Need a deeper dive on this topic? **Ask-An-Expert**

Understand the Risks When Migrating Data to the Cloud

January 24, 2019 | Ask-An-Expert | Cloud Application and Data Controls | By Dave Shackleford, IANS Faculty

What You Will Learn

- The importance of focusing on storage, database and application migration.
- Tips for planning and performing a successful data migration.
- The need for secure communications, backup and other key considerations.

The Challenge: Migrating Successfully

The security team for a large high-tech company wants to ensure it is aware of the risks and follows best practices when migrating data to the cloud. Specifically, the team asks:

- What are the risks associated with migrating from an on-premises data center to the cloud?
- What are the risks associated with migrating from one cloud provider to another, or of transitioning from one cloud management service provider to another?

Three Main Processes to Focus On

When planning and executing a cloud migration, organizations must consider everything from data integrity, business impact, cost, and user experience and impact, to potential downtime, data assessment and data quality. However, three common types of data migrations should take precedence:

- **Storage migration**: Storage migrations focus on moving data from one storage device to a new or different device – on-premises or in the cloud. On the surface, these are the most straightforward types of data migrations – but that doesn't mean you can just copy and paste a 5 TB folder to a new drive. You must plan and execute the migration to ensure success. Keep in mind when migrating sensitive and critical data, it's especially important to understand what data is moving where, and who can (or should) have access to it.

- **Database migration**: Database migrations are required when you need to upgrade the database engine or move the database installation or the database files to a new device. There are more steps to a database migration than a storage migration, and you need to plan a database outage to perform the migration. Organizations should back up the databases, detach the databases from the engine, migrate the files and/or update the database engine, and then restore the files to the new database from the new location.

- **Application migration**: Application migrations usually require some combination of the two options above. Applications can have databases, and they can have installation folders and data folders that need to be migrated. Application migrations may require additional steps per the application vendor.

Plan Your Data Migration

Moving sensitive and critical data can be a delicate task. It's important to make sure your data migration is planned carefully. Organizations should:

- **Create and follow a data migration plan:** Determine what data needs to be moved, how data should be moved, where it's going and who should access it. Set up a data migration plan that outlines each step, considering who will be affected, what the downtime will be, potential technical or compatibility issues, how to maintain data integrity and how to protect that data during the migration.

- **Fully understand the data you're migrating:** Take a good look at what you are migrating. Is it regulated data that requires security controls and specific access management? What data should go where? Who should be able to access what?

- **Extract, transform and de-duplicate data before moving:** It's a good idea to do a full data cleanup before migration. Once the data is migrated, it's probably going to be in that state until the next migration. Make sure you're migrating the right data, while preserving data integrity.

- **Implement data migration policies:** Establish policies to make sure data is going to the right place and ensure it's protected once migrated. You can automate these policies to make the destination data even more secure than the source – and even set up rules to re-permission the data during the migration.

- **Test and validate migrated data:** Make sure everything's where it should be, create an automatic retention policy, clean up stale data and double-check permissions. Back up your old system, so that you'll be able to find any missing files offline, if necessary.

- **Audit and document the entire process:** This helps with audit and compliance initiatives.

Additional Considerations

When an organization attempts a secure cloud migration, it relies on multiple data centers as well as its traditional IT environment, but the data centers and the traditional infrastructure are not connected to one another.

Using a secure IPsec tunnel between the border gateways to interconnect all the environments together and form a larger infrastructure network solves this problem. It allows access to the back-end local services and applications running in local environments – without exposing them to the outside world.

Filtering rules should also be applied to the border gateways to allow access to certain

resources, while preventing access to resources that contain sensitive information.

In addition, one of the most important services to use in a secure cloud migration is a backup service. This allows for agents to be installed on the systems that need to be backed up all over your infrastructure, regardless of where the server is located. Then a single server within a traditional IT network can be authorized to perform backups of the other remote systems, which can be done securely and regularly without exposing anything to the external internet.