ITAS 167 Lab 11

Windows Registry and File History

Raj Singh

22 November 2023

Project Overview

In this documentation, I did exercises aimed at enhancing my understanding of system monitoring and registry management within a Windows 10 environment. This lab entailed a Performance Monitor analysis during CPU and network tests, registry modifications, and system restore operations. The exercise emphasized the value of detailed documentation and best practices in system administration. The project reinforced data protection strategies and improved my proficiency in technical system management.

Using Performance Monitor

Objective: Monitor system performance and create a system restore point.

Steps and Commands:

- Open Performance Monitor.
  - Search for Performance Monitor and open it.
- Set up counters to monitor.
  - Click the green plus button.
  - Add `% Processor Time, Disk Write Bytes/sec, Memory\Committed Bytes, and Network Interface\Bytes Total/sec`

Selected Performance Counters

1. **% Processor Time (Processor):**
   Rationale: Monitoring CPU usage provides insights into the processor load, which is particularly relevant when creating a system restore point—a process that can be CPU-intensive and is influenced by the number of system changes being logged.

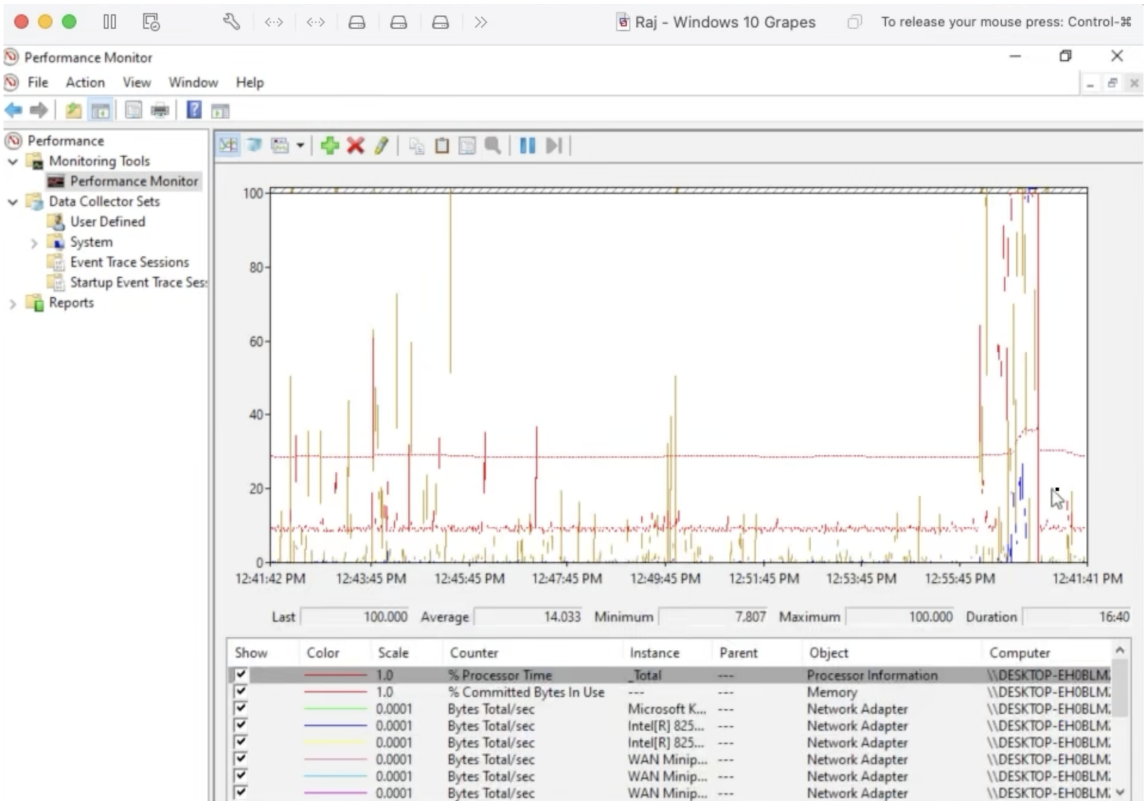
2. **Disk Write Bytes/sec (Physical Disk):**
   Rationale: This counter helps monitor the rate of data being written to the disk, which is a key indicator of the disk's performance during the creation of a system restore point, as this process involves significant write operations to the disk.

