Net3 Technology

Data Backup

Recovering from Backups: A Checklist

There can be quite a few challenges when it comes to backing up data. Here is a comprehensive checklist to make sure all bases are covered for a successful recovery.

STEPS TO TAKE WHEN DEFINING A BACKUP/DR PLAN

1. DISCOVERY: In order to put together a comprehensive DR plan, you have to understand the environment completely. Some questions you need to answer are:

What applications are being used? (ERP, Accounting, CRM, Ops, etc.)
Is there an inventory of servers/endpoints/network devices?
What technologies are present in the environment? (virtualization, clustering, log shipping, etc.)
What does the network look like currently? (Network diagrams, maps, lists of subnets)
Are there redundancies or highly available applications in place?
Where is the data located? (NAS, Endpoints, Cloud, SaaS, etc.)
How much data is being generated daily?
How much data is historical archive?
What are the security mechanisms in place?
What are the biggest risks to the data?
Who is responsible for each application?

2. DEFINITION: Once the discovery of the environment is complete, you can work to define the applications and data that need to be addressed in the DR plan:

What applications are customer facing? (Most Impactful)
What applications are internal facing? (Impactful)
What applications are in management/ops roles? (Least Impactful)
How long does the data need to be kept? (Retention)
How much data loss can be tolerated? (RPO)
How fast do workloads need to be available? (RTO)
What are the policy requirements? (HIPPA, PCI, CJIS, CMMC, etc.)
What are the audit requirements? (Testing Schedules, Documentation, Etc.)
Is there any stakeholder input? (How often should the data be protected from an end user POV?
How critical is the data the end user is putting into the system?)

Recovering from Backups: A Checklist

3. SCOPING: Once you have defined each application and the requirements around protection, you can then scope each application to a product.

Faster RPO's, quick RTO's a Replication
Longer Retentions a Backup
All of the Above a Hybrid

4. IMPLEMENTATION: Implementation can be a busy time. It might help to have a guided implementation so that there are product experts on hand. Make sure to cover the following:

Ensure products are deployed according to best practices.
Test the product to make sure it provides the protection needed for that application.
Thorough testing of all scenarios for DR communication.
Documentation of all product configurations and infrastructure.

5. AUDITING AND TESTING: Once the implementation phase is over, a good audit and testing plan should be put in place.

Failure notifications for backup jobs and failover mechanisms should be instantaneous.
Backup job and failover reviews should be done at least 1x per week.
Test failovers and recoveries on a regular basis. At least 2x per year.
Comprehensive auditing of backups and failover mechanisms should be performed at least 1x a year by someone not involved in the DR process.

If you have any questions about backing up to the cloud, please contact us and Request More Info to speak with a Net3 Engineer.

Net3 Technology is a cloud services provider offering nationwide backup and disaster recovery solutions tailored to fit company requirements with flexible pricing options.