UNITRENDS

UNEXPECTED IT DISASTER RECOVERY FAILURES

HIDDEN RISKS CHECKLIST

IT teams often plan backup and data retention strategies without thoroughly mapping the dependencies and requirements needed for smooth recovery. Many are learning the hard way that failing to align backup plans with specific restore expectations can have devastating consequences.

The following checklist can help you identify and eliminate common reasons for unexpected recovery failure.

01 TEST DISASTER RECOVERY AT LEAST MONTHLY

Did you know? Advanced backup and recovery solutions will automatically test recoverability of applications and document actual recovery time and recovery point.

02 LIST MULTI-TIER APPLICATION RESTORE REQUIREMENTS

Multi-tier or N-tier applications run on multiple servers that need to communicate with one another to operate. If you restore them with the wrong boot order or to a host with a different virtual network you risk recovery failure, data loss, and hours of wasted IT time.

03 ACTIVE DIRECTORY DEPENDENCIES

A domain controller running Microsoft Windows Active Directory (AD) Services authenticates and authorizes all users and computers in a specific Windows domain. The AD server has to be restored before the applications that depend on it.

04 COMPATIBLE BACKUP AND DISASTER RECOVERY INTERFACES

Example: Backing up with a system that uses UEFI (Unified Extensible Firmware Interface) and trying to restore to a server that only supports MBR (master boot record) BIOS will fail.

05 OPERATING SYSTEMS AND APPLICATION VERSIONS

Example: Restoring older backups to newer systems that do not support earlier software versions.

06 PRODUCTION VM DISK CONFIGURATIONS AFFECTING RECOVERY

Example: In VMware, if you configure both disks needed for backup in independent mode, neither disk will can be snap-shotted and backups will be empty.

07 PREVENT JOURNAL WRAP CONDITION

If your backup appliance uses incremental forever backups, you may need to increase the size of your backup journal over time or make other adjustments to your backup. Backup and cloud DR-focused vendors that offer expert installation and support will help you avoid this issue.

08 BACKUP SAAS AND IAAS APPLICATIONS

Example: SaaS applications (O365, Saleforce.com, GSuite) and applications running in IaaS (AWS, Azure, or Google Cloud) are vulnerable to a wide range of downtime and data loss risks that are not covered by cloud providers.