the linked server for content searching.

7. Change the archive server name and IP address to match the test server.

8. Update the archive entries to match the new setup.

a) Install Microsoft SQL Server, and the SOLIDWORKS PDM Server & Client Components

Make sure to install the same SOLIDWORKS PDM version and service pack in the sandbox environment that you use for the production vault. The SOLIDWORKS PDM vault database keeps track of version. If there is a mismatch between the installed version and the database version, clients will not be able to log in to the local view.

To retain consistency in the registry paths for archive server, use the same installation paths that are in use on the production server.

b) Restore the Archive Folders

Restoration of archive folders includes restoring the root folder and the 16 subfolders. Make sure that the actual path for hexadecimal folders matches the path in the registry.
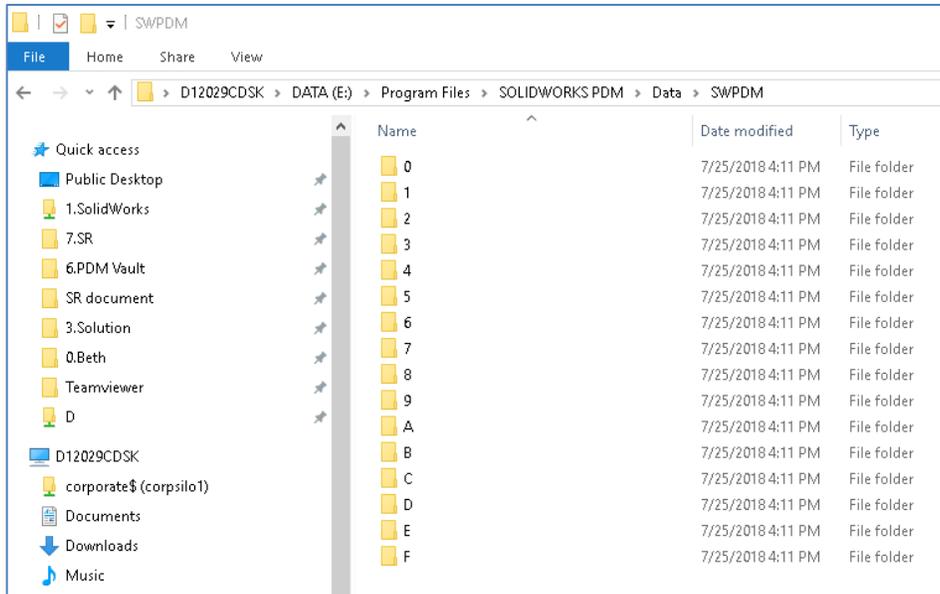
c) Restore the Full Vault Database Backup and the ConisioMasterDB Database

To restore the vault database, follow these steps. You can restore the **ConisioMasterDB** database in the same way. The steps to clean the database apply only to the vault database.