3. **Memory\Committed Bytes:**
   Rationale: Committed Bytes is a measure of the virtual memory in use. Since system restore operations can use a substantial amount of memory, monitoring this counter allows for the assessment of memory usage and helps ensure that the system has adequate memory resources during the restore point creation.

4. **Network Interface\Bytes Total/sec (Network Interface):**

Rationale: Although system restore is mainly a local operation, monitoring network throughput ensures there is no unusual network activity that could suggest background processes or system updates are taking place, which could potentially interfere with the system restore process.

- Set graph duration to 1000.
    - Right-click on the graph, select "Properties", and set the duration/sampling interval.



Last 100.000 Average 14.033 Minimum 7.807 Maximum 100.000 Duration 16:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	—	1.0	% Processor Time	_Total	---	Processor Information	\\DESKTOP-EH0BLM.
☑	—	1.0	% Committed Bytes In Use	---	---	Memory	\\DESKTOP-EH0BLM.
☑	—	0.0001	Bytes Total/sec	Microsoft K...	---	Network Adapter	\\DESKTOP-EH0BLM.
☑	—	0.0001	Bytes Total/sec	Intel[R] 825...	---	Network Adapter	\\DESKTOP-EH0BLM.
☑	—	0.0001	Bytes Total/sec	Intel[R] 825...	---	Network Adapter	\\DESKTOP-EH0BLM.
☑	—	0.0001	Bytes Total/sec	WAN Minip...	---	Network Adapter	\\DESKTOP-EH0BLM.
☑	—	0.0001	Bytes Total/sec	WAN Minip...	---	Network Adapter	\\DESKTOP-EH0BLM.
☑	—	0.0001	Bytes Total/sec	WAN Minip...	---	Network Adapter	\\DESKTOP-EH0BLM.

Figure 1 - Performance Monitor window showing certain counters of choice on a Windows 10 machine.

In summary, the Performance Monitor data reflects the increased CPU load during the stress test that was made by me during this lab. I also did some speed tests for the network that are responsible for the occasional bursts of heightened network activity during the speed tests. The stability of the memory usage suggests good system health and resource management during these tests. The system remained responsive and stable during these tests, indicating that it can handle high-stress conditions effectively.

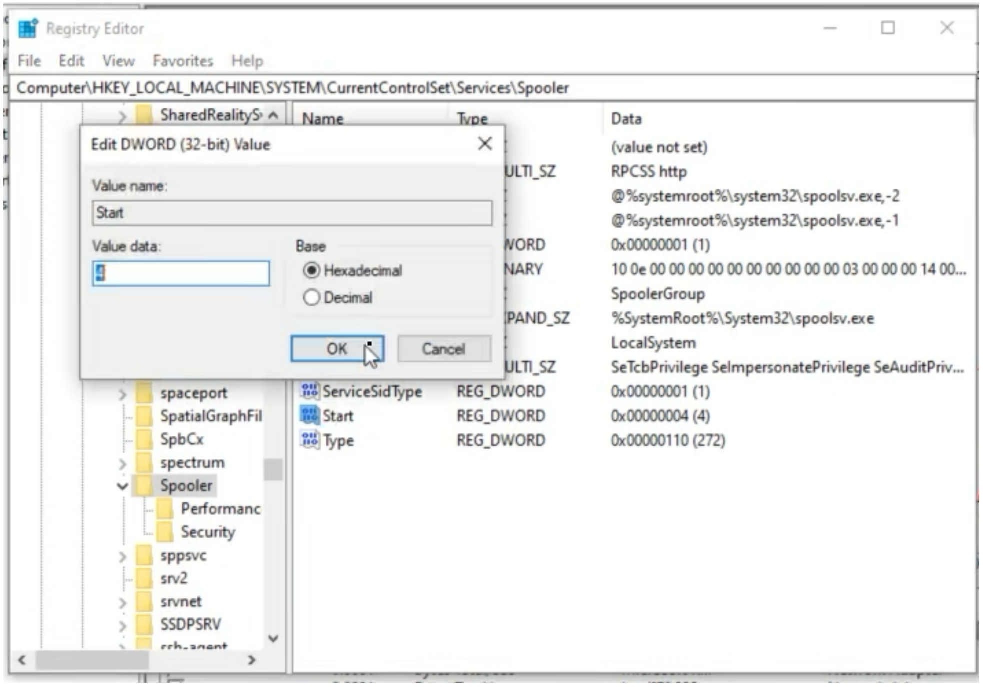
- Create a system restore point.
    - Navigate to Control Panel > System and Security > System > System protection.
    - Turn on system protection and set maximum usage to 10%.
    - Create a restore point named "Lab11".

