User Manual: Detecting Windows Event Log Clears via WMI

Overview

This manual guides you through setting up a persistent WMI subscription to detect when Windows event logs are cleared (Event ID 104 for System/Application logs and 1102 for Security logs). When an event log is cleared, an alert is written to a log file, and optionally, the alert can be sent to a SIEM like Splunk.

Requirements

- Windows 10 / Windows Server (Admin access required)
- PowerShell 5.x or 7.x
- Optional: Splunk HTTP Event Collector (HEC) for forwarding
- File paths: `C:\WMI_Alerts\` (logs and helper script stored here)

Step 1: Prepare the Helper Script

1. Open PowerShell or VS Code as Administrator.
2. Create a directory for alerts:

```
New-Item -ItemType Directory -Path C:\WMI_Alerts -Force
```

3. Create the helper script `WriteEventAlert.ps1`:

C:_Alerts.ps1

```
# Ensure log directory exists
$LogFile = "C:\WMI_Alerts\EventLogCleared.log"
New-Item -ItemType Directory -Path (Split-Path $LogFile) -Force | Out-Null

# Write alert
$time = Get-Date -Format 'yyyy-MM-dd HH:mm:ss'
$msg = "[ALERT] Event Log Cleared | Time=$time | Host=$env:COMPUTERNAME"
Add-Content -Path $LogFile -Value $msg
```

Step 2: Prepare the Main WMI Script

1. Open VS Code or PowerShell ISE as Administrator.

2. Save the following script as `Detect-EventLogClear-WMI.ps1` on your Desktop:

C:-EventLogClear-WMI.ps1

```
# ================================
# CONFIGURATION
# ================================
$Name = "Detect_EventLog_Clear_104"
$ScriptPath = "C:\WMI_Alerts\WriteEventAlert.ps1"
$PSExe = "$env:SystemRoot\System32\WindowsPowerShell\v1.0\powershell.exe"

# ================================
# CLEAN EXISTING SUBSCRIPTION
# ================================
Get-WmiObject -Namespace root\subscription -Class __EventFilter |
    Where-Object Name -eq $Name | Remove-WmiObject -ErrorAction
SilentlyContinue

Get-WmiObject -Namespace root\subscription -Class CommandLineEventConsumer |
    Where-Object Name -eq $Name | Remove-WmiObject -ErrorAction
SilentlyContinue

Get-WmiObject -Namespace root\subscription -Class __FilterToConsumerBinding |
    Remove-WmiObject -ErrorAction SilentlyContinue

# ================================
# EVENT FILTER (Event IDs 104 + 1102)
# ================================
$Query = @"
SELECT * FROM __InstanceCreationEvent
WITHIN 5
WHERE TargetInstance ISA 'Win32_NTLogEvent'
AND (TargetInstance.EventCode = '104' OR TargetInstance.EventCode = '1102')
"@

$Filter = Set-WmiInstance -Namespace root\subscription -Class __EventFilter -
Arguments @{
    Name           = $Name
    EventNamespace = "root\cimv2"
    QueryLanguage  = "WQL"
    Query          = $Query
}

# ================================
# EVENT CONSUMER (use helper script)
# ================================
$CommandLine = "$PSExe -NoProfile -ExecutionPolicy Bypass -File
`"$ScriptPath`""
```

```
$Consumer = Set-WmiInstance -Namespace root\subscription -Class
CommandLineEventConsumer -Arguments @{
    Name = $Name
    CommandLineTemplate = $CommandLine
    RunInteractively = $false
}

# ================================
# BIND FILTER TO CONSUMER
# ================================
Set-WmiInstance -Namespace root\subscription -Class __FilterToConsumerBinding
-Arguments @{
    Filter   = $Filter.__PATH
    Consumer = $Consumer.__PATH
}

Write-Host "[OK] WMI Persistent Subscription CREATED" -ForegroundColor Green
```

Step 3: Set Execution Policy and Run Script

1. Open PowerShell as Administrator
2. Allow scripts to run temporarily:

```
Set-ExecutionPolicy -Scope Process Bypass
```

3. Navigate to the script directory:

```
cd C:\Users\YourUser\Desktop
```

4. Run the main WMI script:

```
.\Detect-EventLogClear-WMI.ps1
```

You should see: `[OK] WMI Persistent Subscription CREATED`

Step 4: Test the Detection

1. Clear event logs to trigger detection:

```
wevtutil cl System
wevtutil cl Application
wevtutil cl Security
```

2. Wait 5–10 seconds.
3. Check alert log:

```
Get-Content C:\WMI_Alerts\EventLogCleared.log
```

Expected output:

```
[ALERT] Event Log Cleared | Time=2026-01-02 18:23:09 | Host=MOHIT
[ALERT] Event Log Cleared | Time=2026-01-02 18:23:20 | Host=MOHIT
```

Summary

Step	Action
1	Create helper script `WriteEventAlert.ps1`
2	Create main WMI script `Detect-EventLogClear-WMI.ps1`
3	Run script as Administrator
4	Trigger events using `wevtutil cl`

This manual allows anyone to set up a working WMI-based event log clearing detection lab from scratch.