

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.

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.



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.

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.



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.

Important

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.

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.

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

1. 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	The root installation



		this file is determined by the contents of the Innovator.XML file	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)

