جمهوری اسلامی ایران
ریاست جمهوری

مرکز مدیریت راهبردی افتا

راهنمای عملی فعال سازی و مدیریت لاگ های امنیتی در ویندوز

نسخه ۰.۴ – آبان ۱۴۰۴

عادی

فهرست مطالب

مقدمه

در سیستم عامل ویندوز، لاگ‌ها یکی از مهمترین منابع برای پایش امنیتی و تحلیل فارنزیک به شمار می‌آیند. این لاگ‌ها می‌توانند اطلاعات حیاتی در مورد ورود و خروج کاربران، اجرای دستورات، تغییرات در سیاست‌های امنیتی، دسترسی به فایل‌ها و حتی فعالیت‌های مخرب مهاجمان را در اختیار تیم امنیتی قرار دهند.

با این حال، ویندوز به صورت پیش‌فرض فضای کمی برای نگهداری لاگ‌ها در نظر گرفته و لاگ‌های حسابرسی (Audit) نیز غیرفعال هستند، همین موضوع باعث می‌گردد که در زمان وقوع حادثه، بخش زیادی از اطلاعات مهم از دست رفته باشد. به همین دلیل، در این مستند به صورت مرحله به مرحله موارد زیر را بررسی خواهیم کرد.

- افزایش حجم لاگ‌ها برای جلوگیری از پاک شدن سریع رویدادها.
- فعال کردن لاگ‌های PowerShell
- پیکربندی حسابرسی پیشرفته (Advanced Audit Policy Configuration) جهت ثبت رخدادهای حیاتی در سیستم.
- فعال‌سازی Command Line Auditing برای مشاهده خط‌فرمان مربوط به اجرای فرآیند در لاگ.
- توضیح تفاوت Basic Audit Policy و Advanced Audit Policy Configuration و رفع مشکل تداخل آنها، جهت اطمینان از اجرای سیاست‌های پیشرفته.

این تنظیمات پایه‌ای اما حیاتی، به مدیران سیستم و کارشناسان امنیت کمک می‌کند تا دید کاملتری نسبت به فعالیت‌های ویندوز داشته باشند و در صورت بروز رخداد امنیتی، بتوانند با استناد به لاگ‌های دقیق و کامل، تحلیل و پاسخ مناسبی ارائه دهند.

بهترین سناریو برای پایش و ثبت رویدادهای امنیتی در ویندوز، استفاده ترکیبی از قابلیت‌های بومی ویندوز (مانند Advanced Audit Policy) و ابزارهای تکمیلی مانند Sysmon (System Monitor از مجموعه Sysinternals مایکروسافت) است.

لاگ‌های ویندوز همراه با پیکربندی دقیق Audit Policy، امکان ثبت رویدادهای حیاتی مانند ورود و خروج کاربران، تغییرات حساب‌های کاربری، تغییرات در سیاست‌های امنیتی و رخدادهای سیستمی را فراهم می‌سازند. در مقابل، Sysmon جزئیات بسیار بیشتری از فعالیت‌های سیستم مانند ایجاد پردازش‌ها، هش فایل‌های اجرایی، ارتباطات شبکه، تغییرات رجیستری و بارگذاری DLLها را ثبت می‌نماید که برای تهدیدیابی[1] و تحلیل حملات پیشرفته بسیار ارزشمند است.

با این وجود، روشی که در این مستند تشریح شده است بر پایه‌ی قابلیت‌های داخلی ویندوز و Group Policy بنا شده و بعنوان یک روش پایه‌ای، ساده‌تر و قابل مدیریت‌تر در سطح سازمانی مطرح است و هدف آن فعال‌سازی حداقل لاگ‌های لازم در

[1] Threat Hunting

بحث امنیت می‌باشد. پیشنهاد حرفه‌ای‌تر استفاده ترکیبی از امکانات بومی ویندوز بهمراه Sysmon است. در انتها سازمان‌ها بایستی مکانیزمی برای انتقال لاگ‌ها به یک SIEM ایجاد نمایند تا دید جامع‌تر و جزئی‌تری از فعالیت‌ها به دست آورند.

افزایش حجم لاگ‌ها

در ویندوز معمولا برای انجام هر تنظیم چندین روش مختلف وجود دارد بعنوان مثال می‌توان حجم لاگ‌ها را از طریق Event Viewer، Registry یا PowerShell تغییر داد. با این حال، در محیط‌های سازمانی معمولا نیاز است این تغییرات بصورت متمرکز و از طریق دامنه روی همه سیستم‌ها اعمال شوند به همین دلیل در این مستند سعی شده است که تغییرات از طریق Group Policy اعمال گردند.

ویندوز به صورت پیش‌فرض حجم کمی برای نگهداری لاگ‌ها در نظر گرفته است (مثلا لاگ Security فقط ۲۰ مگابایت است). این مقدار در محیط‌های عملیاتی و بویژه برای اهداف فارنزیک کافی نیست و باعث می‌گردد لاگ‌ها خیلی سریع بازنویسی و حذف شوند. جدول ۱ حداقل حجم پیشنهادی را برای کلاینت و سرورها نمایش می‌دهد.

