Resolving and Configuring "Audit MPSSVC Rule-Level Policy Change"

Overview

The task was to configure the **Audit MPSSVC Rule-Level Policy Change** policy using PowerShell, ensure compliance with auditing requirements, and verify the changes. This document includes the steps, troubleshooting, and alternative methods used to solve the issue.

Steps Taken to Resolve the Issue

Step 1: Verify Execution Policy

The initial error indicated that scripts were blocked due to PowerShell's execution policy. To resolve this:

1. Open PowerShell as **Administrator**.

Set the execution policy temporarily:

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
```

2. This allowed scripts to run for the current session only.

Verified the change:

```
Get-ExecutionPolicy -Scope Process
```

3.

Step 2: Configure the Policy Using PowerShell Script

We created a PowerShell script to automate the configuration:

Script Content

```
# Define the subcategory and action
$Subcategory = "MPSSVC Rule-Level Policy Change"
$Actions = @("Success", "Failure")
```

```
# Apply settings for Success and Failure
foreach ($Action in $Actions) {
    Write-Host "Setting $Subcategory - $($Action): Enable"
    try {
        AuditPol /Set /Subcategory:"$Subcategory" /$($Action):Enable
        Write-Host "Successfully set $Action for $Subcategory."
    } catch {
        Write-Host "Error applying $Action for $Subcategory: $_"
    }
}

# Verify the settings
Write-Host "\nVerifying the audit policy settings..."
try {
    $PolicyConfig = AuditPol /Get /Category:"Policy Change"
    Write-Host $PolicyConfig
} catch {
    Write-Host "Error verifying policy settings: $_"
}
```

Steps to Execute

1. Saved the script as `ConfigureMPSSVCPolicy.ps1` in `C:\Users\dellybar\Documents`.

Ran the script:

```
.\ConfigureMPSSVCPolicy.ps1
```

2.

Verified the configuration:

```
AuditPol /Get /Category:"Policy Change"
```

3.

Step 3: Troubleshooting Script Errors

Issue: Execution Policy Block

Error: "File cannot be loaded because running scripts is disabled."

Solution: Temporarily set the execution policy using:

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
```

-

Issue: Invalid Variable Reference

Error: "Variable reference is not valid."

- Solution: Corrected the script by using `$($VariableName)` syntax to handle variable references within strings.

Issue: Subcategory Name Not Found

Error: "Error 0x00000057."

Solution: Verified available subcategories using:

```
AuditPol /List /Subcategories
```

- Ensured the correct subcategory name: **"MPSSVC Rule-Level Policy Change"**.

Step 4: Verification Using `AuditPol`

Verified the configuration with the command:

```
AuditPol /Get /Category:"Policy Change"
```

Expected Output:

```
MPSSVC Rule-Level Policy Change
  Success : Enabled
  Failure : Enabled
```

Step 5: Python Alternative

As an alternative, a Python script was provided to set registry values if required. The script used the `winreg` module to make changes to the Windows Registry.

Python Script

```
import winreg as reg
```

```
def set_registry_value(key_path, value_name, value):
    try:
        key = reg.CreateKeyEx(reg.HKEY_LOCAL_MACHINE, key_path, 0, reg.KEY_WRITE)
        reg.SetValueEx(key, value_name, 0, reg.REG_DWORD, value)
        reg.CloseKey(key)
        print(f"Successfully set {value_name} to {value} in {key_path}.")
    except PermissionError:
        print("Error: Please run the script as Administrator.")
    except Exception as e:
        print(f"An error occurred: {e}")

# Example Usage
key_path = r"Software\Policies\Microsoft\Windows\WinRM\Service"
value_name = "AllowBasic"
value = 0  # Disable Basic Authentication
set_registry_value(key_path, value_name, value)
```

Final Steps

1. Verified the policy configuration using `AuditPol`.
2. Documented all changes for compliance and future reference.
3. Ensured scripts were run as Administrator.

Notes

- Ensure you use Administrator privileges for all steps.
- Use `gpupdate /force` to enforce Group Policy changes immediately.
- If errors persist, validate the environment using tools like **Event Viewer** or compliance scanners.

Conclusion

The policy "Audit MPSSVC Rule-Level Policy Change" was successfully configured and verified. This document can be used as a reference for similar configurations in the future.