NEOnet | Northeast Ohio Network for Educational Technology

Backup and Data Availability

Table of Contents

1 NEOnet Backup Procedure

1.1 Purpose

The purpose of this policy is to ensure that all critical data and systems are consistently backed up, protected, and available for recovery in the event of system failures, data corruption, or disasters. This policy outlines the processes and retention standards for backups and replication across all data centers to guarantee business continuity.

1.2 Scope

This policy applies to all virtual machines (VMs), data volumes, and production servers across both data centers. It includes procedures for daily backups, replication, retention, and cloud storage for disaster recovery purposes.

1.3 Backup Frequency and Replication

- **Daily Backups**
  A software-based backup solution is used to back up all virtual machines (VMs) daily at both data centers. This ensures that the latest data is available for restoration in the event of a failure or system issue.
- **Cross-Data Center Copy**
  Each production backup is also replicated to the opposite data center, ensuring that a copy is available in case of a site-wide failure. This provides redundancy across locations for critical systems.
- **Cold-Ready VM Copies**
  In addition to the production backup, a replicated copy of each VM is created at the opposite data center in a cold-ready state after the backup job is completed. This ensures a quick recovery option in case of a failure at one data center.
- **Volume-Based Replication**
  Hourly volume-based replication is performed on the storage array, replicating each data volume to the opposite data center. This continuous replication minimizes data loss and ensures that the latest data is available for recovery.

1.4 Retention Periods

- **Backup Retention**
  A total of **45 days** worth of backups is maintained for both primary backups and replicated copies. This includes historical backups for auditing and operational purposes.
- **Replicated VM Copies**
  The last **four replicated copies** of each backed-up VM are retained at the opposite data center, ensuring that multiple versions are available in case a restoration is needed.
- **Volume Snapshots**
  The last **48 hours** of hourly volume snapshots are retained. Additionally, a single snapshot of each volume is retained for **14 days**, allowing for longer-term recovery options.
- **Immutable Cloud Repository**
  As a final layer of security, a second backup copy is created from the primary backup and sent to an immutable cloud repository. This backup is retained for **14 days** and provides protection against ransomware and other malicious attacks.

1.5 Data Availability

- **On-Premise Availability**
  All backups and replicated data are stored across both data centers to ensure quick recovery and high availability in case of a localized failure. The cold-ready VM copies enable rapid recovery and continuity of operations.
- **Cloud Availability**
  Immutable cloud backups provide a final safeguard in case of catastrophic failure or malicious attacks. These backups are securely stored in the cloud and cannot be altered or deleted, ensuring their integrity for the full retention period.

1.6 Monitoring and Testing

- **Regular Monitoring**
  The backup and replication processes are continuously monitored to ensure successful completion of all jobs. Any failures or issues are addressed promptly to maintain the integrity of the backup system.
- **Disaster Recovery Testing**
  Periodic disaster recovery tests are conducted to validate the integrity of backups and ensure data can be restored within the required timeframes. This testing ensures the effectiveness of both the on-premise and cloud-based recovery systems.

1.7 Compliance and Security

All backups and replication processes comply with organizational security policies and relevant regulatory requirements. The use of immutable cloud storage ensures that critical data remains protected against unauthorized access, alteration, or deletion.

1.8 Policy Review

This policy will be reviewed annually or when significant changes to the infrastructure occur. The goal of the review is to ensure that backup and replication practices remain aligned with business needs and industry best practices.