جدول ۱: حداقل حجم پیشنهادی برای انواع لاگ

نوع لاگ	حداقل حجم برای سرورها به کیلوبایت	حداقل حجم برای کلاینت‌ها به کیلوبایت	توضیحات
Application	۲۰۹۷۱۵۲ (۲ گیگابایت)	۱۰۴۸۵۷۶ (۱ گیگابایت)	لاگ برنامه‌ها و نرم‌افزارهایی مثل آنتی‌ویروس یا SQL Server
Security*	۸۳۸۸۶۰۸ (۸ گیگابایت)	۴۱۹۴۳۰۴ (۴ گیگابایت)	حیاتی‌ترین لاگ برای فارنزیک؛ شامل ورود/خروج، پردازش‌ها و تغییرات امنیتی
Setup	۵۲۴۲۸۸ (۵۱۲ مگابایت)	۲۶۲۱۴۴ (۲۵۶ مگابایت)	مربوط به نصب ویندوز و آپدیت‌ها؛ کم‌کاربردتر
System	۲۰۹۷۱۵۲ (۲ گیگابایت)	۵۲۴۲۸۸ (۵۱۲ مگابایت)	ثبت خطاهای سیستمی، سرویس‌ها و درایورها

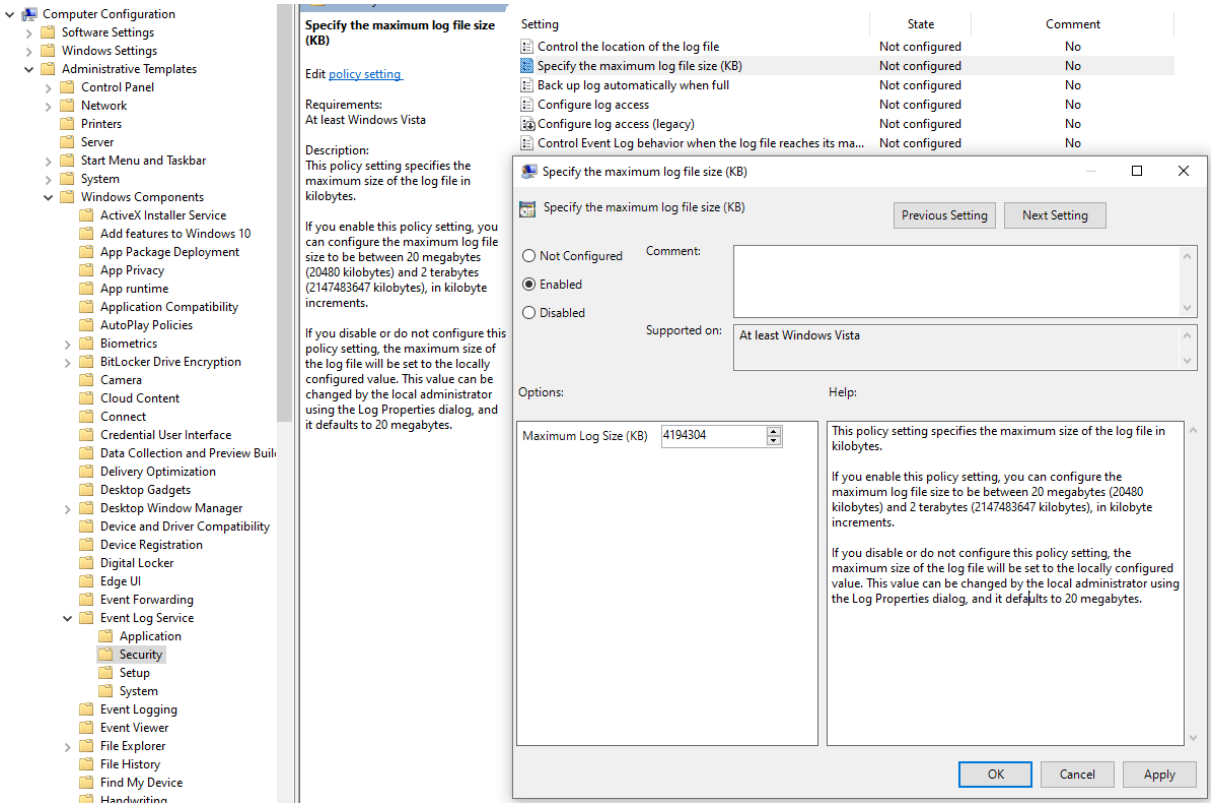
*با توجه به اهمیت بالای لاگ Security برای سرورها، پیشنهاد می‌گردد که حجم این نوع لاگ را سرورها ۱۶۷۷۷۲۱۶ (۱۶ گیگابایت) در نظر بگیرید.

برای افزایش حجم لاگ‌ها مراحل زیر را دنبال نمایید.