1. In Microsoft SQL Server Management Studio, right-click the **Databases** node, and then click **Restore Database**.
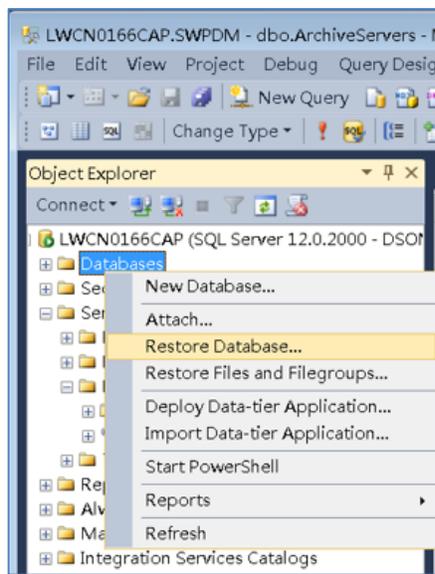
2. In the **Source** group of the **Restore Database** dialog box, select the database you want to restore. After selecting a database, the database name appears automatically in the drop-down list in the **Destination** group. The example in the following image restores the database to its original name.
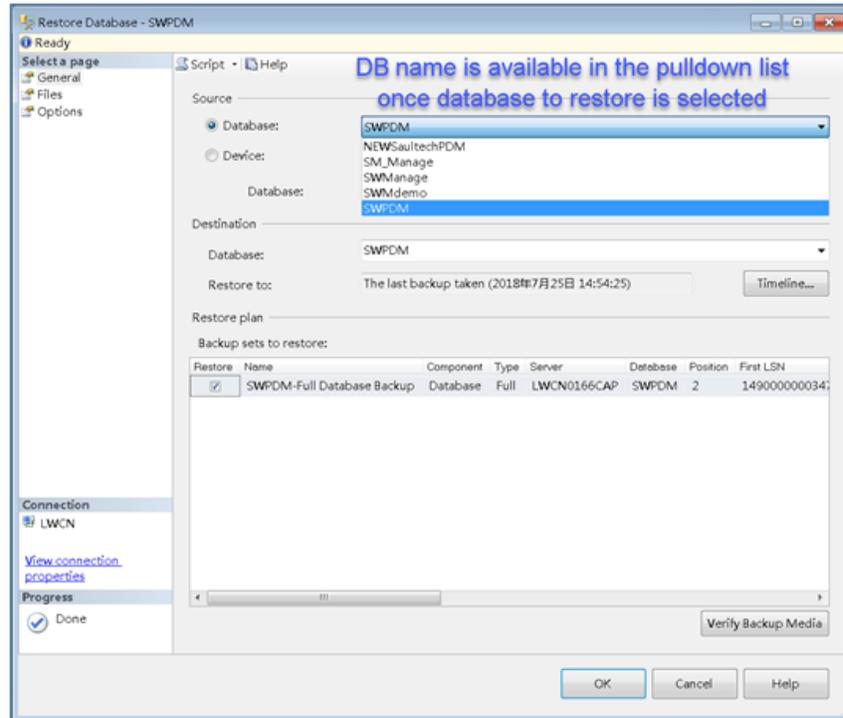
3. On the **Files** page, specify the appropriate locations for the database files.

Select appropriate locations for database (.mdf) and transaction log (.ldf) files
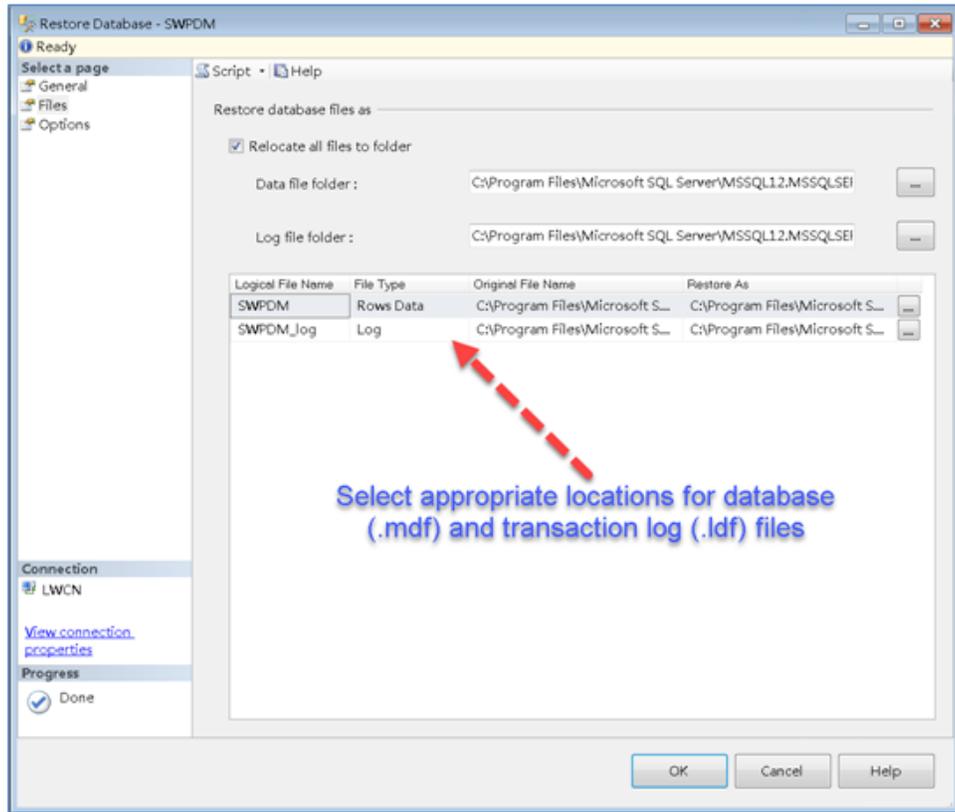
4. In the **Options** tab, for **Recovery state**, keep the default selection of the following option:
   RESTORE WITH RECOVERY. Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored.