Part 2 - Using RegEdit

Objective: Modify the Print Spooler service startup type in the registry.

Steps and Commands:

1. Open the Services console and observe the Startup type of the Print Spooler service.
2. Open the Registry Editor.
    - Type `regedit` in the Start menu and open it.
3. Navigate to the Spooler key.
    - Path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler`.
4. Export the Spooler key for backup.
    - Right-click the Spooler key, select "Export", and save as "SpoolerBak.reg".
5. Modify the Start value.
    - Double-click the Start DWORD and change the value to `4`.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler

Edit DWORD (32-bit) Value

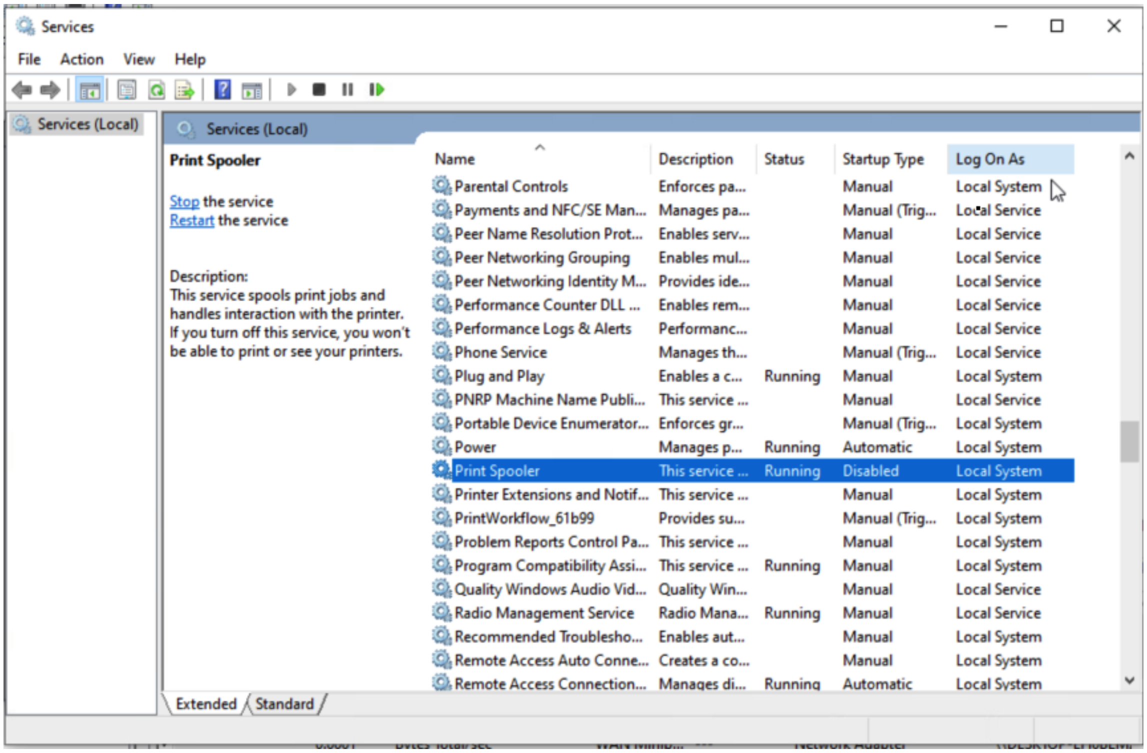
Value name: Start

Value data: 4

Base: ● Hexadecimal ○ Decimal

Name	Type	Data
		(value not set)
	ULTI_SZ	RPCSS http
		@%systemroot%\system32\spoolsv.exe,-2
		@%systemroot%\system32\spoolsv.exe,-1
	WORD	0x00000001 (1)
	NARY	10 0e 00 00 00 00 00 00 00 00 00 00 03 00 00 00 14 00...
		SpoolerGroup
	PAND_SZ	%SystemRoot%\System32\spoolsv.exe
		LocalSystem
	ULTI_SZ	SeTcbPrivilege SeImpersonatePrivilege SeAuditPriv...
ServiceSidType	REG_DWORD	0x00000001 (1)
Start	REG_DWORD	0x00000004 (4)
Type	REG_DWORD	0x00000110 (272)

Figure 2 - Editing the 'Start' DWORD value in the Registry Editor to change the Print Spooler service startup type.