- در Group Policy به مسیر زیر بروید.
  - Computer Configuration → Administrative Templates → Windows Components → Event Log Service
- در این بخش پوشه‌هایی برای هر لاگ وجود دارد (Application, Security, Setup, System).
- در هر پوشه گزینه زیر را فعال نمایید.
  - Specify the maximum log file size (KB) → Enabled
- در قسمت Maximum log file size (KB) مقدار مورد نظر را بر اساس جدول جدول ۱ وارد کنید. به عنوان مثال برای Security Log عدد ۴۱۹۴۳۰۴ (یعنی ۴ گیگابایت) را برای کلاینت‌ها وارد نمایید.

با این روش، همه سیستم‌هایی که این Group Policy را دریافت می‌کنند بصورت یکسان حجم لاگ‌ها را افزایش خواهند داد.

دقت کنید که مراحل را برای هر چهار نوع لاگ Application, Security, Setup, System انجام دهید. در شکل ۱ نحوه افزایش لاگ Security نمایش داده شده است.



شکل ۱: افزایش لاگ Security برای کلاینت‌ها

فعال کردن لاگ‌های PowerShell

برای PowerShell سه نوع لاگ زیر بایستی فعال شوند تا فعالیت‌های مشکوک (مثل اجرای اسکریپت یا دستورات رمزگذاری شده) ثبت گردند.

- Module Logging
- Script Block Logging
- Transcription

در ادامه نحوه فعال کردن هریک توضیح داده شده است.

فعال کردن Module Logging برای PowerShell

در پاورشل، ماژول[1] یک بسته[2] شامل دستورات، توابع، کلاس‌ها و فایل‌های کمکی است که قابلیت‌های جدیدی به محیط PowerShell اضافه می‌کند. به عبارتی می‌توان آنها را همانند کتابخانه‌ها[3] در زبان‌های برنامه‌نویسی یا مثل Add-ons / Plugins برای نرم‌افزارها دانست. برای مشاهده تمامی ماژول‌های PowerShell می‌توانید از دستور زیر در PowerShell استفاده نمایید.

- Get-Module -ListAvailable | select-object Name

برخی از قابلیت‌های لاگ‌گیری PowerShell بر روی ماژول‌ها متمرکزند و زمانیکه Module Logging برای یک ماژول فعال شود، هربار که این ماژول اجرا شود جزئیات آن در لاگ‌ها ثبت می‌گردد. در جدول ۲ مهمترین ماژول‌هایی که بایستی لاگ آنها ثبت گردد مشخص شده‌اند.

جدول ۲: مهمترین ماژول‌های PowerShell در موضوع امنیت

نام ماژول	کاربرد اصلی
ActiveDirectory	اجرای دستورهای مربوط به مدیریت دامنه مثل ایجاد، تغییر یا حذف کاربران و گروه‌ها، مدیریتOU ها و کنترل دسترسی‌ها در محیط دامین.
NetTCPIP	پیکربندی تنظیمات شبکه شامل IP ، Gateway، Routeو Interface ها؛ تغییر این موارد می‌تواند روی ارتباطات شبکه سیستم تأثیر مستقیم بگذارد.
DnsClient	مدیریت و تغییر تنظیمات DNS سیستم، افزودن یا حذف رکوردهای DNS و مشخص کردن سرورهای DNS مورد استفاده.
BitsTransfer	انتقال فایل‌ها از طریق BITS (Background Intelligent Transfer Service) ، شامل دانلود یا آپلود فایل به/از منابع خارجی.
ScheduledTasks	ایجاد، حذف یا تغییر وظایف زمان‌بندی‌شده (Task Scheduler) برای اجرای خودکار برنامه‌ها یا اسکریپت‌ها در زمان مشخص.
NetAdapter	مدیریت کارت‌های شبکه، شامل تغییر تنظیمات کارت شبکه، فعال/غیرفعال‌سازی و مشاهده اطلاعات سخت‌افزار شبکه.
NetSecurity	مدیریت تنظیمات امنیت شبکه مثل Rule های فایروال ویندوز و سیاست‌های IPSec برای کنترل ارتباطات ورودی و خروجی.
CimCmdlets	اجرای دستورها با استفاده از CIM/WMI برای مدیریت منابع سیستم به‌صورت محلی یا از راه دور (مانند پردازش‌ها، سرویس‌ها و سخت‌افزار).
Microsoft.PowerShell.Management	مدیریت اجزای اصلی ویندوز مانند فایل‌ها و فولدرها، سرویس‌ها، رجیستری، Event Logها و متغیرهای محیطی.
Microsoft.PowerShell.Security	کار با تنظیمات امنیتی ویندوز شامل گواهی‌ها(Certificates) ، لیست‌های کنترل دسترسی(ACLs) ، و سیاست‌های امنیتی مرتبط با کاربر یا فایل.