5. To begin the restore operation, click **OK**. After restoring the database, a confirmation message appears to let you know that the database was restored successfully.

d) Clean Up Replication Information

If replicating the original file vault, the restored database has entries for the archive servers that are replicating the vault. Those database records must be deleted so that the restored vault copy does not try to locate them. These steps apply only to the replicated vault and you must follow the steps while practicing a test restore of a replicated vault on a sandbox ONLY. In the case of the disaster recovery of an actual production vault, the replication information is needed.

1. In Microsoft SQL Server Management Studio, locate and right-click the **ArchiveServers** table > **Open Table**.

2. Select the replicate archive servers > **Delete**. Note that you should not delete the first entry in the table.
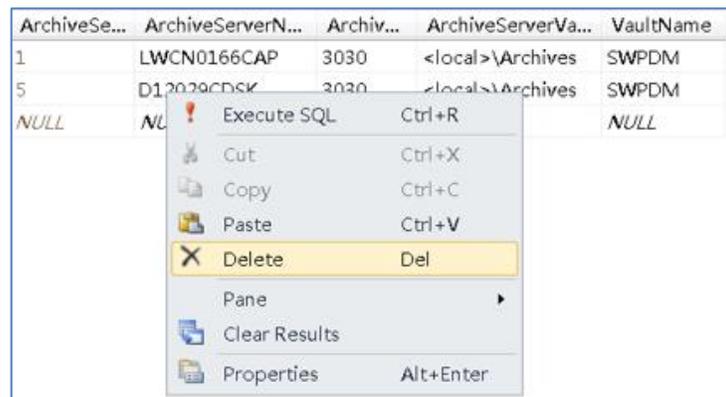
To emulate a non-replicated database, you must empty the **ArchiveServerStored** tables as well.

3. In Microsoft SQL Server Management Studio, right-click the restored database > **New Query**.
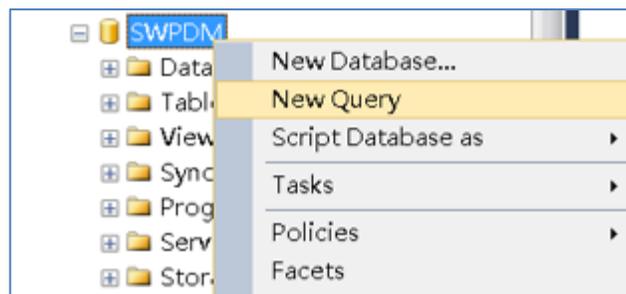
4. In the query pane, type the following statement and then click **Execute** (or go to **Query** > **Execute**):

```
DELETE FROM ArchiveServerStored
```

e) Import Archive Server Settings and Restore the Archive

At this point, the assumption is that on this sandbox, there is a current installation of the archive server components, and that the archive server root folder exists. You can confirm this by reviewing the settings in the following registry key on the sandbox:

```
HKEY_LOCAL_MACHINE\SOFTWARE\SOLIDWORKS\Applications\PDMWorks
Enterprise\ArchiveServer\Computers\<local>\Archives
```

To import the archive server settings, use the **Archive Server Configuration** tool. Follow these steps:

1. On the archive server, from the Windows **Start** menu, go to **All Programs** > **SOLIDWORKS PDM** > **Archive Server Configuration**.

