TECH INSIDER'S GUIDE TO

Backup and Restore Strategies for SQL Server

SHUTTERSTOCK

SQL Server is at the heart of your company; if it goes down, the results could be catastrophic. However, despite its importance, many IT admins don't have a solid backup and restore plan in place. This guide is the first step in developing that plan. By Lafe Low

When you sit down to dinner at your favorite restaurant, you face a handful of choices. After perusing the menu, you'll decide what you want to have as your main course, how you want it prepared, what you'd like as a side dish and the type of dressing you'd like on your salad.

Much like ordering the perfect dinner, you face a range of decisions when crafting the perfect SQL Server backup and restore strategy. And those selections, and the parameters of your SQL Server backup and restore strategy, will be uniquely suited to your organization.

What are your data availability needs? What recovery model will you use? What type of backup media will you use? Will you store locally or in the cloud, or some combination thereof? What about the frequency and type of backups? What resources do you have available? The combined result of these decisions will determine the effectiveness and efficiency of your backup and restore strategy. Your database, and the product information, customer data and transaction records it contains are the lifeblood of your business. When disaster strikes, you need that information back online and running as soon as possible, and as complete as possible. Every instant of downtime is lost or missed revenue.

When considering your backup and restore strategy, there are both technological resources and roles and responsibilities to consider. Ensure you have or are deploying the proper storage resources, as well as who will be tasked with actually conducting the backups and restores. At the very least, you'll need to define the following parameters:

- Frequency and schedule of backups
- Type of backups—whether full backups or differential backups
- Storage location and configuration
- Schedule of testing backup system
- Security and access control to backups
- Restore process and responsibilities
- Acceptable data loss parameters

Whatever decisions you make in the course of developing your SQL Server backup and restore strategy, there are no right or wrong decisions.

The strategy you develop will be uniquely suited to your organization and your needs. The goal is to reduce data loss while making backup data available as quickly and completely as possible. All this must operate within the context of your business goals and requirements. The only wrong decision is to have no strategy at all.

Recovery Model Options

Choosing a recovery model is certainly one of the major decisions in developing a backup and restore strategy. Microsoft recommends one of three recovery models. The choice you make will be based on available resources, database usage patterns and data access requirements, all of which are unique to your business. Your options include:

- Simple recovery
- Full recovery
- Bulk-logged recovery

The simple and full recovery models are the most common—and suitable—for most types of disaster recovery incidents. The recovery model is actually a SQL Server setting, so that will determine how you'll have SQL Server manage the transaction log to support whichever model you select.

Gone are the days when database recovery meant simply backing up to a server in the other room or across state lines.

Simple Recovery: The simple recovery model is a quick snapshot of the database copy. If you need to simplify transaction log management and the whole restore process, choose this model. Simple recovery supports database and file backups, but not log backups. Only transaction log data associated with the actual backed up data will be saved.

On one hand, not backing up transaction logs certainly simplifies the backup and restore process and reduces the drain on resources. The downside to the simple recovery model is you can only restore a database to the point of the most recent backup. Thus, the potential for losing records and data increases, starting from the moment of a backup right up until the next backup begins.

So be sure to schedule frequent backups if you're using simple recovery. In the event of a disaster and database loss, any changes incurred since the last backup would indeed be lost. If that's unacceptable within your business requirements, you're advised to opt for full recovery.

Full Recovery: The full recovery model is just as it sounds. You'll get a full copy of the data—transaction log data included—that will minimize data loss and business risk; however, it will require more storage and management overhead, and greater restore processing time. If you have the resources and can afford the processing overhead, opt for this model.

The full recovery bases its restore on transaction log backups. This is the most effective way to prevent data loss. Because the database is saved with full log backups, you restore the database to any point, which will typically be just before the disaster occurred.

When set up for the full recovery model, it's advisable to perform a series of differential backups between each full backup. This backs up and saves any recent changes or updates to the database, without bogging down the system with too many full backups. Again, the amount of backups and the fact that there are frequent full backups means you'll need significant storage resources to manage your backup copies. The benefit is in greatly reducing the potential data loss.

Bulk-Logged Recovery: Because the full recovery model logs all operations, including bulk operations and bulk loading data, you can use that to accurately restore a database to the specific point of failure. You can augment full recovery performance with the bulk-logged recovery setting. Briefly switch over to bulk-logged recovery when increased performance is more important than the potential for data loss. Bulk logging saves full transaction log data, but not all bulk operations.