Print Spooler

Stop the service
Restart the service

Description:
This service spools print jobs and handles interaction with the printer. If you turn off this service, you won't be able to print or see your printers.

Name	Description	Status	Startup Type	Log On As
Parental Controls	Enforces pa...		Manual	Local System
Payments and NFC/SE Man...	Manages pa...		Manual (Trig...	Local Service
Peer Name Resolution Prot...	Enables serv...		Manual	Local Service
Peer Networking Grouping	Enables mul...		Manual	Local Service
Peer Networking Identity M...	Provides ide...		Manual	Local Service
Performance Counter DLL ...	Enables rem...		Manual	Local Service
Performance Logs & Alerts	Performanc...		Manual	Local Service
Phone Service	Manages th...		Manual (Trig...	Local Service
Plug and Play	Enables a c...	Running	Manual	Local System
PNRP Machine Name Publi...	This service ...		Manual	Local Service
Portable Device Enumerator...	Enforces gr...		Manual (Trig...	Local System
Power	Manages p...	Running	Automatic	Local System
Print Spooler	This service ...	Running	Disabled	Local System
Printer Extensions and Notif...	This service ...		Manual	Local System
PrintWorkflow_61b99	Provides su...		Manual (Trig...	Local System
Problem Reports Control Pa...	This service ...		Manual	Local System
Program Compatibility Assi...	This service ...	Running	Manual	Local System
Quality Windows Audio Vid...	Quality Win...		Manual	Local Service
Radio Management Service	Radio Mana...	Running	Manual	Local Service
Recommended Troublesho...	Enables aut...		Manual	Local System
Remote Access Auto Conne...	Creates a co...		Manual	Local System
Remote Access Connection...	Manages di...	Running	Automatic	Local System

Figure 3 - Windows Services after modification, showing the Print Spooler service running with the startup type set to 'Disabled'.

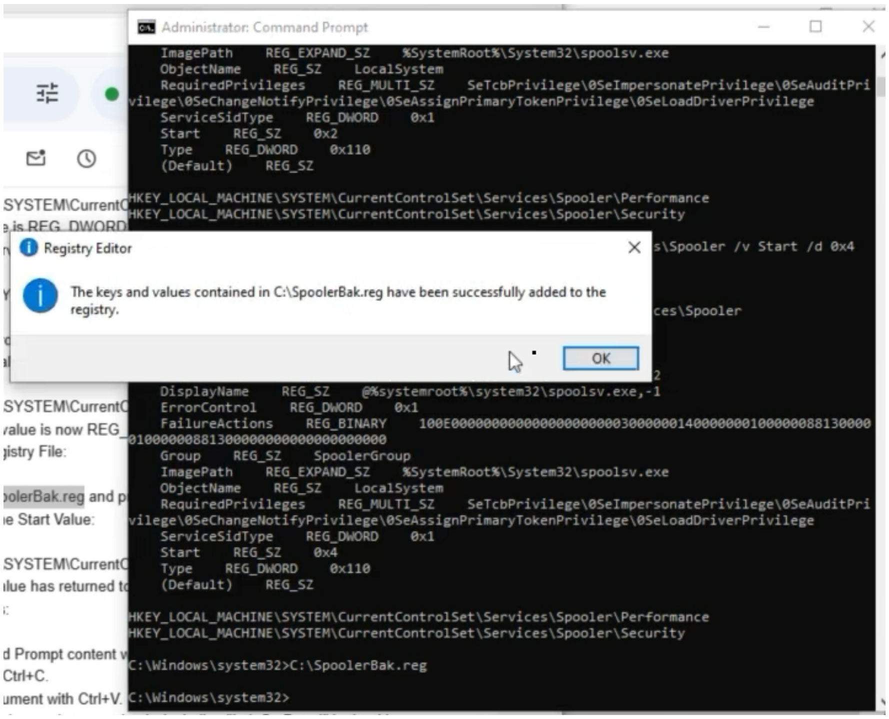
Part 3 - Restoring Registry Settings

Objective: Restore the Print Spooler service startup type from a backup.

