Windows Logging

Introduction

Message Capture

Log Analysis

SNMP

Netflow

SNMP Traps

Proxy Services

Unified Threat Management

Authentication

Network Discovery

Monitoring and Log Management

Windows Logging

- Windows includes an event logging component
- Windows components and applications can use this feature to allow the OS to record messages that those programs decide might be of interest
- IT professionals and software developers are the primary users of the contents of the event logs via programs that can read them and provide a view of them
- They are not directly searched or viewed under normal circumstances

Purpose of Windows Event Log

- System Monitoring and Maintenance
- Troubleshooting and Diagnostics
- Security and Auditing
- Compliance and Reporting
- Forensics and Incident Response

How the Windows Event Log is Used

- Event Categories and Types

  System, Application, Security, Setup, Forwarded

- Viewing and Analyzing Logs

  Event Viewer, log scrapers

- Setting Up Alerts and Monitoring

  Event Viewer, SIEM tools

- Audit Policies and Log Retention

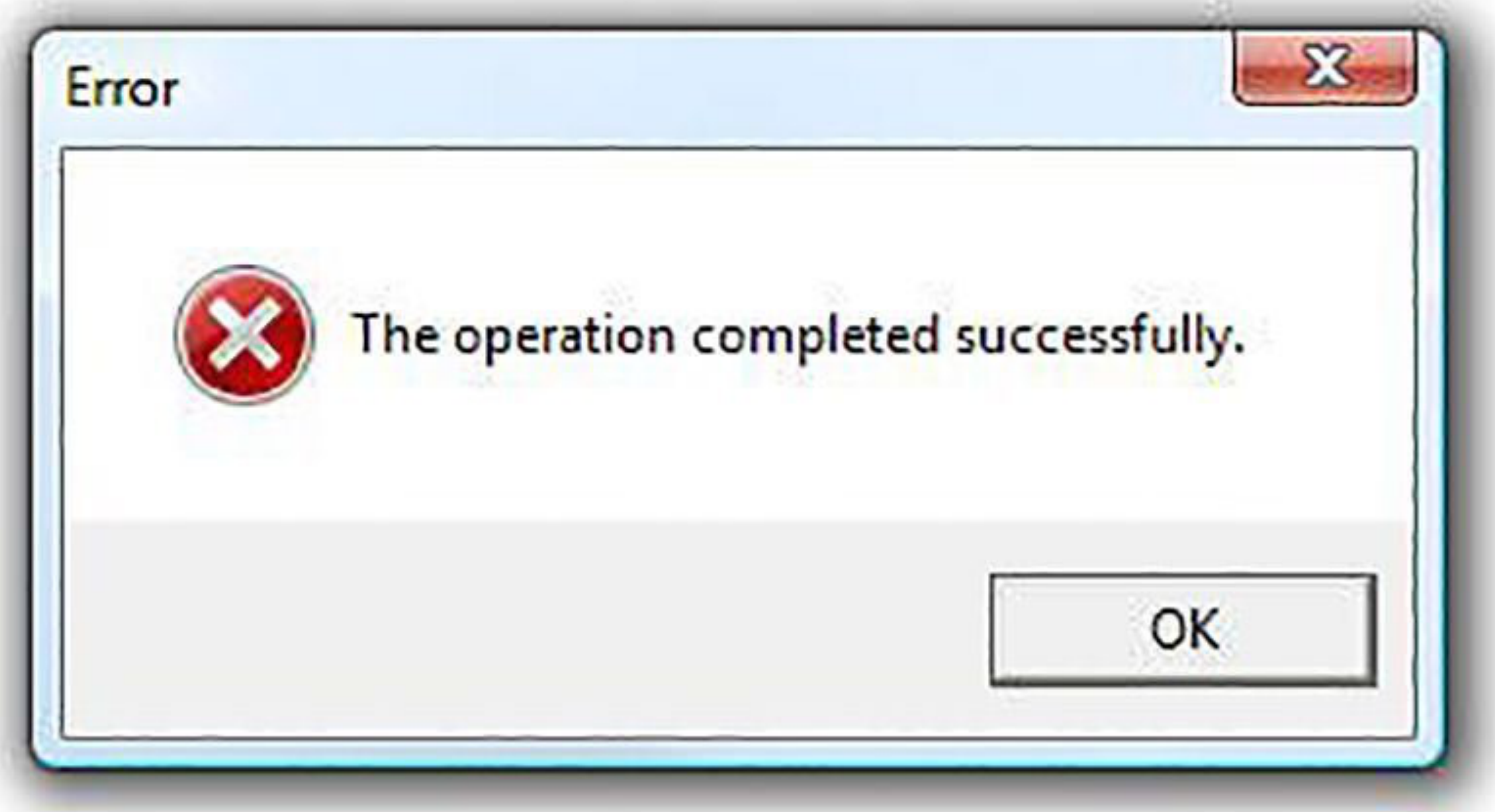
  Group Policy

Common Use Cases of Windows Event Log

- Troubleshooting Issues
- Security Monitoring
- Performance Monitoring
- Audit and Compliance

Windows Realities
Have you tried turning it off and on?

- Windows exhibits non-deterministic behaviour frequently, as do many popular Windows applications
- Windows has a heritage of existing to load programs and not taking responsibility for whether they work predictably
- Any user of Windows systems has learned quickly that when something doesn't produce a desired result, they should just do it again because that works more frequently than you would think
- The ultimate outcome of this practice is accepting that when things are not working, often the quickest way past the problem is to just start over from a fresh boot



The operation completed successfully.

Eventlog Implementation

- Windows creates incredible volumes of log messages - most are not useful because they're incredibly verbose while leaving out actual auditing details that would make most of them useful

- Windows components and applications store logs in plain text log files (.log) scattered all over the system

- Windows eventlog stores logs in XML files (.evtx) by default kept in C:\Windows\System32\winevt\Logs\ in Microsoft-proprietary formats implemented to support categorization and filtering in EventViewer