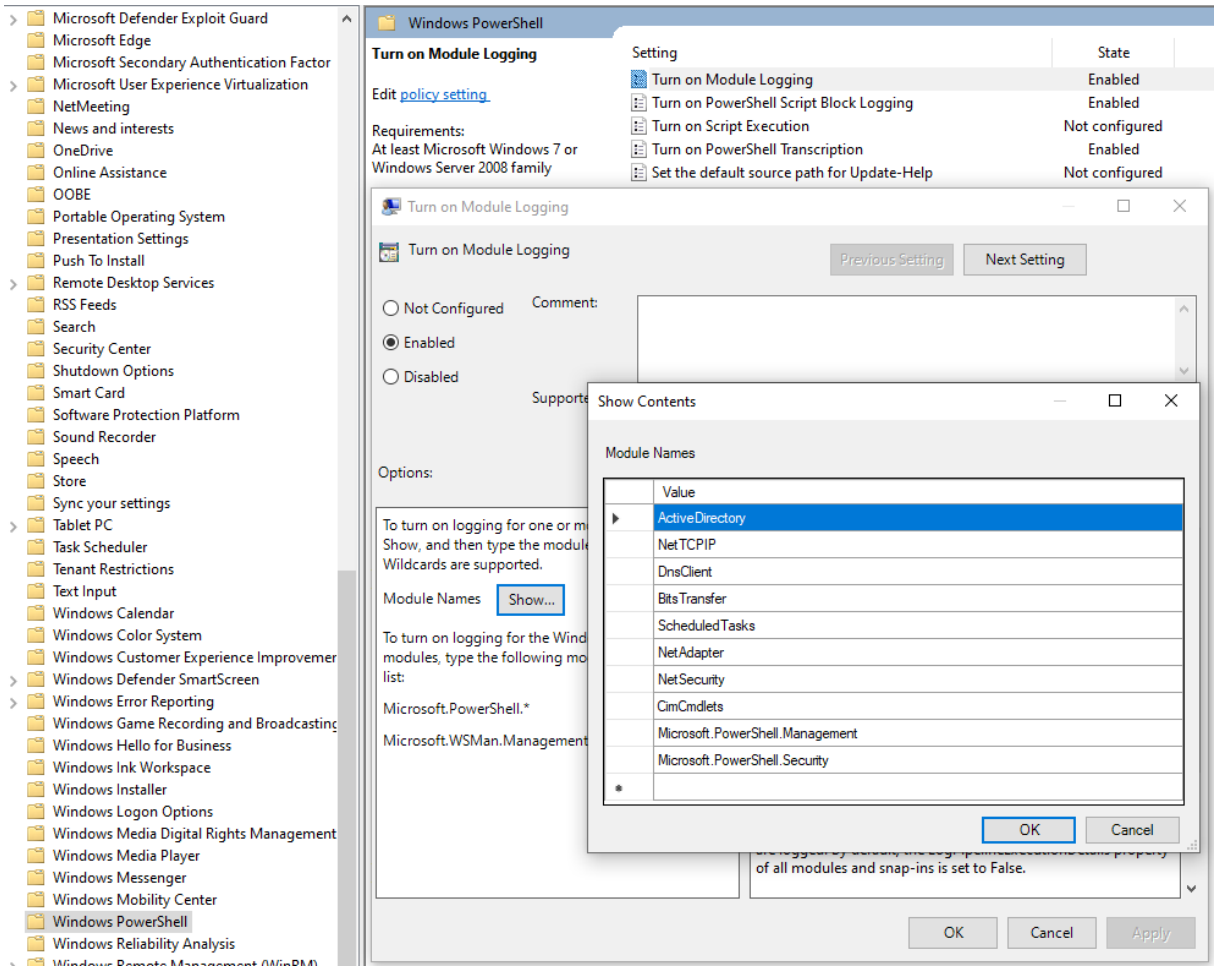
[1] Module
[2] Package
[3] Libraries

برای فعال کردن لاگ Module Logging مراحل زیر را دنبال نمایید.

- در Group Policy به مسیر زیر بروید.
  - Computer Configuration → Administrative Templates → Windows Components → Windows PowerShell
- در این قسمت گزینه زیر را فعال نمایید.
  - Turn on Module Logging → Enabled
- در قسمت Options بر روی دکمه Show کلیک کنید و در پنجره Show Contents ماژول‌های معرفی شده در جدول را مطابق شکل وارد نمایید.

*دقت نمایید که املای صحیح ماژول‌ها را رعایت کنید زیرا در صورت ورود اشتباه، هیچ پیام خطایی نمایان نمی‌گردد اما لاگ ماژول مورد نظر نیز فعال نمی‌شود. در انتها دکمه OK را فشار دهید تا عملیات تایید گردد.

شکل ۲ نمایی از فعال نمودن لاگ Module Logging را نمایش می‌دهد.



شکل ۲: نحوه فعال نمودن لاگ Module Logging

فعال کردن Script Block Logging برای PowerShell

هر دستوری که در PowerShell اجرا شود، ابتدا به صورت یک بلاک دستوری تفسیر می‌گردد. Script Block Logging باعث می‌گردد تمام این بلاک‌های دستوری در لاگ ثبت شوند حتی اگر یک اسکریپت مخرب تلاش کند کد را بصورت داینامیک تولید یا رمزگذاری نماید (به طور مثال با استفاده از Base64)، Script Block Logging نسخه خام (غیر رمز شده) آن را ثبت می‌نماید.

