Name: First G. Macapayad Date: September 30, 2025

Section: BSIT - 4R6

System Monitoring and Performance Tuning -Backup and Recovery Strategies

Monitoring and optimising system performance is the process of determining how well a computer system or network operates. Changes are made to increase its speed and efficiency. The goal of performance tuning is to increase the speed and efficiency of your computer systems.

It is essential to evaluate applicants abilities in system monitoring and performance tuning to make sure you select the best specialist for your IT staff. There are two efficient methods for doing this utilising evaluations. These are tests of practical skills and questions that are based on scenarios.

One of the most trustworthy ways to evaluate system monitoring and performance optimisation abilities is through hands-on skill assessments. These assessments might mimic actual situations that the applicant may encounter at work. Additionally, scenario-based questions are a useful tool for assessing applicants, since candidates may encounter real-life scenarios in these questions when keeping an eye on and adjusting systems.

Data management is the foundation of backup and recovery strategies. These are procedures designed to safeguard data against corruption or loss and guarantee data availability in the event of calamity. Data integrity and business continuity depend on these procedures.

When it's at its peak, your data is perfectly duplicated in a backup copy, which is easily available when you need it. The process of returning data from backup copies to its original or usable condition is known as recovery after a calamity, corruption, or loss of data. The backup copy must be readily available and up to date for the recovery to be successful.

Backups are long-term, static copies of data that can be used for recovery, stored on-site or off-site. Any storage layer, including removable media like tape, can house a backup. They can be readily air-gapped, encrypted, or rendered unchangeable in the event of a cyberattack. To adhere to data protection regulations, backups are utilised to retain data for years under rules and guidelines.

Your digital data cannot be protected without disaster recovery and backup solutions. If data exists in a single location, like a single hard drive or a single cloud instance, it becomes extremely vulnerable. A single unintentional keystroke, a single malware infection, or one equipment failure might destroy everything similar to shredding or dumping a notebook in the wrong pile of documents.