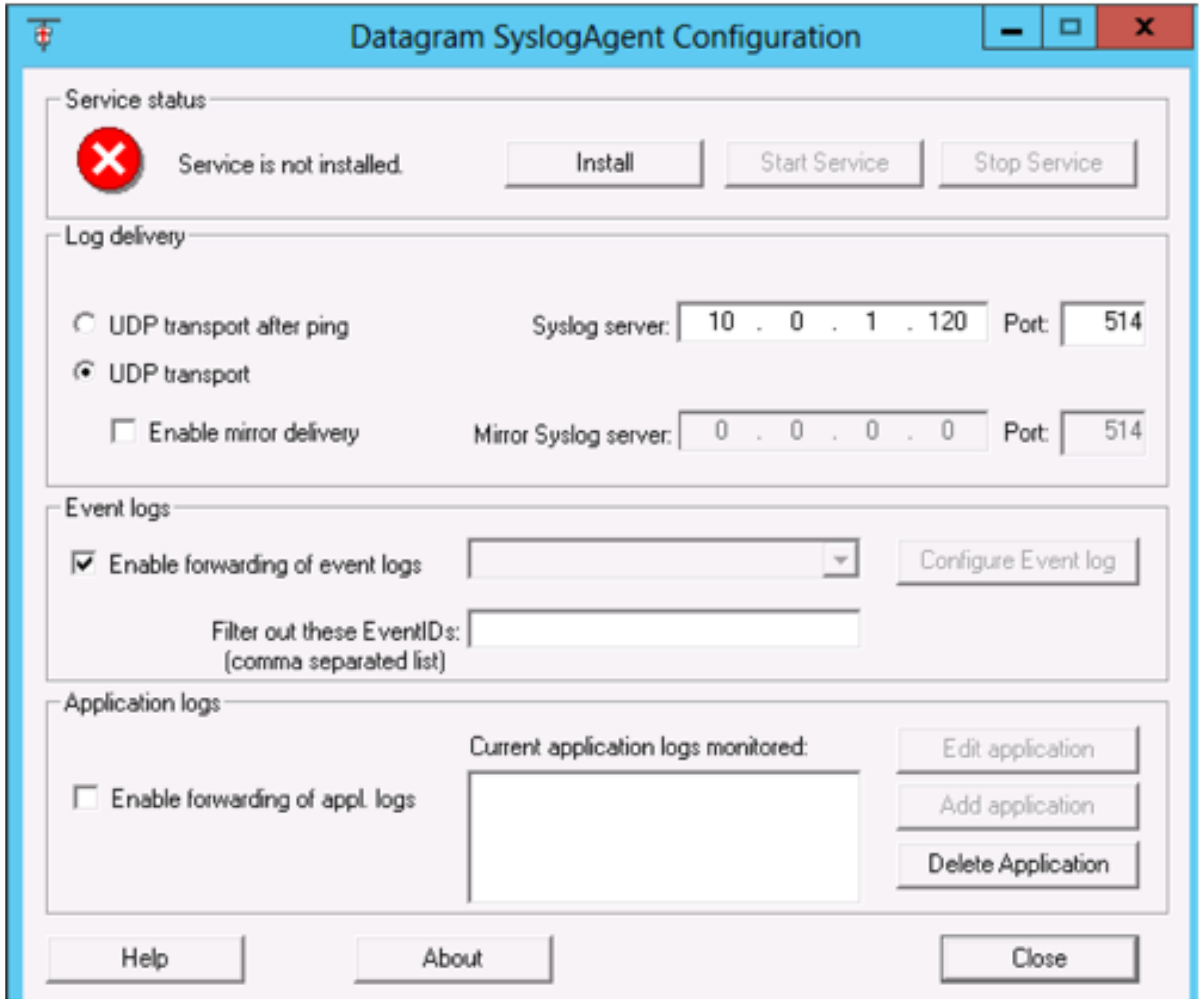
- Some programs write event log entries to files in program-specific formats as well as sending them to the Windows event log

Eventlog Management

- EventViewer can clear the logs, or export them to files which can be read by EventViewer
- Windows eventlog supports centralized eventlogs in certain Microsoft-only environments using winrm - see Loggly's Ultimate Guide To Logging
- 3rd party agent programs can be installed to monitor eventlog files and send entries to any of the major log management software platforms
- Log locations, sizes, retention rules, and preservation are managed using the group policy editor and are found under Computer Configuration -> Administrative Templates -> Windows Components -> Event Log Service - see Understanding the Windows Server Event Log

Windows Event Logs

Integrating With Syslog



Datagram SyslogAgent Configuration

Service status

Service is not installed.

Log delivery

○ UDP transport after ping

● UDP transport

□ Enable mirror delivery

Syslog server: 10 . 0 . 1 . 120 Port: 514

Mirror Syslog server: 0 . 0 . 0 . 0 Port: 514

Event logs

☑ Enable forwarding of event logs

Filter out these EventIDs: (comma separated list)

Application logs

□ Enable forwarding of appl. logs

Current application logs monitored:

- Windows has a Microsoft-specific logging approach and toolset which is incompatible with other logging implementations
- Windows event logs can be centralized but it takes some work and the results may not live up to the expectations
- Various solutions are available to send Windows event logs to a syslog server, they involve a service watching the Windows log files and sending new entries to syslog
- rsyslog.com has a windows agent, datagram syslogagent has been popular, correlog.com has a free agent, newer monitoring systems use tools like beats to feed elasticsearch logging systems and are greatly more useful than polluting syslog services with Windows eventlogs

