Aras Innovator Release 2024

Backup and Recovery Procedures

Document #: D-008088

Last Modified: *02/03/2022*

Copyright Information

Aras Corporation
100 Brickstone Square
Suite 100
Andover, MA 01810
Phone: 978-691-8900

E-mail: support@aras.com

Website: https://www.aras.com/

Table of Contents

1 Backup

An important consideration for any organization is protecting company data through backup. Without a current backup, even companies that employ a mirrored hard drive configuration may only realize limited recoverability.

To help protect against data loss, Aras recommends that companies running Aras Innovator software plan for and implement regular system and data backups. This plan includes the following:

- The purchase of a dedicated backup device and media.
- An appropriate backup schedule.
- Periodic test restores to verify backup integrity.
- Off-site storage of current or recent complete system backups.

A backup plan should also include an associated plan for restoring the data.

1.1 Importance of Backup

Regular backup of hard disks prevents data loss and damage caused by hard disk failures, power outages, virus infection, and many other possible computer problems. Backing up program files, databases, vault storage files, and configuration files on your servers is vital to planning a reliable and functional operation. You must back up your data so that you can restore important information or settings if problems occur.

Numerous unexpected events can cause data loss. Natural disasters, power outages, theft, user error, viruses, and hardware failures are all potential causes for partial or total data loss. Adequate backup and recovery procedures are your insurance against a serious disruption in business processes. The real cost of having a good backup plan in place can only be fully appreciated when critical data is lost.

The business impact of lost and potentially unrecoverable data is typically larger than the up-front investment of purchasing backup hardware and implementing a backup plan. Lost data and system downtime could result in lost revenue and the inability to conduct regular business. A valid and tested current complete backup can protect against data loss and substantially reduce recovery downtime.

1.2 Types of Backup

There are 3 commonly used types of backups:

- **Complete**: A complete backup copies all files in their entirety. With complete backups, you need only the most recent copy of the backup file to restore all the files.
- **Incremental**: An incremental backup copies only those files that were created or changed since the last complete or incremental backup. If you implement a combination of complete and incremental backups, you must have the most recent complete backup set, as well as all the incremental backup sets, to restore your data.

> **Note:** It is important to note that incremental backups must be restored in the order they were backed up.

- **Differential**: A differential backup copies files that were created or changed since the last complete backup. If you implement a combination of complete and differential backups, you must have the last complete and differential backup sets to restore your data.

The following table compares the three most common types of backups.

Table 1: Common Backup Types

Backup type	Advantages	Disadvantages
Complete	Easy-to-find files because complete backups are always on a current backup of your system. When restoring data, requires only the complete backup.	Most time-consuming when backing up. Backups become redundant, if files do not change frequently. Requires more disk, tape, or network drive space.
Incremental	Requires the least amount of data storage space. Least time-consuming when backing up. Backs up only those files that were added or changed since the last complete or incremental backup.	Difficult to find files because they can be on several different media. When restoring data, requires complete backup first and then each incremental backup in order.
Differential	When restoring, requires only the last complete backup and last differential backup. Less time-consuming than complete backups.	Longer restoration time than if files were on a single medium. If large amounts of data change daily, longer backup time is required. Backs up all files that were added or changed since the last complete backup.

1.3 Storage Devices

Storage technology changes rapidly, so it is important to research the merits of various media before you decide. When selecting a storage device, consider drive and media costs, as well as reliability and capacity.

1.3.1 Media Types

The most common type of storage medium for backup is a removable media backup device (4mm DAT, Digital Storage Tape Drive, JAZ Drive, or similar high-capacity backup device). You can also store backups on another hard drive or network drive. However, off-site storage helps protect your data in the event of a disaster.

1.3.2 Size

An ideal storage device has sufficient capacity to back up the entire database and can also detect and correct errors during backup and restore operations. It is important to consider future demands when determining media size requirements.

1.3.3 Number of Media Units

Be sure to purchase enough media units to implement your backup plan for one year. For example, if you are using a tape backup method, you should consider how many tapes you need over the course of a year and then purchase as many tapes as possible up front. You should also replace worn tapes per the manufacturer's recommendation. Failing to purchase enough media to implement your backup plan can potentially limit its effectiveness.

1.3.4 Speed

Consider the bus and media speed. Depending on the amount of data you need to back up, you may require a faster device.

1.4 What Needs to be Backed Up

Identify all data assets that should be backed up. For your Aras Innovator implementation, these assets include, but are not limited to:

- Database files
- Vault storage files
- Program files
- Configuration files

Conduct a review of projects and materials that are stored on central servers and mainframes in your facility to ensure that you have identified all required components.

2 Developing a Backup Plan

Using the appropriate hardware and media, a backup plan is essentially a thorough media rotation schedule. A backup schedule helps ensure data recoverability over time and covers the maximum number of data loss contingencies. Your backup plan must be consistently implemented and tested. You should regularly check the backup logs and perform scheduled test restores to ensure backups are being completed successfully.