این ویژگی برای شناسایی حملاتی مانند Fileless Malware یا Obfuscated Scripts بسیار حائز اهمیت است. برای فعال کردن لاگ Script Block Logging مراحل زیر را دنبال نمایید.

- در Group Policy به مسیر زیر بروید.
  - Computer Configuration → Administrative Templates → Windows Components → Windows PowerShell
- در این قسمت گزینه زیر را فعال نمایید.
  - Turn on PowerShell Script Block Logging → Enabled
- در قسمت Options، گزینه Log script block invocation start/stop events را فعال نمایید و در نهایت با فشردن دکمه OK، مراحل را تایید نمایید.

فعال کردن Transcription برای PowerShell

فعال کردن Transcription باعث می‌گردد تمام دستورات PowerShell و خروجی آنها در یک فایل متنی ذخیره شوند. فایل لاگ شامل اطلاعاتی مانند زمان، کاربر اجراکننده، نام کامپیوتر و متن کامل دستورات و نتایج آنها است. بدین ترتیب مشخص می‌گردد چه فردی چه دستوری را در PowerShell اجرا کرده است.

برای فعال کردن لاگ Transcription مراحل زیر را دنبال نمایید.

- در Group Policy به مسیر زیر بروید.
  - Computer Configuration → Administrative Templates → Windows Components → Windows PowerShell
- در این قسمت گزینه زیر را فعال نمایید.
  - Turn on PowerShell Transcription → Enabled
- در قسمت Options می‌توانید مسیر ذخیره‌سازی فایل‌های لاگ را از طریق گزینه Transcript output directory مشخص نمایید. مسیر ذخیره لاگ به صورت پیش‌فرض در مسیر C:\Users\<Username>\Documents قرار دارد.
- در نهایت با فشردن دکمه OK، مراحل را تایید نمایید.

فعال کردن Audit Logها در ویندوز

لاگ‌های حسابرسی (Audit Logs) در ویندوز نقش حیاتی در پایش امنیتی و تحلیل فارنزیک دارند. این لاگ‌ها اطلاعات دقیقی از فعالیت‌های کاربران و سیستم ارائه می‌دهند از جمله ورود و خروج به سیستم، ایجاد یا تغییر حساب‌های کاربری، اجرای پردازش‌ها، تغییر در تنظیمات امنیتی و دسترسی به فایل‌ها و منابع حساس.

در حالت پیش‌فرض بسیاری از این لاگ‌ها غیرفعال هستند، به همین دلیل در صورت وقوع حادثه امنیتی بخش زیادی از ردپاهای مهاجم یا حتی خطاهای سیستمی مهم ثبت نمی‌شوند. فعال‌سازی درست Audit Logها باعث می‌شود:

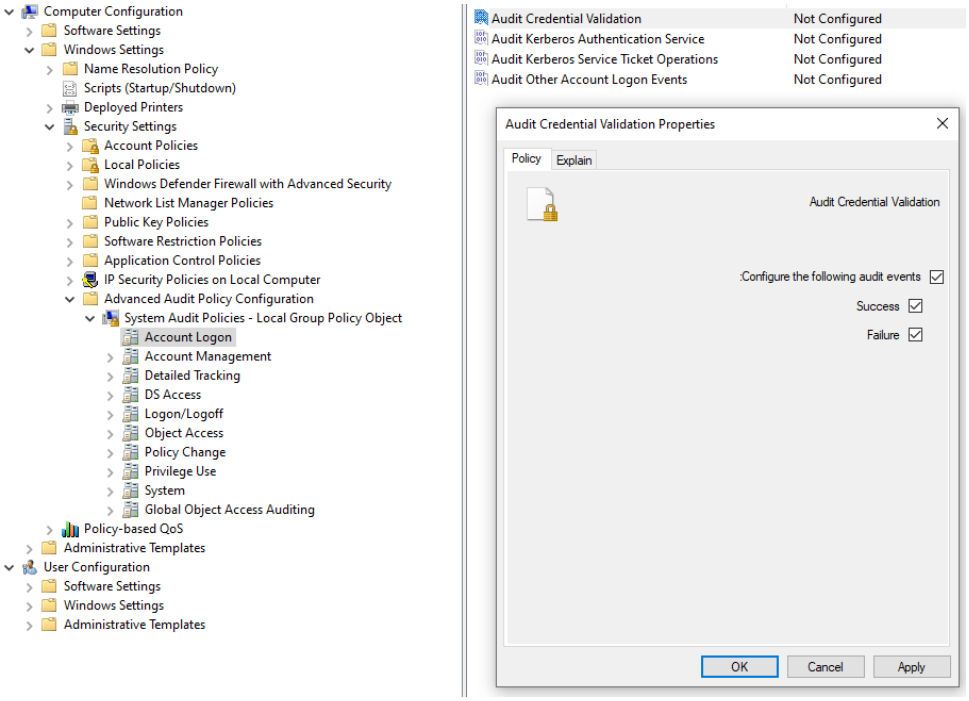
- رویدادهای حیاتی برای تشخیص نفوذ و حملات ثبت شوند.
- امکان بازسازی فعالیت مهاجم در هنگام فارنزیک فراهم شود.
- تغییرات مهم در حساب‌های کاربری، سیاست‌ها یا دسترسی‌ها شفاف و مستند باشند.
- تیم امنیتی بتواند پایش مداوم و پاسخ سریع به رخدادها داشته باشد.

