Lab 4 – Patch Validation and Policy Enforcement

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

---

1. Purpose

The purpose of this lab was to verify that Windows Server 2022 is fully patched, confirm that Group Policy security logging settings are applied correctly, enable and validate advanced audit policies, and provide evidence of compliance for security audit requirements.

---

2. Patch Validation

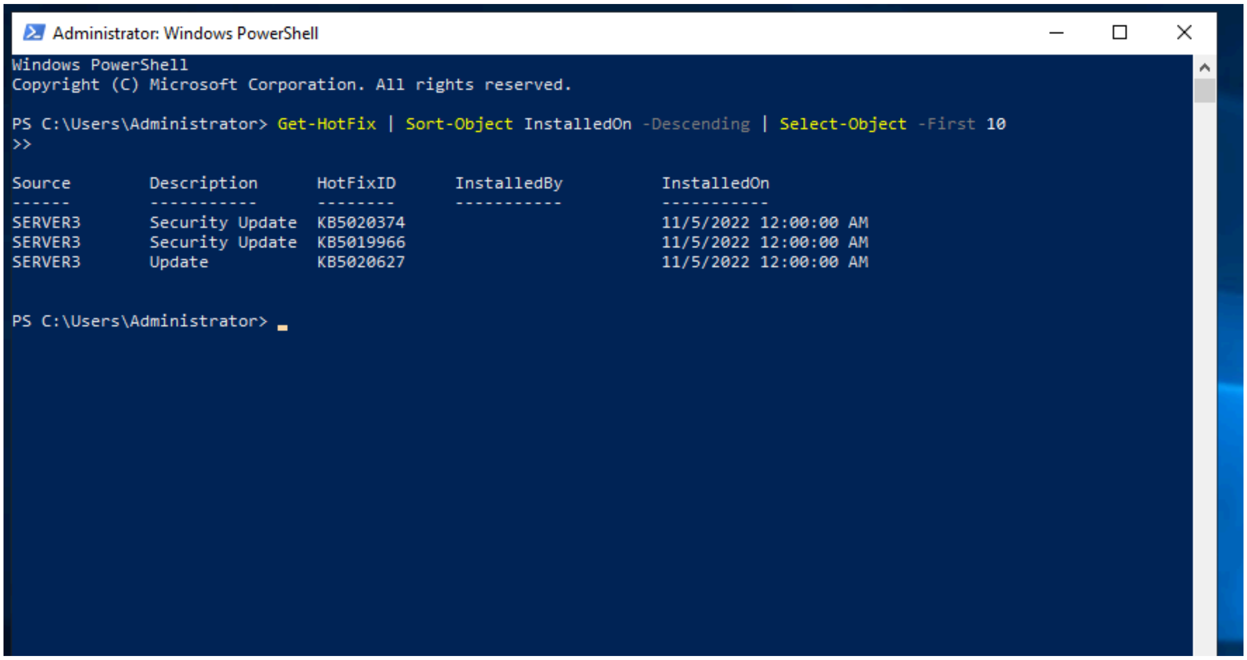
Patch level was verified using PowerShell to list the most recent hotfixes and installed KB updates.

Commands executed:

```
Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object
-First 10
systeminfo | Select-String "KB"
```

These commands confirmed that the server is fully up to date with the latest cumulative and security patches.

Evidence:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 10
>>

Source        Description      HotFixID      InstalledBy          InstalledOn
------        -----------      --------      -----------          -----------
SERVER3       Security Update  KB5020374                          11/5/2022 12:00:00 AM
SERVER3       Security Update  KB5019966                          11/5/2022 12:00:00 AM
SERVER3       Update           KB5020627                          11/5/2022 12:00:00 AM