It is also recommended that you regularly store complete backups off-site. This protects the company's data in the event of a fire or other natural disaster. It is important to rotate the media that you store off- site as part of the backup plan.

2.1 Backup and Recovery Strategy

When you are planning a backup and recovery strategy, you need to consider the following factors:

- Database availability

  What is the database availability requirement for business operations? Is it required for 7X24X365 availability or only during standard business hours? You can adopt different database backup methods and frequencies according to the availability requirement.

- Data loss tolerance

  How much data can you afford to lose due to a database crash? Can you afford to lose one day or one week's worth of data in the event of a database crash? Can you re-enter user data if there is a database failure? If your database cannot tolerate data loss due to failure, then a good data protection backup method needs to be adopted.

- Recovery time

  How much time can you afford to spend recovering a database in the event of a crash? Different backup methods have different recovery times. Physical methods for backup and recovery are much faster than logical backups, and backups to disk are much faster than to tape. Recovery is also much faster from disk than from tape.

- Technical skills

  What are the technical skills of your database or systems administrator? Some backup methods require more database knowledge than others.

- Hardware or software investment

  How much hardware or software investment do you want to put into to the system? Some advanced features, such as high availability, require more of an investment in hardware and software. You can determine the safest backup method for your environment based on database requirements, database running mode, and your recovery scenario. However, the final decisions about the backup and recovery strategy you use is beyond the scope of this document.

2.2 Implementing Backup Procedures

For best backup results, follow these guidelines:

- Schedule online backups when there is minimal database access.
- Have a fixed schedule for online backups so users can plan for database slowdowns.
- Test your backup strategy to see if it is effective; make changes if any area is weak.
- Plan to save several versions back; retain enough versions for your business needs.
- Perform database consistency checks before export or after import.
- Back up the master database before and after it is altered; if you save the original database creation scripts, you can use the same scripts to recreate it.
- For a distributed system, plan on coordinating backup procedures so each site can be backed up individually without destroying the integrity of the data at other sites.
- Some databases recommend that you export and re-import the database on a monthly basis to maintain optimum performance.

2.3 Backing Up a SQL Server Database

The following procedure walks you through a complete database backup operation for SQL Server using the SQL Server Management Studio. **This procedure is provided as a guideline only**. The procedure for your operation may differ based on the type of backup you are performing and your backup storage (**Destination**) media type.

1. Start SQL Server Management Studio.
2. Expand the tree under **Console Root** until you get to the **Databases** folder.
3. Select the database that you need to backup.
4. Right click on the database and navigate to **Tasks > Backup**.
5. Make sure the correct database is selected in the **Database** field.
6. In the **Name** field, enter a name for the backup (Description is optional).
7. Make sure the Backup type is set to **Full**.
8. If the filepath highlighted in the Destination area is not satisfactory, click **Remove…** then **Add…** to select a new name and path for the .bak file.
9. Choose **Database** from the backup component.
10. Click **Add…** in the **Destination** area to set the folder and name for the backup file.
11. Choose the appropriate **Overwrite** method (Append or Overwrite existing).
12. Click **OK** to begin the backup process.

2.4 Backing Up Vault Storage

Information in the Aras Innovator database is used to manage physical files that are stored in a separate vault location. To maintain system integrity and reliability, you must back up the vault storage files when the database is backed up. Vault storage files are stored in a directory tree structure on a file server.

Note:	It is possible to have any number of vault storage areas on any number of servers. You must back up all vault locations in conjunction with a database backup.

If you do not perform the backups in tandem, it is possible for a restored database to point to files that do not exist.

2.5 Backing Up Program Files

Aras Innovator is a web-based application running on a web server. The Aras Innovator program files are stored in a directory tree structure on a web server. These files do not contain data, and therefore do not change unless the version of the application is updated. It is recommended that you back up the application when new versions of the software are installed. It is not necessary to back up the program files on a frequent basis.

2.6 Backing Up Configuration Files

There are a small number of configuration files that are used to control Aras Innovator operation. These files are critical to the proper operation of Aras Innovator. These files do not change unless some aspect of the configuration is changed, such as a new database being added. However, the files are quite small, so you may choose to back up the files as part of your regular backup procedures. The files that need to be backed up are

Table 2: Configuration Files

File	Could be renamed	Purpose	Default or common location
InnovatorServerConfig.XML	√	Contains database configuration information and license key. Actual name and location of this file is determined by the contents of the Innovator.XML file	The root installation folder of Aras Innovator
VaultServerConfig.XML	√	Provides name and location of vault. Actual name and location of this file is determined by the VaultServer.XML file at the vault URL location. If there are multiple vaults, there are multiple copies of VaultServer.XML pointing to different config files.	The root installation folder of Aras Innovator

File	Could be renamed	Purpose	Default or common location
SelfServiceReportingconfig.xml	√	Contains the configuration information for SelfServiceReporting to connect to the database.	The root installation folder of Aras Innovator
ConversionServerConfig.xml	√	Contains the configuration information for the Conversion server to apply the correct converters, with the correct arguments.	The root installation folder of Aras Innovator
appsettings.json	No	References the URL to the InnovatorServer, as well as the listening URL for the Agent Service.	The installation folder for the Agent Service (\AgentService)
conversion.config	No	Contains the configuration information for conversion tasks to be processed in one or more databases.	The installation folder for the Agent Service (\AgentService)
replication.config	No	Contains the configuration information to enable vault replication.	The installation folder for the Agent Service (\AgentService)

3 Data Recovery

In the case of system failure, recovery procedures use previous backups to recreate a system that is as complete, accurate, and up to date as possible. You can also use backups to restore data that has been inadvertently deleted or modified.

