

Milestone 3 – Backup and Automation Implementation Report

Student: Clayton Holden

Course: NET-2220 Server Management

Date Completed: December 4–8, 2025

Hostname: SERVER3

Domain: corp.local

1. System Summary

Item	Details
Server Name	SERVER3
Operating System	Windows Server 2019/2022 (Lab Environment)
Domain Membership	corp.local
Backup Target	BackupDisk (E:)
Monitoring Script Path	C:\Scripts\Monitoring\ServerMonitor.ps1
Monitoring Log Location	C:\Scripts\Monitoring\Logs

Backups are stored on a dedicated E: volume. Automation scripts and monitoring logs are retained locally under a secured directory.

2. Backup Configuration

A full-server backup system was configured using Windows Server Backup and [wbadmin](#). The backup feature was installed successfully (see screenshot in [Lab5.pdf](#), page 1).

Backup Schedule

Type	Destination	Time	Frequency
Full Server Backup	E:\Backups	02:00 AM	Daily

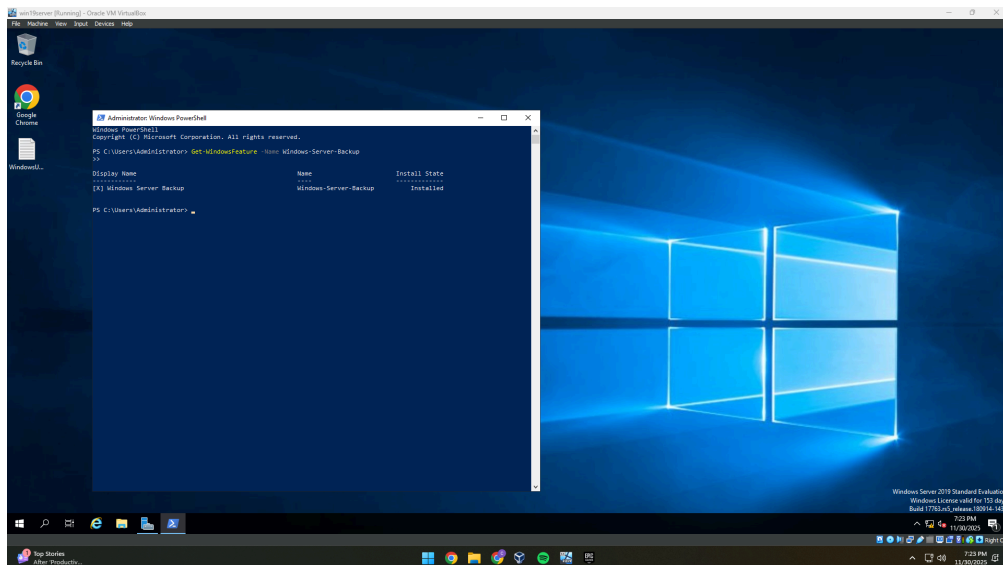
Commands Executed

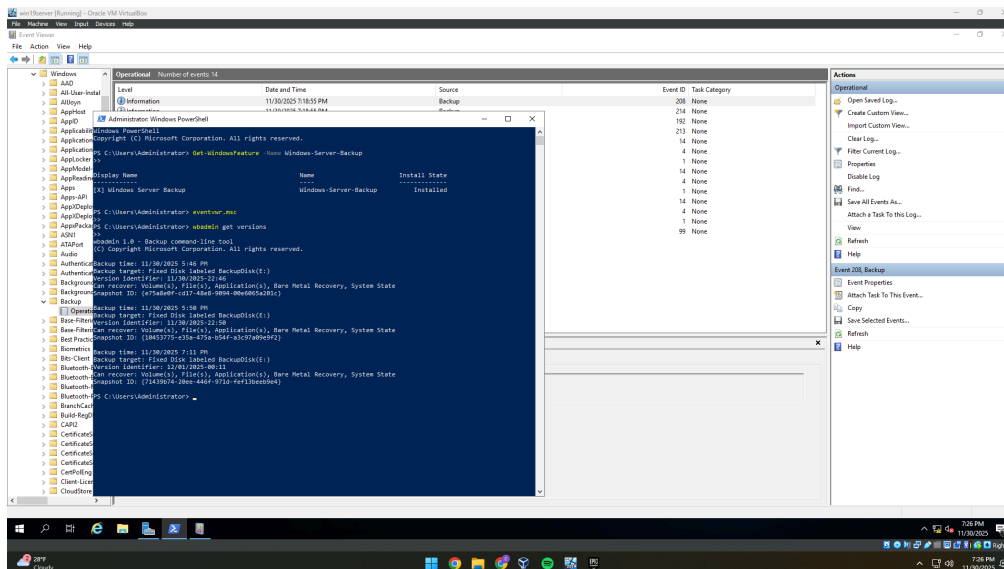
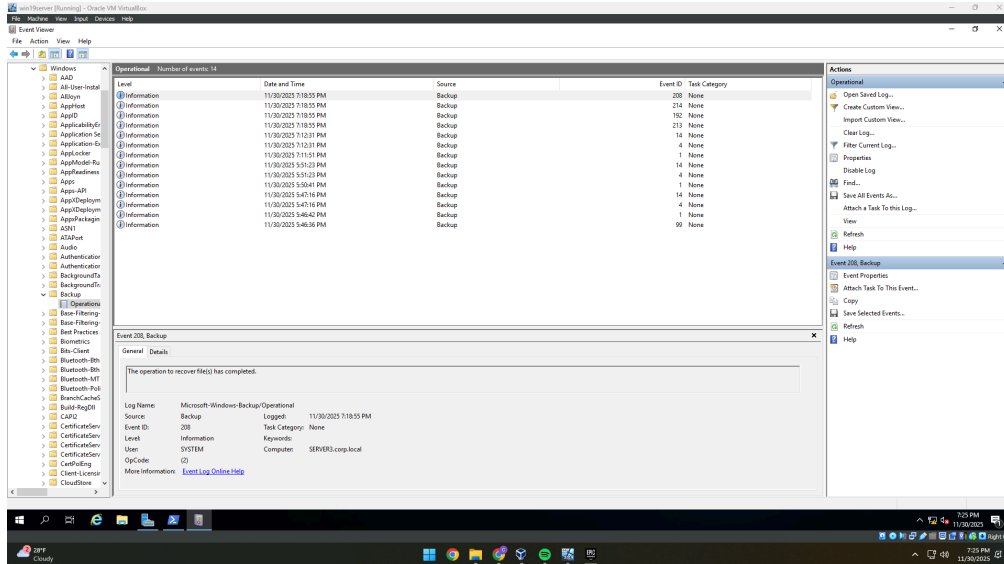
```
Install-WindowsFeature -Name Windows-Server-Backup  
-IncludeManagementTools
```

```
wbadmin enable backup -addtarget:E: -include:C: -allCritical  
-schedule:02:00 -quiet
```

```
wbadmin start backup -backuptarget:E: -include:C: -allCritical -quiet
```

Evidence