2. Go to **Tools** > **Backup setting**s > **Load backup** > select the path to the DAT file created by following steps discussed in the Backing up archive server settings section of this document.
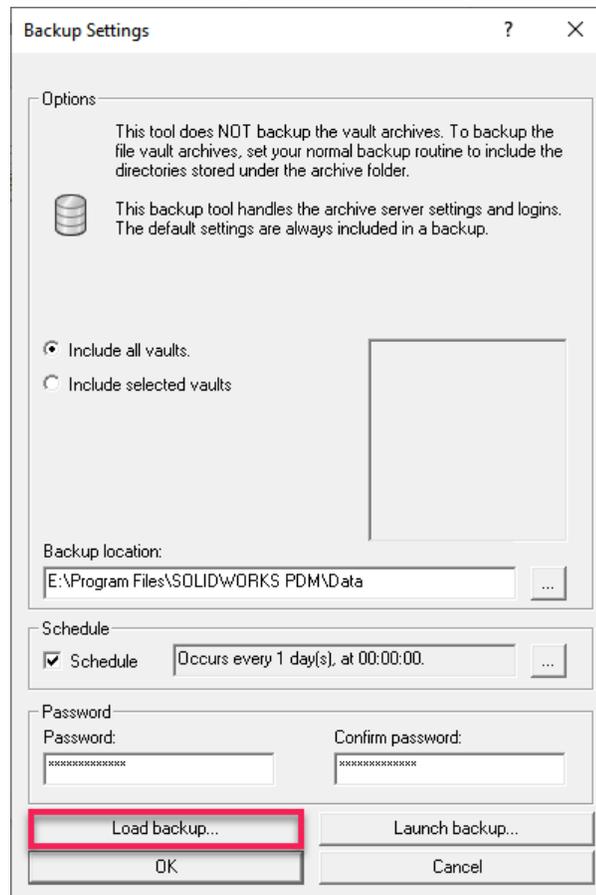
An archive server setting contains the registry pointers for hexadecimal folders. After restoring the archive, the registry location should display the full path in the following image.
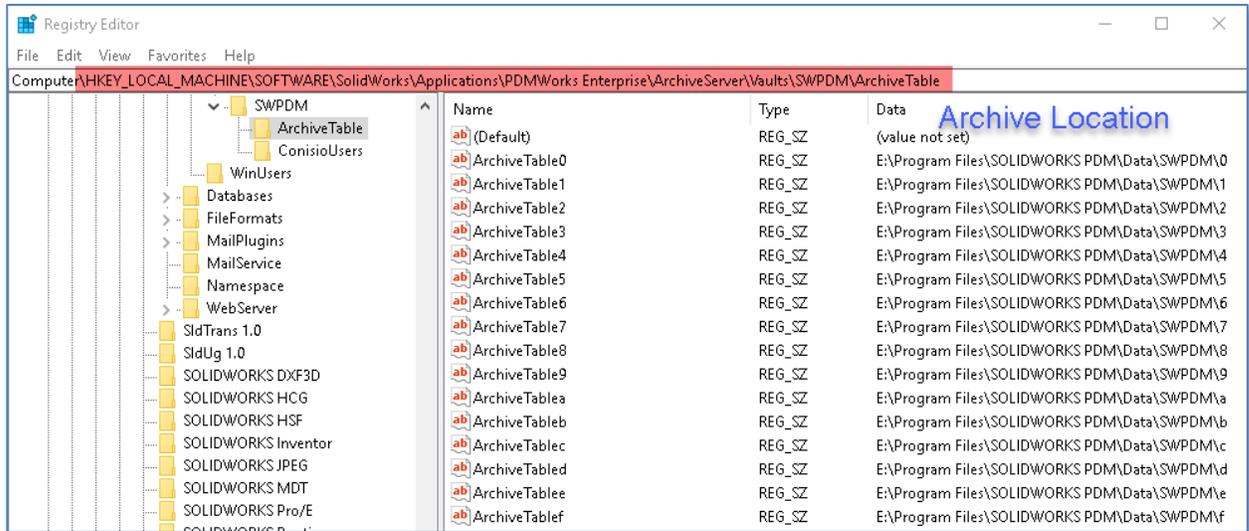
f) Recreate the Linked Server for Content Searching

For content search to work the vault, the SQL Server needs to have a linked server available for the restored vault database.

To allow indexing of the file vault database, follow these steps to create a linked server entry:

1. In Microsoft SQL Server Management Studio, right-click the file vault database > **New Query**.

2. In the query pane, type the following statement and then press the **Execute** button.

```
Exec Sys_IndexServerLink 1
```