بنابراین، فعال‌سازی و پیکربندی صحیح Audit Logها یکی از گام‌های کلیدی در امن‌سازی ویندوز و آماده‌سازی سیستم برای تحلیل‌های بعدی است.

برای فعال‌سازی Audit Logها از طریق Group Policy به روش زیر عمل نمایید.

- در Group Policy به مسیر زیر بروید.
  - Computer Configuration → Windows Settings → Security Settings → Advanced Audit Policy Configuration → System Audit Policies

در این بخش دسته‌های مختلفی مانند Account Logon، Account Management، Detailed Tracking و غیره نمایش داده می‌شوند. با باز کردن هر دسته می‌توانید زیرگروه‌ها را مشاهده کرده و برای هرکدام تعیین کنید که رویدادهای Success، Failure یا هر دو ثبت شوند. جدول زیر تنظیمات لازم برای هر دسته را نمایش می دهد. در شکل ۳ نمایی از Advanced Audit Policy Configuration نمایش داده شده است.



شکل ۳: Advanced Audit Policy Configuration

در ادامه مشخص شده است که برای هر دسته چه زیرگروه‌ها و برای آنها چه رویدادهای (Success، Failure) فعال گردند.

Account Logon

- Audit Credential Validation → Success & Failure
- Audit Kerberos Authentication Service → Success & Failure
- Audit Kerberos Service Ticket Operations → Success & Failure

این دسته امکان کشف لاگین‌های جعلی، حملات Pass-the-Hash و تلاش‌های مشکوک برای ورود به دامنه را فراهم می‌کند.

Logon/Logoff

- **Audit Logon** → Success & Failure
- **Audit Logoff** → Success
- **Audit Special Logon** → Success
- **Audit Other Logon/Logoff Events** → Success & Failure
- **Audit Network Policy Server** → Success & Failure

این دسته امکان تشخیص ورودهای غیرمجاز (مثلاً RDP مشکوک) و ردیابی زمان و محل ورود کاربران را فراهم می‌کند.

Account Management

- Audit User Account Management → Success & Failure
- Audit Computer Account Management → Success & Failure
- Audit Security Group Management → Success & Failure
- Audit Distribution Group Management → Success & Failure
- Audit Application Group Management → Success & Failure

این دسته امکان شناسایی ایجاد یا حذف حساب‌های غیرمجاز و اضافه شدن ناگهانی کاربران به گروه‌های با دسترسی بالا را فراهم می‌کند.

DS Access (Domain Controller)

*این دسته برای سیستم‌هایی است که عضو دامنه هستند فعال شود:

- Audit Directory Service Access → Success & Failure
- Audit Directory Service Changes → Success & Failure

این دسته امکان کشف تغییرات مشکوک در Active Directory، مثل ایجاد حساب کاربری مخفی یا تغییر مجوزها را فراهم می‌کند.

Object Access

- Audit File Share → Success & Failure
- Audit File System → Success & Failure
- Audit Registry → Success & Failure
- Audit Removable Storage → Success & Failure
- Audit Filtering Platform Packet Drop / Connection → Success & Failure

این دسته امکان کشف دسترسی غیرمجاز به فایل‌های حساس، تغییر در رجیستری و کپی داده‌ها روی USB را فراهم می‌کند.

Policy Change

- Audit Audit Policy Change → Success & Failure
- Audit Authentication Policy Change → Success & Failure
- Audit Authorization Policy Change → Success & Failure

این دسته امکان شناسایی تغییرات غیرمجاز در سیاست‌های امنیتی، مثل غیرفعال کردن فایروال یا تغییر Audit Policy را فراهم می‌کند.

Privilege Use

- Audit Sensitive Privilege Use → Success & Failure

این دسته امکان تشخیص استفاده یا سوءاستفاده از دسترسی‌های ویژه توسط مهاجم را فراهم می‌کند.

Detailed Tracking

- Audit Process Creation → Success
- Audit Process Termination → Success
- Audit DPAPI Activity → Failure
- Audit RPC Events → Success & Failure

این دسته امکان ردیابی دقیق اجرای پردازش‌ها و دستورات، از جمله بدافزارها یا اسکریپت‌های مشکوک رو فراهم می‌کند.