Incident Response Use of Eventlog

- Knowing when to examine Windows logs due to a security incident involves recognizing signs that indicate potential threats or suspicious activities.
- Key indicators that might prompt you to investigate:
- Unusual Login Activity
- Unexpected System Changes
- File and Folder Access Anomalies
- Suspicious Network Activity
- Unauthorized Use of Administrative Privileges
- Antivirus or Endpoint Protection Alerts
- System Crashes or Reboots
- Changes in Log Settings
- New User Accounts or Services
- Unusual Application Activity

Indicator: Unusual Login Activity

- Unusual Login Activity:
  - Multiple failed login attempts in a short period.
  - Successful logins from unusual locations or during odd hours.
  - Logins using disabled or expired accounts.
  - Logins from accounts that don’t typically access certain systems.
- Logs to check: Security logs (Event ID 4624 for logins, 4625 for failed attempts, and 4776 for NTLM authentication).

Indicator: Unexpected System Changes

- Unexpected System Changes:
  - Unauthorized changes to user permissions or group memberships.
  - Installation or removal of software without prior notice.
  - Modifications to system configurations or registry settings.
- Logs to check: Security logs (Event IDs 4732/4733 for group changes, 4670 for permissions changes)

Indicator: File and Folder Access Anomalies

- File and Folder Access Anomalies:
    - Large numbers of file modifications, deletions, or accesses.
    - Access to sensitive or confidential files by users who shouldn’t have access.
    - Unusual creation or execution of new files or scripts.
- Logs to check: Object Access logs (Event IDs 4663 for file access, 4660 for deletions)

Indicator: Suspicious Network Activity

- Suspicious Network Activity:
  - Unexpected outbound connections, especially to unknown IP addresses.
  - Large data transfers, indicating possible data exfiltration.
  - Port scanning or unusual communication patterns.
- Logs to check: Firewall logs, Event ID 5156 for successful connections

Indicator: Unauthorized Use of Administrative Privileges

- Unauthorized Use of Administrative Privileges:
  - Users elevating their privileges without proper authorization.
  - Execution of PowerShell or other command-line tools by non-administrators.
- Logs to check: Security logs (Event ID 4672 for special privilege use, 4688 for process creation), PowerShell logs

Indicator: Antivirus or Endpoint Protection Alerts

- Antivirus or Endpoint Protection Alerts:
  - Alerts about detected malware or potentially unwanted programs.
  - Alerts about disabled or tampered security software.
- Logs to check: Application logs, Endpoint security solution logs
- These may not be found in any Windows log, but may be visible only in the UI of the tool that found the problem

Indicator: System Crashes or Reboots

- System Crashes or Reboots:
  - Unexpected system reboots or shutdowns.
  - Blue screen events or other critical errors.
- Logs to check: System logs (Event ID 6008 for unexpected shutdowns)

Indicator: Changes in Log Settings

- Changes in Log Settings:
  - Audit policy changes, such as disabling logging or clearing log files.
  - Frequent or complete log deletions.
- Logs to check: Security logs (Event ID 1102 for log clearance, 4719 for audit policy changes)

Indicator: New User Accounts or Services

- New User Accounts or Services:
  - Creation of new user accounts, especially with administrative privileges.
  - Installation of new services that weren’t authorized or expected.
- Logs to check: Security logs (Event ID 4720 for new accounts, 7045 for service installations)

Indicator: Unusual Application Activity

- Unusual Application Activity:
  - Execution of programs or scripts that are uncommon or suspicious.
  - Programs communicating with the internet unexpectedly.
- Logs to check: Application logs, PowerShell logs, and Process Tracking (Event ID 4688)

Best Practices

- Regularly monitor logs with a Security Information and Event Management (SIEM) tool
- Set up alerts for high-priority events to receive immediate notifications
- Maintain baselines of normal activity to help distinguish between legitimate and malicious actions

Software can be chaotic, but we make it work
Expert
Trying Stuff Until it Works
O RLY?
The Practical Developer
@ThePracticalDev

Windows Logging Lab

- Examine existing event logs
- Locate and examine event logs which are not evtx files
- Summarize the presence or absence of the eventlog indicators on your system