.
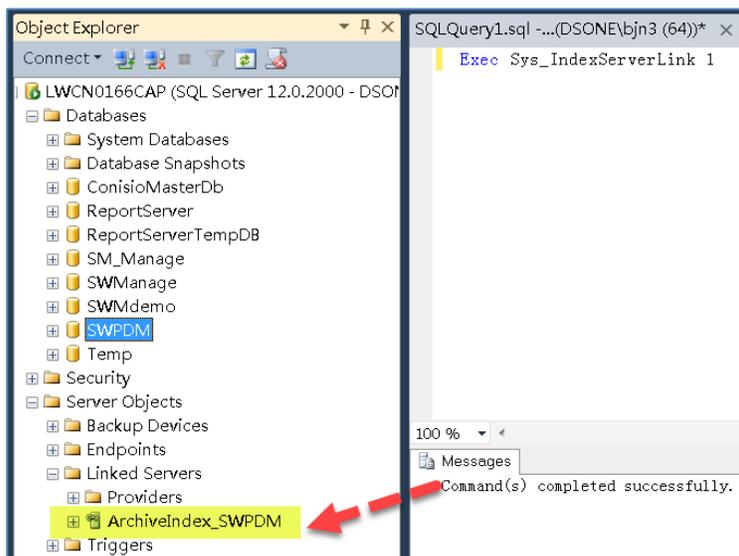
g) Update Archive Entries to Match the New Setup

Follow this process to ensure that the archive entries match the new setup.

1. Edit the **Archiveservers** table to match the new server name as shown in the following image.

2. Redirect the server registries to the sandbox environment.

Note that the following registry key points to the original server location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\SOLIDWORKS\Applications\ PDMWorks
Enterprise \ArchiveServer\Vaults\[Vaultname]\Server
```

It is necessary to point this registry key to the host name and IP address of the sandbox when applicable.
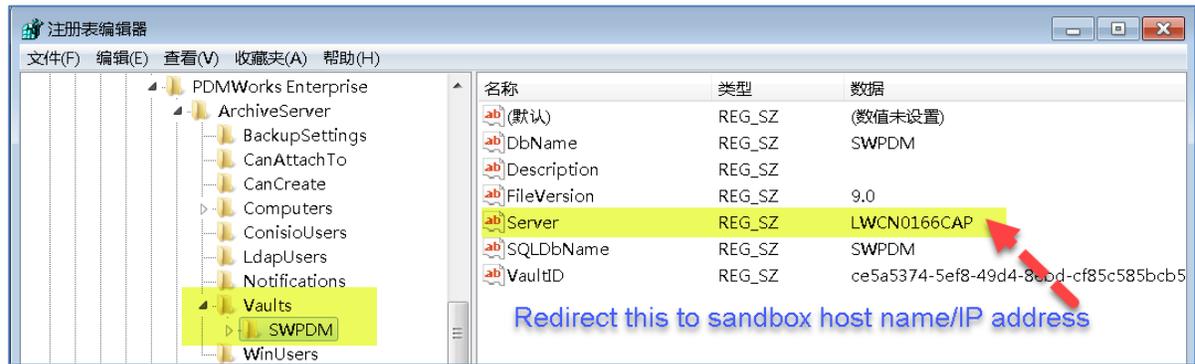
After completing these steps, open the **SOLIDWORKS PDM Administration** tool. The vault is now available in the list. Create a local view and test the restored vault.

8) Possible Problems When Working with "nonsynchronous" Server Components

In a production environment, it is more likely to have an asynchronous setup after the restore. In is not uncommon to experience some data loss. This section discusses the possibility of common scenarios.

a) Database is the latest available and archive restored from the last backup

In these cases, there are database entries for files added and checked in after the most recent archive server backup. Therefore, these files appear for authenticated users. However, the **Get** and **Check Out** functions for such files return the following errors:

Error on **Get**:
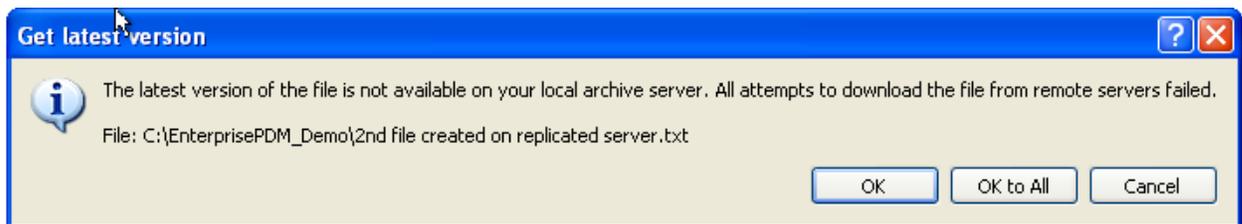
Error on **Check Out**:
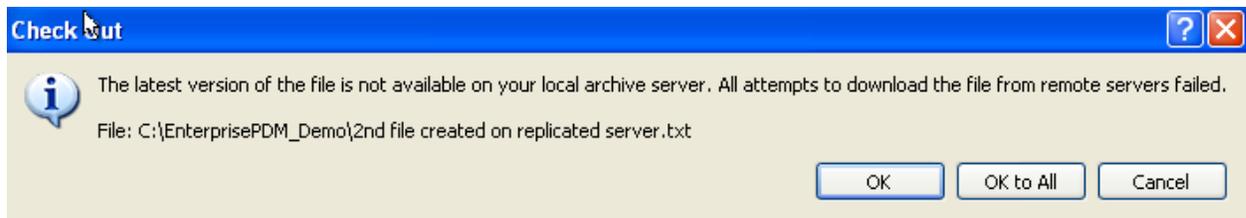
It is possible that these recent files are still available in user's local cache. If so, you can use the following method to recover any available data.

For files that are new (that is, no single version of the file exists prior to the most recent archive server backup), follow these steps:

1. Have the user switch to offline mode.

2. Exit SOLIDWORKS PDM by right-clicking the tray icon and selecting **Exit**.

3. Copy all of the files in the user's local view to a temporary folder. You can use the **Copy** and **Paste** commands for this, or you can use the **xcopy** command. Use the following syntax for the **xcopy** command:

```
Xcopy <source path/vault root folder path> <destination folder>
\E
```

The **\E** switch copies all directories. To learn more about the switches, at the command prompt, type **xcopy/?**.

4. Go online. Delete and destroy such files from vault.

5. Add those files again from temporary folder to the vault, and then check the files in.

For files where newer versions are added before the archive server failed, do the following (perform this carefully per file basis):

6. Follow steps 1 through 3.

7. At step 4, instead of destroying the files, roll the files back to the last available version. Then, check out that document > copy and paste the files from the temporary folder, which adds the next version > check in that version.

b) Archives are the latest available and the database is restored from the last backup

Before proceeding, it is important to know about the cleaner service. When a user deletes and destroys certain documents in the vault, the database entries for those documents are deleted immediately. However, to avoid burden to the archive server, a "cleaner service" runs by default at 3.00 AM (archive server local time) every day. The cleaner service removes the archives for the database entries that were removed. For information about how to run the cleaner service on demand, see the Knowledge Base solution S-022299.

In this case, the database is missing information for archives added, deleted, or destroyed after the last backup. Imagine that a user deletes and destroys some documents after the last database backup. These documents still appear because the restored database has their entries. On **Get** or **Check Out**, the user will see the same errors discussed earlier in this section because the corresponding archives are missing. Because these files are no longer necessary (the reason the user deleted and destroyed them), it is possible to log in as Admin and again delete and destroy those files to eliminate these inconsistencies.

For documents or document versions added after the last database backup, this information is missing in restored database. Therefore, these files or file versions do not appear. To recover files that are available in the user's local cache, follow these steps:

1. Have the user switch to offline mode.

2. Exit SOLIDWORKS PDM by right-clicking the tray icon and selecting **Exit**.

3. Copy all of the files in the user's local view to a temporary folder.

4. Go online.

5. Check out such files. The system prompts you to confirm the file overwrite in local cache. Confirm to proceed.

6. Overwrite the files from the temporary folder. The system once again prompts to confirm the overwrite action. This creates the next file version. Check in this file version.

For files that are new (never exists before the last database backup), follow these steps:

1. Have the user switch to offline mode.

2. Exit SOLIDWORKS PDM by right-clicking the tray icon and selecting **Exit**.

7. Copy all of the files in the user's local view to a temporary folder.

3. Force run the cleaner service (see Knowledge Base solution S-022299). This action removes all archives for which the database entry does not exist.

4. Add files from the temporary folder and check them in.

c) Handling inconsistencies due to cold storage

If you experience inconsistencies resulting from cold storage, you should consult the SOLIDWORKS Technical Support team. Such cases may need different treatment depending on whether the cold storage schema is designed to remove the files, or to move files to an isolated location. This scenario is beyond the scope of this SolidPractice and therefore not discussed further.

DS SOLIDWORKS

DS DASSAULT SYSTEMES | **IF WE** ask the right questions we can change the world.