System

- Audit Security System Extension → Success & Failure
- Audit System Integrity → Success & Failure
- Audit IPSec Driver / Other System Events → Success & Failure

این دسته امکان شناسایی تلاش برای خاموش کردن سرویس‌های امنیتی، دستکاری سیستم یا تغییرات غیرعادی در سطح کرنل را فراهم می‌کند.

Global Object Access Auditing

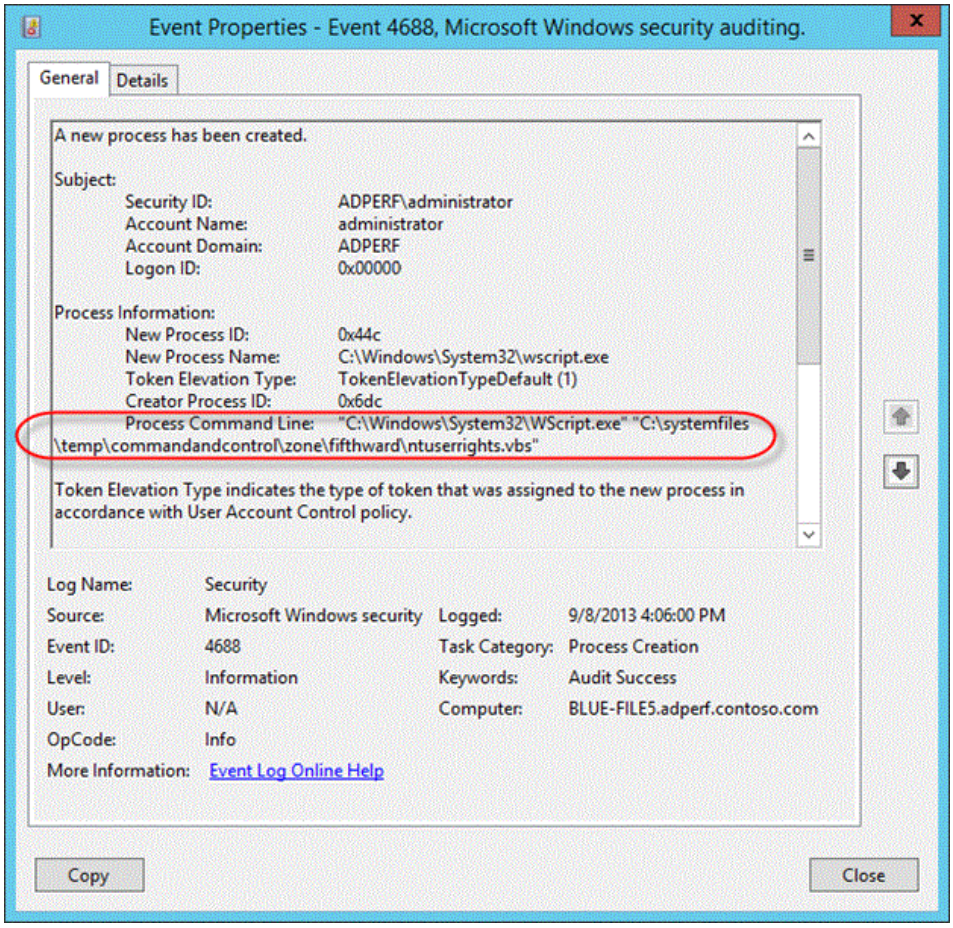
قابلیت Global Object Access Auditing باعث می‌گردد تمامی دسترسی‌ها به فایل‌ها (File System) و کلیدهای رجیستری (Registry Keys) در کل سیستم ثبت گردند. بعبارت دیگر، برخلاف NTFS Auditing که لاگ مربوطه تنها برای پوشه‌های مشخص شده فعال می‌گردد این قابلیت باعث می‌شود لاگ مربوط به هر نوع عملیات برروی فایل و رجیستری در کل سیستم ثبت شود. ثبت مداوم رخدادهای دسترسی به فایل‌ها و رجیستری می‌تواند باعث ایجاد مشکلات زیر شود.

- پرشدن سریع حجم لاگ Security و درنتیجه ازدست رفتن لاگ‌های قدیمی به دلیل بازنویسی لاگ‌های جدید بر روی آنها.
- کاهش محسوس کارایی سیستم.

به همین دلیل، توصیه می‌شود Global Object Access Auditing فقط در شرایط خاص مثلا برای سناریوی تحلیل رخداد که نیاز به ردیابی دقیق تمام دسترسی به فایل‌ها را دارد فعال شود..

فعال‌سازی Command Line Auditing

Command Line Auditing در ویندوز قابلیتی است که باعث می‌شود وقتی یک فرآیند (Process) در سیستم ایجاد می‌شود، علاوه بر نام فایل اجرایی (مثلاً cmd.exe یا powershell.exe) آرگومان‌ها و سوئیچ‌های خط فرمان که همراه آن اجرا شده‌اند هم در لاگ‌های امنیتی ثبت شوند. شکل ۴ نحوه نمایش آن را نشان می‌دهد.