PS C:\Users\Administrator>
```

---

3. Group Policy Security Settings

Using Group Policy Management, the **Default Domain Policy** was updated with the following settings:

- Security log size: **32,768 KB**
- Application log size: **16,384 KB**

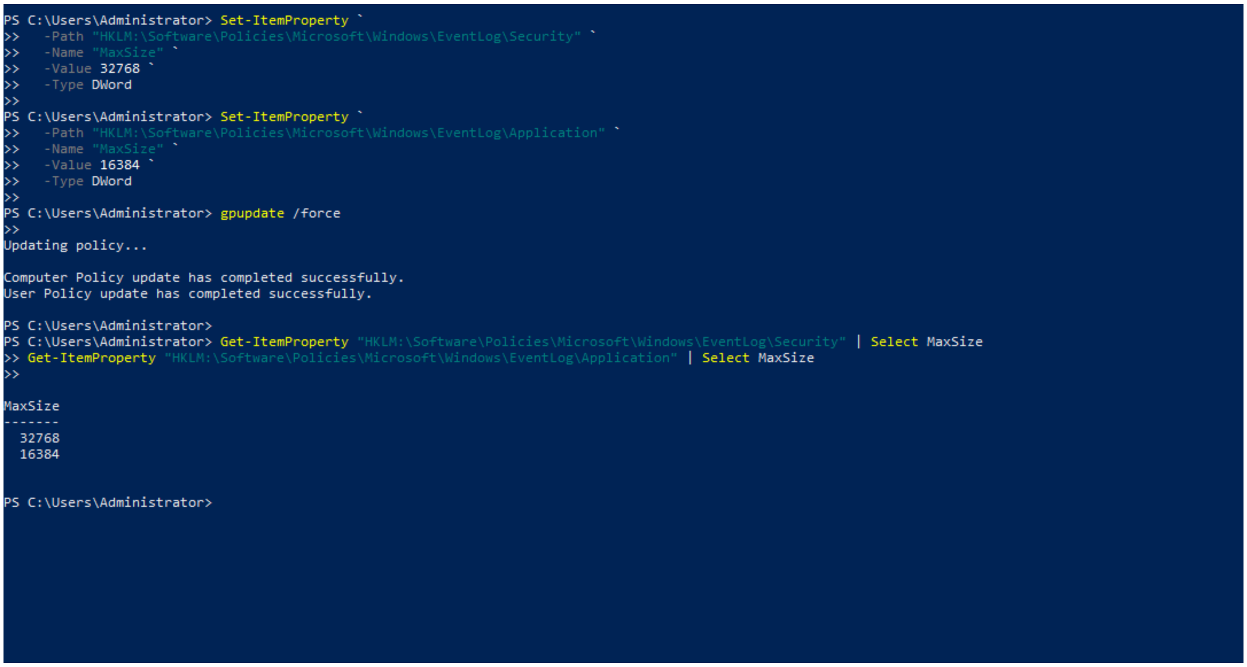
These values match CIS/NIST recommendations for baseline domain logging.

A policy refresh was performed:

```
gpupdate /force
```

Verification was completed by reviewing the Event Log policy registry entries and GPMC settings.

Evidence:



```
PS C:\Users\Administrator> Set-ItemProperty `
>>   -Path "HKLM:\Software\Policies\Microsoft\Windows\EventLog\Security" `
>>   -Name "MaxSize" `
>>   -Value 32768 `
>>   -Type DWord
>>
PS C:\Users\Administrator> Set-ItemProperty `
>>   -Path "HKLM:\Software\Policies\Microsoft\Windows\EventLog\Application" `
>>   -Name "MaxSize" `
>>   -Value 16384 `
>>   -Type DWord
>>
PS C:\Users\Administrator> gpupdate /force
>>
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ItemProperty "HKLM:\Software\Policies\Microsoft\Windows\EventLog\Security" | Select MaxSize
>> Get-ItemProperty "HKLM:\Software\Policies\Microsoft\Windows\EventLog\Application" | Select MaxSize
>>

