Digital Forensics

- Things to consider
  - NTP - Enable Network Time Protocol for all devices
  - Ensure Windows Client synchronized with AD
  - Decide on GMT offset or a consistent time zone across organization
  - Establish central logging capability
  - Out of band notification capability, can't be monitor by an insider or attacker

- Things to avoid
  - Don't shutdown until you've completed evidence collection
  - Attacker may have altered the startup/shutdown scripts/services to destroy evidence.
  - Run your evidence gathering programs from appropriately protected media
  - Don't run programs that modify the access time of all files on the system (e.g., 'tar' or 'xcopy')
  - Simply disconnecting or filtering from the network may trigger wiping of evidence

Server Event Logs

- Windows Event Viewer
  - logs application and system messages
  - errors, information messages, and warnings
  - Events are placed in different categories
    - Application: events related to Windows system components, such as drivers and built-in interface elements.
    - System: events related to programs installed on the system.
    - Security: When security logging is enabled (it's off by default in Windows), this log records events related to security, such as logon attempts and resource access.
- Windows Event ID
  - Define the uniquely identifiable events that a Windows computer can encounter
  - When the audit log was cleared, the system generate event 1102
  - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

- Windows Event ID
  - Services Events
    - Analyze logs for suspicious services running at boot time
    - Review services started or stopped around the time of a suspected compromise
      - 7034 – Service crashed unexpectedly
      - 7035 – Service sent a Start/Stop control
      - 7036 – Service started or stopped
      - 7040 – Start type changed (Boot | On Request | Disabled)
      - 7045 – A service was installed on the system (Win2008R2+)
      - 4697 – A service was installed on the system (from Security log)

- Windows Event ID
  - Account Authentication Events
    - 4776: Successful/Failed account authentication Event ID Codes (Kerberos protocol)
    - 4768: Ticket Granting Ticket was granted (successful logon)
    - 4769: Service Ticket requested (access to server resource)
    - 4771: Pre-authentication failed (failed logon)

- Windows Event ID
  - Success/Fail Logons
    - 4624 – Successful Logon
    - 4625 – Failed Logon
    - 4634 | 4647 – Successful Logoff
    - 4648 – Logon using explicit credentials (Runas)
    - 4672 – Account logon with superuser rights (Administrator)
    - 4720 – An account was created

- Windows Event ID
  - Logon details
    - Nature of account authorizations on a system
    - Date
    - Time
    - Username
    - Hostname
    - Success/failure status of a logon
    - Logon Events also enables us determine by exactly what means a logon was attempted

- Windows Event ID
    - Logon Types
        - Event ID 4624
            - 2 Logon via console
            - 3 Network Logon
            - 4 Batch Logon
            - 5 Windows Service Logon
            - 7 Credentials used to unlock screen
            - 8 Network logon sending credentials (cleartext)
            - 9 Different credentials used than logged on user
            - 10 Remote interactive logon (RDP)
            - 11 Cached credentials used to logon
            - 12 Cached remote interactive (similar to Type 10)
            - 13 Cached unlock (similar to Type 7)

- Tracking Remote Desktop Activity
    - RemoteDesktopServices-RdpCoreTS > Operational
        - Event ID 131
            - The server accepted a new TCP/UDP connection from client
    - TerminalServices-LocalSessionManager > Operational
        - Event ID 21
            - Remote Desktop Services: Session logon succeeded
            - User
            - Session ID
            - Source Network Address
    - TerminalServices-RemoteConnectionManager > Operational
        - Event ID 1149
            - Remote Desktop Services: User authentication succeeded
            - User
            - Domain
            - Source Network Address

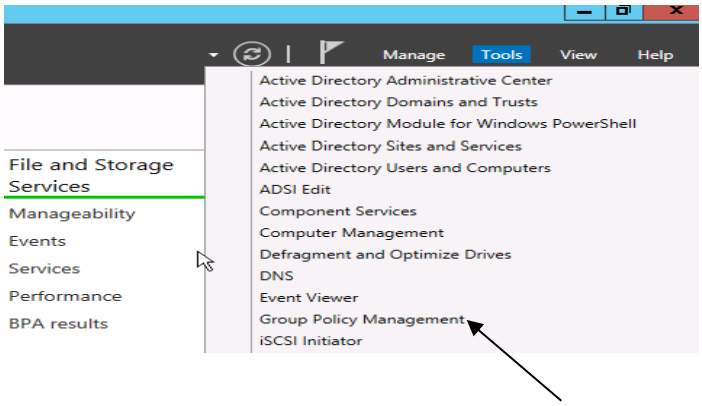
Requirements for Event Viewer logs for Server and local network devices

*The following Group Policies must be enabled

RETAIN SECURITY EVENT LOG FOR 90 DAYS GROUP POLICY

1. Launch **Server Manager**.

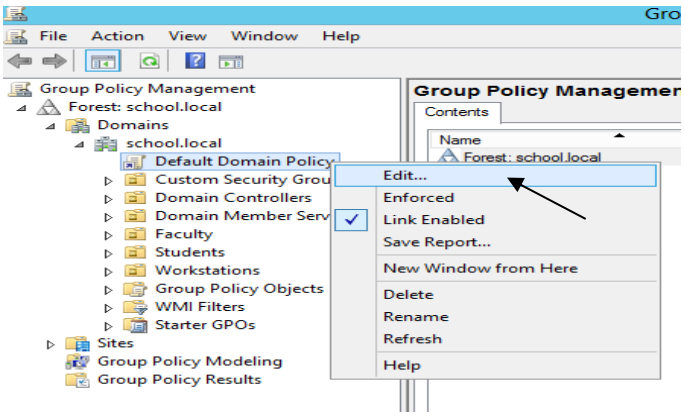
2. Click on **Tools** and select **Group Policy Management** from the drop-down list.



