druva

Top 4 critical steps for cloud backup and disaster recovery planning

The volume and value of your organization's data is increasing, driving the need to implement innovative cloud backup and disaster recovery (DR) strategies. But, creating a comprehensive cloud backup and DR plan is easier said than done. To help move your plan forward, here are some key steps you should consider.

Step 1: Perform a business impact analysis

A comprehensive backup and DR planning process must begin with an accurate assessment of your current virtualized environment. How much data are you currently managing? Where is it located? How critical is it to your business operations?

Step 2: Perform a risk assessment

A risk assessment is focused on potential external situations that could negatively impact your business and the likelihood of such situations occurring. These could include natural disasters as well as man-made events. When you're preparing a risk assessment, be sure to leverage all available records to assess the threat of a disaster.

Step 3: Design a risk management strategy

What can I do to mitigate the damage? This is when you need to decide upon a specific solution for backup and DR. Consider RPO/RTO, data residency laws, and budget for implementation. You can calculate the ROI of competing vendors and select the one that best fits your organization's requirements.

Step 4: Configure and test (and keep testing!)

You need to know whether your backup and DR solution is configured correctly before you actually have to use it. The only way to achieve that is by regularly testing your DR solution. A cloud-native backup and DR solution allows you to immediately spin up your virtual machines in the cloud for development testing (dev-test) purposes.

Innovate your cloud backup and disaster recovery plan—check out druva.com/cloud-disaster-recovery to learn more.

Q320-20079