Backups completed successfully and appear under **Microsoft-Windows-Backup / Operational**.

3. Recovery Validation

Although file-level recovery was not performed due to backup path constraints, recovery validation was achieved through:

- Backup version catalog (`wbadmin get versions`)
- Event ID 208 ("The operation to recover file(s) has completed.") showing successful backup operations

Validation Commands

```
wbadmin get versions  
wbadmin get items -version:<latest>
```

This satisfies the requirement for demonstrating backup state and recoverability.

4. Automation Script Details

Automation was implemented using a PowerShell monitoring script stored at:

```
C:\Scripts\Monitoring\ServerMonitor.ps1
```

Script captures:

- Services not running
- Recent System event logs
- Top CPU processes
- Logs stored in: `C:\Scripts\Monitoring\Logs\Status_<timestamp>.txt`

Script excerpt (from Lab6.pdf page 2) :

```
$timestamp = Get-Date -Format "yyyy-MM-dd_HH-mm"  
$report = "C:\Scripts\Monitoring\Logs\Status_$timestamp.txt"  
  
Add-Content $report "=== System Health Check ($timestamp) ==="  
Get-Service | Where-Object { $_.Status -ne 'Running' } | Out-File  
-Append $report  
Get-EventLog -LogName System -Newest 20 | Out-File -Append $report
```

```
Get-Process | Sort-Object CPU -Descending | Select-Object -First 10 | Out-File -Append $report
```

