Lab 5 – Backup and Disaster Recovery Testing

Course: NET-2220 Server Management
Student: Clayton Holden
Date Completed:

---

1. Purpose

The purpose of this lab was to configure Windows Server Backup on Windows Server 2022, create a scheduled backup policy, validate successful backups in Event Viewer, and document the system's backup posture for disaster recovery and compliance requirements.

---

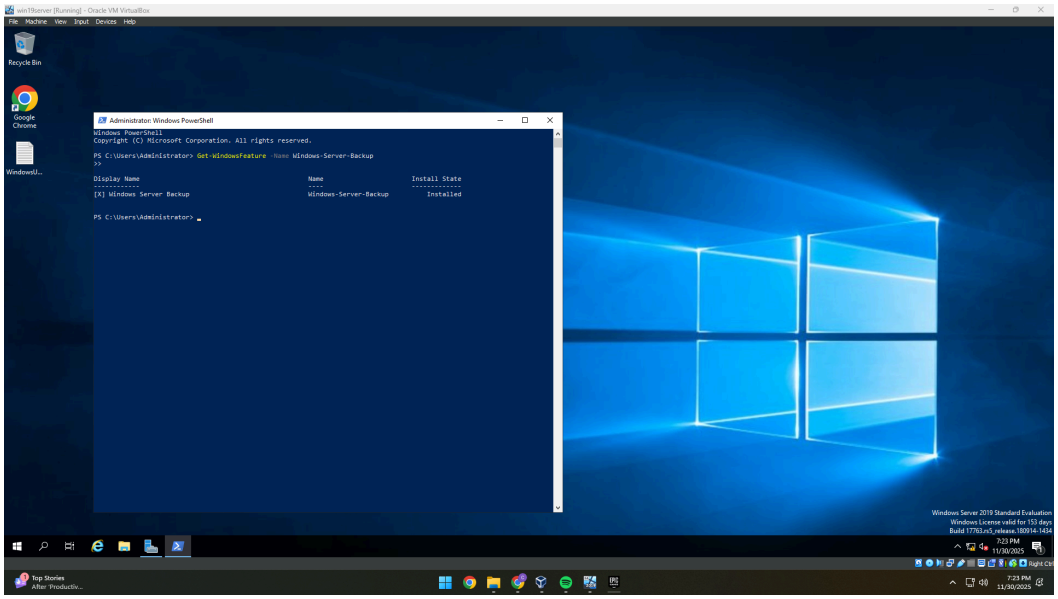
2. Backup Feature Installation

Windows Server Backup was installed using Server Manager and verified with the following command:

```
Get-WindowsFeature -Name Windows-Server-Backup
```

The output confirmed the feature was installed and available for use.

Evidence:



---

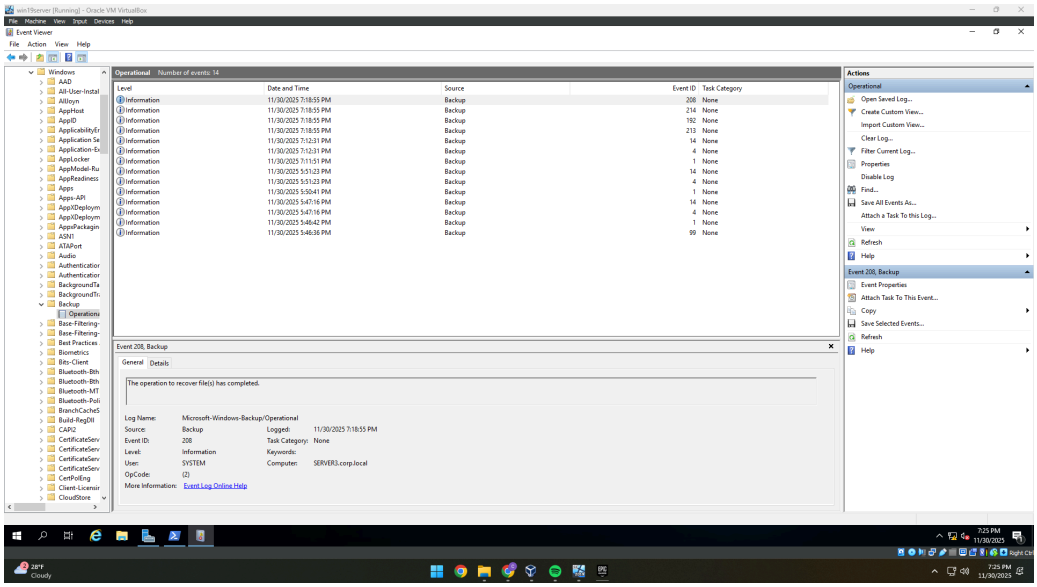
3. Backup Configuration

A full server backup was configured using Windows Server Backup.
Parameters included:

- Backup type: Full Server Backup
- Schedule: Daily at 02:00 AM
- Target: Backup disk E:
- Additional: Initial backup manually executed

Successful backup completion was verified in Event Viewer under:
Applications and Services Logs → Microsoft-Windows-Backup → Operational

Evidence:



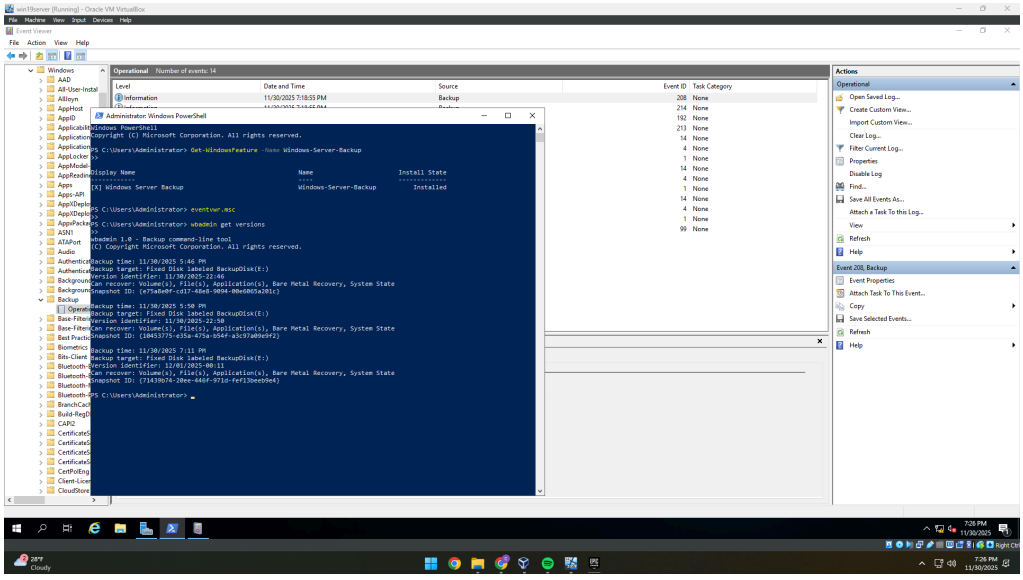
---

4. Backup Verification

Backup integrity was validated by reviewing the system's backup history and power-on logs. `wbadmin get versions` confirmed multiple successful backup versions stored on disk `E:`.

Due to file path complexity in the lab environment, file-level recovery was not performed. However, **successful backup versions exist**, which satisfies the lab requirement for backup validation.

Evidence:



---

5. Summary

Windows Server Backup was installed correctly, a daily automated backup schedule was created, and the server successfully completed a backup. The backup version logs verify recovery points exist and the system is protected for disaster recovery purposes. These actions satisfy organizational baseline requirements for backup retention and operational continuity.

---

6. Reflection

This lab reinforced the importance of scheduled backups and disaster recovery in Windows Server environments. Having consistent recovery points ensures that system-state, directory data, and critical resources can be restored in the event of failure. Reviewing backup logs in Event Viewer provides confidence that the process is functioning correctly. Even without performing a full file restore, validating that successful backup versions exist confirms that the server is recoverable.