Storage Options

Another major component of your SQL Server backup and restore strategy will be where and how you'll store your backup database copies.

Gone are the days when database recovery meant simply backing up to a server in the other room or across state lines. Although those are still valid options for smaller organizations and simpler database structures, you have a myriad of options for using other storage devices, hosted services, the cloud or a combination of all those:

- Local server, NAS device or some other storage appliance
- Managed services provider
- Public/private/hybrid cloud

Local Server: For smaller organizations with less complex data storage and restore requirements, simply using a local server or several servers as backup is perfectly acceptable and sufficient. If this is an appropriate route for your organization, there are some options.

It should go without saying that you shouldn't store your backup database copies in the same physical location or on the same physical server as your primary database. A fire or some other catastrophic damage isn't going to differentiate between your primary server and the backup stored in the closet.

For differential backups, you can create additional logical volumes or partitions on both your primary and backup server. You can also make use of virtual machines and virtual servers as part of your backup infrastructure. Even as your organization grows and expands its backup and restore strategy to include additional storage scenarios, you can continue to maintain local physical and virtual backup.

The simple recovery model is a quick snapshot of the database copy.

Local storage or a network of physical storage devices can also include network-attached storage (NAS) or some sort of storage appliance. NAS devices typically contain a number of hard drives, set up in logical, redundant storage containers or a RAID array. These are an excellent option as your organization grows and its needs for backup and restore resources increase.

Managed Services Providers: Contracting with a managed services provider to administer your backup and restore needs falls more into the human side of the resource equation. Even if you've equipped your organization with a small network of local servers or a NAS device, you may also contract with a managed services provider to manage, test and update those devices. A managed services provider can also assist in developing and deploying your entire backup and restore infrastructure. This is a good option for companies short on manpower or expertise, that need to effectively manage their own backup and restore.

Public/Private/Hybrid Cloud: Moving into the cloud continues to emerge as a more valid option. The historical objections of security and access control companies have had in resisting the cloud are being methodically and efficiently assuaged.

Using the cloud as part of the backup and restore infrastructure could be as simple as relying on the cloud for storage, to establishing a more complex array of compartmentalized data storage in both the public and private clouds based on the sensitivity and access requirements for the data in question.

You may use something like Microsoft Azure or Amazon Web Services (AWS) simply for backup storage. You could manage this directly on your own or use any of an array of storage services provided by specific managed services providers. That way you get the benefit of public cloud datacenters run by AWS and Microsoft, with some of the services you might need provided by the MSP.

You can also opt for a hybrid solution, storing less sensitive data like part numbers and inventory control in the public cloud, and more sensitive data like customer data or financial information in a private cloud. That type of hybrid solution can resolve any security and access control concerns.

Scheduling Backups

Setting up a schedule for automated backups—both full backups and differential backups—is a delicate balance. You want to reduce your exposure to data loss in the event of a failure, but don't want to get bogged down with too many large backup files.

In developing a schedule of backups, you have to consider your business requirements and your available resources in equal measure. If your business requires a nightly backup, but that quickly overwhelms your storage available for backups, you need to invest in more storage.

Testing Backups

Once your backup and restore strategy is fully developed and in place, you must also test the system to ensure it will be effective when the time comes—and the time will come. You don't want the live test to be the first time the power goes out or your building's sprinkler system decides to test itself.

Fully and regularly testing your backup and restore strategy is essential. And bear in mind you're not only testing the technology, you're also testing your process and the division of responsibilities in the event of a disaster. You're also testing the efficiency of your backup and restore process to ensure minimal loss of data and ease of restore. The longer your database is down and you have no access to your corporate data, the more money your business is losing.

Test your system to ensure that it meets your needs for data availability, speed of data restore, minimal loss of data and system performance. As you're scheduling regular backups, it's not a bad idea to also schedule regular system tests.

Back It Up

Planning your backup and restore infrastructure and process is essential. You need a solid plan to ensure you have the proper technology and processes in place to handle any disaster scenario. You don't want to find out after the fact that you didn't have the right strategy in place. **VR**

Lafe Low is an 1105 Enterprise Computing Group features editor.