ECS Backup Guide

Introduction

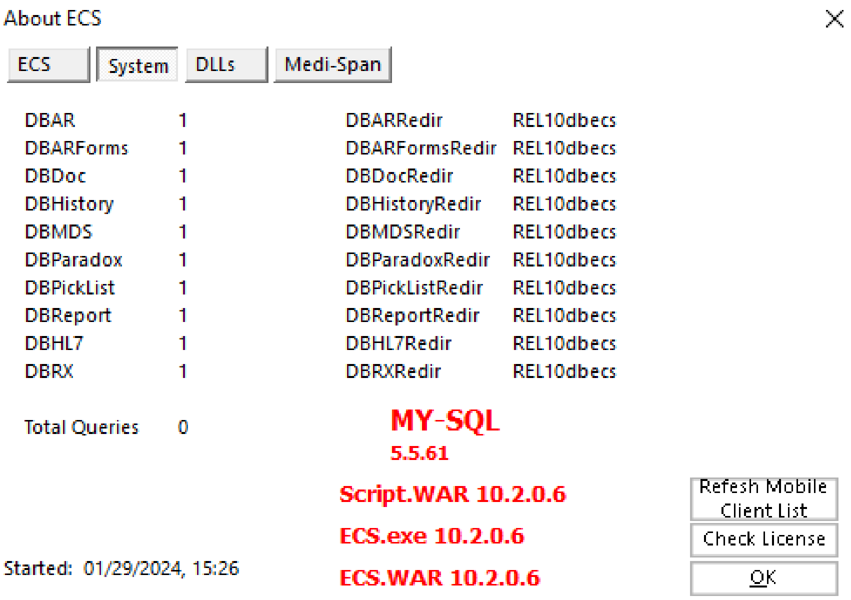
American Data's ECS relies on a backend database engine to store the configuration and resident data saved within the program. All customizations, users, groups, reports, and tasks are often unique to the customer, so in addition to protecting ePHI, ECS database backups are also critical for protecting the current state of your ECS configuration.

If you host your instance of ECS through our optional American Data Cloud services, your backups are already taken care of by American Data Technical Support and our hosting partner(s) here in the US. However, clients who host their own instance of ECS on their own servers (either managed on premises or hosted elsewhere by another party) are responsible for the protection of their own data.

The following guide will outline some important backup items and suggestions to protect your ECS data from common causes of loss.

Finding SQL Server Type

To better understand backup requirements for your self-hosted instance of ECS, you must first know which of the two types of SQL your system runs on. You can check this within ECS by going to **Help>About** from the **ECS-American Data** menu and choosing the **System** tab



DBAR	1	DBARRedir	REL10dbecs
DBARForms	1	DBARFormsRedir	REL10dbecs
DBDoc	1	DBDocRedir	REL10dbecs
DBHistory	1	DBHistoryRedir	REL10dbecs
DBMDS	1	DBMDSRedir	REL10dbecs
DBParadox	1	DBParadoxRedir	REL10dbecs
DBPickList	1	DBPickListRedir	REL10dbecs
DBReport	1	DBReportRedir	REL10dbecs
DBHL7	1	DBHL7Redir	REL10dbecs
DBRX	1	DBRXRedir	REL10dbecs

Total Queries 0

MY-SQL
5.5.61

Script.WAR 10.2.0.6

ECS.exe 10.2.0.6

ECS.WAR 10.2.0.6

Started: 01/29/2024, 15:26

MySQL Database Engine

Backup Overview

MySQL is a free database engine option supported by American Data's ECS. Database tables can be backed up utilizing a simple mysqldump script, or by doing a file-level backup of the database folder on the database server. This can be accomplished with backup software, or through simple scripting.

In a MySQL-based ECS configuration, most customers will find their ECS database in a path like the one that follows: D:\AmericanData\MySQL\Data\dbecs. This database folder is at the top of the list of important data for ECS that needs to be protected.

As always, if you are not sure what you need to backup to protect your self-hosted instance of ECS, please contact American Data Technical Support for questions. We can direct you to the location of your critical data on your servers so that you can work with your IT support group to ensure it is backed up.

Microsoft SQL Server Database Engine

Backup Overview

Microsoft SQL Server (MSSQL) is a popular Windows-based database engine supported by American Data's ECS program. It requires a paid license to run but offers more extensive options with respect to backup/recovery and high availability.

In many cases the organization's IT support may already utilize a Microsoft SQL server for another application and choose to house the ECS database in another instance of that SQL environment.

Regardless of the type of environment, the database for ECS will be called "dbecs" or some variation thereof.

MSSQL has several recovery models built into the database engine that determine how your backup and recovery work. Your IT support will need to choose one of these models to adhere to for data backup and recovery.

