Full Restore Testing

The complete restoration of backups in a controlled environment to ensure that all data can be fully recovered

What is Full Restore Testing

As your trusted IT solutions provider, we recommend that you regularly perform disaster recovery tests on your backup systems and software. This in effect is a 'full test restore' of your backup. Regular 'full test restores' of backups are essential for ensuring that your backups are reliable and that you can recover your data in the event of a data loss disaster.

How Does Full Restore Testing Work

We do complete selective restores of data during maintenance visits. However, a 'full test restore' and a 'selective restore' are two different approaches to restoring data from a backup. Here's how they differ:

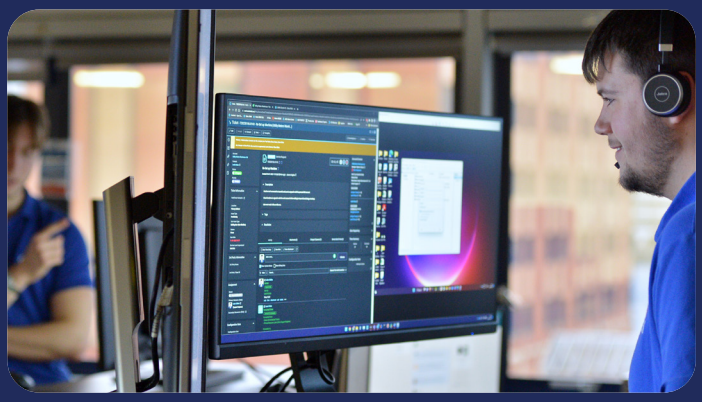
1. **Selective restore:** In a selective restore, only specific data is restored from the backup. This type of restore is typically done when only certain files or folders need to be recovered, rather than the entire system. Selective restores are usually faster than full test restores because they involve restoring only a subset of the data. However, it's important to note that selective restores may not be able to restore the system to its previous state if important data is missing.

2. **Full test restore:** In a full test restore, all data from the backup is restored to a test environment. This type of restore is typically done to test the integrity of the backup and to ensure that the backup can be successfully restored in the event of a disaster. A full test restore may be done periodically to ensure that the backup is up-to-date and that all necessary data can be recovered in case of a disaster.

In summary, a full test restore is a comprehensive restore of all data from a backup, while a selective restore only restores specific data as needed/required. Both approaches have their uses and are important parts of a backup and disaster recovery strategy.

The Importance of Full Restore Testing

Doing a full restore test ensures that you have captured all the data you need, that your backups are working correctly, and that you have a plan for recovering your data in the event of a disaster. A full test restore gives you and your team the opportunity to practice the steps necessary for a successful data recovery. This helps reduce the time it takes to complete the recovery process in the event of an actual disaster. Running full test restores regularly, can help you identify any potential issues with your data backups and allow you to take corrective action before any disaster occurs.



The Outcome

Doing a full test restore gives you and your team the opportunity to practice the steps necessary for a successful data recovery and helps reduce the time it takes to complete the recovery process in the event of an actual disaster. Running full test restores regularly, can help you identify any potential issues with your data backups and allow you to take corrective action before any disaster occurs.

The frequency of performing a full test restore of backups depends on the specific requirements and policies of your organisation. However, it is generally recommended to perform a full test restore at least every 6 months or after any major changes to your IT infrastructure or backup environment. The frequency of these can be agreed with your account manager.

What This Product Does:

Comprehensive Backup Validation: Verifies the integrity and recoverability of your entire backup system.

Disaster Recovery Simulation: Tests the full restore process to ensure readiness for real-world scenarios.

Identifies Backup Issues: Detects and reports any data inconsistencies or errors for corrective action.

Provides Regular Testing: Scheduled testing ensures backup reliability over time.

Supports Compliance Needs: Assists in meeting regulatory requirements for data integrity and recovery.

What This Product Doesn't Do:

Real-Time Recovery: Testing is performed in a controlled environment, not during an active disaster.

Guarantee Instantaneous Recovery: Full tests identify potential delays or issues but are not designed for live recovery scenarios.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk

Full Restore Testing

Why is This Not Included in My Support?

Full disaster recovery (DR) tests can take a long time due to the complexity and scope of the test. A full DR test involves simulating a complete disaster scenario, such as a site-wide outage or a major system failure and testing the recovery process to ensure that critical systems and data can be restored within the required recovery time objective (RTO) and recovery point objective (RPO).

Here are some reasons why full DR tests can take a long time:

- Large amounts of data: Recovering large amounts of data can take a significant amount of time, especially if the data needs to be transferred over a network or from physical media. This can slow down the recovery process and extend the time required for the DR test.
- Complex IT infrastructure: Modern IT infrastructures are complex and interconnected, with multiple applications, databases, and systems that need to be recovered in a specific order. Coordinating the recovery of all these components can take a long time and require a high degree of technical expertise.
- Testing multiple locations: A full DR test may also involve testing recovery procedures across multiple locations, such as a backup data center or a cloud environment. This requires coordination and testing across different networks and systems, which can add to the time required for the test.

In summary, full DR tests can take a long time due to the complexity and scope of the test. However, regular testing and validation of disaster recovery plans is essential to ensure that critical systems and data can be recovered in the event of a disaster, and that your organization can meet its RTO and RPO objectives.

Why You Can't Rely on Backup Logs/Reports to be Sure of Data Integrity and Ability to Restore:

Backups are an essential part of data protection and disaster recovery planning. However, backups alone cannot guarantee data integrity.

There are several reasons why you cannot rely solely on backup logs to ensure data integrity:

- Backup logs do not verify data consistency: Backup logs provide a record of when backups were taken, but they do not verify the integrity or consistency of the data that was backed up. Data corruption or errors can occur during the backup process, and these issues may not be detected until an attempted restore.
- Backup logs do not guarantee recoverability: Backup logs do not guarantee that your data can be recovered. Even if backups were taken correctly, there is no guarantee that the data can be restored in the event of a disaster or system failure. Regular testing and validation of backups is essential to ensure recoverability.
- Backup logs can sometimes be inaccurate or incomplete, especially if there are issues with the backup software or hardware. This can make it difficult to identify problems with the backup process and can lead to data loss if issues are not detected and addressed.
- Backup logs cannot protect against human error, such as accidental deletion of data or misconfiguration of backups. Implementing data protection policies and procedures that incorporate human error prevention strategies is essential for ensuring data integrity.

In summary, backup logs provide valuable information about the backup process, but they cannot guarantee data integrity or recoverability. Regular testing and validation of backups, as well as implementing data protection policies and procedures, are critical to ensure data integrity and protect against data loss.

T: 0161 233 0099

E: enquiries@apexcomputing.co.uk