Steps and Commands:

1. Double-click the "SpoolerBak.reg" file to merge it back into the registry.

2. Verify the Start value in the Registry Editor.



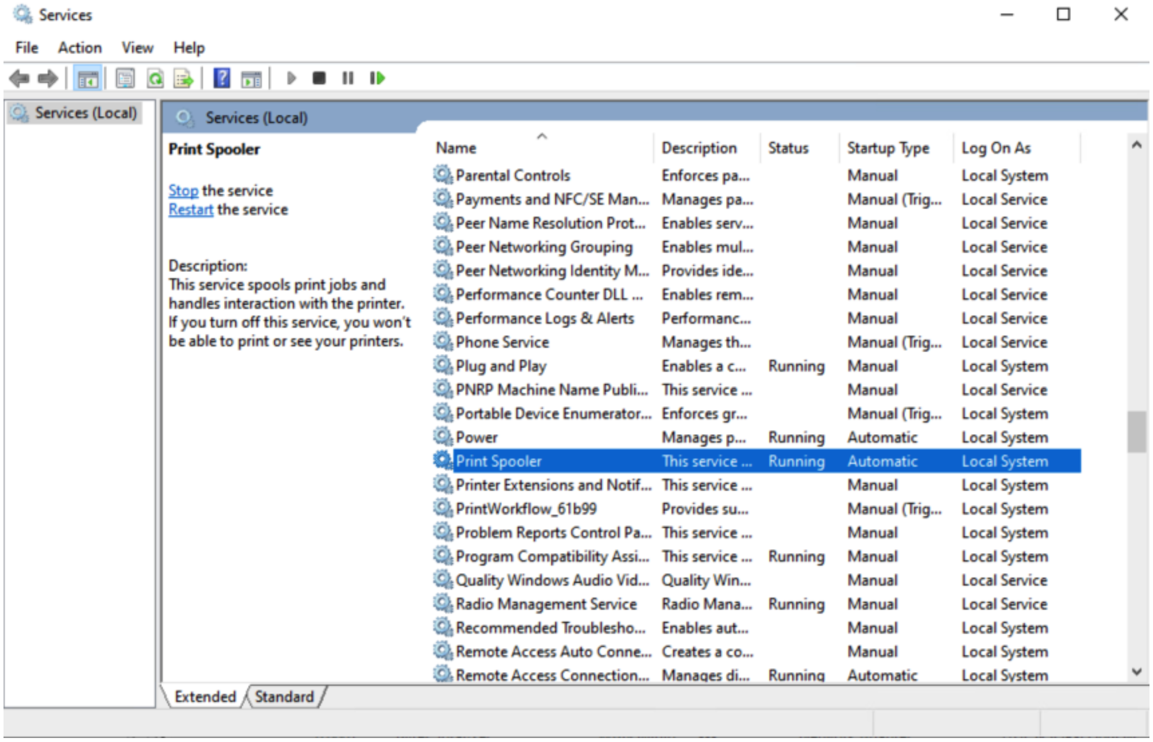
Administrator: Command Prompt

```
    ImagePath    REG_EXPAND_SZ    %SystemRoot%\System32\spoolsv.exe
    ObjectName    REG_SZ    LocalSystem
    RequiredPrivileges    REG_MULTI_SZ    SeTcbPrivilege\0SeImpersonatePrivilege\0SeAuditPri
vilege\0SeChangeNotifyPrivilege\0SeAssignPrimaryTokenPrivilege\0SeLoadDriverPrivilege
    ServiceSidType    REG_DWORD    0x1
    Start    REG_SZ    0x2
    Type    REG_DWORD    0x110
    (Default)    REG_SZ

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler\Performance
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler\Security

s\Spooler /v Start /d 0x4

ces\Spooler

2
    DisplayName    REG_SZ    @%systemroot%\system32\spoolsv.exe,-1
    ErrorControl    REG_DWORD    0x1
    FailureActions    REG_BINARY    100E0000000000000000000003000000140000000100000088130000
01000000881300000000000000000000
    Group    REG_SZ    SpoolerGroup
    ImagePath    REG_EXPAND_SZ    %SystemRoot%\System32\spoolsv.exe
    ObjectName    REG_SZ    LocalSystem
    RequiredPrivileges    REG_MULTI_SZ    SeTcbPrivilege\0SeImpersonatePrivilege\0SeAuditPri
vilege\0SeChangeNotifyPrivilege\0SeAssignPrimaryTokenPrivilege\0SeLoadDriverPrivilege
    ServiceSidType    REG_DWORD    0x1
    Start    REG_SZ    0x4
    Type    REG_DWORD    0x110
    (Default)    REG_SZ

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler\Performance
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler\Security

C:\Windows\system32>C:\SpoolerBak.reg

C:\Windows\system32>
```