3.1 Recovery Strategy

When faced with the prospect of restoring data from backups, it is important to consider exactly what needs to be restored. The goal of effective data recovery is to restore the data that has been lost or destroyed without affecting files that are correct. It is extremely important to know and understand what files must be restored as a unit. For example, if you need to restore the database, then you must also restore the vault storage to ensure that pointers are correct.

3.2 Recovering Databases

The following procedure walks you through a complete database restore operation for SQL Server using the SQL Server Enterprise Manager. **This procedure is provided as a guideline only**. The procedure for your operation may differ based on the type of backup you are restoring from and your backup storage media type.

1. Start SQL Server Management Studio.
2. Expand the tree under **Console Root** until you get to the **Databases** folder.
3. Select the database that you want to restore.
4. Right click on the Database folder and navigate to **Restore Database…**
5. Select the **Device>Ellipse button>Add** to select the backup file.
6. Click **OK**.
7. Make sure the correct database is selected in the **Database** field.
8. Click **OK** in the earlier dialog to return to the Restore dialog.
9. Click **OK** to begin the restore process.

3.3 Recovering Vault Storage Files

In order to maintain system integrity and reliability, you should restore the vault storage files when the database is restored. Vault storage files are stored in a directory tree structure on a file server.

Note:	It is possible to have any number of vault storage areas on any number of servers. All vault locations must be restored in conjunction with a database restore.

If you do not perform the restore operations in tandem, it is possible for a restored database to point to files that do not exist.

3.4 Recovering Program Files

The Aras Innovator program files are stored in a directory tree structure on a web server. There are also DLL files that must be registered as part of the installation procedure. In the case of lost or damaged files, the program files can be restored from backup. However, if the server system files have also been lost, it may be necessary to re-install the application rather than simply restore the program files.

3.5 Recovering Configuration Files

Aras Innovator configuration files are quite small and change infrequently. You can restore them from backup or recreate them from scratch with little effort.

3.6 Complete System Recovery

If your server stops working properly, or if you want to revert your system to a previous state, you may want to completely restore from a system backup.

Note: This is an operation that should not be taken lightly, as all changes to the system done since the last backup may then be irremediably lost.

4 Best Practices

No industry today can afford to leave its corporate data unprotected. Because data is the life blood of any enterprise, protecting it becomes an inevitable task. All it needs for corporate data to be safe and secure is a sound and wise investment in a backup and restore strategy and its implementation. If an organization considers data important, then it must focus on data protection and adhere to the common best practices described here.

4.1 Adhere to a regular and frequent backup schedule

The best way to ensure that backups are done in a consistent and timely manner is to establish a backup schedule. When creating a backup schedule, the goal is the ability to restore the entire system, or systems, in a reasonable amount of time. However, disaster recovery is not the only consideration.

Daily convenience also needs to be considered. A good backup scheme should incorporate an easy way to restore individual files that may inadvertently get deleted. Other considerations include the amount of time needed to do backups and how much that interferes with the daily use of the system.

4.2 Document your backup and recovery procedures

Documentation is one of the key components to having a successful disaster recovery process. Without documentation it is very difficult to perform a planned recovery. What happens in most instances is that the recovery process is handled in fire-fighting mode. Several actions are taken to fix the problem at hand, without knowing what fixed the problem, or possibly creating subsequent problems.

4.3 Automate as many backup tasks as possible

Automate all possible jobs and maintenance plans on the server for things such as database backups, integrity checks, transaction log backups, etc. Automation ensures that the tasks are done consistently and quickly, making it less likely that tasks are skipped or ignored.

4.4 Create and retain backup logs

It is always best to create a backup log for each backup and print the files for reference. Keep a book of logs to make it easier to locate specific files. The backup log is helpful when restoring data; you can print it or read it from any text editor. If the tape containing the backup set catalog is corrupted, the printed log can help you locate a file.

4.5 Keep backups in more than one location

It is recommended that you keep at least three copies of the backup media. Keep at least one copy off-site in a properly controlled environment.

4.6 Perform Trial Restorations

You do not want to discover the flaws in your backup and recovery procedure when you are trying to restore data. Perform a trial restoration periodically to verify that your files were properly backed up. A trial restoration can uncover hardware problems that do not show up when you verify software.