شکل ۴: نحوه نمایش Command Line در لاگ ایجاد یک فرآیند

برای فعال‌سازی Command Line Auditing مراحل زیر را دنبال نمایید.

- در Group Policy به مسیر زیر بروید.

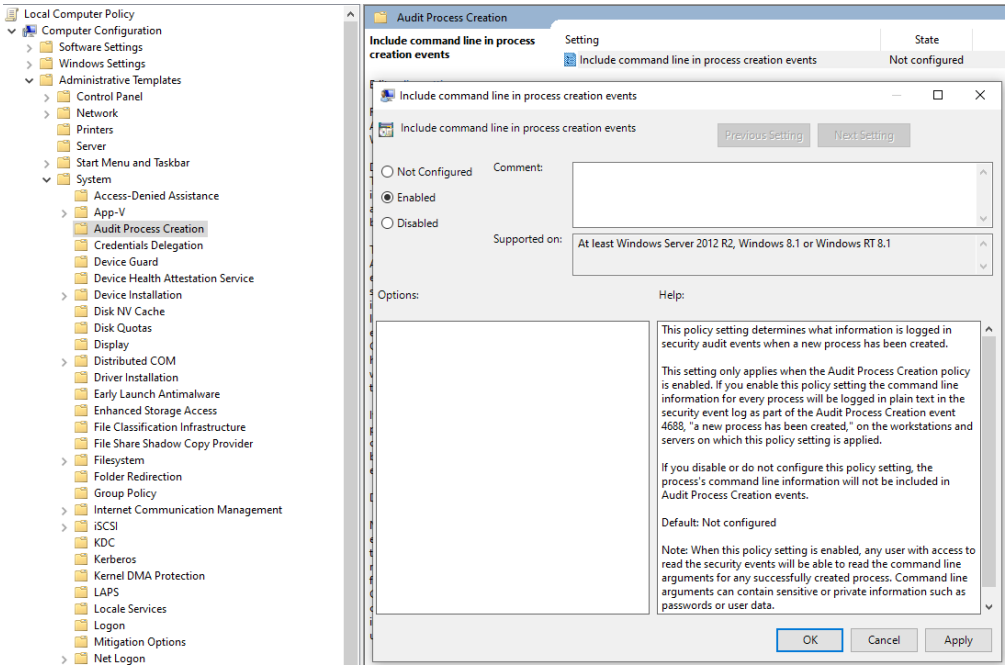
▪ Computer Configuration → Administrative Templates → System → Audit Process Creation

- در این قسمت گزینه زیر را فعال نمایید.

▪ Include command line in process creation events → Enabled

از این پس با اجرای هر فرآیند علاوه بر نام آن، Command Line مربوط به آن نیز در لاگ Security (Event ID 4688) ذخیره می‌گردد.

در شکل ۵ نمایی از نحوه فعال‌سازی Command Line Auditing نمایش داده شده است.



شکل ۵: فعال‌سازی Command Line Auditing

تفاوت Basic Audit Policy و Advanced Audit Policy Configuration و رفع تداخل آن‌ها

در ویندوز دو روش برای تنظیمات حسابرسی (Audit) وجود دارد:

- Basic Audit Policy
  - از مسیر: Local Security Policy → Local Policies → Audit Policy
  - این روش قدیمی‌تر است و تنها ۹ گزینه کلی دارد (شامل Logon/Logoff، Object Access و غیره). تنظیمات آن در سطح Category انجام می‌شود و جزئیات کمی دارد.
- Advanced Audit Policy Configuration
  - از مسیر: Group Policy → Advanced Audit Policy Configuration
  - این روش جدیدتر (از ویندوز ۷ و Server 2008 R2 به بعد) است.
  - تنظیمات در سطح Subcategory انجام می‌شود (بیش از ۵۰ زیرگروه مثل Process Creation، Logoff، Removable Storage و غیره را داراست).
  - بسیار دقیق‌تر و توصیه شده است.

مشکل تداخل

اگر همزمان هم Basic Audit Policy و هم Advanced Audit Policy Configuration فعال باشند در برخی شرایط ویندوز فقط Basic را اعمال می‌کند و Advanced را نادیده می‌گیرد، در نتیجه این ابهام بوجود می‌آید Advanced فعال است، ولی لاگ‌ها طبق Basic جمع‌آوری می‌شوند. همین موضوع باعث سردرگمی و از دست رفتن لاگ‌های حیاتی می‌شود.

روش رفع تداخل

برای رفع تداخل بایستی در ویندوز تنظیماتی اعمال گردد که ویندوز Advanced Audit را در اولویت قرار دهد. برای اینکار مراحل زیر را دنبال نمایید.

- در Group Policy به مسیر زیر بروید.
  - Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options
- در این قسمت گزینه زیر را فعال نمایید.
  - Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings → Enabled

در **Error! Reference source not found.** نمایی از نحوه اجبار ویندوز به استفاده از Advanced Audit نمایش داده شده است.