LCloud, we need (AWS) backup!

AWS Backup allows you to create backups, facilitates centralization and automation of their creation in the AWS cloud, as well as on-premise. Eliminating the need to create your own scripts and manual configuration.

Scenarios of backup plans

Cloud-native backup provides a centralized console for automating and managing backups as part of AWS services.

Hybrid backup provides a common way to backup application data in the cloud as well as in the local environment.

On-premise backup provides a common way to back up application data both in the cloud and in the local environment. In the case of AWS Backup, it complements the AWS Storage Gateway service.

Service integrated with:

- Amazon RDS
- AWS Storage Gateway
- Amazon EFS
- Amazon EBS
- Amazon Dynamo DB

How do you configure AWS Backup?

1. Create the selected Backup Plan

Choose a plan from the options available in the AWS console:

- Create an existing plan based on AWS policies
- Build your own plan
- Build a plan based on JSON

2. Configure a Backup Rule

At this stage, focus on the configuration of data related to the frequency of backups and tag recovery.

3. Assign resources

The next action is assigning appropriate resources subject to the given Backup Plan. You can create one or more backup rules. Also specify tags which presence attaches the resource to the backup policy.

4. Start the backup

After configuration, it's time to launch AWS Backup. After verifying the copy, it's a good idea to remove any AWS resources that you do not need to keep in order not to incur unnecessary fees.

Additional functionalities

Backups on demand

You can back up selected resources on demand. Select the desired resource and its storage location, and then create a backup.

Recovery Points

You can find the list of recovery points in Backup Vaults, where you can check and restore previously created tables in Backaup Plan.

Security

The service provides access control and encryption features that help protect data and meet compliance requirements. By using AWS Identity and Access Management (IAM), you can manage backup authorizations, such as:

- control.
- restoring backups,
- management of backup plans,
- assigning resources to backup plans.

What do you gain?

- *Centralized backup management.*
- *A solution based on the ability to create backups that comply with business requirements and legal regulations.*
- *Possibility to tag resources to implement backup strategies in all applications. Ensuring that all resources are archived and protected.*
- *Automation of backup planning.*
- *Automated retention management - backup storage for as long as required.*
- *Security by encrypting backup data.*
- *Access control and backup life cycle monitoring.*

www.lcloud.pl/en