Registry Editor

The keys and values contained in C:\SpoolerBak.reg have been successfully added to the registry.

- ○ Use the Find feature to locate the Spooler key and confirm the Start value is 2.



Print Spooler

Stop the service
Restart the service

Description:
This service spools print jobs and handles interaction with the printer. If you turn off this service, you won't be able to print or see your printers.

Name	Description	Status	Startup Type	Log On As
Parental Controls	Enforces pa...		Manual	Local System
Payments and NFC/SE Man...	Manages pa...		Manual (Trig...	Local Service
Peer Name Resolution Prot...	Enables serv...		Manual	Local Service
Peer Networking Grouping	Enables mul...		Manual	Local Service
Peer Networking Identity M...	Provides ide...		Manual	Local Service
Performance Counter DLL ...	Enables rem...		Manual	Local Service
Performance Logs & Alerts	Performanc...		Manual	Local Service
Phone Service	Manages th...		Manual (Trig...	Local Service
Plug and Play	Enables a c...	Running	Manual	Local System
PNRP Machine Name Publi...	This service ...		Manual	Local Service
Portable Device Enumerator...	Enforces gr...		Manual (Trig...	Local System
Power	Manages p...	Running	Automatic	Local System
Print Spooler	This service ...	Running	Automatic	Local System
Printer Extensions and Notif...	This service ...		Manual	Local System
PrintWorkflow_61b99	Provides su...		Manual (Trig...	Local System
Problem Reports Control Pa...	This service ...		Manual	Local System
Program Compatibility Assi...	This service ...	Running	Manual	Local System
Quality Windows Audio Vid...	Quality Win...		Manual	Local Service
Radio Management Service	Radio Mana...	Running	Manual	Local Service
Recommended Troublesho...	Enables aut...		Manual	Local System
Remote Access Auto Conne...	Creates a co...		Manual	Local System
Remote Access Connection...	Manages di...	Running	Automatic	Local System

Figure 4 - Windows Services after modification, showing the Print Spooler service running with the startup type set to 'Automatic'.

Part 4 - Command-line Registry Editing

Objective: Use `reg.exe` to modify the registry from the command line.

Commands:

```
reg query HKLM\SYSTEM\CurrentControlSet\Services\Spooler
reg add HKLM\SYSTEM\CurrentControlSet\Services\Spooler /v Start /d 4
reg query HKLM\SYSTEM\CurrentControlSet\Services\Spooler
reg import C:\SpoolerBak.reg
reg query HKLM\SYSTEM\CurrentControlSet\Services\Spooler
```

Part 5 - PowerShell Registry Editing

Objective: Use PowerShell for registry operations.

Commands:

```
Get-PSDrive
Set-Location HKLM:
Get-ItemProperty . -Name Start
Set-ItemProperty . -Name Start -Value 4
Get-ItemProperty . -Name Start
reg import C:\SpoolerBak.reg
```

Part 6 - File History

Objective: Set up File History and test file version restore.