MSSQL Recovery Models

Simple

- Common for smaller organizations without a dedicated database administrator.
- Full backups are taken and kept on a retention schedule.
- MSSQL Transaction log files are not used for point-in-time restoration.
- Database restoration occurs only using the full database backup files, which revert the database to the point when the backup was taken.

Full

- Allows for point-in-time restore utilizing the MSSQL transaction logs.
- Requires truncation of the transaction logs through regular full backups, and scripting to free up space in the transaction logs.
- Does not require a database administrator to utilize but does take additional monitoring and troubleshooting (if maintenance is not being performed).

Bulk Logged

- An adjunct of the full recovery model that permits high-performance bulk copy operations.
- Can only recover to the end of any backup- no point-in-time recovery.
- Reduces log space by minimizing logging on bulk operations.
- This is not common for use with ECS.

As always, if you are not sure what you need to backup to protect your self-hosted instance of ECS, please contact American Data Technical Support for questions. We can direct you to the location of your critical data on your servers so that you can work with your IT support group to ensure it is backed up.

Media Server and ECSApps Folder Backups

In addition to the SQL database used by ECS to store data, there are a few other critical items to backup to ensure the latest backed up state of ECS can be fully recovered.

1) ECS Media Server data
   a. ECS Media Server is a separate media storage location for documents and images attached to a resident's record in ECS
   b. The Media folder will be located on the Tomcat server for ECS, usually on D:\AmericanData\Media.
   c. In some cases, the Tomcat server is on the same server as the databases (MySQL or MSSQL), but sometimes the Tomcat service is on its own server.
2) ECSApps program files
   a. For the expedited recovery of ECS from a backup, it is helpful to also have a copy of the current program files. These are stored on the database or Tomcat server (In many cases the database and Tomcat server will be the same server)
   b. American Data can often restore the program files if a backup is not available, but it will take longer to package and send the appropriate version- especially if it is an outage that limits our access to the client via internet.
   c. These should be located at a path like D:\AmericanData\ECSApps\Update for most customers.

Backup and Retention Practices

Backup and retention practices vary widely depending on several factors, but it is important to set policies for your organization regarding backups that consider both likely and unlikely scenarios for which data recovery from backup may be necessary.

An organization looking to establish a backup and retention plan will need to consider questions like:

1) How large (in Gigabytes) is a single backup for ECS?
2) How long will you keep the backup file/folder for recovery to that point in time after it is taken?
3) Where is the backup being replicated to for safe storage?
4) Is a copy of the replicated backup also stored offline (air-gapped)
5) As time progresses and more backups are taken, when will be an appropriate time to go back and delete the earlier backups?
6) Will you keep quarterly copies of the data going back 1 year?

This is where backup software becomes appealing for backup and retention planning. Vendors sell products that offer automation for backup and retention that greatly simplifies the task of data protection. There are many vendors offering specialized backup software products, but one such example is a product called Veeam.

Ransomware

One of the most common threats facing healthcare and other critical industries is Ransomware. Attackers use malicious software running within your network to encrypt (lock) your files so they cannot be accessed, then request payment in the form of cryptocurrency to provide the "keys" to unlock your data.

These attackers often use malicious software in a dormant state to surveil the organization's backup procedures in hopes of being able to infect the organization's backups. This ensures that once the breach becomes known, the organization will not be able to rely on backups to avoid paying the ransom.

Because of this threat, it is imperative that organizations store multiple copies of data in both online and offline states. Doing so will help ensure your ECS data is protected and recoverable in an attack.

Talk to your IT support team about what safeguards they have in place to deal with Ransomware threats in the healthcare industry.

Off-site Backups

Maintaining copies of data off-site, in multiple locations is highly recommended. Establishing "distance" and additional layers of security between the source of an attack and your backup sets is one of the first steps to ensuring things like Ransomware aren't successful in their attack.

Air-gapped Backups

In addition to off-site backups, American Data also recommends moving at least occasional backups off the organization's network, off-premises, and offline. This is often referred to as "air-gapping" as there is no ability for a malicious actor to reach the backup data when it is not online and accessible.

For some smaller organizations this may be as simple as an authorized staff member taking home an external storage device with a backup copy of ECS, whereas for larger organizations the process may be more sophisticated.

Air-gapping backups ensure that you have an additional restore point that exists outside the standard automation of backups for ECS. This helps ensure that even if the backup processes were infected (rending the latest backups potentially unusable), the offline backup could be used to recover at least the majority of data lost in an attack.

Additional Backup Information

For questions, please contact American Data Technical Support. We can work with your IT Support team to help them ensure they have a backup plan for ECS.

American Data can also assist with backup testing (where a backup set is restored to ensure viability in the event of an emergency).

American Data Technical Support
800-464-9942
tech@american-data.com