3. Expand Forest: **yourdomain.local.**

4. Expand **Domains** and then expand **yourdomain.local** and navigate to **Default Domain Policy**.

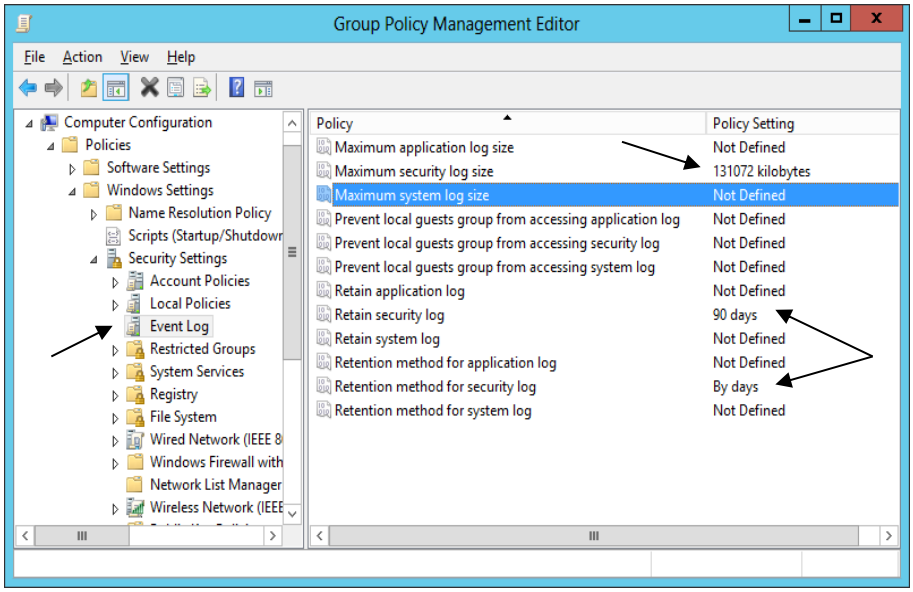
5. Right-click the **Default Domain Policy** and click **Edit**.



6. Expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** and select **Event Log.**

7. Set the policy setting **Retain Security Log** to **90** days. You will automatically prompted to change the **Retention method to days**. Click **OK.**

8. Set the Maximum-Security Log Size to 131072 kilobytes (128MB).



AUTO-BACKUP AND CLEAR EVENT LOGS (AT LEAST WINDOWS VISTA)

9. Expand **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Components** > **Event Log Service** and select **Security**.

10. Enable the **Backup log automatically when full** setting.

11. Close the **Group Policy Management Editor.**

SECURITY EVENT AUDITING – SECURITY EVENT LOG CONTENTS

1. Launch **Server Manager**.

2. Click on **Tools** and select **Group Policy Management** from the drop down list.

3. Expand Forest: **yourdomain.local.**

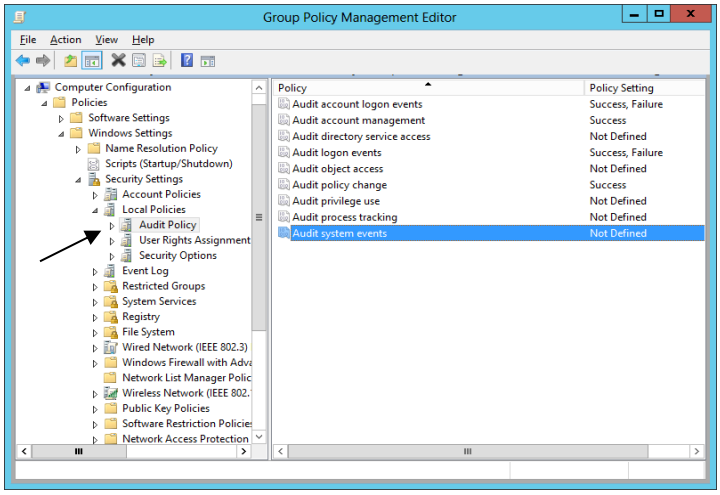
4. Expand **Domains** and then expand **yourdomain.local** and navigate to **Default Domain Policy**.

5. Right-click the **Default Domain Policy** and click **Edit**.

6. Expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** and select **Audit Policy.**

7. Enable auditing for the following Policy Settings:

    a. Audit Account Logon Events – (Success AND Failure)
    b. Audit Account Management – (Success)
    c. Audit logon event – (Success AND Failure)
    d. Audit policy change – (Success)



8. Close the **Group Policy Management Editor.**