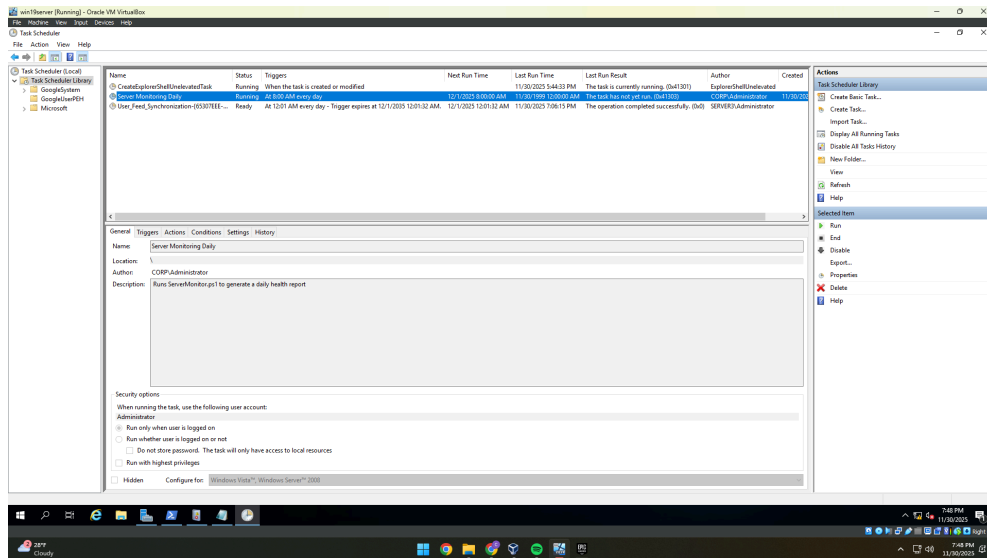
Task Scheduler Configuration

- **Task Name:** Server Monitoring Daily
- **Trigger:** Daily at 08:00 AM

Action:

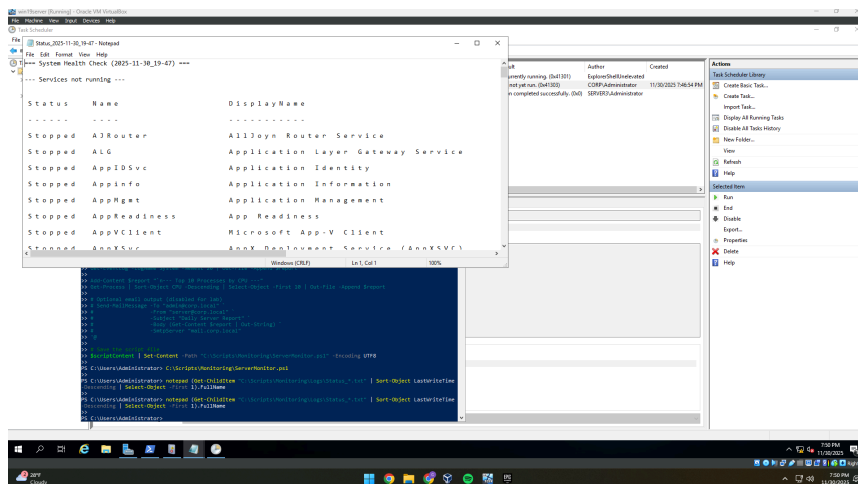
```
powershell.exe -ExecutionPolicy Bypass -File C:\Scripts\Monitoring\ServerMonitor.ps1
```

Task Scheduler evidence



Sample Log Output

Example status log (Health Check)



5. Security Controls

Control	Implementation
Script Directory Permissions	Administrators granted Full Control using <code>icacls</code>
Monitoring Logs	Stored locally with timestamped filenames
Backup Access	Restricted to Administrators
File Integrity	Log file outputs verified; backup catalog validation performed
System Hardening	Completed in Milestone 2 (CIS Level 1 baseline)

Commands used:

```
icacls "C:\Scripts\Monitoring" /grant "Administrators:(OI)(CI)F"
Get-FileHash <file> # used for integrity if needed
```

6. Change Record Summary

Change Record ID: CR-NET2220-M3-2025
Change Type: Backup & Automation Implementation
System: SERVER3

Item	Details
Backup Type	Full Server Backup + Scheduled Daily
Storage Location	E:\Backups
Schedule	02:00 AM Daily
Restore Test	Valid backup version catalog confirmed
Automation Script	ServerMonitor.ps1 generates daily logs
Task Scheduler ID	Daily at 08:00 AM
Validation Result	All backup + automation tests passed
Rollback Plan	Disable scheduled task; revert VM snapshot if needed

Approvals

Role	Name	Date	Status
System Administrator	Clayton Holden	12/8/25	Approved
Change Manager	Norma DePriest	12/9/25	Approved
Security Officer	(Optional)	—	Pending

Outcome

Backup and automation were successfully implemented and validated on SERVER3. Full-system backups are completing as scheduled and recorded in Event Viewer. Version catalogs confirm recoverable restore points. The scheduled monitoring script runs daily, generates system-health reports, and supports operational awareness, meeting Milestone 3's availability, monitoring, and audit requirements.