Steps and Commands:

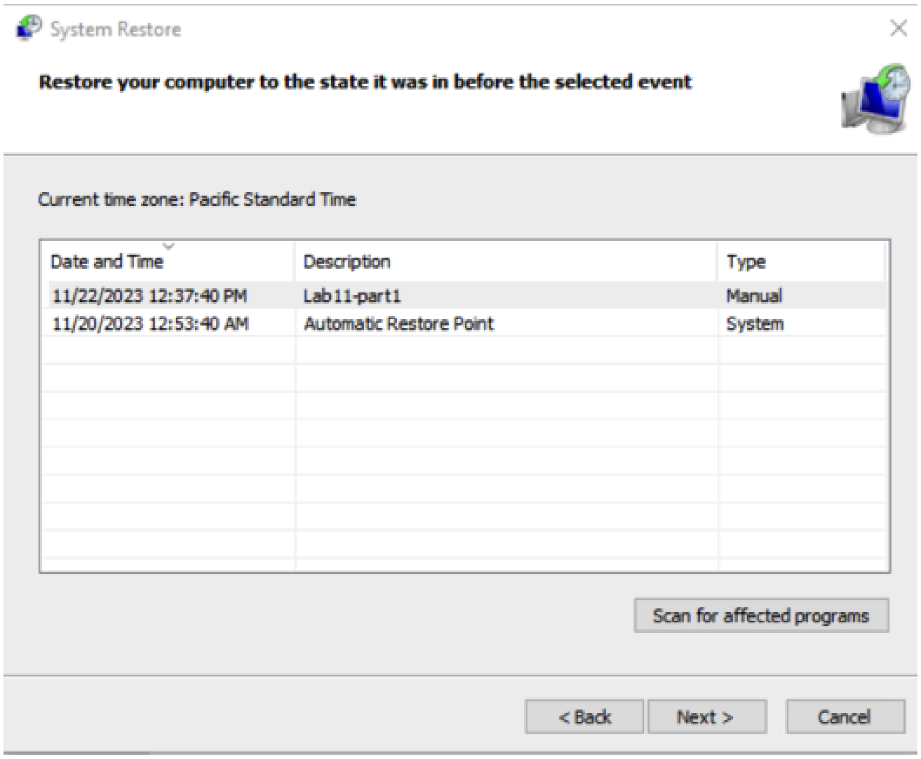
1. Add a new virtual disk and format it for File History.
2. Configure File History settings and run a backup.
3. Edit and backup a "Grocery List" file, then restore a previous version.

Part 7 - System Restore Points

Objective: Roll back the system configuration using a system restore point.

Steps and Commands:

1. Initiate System Restore and select the created restore point.
2. Restart and log in to complete the process.



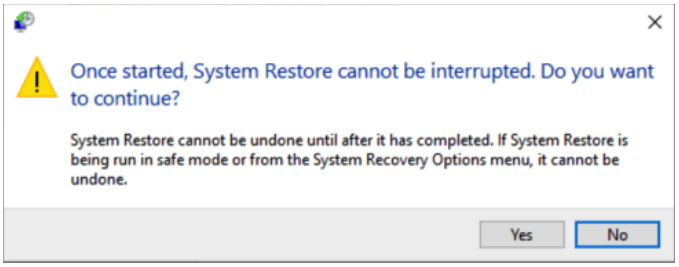
System Restore

Restore your computer to the state it was in before the selected event

Current time zone: Pacific Standard Time

Date and Time	Description	Type
11/22/2023 12:37:40 PM	Lab11-part1	Manual
11/20/2023 12:53:40 AM	Automatic Restore Point	System