MaxSize
-------
  32768
  16384


PS C:\Users\Administrator>
```

4. Audit Policy Enforcement

Advanced audit policy settings were enabled using PowerShell:

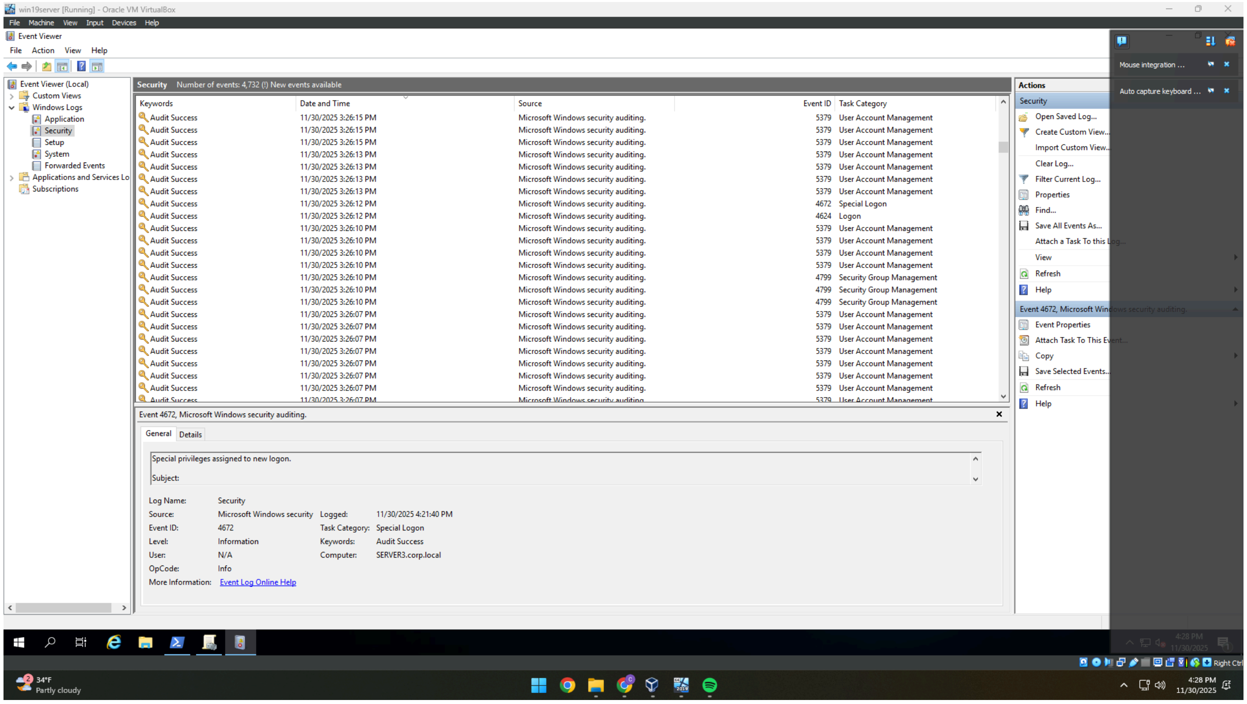
```
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
auditpol /set /subcategory:"User Account Management" /success:enable
/failure:enable
auditpol /set /subcategory:"Security Group Management" /success:enable
auditpol /set /subcategory:"Audit Policy Change" /success:enable
/failure:enable
```

Audit policy results were verified in:

```
auditpol /get /category:*
```

To confirm that auditing was active, the Security event log was reviewed. Log entries for logon events, account changes, and policy changes were visible and confirmed that audit logging is functioning as expected.

Evidence:



Security Number of events: 4,732 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	11/30/2025 3:26:15 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:15 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:15 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:13 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:13 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:13 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:13 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:12 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	11/30/2025 3:26:12 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	11/30/2025 3:26:10 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:10 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:10 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:10 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:10 PM	Microsoft Windows security auditing.	4799	Security Group Management
Audit Success	11/30/2025 3:26:10 PM	Microsoft Windows security auditing.	4799	Security Group Management
Audit Success	11/30/2025 3:26:10 PM	Microsoft Windows security auditing.	4799	Security Group Management
Audit Success	11/30/2025 3:26:07 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:07 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:07 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:07 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:07 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:07 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:07 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	11/30/2025 3:26:07 PM	Microsoft Windows security auditing.	5379	User Account Management

Event 4672, Microsoft Windows security auditing.

General Details

Special privileges assigned to new logon.

Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	11/30/2025 4:21:40 PM
Event ID:	4672	Task Category:	Special Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	SERVER3.corp.local
OpCode:	Info		
More Information:	Event Log Online Help		

5. Results Summary

All required security patches were confirmed installed.
Event Log sizes were configured through Group Policy, and audit policies were properly enabled.
Security log entries validated that the system is capturing logon activity, account management changes, and policy modifications.
These controls ensure visibility into authentication events and configuration changes, supporting incident response and compliance requirements.

6. Reflection

This lab demonstrated the importance of validating patch status and enforcing consistent audit policies across a Windows Server environment. Ensuring that the server is up to date reduces exposure to known vulnerabilities, while proper audit configuration provides essential visibility into authentication and administrative activity. These controls form the foundation of monitoring, forensic investigation, and compliance with organizational security standards.