Backup and Disaster Recovery Plan Checklist

aws PARTNER

Determine Recovery Objectives (RTO and RPO)

- Determine which workloads are the most mission-critical to your organization, and what recovery time objective (RTO) and recovery point objective (RPO) are required for these workloads. RTO is the amount of time required to recover from a disaster after notification of business disruption. RPO is the window of time in which data loss is tolerable.

Identify Stakeholders

- Identify all those who need to be updated once disaster strikes. Make sure to include stakeholders involved in performing the actual recovery from a disaster (such as engineers, technical support, etc.).

Establish Communication Channels

- Create a list of all teams responsible for DR, along with their roles and contact information. Establish a complete chain of command, including relevant executive leadership and accountable individuals from each of the engineering teams (such as network, systems, database, and storage).

Collect All Infrastructure Documentation

- Infrastructure documentation is recommended, especially given the pressure that comes with a disaster. Map all network connections, Setup of systems and usage, storage and databases, cloud templates.

Choose the Right Technology

- Before selecting a DR solution, consider total cost of ownership (TCO), which can be higher for on-premises DR than cloud-based strategies because of duplicate hardware and software licensing costs.

Define Incident Response Procedure

- Define in detail what is considered a disaster. What is the length of time systems must be affected to be considered a disaster? How will you verify that the disaster is really happening and how the disaster will be reported?

Define Action Response Procedure and Verification Process

- Outline how to perform failover to the DR target site with all necessary steps. Even if your recovery process uses a DR tool with automated components, prepare the action response procedure in writing to define how the necessary services will be started, verified, and controlled.

Perform Regular Testing

- Testing your DR plan in action is essential but often neglected. DR drills demonstrate whether your DR solution is sufficient, it will also prepare your engineers and supporting teams to respond quickly and accurately.

Stay Up to Date

- Review how past DR test were handled and make note of the findings. Continue to update your DR strategy to reflect changes you make to your primary production environment.

Prepare for Failback to Primary Infrastructure

- You may need to plan for downtime or a partial disruption of your business during the failback process to your primary site. There are solutions available that simplify failback to your primary infrastructure.

For more information on AWS Cloud Backup and Disaster Recovery solutions, contact us today.