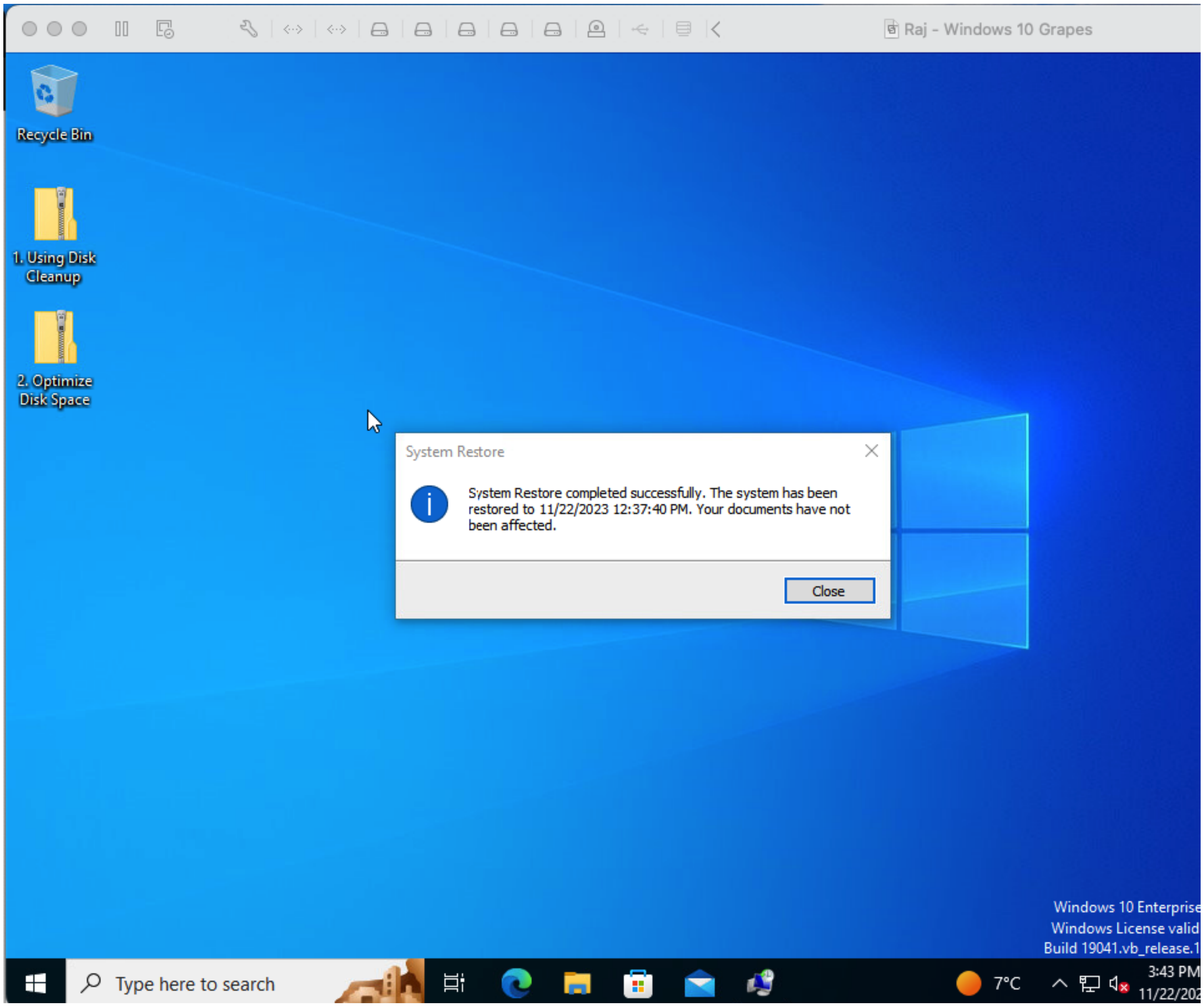
Figure 5 -System Restore window listing available restore points including the manually created restore point.



Once started, System Restore cannot be interrupted. Do you want to continue?

System Restore cannot be undone until after it has completed. If System Restore is being run in safe mode or from the System Recovery Options menu, it cannot be undone.

Figure 5 -System Restore confirmation prompt warning that the process cannot be interrupted once started.



System Restore

System Restore completed successfully. The system has been restored to 11/22/2023 12:37:40 PM. Your documents have not been affected.

Close

Figure 6: Successful System Restore notification indicating the system has been reverted to a previous state without affecting documents.

Conclusion

Reflecting on System Proficiency and Best Practices

Upon the completion of this lab exercise, I've successfully navigated through advanced system administrative tasks that have bolstered my technical proficiency with Windows 10. The documentation has chronicled each step, accompanied by relevant command-line snippets and graphical interface actions, to offer a clear record of the procedures involved.

Key Takeaways:

- Performance monitoring offers real-time insights into system resource utilization, essential for proactive system management.
- Registry editing, while powerful, requires precision and an understanding of the potential impact on system behavior.
- System restore points and File History are invaluable tools in my arsenal for data protection and system recovery.

As this documentation is concluded, I reinforce the importance of systematic documentation, attention to detail, and adherence to best practices when conducting system administration tasks. The knowledge and experience gained here lay a solid foundation for efficient system management and troubleshooting in professional IT environments.