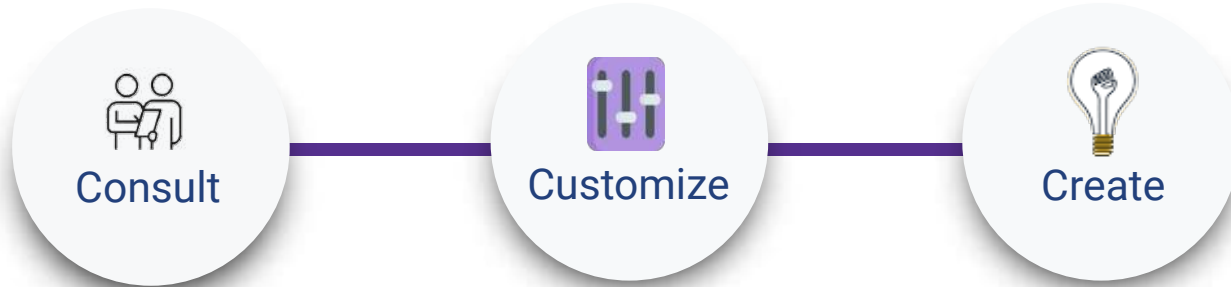




A Complete Guide to Backup and Disaster Recovery on Amazon Web Services

Guide






Amazon Web Services


Moving data to the cloud is one way to help increase availability and reliability, as compared to on-premises infrastructure. However, even the best-managed clouds can fail. That's why having a data backup and recovery plan in place is critical, even if you use the cloud. With that need in mind, this whitepaper explains backup and disaster recovery best practices for Amazon Web Services (AWS). It discusses the various services offered by AWS and explains how they can be used to facilitate efficient and reliable backup and recovery.








3-2-1 Backup Strategy

To ensure your data is safe and up to date, we recommend the 3-2-1 backup strategy, which is defined as follows:

-  Have at least 3 copies of your data.
-  Keep two copies of your data on two different types of media.
-  Store one copy of your data offsite.

Types of Cloud Storage:


 AWS offers several types of storage options, each of which can be used to support different backup needs.


-  File-Level Backup
-  Image-Based Backup Level
-  SQL Database Backup
-  Microsoft Exchange Backup
-  NAS Backup
-  Mac & Linux Backup
-  EC2 Backup


Amazon Web Services


Amazon Web Services offers different classes of storage for various usage scenarios. This allows organizations to reduce storage costs for backups which are not accessed often. Classes have a high level of reliability and support SSL data encryption during transmission, but differ in cost.

Contact Us

 info@onqloud.com

 +971 6 5441665

 UAE, India.

 www.onqloud.com